Veeam ONE

Version 13

User Guide

March, 2026

© 2026 Veeam Software.

All rights reserved. All trademarks are the property of their respective owners.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form by any means, without written permission from Veeam Software (Veeam). The information contained in this document represents the current view of Veeam on the issue discussed as of the date of publication and is subject to change without notice. Veeam shall not be liable for technical or editorial errors or omissions contained herein. Veeam makes no warranties, express or implied, in this document. Veeam may have patents, patent applications, trademark, copyright, or other intellectual property rights covering the subject matter of this document. All other trademarks mentioned herein are the property of their respective owners. Except as expressly provided in any written license agreement from Veeam, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

NOTE

Read the End User Software License Agreement before using the accompanying software programs. Using any part of the software indicates that you accept the terms of the End User Software License Agreement.

Contents

CONTACTING VEEAM SOFTWARE 19
ABOUT THIS DOCUMENT 20
ABOUT VEEAM ONE 21
Veeam ONE Architecture 23
DEPLOYMENT PLANNING AND PREPARATION 24
Supported Platforms and Applications 25
Deployment Scenarios 28
All-in-One Deployment 29
Custom Deployment 30
System Requirements 32
Limitations 38
Connection Settings 39
Permissions 40
Connection to Veeam Backup & Replication Servers 41
Connection to Veeam Backup for Microsoft 365 Servers 43
Connection to Virtualization Servers 44
Connection to VMware Cloud Director Servers 46
Connection to PostgreSQL 47
Veeam ONE Service Account 48
Connection to Microsoft SQL Server 49
Connection to VM Guest OS 50
Connection to ServiceNow 51
Configuring Permissions to Remotely Access WMI 52
Connection Under UAC 58
Authorizing with Veeam ONE 59
Remote Access 60
Ports 61
Firewall Rules 72
Sizing and Scalability Best Practices 73
System Requirements for Large-Scale Deployment 74
Walkthrough: Deploy and Configure Veeam ONE 80
LICENSING VEEAM ONE 86
Licensed Objects 87
License Types and Packages 89
Installing License 93
Viewing License Information 94
Submitting License Usage Report 99

Updating License 103
License Usage Statistics 105
License Expiration 106
Exceeding License Limit 107
SECURITY GUIDELINES 109
General Security Considerations 110
Securing Veeam ONE Infrastructure 112
Veeam ONE Certificates 114
Generating Self-Signed Certificates 115
Importing Certificate from Certificate Store 117
Importing Certificate from PFX Files 118
Using Certificate Signed by Internal CA 119
INSTALLING VEEAM ONE 120
All-in-One Installation 121
Step 1. Launch Splash Window 122
Step 2. Select Component 123
Step 3. Accept License Agreements 124
Step 4. Provide License 125
Step 5. Specify Service Account Credentials 126
Step 6. Perform System Configuration Check 127
Step 7. Review Installation Summary 128
Step 8. Select Architectural Components 129
Step 9. Choose Monitoring Database 130
Step 10. Choose Reporting Database 132
Step 11. Choose Data Locations 133
Step 12. Choose Data Collection Mode 135
Step 13. Specify Connection Ports 137
Step 14. Review Installation Summary 139
Step 15. Add Veeam ONE Service Account to Veeam ONE Administrators Group 140
Custom Installation 141
Installing Veeam ONE Server 142
Installing Veeam ONE Web Services 162
Installing Veeam ONE Client 175
Step 1. Launch Splash Window 176
Step 2. Select Component 177
Step 3. Accept License Agreements 178
Step 4. Perform System Configuration Check 179
Step 5. Choose Installation Path 180
Step 6. Specify Veeam ONE Server Name 181
Step 7. Review Installation Summary 182

Step 8. Check Veeam ONE Client Settings 183
Installing Veeam ONE in Unattended Mode 184
Before You Begin 185
Installation Command-Line Syntax 187
Upgrading to Veeam ONE 13 207
Step 1. Launch Splash Window 208
Step 2. Select Component 209
Step 3. Accept License Agreements 210
Step 4. Review Components to Upgrade 211
Step 5. Provide License 212
Step 6. Specify Service Account Credentials 213
Step 7. Perform System Configuration Check 214
Step 8. Choose Reporting Database 215
Step 9. Specify Connection Ports 216
Step 10. Upgrade Analytics Service Agents 217
Step 11. Begin Upgrade 218
Step 12. Change Default Certificate 219
Step 13. Specify Guest OS Credentials for Microsoft Hyper-V VMs 221
Step 14 Apply Available Updates 222
Upgrading Veeam ONE Client 223
Uninstalling Veeam ONE 224
GETTING STARTED WITH VEEAM ONE 225
Accessing Veeam ONE Components 226
Navigating Veeam ONE Web Client 229
Navigating Veeam ONE Client 232
Toolbar and Main Menu 233
Inventory Pane 235
Configuration Issues Pane 242
Information Pane 243
Actions Pane 244
Configuring Notification Settings 246
Step 1. Configure SMTP Server Settings 247
Step 2. Configure Email Notification Settings 251
Step 3. Configure Email Frequency 253
Step 4. Configure SNMP Settings 256
Step 5. Configure ServiceNow Integration 258
Step 6. Configure Syslog Integration 260
Step 7. Review Summary 262
CONFIGURING VEEAM ONE 263
Data Collection 264

Adding Data Source ... 266
Veeam Analytics Service ... 301
Advanced Actions ... 306
Viewing Data Collection Session Details ... 309
Task Sessions ... 311
Reporting Settings ... 313
Customizing Report Branding ... 314
Configuring SSRS Server Settings ... 316
Database ... 318
Veeam Intelligence Settings ... 321
Security ... 322
Veeam ONE Web Client Appearance ... 329
General Configuration Details ... 330
Veeam ONE Client Settings ... 331
General Settings ... 332
Color Settings ... 333
Charts Settings ... 334
Tabs View Settings ... 339
Other Settings ... 342
Veeam ONE Server Settings ... 344
Mail Server Settings ... 345
Notification Policy ... 346
SNMP Traps ... 347
ServiceNow Integration ... 348
Syslog Integration ... 350
Guest OS Credentials ... 352
Monitored Datastores ... 354
Monitored VMs ... 355
Business View ... 356
Login Sessions ... 359
Audit Log ... 360
Banners ... 362
Other Settings ... 363
Choosing Objects to Monitor and Report On ... 365
Choosing VMs and VM Containers to Monitor and Report On ... 366
Choosing Datastores to Report On ... 379
Data Collection Schedule ... 380
Security Groups ... 381
Data Retention ... 384
Changing Veeam ONE Service Account ... 385

VEEAM THREAT CENTER 386
VEEAM INTELLIGENCE 390
ALARMS OVERVIEW 393
JOBS CALENDAR 395
DASHBOARDS 400
Viewing Dashboards 401
Creating Custom Dashboards 403
Step 1. Create Dashboard 404
Step 2. Add Widgets to Dashboard 405
Setting Dashboard Preview Image and Color 407
Managing Dashboard Layout 408
Scheduling Dashboards 409
Managing Dashboard Schedules 410
Viewing Dashboard Delivery Results 411
Cloning Dashboards 412
Sharing Dashboards 413
Modifying Dashboards 415
Deleting Dashboards 416
Managing Widgets 417
Changing Widget Properties 418
Creating a Widget Report 419
Deleting Widgets 420
Predefined Veeam ONE Dashboards 421
Veeam Backup & Replication Dashboard 422
Heatmap 425
Veeam Backup for Microsoft 365 427
Veeam Backup for Microsoft 365 - Security and Audit Overview 429
vSphere Trends 431
vSphere Alarms 432
vSphere Hosts and Clusters 434
vSphere Datastores 436
vSphere VMs 438
vSphere Infrastructure 440
vSphere Capacity Planning 442
Hyper-V Trends 444
Hyper-V Alarms 445
Hyper-V Hosts and Clusters 447
Hyper-V Datastores 449
Hyper-V VMs 451
Hyper-V Infrastructure 453

REPORTS 455
Viewing Reports 456
Date and Time Format in Reports 459
Saving Reports 460
Modifying Reports 461
Organizing Reports 462
Creating Folders 463
Renaming Folders 464
Deleting Folders 465
Moving Reports 466
Scheduling Reports 467
Scheduling Delivery for Multiple Reports 468
Managing Report Schedules 469
Viewing Scheduled Report Delivery Results 470
Cloning Reports 471
Deleting Reports 472
Sharing Reports 473
Exporting and Importing Reports 475
Predefined Veeam ONE Reports 477
Active Checkpoints 478
Active Snapshots 480
Agent Backup Job and Policy History 481
Alarms Current State Overview (Hyper-V) 482
Alarms Current State Overview (vSphere) 484
Alarms Overview (Hyper-V) 485
Alarms Overview (vSphere) 489
Backup Alarms Overview 490
Backup Billing 491
Backup Copy Job 493
Backup Infrastructure Assessment 495
Backup Infrastructure Audit 500
Backup Infrastructure Custom Data 501
Backup Inventory 502
Backup Objects Change Tracking 504
Backup Security and Compliance 505
Backup SLA Compliance (Veeam Backup for Microsoft 365) 506
Backups on Repository 507
Backups on Tape 508
Capacity Planning (Hyper-V) 509
Capacity Planning (vSphere) 513

Capacity Planning for Backup Repositories 515
Catalogs Overview 516
CDP SLA Compliance 517
Cloud Connect Inventory 519
Cloud Connect Replication Provisioning 521
Cloud Connect User Report (Backup) 523
Cloud Connect User Report (Replication) 524
Cluster Configuration (Hyper-V) 525
Cluster Configuration (vSphere) 527
Cluster Hosts Performance 528
Cluster Performance 529
Computer Backup Status 530
Computers with no Archive Copy 531
Configuration Assessment 533
Current Backup Alarms State Overview 539
Custom Infrastructure 540
Data Change Rate History 541
Data Sovereignty Overview 543
Data Sovereignty Violations 544
Database Log Protection History 545
Database Processing Verification 547
Datastore Capacity 548
Datastore Configuration (Hyper-V) 549
Datastore Configuration (vSphere) 551
Datastore Performance 552
Datastore Performance Assessment 556
Datastore Space Usage History 558
Delegated Restore Permissions Overview 559
Exported Tapes 560
Failover Cluster Performance 561
Garbage Files 565
GFS Backup Files 566
Guest Disk Free Space (Hyper-V) 567
Guest Disk Free Space (vSphere) 571
Host Configuration (Hyper-V) 573
Host Configuration (vSphere) 576
Host Configuration Chargeback 577
Host Failure Modelling (Hyper-V) 579
Host Failure Modelling (vSphere) 582
Host Performance (Hyper-V) 583

Host Performance (vSphere) 587
Host Resource Usage Chargeback 588
Host Uptime (Hyper-V) 594
Host Uptime (vSphere) 596
How Many More VMs Can be Provisioned 597
Hyper-V Custom Performance 599
Hyper-V Raw Performance Data 601
Hypervisor Version 603
Idle Templates 604
Idle VMs (Hyper-V) 605
Idle VMs (vSphere) 609
Immutable Workloads 611
Inefficient Datastore Usage 613
Infrastructure Changes Audit 614
Infrastructure Changes by Object 617
Infrastructure Overview (Hyper-V) 619
Infrastructure Overview (Visio) 623
Infrastructure Overview (vSphere) 627
Inventory 628
Job Configuration Change Tracking 629
Job Configuration Dump 630
Job Data Exclusions 631
Job History 632
Job History (Veeam Backup for Microsoft 365) 633
Latest Job Status 634
Latest Job Status (Veeam Backup for Microsoft 365) 635
Local Datastore Performance 636
Malware Detection 639
Multiple Clusters Performance 640
Multiple Organizations vDC Performance 641
Multiple vApps Performance 645
Organization Configuration 649
Organization VDC Performance 653
Orphaned VM Snapshots 657
Orphaned VMs 658
Over-Provisioned Backup Repositories 659
Over-Provisioned Datastores (Hyper-V) 660
Over-Provisioned Datastores (vSphere) 662
Oversized VMs (Hyper-V) 663
Oversized VMs (vSphere) 665

Performance Assessment 667
Permissions by Object 672
Permissions by User 673
Powered Off VMs (Hyper-V) 674
Powered Off VMs (vSphere) 676
Protected Cloud Instances 678
Protected Computers 680
Protected Files and Object Storage 682
Protected Objects (Veeam Backup for Microsoft 365) 684
Protected VMs 685
Protected VMs (KVM Environments) 687
Protected VMs (Nutanix AHV) 688
Protected VMs Job Schedule 689
Provider VDCs Performance 690
Recovery Verification Overview 694
Replica Billing 695
Report Builder 697
Resource Pool and vApp Performance 698
Restore Operator Activity 699
Restore Operator Activity (Veeam Backup for Microsoft 365) 700
Scale-Out Backup Repository Configuration 702
Tape Backup Jobs 703
Tape GFS Backup Files 704
Tape GFS Configuration 705
Tape Media Retention Period 706
Tape Vaults Overview 707
Tenants Backup Compatibility 709
Undersized VMs (Hyper-V) 710
Undersized VMs (vSphere) 712
Unmapped Datastore LUNs 715
vApp Configuration 716
vApp Performance 719
Veeam Backup Files Growth 723
Verified VMs 724
VM Backup Compliance Overview 725
VM Change Rate Estimation (Hyper-V) 726
VM Change Rate Estimation (vSphere) 728
VM Configuration Assessment 730
VM Configuration Chargeback 733
VM Daily Protection Status 737

VM Failover Plan Overview 739
VM Performance (Hyper-V) 741
VM Performance (VMware Cloud Director) 743
VM Performance (vSphere) 744
VM Performance Chargeback 745
VM Uptime (Hyper-V) 749
VM Uptime (VMware Cloud Director) 751
VM Uptime (vSphere) 753
VMs Backed Up by Multiple Jobs 755
VMs Configuration (Hyper-V) 756
VMs Configuration (vSphere) 760
VMs Growth (Hyper-V) 761
VMs Growth (vSphere) 763
VMs with no Archive Copy 764
vSphere Custom Performance 766
vSphere Raw Performance Data 769
Windows Cluster Shared Volume Performance 772
Workload Protection History 777
DEPLOYMENT PROJECTS 779
Getting Started with Deployment Projects 781
Creating Deployment Projects 782
Step 1. Launch Add Deployment Project Wizard 783
Step 2. Specify Deployment Project Name and Description 784
Step 3. Specify Deployment Infrastructure 785
Step 4. Define Project Scenarios 786
Adjusting Performance Thresholds 792
Calculating Deployment Projects 793
Viewing Deployment Project Report 794
Completing Deployment Projects 797
Modifying Deployment Projects 798
Deleting Deployment Projects 799
Deployment Project Statuses 800
SCHEDULING 801
Managing Delivery Schedules 808
MULTI-TENANT MONITORING AND REPORTING 809
How Access to Virtual Infrastructure Objects is Restricted 810
Permissions and Security Groups 811
Functional Restrictions 814
Configuring Access for Users with Restricted Permissions 815
Step 1. Check Veeam ONE Security Group Membership 816

Step 2. Check Requirements to User Account 817
Step 3. Assign Permissions on Infrastructure Inventory Objects 819
Step 4. Log in to Veeam ONE as User with Restricted Permissions 820
Reports for Users with Restricted Permissions 821
VEEAM BACKUP & REPLICATION MONITORING 825
Veeam Intelligent Diagnostics 826
Managing Veeam Analytics Service 828
Managing Signatures 829
Performing Log Analysis 830
Veeam Backup & Replication Summary Dashboards 832
Backup Infrastructure Summary 833
Backup Repositories Overview 835
Backup Repository Summary 837
Backup Proxies Overview 844
Backup Proxy Summary 850
WAN Accelerators Overview 855
WAN Accelerator Summary 857
Tape Servers Overview 859
Tape Server Summary 860
Cloud Repositories Overview 861
Cloud Repository Summary 863
Cloud Gateways Overview 865
Cloud Gateway Pool Summary 867
Cloud Gateway Summary 868
Veeam Backup & Replication Alarms 870
Data Protection 871
Virtual Machines 872
Computers 876
Unstructured Data 879
Databases 884
Networks 888
Veeam Backup & Replication Performance Charts 890
CPU Performance Chart 891
Memory Performance Chart 892
Disk Performance Chart 893
Network Performance Chart 894
Cache Performance Chart 895
Data Transfer 896
Protected Data 898
Virtual Machines 899

Computers 900
Unstructured Data 901
Veeam Backup & Replication Events 902
Top Cloud Tenants 904
Top Cloud Gateways 905
VEEAM BACKUP FOR MICROSOFT 365 MONITORING 906
Veeam Backup for Microsoft 365 Summary Dashboards 908
Veeam Backup for Microsoft 365 Infrastructure Summary 909
Veeam Backup for Microsoft 365 Repositories Overview 911
Veeam Backup for Microsoft 365 Repository Summary 914
Veeam Backup for Microsoft 365 Proxies Overview 918
Veeam Backup for Microsoft 365 Proxy Summary 920
Veeam Backup for Microsoft 365 Proxy Pools Summary 922
Veeam Backup for Microsoft 365 Alarms 924
Veeam Backup for Microsoft 365 Data Protection 925
Veeam Backup for Microsoft 365 Performance Charts 927
CPU Performance Chart 928
Memory Performance Chart 929
Disk Performance Chart 930
Network Performance Chart 931
Veeam Backup for Microsoft 365 Protected Data 932
Veeam Backup for Microsoft 365 Events 933
VMWARE VSPHERE MONITORING 934
VMware vSphere Summary Dashboards 935
VMware vSphere Infrastructure Summary 936
Host Summary 938
Virtual Machine Summary 940
Datastore Summary 942
VMware vSphere Alarms 944
VMware vSphere Performance Charts 945
Overview 947
CPU Performance Chart 948
Memory Performance Chart 950
Network Performance Chart 954
Datastore Performance Chart 957
Virtual Disks Performance Chart 960
Storage Path Performance Chart 961
Storage Adapter Performance Chart 963
Disk Space Chart 965
Disk I/O Chart 966

Disk Issues Chart 968
Customizing VMware vSphere Performance Charts 969
VMware vSphere Tasks & Events 974
Viewing Events on Performance Charts 976
VMware vSphere Virtual Machines 978
VMware vSphere Hosts 980
VMware vSphere Datastores 982
VMware vSphere Top Objects 984
Host Hardware State 986
VMware Remote Console (VMRC) 987
VMware vSphere In-Guest Processes 989
VMware vSphere In-Guest Services 991
Launching vSphere Client 993
VMWARE CLOUD DIRECTOR MONITORING 994
VMware Cloud Director Summary Dashboards 995
VMware Cloud Director Infrastructure Summary 996
Provider VDCs Overview 997
Provider VDC Summary 998
Organizations Overview 999
Organization Summary 1000
Organization VDC Summary 1002
vApp Summary 1003
Virtual Machine Summary 1005
VMware Cloud Director Alarms 1007
VMware Cloud Director Performance Charts 1008
VMware Cloud Director Resources 1009
Provider VDCs 1010
Datastore Resources 1011
Host Resources 1012
Organizations 1013
Organization VDCs 1014
vApps 1015
Tracking Blocking Tasks 1016
Troubleshooting Virtual Machine Performance 1017
HYPER-V MONITORING 1018
Microsoft Hyper-V Summary Dashboards 1019
Microsoft Hyper-V Infrastructure Summary 1020
Host Summary 1022
Virtual Machine Summary 1024
Local Storage Summary 1026

SMB Share Summary 1028
Cluster Shared Volume Summary 1029
Microsoft Hyper-V Alarms 1030
Microsoft Hyper-V Performance Charts 1031
Overview 1033
CPU Performance Chart 1034
Memory Performance Chart 1036
Network Performance Chart 1039
Virtual Switch Performance Chart 1042
Cluster/Host Disk Performance Chart 1043
VM Disk Performance Chart 1045
Disk Space Chart 1047
Local Volume Performance Chart 1048
Cluster Shared Volume Disk Performance Chart 1050
SMB Share Disk Performance Chart 1053
HA SMB Performance Chart 1054
Volume Cache Performance Chart 1056
Customizing Microsoft Hyper-V Performance Charts 1057
Microsoft Hyper-V Tasks & Events 1062
Microsoft Hyper-V Virtual Machines 1064
Microsoft Hyper-V Hosts 1066
Microsoft Hyper-V Datastores 1068
Microsoft Hyper-V Top Objects 1070
Microsoft Hyper-V VM Console 1072
Microsoft Hyper-V In-Guest Processes 1074
Microsoft Hyper-V In-Guest Services 1076
BUSINESS VIEW 1078
Configuring Categorization Model 1080
Creating Business View Categories and Groups 1082
Adding Objects to Groups Manually 1099
Importing and Exporting Categorization Data 1102
Editing Business View Categories 1110
Deleting Business View Categories 1111
Business View Monitoring 1112
Business View Summary Dashboards 1113
Business View Alarms 1123
Business View Objects 1124
Business View Performance Charts 1128
Troubleshooting Performance of Categorized Objects 1129
Business View Reporting 1130

WORKING WITH ALARMS 1132
About Alarms 1133
How Alarms Work 1134
Alarm Rules 1135
Alarm Severity 1137
Alarm Assignment Options 1138
Alarm Notification Options 1139
Alarm Remediation Actions 1140
Advanced Alarm Options 1141
Alarm Reports 1142
Configuring Alarms 1143
Creating Alarms 1144
Modifying Alarms 1168
Changing Alarm Assignment Scope 1171
Copying Alarms 1177
Disabling and Enabling Alarms 1178
Deleting Alarms 1179
Exporting and Importing Alarms 1180
Suppressing Alarms 1182
Modeling Alarm Number 1186
Configuring Alarm Notifications 1189
Working with Triggered Alarms 1214
Viewing Triggered Alarms 1215
Resolving Alarms 1218
Acknowledging Alarms 1221
Approving Alarm Remediation Actions 1224
Viewing Alarm History 1226
Exporting Triggered Alarms 1227
Working with Internal Alarms 1228
Viewing Internal Alarms 1229
Configuring Internal Alarms 1230
Predefined Alarms 1231
Veeam Backup & Replication Alarms 1232
Veeam Backup for Microsoft 365 Alarms 1246
VMware vSphere Alarms 1250
Microsoft Hyper-V Alarms 1286
Internal Alarms 1305
Alarm Rules Reference 1314
Alarm Rules for VMware vSphere 1315
Alarm Rules for Microsoft Hyper-V 1322

Alarm Rules for Veeam Backup & Replication 1326
Alarm Rules for Veeam Backup for Microsoft 365 1332
Rules for Internal Alarms 1334
Remediation Actions 1335
APPENDICES 1343
Creating Veeam ONE Database with SQL Script 1344
Data Collection Modes 1346
Scheduling Script Examples 1368
Example A. Copying a Report to Network Shares 1369
Example B. Sorting Reports by Name 1372
About This Document 1377
Veeam ONE Settings Utility 1378
General Settings 1379
Veeam ONE Server Settings 1382
Veeam ONE Web Settings 1387
Scalability 1389
Exporting Logs 1391
Grouping Expressions Syntax 1392
Object Properties 1393
Operators 1404
Functions 1406
Keywords 1410
Constants 1412

Contacting Veeam Software

At Veeam Software we value feedback from our customers. It is important not only to help you quickly with your technical issues, but it is our mission to listen to your input and build products that incorporate your suggestions.

Customer Support

Should you have a technical concern, suggestion or question, visit the Veeam Customer Support Portal to open a case, search our knowledge base, reference documentation, manage your license or obtain the latest product release.

Company Contacts

For the most up-to-date information about company contacts and office locations, visit the Veeam Contacts Webpage.

Online Support

If you have any questions about Veeam products, you can use the following resources:

- Full documentation set: veeam.com/documentation-guides-datasheets.html
- Veeam R&D Forums: forums.veeam.com

About This Document

This guide is intended for IT managers, virtual infrastructure administrators, and other personnel responsible for the product deployment and operation.

This document describes the features included in the Veeam ONE. It also provides usage examples and gives step-by-step instructions that will help you better understand how to install the Veeam ONE and monitor your Veeam Backup infrastructure, services and jobs.

Intended Audience

The document is intended for backup administrators and other IT professionals who plan to deploy and use Veeam Backup & Replication. This guide assumes that you have a good understanding of Veeam Backup & Replication and VMware vSphere.

About Veeam ONE

Veeam ONE is a comprehensive solution developed by Veeam Software for managing virtual and data protection environments. Veeam ONE enables real-time monitoring, business documentation and management reporting for Veeam Backup & Replication, Veeam Backup for Microsoft 365, VMware vSphere, VMware Cloud Director and Microsoft Hyper-V.

Veeam ONE is designed to give IT administrators peace-of-mind to manage every aspect of the modern virtual environment. Every Veeam ONE capability meets a specific business challenge — from monitoring the state of VMs and their performance, generating reports for capacity planning and upgrade purposes, to providing management with transparent and granular views of the virtual infrastructure from a business-oriented perspective.

Veeam ONE incorporates the following software components:

- **Veeam ONE Web Client** provides a set of dashboards and reports that allow you to verify configuration issues, optimize resource allocation and utilization, track implemented changes, plan capacity growth and track whether mission-critical workloads are properly protected in the virtualized datacenter.

  Veeam ONE Web Client — part of an integrated Veeam ONE solution includes detailed reports and dashboards for documentation, analysis, decision-making, chargeback, change tracking, capacity planning and optimization of resource utilization.

- **Veeam ONE Client** is the primary tool used for monitoring the virtual environment, Veeam Backup & Replication and Veeam Backup for Microsoft 365 infrastructures. Main functionality of Veeam ONE Client includes:

  - Manage: viewing and interacting with alarms and monitoring data.
  - Analyze: viewing performance of virtual and backup infrastructure components.
  - Track: monitoring the efficiency of data protection operations.
  - Troubleshoot: identifying and solving key issues and errors in your infrastructure components.
  - Administer: group your virtual infrastructure and administer monitoring settings.

  Veeam ONE Client comes as a part of the integrated Veeam ONE solution. It is the primary tool for monitoring Veeam Backup & Replication, Veeam Backup for Microsoft 365, VMware vSphere, VMware Cloud Director, and Microsoft Hyper-V environments. Veeam ONE Client provides complete visibility of the virtual and backup infrastructure. With Veeam ONE Client, you can monitor the virtual and backup environment from different perspectives:

  - **Data protection monitoring**

    Veeam ONE integrates with Veeam Backup & Replication and Veeam Backup for Microsoft 365 to collect real-time statistics from backup servers. You can track the latest status of data protection operations in the managed environment, receive immediate alarms whenever a potential problem can cause data loss, monitor performance of backup infrastructure components to optimize workloads, and plan capacity of backup infrastructure resources.

  - **Virtual infrastructure monitoring**

    Veeam ONE Client discovers the virtual infrastructure and provides complete visibility of its health status and performance. With predefined and custom alarms, performance charts, dashboards, reports, and an extensive knowledge base, you can always stay aware of the important events and eliminate potential problems in the virtual environment.

- **VMware Cloud Director monitoring**

  Veeam ONE Client provides monitoring capabilities for multi-tenant clouds provisioned with VMware Cloud Director. A comprehensive view of cloud resources allows you to sustain consistent processes for VMware Cloud Director operational framework and maintain established service levels.

- **Business view monitoring**

  Veeam ONE Client allows you to monitor and alert on the virtual infrastructure presented from the business perspective — the perspective that is based on your company needs and priorities. You can group virtual infrastructure objects by such criteria as business unit, department, purpose, SLA and so on.

Veeam ONE Architecture

Veeam ONE relies on client-server architecture to work effectively in environments of any size and complexity. Veeam ONE architecture includes the following structural components:

- **Veeam ONE Server**

  Veeam ONE Server is responsible for collecting data from virtual infrastructure, Veeam Backup & Replication and Veeam Backup for Microsoft 365 servers, and storing this data in the database. As part of Veeam ONE Server, the following components are installed: Veeam ONE Monitoring Service, Veeam ONE Reporting Service, Veeam ONE Error Reporting Service, Veeam ONE Web API and Veeam Analytics service.

- **Veeam ONE Web Services**

  Veeam ONE Web Services enable access to Veeam ONE web server and handle rendering of reports.

- **Veeam ONE Client**

  Veeam ONE Client is a client component of Veeam ONE Server. Veeam ONE Client communicates with the Veeam ONE Server installed locally or remotely.

- **Veeam ONE Monitoring Database**

  Veeam ONE Monitoring database stores data used by product components. The database is hosted on a Microsoft SQL Server that can run remotely, or can be co-installed with other Veeam ONE components.

- **Veeam ONE Reporting Database**

  Veeam ONE Reporting database stores data used by product components. The database is hosted on a PostgreSQL server that can run remotely, or can be co-installed with other Veeam ONE components. Temporary tables are deleted when the Reporter session ends, or after a timeout if the session-based deletion does not occur.

- **Veeam Analytics Service**

  Veeam Analytics service is a component that enables communication with Veeam Backup & Replication servers, collects monitoring and reporting data, and sends remediation commands.

  Veeam Analytics service is automatically deployed when you add Veeam Backup & Replication servers to Veeam ONE to improve data collection performance in large-scale Veeam Backup & Replication infrastructures. For details on Veeam Analytics service, see Veeam Analytics Service and Veeam Intelligent Diagnostics.

  Veeam Analytics service can work in the following modes:

  - **Server**

    In this mode, Veeam Analytics service is responsible for analyzing logs, data and signature updates.

    Veeam Analytics service is included into Veeam ONE installation package and is automatically deployed on the machine running Veeam ONE server during product installation.

  - **Client**

    In this mode, Veeam Analytics service is responsible for collecting logs and data and executing remediation actions on Veeam Backup & Replication servers.

    By default, Veeam Analytics service client is deployed on Veeam Backup & Replication servers when you connect these servers to Veeam ONE.

Veeam ONE architectural components are installed on a single machine, or run on dedicated machines. For details, see Deployment Scenarios.

Deployment Planning and Preparation

Before installing Veeam ONE, check supported virtualization platforms, system requirements, permissions and network ports used for data transmission.

Supported Platforms and Applications

Veeam ONE supports the following virtualization platforms and applications:

VMware vSphere Environment

Specification	Requirement
Platforms	• VMware vSphere 9.0 • VMware vSphere 8.0 (up to Update 3) • VMware vSphere 7.0 (up to 7.0 Update 3) • VMware Cloud on AWS
Software	• vCenter Server 9.0 • vCenter Server 8.0 (optional*) (up to 8.0 Update 3) • vCenter Server 7.0 (optional*) (up to 7.0 Update 3) • Cloud Director 10.4, 10.5, 10.6
Hosts	• ESXi 9.0 • ESXi 8.0 (up to 8.0 Update 3) • ESXi 7.0 (up to 7.0 Update 3) **Note:** Free versions of VMware vSphere ESXi are supported.

NOTE:

- Only English language versions of VMware infrastructures are supported.
- Standalone ESXi hosts are fully supported, so vCenter Server and VMware Cloud Director are optional. However, whenever they are present, we highly recommend that you register both with Veeam ONE.

* Adding VMware vSphere infrastructure using vCenter Server is not mandatory.

Microsoft Hyper-V Environment

Specification	Requirement
Platforms	• Windows Server 2025 • Windows Server 2022 • Windows Server 2019 (including 1809) • Windows Server 2016 (including 1709 and 1803) • AzureStack HCI

Specification	Requirement
Software	• Microsoft System Center 2025 Virtual Machine Manager (optional*) • Microsoft System Center 2022 Virtual Machine Manager (optional*) • Microsoft System Center 2019 Virtual Machine Manager (optional*) • Microsoft System Center 2016 Virtual Machine Manager (optional*) **Notes:** • Semi-Annual Channel (SAC) releases are supported. • Adding Microsoft Hyper-V infrastructure using SCVMM is not mandatory.
Hosts	• Windows Server Hyper-V 2025 • Windows Server Hyper-V 2022 • Windows Server Hyper-V 2019 • Windows Server Hyper-V 2016 **Notes:** • Semi-Annual Channel (SAC) releases are supported. • Free versions of Microsoft Windows Server Hyper-V and Microsoft Hyper-V Server are supported.

* Adding Microsoft Hyper-V infrastructure using SCVMM is not mandatory.

Integration with VMware Cloud Director

Veeam ONE offers monitoring and reporting capabilities for VMware Cloud Director version 10.1, 10.2, 10.3, 10.4 and 10.5.

Integration with Veeam Backup & Replication

Veeam ONE offers monitoring and reporting capabilities for the following versions of Veeam Backup & Replication and Veeam Backup Enterprise Manager:

- Veeam Backup & Replication 13 (recommended)
- Veeam Backup & Replication 12 or later builds (compatible)

Considerations and Limitations

Consider the following limitations when integrating Veeam Backup & Replication with Veeam ONE:

- Veeam ONE is not compatible with Veeam Backup & Replication versions that are higher than the Veeam ONE version you are using. For example, Veeam Backup & Replication version 13 cannot be added to Veeam ONE version 12.3.
- Monitoring and reporting capabilities depend on licenses installed in Veeam Backup & Replication and Veeam ONE. For details on license compatibility, see Compatibility with Veeam Backup & Replication Licenses.
- Infrastructure topology view in Veeam ONE and Veeam Backup & Replication must match. Otherwise, Veeam ONE Web Client might show invalid data for Veeam Backup & Replication reports and dashboards.

- MFA must be disabled for the account under which Veeam Analytics service connects to Veeam Backup & Replication before installing Veeam Analytics service on the Veeam Backup & Replication server. For details, see section Disabling MFA for Service Accounts of the Veeam Backup & Replication User Guide.
- It is recommended to install Veeam Analytics service to improve data collection performance in large-scale Veeam Backup & Replication infrastructures. For details on Veeam Analytics service, see Veeam Intelligent Diagnostics.
- If you move Veeam Backup & Replication servers to a different Veeam ONE instance and delete from the current instance, the Veeam Backup & Replication servers become unregistered for all integrations. To solve this, clear the **Allow Veeam Backup & Replication console to display analytics data** check box in **Connection Settings** and select it in the new Veeam ONE instance. For details, see Changing Server Connection Settings.
- If you remove Veeam Backup & Replication or Veeam Backup Enterprise Manager servers from Veeam ONE, or remove Veeam Backup & Replication servers from Veeam Backup Enterprise Manager monitored by Veeam ONE, the collected historical data will be lost. This occurs even if the server is added back to Veeam ONE or Veeam Backup Enterprise Manager.

Integration with Veeam Backup for Microsoft 365

Veeam ONE offers monitoring and reporting capabilities for the following versions of Veeam Backup for Microsoft 365:

- Veeam Backup for Microsoft 365 7 or later builds
- Veeam Backup for Microsoft 365 8 or later builds

> **NOTE**
>
> Before connecting Veeam Backup for Microsoft 365 server to Veeam ONE make sure that:
>
> - License compatibility requirements are met: Compatibility with Veeam Backup for Microsoft 365 Licenses.
> - REST API requirements are met to connect a Veeam Backup for Microsoft 365 server to Veeam ONE: Configuring REST API and Restore Portal on Separate Machine.

Deployment Scenarios

Veeam ONE supports two deployment scenarios:

- **All-in-one**

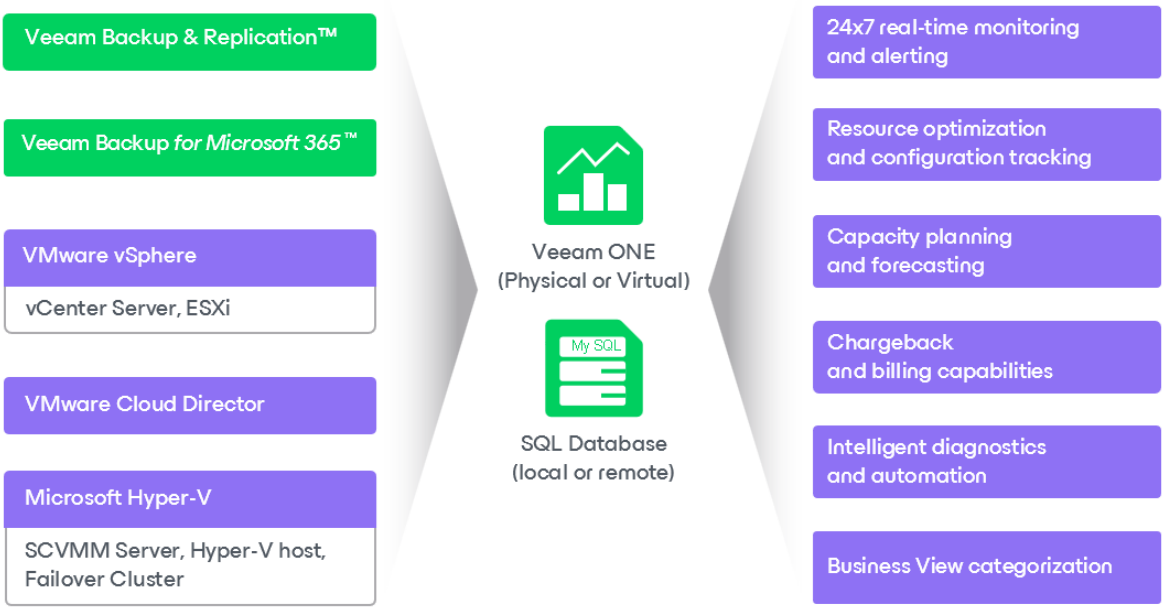
  The all-in-one deployment scenario is ideal if you want to consolidate the entire product functionality in one place by installing all product architectural components on a single machine. This scenario is preferable for small- to medium-scale deployments.

- **Custom**

  The custom deployment scenario is more suitable if you want to separate client/server roles and install product architectural components on different machines. This scenario is recommended for large-scale deployments. For details on large-scale deployment recommendations, see Sizing and Scalability Best Practices.

All-in-One Deployment

The following diagram illustrates the all-in-one Veeam ONE deployment scenario.



In the all-in-one deployment scenario:

- All Veeam ONE architectural components (Veeam ONE Server, Veeam ONE Web Services, Veeam ONE and Veeam ONE agent server) are installed altogether on a single machine (either physical or virtual).
- To store data retrieved from connected servers, a local or remote Microsoft SQL Server instance is required. If you have a Microsoft SQL Server instance that meets Veeam ONE system requirements, you can adopt it for Veeam ONE deployment. Otherwise, you can install a new Microsoft SQL Server instance during the product installation — Veeam ONE setup package includes Microsoft SQL Server 2017 Express Edition.

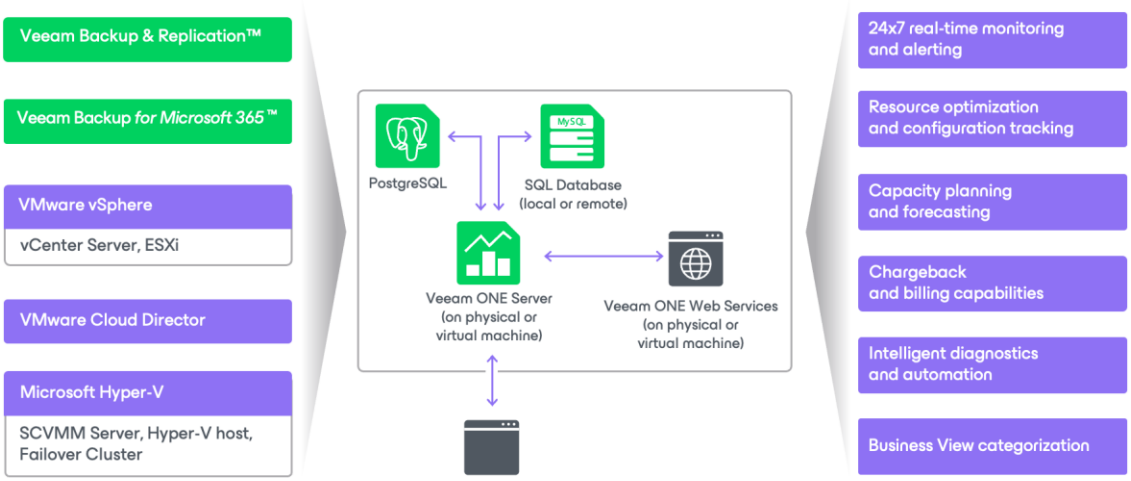
  > **NOTE:**
  > - For production deployments, it is recommended to use a remote Microsoft SQL Server installation. It is also recommended to run Veeam ONE services on a dedicated server. Such distributed installation will improve performance of Veeam ONE services.
  > - If you choose to host Veeam ONE database on Microsoft SQL Server Express, consider is a 10 GB database size limitation for this edition. For details, see Editions and Supported Features for SQL Server.

- To enable multi-user access to real-time performance statistics and configurable alarms, you can additionally install one or more instances of Veeam ONE Client on separate machines. Thus, you will be able to access Veeam ONE functionality either from a local machine or from remote computers.

For instructions on the all-in-one deployment procedure, see All-in-One Installation.

Custom Deployment

The following diagram illustrates the custom Veeam ONE deployment scenario.



The custom deployment scenario relies on a distributed architecture where server and client parts are separated and installed on different machines (physical or virtual). In the custom deployment scenario:

- Veeam ONE Server and Veeam ONE Web Services components are installed on separate machines.
- To enable multi-user access to real-time performance statistics and configurable alarms, you can install one or more instances of Veeam ONE Client on remote machines.
- To store data retrieved from connected servers, a local or remote Microsoft SQL Server instance is required as a supporting system. If you already have a Microsoft SQL Server instance that meets Veeam ONE system requirements, you can adopt it for Veeam ONE deployment. Otherwise, you can install a new Microsoft SQL Server instance during the product installation — Veeam ONE setup package includes Microsoft SQL Server 2017 Express Edition.
- Veeam ONE 13 and above's new reporting engine requires the reporter database to be hosted on a local or remote PostgreSQL instance. You can use an existing PostgreSQL instance that meets Veeam ONE system requirements or install a new instance during product setup. Veeam ONE includes PostgreSQL 17.6 as part of the installation package. For details on Veeam ONE13's new reporting engine, see Viewing Reports.

NOTE:

- For production deployments, it is recommended to use a remote Microsoft SQL Server and PostgreSQL installation. It is also recommended to run Veeam ONE services on a dedicated server. Such distributed installation will improve performance of Veeam ONE services.
- If you choose to host Veeam ONE database on Microsoft SQL Server Express, consider is a 10 GB database size limitation for this edition. For details, see Editions and Supported Features for SQL Server.

The custom installation relies on a client-server model for data collection and communication.

- Server component collects data from virtual environment, Veeam Backup & Replication and Veeam Backup for Microsoft 365 servers and stores this data in the database.
- Veeam ONE Web Services enable access to Veeam ONE web server and handle rendering of reports.
- Veeam ONE Client communicates with Veeam ONE Server directly to obtain real-time virtual infrastructure performance data and data protection statistics.

For a successful Veeam ONE deployment, it is essential that the client components are aware of the Veeam ONE Server and internal Web API location, and can connect to them to retrieve and process data.

For instructions on the custom installation procedure, see Custom Installation.

System Requirements

Before you deploy Veeam ONE, make sure that your environment meets the necessary system requirements.

All-in-One Deployment

If you plan to use the all-in-one deployment scenario, the machine on which you plan to deploy Veeam ONE must meet the following hardware requirements:

- **CPU:** x86-x64 processor, 4 cores minimum*
- **Memory:** 8 GB RAM minimum, 16 GB RAM recommended. Using modern high clock speed memory (DDR3 and higher) and an independent database server improves data processing performance.*
- **Hard Disk Space:** 50 GB for product operation and sufficient disk space for Microsoft SQL Server and Veeam ONE database. Use the Veeam ONE Database Calculator to size application data.

*Regardless of the number of protected workloads, for every connected Veeam Backup & Replication server, additional 0.03 vCPU core and 60 MB RAM are required.

Check OS and software requirements for the following Veeam ONE components:

Veeam ONE Server

Specification	Requirement
OS	Only 64-bit versions of the following operating systems are supported: • Microsoft Windows Server 2025 • Microsoft Windows Server 2022 • Microsoft Windows Server 2019 • Microsoft Windows Server 2016 • Microsoft Windows 11 (Professional and Enterprise editions with minimum supported version 22H2) • Microsoft Windows 10 version 1909 and LTS builds (Minimum supported version 21H2 for LTSC channel and 22H2 for GA) **Note:** Semi-Annual Channel (SAC) releases are supported.

Specification	Requirement
Software	The following components are included in the Veeam ONE setup package and can be installed automatically: • Microsoft ASP.NET Core Shared Framework 8.0.17 • Microsoft Windows Desktop Runtime 8.0.17 • Microsoft .NET Runtime 8.0.17 • Microsoft .NET Framework 4.7.2 • Microsoft System CLR Types for SQL Server 2014 • Microsoft SQL Server 2014 Management Objects • Microsoft Internet Information Services (IIS) 10.0 or later • Microsoft Application Request Routing 3.0 • IIS URL Rewrite Model 2.1 • Microsoft Universal C Runtime To connect SCVMM servers to Veeam ONE, the following software is required: • System Center 2025 Virtual Machine Manager console (for connecting SCVMM 2025 servers) • System Center 2022 Virtual Machine Manager console (for connecting SCVMM 2022 servers) • System Center 2019 Virtual Machine Manager console (for connecting SCVMM 2019 servers) • System Center 2016 Virtual Machine Manager console (for connecting SCVMM 2016 servers) • Microsoft PowerShell 3.0 (required for SCVMM 2016, and SCVMM 2019 consoles) Be sure to install the same versions of the Admin UI and the SCVMM Server, and to update both components to the same update version.
Other	• Windows Management Instrumentation service must be enabled to allow data collection from Veeam Backup & Replication servers. • File and Print Sharing service must be enabled to enable remote Veeam ONE Client connections to the Veeam ONE service.

Microsoft SQL Server for Veeam ONE

> **NOTE**
>
> All versions of Microsoft SQL Server must have a supported compatibility level of 130 or later.

Specification	Requirement
Software	**Microsoft SQL Server (Full and Express Editions):** • Microsoft SQL Server 2025 • Microsoft SQL Server 2022 • Microsoft SQL Server 2019 • Microsoft SQL Server 2017 (Microsoft SQL Server 2017 Express edition without cumulative updates is included in Veeam ONE installation package) • Microsoft SQL Server 2016 • Microsoft Azure SQL Database • Amazon RDS for SQL Server **Reporting Services (optional):** • Microsoft SQL Server Reporting Services 2025 • Microsoft SQL Server Reporting Services 2022 • Microsoft SQL Server Reporting Services 2019 • Microsoft SQL Server Reporting Services 2017 • Microsoft SQL Server Reporting Services 2016

NOTE:

- For production deployment of Veeam ONE, it is recommended to use Microsoft SQL Server Standard Edition or higher and Microsoft SQL Server Reporting Services Standard Edition or higher.
- For large-scale deployments with, it is recommended to use Microsoft SQL Server Standard Edition or higher. For details on large-scale deployment recommendations, see Sizing and Scalability Best Practices.
- For production deployment of Veeam ONE, it is recommended to use Microsoft SQL Server Reporting Services Standard Edition or higher. Note that if you use Microsoft SQL Server Reporting Services Developer, Web or Express Editions, Veeam ONE functionality may be limited.
- Ensure you have sufficient space on disk for Veeam ONE database. The database can quickly grow in size due to a large amount of collected data, or because of Microsoft SQL Server configuration. For details, see KB2210.
- If you choose to host Veeam ONE database on Microsoft SQL Server Express, be informed there is a 10 GB database size limitation for this edition. For details, see Editions and Supported Features for SQL Server.
- You can run Veeam ONE database in Microsoft SQL Server Always ON availability group. For details, see KB2312.
- In order for the Veeam ONE database to be added to the Always ON Availability Group (AOAG), its recovery model must be switched to *Full* mode. Consequently, the database begins generating transaction logs that must be managed because Veeam ONE is designed to operate with a *Simple* recovery model database and does not truncate its transaction logs.
- You can host Veeam ONE database installation on Amazon Web Services Relational Database Service (AWS RDS).
- Veeam ONE supports only .NET version 8.0. Using any .NET version other than 8.0 can result in errors or failure in Veeam ONE.
- Lightweight pooling must be disabled on the SQL Server.

Veeam ONE Reporting Database

Specification	Requirement
Software	**PostgreSQL** Local or remote installation of the following versions: • PostgreSQL 14.x • PostgreSQL 15.x • PostgreSQL 16.x • PostgreSQL 17.x (PostgreSQL 17.6 is included in the Veeam ONE v13 setup) • PostgreSQL 18.x Note - the PostgreSQL instance must have UTF-8 as the default encoding for the database.

Veeam ONE Web Services

Specification	Requirement
Hardware	**CPU**: x86-x64 processor (minimum 2 cores). Using faster multi-core processors improves data processing performance. **Memory**: 2 GB RAM (minimum). Using modern high clock memory (DDR3 and higher) improves data processing performance.
OS	Only 64-bit versions of the following operating systems are supported: • Microsoft Windows Server 2025 • Microsoft Windows Server 2022 • Microsoft Windows Server 2019 • Microsoft Windows Server 2016 • Microsoft Windows 11 (Professional and Enterprise editions with minimum supported version 22H2) • Microsoft Windows 10 version 1909 and LTS builds (Minimum supported version 21H2 for LTSC channel and 22H2 for GA) **Note:** Semi-Annual Channel (SAC) releases are supported.
Software	The following components are included in the Veeam ONE setup package and can be installed automatically: • Microsoft .NET Runtime 8.0.17 • Microsoft ASP.NET Core Shared Framework 8.0.17 • Microsoft Windows Desktop Runtime 8.0.17 • Microsoft .NET Framework 4.7.2 • Microsoft System CLR Types for SQL Server 2014 • Microsoft SQL Server 2014 Management Objects • Microsoft Internet Information Services (IIS) 10.0 or later • Microsoft Application Request Routing 3.0 • IIS URL Rewrite Module 2.1 • Microsoft Universal C Runtime

Veeam ONE Client

Specification	Requirement
OS	Only 64-bit versions of the following operating systems are supported: • Microsoft Windows Server 2025 • Microsoft Windows Server 2022 • Microsoft Windows Server 2019 • Microsoft Windows Server 2016 • Microsoft Windows 11 (Professional and Enterprise editions with minimum supported version 22H2) • Microsoft Windows 10 version 1909 and LTS builds (Minimum supported version 21H2 for LTSC channel and 22H2 for GA) **Note:** Semi-Annual Channel (SAC) releases are supported.
Software	The following components are included in the Veeam ONE setup package and can be installed automatically: • Microsoft Windows Desktop Runtime 8.0.17 • Microsoft Core XML 6.0 Parser and SDK • Microsoft Windows Installer 4.5

Veeam ONE Web Client

Specification	Requirement
Software	• The latest versions of Microsoft Edge, Google Chrome or Mozilla Firefox. Microsoft Edge Legacy is not supported. • The browser must have JavaScript enabled • Microsoft Office 2010, 2013, 2016, 2019, or Microsoft Office 365 • Microsoft Visio 2010, 2013, 2016, 2019 • Any up-to-date PDF viewer • 1280x720 minimum screen resolution.

Custom Deployment

If you plan to use the custom deployment scenario, the machines on which you plan to deploy Veeam ONE components must be sized depending on the managed workloads. For details on hardware recommendations for custom deployments, see System Requirements for Large-Scale Deployment.

Limitations

You cannot install the following Veeam ONE components on a Domain Controller: Veeam ONE Server, Veeam ONE Web Services, Veeam ONE Database, Veeam Analytics service.

> **NOTE:**
>
> Veeam ONE is not currently able to collect guest disk space usage data from Linux VMs running in a Hyper-V environment.

Connection Settings

To ensure that Veeam ONE can update the license and Veeam Intelligent Diagnostics signatures and send license usage statistics to the Veeam licensing server, check that:

- The firewall on Veeam ONE Server allows connections required for proper communication between Veeam ONE components. For more information, see Ports and Firewall Rules.
- [If you connect to the Internet through a proxy server] `winhttp` proxy settings are properly configured on Veeam ONE Server.
- TLS 1.2 is enabled on Veeam ONE Server.

Permissions

This section describes privileges required for the proper operation of Veeam ONE.

Connection to Veeam Backup & Replication Servers

Veeam Backup server or Enterprise Manager server on Microsoft Windows

To connect Veeam Backup & Replication servers you must specify:

1. **Veeam Analytics service** deployment credentials:
   - This account must have an access to the administrative share on the machine where Veeam Analytics service is deployed.
2. **Backup Monitoring** credentials:
   - This account must have the Veeam Backup Administrator role assigned.

     This role must be assigned to the account on the machine that runs Veeam Backup & Replication.
   - Must be a member of the Performance Monitor Users and Event Log Readers security groups.

     These permissions must be granted to the account on machines that run:
     - Veeam Backup & Replication on Microsoft Windows.
     - Backup proxy, backup repository, WAN Accelerator, tape server and cloud gateway components (Windows-based) (required to collect performance data from these servers).
   - Must have permissions to remotely access WMI.

     This includes remote access, activation and launching the DCOM application of WMI, and remote access to the root WMI namespace and sub-namespaces. For details on granting these permissions, see Configuring Permissions to Remotely Access WMI.

     This permission must be granted to the account on machines that run:
     - Veeam Backup & Replication on Microsoft Windows.
     - Backup proxy, backup repository (Windows-based), WAN Accelerator, tape server and cloud gateway components (required to collect performance data from these servers).

NOTE:

You must use the account with local Administrator permissions in the following cases:

- When you install Veeam Analytics service on a Veeam Backup & Replication server you must disable MFA for the account under which Veeam Analytics service connects to Veeam Backup & Replication. For details, see section Disabling MFA for Service Accounts of the Veeam Backup & Replication User Guide.
- If machines that run Veeam ONE server and Veeam Backup & Replication server belong to different domains or workgroups.
- If you are using the default local administrator account, UAC settings do not affect elevation behavior. If you are using a custom local administrator account, you must either configure the `LocalAccountTokenFilterPolicy` registry key or disable UAC to ensure proper elevation. UAC behavior is affected if a custom user is added to the local Administrators group, regardless of whether Veeam Backup & Replication and Veeam ONE are deployed on the same domain, different domains, or workgroups.

Veeam Backup server or Enterprise Manager server on Linux

To connect Veeam Backup & Replication servers you must specify:

- **Veeam Analytics service** deployment credentials.

  This account must have the Veeam Backup Administrator role assigned.

  This role must be assigned to the account on the machine that runs Veeam Backup & Replication.

NOTE:

You must use the account with local Administrator permissions in the following cases:

- When using a user account other than the default `veeamadmin`, it is recommended to assign the Service Account role in Veeam Host Management and also Veeam Backup Administrator permissions in Veeam Backup & Replication. For details on roles and permissions, see Configuring Users and Configuring Roles in the Veeam Backup & Replication User Guide.

  For newly created local users in Veeam Host Management with a role other than Service Account, the user must first log in to the Veeam Software Appliance Web Client to change the password. Otherwise, an error occurs when connecting to the backup server to deploy Veeam Analytics service.

Connection to Veeam Backup for Microsoft 365 Servers

The account used to connect Veeam Backup for Microsoft 365 servers must have *Local Administrator* permissions on the machine where Veeam Backup for Microsoft 365 server is installed.

Connection to Virtualization Servers

This section describes permissions to accounts used to connect virtualization servers.

VMware vSphere Servers

The account used to connect vCenter Server and ESXi hosts must have the following privileges:

- **Datastore.Browse datastore**

  Required for collecting datastore details

- **Global.Global tag** (not required VMware vSphere version 6.5 or later)

  Required for running remediation actions

- **Global.Licenses**

  Required for collecting license information

- **Host.CIM.CIM Interaction**

  Required for gathering of ESXi host hardware data

- **Host.Configuration.Connection**

  Required for gathering of ESXi host hardware data

- **Host profile.Edit**

  Required for collecting Host profile properties

- **Host profile.View**

  Required for collecting Host profile properties

- **Virtual machine.Interaction.Answer question**

  Required for using VM Console and viewing snapshot information

- **Virtual machine.Interaction.Console interaction**

  Required for accessing VM console from Veeam ONE Client

- **Virtual machine.Snapshot management.Remove Snapshot**

  Required for running remediation actions

- vSphere Tagging Privileges:
  - **vSphere Tagging.Assign or Unassign vSphere Tag**
  - **vSphere Tagging.Create vSphere Tag**
  - **vSphere Tagging.Create vSphere Tag Category**
  - **vSphere Tagging.Delete vSphere Tag**
  - **vSphere Tagging.Delete vSphere Tag Category**
  - **vSphere Tagging.Assign or Unassign vSphere Tag on Object**

    Required for collecting and updating tags on the vCenter Server side. The privileges must be assigned at the vCenter Server level.

> **NOTE:**
>
> Names of privileges are provided for the latest supported version of VMware vSphere, and may vary for different platform versions.

Microsoft Hyper-V Hosts and Clusters

The account used to connect standalone Microsoft Hyper-V hosts must:

- Be a member of the **Hyper-V Administrators** and **Performance Monitor Users** security groups.
- Have permissions to remotely access WMI on Microsoft Hyper-V hosts.

  This includes remote access, activation and launching the DCOM application of WMI, and remote access to the root WMI namespace and sub-namespaces. For details on granting these permissions, see Configuring Permissions to Remotely Access WMI.

The account used to connect Microsoft Hyper-V clusters must have local Administrator permissions on these clusters.

Microsoft SCVMM

The account used to connect an SCVMM Server must have in SCVMM an assigned user role that is based on the **Read-Only Administrator** profile.

To monitor clusters and hosts managed by SCVMM, the minimal required permissions for these hosts and clusters must be granted to the same account. For details, see Microsoft Hyper-V Hosts and Clusters.

Connection to VMware Cloud Director Servers

The account used for connecting to VMware Cloud Director must have *system administrator* privileges.

Connection to PostgreSQL

The account used for installation, upgrade and operation requires the superuser role.

Veeam ONE Service Account

The service account must have *Local Administrator* and *Log on as a service* permissions on the machine where Veeam ONE is installed.

> **NOTE:**
>
> You cannot use the *Local System* account as the service account during product installation. If you want to use *Local System* to run Veeam ONE services you can configure it later. For details, see Changing Veeam ONE Service Account.

Connection to Microsoft SQL Server

The account used to connect to the Microsoft SQL Server hosting the Veeam ONE database during installation must have the following permissions:

- *Public* role — default permissions for SQL users
- *CREATE ANY DATABASE* permissions — required for database creation during setup
- *db_owner* role on the Veeam ONE database — required for communication of Veeam ONE services with the database
- *db_datareader* permissions on the **master** database — required to verify that only one product installation writes data to the database
- *public*, *db_datareader*, *SQLAgentUserRole* permissions on the **msdb** database — required for setup and database index optimization
- [For Always-On Availability Groups] *VIEW SERVER STATE*, *VIEW ANY DEFINITION* permissions — required to check database existence and to verify that Veeam ONE will write data to the primary replica of the database

After installation, the account used for upgrades and communication of Veeam ONE services with Veeam ONE database must have the following permissions:

- *Public* role (default permissions)
- *db_owner* role on the Veeam ONE database
- *db_datareader* permissions on the **master** database
- [For Always-On Availability Groups] *VIEW SERVER STATE*, *VIEW ANY DEFINITION* permissions

For details on permission requirements for SQL Server Reporting Services connection, see Configuring SSRS Server Settings.

Connection to VM Guest OS

The account used to collect data from guest OSes of Windows VMs, must have the following permissions:

- **Local Administrator** on the guest OS
- **List folder contents** on all guest OS volumes

> **NOTE:**
>
> To collect data from non-domain Windows VMs, or VMs with an unelevated *local Administrator* account, you must complete additional configuration steps to allow Veeam ONE perform data collection. For details, see Connection Under UAC.

Connection to ServiceNow

The account used to connect to ServiceNow instance must have the following permissions.

- **Read** permissions on the following tables:
  - */api/now/table/sys_user*

    Required to check user availability on the ServiceNow side.
  - */api/now/table/sys_user_group*

    Required to check the availability of the assignment group on the ServiceNow side.
  - */api/now/table/sys_choice.**

    Required to check the availability of the close code on the ServiceNow side.
  - */api/now/table/incident.**
- **Create** permissions on the following tables:
  - */api/now/table/sys_user.**
  - */api/now/table/sys_user*

    Required to create a Veeam ONE caller in ServiceNow.
  - */api/now/table/sys_user_group.**
  - */api/now/table/sys_user_group*

    Required to create a Veeam ONE Support group in ServiceNow.
  - */api/now/table/incident.**
- **Write** permissions on the following tables:
  - */api/now/table/incident.**
  - */api/now/table/incident.state*

Configuring Permissions to Remotely Access WMI

Veeam ONE collects data from Microsoft Windows machines using WMI. To make sure that Veeam ONE can collect data using WMI, the account under which you connect Microsoft Windows machines must have permissions to remotely access WMI.

For details on administrator permissions for connecting Veeam Backup & Replication and Veeam Backup Enterprise Manager see Connection to Veeam Backup & Replication Servers.

Permissions to access WMI remotely must be granted on:

- Microsoft Hyper-V hosts and clusters
- Veeam Backup & Replication servers

To configure permissions for remote access to WMI:

1. Grant permissions to remotely access root WMI namespace and sub-namespaces.
2. Grant remote access, launch and activation permissions for DCOM application.
3. Grant remote launch and activation permissions for WMI.

> **TIP:**
>
> Instead of performing steps 2 and 3, you can add the user account to the Distributed COM Users group on target machines.

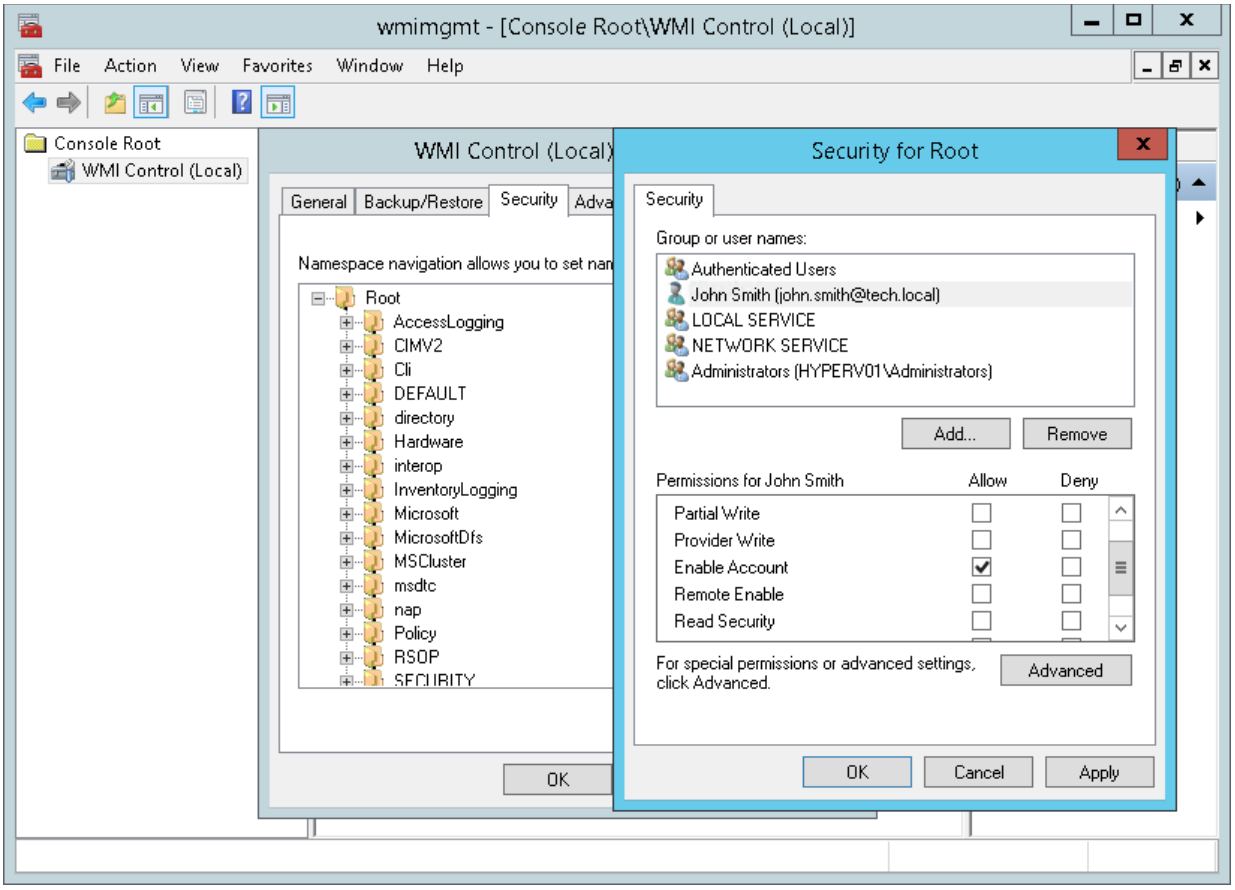
Step 1. Grant Permissions to Remotely Access Root WMI Namespace and Sub-Namespaces

To grant to an account permissions for remote access to WMI:

1. Log on to a target Microsoft Windows machine as an Administrator.
2. Open the WMI Control Console.

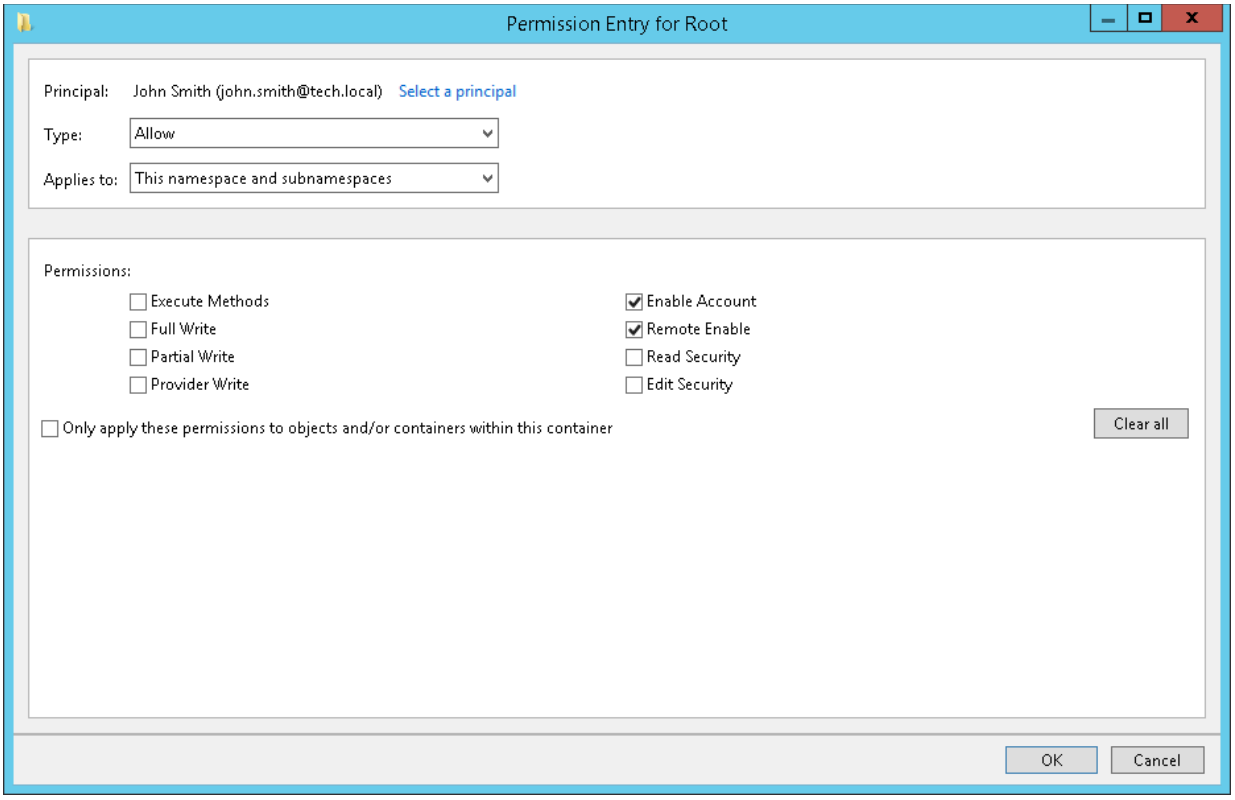
   To do so, choose **Start** > **Run**, type `wmimgmt.msc` and click **OK**.
3. Right-click **WMI Control** and select **Properties**.
4. In the **WMI Control Properties** window, open the **Security** tab.
5. On the **Security** tab, select the **Root** namespace.
6. Click **Security**.

7. In the **Security for Root** window, add the necessary user account.



8. Click **Advanced**.
9. In the **Advanced Security Settings for Root** window, select the user account and click **Edit**.
10. In the **Permission Entry for Root** window, do the following:
    a. In the **Applies to** list, select **This namespace and subnamespaces**.
    b. In the **Permissions** section, select **Enable Account** and **Remote Enable**.

c. Click **OK**.



11. In the **Advanced Security Settings for Root** window, click **OK**.
12. In the **Security for Root** window, click **OK**.
13. In the **WMI Control Properties** window, click **OK**.
14. Close the WMI Control Console.

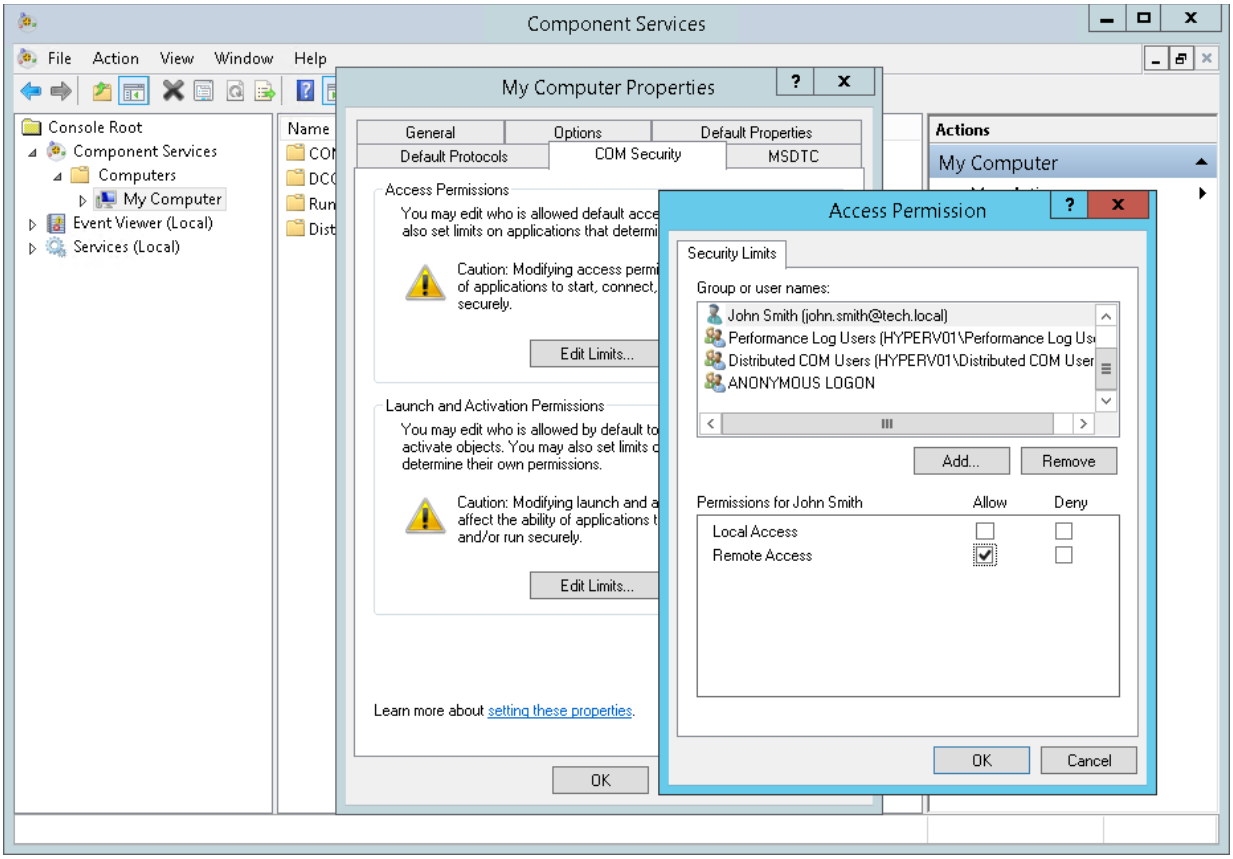
Step 2. Grant Remote Access, Launch and Activation Permissions for DCOM Application

To grant to an account remote access, launch and activation permissions:

1. Open the Component Services Console.

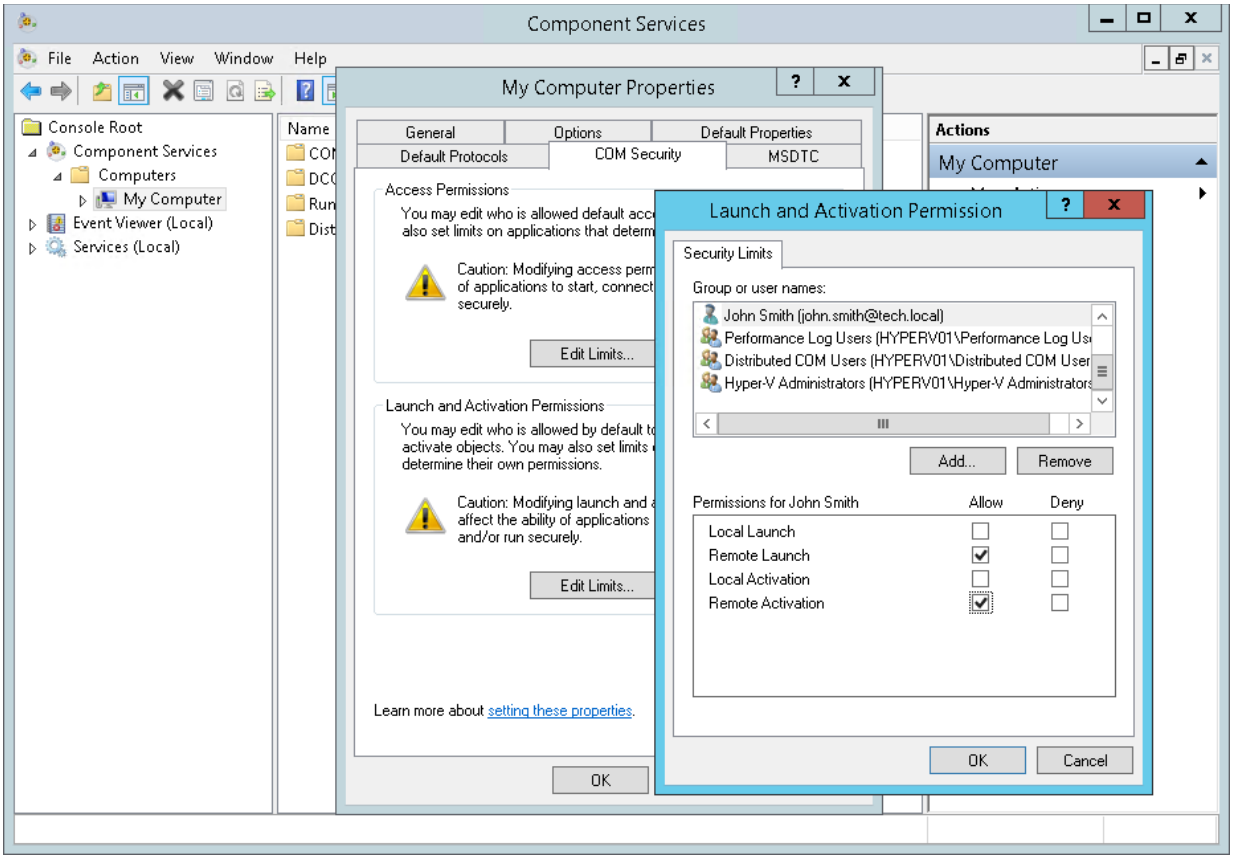
   To do so, choose **Start** > **Run**, type `dcomcnfg` and click **OK**.
2. In the navigation tree, go to **Component Services** > **Computers** > **My Computer**.
3. Right-click **My Computer** and select **Properties**.
4. In the **My Computer Properties** window, open the **COM Security** tab.
5. In the **Access Permissions** section, click **Edit Limits**.
6. In the **Access Permission** window, add the necessary user account.
7. Select the **Remote Access** permissions.

8. Click **OK**.



9. In the **Launch and Activation Permissions** section, click **Edit Limits**.
10. In the **Launch and Activation Permission** window, add the necessary user account.
11. Select the **Remote Launch** and **Remote Activation** permissions.

12. Click **OK**.



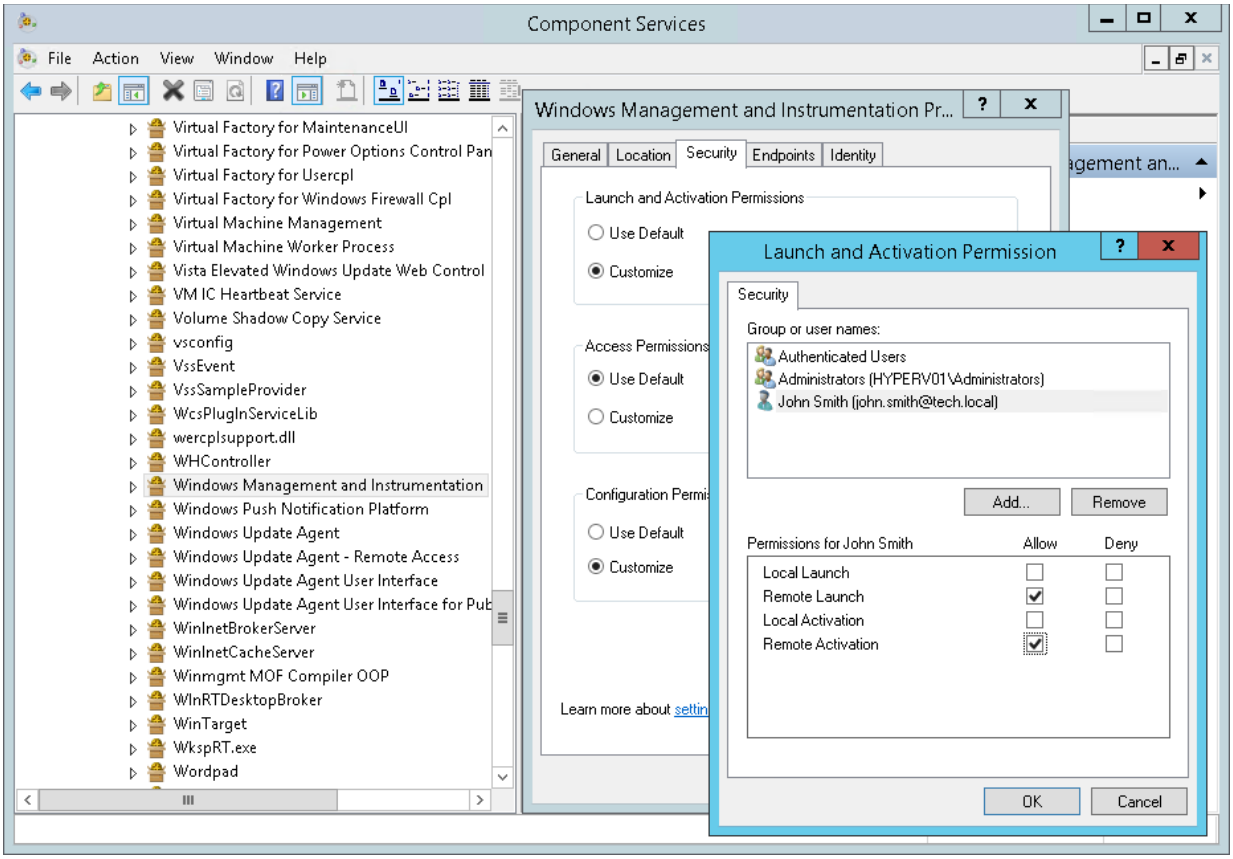
13. In the **My Computer Properties** window, click **OK**.

Step 3. Grant Remote Launch and Activation Permissions for WMI

To grant remote launch and activation permissions for WMI:

1. Still in the Component Services Console, in the navigation tree, go to **Component Services** > **Computers** > **My Computer** > **DCOM Config** > **Windows Management and Instrumentation**.
2. Right-click **Windows Management and Instrumentation** and select **Properties**.
3. In the **Windows Management and Instrumentation Properties** window, open the **Security** tab.
4. In the **Launch and Activation Permissions** section, click **Edit**.
5. In the **Launch and Activation Permission** window, add the necessary user account.

6. Select the **Remote Launch** and **Remote Activation** permissions.



7. In the **Launch and Activation Permission** window, click **OK**.
8. In the **Windows Management and Instrumentation Properties** window, click **OK**.
9. Close the Component Services Console.

NOTE:

If you are using the default local administrator account, UAC settings do not affect elevation behavior. If you are using a custom local administrator account, you must either configure the `LocalAccountTokenFilterPolicy` registry key or disable UAC to ensure proper elevation. UAC behavior is affected if a custom user is added to the local Administrators group, regardless of whether Veeam Backup & Replication and Veeam ONE are deployed on the same domain, different domains, or workgroups.

Alternative Methods of Configuring Permissions to Remotely Access WMI

As an alternative to the method described above, you can use a domain user account that is member of the local Administrators group on target Microsoft Windows machines. Administrators have all the required permissions by default.

You can also use a local Administrator account for connecting remote Microsoft Windows machines. However, this method will not work if remote machines have the User Account Control enabled.

Connection Under UAC

Veeam ONE collects data from Microsoft Windows servers using WMI. For some configurations, UAC access token filtering can prevent running WMI commands on connected machines, which in turn will cause data collection failures. If you are using the default local administrator account, UAC settings do not affect elevation behavior. If you are using a custom local administrator account, you must either configure the `LocalAccountTokenFilterPolicy` registry key or disable UAC to ensure proper elevation. UAC behavior is affected if a custom user is added to the local Administrators group, regardless of whether Veeam Backup & Replication and Veeam ONE are deployed on the same domain, different domains, or workgroups.

The affected configurations are:

- Non-domain machines (machines in a workgroup)
- Machines with an unelevated local Administrator account (the account that is not Built-in Administrator)

For details on UAC access token filtering, see Microsoft Learn.

Machines in a Workgroup

To allow Veeam ONE collect data from machines in a workgroup, perform the following steps:

1. Set the network location to private:
   a. Log on to a machine as Administrator.
   b. Open the **Network & Internet** settings.
   c. In the list of active networks, click the necessary network and click **Properties**.
   d. Change network profile to *Private*.
      In some Windows OS versions, this location is called *Home* or *Work*.
2. To configure Windows Remote Management, in the command prompt, type `winrm quickconfig` and press `[Enter]`.

Domain Machines

To allow Veeam ONE collect data from domain machines, create the `LocalAccountTokenFilterPolicy` registry entry on the machine. For details, see this Microsoft Learn article.

Authorizing with Veeam ONE

To authorize with Veeam ONE software components (Veeam ONE Client and Veeam ONE Web Client), a user must have the *Allow log on locally* privilege assigned.

By default, this privilege is assigned to users included in the local Administrators group. For users not included in the local Administrators group, you must assign this privilege manually. For details, see Microsoft Learn.

NOTE:

- In the custom deployment scenario, you must assign the Allow log on locally privilege on the machines that host the Veeam ONE Server and Veeam ONE Web Services architectural components.
- If the Windows security policy *Deny access to this computer from the network* is set to deny network logon for local accounts and members of the Administrators group, local administrator accounts may be assigned the *Limited Scope* user role in Veeam ONE Web Client.

  In this situation, Veeam ONE Web Client cannot validate local administrator group membership because it relies on a Windows network logon (Logon Type 3).

  To ensure proper validation and access, we recommend using domain accounts or groups for Veeam ONE administration.

Remote Access

To be able to access Veeam ONE software components installed on a remote machine, you can use one of the following options.

Remote Access to Veeam ONE Web Client through Web Browser

Veeam ONE Web Client console can be accessed using a web browser on a remote machine. For details on how to access Veeam ONE software components, see Accessing Veeam ONE Components.

To access Veeam ONE Web Client console remotely, a user must be a member of the *Veeam ONE Administrators*, *Veeam ONE Read-Only Users* or *Veeam ONE Power Users* group on the machines where Veeam ONE Web Services and Veeam ONE Server components are installed. For details on Veeam ONE security groups, see Security Groups.

Remote Access for Multi-Tenant Monitoring and Reporting

Veeam ONE supports multi-tenant access to its monitoring and reporting capabilities. Authorized users can remotely monitor a subset of the vCenter Server or VMware Cloud Director infrastructure and create reports.

To monitor and report on a restricted scope of the virtual infrastructure, a user must have permissions assigned on objects of the vCenter Server or VMware Cloud Director inventory hierarchy. For details, see Multi-Tenant Monitoring and Reporting.

Ports

The following table lists connection settings required for proper communication between Veeam ONE components, virtualization servers, VMware Cloud Director servers, Veeam Backup & Replication servers and Veeam Backup for Microsoft 365 servers.

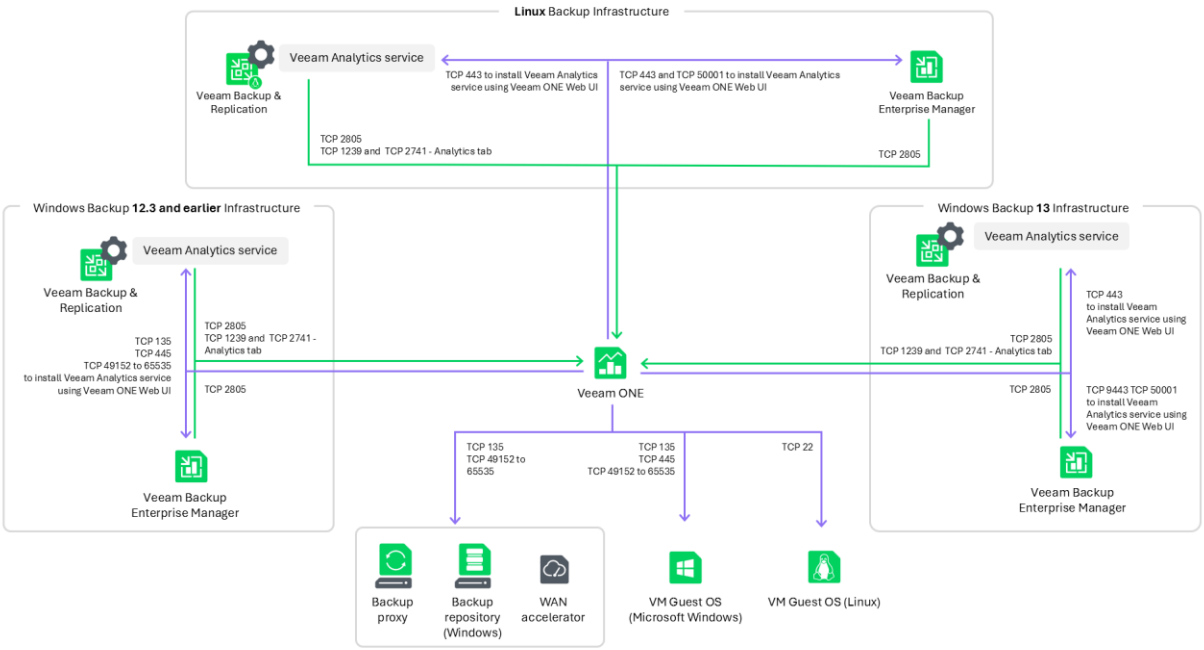
Communication with Virtualization Servers

From	To	Protocol	Port	Notes
Veeam ONE	ESXi server	TCP	443	Required to collect data from the ESXi server over HTTPS. Note that you must open this port manually. To learn how to check the current state of the vSphere API port, see the VMware vSphere documentation.
		TCP	5989	Required to collect ESXi host hardware details via CIM XML.
	vCenter Server	TCP	443	Required to collect data from vCenter Server over HTTPS. To learn how to check the current state of the vSphere API port, see the VMware vSphere documentation.
		TCP	10080	Default port used to access the vCenter Inventory Service and collect vCenter Server tags.
	Platform Services Controller (PSC)	TCP	443	Default port used to access vCenter Server PSCs over HTTPS to collect and assign VMware Tags data. Required for vCenter Server starting from version 6.5.
	VMware Cloud Director	TCP	443	Required to collect data from vCloud Director REST API. Note that you must open this port manually. For more information about vCloud Director API, see VMware documentation.
	SCVMM	TCP	8100	Default port used to communicate with the VMM server through WCF. Required by the Veeam ONE Service.

From	To	Protocol	Port	Notes
	Hyper-V server	TCP	135 445	Required to gather CPU and memory performance data from the Microsoft Hyper-V server through WMI. Port 445 is also required to access remote registry. For more information about enabling and disabling WMI traffic, see Connecting to WMI Remotely with VBScript and Setting up a Remote WMI Connection. Note that to gather performance data from Windows Server 2012 and 2012 R2, you must additionally enable network discovery.
		TCP	49152 to 65535	Dynamic RPC port range for Microsoft Windows 2008 and later. For more information, see this Microsoft KB article. **Note:** If you use default Microsoft Windows firewall settings, you do not need to configure dynamic RPC ports. During setup, Veeam ONE automatically creates a firewall rule for the runtime process. If you use firewall settings other than default ones or application-aware processing fails with the *"RPC function call failed"* error, you need to configure dynamic RPC ports. For more information on how to configure RPC dynamic port allocation to work with firewalls, see this Microsoft KB article.

Communication with Backup Infrastructure Components

The following diagram illustrates the key ports connections configured between the Veeam Backup & Replication server and Veeam ONE:



From	To	Protocol	Port	Notes
Veeam ONE	Veeam Backup & Replication server (Windows) version 12.3 and earlier	**Note:** all of these ports below for Veeam Backup & Replication server (Windows) are required to install Veeam Analytics service using Veeam ONE Web Client.		
		TCP	135 445	Required to collect data through WMI and install Veeam Analytics service using Veeam ONE Web Client. Port 445 is also required to access remote registry. For more information about enabling and disabling WMI traffic, see Connecting to WMI Remotely with VBScript and Setting up a Remote WMI Connection.

From	To	Protocol	Port	Notes
		TCP	49152 to 65535	Dynamic RPC port range for Microsoft Windows 2008 and later. For more information, see this Microsoft KB article. **Note:** If you use default Microsoft Windows firewall settings, you do not need to configure dynamic RPC ports. During setup, Veeam ONE automatically creates a firewall rule for the runtime process. If you use firewall settings other than default ones or application-aware processing fails with the *"RPC function call failed"* error, you need to configure dynamic RPC ports. For more information on how to configure RPC dynamic port allocation to work with firewalls, see this Microsoft KB article.
	Veeam Backup & Replication server (Windows) version 13.0.1 and newer	TCP	443	Required to install Veeam Analytics Service using Veeam ONE Web Client.
	Veeam Backup & Replication server (Linux)	TCP	443	Required to install Veeam Analytics Service using Veeam ONE Web Client.
	Veeam Backup Enterprise Manager	**Note:** all of these ports below for Veeam Backup Enterprise Manager (Windows) are required to install Veeam Analytics service using Veeam ONE Web Client.		

From	To	Protocol	Port	Notes
	(Windows) version 12.3 and earlier	TCP	135 445	Required to collect data through WMI and install Veeam Analytics service using Veeam ONE Web Client. Port 445 is required to access remote registry. For more information about enabling and disabling WMI traffic, see Connecting to WMI Remotely with VBScript and Setting up a Remote WMI Connection.
		TCP	49152 to 65535	Dynamic RPC port range for Microsoft Windows 2008 and later. For more information, see this Microsoft KB article. **Note:** If you use default Microsoft Windows firewall settings, you do not need to configure dynamic RPC ports. During setup, Veeam ONE automatically creates a firewall rule for the runtime process. If you use firewall settings other than default ones or application-aware processing fails with the *"RPC function call failed"* error, you need to configure dynamic RPC ports. For more information on how to configure RPC dynamic port allocation to work with firewalls, see this Microsoft KB article.
	Veeam Backup Enterprise Manager (Windows) version 13.0.1 and newer	TCP	443 50001	Required to install remote Veeam Analytics service using Veeam ONE Web Client.
	Veeam Backup Enterprise Manager (Linux)	TCP	443 50001	Required to install remote Veeam Analytics service using Veeam ONE Web Client.

From	To	Protocol	Port	Notes
	Backup proxy, Backup repository, WAN accelerator (Windows)	TCP	135	Required to gather CPU and memory performance data from the backup proxy through WMI. For more information about enabling and disabling WMI traffic, see Connecting to WMI Remotely with VBScript and Setting up a Remote WMI Connection. Note that to gather performance data from Windows Server 2012 and 2012 R2, you must additionally enable network discovery.
		TCP	49152 to 65535	Dynamic RPC port range for Microsoft Windows 2008 and later. For more information, see this Microsoft KB article. **Note:** If you use default Microsoft Windows firewall settings, you do not need to configure dynamic RPC ports. During setup, Veeam ONE automatically creates a firewall rule for the runtime process. If you use firewall settings other than default ones or application-aware processing fails with the *"RPC function call failed"* error, you need to configure dynamic RPC ports. For more information on how to configure RPC dynamic port allocation to work with firewalls, see this Microsoft KB article.
	VM Guest OS (Microsoft Windows)	TCP	135 445	Required to monitor Microsoft Windows VM guest OS processes and services through WMI. For more information about enabling and disabling WMI traffic, see Connecting to WMI Remotely with VBScript and Setting up a Remote WMI Connection.

From	To	Protocol	Port	Notes
		TCP	49152 to 65535	Dynamic RPC port range for Microsoft Windows 2008 and later. For more information, see this Microsoft KB article. **Note:** If you use default Microsoft Windows firewall settings, you do not need to configure dynamic RPC ports. During setup, Veeam ONE automatically creates a firewall rule for the runtime process. If you use firewall settings other than default ones or application-aware processing fails with the *"RPC function call failed"* error, you need to configure dynamic RPC ports. For more information on how to configure RPC dynamic port allocation to work with firewalls, see this Microsoft KB article.
	VM Guest OS (Linux)	TCP	22	Required to monitor Linux VM guest OS processes and services through SSH.
Veeam Backup & Replication server / Veeam Backup Enterprise Manager	Veeam ONE Server	TCP	2805 (by default)	Required for communication between remote Veeam Analytics Service and Veeam ONE Monitoring service. This is required for data collection.
Veeam Backup & Replication server	Veeam ONE Server	TCP	1239 2741	Required to use the Analytics tab in the Veeam Backup & Replication. If the backup console is deployed on a separate VM, these ports must also be opened on that machine.

Communication with Veeam Backup for Microsoft 365

From	To	Protocol	Port	Notes
Veeam ONE	Veeam Backup for Microsoft 365	TCP	135 445	Required to gather CPU and memory performance data from Veeam Backup for Microsoft 365 through WMI. For more information about enabling and disabling WMI traffic, see Connecting to WMI Remotely with VBScript and Setting up a Remote WMI Connection.
		TCP	49152 to 65535	Dynamic RPC port range for Microsoft Windows 2008 and later. For more information, see this Microsoft KB article. **Note:** If you use default Microsoft Windows firewall settings, you do not need to configure dynamic RPC ports. During setup, Veeam ONE automatically creates a firewall rule for the runtime process. If you use firewall settings other than default ones or application-aware processing fails with the *"RPC function call failed"* error, you need to configure dynamic RPC ports. For more information on how to configure RPC dynamic port allocation to work with firewalls, see this Microsoft KB article.
		TCP	4443	Required to collect data from Veeam Backup for Microsoft 365 REST API over HTTPS.
		TCP	5985 5986	Required to remotely enable the Veeam Backup for Microsoft 365 REST API service when adding a server to Veeam ONE and also for installing certificates for federated authentication. Port 5986 is used for communication over HTTPS.

Other Communications

From	To	Protocol	Port	Notes
Veeam ONE	Veeam License Update Server	TCP	443	Default port used to access Veeam License Update Server over HTTPS to automatically update license and Veeam Intelligent Diagnostics signatures. Veeam License Update Server endpoints: • `one.butler.veeam.com`
		TCP	80	Required for certificate validation when Veeam ONE connects to Veeam License Update Server to check if the new license is available and download it. Certificate verification endpoints: • `*.ss2.us` • `*.amazontrust.com` Consider that certificate verification endpoints (CRL URLs and OCSP servers) are subject to change. The actual list of addresses can be found in the certificate itself.
	SMTP server	TCP	25	Default port used by the SMTP server to send email notifications. The actual port number depends on the configuration of your environment.
	File Server (SMB)	TCP	445	Port required to get information about used and free space on SMB shares used by connected Microsoft Hyper-V hosts and clusters.
	Veeam Intelligence	TCP	443	Port required to connect Veeam ONE Server to Veeam CDN Connection Veeam Intelligence endpoints: • `cdn.rest-ai.veeam.com` • `js.veeam.com`

From	To	Protocol	Port	Notes
		TCP	443	Port required to connect Veeam ONE Server and workstation to AI service Veeam Intelligence endpoints: • `rest-ai.veeam.com`
Veeam ONE Server	Microsoft SQL Server	TCP	1433	Port used for communication with the Microsoft SQL Server on which the Veeam ONE database is deployed. Additional ports may need to be open depending on your configuration. For details, see Microsoft Docs.
	PostgreSQL	TCP	5432	Used by Veeam ONE Web Client to communicate with the PostgreSQL database. Additional ports may need to be open depending on your configuration. For details, see Microsoft Docs.
	Veeam ONE Server	TCP	2714	Port used for communication between Reporting and Monitoring Service on the Veeam ONE Server. Port required to be open for internal communication.
		TCP	2743	Used by Veeam ONE Web Client to communicate with the caching service. Port required to be open for internal communication.
Veeam ONE Web Service	Veeam ONE Server	TCP	2741	Port used for communication with Veeam ONE internal Web API.
		TCP	2742	Port used for communication between Veeam ONE Web Services and Reporting Service on the Veeam ONE Server.
Veeam ONE Client	Veeam ONE Server	TCP	139 445	Used by Veeam ONE Client to communicate with the Veeam ONE Server. These ports are also associated with the File and Printer Sharing service.
		UDP	137	

From	To	Protocol	Port	Notes
Workstation web browser	Veeam ONE Web Services	TCP	1239	Default port to access Veeam ONE Web Services from a user workstation over HTTPS. A different port number can be chosen during setup.

Firewall Rules

The following table lists exceptions that should be enabled in Windows Firewall Settings.

Server	App/Feature	Details
Hyper-V host	Remote Event Log Management: • Remote Event Log Management (NP-In) • Remote Event Log Management (RPC) • Remote Event Log Management (RPC-EPMAP) COM+ Network Access: • COM+ Network Access (DCOM-In)	Required to collect events data from Hyper-V hosts.
Veeam Backup & Replication server	Remote Event Log Management: • Remote Event Log Management (NP-In) • Remote Event Log Management (RPC) • Remote Event Log Management (RPC-EPMAP) COM+ Network Access: • COM+ Network Access (DCOM-In)	Required to collect events data from Veeam Backup & Replication servers.
Veeam Backup for Microsoft 365 Server	COM+ Network Access: • COM+ Network Access (DCOM-In) Network Discovery: • Network Discovery (LLMNR-UDP-In)	Required to gather CPU and memory performance data from Veeam Backup for Microsoft 365 servers.

Sizing and Scalability Best Practices

This section provides deployment guidelines for achieving maximum performance of Veeam ONE 13 in large-scale environments, that is environments with 10,000 VMs and more. You can also use these guidelines for smaller environments.

The recommended deployment configuration can be equally used for POC deployments and deployments in production.

System Requirements for Large-Scale Deployment

The required deployment configuration relies on the custom deployment scenario, where Veeam ONE components are hosted as follows:

- Veeam ONE Server (on a dedicated machine)
- Microsoft SQL Server (on a dedicated machine)
- Veeam ONE UI (co-installed with Veeam ONE Server or run on a standalone machine)

Veeam ONE supports both virtual and physical servers for installation. This document describes a scenario where Veeam ONE components are installed on virtual machines.

Veeam ONE Server

For the Veeam ONE Server component, use a server that meets the following requirements.

Hardware Recommendations

Specification	Veeam Backup Data Only[1]	Virtual Infrastructure
CPU	The amount of required CPU resources depends on the number of workloads being protected in the managed infrastructure: • 2-4 vCPUs for 1,000-10,000 protected workloads • 4-6 vCPUs for 10,000-20,000 protected workloads • 6-8 vCPUs for 20,000-40,000 protected workloads • 8-10 vCPUs for 40,000-60,000 protected workloads Regardless of the number of protected workloads: • For every connected Veeam Backup for Microsoft 365 server, additional 1 vCPU core is required. • For every connected Veeam Backup & Replication server, additional 0.03 vCPU core is required.	The amount of required CPU resources depends on the number of hosts in the managed infrastructure: • 4 vCPUs for up to 1,500 VMs • 4-12 vCPUs for 1,500-10,000 VMs • 12-16 vCPUs for 10,000-20,000 VMs • 16+ vCPUs for 20,000+ VMs

Specification	Veeam Backup Data Only[1]	Virtual Infrastructure
RAM	The amount of required memory resources depends on the number of workloads being protected in the managed infrastructure: • 4 GB for up to 1,000 protected workloads • 4–15 GB for 1,000–10,000 protected workloads • 15–30 GB for 10,000–20,000 protected workloads • 30–50 GB for 20,000-40,000 protected workloads • 50–80 GB for 40,000 - 60,000 protected workloads Regardless of the number of protected workloads: • For every connected Veeam Backup for Microsoft 365 server, additional 500 MB RAM is required. • For every connected Veeam Backup & Replication server, additional 60 MB RAM is required.	50 MB per 15 managed VMware VMs and 600 MB per managed vCenter Server. **Note**: This requirement assumes that there are no standalone hosts in the managed infrastructure. All hosts must be included in clusters, and clusters must be managed by vCenter Server/SCVMM. Such configuration results in fewer connections to virtual servers during data collection, and requires less memory resources. In environments with standalone hosts connected to Veeam ONE directly, memory requirements will be higher.
Disk	50 GB recommended space for Veeam ONE cache and Veeam Intelligent Diagnostics logs.	
Bandwidth	1 Mbit/sec for 100 hosts	

[1]Under the condition that a protected workload is included in one data protection job scheduled to run daily, that is, has one restore point per day. For example, if a workload is included in two data protection jobs, consider it as two protected workloads, as it will consume twice as much computing resources.

Software and OS Requirements

Specification	Requirement
OS	Only 64-bit versions of the following operating systems are supported: • Microsoft Windows Server 2025 • Microsoft Windows Server 2022 • Microsoft Windows Server 2019 • Microsoft Windows Server 2016 • Microsoft Windows 11 (Professional and Enterprise editions with minimum supported version 22H2) • Microsoft Windows 10 version 1909 and LTS builds (Minimum supported version 21H2 for LTSC channel and 22H2 for GA) **Note:** Semi-Annual Channel (SAC) releases are supported.
Software	The following components are included in the Veeam ONE setup package and can be installed automatically: • Microsoft ASP.NET Core Shared Framework 8.0.17 • Microsoft Windows Desktop Runtime 8.0.17 • Microsoft .NET Runtime 8.0.17 • Microsoft .NET Framework 4.7.2 • Microsoft System CLR Types for SQL Server 2014 • Microsoft SQL Server 2014 Management Objects • Microsoft Internet Information Services (IIS) 10.0 or later • Microsoft Application Request Routing 3.0 • IIS URL Rewrite Model 2.1 • Microsoft Universal C Runtime To connect SCVMM servers to Veeam ONE, the following software is required: • System Center 2025 Virtual Machine Manager console (for connecting SCVMM 2025 servers) • System Center 2022 Virtual Machine Manager console (for connecting SCVMM 2022 servers) • System Center 2019 Virtual Machine Manager console (for connecting SCVMM 2019 servers) • System Center 2016 Virtual Machine Manager console (for connecting SCVMM 2016 servers) • Microsoft PowerShell 3.0 (required for SCVMM 2016, and SCVMM 2019 consoles) Be sure to install the same versions of the Admin UI and the SCVMM Server, and to update both components to the same update version.

Specification	Requirement
Other	• Windows Management Instrumentation service must be enabled to allow data collection from Veeam Backup & Replication servers. • File and Print Sharing service must be enabled to enable remote Veeam ONE Client connections to the Veeam ONE service.

Microsoft SQL Server

For the Veeam ONE database, use a server that meets the following requirements.

Hardware Recommendations

Specification	Veeam Backup Data Only	Virtual Infrastructure
CPU, RAM	CPU and RAM sizing requirements are the same as for the Veeam ONE Server. Note: the Standard Edition of SQL Server does not allow the use of more than 4 CPU sockets (or more than 24 cores in total). If the recommended amount of cores or sockets exceeds these limits, SQL Server Enterprise Edition must be used. **Important!** These requirements assume that the Veeam ONE database is hosted on a dedicated Microsoft SQL Server. If the SQL Server is shared by several applications, compute requirements will be higher. To calculate the amount of resources required by other applications, see application-specific sizing recommendations for Microsoft SQL Server.	
Disk	Install the OS and Microsoft SQL Server on different drives. **OS Drive**: 50 GB **Application drive**: Use the Veeam ONE Database Calculator to size application data. With partitioning scripts, you will have the following distribution of the Veeam ONE database size: • **Primary Tables**: 20% • **Partitioned Tables**: 80% Size the following tables in accordance with Microsoft SQL Server recommendations: • **Primary Logs** • **Partitioned Logs** • **TempDB** **Other**: SSD RAID storage with broadband connectivity must be used for the TempDB table.	
Other	If you use a virtualized Microsoft SQL Server, this server must run on a separate LUN/datastore from Veeam ONE Server.	

Software and OS Requirements

Specification	Requirement
Software	**Microsoft SQL Server (Full and Express Editions):** • Microsoft SQL Server 2025 • Microsoft SQL Server 2022 • Microsoft SQL Server 2019 • Microsoft SQL Server 2017 (Microsoft SQL Server 2017 Express edition without cumulative updates is included in Veeam ONE installation package) • Microsoft SQL Server 2016 • Microsoft Azure SQL Database • Amazon RDS for SQL Server **Reporting Services (optional):** • Microsoft SQL Server Reporting Services 2025 • Microsoft SQL Server Reporting Services 2022 • Microsoft SQL Server Reporting Services 2019 • Microsoft SQL Server Reporting Services 2017 • Microsoft SQL Server Reporting Services 2016

Database Size

To calculate an expected size of the Veeam ONE database, use the Veeam ONE Database Calculator. The calculator helps estimate disk space required to store VMware vSphere, Microsoft Hyper-V and Veeam Backup & Replication data.

For details, see https://www.veeam.com/kb2246.

Veeam ONE UI

Veeam ONE Client and Veeam ONE Web Services components can be installed on the same machine, or can run separately.

For security purposes, it is recommended to install these components on a machine that does not host the Microsoft SQL Server and Veeam ONE Server components.

Veeam ONE Web Services

For the Veeam ONE Web Services component, use a machine that meets the following requirements:

Specification	Requirement
CPU	Modern processor (minimum 2 cores). Using faster multi-core processors improves data processing performance.
RAM	2 GB minimum

Veeam ONE Client

Veeam ONE Client has no specific requirements, and can be installed on any machine. For Veeam ONE Client, use a machine that meets the following requirements:

Specification	Requirement
CPU	Modern x86/x64 processor
RAM	2–4 GB recommended

Walkthrough: Deploy and Configure Veeam ONE

To deploy and configure Veeam ONE for a large-scale environment, complete the following steps:

1. [Optional] Pre-create the Veeam ONE database.
2. Install Veeam ONE Server.
3. Install Veeam ONE Web Client and Veeam ONE Client.
4. Configure connection to the SSRS Server.
5. Configure data retention.

Step 1. Pre-create Veeam ONE Database (Optional)

If you do not want to create the Veeam ONE database automatically using the Veeam ONE Setup wizard, you can pre-create it before installing Veeam ONE Server.

For details, see Creating Veeam ONE Database with SQL Script.

Step 2. Install Veeam ONE Server

Install the Veeam ONE Server component on a dedicated machine. For detailed installation instructions, see Installing Veeam ONE Server.

Step 3. Install Veeam ONE Web UI and Veeam ONE Client

Install Veeam ONE Web Client component and Veeam ONE Client.

For detailed installation instructions, see sections Installing Veeam ONE Web Services and Installing Veeam ONE Client.

Step 4. Configure Connection to SSRS Server

Configure a connection to Microsoft SSRS Server in Veeam ONE Web Client:

1. Log in to Veeam ONE Web Client as *Veeam ONE Administrator*.
2. Open **Configuration**.
3. In the configuration menu, click **Reporting**.
4. Select the **Use SSRS server for generating reports** check box.
5. In the **Server URL** field, type an URL to the Reporting Services report server page.

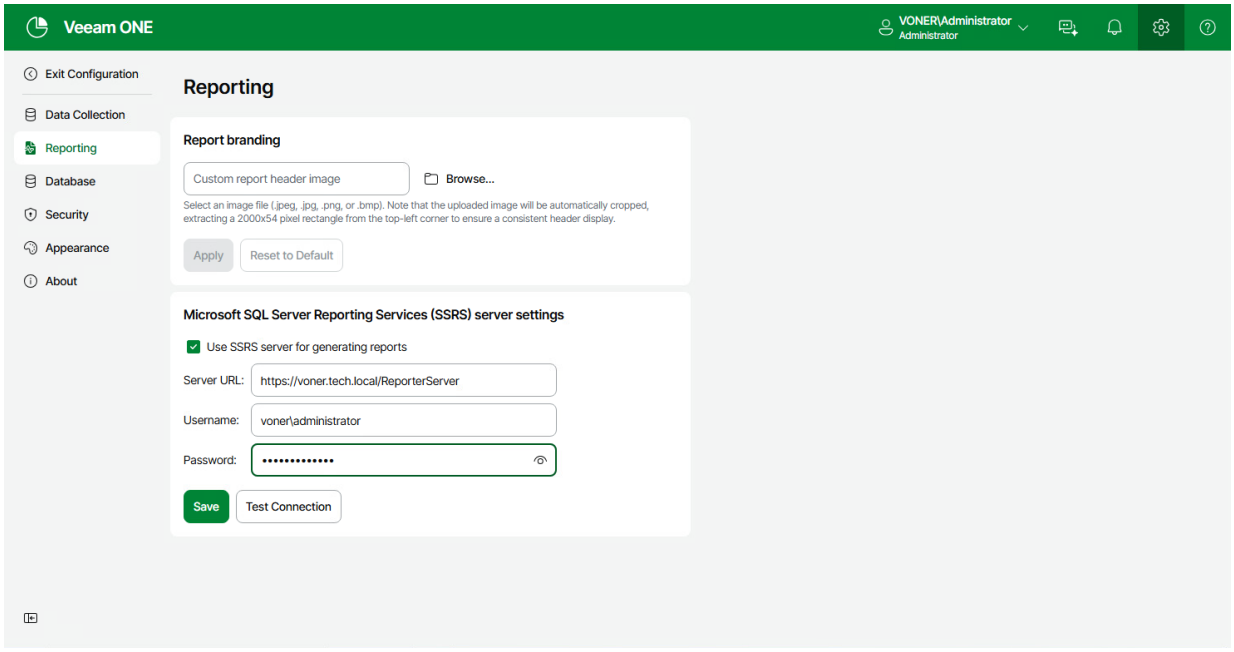
   The URL must have the following form:

   `http://[ServerName]:port/ReportServer`

   If you configured a named instance for Microsoft SQL Server, the URL must look as follows:

   `http://[ServerName]:port/ReportServer_NAMEDSQLINSTANCE`
6. In the **Username** and **Password** fields, type credentials for connecting to the SSRS Server.

   For details on permission requirements for SQL Server Reporting Services connection, see Configuring SSRS Server Settings.
7. Test connection to the SSRS Server and click **Save**.



Step 5. Configure Data Retention

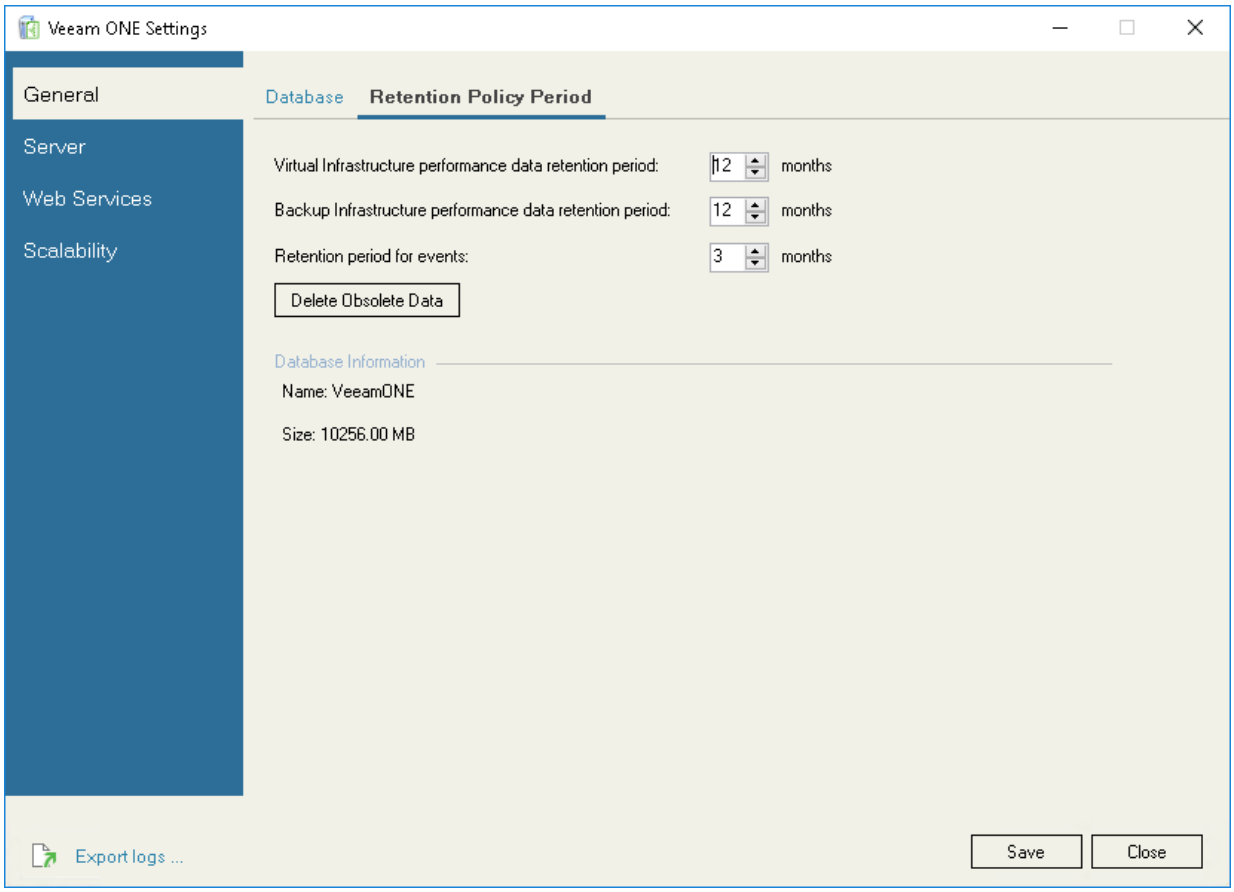
In Veeam ONE Settings utility, review and change retention settings.

It is recommended to make the retention period for events 3 months or less, as events data take up a lot of space in the database. The retention period for virtual infrastructure and backup performance data is normally set to 6-12 months.

Decreasing the default retention values helps maintain a lower size of the Veeam ONE database, but results in reducing the period for which performance and events data is available in Veeam ONE Client and Veeam ONE Web Client.

1. In the menu on the left, click **General**.
2. Open the **Retention Policy Period** tab.
3. Specify for which period virtual infrastructure performance data, backup infrastructure performance data and events data must be stored.

   Specified retention values will be applied at the end of the current week. To apply retention settings immediately, click **Delete Obsolete Data**.
4. Click **Save**.
5. In the displayed dialog box, click **OK** to restart Veeam ONE services.



Licensing Veeam ONE

To achieve full capability of Veeam ONE, you must obtain a license file and install it on the Veeam ONE server. If you do not install the license key, the product will operate in the *Community* (free) edition.

Licensed Objects

Veeam ONE can be licensed in two ways: per-socket and per-instance.

Per Socket Licensing

Veeam ONE can be licensed by the number of CPU sockets on managed VMware vSphere and Microsoft Hyper-V hosts. A license is required for every occupied motherboard socket as reported by the hypervisor API. A managed host is a host that is included in the monitoring and reporting scope with Veeam ONE inclusion rules. For details, see Choosing VMs and VM Containers to Monitor and Report On.

Per Instance Licensing

Veeam ONE can be licensed by the number of instances. An **instance** is a unit (or token) that is assigned to an object to make it manageable in Veeam ONE.

Veeam ONE per-instance license apply to the following types of objects:

- VMs protected by the monitored Veeam Backup & Replication servers and VMs included in the monitoring and reporting scope with Veeam ONE inclusion rules. For details on configuring monitoring scope for the virtual infrastructure, see Choosing VMs and VM Containers to Monitor and Report On.

  VMs protected by the monitored Veeam Backup & Replication servers and VMs included in the monitoring and reporting scope at the same time consume one instance from a license scope. Powered off replicas do not consume instances.

- Computers protected with Veeam Agent for Windows, Linux, Mac, IBM AIX and Oracle Solaris that are managed by Veeam Backup & Replication servers that you connect to Veeam ONE.

  The number of instances consumed by a managed computer depends on the mode in which the Veeam Agent job operates. For details on Veeam Agent licensing coefficients, see section *Instance calculation for Veeam Universal License* of the Veeam Licensing Policy.

- File shares protected by Veeam Backup & Replication servers that you connect to Veeam ONE. File shares are licensed per 500 GB of protected data.

- Nutanix AHV, oVirt Kernel-based and Proxmox VMs protected by Veeam Backup & Replication servers that you connect to Veeam ONE.

- Cloud VMs, cloud databases and cloud file shares protected by Veeam Backup for Microsoft Azure, Veeam Backup for AWS and Veeam Backup for Google Cloud integrated with Veeam Backup & Replication servers that you connect to Veeam ONE.

- Microsoft 365 user accounts whose data is protected with Veeam Backup for Microsoft 365 servers connected to Veeam ONE.

  > **NOTE:**
  > - Rental program for Veeam Cloud & Service Providers (VCSP) includes free license usage for Veeam Backup for Microsoft 365 monitoring. Consider that when you generate the license, Microsoft 365 (10 users pack) costs 2 PPU. When you submit your monthly license usage report, the cost of the license will be changed to 0 PPU.
  > - If you have full monitoring enabled with your licenses for Veeam ONE and Veeam Backup for Microsoft 365, monitoring of Veeam Backup for Microsoft 365 does not consume any license units.

- Enterprise Applications protected with Veeam Plug-ins for SAP HANA, Oracle RMAN, SAP on Oracle, Microsoft SQL Server, SAP MaxDB.
- Object Storage data protected by Veeam Backup & Replication servers that you connect to Veeam ONE. Object storage protection is licensed per 500 GB of protected data.

Rental licenses intended for Veeam Cloud & Service Providers (VCSP) use **points** as license units. For details on rental licenses, see Veeam ONE.

> **NOTE:**
>
> Infrastructure topology view in Veeam ONE and Veeam Backup & Replication must match. Otherwise license instances may be consumed incorrectly.

New Objects

To provide more flexibility and introduce a trial period for object management, Veeam ONE offers the concept of *New objects* for *Rental* licenses. New objects are objects that were discovered within the current calendar month. New objects are tracked separately. The **Used points** license counter reflects the number of points required for the new objects, that is the number of new objects multiplied by the object coefficient.

New objects do not consume the license points until the beginning of the new month. On the first day of the new month, the number of new objects is added to the number of managed objects and the **New points** counter in the license resets. New objects are not included in a license usage report.

> **NOTE:**
>
> The *New objects* counter in Veeam ONE does not include:
>
> - File shares protected by Veeam Backup & Replication
> - Nutanix VMs, Microsoft Azure VMs and AWS EC2 instances that are not included in the New objects counter on the monitored Veeam Backup & Replication server

License Types and Packages

Veeam Software offers paid and free licenses for Veeam ONE.

Paid Licenses

Veeam Software offers the following types of paid licenses for Veeam ONE:

- **Perpetual license** is a permanent full license. The perpetual license does not have an expiration date and allows using Veeam ONE versions issued before support expiration date.
- **Subscription license** is a full license that expires at the end of the subscription term. The subscription license term is normally 1-3 years from the license issue date.
- **Rental license** is a full license intended for Veeam Cloud & Service Providers (VCSP). The license expiration date is set according to the chosen rental program (normally 1-12 months from the license issue date).

  For details on Veeam ONE licensing for Veeam Cloud & Service Providers (VCSP), see section Veeam ONE of the Veeam Rental Licensing and Usage Reporting Guide.

The following terms apply to Veeam ONE paid licenses:

License Type	Licensing
Perpetual license	Per socket/Per instance
Subscription license	Per socket/Per instance
Rental license	Per point

Free Licenses

Veeam Software offers the following types of free licenses for Veeam ONE:

- **Evaluation license** is a full license that can be used for product evaluation. The trial license is valid for 30 days from the moment of product download.
- **Community Edition license** is a license with a limited set of features* but with no restrictions on the number of virtualization hosts, management servers and failover clusters you can monitor and report on. The community license includes 10 Veeam Backup & Replication monitored instances free of charge and does not have an expiration date. The community version does not require a license file during installation.
- **NFR license** is a full license that can be used for product demonstration, training and education. This license is not for resale or commercial use.

*For details on Veeam ONE Community Edition limitations, see Feature Comparison.

License Packages

Veeam ONE accepts licenses of the following packages:

- ONE

- Essentials
- Suite

> **NOTE:**
>
> The *Suite* package matches *Veeam Data Platform Advanced* from the Pricing and Packaging page.

For details on license packages, see Pricing and Packaging.

Compatibility with Veeam Backup & Replication Licenses

Veeam ONE allows monitoring of Veeam Backup & Replication servers if the following conditions are met for *Subscription* and *Perpetual* licenses:

			Veeam ONE License		
			Per Socket	Per Instance	
				Package = Suite/Essentials	Package = ONE
Veeam Backup & Replication License	Per Socket	Package = Backup	All workloads[1]	All workloads	All workloads
		Package = Suite/Essentials	All workloads[1]	All workloads	All workloads
	Per Instance	Package = Backup	Cannot add to Veeam ONE	Cannot add to Veeam ONE	Cannot add to Veeam ONE
		Package = Suite/Essentials	All workloads[2]	All workloads	Cannot add to Veeam ONE
	Merged	Sockets (Package = Backup) Instances (Package = Backup)	VM workloads only	Cannot add to Veeam ONE	All workloads
		Sockets (Package = Suite) Instances (Package = Backup)	VM workloads only	VM workloads only	All workloads

			Veeam ONE License		
			Per Socket	Per Instance	
				Package = Suite/Essentials	Package = ONE
		Sockets (Package = Backup) Instances (Package = Suite)	All workloads[2]	Non-VM workloads only	All workloads
		Sockets (Package = Suite) Instances (Package = Suite)	All workloads[2]	All workloads	All workloads
		Sockets (Package = Essentials) Instances (Package = Suite)	All workloads[2]	All workloads	All workloads

where:

- **VM workloads only** — include VMs protected by the monitored Veeam Backup & Replication servers and VMs included in the monitoring and reporting scope with Veeam ONE inclusion rules.
- **Non-VM workloads only** — include other workloads protected by Veeam Backup & Replication servers that you connect to Veeam ONE: computers protected with Veeam Agent for Windows, Veeam Agent for Linux, Veeam Agent for Mac, Veeam Agent for IBM AIX, Veeam Agent for Oracle Solaris, file shares, Nutanix AHV VMs, Microsoft Azure VMs, AWS EC2 instances and Google Cloud Platform VMs.

1. Includes free instances that can be used for monitoring non-VM workloads.
2. Veeam ONE does not consume free instances included in the license file.

NOTE:

Veeam ONE does not accept merged license files. If you install a merged socket and instance license, it behaves as a per socket license.

Compatibility with Veeam Backup for Microsoft 365 Licenses

Veeam ONE allows monitoring of Veeam Backup for Microsoft 365 servers if the following conditions are met for the licenses:

			Veeam ONE License					
			Rental	Subscription	Perpetual	Community	NFR	Evaluation
Veeam Backup for Microsoft 365 License	Subscription	Package = M365	×	×	×	×	×	✓
		Package = M365Suite	✓	✓	✓	✓	×	✓
	Rental	Package = M365	✓	×	×	×	×	✓
	Evaluation	Package = M365Suite	✓	✓	✓	✓	✓	✓
	Community	Package = M365Suite	×	✓	✓	×	✓	✓
	NFR	Package = M365	×	×	×	×	×	×
		Package = M365Suite	×	×	×	✓	✓	✓

Installing License

Veeam ONE license is provided during the product installation.

If you do not provide a license file during installation, you can provide it later:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. In the main menu, click **License**.
3. In the **License Information** window, navigate to the **License** tab and click **Install**.
4. Specify a path to the license file and click **Open**.
5. Select the **Update license automatically** check box to enable automatic license update and usage reporting.

   Automatic usage reporting implies sending license usage statistics to Veeam. For details, see License Usage Statistics.

6. Select the the **Receive proactive support** check box to send infrastructure statistics to Veeam.

   Proactive support sends anonymized information such as infrastructure details, number of jobs, and job types to Veeam support servers automatically. This allows Veeam to better analyze and understand your individual support needs.

7. In the **License Information** window, click **Save**.

Viewing License Information

You can check details of the installed license in the **License Information** window.

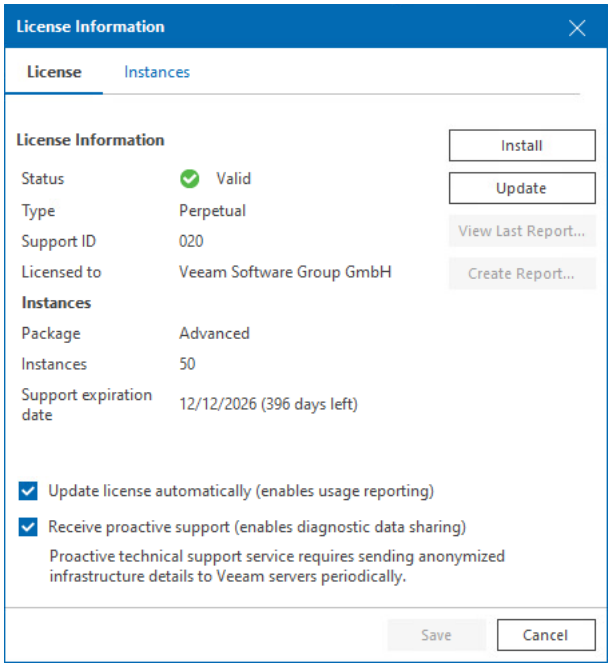
To access the **Licensed Information** window:

1. Open Veeam ONE Client.

   For details, Accessing Veeam ONE Components.

2. In the main menu, click **License**.

   The **License Information** window will display license details.



License Information

The **License Information** section provides information about the current Veeam ONE license:

- **Status** – status of the installed license (*Valid*, *Valid (License key is about to expire)*, *Invalid*, *Expired (N days of grace period remaining)*, *Warning (License exceeded)*, *Not Installed*).
- **Type** – type of the installed license (*Perpetual*, *Subscription*, *Rental*, *Community*, *Evaluation*, *NFR*).
- **Licensed to** – name of the user or company to which the license was issued.
- **Expiration date** – date when the license will expire.
- **Package** – license package (*ONE*, *Suite*, *Essentials*).
- **Instances** – number of instances that can cover managed objects.
- [For *Rental* license only] **Points** – number of points that can cover managed objects.
- **Sockets** – number of sockets that the license covers.
- **Expiration date** – date when the license will expire.
- [For *Perpetual* license only] **Support expiration date** – date when product support will expire.

- **Support ID** — customer identification number required when contacting Veeam Technical Support.

License Usage

The **Sockets** and **Instances** tabs provide details on the number of currently used sockets, instances or points, and the number of managed objects with object multipliers for your license type.

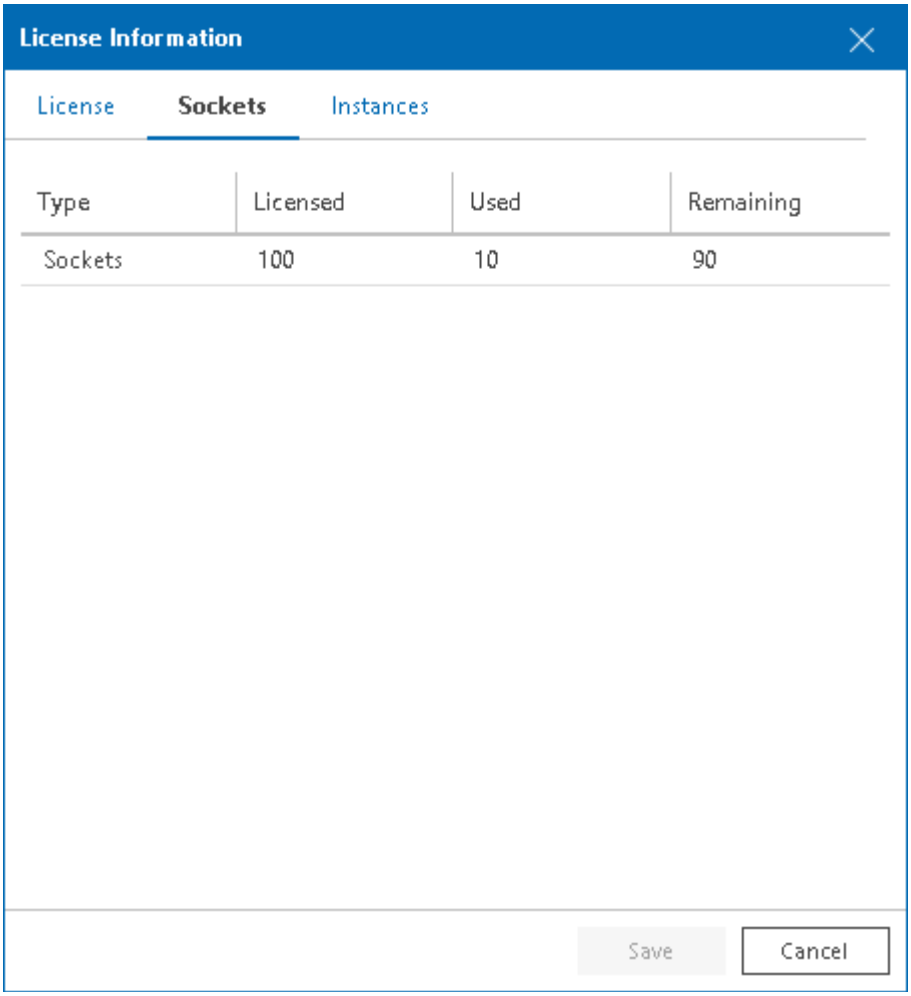
These tabs contain the following information:

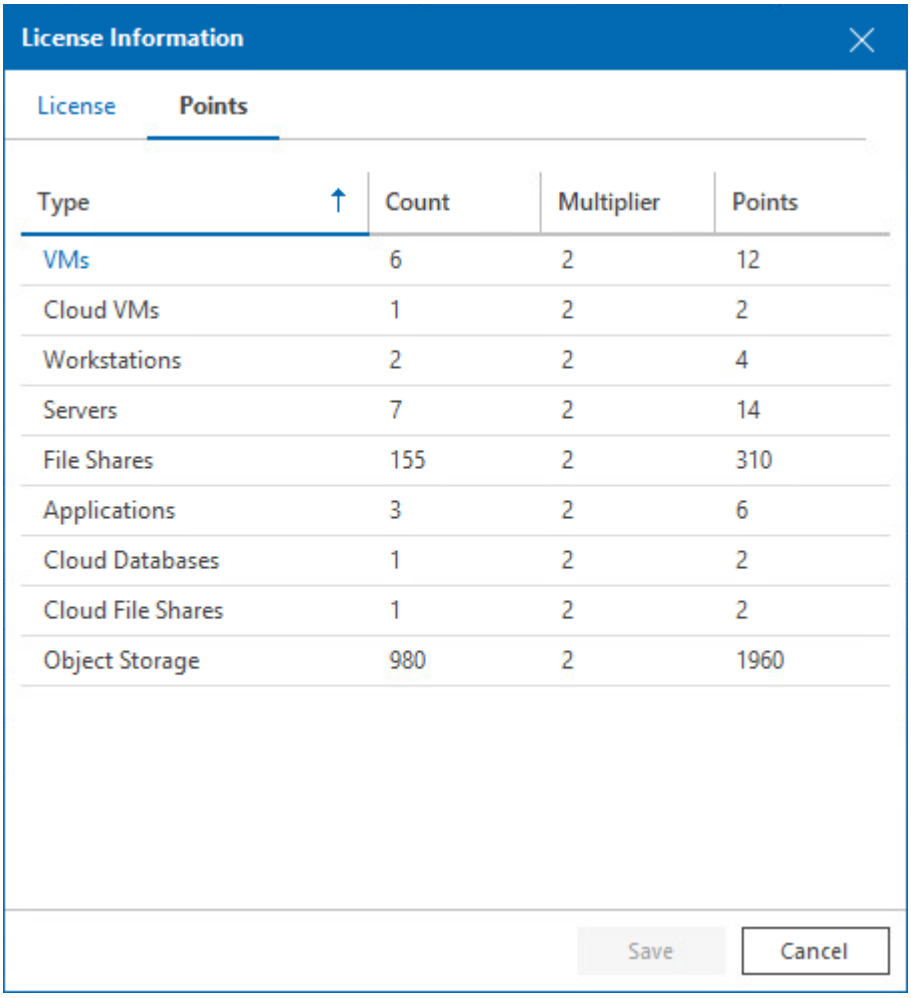
- **Sockets** — number of licensed, used and remaining sockets on managed VMware vSphere and Microsoft Hyper-V hosts.
- [For *Rental* license only] **Used points** — number of points consumed by managed objects out of the total number of instances available in the license.
- **New** — number of objects that were discovered less than a month ago (within the current calendar month). For details on new objects, see Licensed Objects.
- **VMs** — number of managed VMs out of the total number of discovered VMs on managed VMware vSphere and Microsoft Hyper-V hosts and Veeam Backup & Replication servers.

  Click a link in the **Type** column to drill down to details on protected workloads.
- **Workstations** — number of managed Veeam Agents that run in *Workstation* mode and are managed by Veeam Backup & Replication servers connected to Veeam ONE.
- **Servers** — number of managed Veeam Agents that run in Server mode discovered and are managed by Veeam Backup & Replication servers connected to Veeam ONE.
- **File Shares** — number of managed data blocks (500 GB each) of file shares protected by Veeam Backup & Replication servers connected to Veeam ONE.
- **Cloud VMs** — number of Microsoft Azure VMs, Google Cloud VMs and AWS EC2 instances protected by Veeam Backup for Microsoft Azure, Veeam Backup for AWS and Veeam Backup for Google Cloud integrated with Veeam Backup & Replication servers that you connect to Veeam ONE.
- **Cloud File Shares** — number of AWS EFS and Microsoft Azure file shares protected by Veeam Backup for Microsoft Azure, Veeam Backup for AWS and Veeam Backup for Google Cloud integrated with Veeam Backup & Replication servers that you connect to Veeam ONE.
- **Cloud Databases** — number of Microsoft Azure SQL, AWS RDS, Google Cloud SQL databases protected by Veeam Backup for Microsoft Azure, Veeam Backup for AWS and Veeam Backup for Google Cloud integrated with Veeam Backup & Replication servers that you connect to Veeam ONE.
- [For *Rental* license only] **Microsoft 365 users** — number of users protected by Veeam Backup for Microsoft 365 and number of consumed instances.

  Click a link in the **Type** column to drill down to details on protected workloads.
- **Applications** — number of enterprise applications protected with Veeam Plug-ins for SAP HANA, Oracle RMAN, SAP on Oracle, SAP on MadDB.

- **Object Storage** — number of managed data blocks (500 GB each) of Amazon S3, Azure Blob and S3 compatible storage data protected by Veeam Backup & Replication servers connected to Veeam ONE


License Information
License
Sockets
Instances
Type
Licensed
Used
Remaining
Sockets
100
10
90
Save
Cancel


License Information
License
Points
Type
Count
Multiplier
Points
VMs 6 2 12
Cloud VMs 1 2 2
Workstations 2 2 4
Servers 7 2 14
File Shares 155 2 310
Applications 3 2 6
Cloud Databases 1 2 2
Cloud File Shares 1 2 2
Object Storage 980 2 1960
Save
Cancel

Submitting License Usage Report

If you use a *Rental* license, you must submit a license usage report to Veeam every month. The license usage report reflects the maximum number of instances consumed by workloads that you were managing with Veeam ONE within the previous calendar month: VMs, file shares and Veeam Agents (*Workstation* and *Server*), cloud instances (cloud VMs, cloud databases and cloud file shares), enterprise applications, object storage and Microsoft 356 users.

There are two methods to submit a license usage report:

- You can submit a license usage report in Veeam ONE Client (recommended). For details, see Submitting License Usage Report in Veeam ONE Client.
- You can submit a license usage report manually by sending an email with a generated report to a Veeam sales representative. For details, see Submitting Offline License Usage Report.

Submitting License Usage Report in Veeam ONE Client

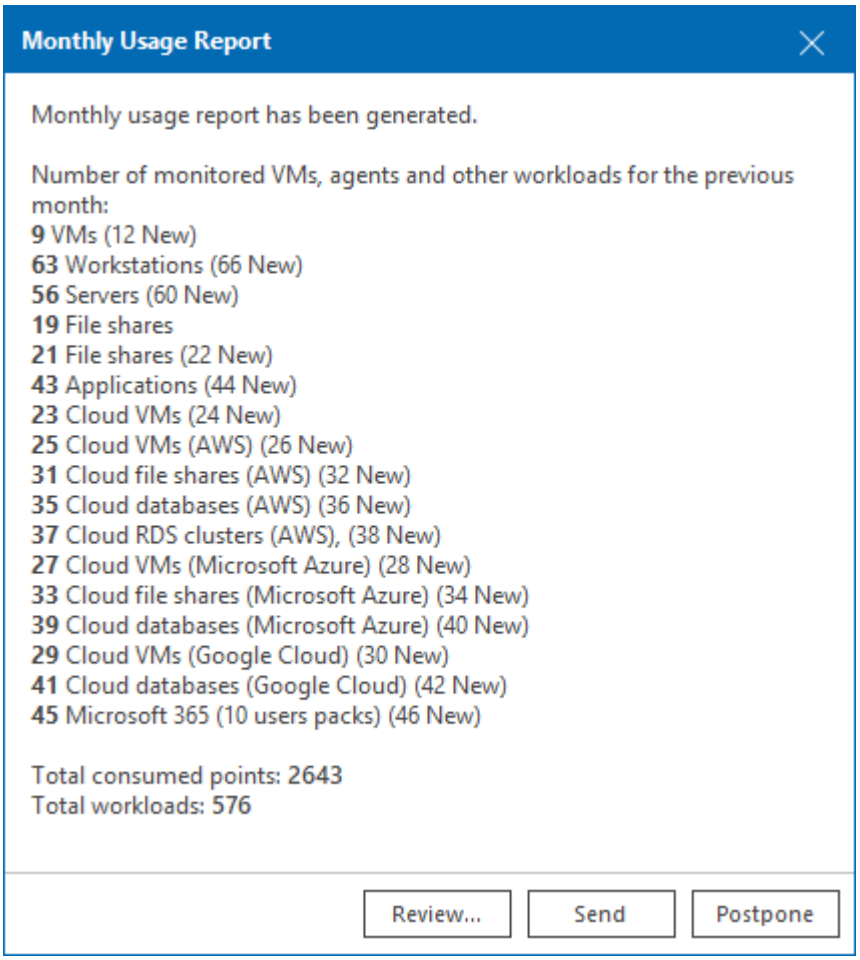
If Veeam ONE server has access to Internet, you can submit a license usage report in Veeam ONE Client. When you submit a license usage report in Veeam ONE Client, Veeam ONE sends license usage statistics to the Veeam License Update Server.

This method is available only if license auto update is enabled. For details on automated license update, see Updating License.

License usage reporting is performed in the following way:

1. Veeam ONE collects statistics on the current license usage.
2. On the first day of the new month, Veeam ONE generates a license usage report based on the maximum number of managed objects in the previous month.

3. Veeam ONE informs you about the generated report with a notification window in Veeam ONE Client each time you access the console.



4. You can review the report, adjust it and send it to Veeam.

   If you do not send and save the report, on the third day of the month, Veeam ONE will save and send the report automatically. You can access the report on the Veeam ONE server, in the `%ProgramData%\Veeam\Licensing\Veeam ONE Report` folder.

To submit a license usage report in Veeam ONE Client:

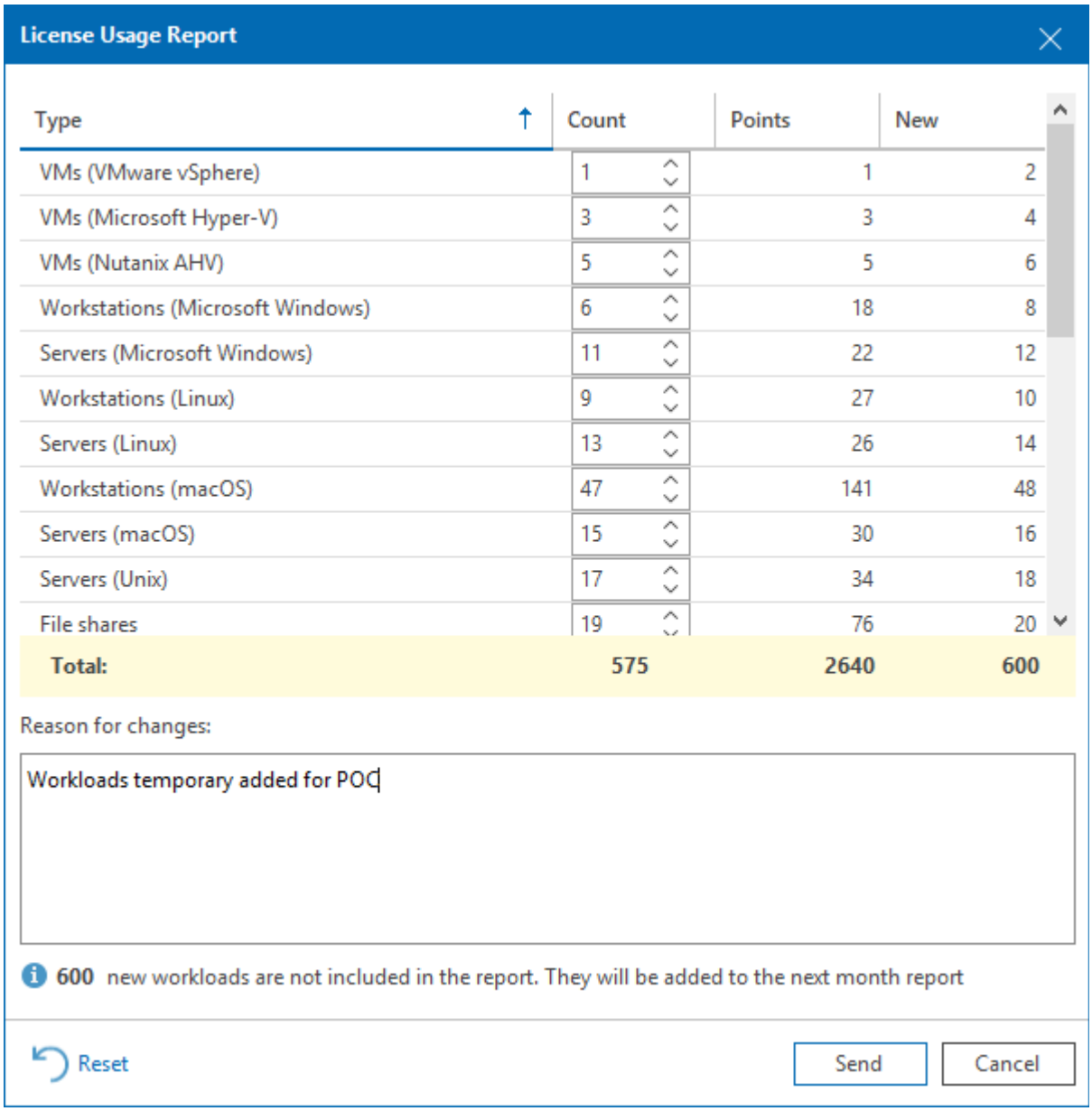
1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. In the main menu, click **License**.
3. In the **License Information** window, click **Create Report**.
4. In the **License Usage Report** window, you can adjust the number of managed workloads before you submit the report.
5. If you have reduced the number of workloads, the **Reason for changes** field, specify a reason for reducing report statistics or any additional information.
6. Click **Send**.

   Veeam ONE will display a dialog box with the submission result.

7. Click **OK** to acknowledge the result and close the dialog box.



Submitting Offline License Usage Report

If Veeam ONE server does not have access to Internet or has connection problems, you can submit an offline license usage report. When you submit an offline license usage report, Veeam ONE generates a file with license usage statistics.

The report file can be generated in the `JSON`, `PDF` or `XLS` format. You must send a report in the `JSON` format to Veeam. You can save the report in the `PDF` or `XLS` formats for your own needs.

This method is available only if license auto update is disabled. For details, see Updating License.

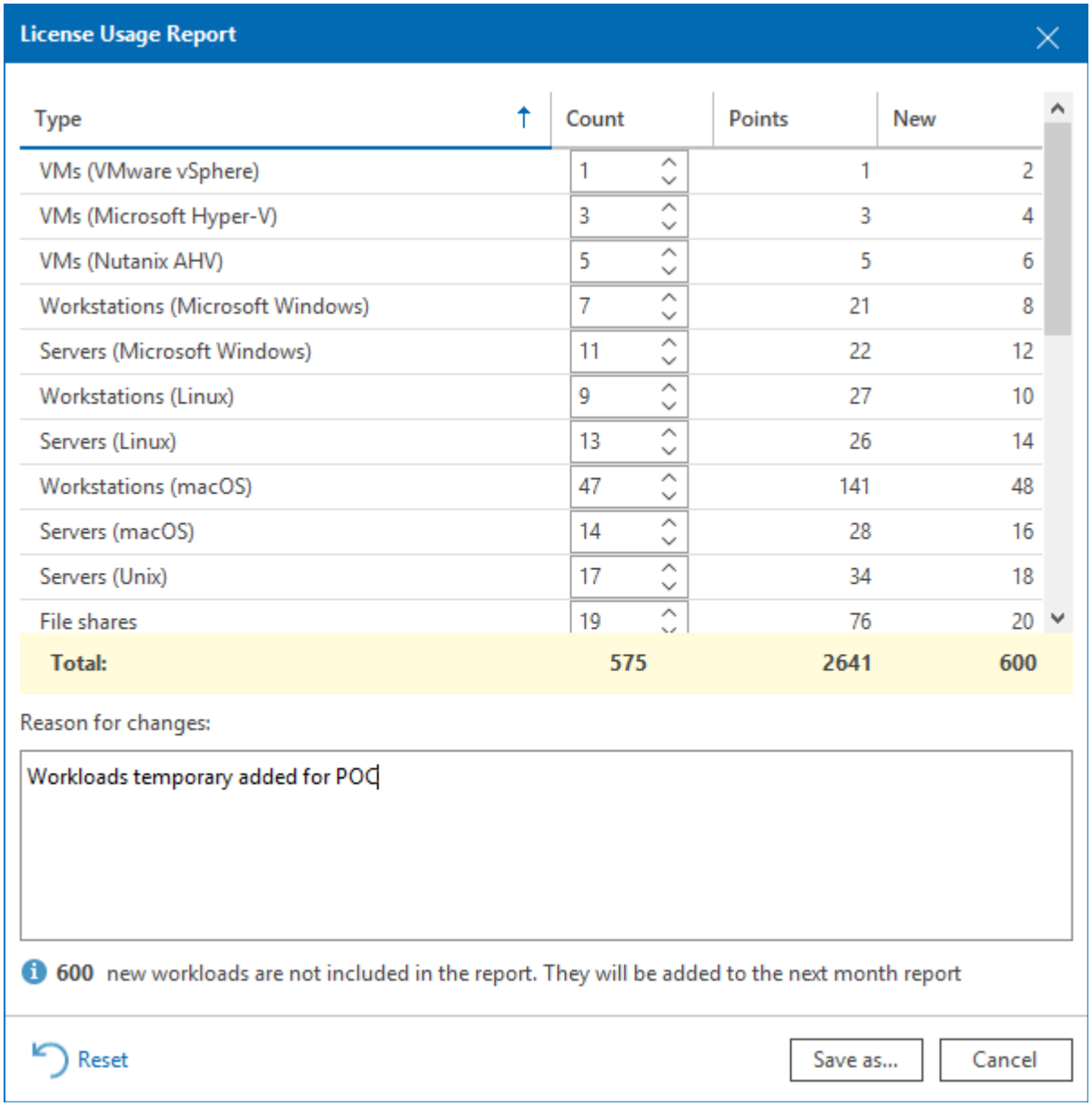
To submit an offline license usage report:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. In the main menu, click **License**.

3. In the **License Information** window, click **Create Report**.
4. In the **License Usage Report** window, you can adjust the number of managed workloads before you submit the report.
5. If you have reduced the number of workloads, the **Reason for changes** field, specify a reason for reducing report statistics or any additional information.
6. Click **Save as** and choose a folder to which you want to save the report.
7. When the report is generated, Veeam ONE will display a dialog box notifying that the report was created. In the dialog box, click **Open folder** to navigate to the folder where the report resides.
8. Review the report and send it to a Veeam sales representative.



Updating License

When the license expires, you can update it from the Veeam licensing server. You can use the following methods to update Veeam ONE license:

- Update the license manually
- Update the license automatically

> **NOTE:**
>
> To prevent potential conflicts with license updates, ensure that the date and time settings on the machines hosting Veeam ONE components are synchronized with the NTP (Network Time Protocol) servers within your organization.

Updating License Manually

You can update the license from the Veeam License Update Server manually on demand. When you update the license manually, Veeam ONE connects to the Veeam License Update Server, downloads a new license from it (if the license is available), and installs it on the Veeam ONE server.

To update the license:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. In the main menu, click **License**.
3. In the **License Information** window, navigate to the **License** tab.
4. Click **Update**.

   Veeam ONE will connect to the Veeam licensing server, download the new license from it (if available), install it on the Veeam ONE server, and display a dialog box with the license update result.

5. Click **Save** to acknowledge the result and close the dialog box.

Updating License Automatically

You can instruct Veeam ONE to update the license automatically. License auto-update is available for all types of licenses and is mandatory for *Free* licenses (*Community Edition*, *Evaluation*, *NFR*). Automatic license update removes the need to download and install the license manually each time when you purchase the license extension. If the automatic update option is enabled, Veeam ONE proactively communicates with the Veeam License Update Server to obtain and install a new license before the current license expires.

How Automatic License Update Works

To update the license automatically, Veeam ONE performs the following actions:

1. After you enable automatic license update, Veeam ONE starts sending requests to the Veeam License Update Server on the web (one.butler.veeam.com) and checks if a new license key is available. Veeam ONE sends requests once a week. Communication with the Veeam License Update Server is performed over the HTTPS protocol.

2. Seven days before the expiration date of the current license, Veeam ONE starts sending requests once a day.
3. When a new license key becomes available, Veeam ONE automatically downloads it and installs on the Veeam ONE server.

Automatic license update can complete with the following results:

- **Operation is successful**. A new license key is successfully generated, downloaded and installed on the Veeam ONE server.
- **A new license is not required**. The currently installed license key does not need to be updated.
- **Veeam License Update Server has failed to generate a new license**. Such situation can occur due to an error on the Veeam License Update Server side.
- **Veeam ONE has received an invalid answer**. Such situation can occur due to connectivity issues between the Veeam License Update Server and Veeam ONE server.

Automatic Update Retries

If Veeam ONE fails to update the license, it triggers the *Veeam ONE license update failure* alarm, and retries to update the license.

Veeam ONE retries to update the license key in the following way:

- If Veeam ONE fails to establish a connection to the Veeam License Update Server, retry takes place every 60 minutes.
- If Veeam ONE establishes a connection but there occurs a general license key generation error, the retry takes place every 24 hours.

The retry period ends one month after the license expiration date or the support expiration date (whichever is earlier). The retry period is equal to the number of days in the month of license expiration. For example, if the license expires in January, the retry period will be 31 days. If the license expires in April, the retry period will be 30 days.

Enabling Automatic License Update

By default, automatic license update is disabled. To enable automatic license updates:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.
2. In the main menu, click **License**.
3. In the **License Information** window, on the **License** tab, select the **Update license automatically (enables usage reporting)** check box.
4. Click **Save**.

> **NOTE:**
> - Enabling license auto update activates License Usage Statistics. You cannot use license auto update without automatic usage reporting.
> - License auto-update is enabled by default for *Free* licenses (*Community Edition*, *Evaluation*, *NFR*) and cannot be disabled.

License Usage Statistics

If you have enabled automatic update of Veeam ONE license, Veeam ONE will collect and send data on license usage automatically by default. For details on how to enable automatic license update, see Updating License.

As part of this process, Veeam ONE collects statistics on the current license usage and sends it periodically to the Veeam License Update Server. The collected data provides information about the contract ID, license ID, product installation ID, and the maximum number of protected workloads managed by Veeam Backup & Replication over the past week (high watermark), the maximum number of Veeam backup agents managed in Veeam ONE, and the maximum number of workloads protected by other Veeam products integrated with Veeam ONE. The process runs in the background mode, once a week at a random time and day. For details on Veeam products that can be integrated with Veeam ONE, see About Veeam ONE.

The collected data does not include information on Veeam ONE usage by any individual person identifiable for Veeam, or any data gathered by Veeam ONE.

Veeam may also use collected data for any other internal business purposes it deems appropriate, including (but not limited to) evaluation, improvement and optimization of Veeam licensing models.

> **IMPORTANT!**
>
> Even after you have enabled automatic license update and Veeam ONE has started sending usage statistics, you are still required to submit license usage to your aggregator. For details, see Submitting License Usage Report.

Veeam may also use collected data for any other internal business purposes it deems appropriate, including (but not limited to) evaluation, improvement and optimization of Veeam licensing models. For details on license limits, see Exceeding License Limit.

By enabling license auto update you agree with collection, transmission and use of the reporting data. You must not enable license auto update in case you do not agree with such collection, transmission and use.

License Expiration

Veeam ONE license period is set in accordance with the chosen licensing program.

For *Subscription* and *Rental* licenses, Veeam ONE offers a grace period after the license expiration date. This mechanism ensures a smooth license update and provides sufficient time to install a new license file.

During the grace period, Veeam ONE keeps working in a full-version mode. The license status in the **License Information** window will appear as *Expired (<number> days of grace period remaining)*.

You must update your license before the end of the grace period. If you do not update the license until the end of the grace period, Veeam ONE will switch to the community mode.

If support period is expired for a *Perpetual* license, the product will continue to work in a full-version mode. However, you will not be able to upgrade Veeam ONE and install updates and patches.

The duration of the grace period is defined by the type of license.

License Type	Grace Period
Perpetual license	Not applicable
Subscription license	30 days
Rental license	60 days

Exceeding License Limit

In some situations, the number of actually managed objects may exceed the license limit. For example, this may happen when some VMs or hosts are temporarily managed for testing or POC.

For per-instance licenses, Veeam ONE allows you to manage more objects than covered by the number of instances specified in the license. On the first month, the exceeding limit is equal to the number of instances the license covers. For example, if your license covers 500 instances, Veeam ONE allows you to manage objects that consume up to 1000 instances.

Starting from the second month, the exceeding limit varies according to the license type and state of license auto update setting:

License Type	Auto Update Enabled*	Auto Update Disabled
Subscription Perpetual (per instance)	Up to 20 instances or 20% of the total instance count (whichever number is greater)	Up to 10 instances or 10% of the total instance count (whichever number is greater)
Rental	Up to 20 instances or 20% of the total instance count (whichever number is greater)	Up to 20 instances or 20% of the total instance count (whichever number is greater)

*and you have successfully submitted license usage report during the last 30 days.

If the license limit is exceeded by no more than the specified percentage or number, Veeam ONE continues to manage all objects.

If the license limit is exceeded by more than the specified percentage or number, all objects exceeding the licensed number and the allowed increase are excluded from monitoring and reporting. To determine what objects to manage, Veeam ONE uses the last-in first-out method (LIFO): objects that were discovered last are removed first from the monitoring and reporting scope.

An increase in the number of managed objects up to the specified percentage is allowed only for a limited period of time. The duration of this grace period is equal to the duration of the license key.

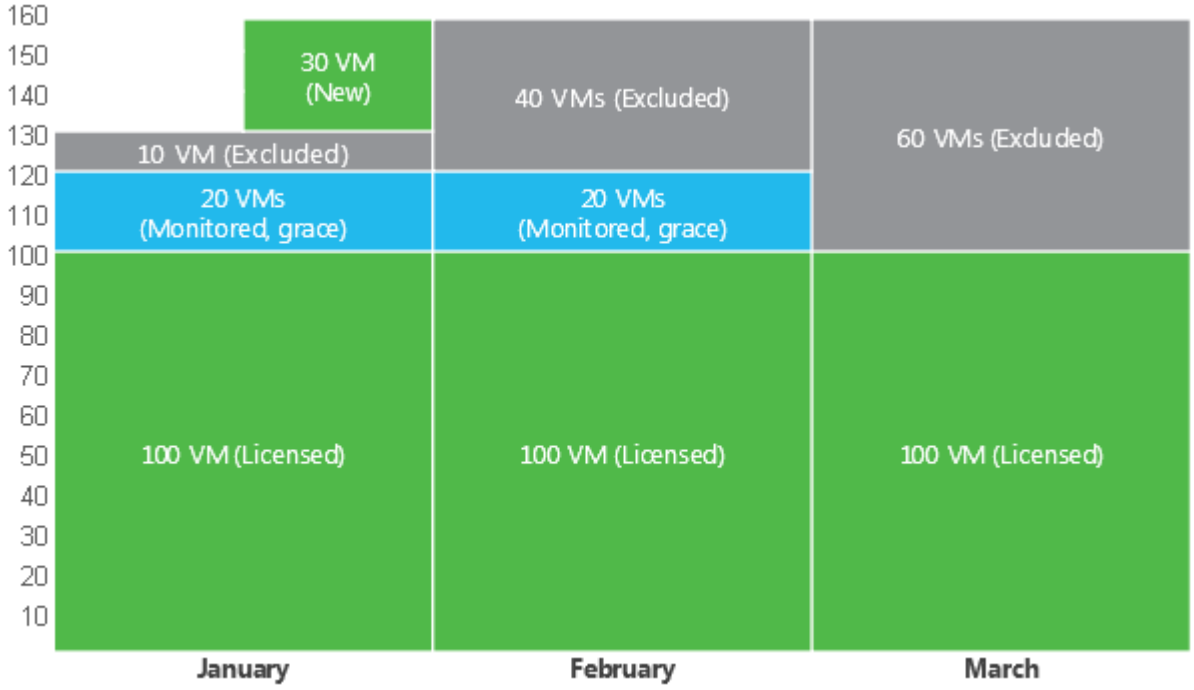
By the end of the grace period, you must update the existing license or decrease the number of managed objects. Otherwise, Veeam ONE will exclude from monitoring and reporting objects that exceed the license limit. VMs are excluded with the help of an automatic exclusion rule that is created by Veeam ONE. You can review VMs covered by this rule in Veeam ONE server settings. For details, see Choosing VMs and VM Containers to Monitor and Report On. If you exceed the number of monitored computers with installed Veeam Agents, file shares and VMs protected on monitored Veeam Backup & Replication servers, Veeam ONE will not exclude any objects from monitoring or reporting. For objects that exceed the license limit, Veeam ONE Web Client will generate Veeam Backup & Replication reports with the Veeam watermark.

In addition to managing objects that exceed the license limit by no more than the specified percentage, Veeam ONE allows you to monitor any number of new objects (that is, objects that are monitored for the first time in the current month). Exceed by new objects is supported for *Rental* licenses only.

Consider the following example. Veeam ONE uses a *Rental* license with the license auto update disabled and the expiration date set to 60 days from the license issue date. At the beginning of January the number of VMs is 130, while a license covers 100 VMs. The period for exceeding the license limit is 60 days. Within the first 60 days (in January and February), Veeam ONE will manage 100 + 20 VMs that were discovered first (license limit + 20%). 10 VMs that were discovered last will be excluded from monitoring and reporting. In addition, in the middle of January, Veeam ONE discovers 30 new VMs. Veeam ONE will manage these VMs until the end of the month.

If the license is not updated and the license limit is not increased, Veeam ONE will exclude from monitoring and reporting:

- 30 VMs that exceed the license limit
- 30 VMs that were discovered in January



Exceeding Sockets Limit

For per-socket licenses, Veeam ONE does not offer any grace period. If the number of sockets exceeds the license limit, Veeam ONE will exclude from monitoring and reporting hosts above the license limit.

Security Guidelines

This section includes security features and recommendations for the Veeam ONE infrastructure that will help you prevent potential security issues and reduce the risk of compromising sensitive data.

In This Section

- General Security Considerations
- Securing Veeam ONE Infrastructure
- Veeam ONE Certificates

General Security Considerations

General security considerations include best practices which help you to harden Veeam ONE infrastructure, build a more secure environment, and mitigate risks of being compromised. Ensure that your infrastructure meet the common recommendations described in this section. For more information about hardening specific Veeam ONE components, see Securing Veeam ONE Infrastructure.

Network

To secure the communication channel for network traffic, consider the following recommendations:

- Create network segmentation policies to define network boundaries, control traffic between subnets and limit access to security-sensitive Veeam ONE components.
- Make sure that only ports used by Veeam ONE components are opened. For more information, see Ports.
- Use an isolated network to transport data between Veeam ONE components.
- Disable outdated network protocols:
  - SSL 2.0 and 3.0 as they have well-known security vulnerabilities and are not NIST-approved. For more information, see NIST guidelines.
  - TLS 1.0 and 1.1 if they are not needed. For more information, see NIST guidelines.
  - LLMNR and NetBIOS broadcast protocols to prevent spoofing and man-in-the-middle (MITM) attacks.
  - SMB 1.0 protocol as it has a number of serious security vulnerabilities including remote code execution. For more information, see this Microsoft article.

User Permissions

Administrator privileges on the machine where Veeam ONE Server is deployed allow users to access other infrastructure components. If an attacker gains such permissions, they can erase most of the production data as well as compromise other systems in your environment. To mitigate risks, use the principle of least privilege. Provide the minimal required permissions needed for the accounts to operate correctly. For more information, see Security Groups and Permissions.

File System

Do not add paths writable by untrusted users to the PATH environment variable. A potential attacker may exploit this vulnerability to execute malware or access sensitive data. For more information, see this CWE article.

Security Audit

Perform regular security audits to assess your Veeam ONE infrastructure against security criteria and understand if it is compliant with best practices, industry standards, and federal regulations.

To reduce the risk of exploiting vulnerabilities by attackers, follow these recommendations:

- Regularly install the latest security updates and patches on Veeam ONE Server and Veeam ONE components.
- Develop an update management strategy to prevent a negative impact on the production environment.

TIP:

You can subscribe to Veeam security advisories published in the Veeam Knowledge Base to stay up to date with the latest security updates.

Microsoft Windows Server

To secure Microsoft Windows-based components for Veeam ONE infrastructure, consider the following recommendations:

- Use operating system versions with Long Term Servicing Channel (LTSC). For these versions, Microsoft provides extended support including regular security updates. For more information, see this Microsoft article.
- Turn on Microsoft Defender Firewall with Advanced Security. Set up rules for inbound and outbound connections according to your infrastructure and Microsoft best practices. For more information, see this Microsoft article.
- Disable remote services if they are not needed:
  - Remote Desktop Service
  - Remote Registry service
  - Remote PowerShell
  - Windows Remote Management service

NOTE:

Specific Veeam ONE components require additional configuration described in the Securing Veeam ONE Infrastructure section.

Securing Veeam ONE Infrastructure

This section includes recommendations for hardening specific Veeam ONE components in addition to general security considerations.

Infrastructure Planning

For large-scale environments, it is recommended to add Veeam ONE Server and other components to a management domain in a separate Active Directory forest.

For medium-sized and small environments, Veeam ONE components can be placed to a separate workgroup.

In both cases, Veeam ONE components should be placed to a separate network where applicable.

Veeam ONE Server

To secure Veeam ONE Server, consider the following recommendations:

- **Restrict outbound connections**. To enable product update check, automatic license update, and license usage reporting, Veeam ONE Server must be connected to the internet and be able to send requests to servers on the internet. Allow only HTTPS connections to the Veeam License Update Server (`one.butler.veeam.com`), Veeam Intelligence endpoints, and Microsoft WSUS servers or Microsoft Update sites.
- **Restrict inbound connections**. Inbound connectivity to Veeam ONE Server from the internet must not be allowed.
- **Restrict collecting data from untrusted Linux VMs**. Do not disable SSH fingerprint validation for machines that do not meet specific conditions. For more information, see Guest OS Credentials.
- **Enable automatic update of Veeam Intelligent Diagnostics signatures**. To get relevant information about known issues in configuration and performance of backup infrastructure, make sure that Veeam Intelligent Diagnostics signatures are updated regularly. For more information, see Other Settings.
- **Use the recommended Access Control List (ACL) for the custom installation folder**. If you specify a custom installation folder for Veeam ONE, use the recommended ACL configuration to prevent privilege escalation and arbitrary code execution (ACE) attacks. Remove all inherited permissions from this folder. Then, add the following permissions:
    - Administrators: Full control, applies to this folder, subfolders and files
    - SYSTEM: Full control, applies to this folder, subfolders and files
    - CREATOR OWNER: Full control, applies to subfolders and files only
    - Users: Read & Execute, applies to this folder, subfolders and files

Veeam ONE Database

The Veeam ONE configuration database stores credentials of user accounts required to connect to virtualization servers and other systems in the backup infrastructure. All passwords stored in the database are encrypted. However, users that have administrator privileges on backup servers can decrypt passwords which is a potential threat.

To secure the Veeam ONE configuration database, consider the following recommendations:

- Check that only authorized users can access Veeam ONE Server and the server that hosts the Veeam ONE configuration database (if the database runs on a dedicated server).
- To protect Veeam ONE data, back up the Veeam ONE database on a regular basis. Also, make sure that the repository for Veeam ONE database backups is not located in the same network with Veeam ONE Server. For more information, see Database.

Veeam ONE Web Services

The Veeam ONE Web Services component uses Microsoft IIS Web Server. To reduce the attack surface, follow CIS Benchmark security guidelines for your Microsoft IIS version.

Veeam ONE Clients

To secure Veeam ONE clients, consider the following recommendations:

- **Use client certificates for user authentication**. To protect user accounts with additional user verification, allow users to log in to Veeam ONE Web Client with multi-factor authentication (MFA) through client certificate configuration. For more information, see Configuring Client Certificate Mapping Authentication.
- **Configure user session settings and timeouts**. To reduce the number of user sessions opened for a long time in Veeam ONE Client, set the idle timeout to automatically log off users and administrators. Also, limit the number of simultaneous login sessions under the same user credentials to one. For more information, see Login Sessions.
- **Disable multi-tenant access**. Restrict access to Veeam ONE Web Client and Veeam ONE Client for users who are not included in Veeam ONE security groups. For more information, see Other Settings.

Veeam ONE Certificates

When you configure Veeam ONE infrastructure, you can specify what TLS certificate must be used to establish a secure connection between Veeam ONE components. Veeam ONE offers the following options for TLS certificates:

- Keep the default self-signed TLS certificate generated by Veeam ONE during installation or upgrade.
- Generate a new self-signed TLS certificate. For more information, see Generating Self-Signed Certificates.
- Select an existing TLS certificate from the certificate store. For more information, see Importing Certificate from Certificate Store.
- Import a TLS certificate from a file in the PFX format. For more information, see Importing Certificate from PFX Files.

If you plan to use a certificate issued by your own Certificate Authority (CA), make sure that the certificate meets the requirements. For more information, see Using Certificate Signed by Internal CA.

Generating Self-Signed Certificates

To generate self-signed TLS certificates, Veeam ONE uses RSA algorithm with a 2048-bit key length and SHA-2 hashing algorithm. The created TLS certificate is saved to the *Shared* certificate store. The following types of users can access the generated TLS certificate:

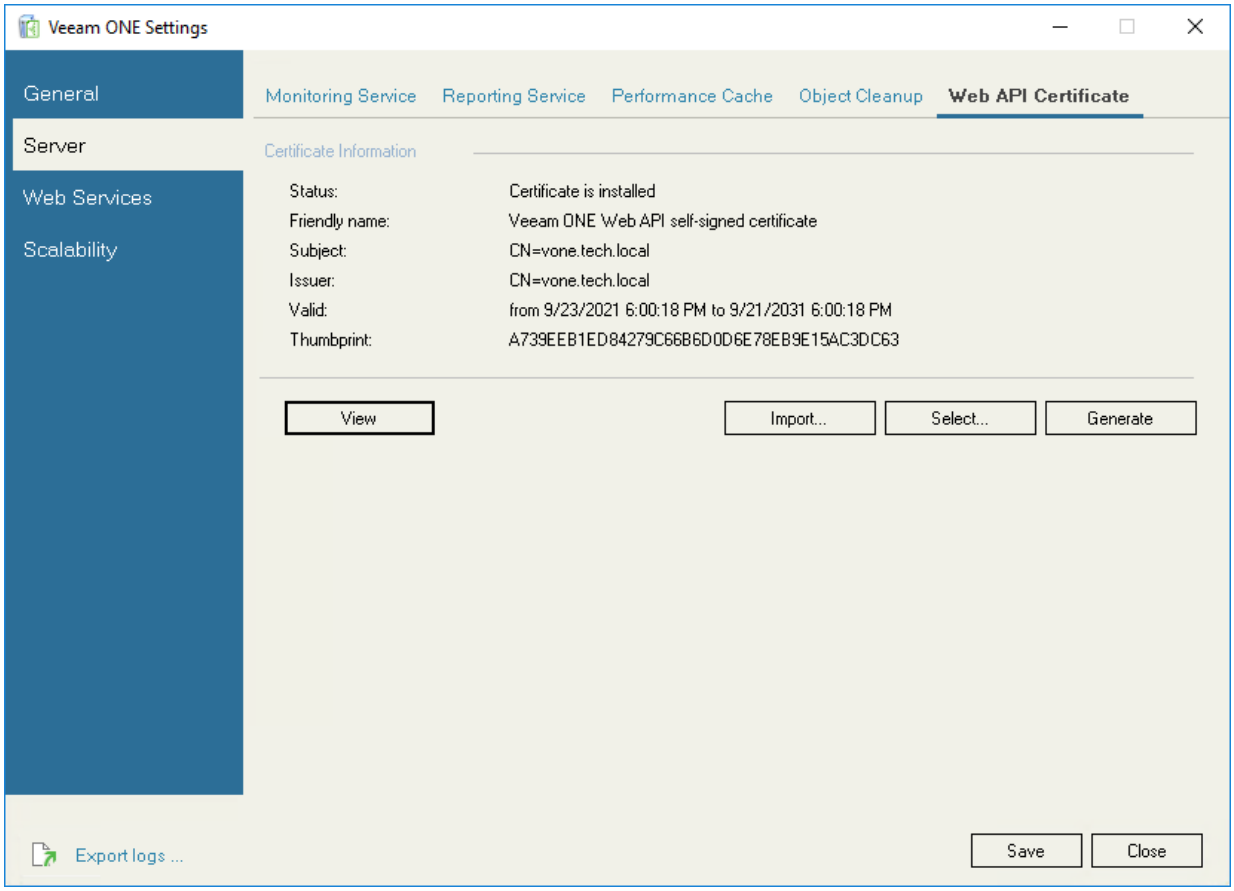
- User who created the TLS certificate
- LocalSystem user account
- Local Administrators group

> **NOTE:**
>
> When you generate a self-signed TLS certificate with Veeam ONE, you cannot include several aliases to the certificate and specify a custom value in the *Subject* field. The *Subject* field value is taken from the Veeam ONE license installed on Veeam ONE Server.

To generate a new self-signed TLS certificate, do the following:

1. Run the Veeam ONE Settings utility.

   For more information, see Veeam ONE Settings Utility.
2. In the **Server** section, open the **Web API Certificate** tab.
3. Click **Generate**.
4. To use a newly generated certificate, in the displayed window, click **Yes**.



NOTE:

If you replace the default certificate with another self-signed certificate, you must configure a trusted connection between the Veeam ONE Web Client and a web browser later. For details, see Accessing Veeam ONE Components.

Importing Certificate from Certificate Store

If Veeam ONE Server has been issued a TLS certificate signed by a CA and the TLS certificate is located in the Microsoft Windows certificate store, you can use this certificate to establish a secure connection between Veeam ONE components.

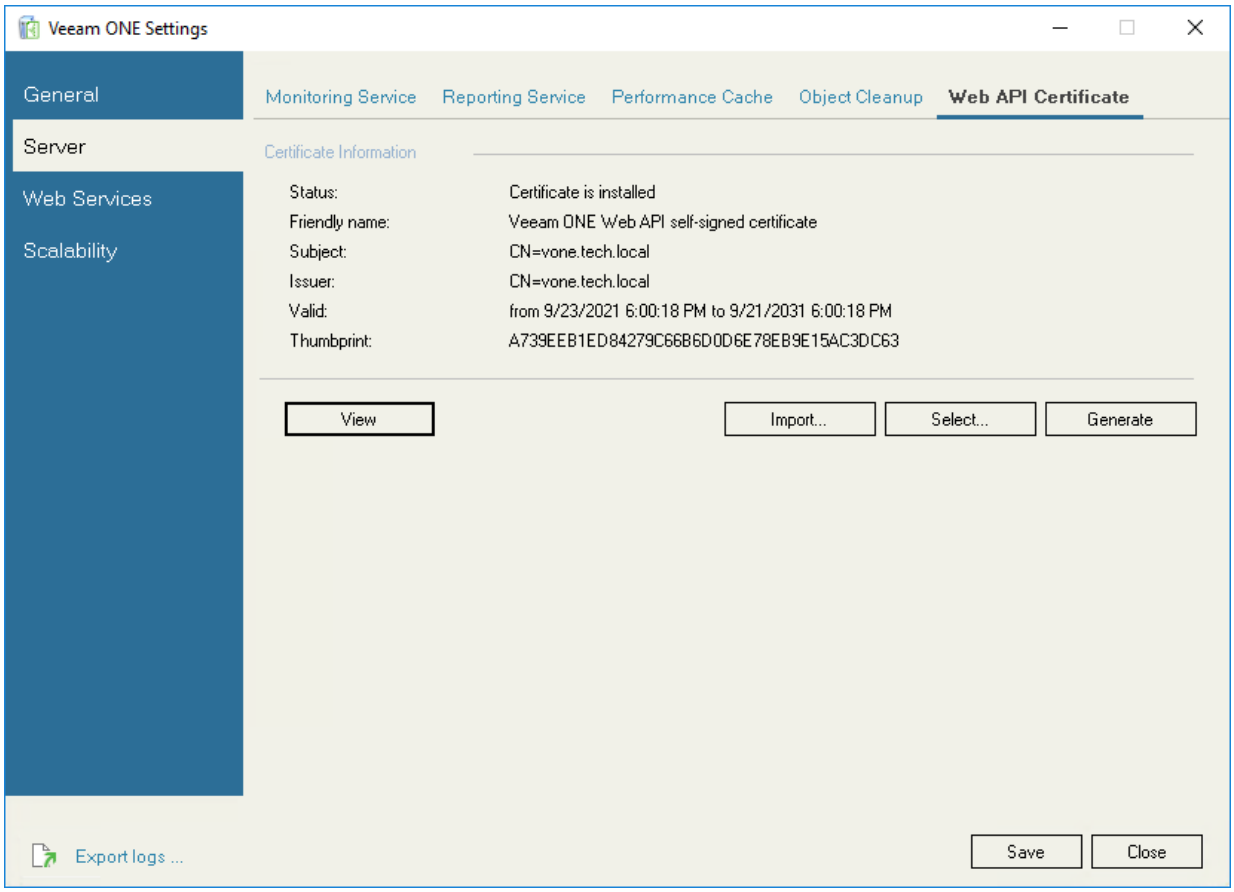
To select a certificate from the Microsoft Windows certificate store, do the following on the machine where Veeam ONE server component is installed:

1. Run the Veeam ONE Settings utility.

   For more information, see Veeam ONE Settings Utility.

2. In the **Server** section, open the **Web API Certificate** tab.

3. Click **Select** and select the certificate from the **Trusted Root Certificate Authorities** store.



Importing Certificate from PFX Files

You can import the following certificates in the PFX format:

- A TLS certificate used by your organization and signed by a CA.
- A self-signed TLS certificate generated with a third-party tool.

NOTE:

Consider the following:

- The TLS certificate must pass validation on Veeam ONE Server. Otherwise, you will not be able to import the TLS certificate.
- If a PFX file contains a certificate chain, only the end entity certificate will be imported.

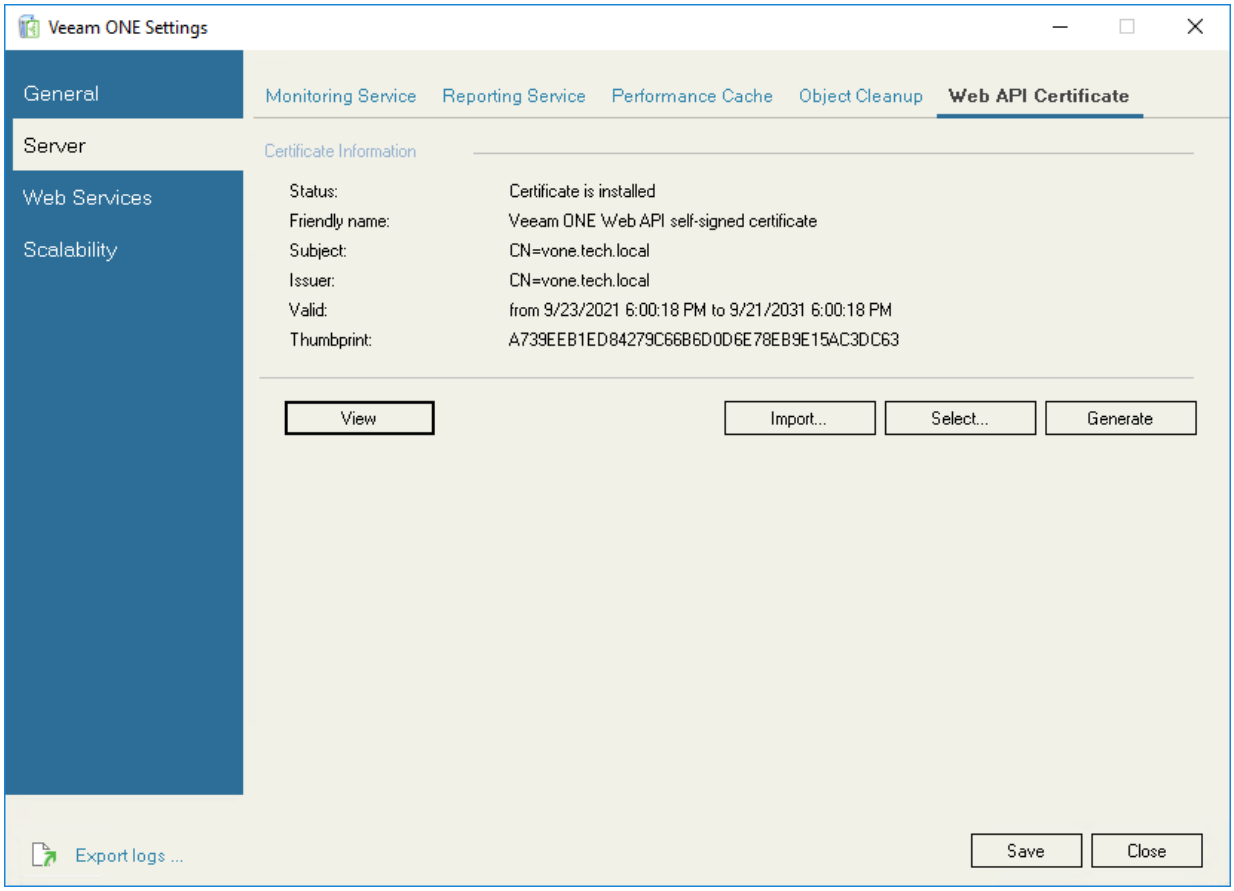
To import a TLS certificate from a PFX file, do the following on the machine where Veeam ONE server component is installed:

1. Run the Veeam ONE Settings utility.

   For more information, see Veeam ONE Settings Utility.

2. In the **Server** section, open the **Web API Certificate** tab.

3. To import the certificate, click **Import** and browse the certificate file.



Using Certificate Signed by Internal CA

If you want to use a certificate signed by your own Certification Authority (CA), consider the following:

- Make sure that Veeam ONE server trusts the CA. That means that the Certification Authority certificate must be added to the Trusted Root Certification Authority store on the Veeam ONE server. Also, Certificate Revocation List (CRL) must be accessible from the Veeam ONE server.
- If you use Windows Server Certification Authority, issue a Veeam ONE certificate based on the built-in Subordinate Certification Authority template or templates similar to it. You can manage templates with the Certificate Templates MMC snap-in.

Veeam ONE Website Certificate Requirements

- The certificate subject is equal to the fully qualified domain name of the Veeam ONE server. For example: `oneserver.domain.local`.
- The **Subject Alternative Name** field contains the FQDN of the Veeam ONE server. For example: `DNS:oneserver.domain.local`.
- The minimum key size is 2048 bits.
- The key usage is `Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment`.
- The enhanced key usage is `Server Authentication (1.3.6.1.5.5.7.3.1)`.

Veeam ONE Web API Certificate Requirements

- The certificate subject is equal to the fully qualified domain name of the Veeam ONE server. For example: `oneserver.domain.local`.
- The **Subject Alternative Name** field contains the FQDN of the Veeam ONE server. For example: `DNS:oneserver.domain.local`.
- The minimum key size is 2048 bits.
- The key usage is `Digital Signature, Non-Repudiation`.
- The enhanced key usage is `Server Authentication (1.3.6.1.5.5.7.3.1)`.

Installing Veeam ONE

This section will guide you through the process of Veeam ONE installation.

Before You Begin

Before you begin installation, check the following prerequisites:

- Check platform and system requirements.

  Check that your virtual platform is supported. Make sure the machine where Veeam ONE will be installed meets hardware and software requirements.

- Check account permissions.

  Make sure the user account under which Veeam ONE will be installed has sufficient permissions.

- Check ports.

  Make sure all required ports are open for communication between Veeam ONE components, virtualization servers, VMware Cloud Director servers and Veeam Backup & Replication servers.

- Check your Secondary Logon service is enabled

  Make sure that your Secondary Logon service is enabled. Disabling a Secondary Logon can affect the installation process if your Veeam ONE service account is different from the account under which the installation wizard is running.

- Download the Veeam ONE installation image file at https://www.veeam.com/downloads.html.

  Burn the downloaded `ISO` image file to a CD/DVD or mount the installation image using disk image emulation software. If you install Veeam ONE on a VM, use built-in tools of the virtualization management software to mount the installation image to the VM.

- [Optional] Creating Veeam ONE Database with SQL Script.

  Normally, the setup automatically creates the Veeam ONE database in the course of installation. However, in some circumstances it might be necessary to create the database with a SQL script instead of using the **Veeam ONE Setup** wizard. Before installing Veeam ONE, you can create the Veeam ONE database by executing a SQL script that is included with the Veeam ONE installation image.

All-in-One Installation

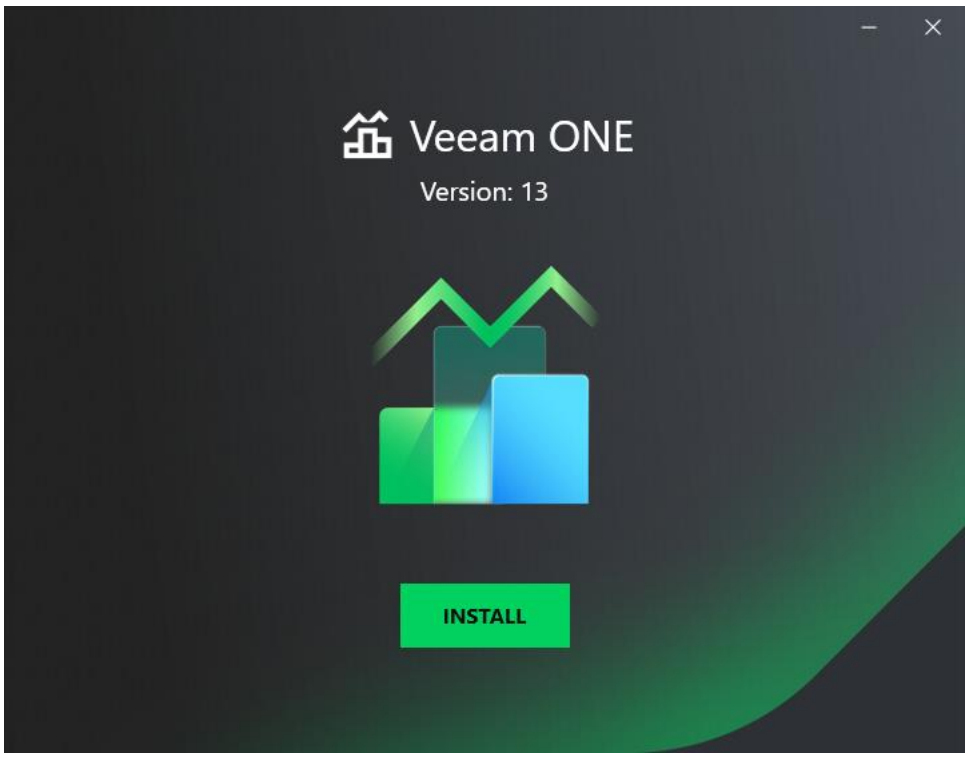
In the all-in-one deployment scenario, all Veeam ONE components are installed on a single machine. For details on this scenario, see All-in-One Deployment.

To install Veeam ONE using the typical scenario, follow these steps.

Step 1. Launch Splash Window

After you mount or insert the disk with Veeam ONE installation image, **Autorun** will open a splash screen with installation options. On the splash window, click **Install** to launch the **Veeam ONE Setup** wizard.

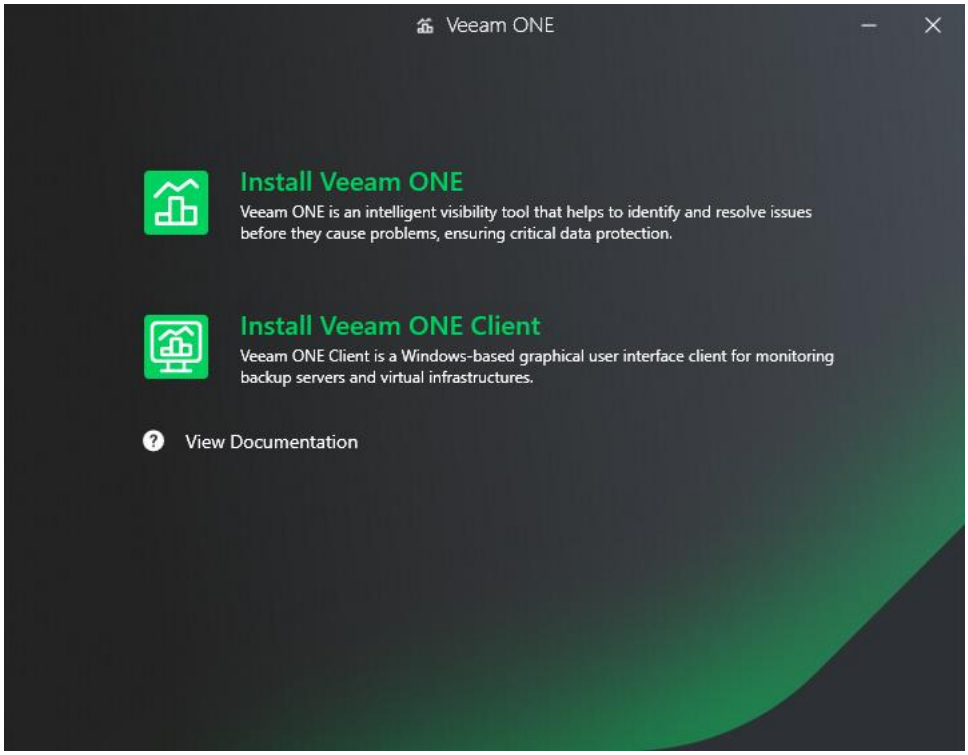
If **Autorun** is disabled, run the `Setup.exe` file from the installation image. Alternatively, you can right-click the new disk in **My Computer** and select **Execute Veeam ONE Autorun**.



Step 2. Select Component

At the **Select Veeam ONE Component** step of the wizard, select **Install Veeam ONE**.

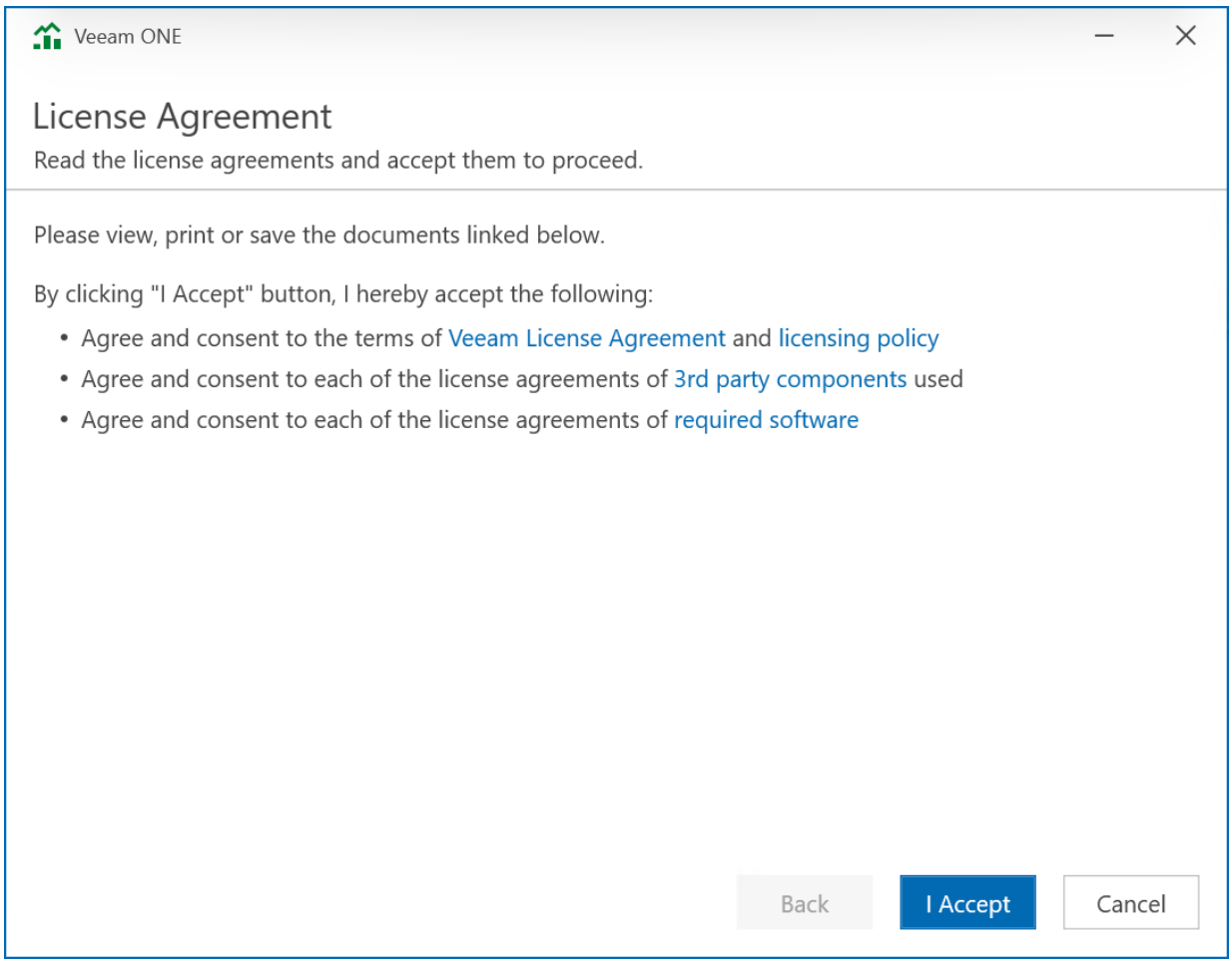
To open Veeam Help Center from the setup wizard, click **View Documentation**.



Step 3. Accept License Agreements

At the **License Agreement** step of the wizard, read and accept Veeam license agreement, licensing policy, 3rd party components and required software license agreements. You will not be able to continue installation until you accept license agreements.

To read the terms of the license agreements, click the individual links.

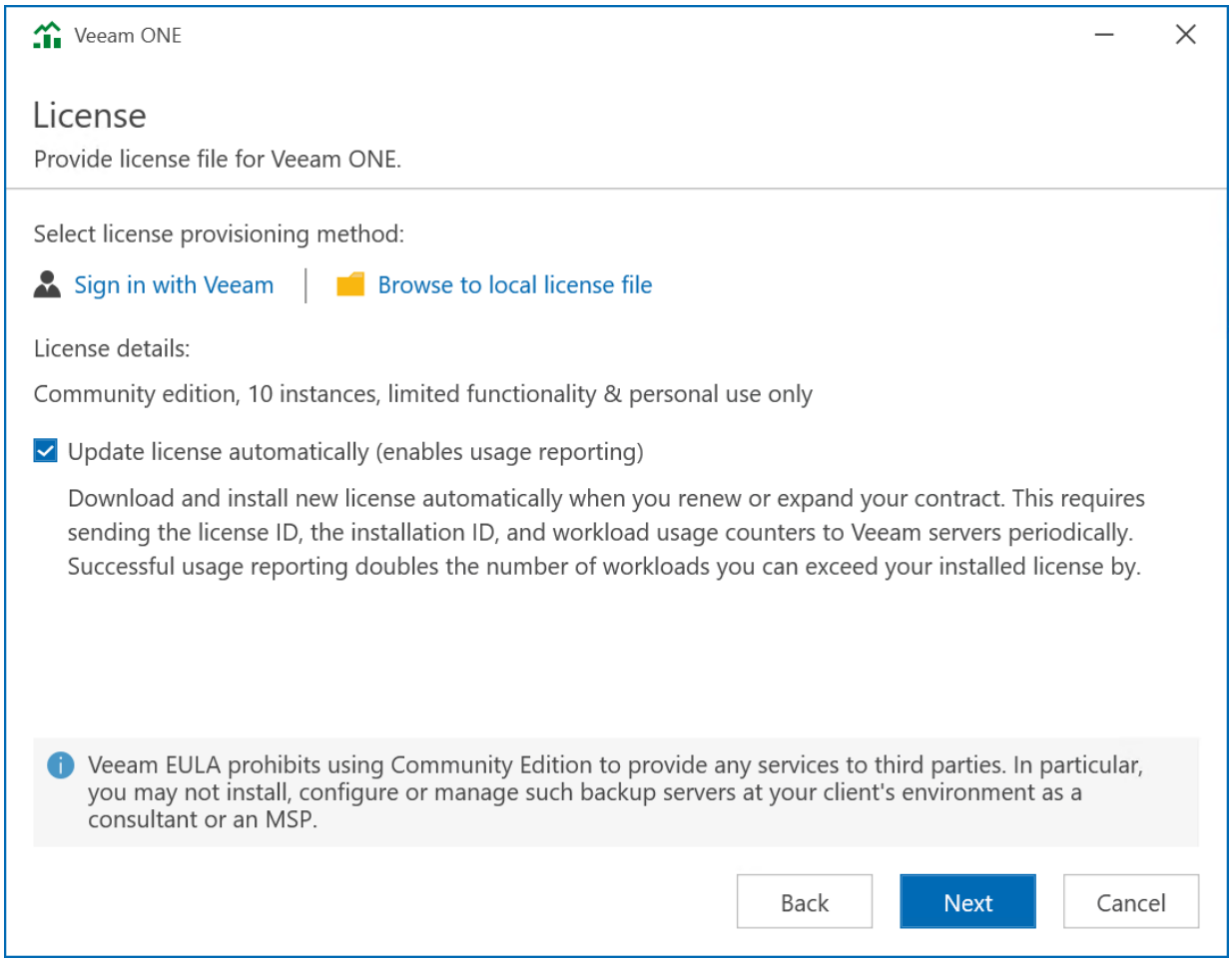


Step 4. Provide License

At the **License** step of the wizard, click one of the two options to provide a license:

- **Sign in with Veeam** – open the Veeam account Sign in screen to log in with your Veeam account credentials if you already have a registered license on your account.
- **Browse to local license file** – specify the local path to the license file.

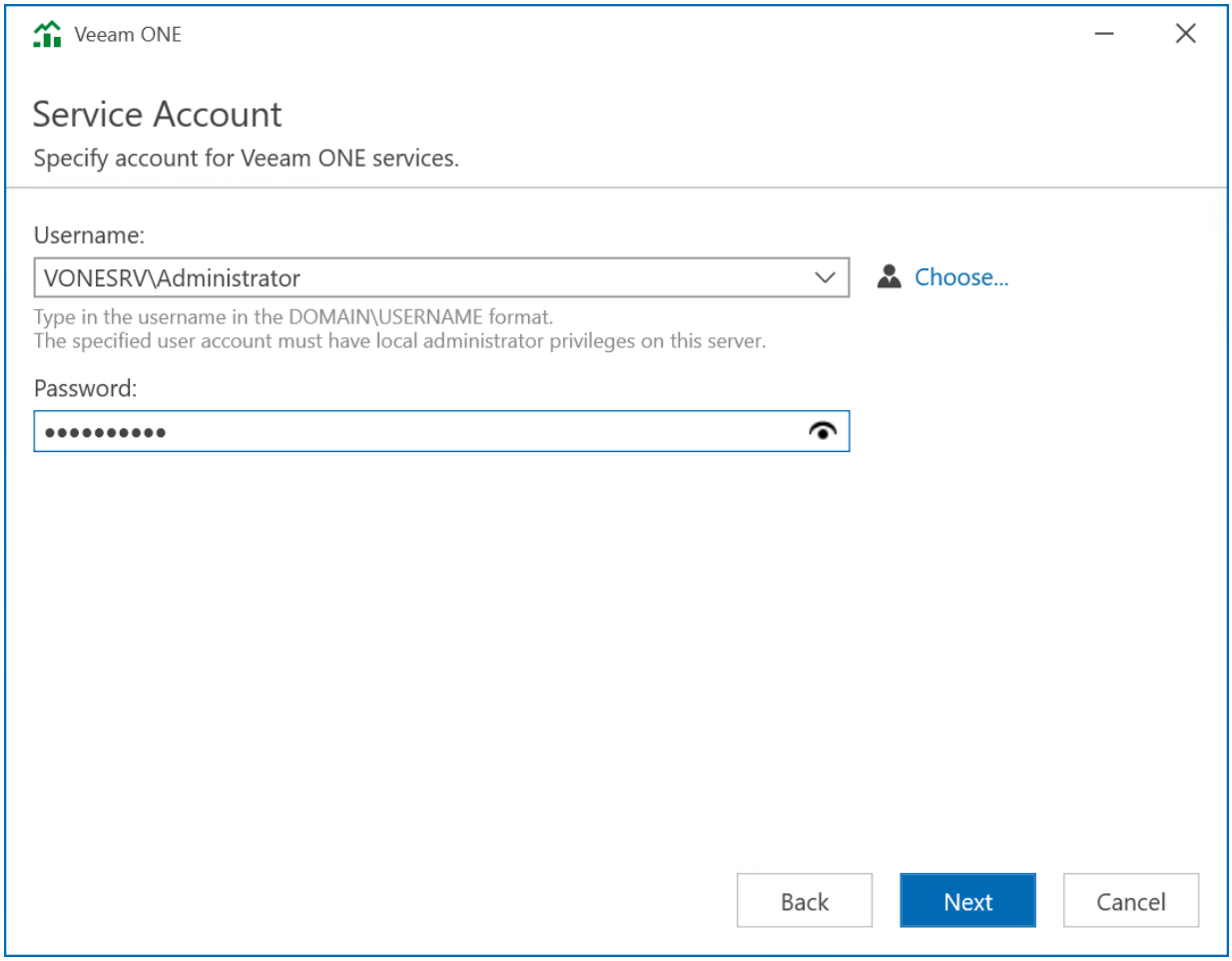
To install new licenses automatically when you renew or expand your contract, select the **Update license automatically** check box. If you enable the automatic license update, and therefore enable usage reporting, you will double the number of workloads by which you can exceed your installed license. Note that for *Evaluation* and *NFR* licenses automatic license update must be enabled.



Step 5. Specify Service Account Credentials

At the **Service Account** step of the wizard, specify credentials of the account under which the Veeam ONE services will run. The user name must be specified in the *DOMAIN|USERNAME* format. Alternatively click **Choose** to select an existing user account.

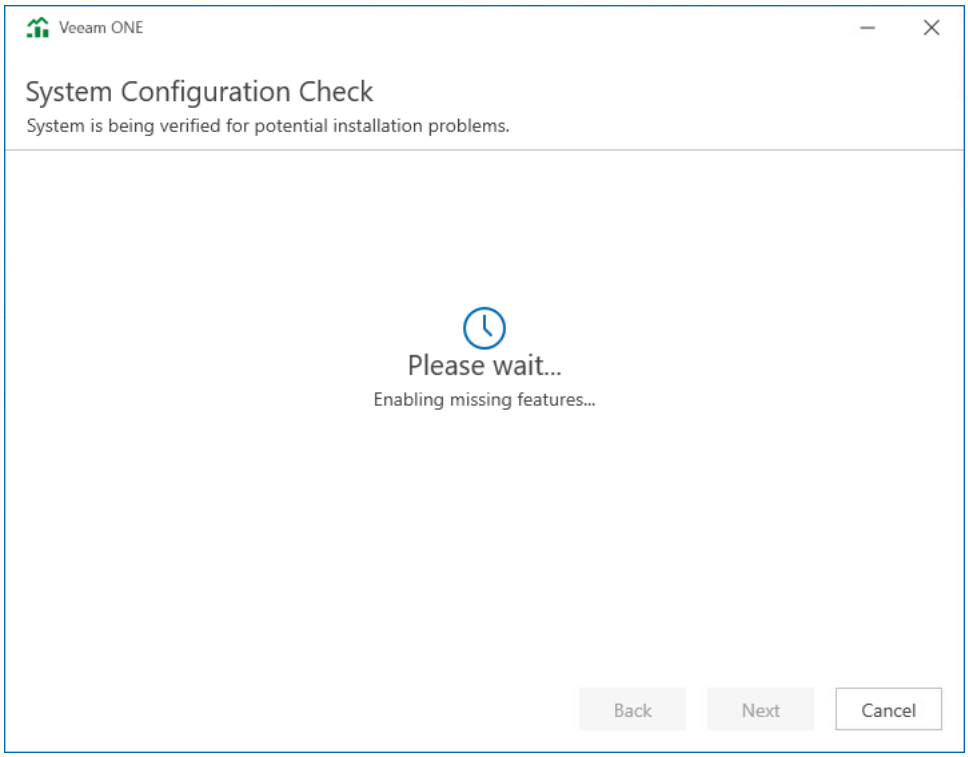
For details on required permissions for the service account, see Veeam ONE Service Account.



Step 6. Perform System Configuration Check

Before proceeding with the installation, the installer will perform system configuration check to determine if all prerequisite software is available on the machine. To learn what software is required for Veeam ONE, see System Requirements.

If some of the required software components are missing, the setup wizard will enable the missing software components and features automatically.

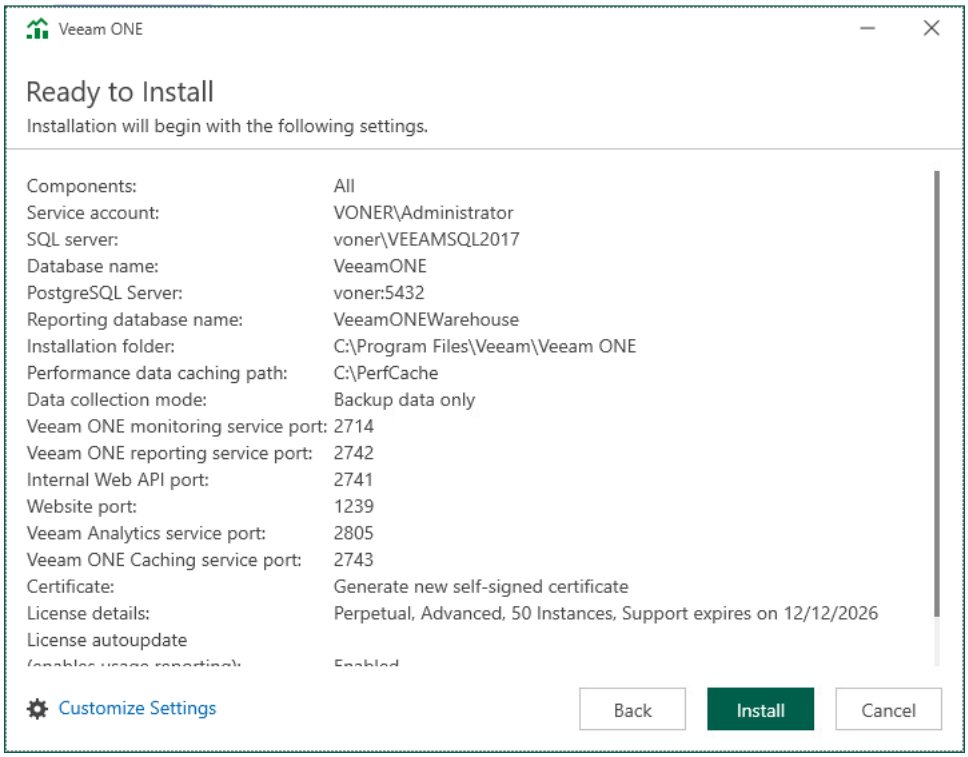


Step 7. Review Installation Summary

At the **Ready to Install** step of the wizard, review installation configuration to ensure that you have provided correct settings.

If you need to change any settings in the installation summary, click **Customize Settings** and proceed to Step 8. Select Architectural Components.

Click **Install** to begin the installation.

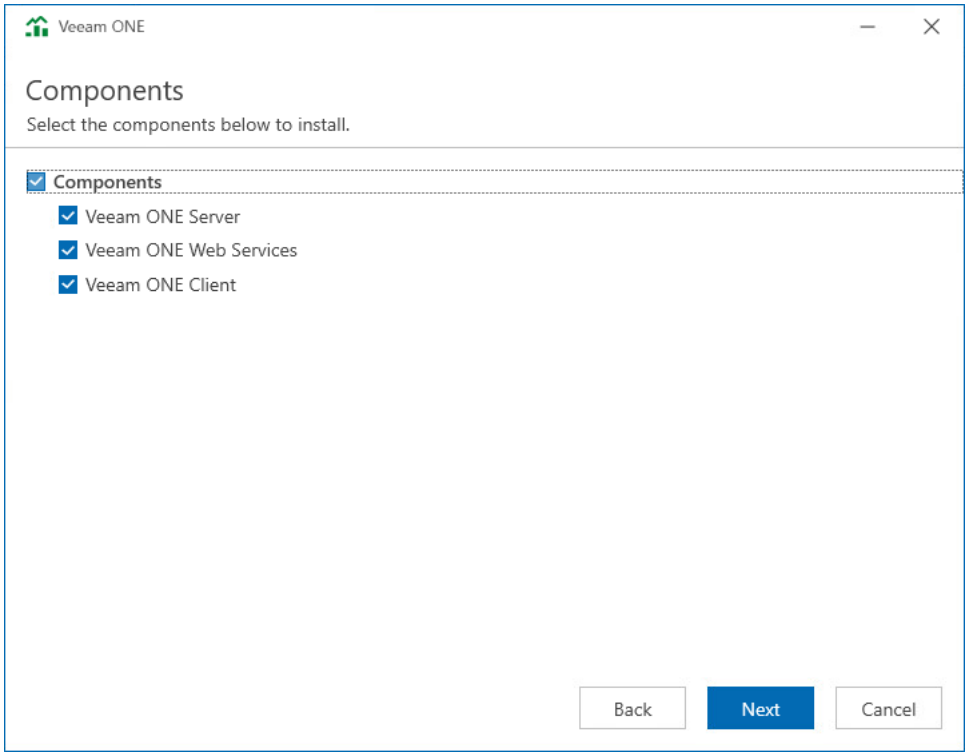


When the installation completes, click **Finish** to close the wizard.

Step 8. Select Architectural Components

For an All-in-One installation, select the **Components** check box to install all components:

- Veeam ONE Server
- Veeam ONE Web Services
- Veeam ONE Client



Step 9. Choose Monitoring Database

At the **Monitoring Database** step of the wizard, choose a Microsoft SQL Server instance that will host the Veeam ONE database.

- If you do not have a Microsoft SQL Server instance that you can use for Veeam ONE database, select the **Install new instance of SQL Server** option.

  If this option is selected, the setup will install Microsoft SQL Server 2017 Express locally, on the computer where you are installing Veeam ONE.

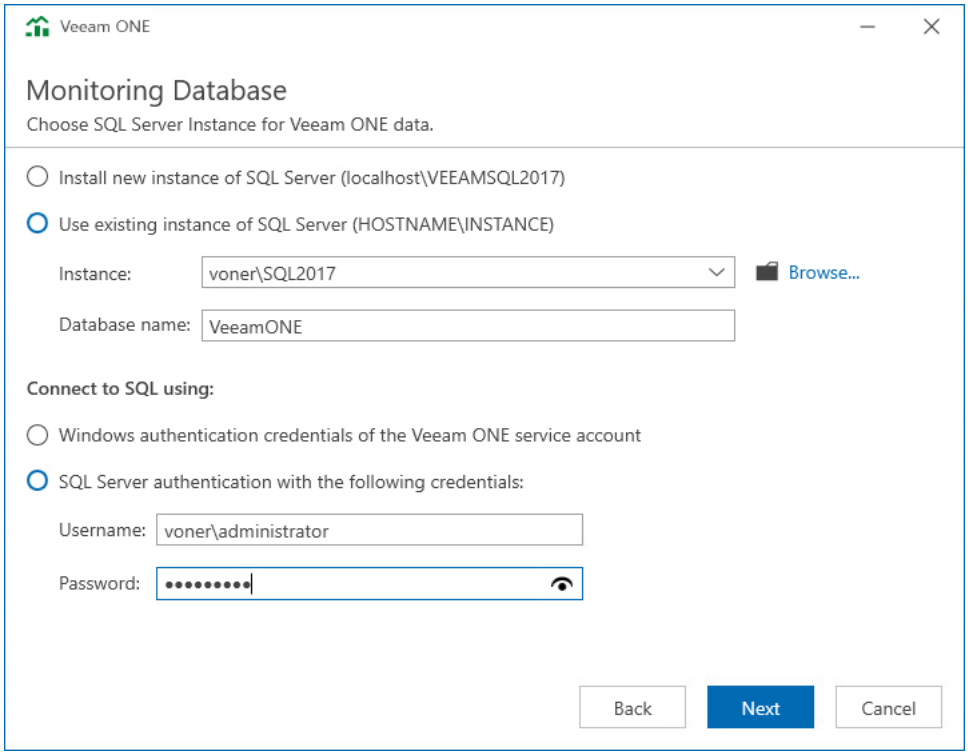
  > **NOTE:**
  > - If a Microsoft SQL Server instance that meets Veeam ONE system requirements is detected on the machine, you can only use the existing local Microsoft SQL Server instance or choose a one that runs remotely. The option to install a new Microsoft SQL instance will be unavailable in this case.
  > - If you choose to host Veeam ONE database on Microsoft SQL Server Express, consider is a 10 GB database size limitation for this edition. For details, see Editions and Supported Features for SQL Server.

- If you want to use an existing local or remote Microsoft SQL Server instance, select the **Use existing instance of SQL Server** option and choose a local Microsoft SQL Server instance or browse to a Microsoft SQL Server instance running remotely. You can enter the address of a preferred Microsoft SQL Server manually or use the **Browse** button to choose among available remote instances.

  In the **Database name** field, specify the name of the database that will be created by Veeam ONE. Provide credentials for the account that will be used by Veeam ONE components to access the database. You can enter credentials explicitly or use Windows authentication credentials of the Veeam ONE service account to connect to the Microsoft SQL Server. For details on required permissions for the account, see Connection to Microsoft SQL Server.

- If you already have an existing Veeam ONE database that you want to use in your deployment, select the **Use existing instance of SQL Server** option and choose a Microsoft SQL Server instance that hosts the database. This can be a database that you have previously created with a SQL script. In the **Database name** field, specify the name of the database.

  Provide credentials for the account that will be used by Veeam ONE components to access the database. You can enter credentials explicitly or use Windows authentication credentials of the Veeam ONE service account to connect to the Microsoft SQL Server. For details on required permissions for the account, see Connection to Microsoft SQL Server.



Step 10. Choose Reporting Database

At the **Reporting Database** step of the wizard, choose a PostgreSQL Server instance that will host the Veeam ONE reporting database.

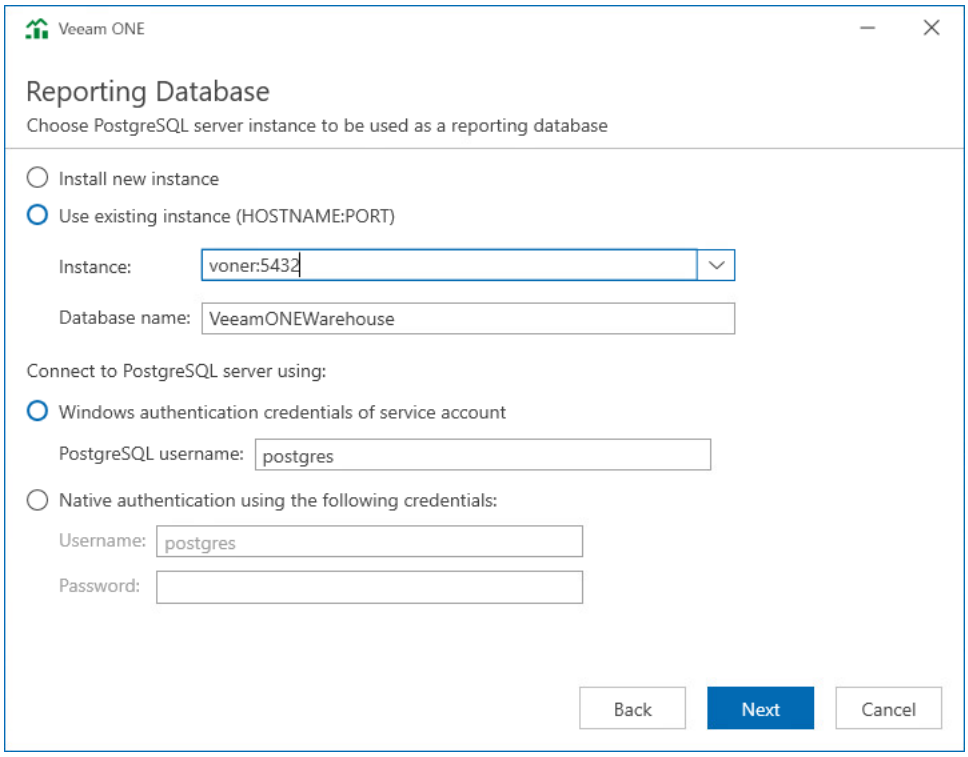
The reporting database is a dedicated database that stores PostgreSQL logs and metrics related to system activities, performance, and other relevant data for analysis and reporting purposes.

- If you do not have a PostgreSQL instance that you can use for Veeam ONE database, select the **Install new instance** option.

  If this option is selected, the setup will install PostgreSQL locally, on the computer where you are installing Veeam ONE.

- If you want to use an existing local or remote PostgreSQL instance, select the **Use existing instance** option and enter the instance and database name.

- In the **Connect to PostgreSQL server using** section, select an authentication mode to connect to the database server instance: Microsoft Windows authentication or native database server authentication. If you select the native authentication, enter credentials of the PostgreSQL database account.



Step 11. Choose Data Locations

In the **Installation path**, choose the installation directory. In the typical installation mode, the setup installs all components to a single directory and creates a subdirectory for every Veeam ONE component.

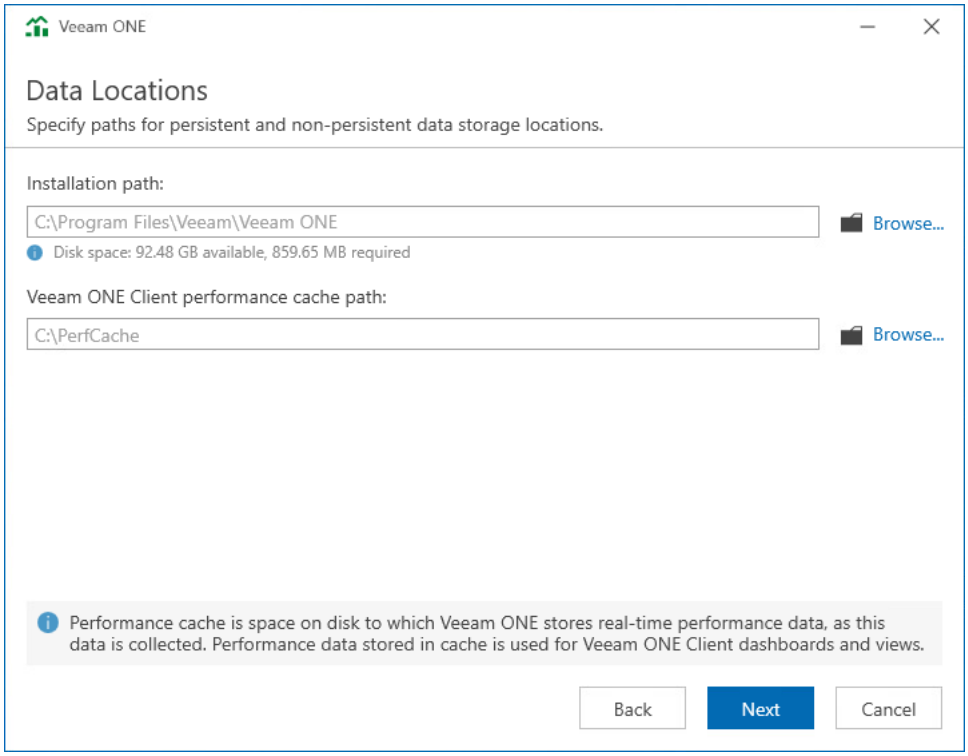
In the **Veeam ONE Client performance cache path**, choose a directory where the performance cache must be located.

Performance cache is space on disk to which Veeam ONE stores real-time performance data, as this data is collected. Performance data stored in cache is used for Veeam ONE Client dashboards and views. Disk-based performance cache allows significantly decrease RAM utilization on the machine that runs the Veeam ONE Server component.

By default, the performance cache is stored to the `C:\PerfCache` folder. To store the cache to a different folder, click **Browse** next to the **Path** field and specify a path to the new folder.

When choosing a location for performance cache, consider the following recommendations:

- Make sure that the disk where the performance cache is located can quickly complete read and write requests. Do not locate the cache remotely in networks with high latency values.
- For large monitoring environments, place the performance cache on an SSD local to the machine where the Veeam ONE Server component runs. For small and medium monitoring environments, a HDD is normally enough.
- Length of the performance cache folder path must not exceed the Windows Max Path Limitation value. For details, see Microsoft Learn.
- Make sure there is enough disk space for performance cache. The cache is cleared on an hourly basis, as new data is collected; however, in large monitoring environments it can take significant disk space. For example, in the custom deployment mode, during peak loads, the cache can take up to 6 GB disk space for each 1000 VMs.



The typical installation requires around 850 MB of free space on a disk (plus additional space if you choose to install Microsoft SQL Server instance on the same machine). Be aware that depending on the size of your virtual infrastructure and frequency of data collection, the database may grow large and require more space. Be sure to adjust to this condition by freeing up more disk space when needed.

Step 12. Choose Data Collection Mode

At the **Data Collection Mode** step of the wizard, choose the mode in which Veeam ONE will collect data from virtualization and Veeam Backup & Replication servers.

Data collection mode determines what metrics Veeam ONE will collect, and specifies the product configuration in a number of areas. Choosing an appropriate data collection mode allows you to optimize monitoring and reporting performance and improve user experience in Veeam ONE. To learn the difference between the data collection modes, see Data Collection Modes.

Veeam Backup Data Only

The **Veeam backup data only** mode is recommended for users who want to focus on Veeam Backup & Replication and Veeam Backup for Microsoft 365 monitoring and reporting, and do not need a deep visibility of the virtual infrastructure.

In this mode, Veeam ONE collects all inventory, configuration and performance metrics from Veeam Backup & Replication and Veeam Backup for Microsoft 365 servers. It also collects inventory and configuration metrics from virtualization servers, but skips virtual infrastructure performance metrics. As a result, Veeam ONE dashboards, reports and alarms display backup-related data only. For VMware vSphere and Microsoft Hyper-V objects, performance data is not available.

This mode results in the least possible size of the Veeam ONE database and the lowest load on the Veeam ONE server.

Veeam Backup Data and Virtual Infrastructure Performance Monitoring

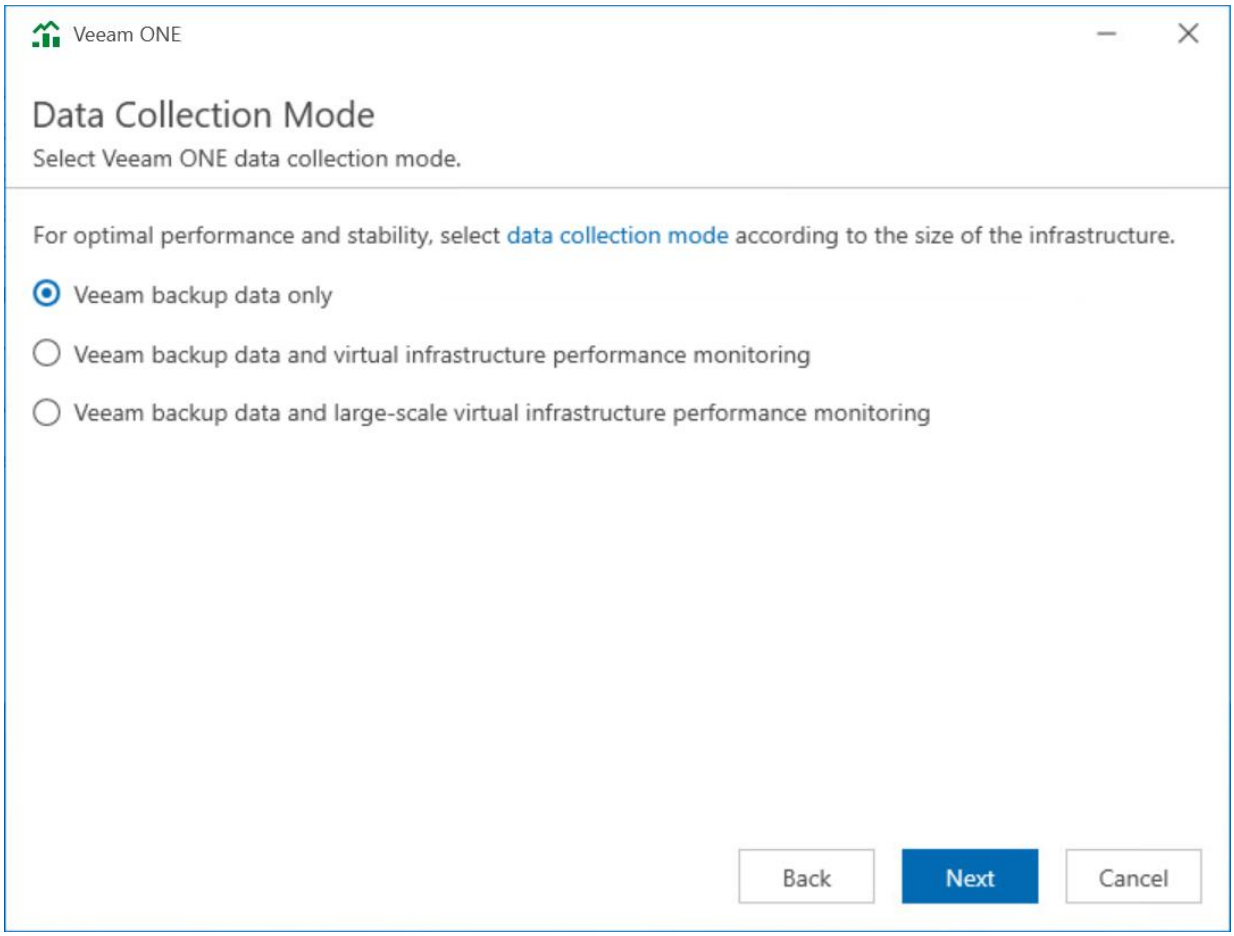
The **Veeam backup data and virtual infrastructure performance monitoring** modes are recommended for users who want to monitor and report on the virtual environment, Veeam Backup & Replication and Veeam Backup for Microsoft 365 infrastructures.

- **Veeam backup data and virtual infrastructure performance monitoring** mode is recommended for small to medium environments up to 100 hosts and 1500 VMs. In this mode, Veeam ONE collects all inventory, configuration and performance metrics, and makes collected data available in dashboards, reports and alarms.

  This mode provides the greatest data granularity level, but results in a greater load on the Veeam ONE server and a larger size of Veeam ONE database.

- **Veeam backup data and large-scale virtual infrastructure performance monitoring** mode is recommended for large environments with more than 100 hosts and 1500 VMs. In this mode, Veeam ONE collects all metrics required for alarms and reports.

  This mode results in a lower load on the Veeam ONE server and a smaller size of the Veeam ONE database.



Step 13. Specify Connection Ports

At the **Port Configuration** step of the wizard, specify connection settings for Veeam ONE components, Veeam ONE Web API and Veeam Analytics service:

- In the **Veeam ONE monitoring service port** field, type a number of the port that will be used to interact with Veeam ONE Monitoring service.

  The default port number is `2714`.

- In the **Veeam ONE reporting service port** field, type a number of the port that will be used to interact with Veeam ONE Reporting service.

  The default port number is `2742`.

- In the **Veeam ONE Web API port** field, type a number of the port that will be used by Veeam ONE Monitoring service and Web Services component to interact with Veeam ONE Reporting service.

  The default port number is `2741`.

- In the **Website port** field, type a number of the port that will be used to access the Veeam ONE Web Client through a web browser.

  The default port number is `1239`.

- In the **Veeam Analytics service port** field, type a number of the port that Veeam Analytics service will use to collect data from connected Veeam Backup & Replication servers.

  The default port number is `2805`.

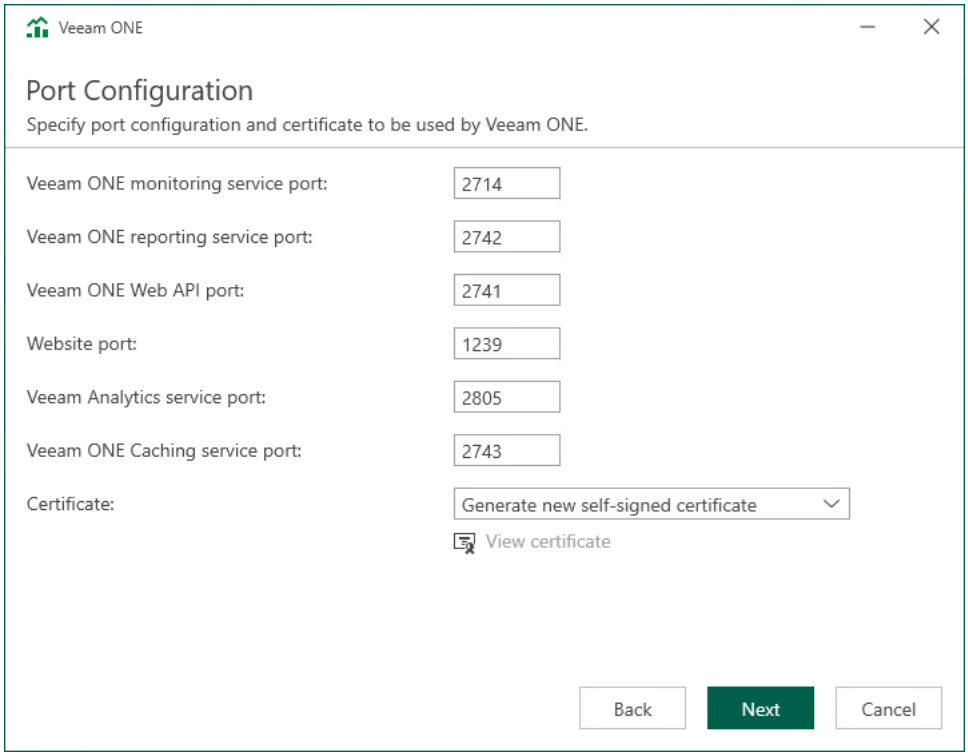
- In the **Veeam ONE Caching service port** field, type a number of the port that the Veeam ONE Caching service will use to provide cached report data by Veeam ONE Reporting service requests.

  The default port number is `2743`.

- In the **Certificate** list, choose a certificate that will be used to secure traffic between the web browser, Veeam ONE Web Services and Veeam ONE Reporting service.

  You can choose an existing certificate installed on the machine. If the setup wizard does not find an appropriate certificate to be used, it generates a self-signed certificate.

  > **NOTE:**
  > - If you generate or choose a self-signed certificate, you must configure a trusted connection between the Veeam ONE Web Client website and a web browser later. For details, see Configuring Trusted Connection.
  > - You can change the selected certificate after installation. For details on changing Veeam ONE Web Client website certificate, see Change Default Certificate. For details on changing Veeam ONE Reporting service certificate, see Veeam ONE Server Settings.

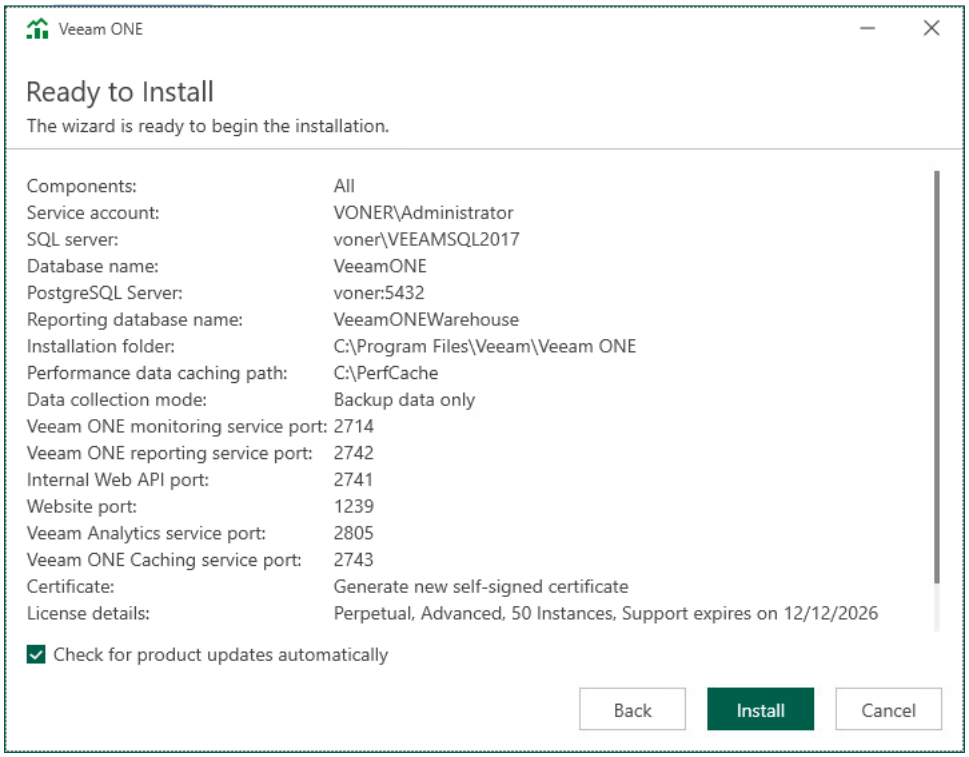

Veeam ONE
Port Configuration
Specify port configuration and certificate to be used by Veeam ONE.
Veeam ONE monitoring service port:
2714
Veeam ONE reporting service port:
2742
Veeam ONE Web API port:
2741
Website port:
1239
Veeam Analytics service port:
2805
Veeam ONE Caching service port:
2743
Certificate:
Generate new self-signed certificate
View certificate
Back
Next
Cancel

Step 14. Review Installation Summary

At the **Ready to Install** step of the wizard, review installation configuration to ensure that you have provided correct settings.

Select the **Check for product updates automatically** check box if you want Veeam ONE to automatically check and download available updates.

Click **Install** to begin the installation.



Step 15. Add Veeam ONE Service Account to Veeam ONE Administrators Group

When Veeam ONE installation completes, the installer will prompt you to perform the logoff and logon procedure to create new user groups that will be used to accommodate user accounts for accessing Veeam ONE locally and remotely.

Check that the Veeam ONE service account is included in the *Veeam ONE Administrators* user group. If this account is not a member of the *Veeam ONE Administrators* user group, add it to the group manually.

For details on Veeam ONE user groups, see Security Groups.

Custom Installation

The custom installation scenario implies installing the Veeam ONE Server components (Monitoring service, Reporting service, Veeam ONE Web API) on one machine, and installing the Veeam ONE Web Services component (Veeam ONE Web Client) on another machine. You can also choose to install both components on a single machine in the course of a single installation session. If you choose to install both the Veeam ONE Server and Veeam ONE Web Services components, the custom deployment will mirror the typical, but will not include Veeam ONE Client. You must install Veeam ONE Client separately.

IMPORTANT!

- If you install the Veeam ONE Server and Veeam ONE Web Services components on separate machines, mind the following limitation: you cannot install the server part on the computer that is already hosting the client part, and conversely.
- If you migrate the Veeam ONE Server components to another machine, you must reinstall Veeam ONE Web Services and specify new connection settings at Step 11 of the installation wizard.

Custom installation is only available if you provide either evaluation or paid license. For Veeam ONE Community Edition, the custom installation option is not available. For details on the custom deployment scenario, see Custom Deployment.

The custom installation must proceed in the following order:

1. **Install Veeam ONE Server and set up the database**.

   Run the **Veeam ONE Setup** wizard on a machine that will host the Veeam ONE Server component. At this step, you must choose existing Microsoft SQL Server and PostgreSQL instances or install new embedded instances and specify the name of the database that will be created by the setup. For details, see Installing Veeam ONE Server.

2. **Install the Veeam ONE Web Services**.

   Run the **Veeam ONE Setup** wizard on a machine that will host the Veeam ONE Web Services component. For details, see Installing Veeam ONE Web Services.

3. **Install and configure Veeam ONE Client**.

   Run the **Veeam ONE Client** wizard to enable user access to the Veeam ONE monitoring functionality. If necessary, you can install several instances of Veeam ONE Client on separate machines to provide access to Veeam ONE Client for multiple users. For details, see Installing Veeam ONE Client.

Installing Veeam ONE Server

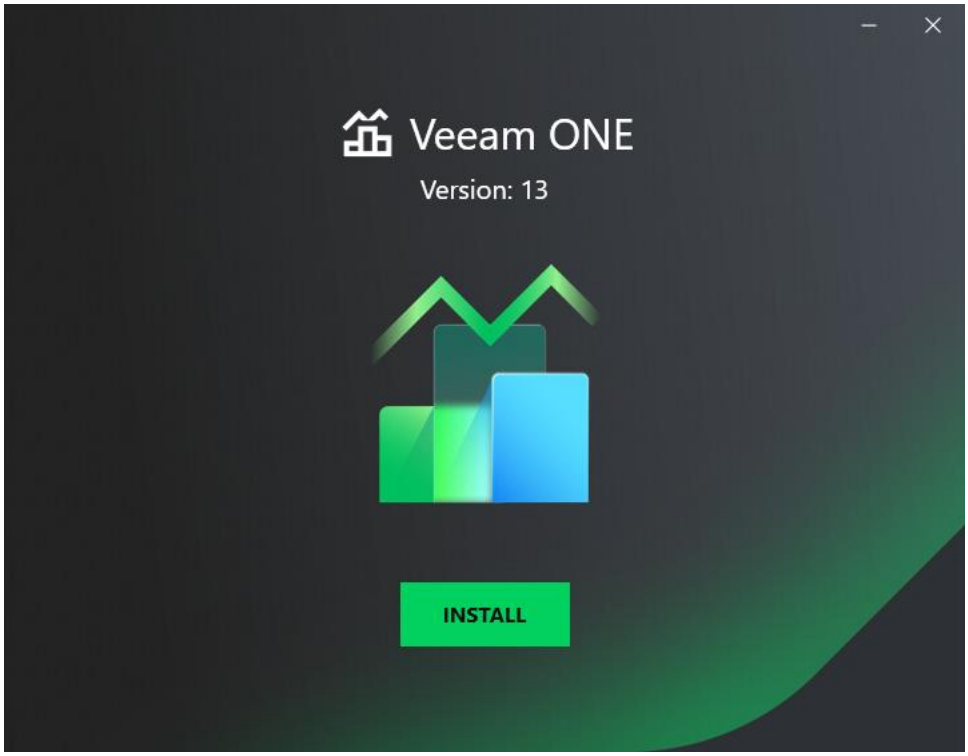
To install Veeam ONE Server, follow these steps:

1. Launch Splash Window.
2. Select Component.
3. Accept License Agreements.
4. Choose License Method.
5. Specify Service Account Credentials.
6. Perform System Configuration Check.
7. Review Installation Summary.
8. Select Architectural Components.
9. Choose Monitoring Database.
10. Choose Reporting Database.
11. Choose Data Location.
12. Choose Data Collection Mode.
13. Specify Connection Ports.
14. Review Installation Summary.
15. Add Veeam ONE Service Account to Veeam ONE Administrators Group.

Step 1. Launch Splash Window

After you mount or insert the disk with Veeam ONE installation image, **Autorun** will open a splash screen with installation options. On the splash window, click **Install** to launch the **Veeam ONE Setup** wizard.

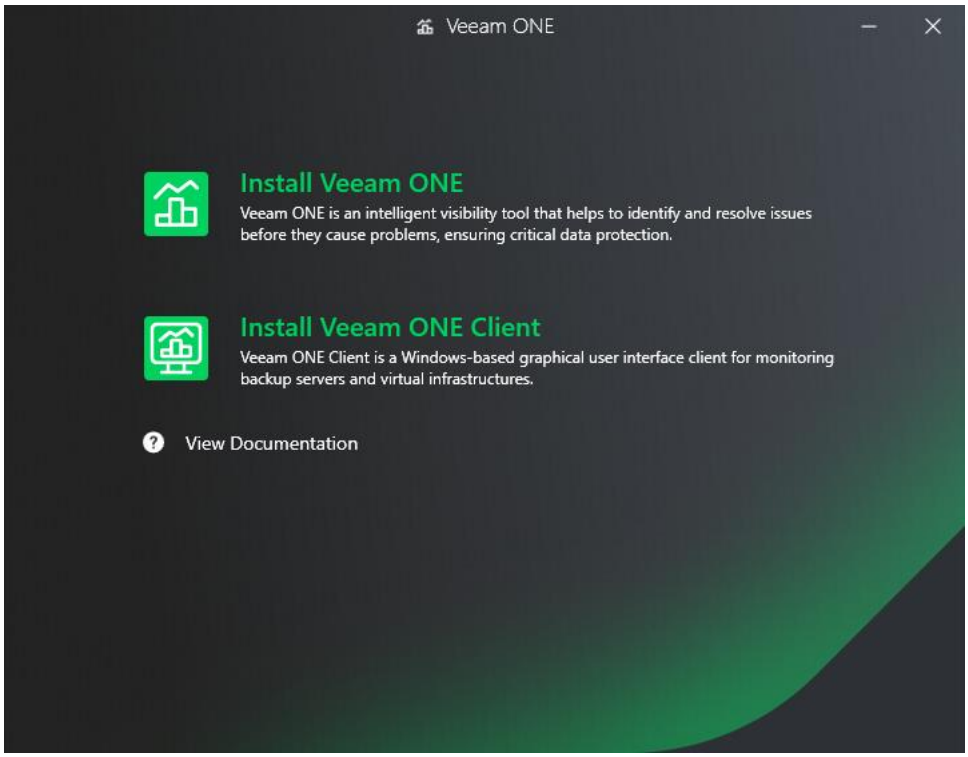
If **Autorun** is disabled, run the `Setup.exe` file from the installation image. Alternatively, you can right-click the new disk in **My Computer** and select **Execute Veeam ONE Autorun**.



Step 2. Select Component

At the **Select Veeam ONE Component** step of the wizard, select **Install Veeam ONE**.

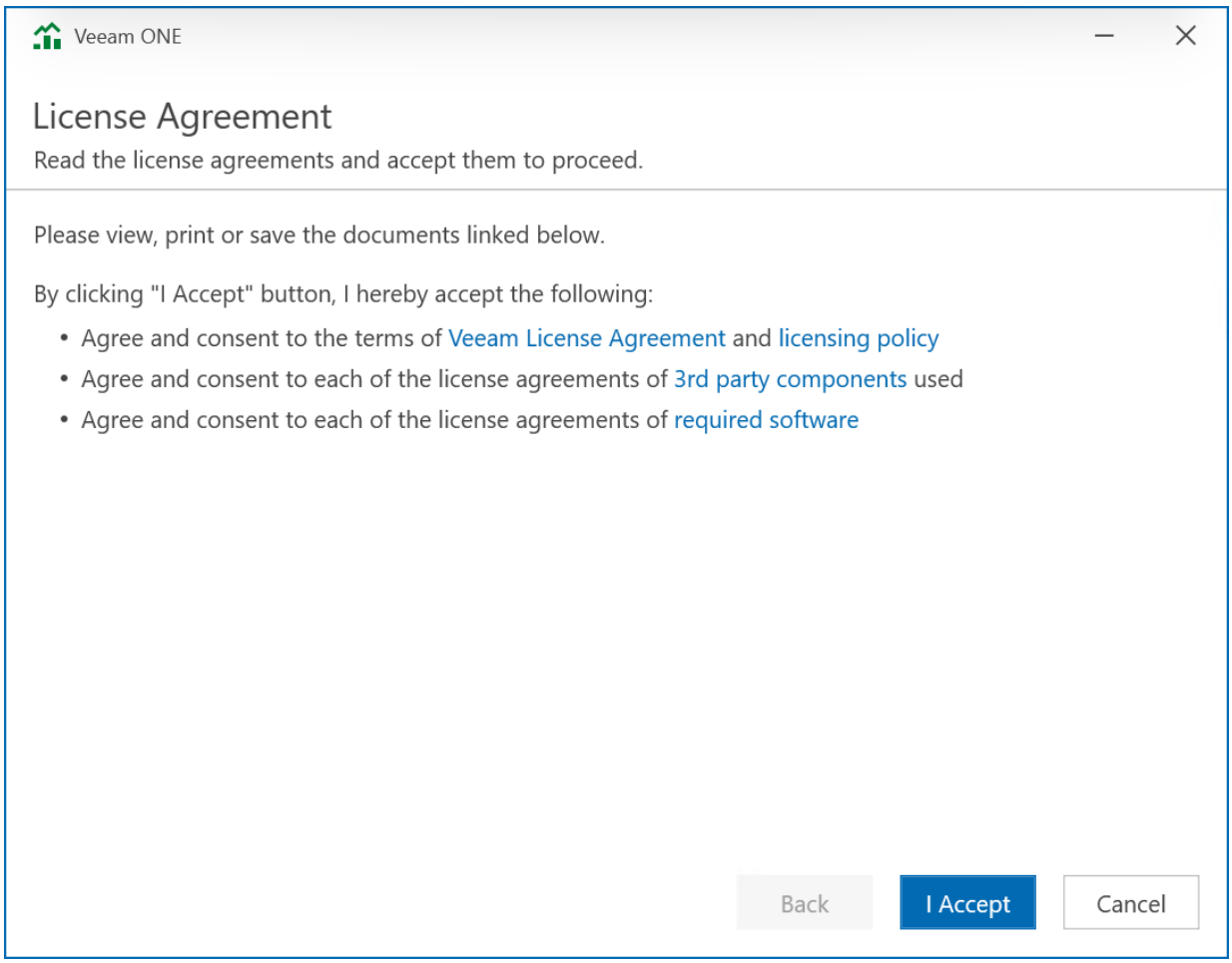
To open Veeam Help Center from the setup wizard, click **View Documentation**.



Step 3. Accept License Agreements

At the **License Agreement** step of the wizard, read and accept Veeam license agreement, licensing policy, 3rd party components and required software license agreements. You will not be able to continue installation until you accept license agreements.

To read the terms of the license agreements, click the individual links.

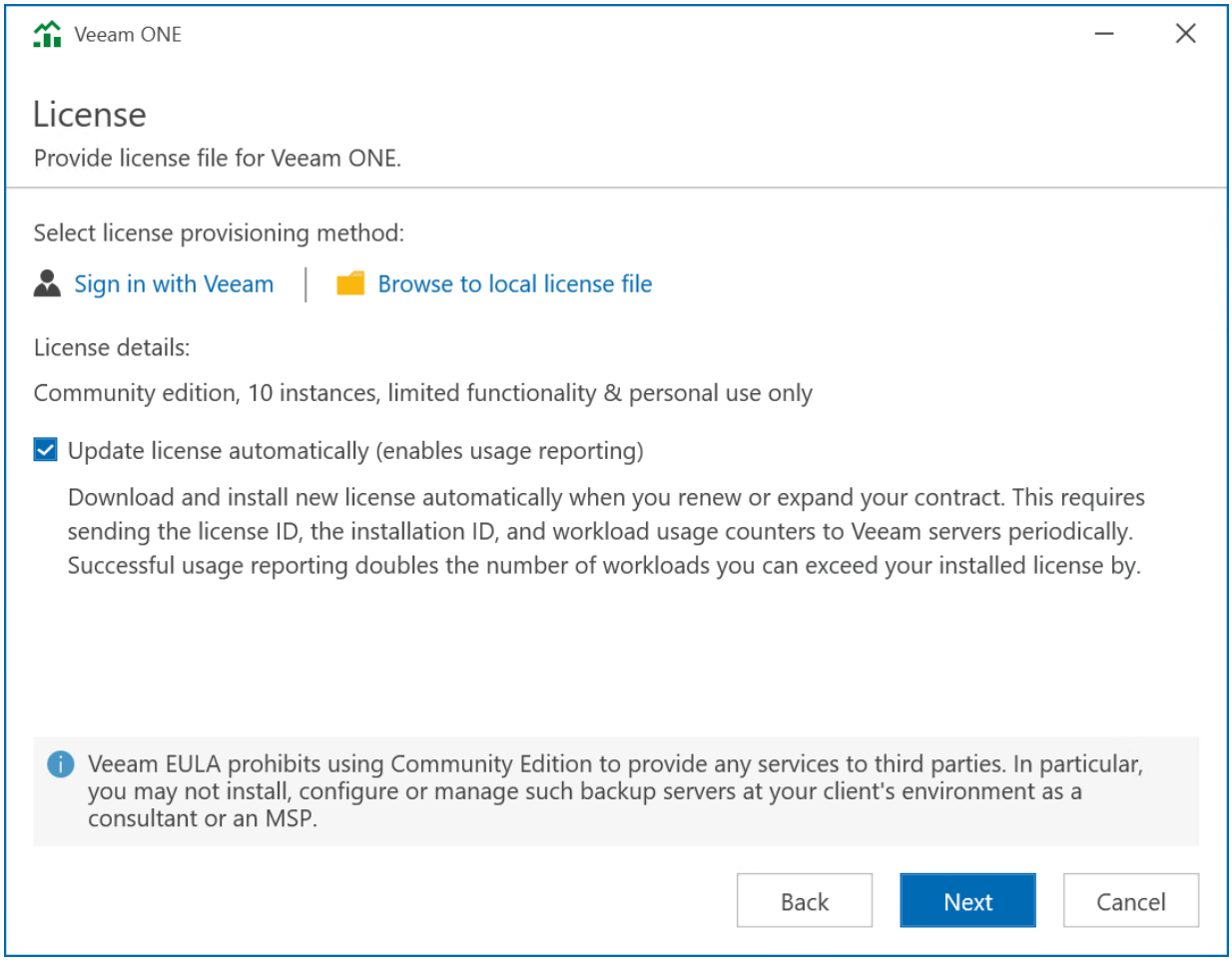


Step 4. Provide License

At the **License** step of the wizard, click one of the two options to provide a license:

- **Sign in with Veeam** – open the Veeam account Sign in screen to log in with your Veeam account credentials if you already have a registered license on your account.
- **Browse to local license file** – specify the local path to the license file.

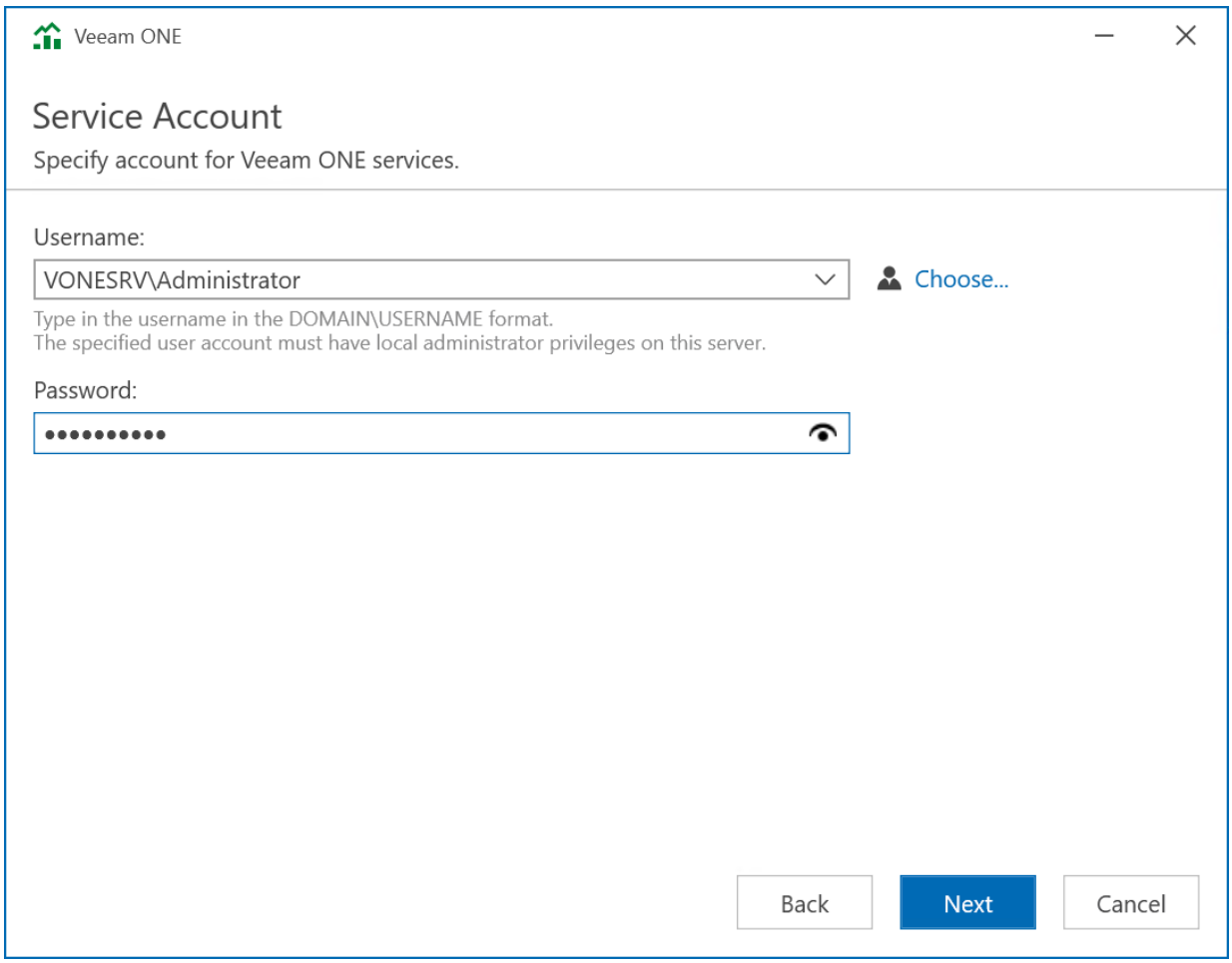
To install new licenses automatically when you renew or expand your contract, select the **Update license automatically** check box. If you enable the automatic license update, and therefore enable usage reporting, you will double the number of workloads by which you can exceed your installed license. Note that for *Evaluation* and *NFR* licenses automatic license update must be enabled.



Step 5. Specify Service Account Credentials

At the **Service Account** step of the wizard, specify credentials of the account under which the Veeam ONE services will run. The user name must be specified in the *DOMAIN|USERNAME* format. Alternatively click **Choose** to select an existing user account.

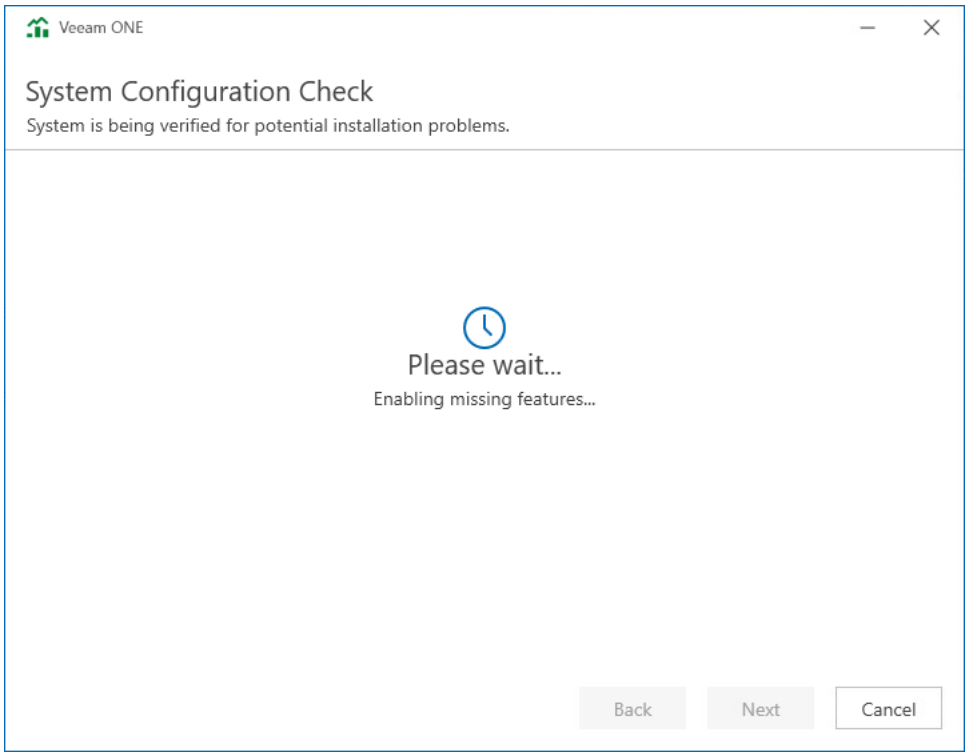
For details on required permissions for the service account, see Veeam ONE Service Account.



Step 6. Perform System Configuration Check

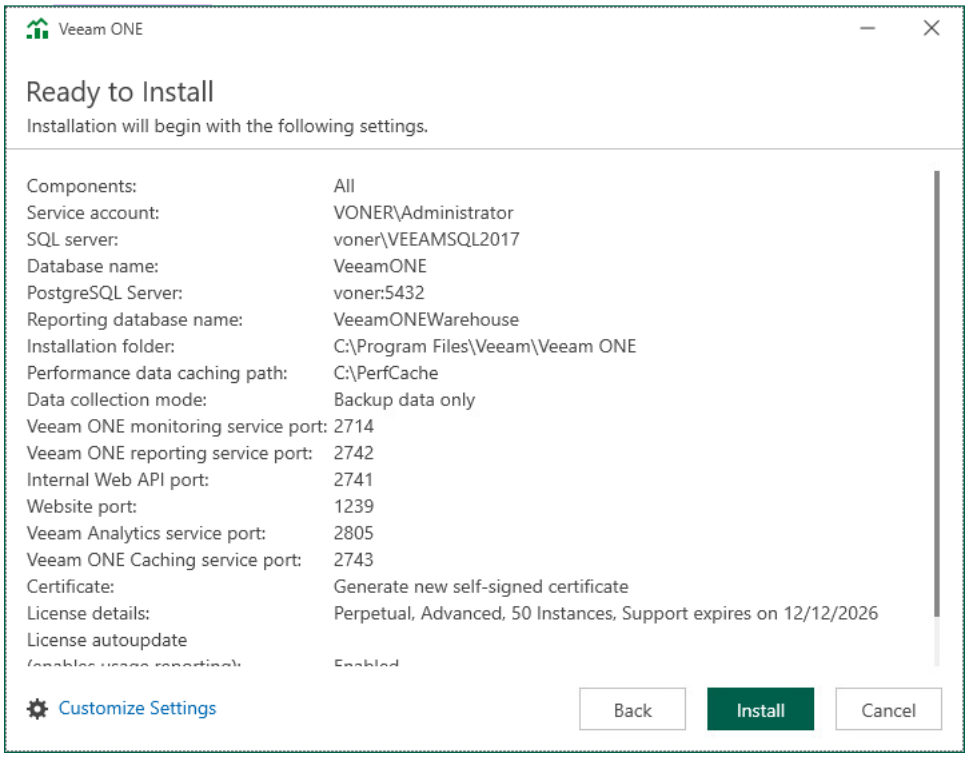
Before proceeding with the installation, the installer will perform system configuration check to determine if all prerequisite software is available on the machine. To learn what software is required for Veeam ONE, see System Requirements.

If some of the required software components are missing, the setup wizard will enable the missing software components and features automatically.



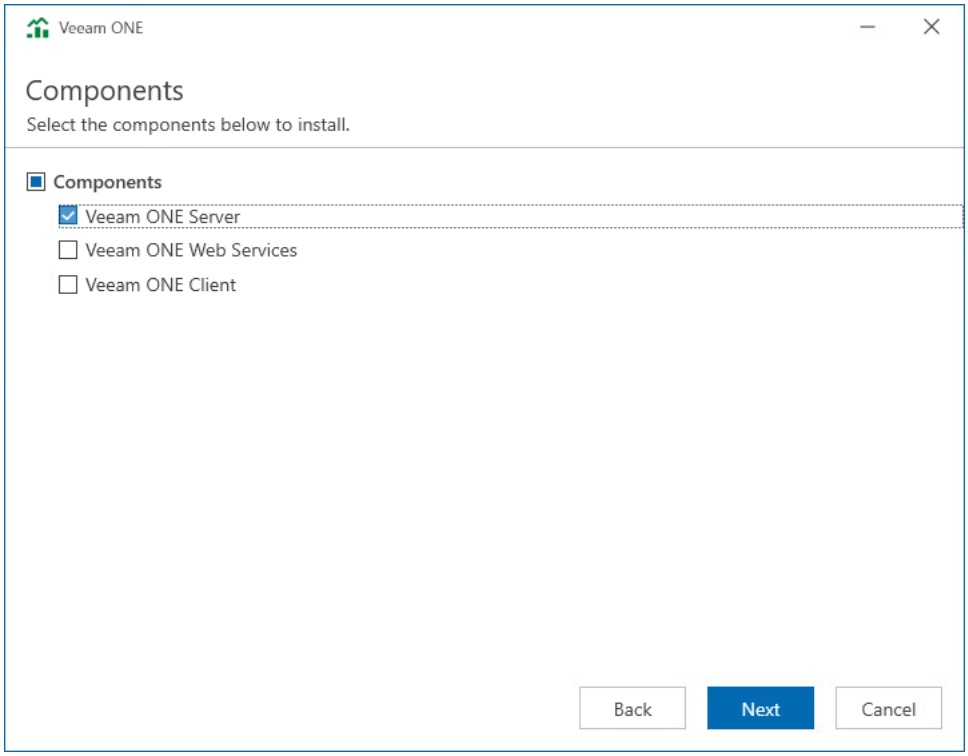
Step 7. Review Installation Summary

At the **Ready to Install** step of the wizard, review installation configuration and click **Customize Settings**.



Step 8. Select Architectural Components

At the **Components** step of the wizard, choose to install **Veeam ONE Server** only.



Step 9. Choose Monitoring Database

At the **SQL Server Instance** step of the wizard, choose a Microsoft SQL Server instance that will host the Veeam ONE database. If you are installing Veeam ONE Server and Veeam ONE Web Services on different machines, make sure that both components share a common database.

To install Veeam ONE Server, select Microsoft SQL Server as follows:

- If you do not have a Microsoft SQL Server instance that you can use for Veeam ONE, select the **Install new instance of SQL Server** option.

  If this option is selected, the setup will install Microsoft SQL Server 2017 Express locally, on the computer where you are installing Veeam ONE.

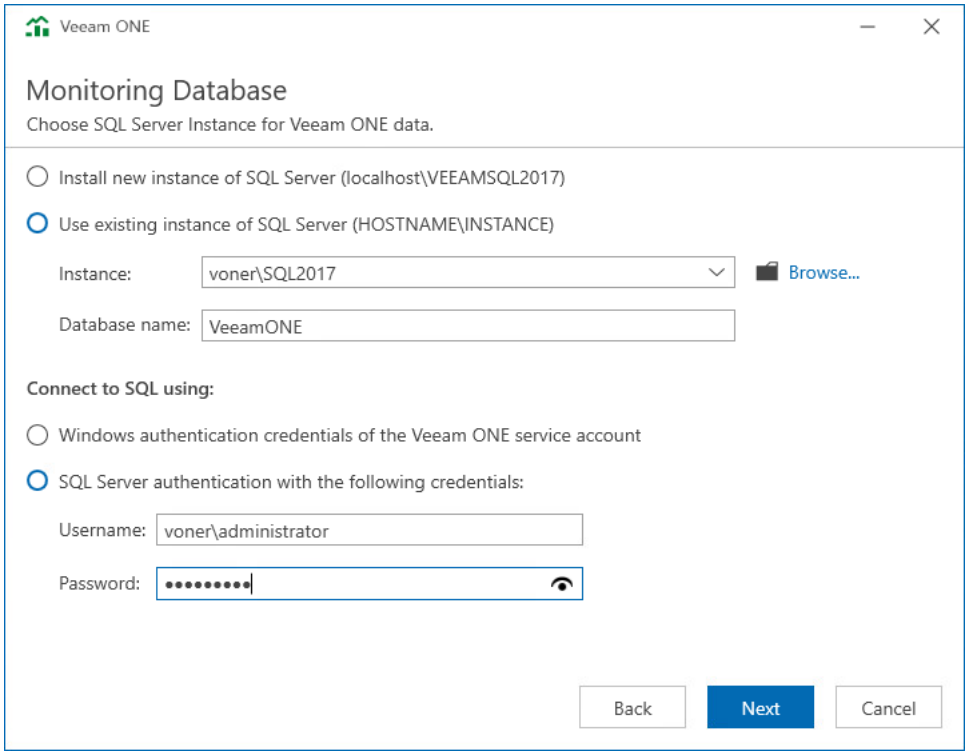
  > **NOTE:**
  > - If a Microsoft SQL Server instance that meets Veeam ONE system requirements is detected on the machine, you can only use the existing local Microsoft SQL Server instance or choose a one that runs remotely. The option to install a new Microsoft SQL instance will be unavailable in this case.
  > - If you choose to host Veeam ONE database on Microsoft SQL Server Express, consider is a 10 GB database size limitation for this edition. For details, see Editions and Supported Features for SQL Server.

- If you intend to use an existing local or remote Microsoft SQL Server instance, select the **Use existing instance of SQL Server** option and choose a local Microsoft SQL Server instance or browse to a Microsoft SQL Server instance running remotely. You can enter the address of the preferred Microsoft SQL Server manually or use the **Browse** button to choose among available remote instances.

  In the **Database name** field, specify the name of the database that will be created by Veeam ONE. Provide credentials for the account that will be used by Veeam ONE components to access the database. You can enter credentials explicitly or use Windows authentication credentials of the Veeam ONE service account to connect to the Microsoft SQL Server. For details on required permissions for the account, see Connection to Microsoft SQL Server.

- If you already have an existing Veeam ONE database that you want to use in your deployment, select the **Use existing instance of SQL Server** option and choose the Microsoft SQL Server instance that hosts the database. This can be a database that you have previously created with a SQL script. In the **Database name** field, specify the name of the database.

  Provide credentials for the account that will be used by Veeam ONE components to access the database. You can enter credentials explicitly or use Windows authentication credentials of the service account to connect to the Microsoft SQL Server. For details on required permissions for the account, see Connection to Microsoft SQL Server.



Step 10. Choose Reporting Database

At the **Reporting Database** step of the wizard, choose a PostgreSQL Server instance that will host the Veeam ONE reporting database.

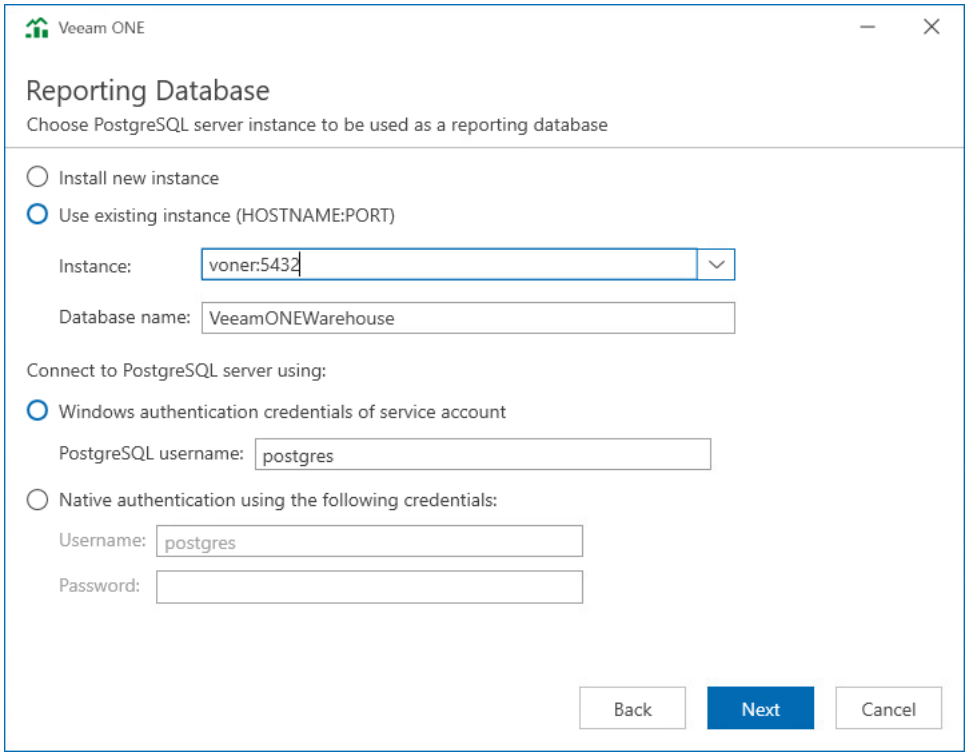
The reporting database is a dedicated database that stores PostgreSQL logs and metrics related to system activities, performance, and other relevant data for analysis and reporting purposes.

- If you do not have a PostgreSQL instance that you can use for Veeam ONE database, select the **Install new instance** option.

  If this option is selected, the setup will install PostgreSQL locally, on the computer where you are installing Veeam ONE.

- If you want to use an existing local or remote PostgreSQL instance, select the **Use existing instance** option and enter the instance and database name.

- In the **Connect to PostgreSQL server using** section, select an authentication mode to connect to the database server instance: Microsoft Windows authentication or native database server authentication. If you select the native authentication, enter credentials of the PostgreSQL database account.



Step 11. Choose Data Location

In the **Installation path**, choose the installation directory. In the typical installation mode, the setup installs all components to a single directory and creates a subdirectory for every Veeam ONE component.

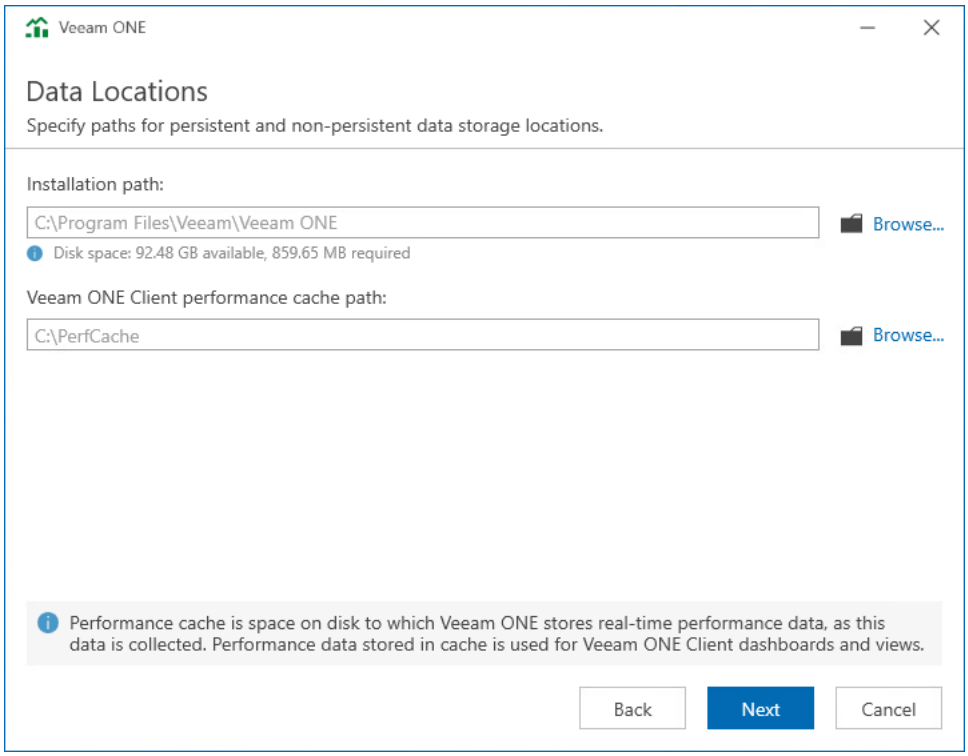
In the **Veeam ONE Client performance cache path**, choose a directory where the performance cache must be located.

Performance cache is space on disk to which Veeam ONE stores real-time performance data, as this data is collected. Performance data stored in cache is used for Veeam ONE Client dashboards and views. Disk-based performance cache allows significantly decrease RAM utilization on the machine that runs the Veeam ONE Server component.

By default, the performance cache is stored to the `C:\PerfCache` folder. To store the cache to a different folder, click **Browse** next to the **Path** field and specify a path to the new folder.

When choosing a location for performance cache, consider the following recommendations:

- Make sure that the disk where the performance cache is located can quickly complete read and write requests. Do not locate the cache remotely in networks with high latency values.
- For large monitoring environments, place the performance cache on an SSD local to the machine where the Veeam ONE Server component runs. For small and medium monitoring environments, a HDD is normally enough.
- Length of the performance cache folder path must not exceed the Windows Max Path Limitation value. For details, see Microsoft Learn.
- Make sure there is enough disk space for performance cache. The cache is cleared on an hourly basis, as new data is collected; however, in large monitoring environments it can take significant disk space. For example, in the custom deployment mode, during peak loads, the cache can take up to 6 GB disk space for each 1000 VMs.



The typical installation requires around 850 MB of free space on a disk (plus additional space if you choose to install Microsoft SQL Server instance on the same machine). Be aware that depending on the size of your virtual infrastructure and frequency of data collection, the database may grow large and require more space. Be sure to adjust to this condition by freeing up more disk space when needed.

Step 12. Choose Data Collection Mode

At the **Data Collection Mode** step of the wizard, choose the mode in which Veeam ONE will collect data from virtualization and Veeam Backup & Replication servers.

Data collection mode determines what metrics Veeam ONE will collect, and specifies the product configuration in a number of areas. Choosing an appropriate data collection mode allows you to optimize monitoring and reporting performance and improve user experience in Veeam ONE. To learn the difference between the data collection modes, see Data Collection Modes.

Veeam Backup Data Only

The **Veeam backup data only** mode is recommended for users who want to focus on Veeam Backup & Replication and Veeam Backup for Microsoft 365 monitoring and reporting, and do not need a deep visibility of the virtual infrastructure.

In this mode, Veeam ONE collects all inventory, configuration and performance metrics from Veeam Backup & Replication and Veeam Backup for Microsoft 365 servers. It also collects inventory and configuration metrics from virtualization servers, but skips virtual infrastructure performance metrics. As a result, Veeam ONE dashboards, reports and alarms display backup-related data only. For VMware vSphere and Microsoft Hyper-V objects, performance data is not available.

This mode results in the least possible size of the Veeam ONE database and the lowest load on the Veeam ONE server.

Veeam Backup Data and Virtual Infrastructure Performance Monitoring

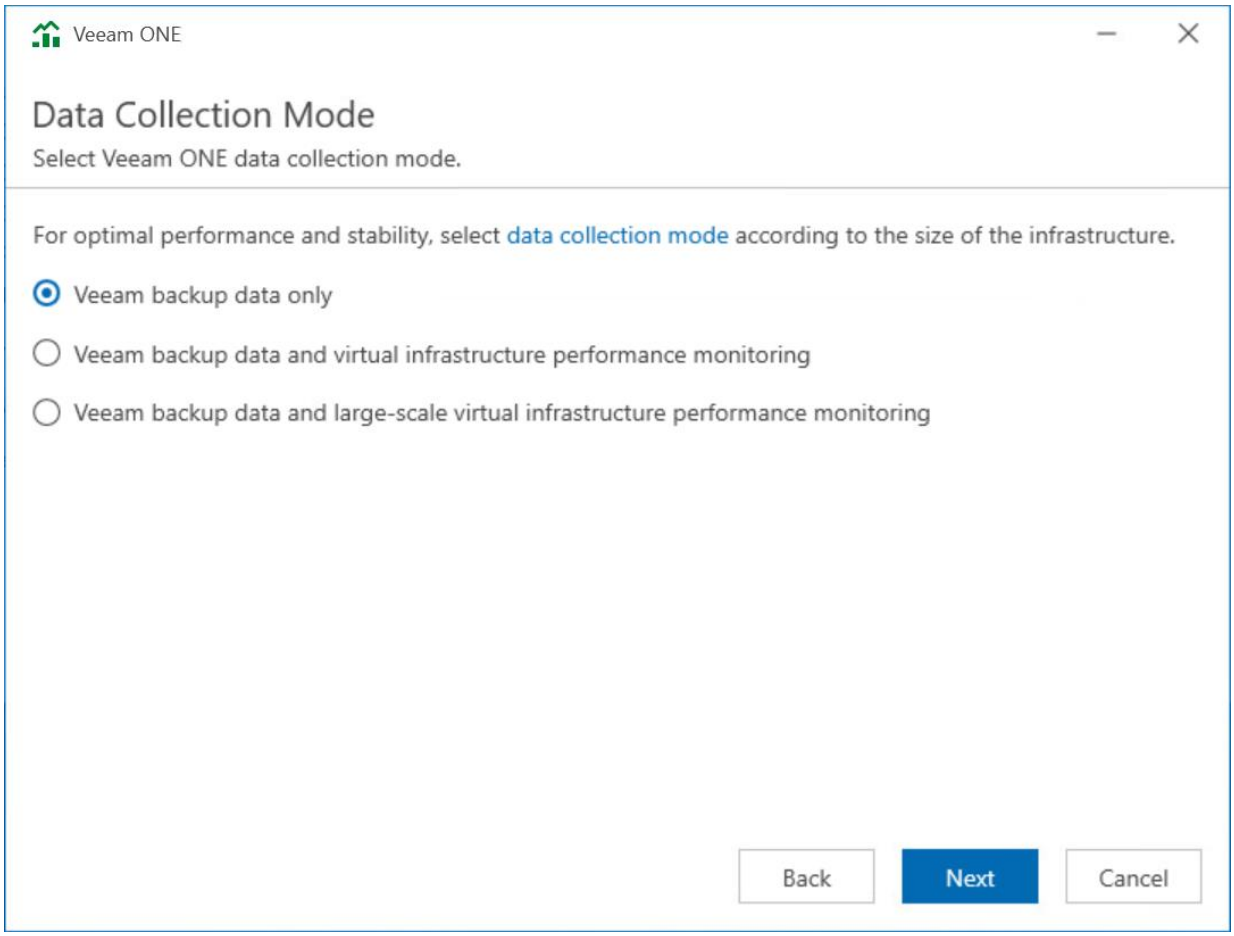
The **Veeam backup data and virtual infrastructure performance monitoring** modes are recommended for users who want to monitor and report on the virtual environment, Veeam Backup & Replication and Veeam Backup for Microsoft 365 infrastructures.

- **Veeam backup data and virtual infrastructure performance monitoring** mode is recommended for small to medium environments up to 100 hosts and 1500 VMs. In this mode, Veeam ONE collects all inventory, configuration and performance metrics, and makes collected data available in dashboards, reports and alarms.

  This mode provides the greatest data granularity level, but results in a greater load on the Veeam ONE server and a larger size of Veeam ONE database.

- **Veeam backup data and large-scale virtual infrastructure performance monitoring** mode is recommended for large environments with more than 100 hosts and 1500 VMs. In this mode, Veeam ONE collects all metrics required for alarms and reports.

  This mode results in a lower load on the Veeam ONE server and a smaller size of the Veeam ONE database.



Step 13. Specify Connection Ports

At the **Port Configuration** step of the wizard, specify connection settings for Veeam ONE Monitoring Service, Veeam ONE Reporting Service, internal Web API and Veeam Analytics service:

- In the **Veeam ONE monitoring service port** field, type a number of the port that will be used to interact with Veeam ONE Monitoring service.

  The default port number is `2714`.

- In the **Veeam ONE reporting service port** field, type a number of the port that will be used to interact with Veeam ONE Reporting service.

  The default port number is `2742`.

- In the **Internal Web API port** field, type a number of the port that will be used by Veeam ONE Monitoring service and Web Services component to interact with Veeam ONE Reporting service.

  The default port number is `2741`.

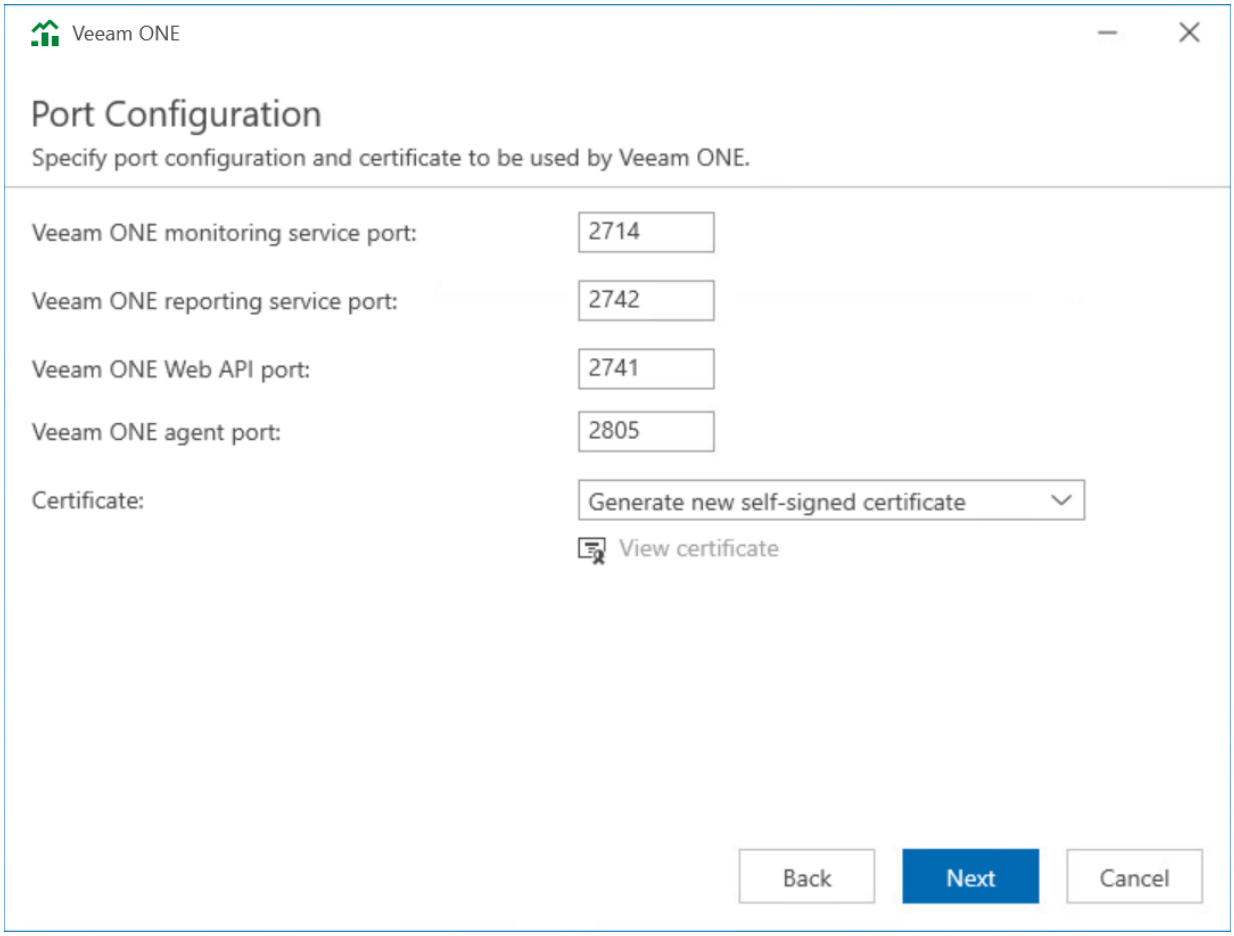
- In the **Veeam ONE agent port** field, type a number of the port that Veeam ONE Agent will use to collect data from connected Veeam Backup & Replication servers.

  The default port number is `2805`.

- In the **Certificate** list, choose a certificate that will be used to secure traffic between the web browser, Veeam ONE Web Services and Veeam ONE Reporting service.

  You can choose an existing certificate installed on the machine. If the setup wizard does not find an appropriate certificate to be used, it generates a self-signed certificate.

You can change the certificate later in Veeam ONE Settings utility. For details, see Veeam ONE Server Settings.

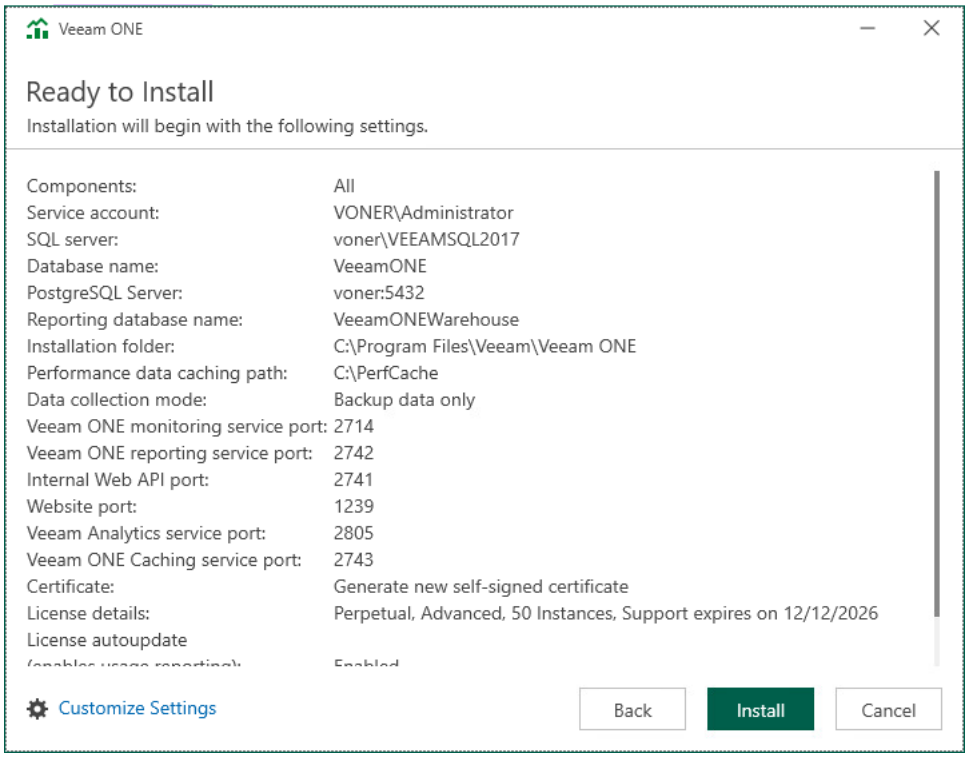


Step 14. Review Installation Summary

At the **Ready to Install** step of the wizard, review installation configuration to ensure that you have provided correct settings.

Select the **Check for product updates automatically** check box if you want Veeam ONE to automatically check and download available updates.

Click **Install** to begin the installation.



When the installation completes, click **Finish** to close the wizard.

Step 15. Add Veeam ONE Service Account to Veeam ONE Administrators Group

When Veeam ONE installation completes, the installer will prompt you to perform the logoff and logon procedure to create new user groups that will be used to accommodate user accounts for accessing Veeam ONE locally and remotely.

Check that the Veeam ONE service account is included in the *Veeam ONE Administrators* user group on the machines where the Veeam ONE Server is installed. If this account is not a member of the *Veeam ONE Administrators* user group, add it to the group manually.

For details on Veeam ONE user groups, see Security Groups.

Installing Veeam ONE Web Services

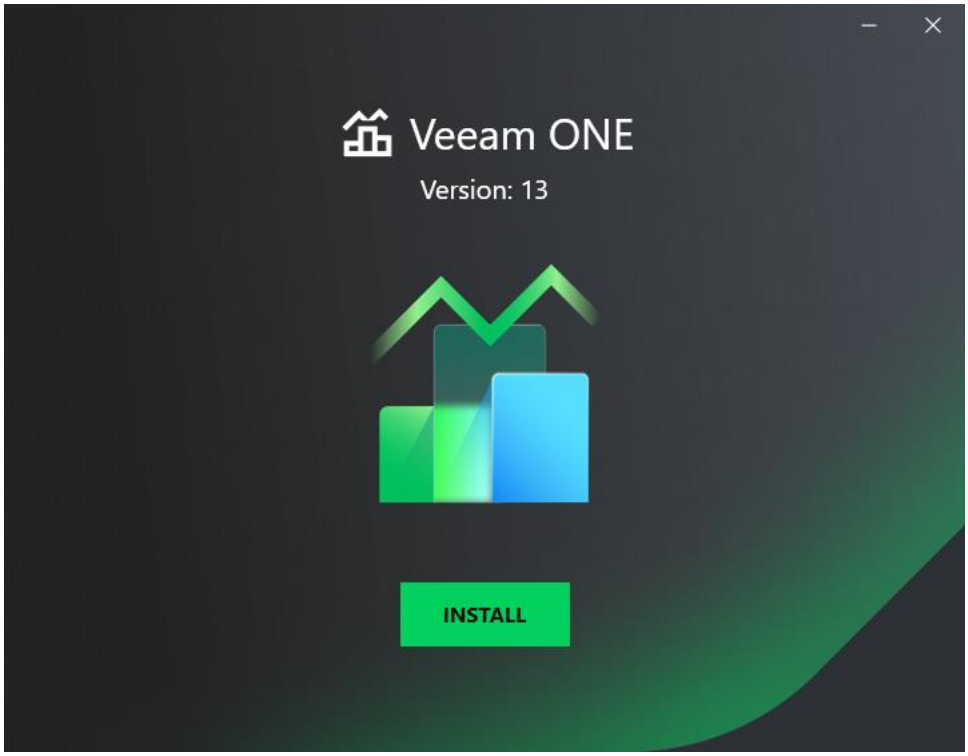
To install Veeam ONE Web Services, follow these steps:

1. Launch the splash window.
2. Select Component.
3. Accept License Agreements.
4. Provide License.
5. Specify Service Account.
6. Perform System Configuration Check.
7. Review Installation Summary.
8. Select Architectural Components.
9. Choose Data Location.
10. Specify Connection Ports.
11. Specify Veeam ONE Server Connection Details.
12. Review Installation Summary.

Step 1. Launch Splash Window

After you mount or insert the disk with Veeam ONE installation image, **Autorun** will open a splash screen with installation options. On the splash window, click **Install** to launch the **Veeam ONE Setup** wizard.

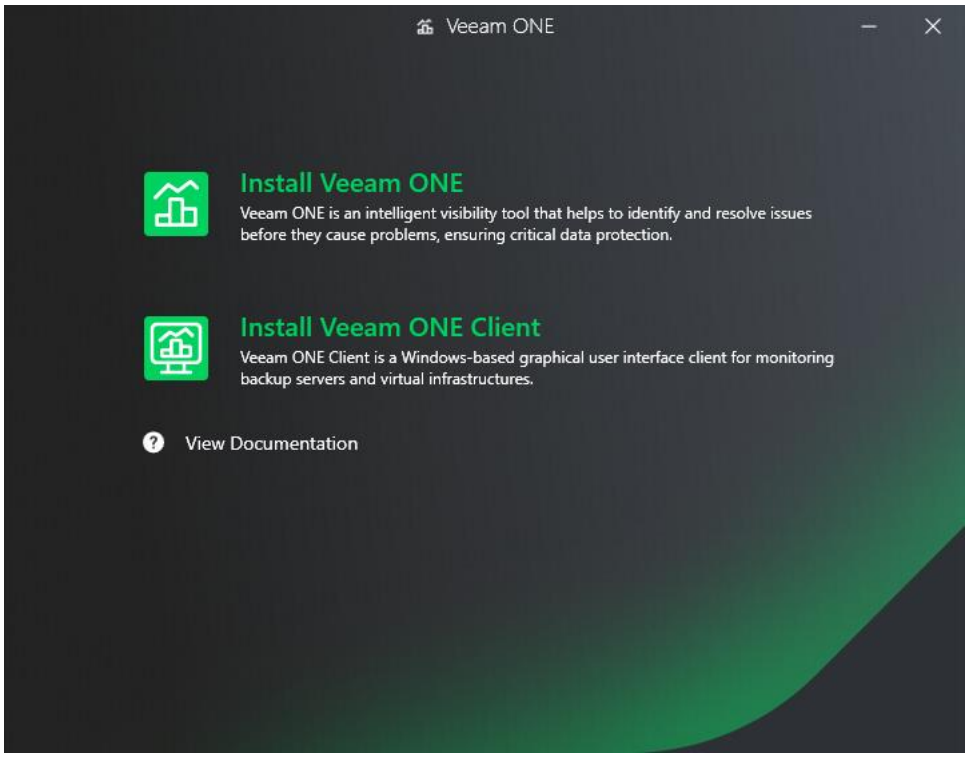
If **Autorun** is disabled, run the `Setup.exe` file from the installation image. Alternatively, you can right-click the new disk in **My Computer** and select **Execute Veeam ONE Autorun**.



Step 2. Select Component

At the **Select Veeam ONE Component** step of the wizard, select **Install Veeam ONE**.

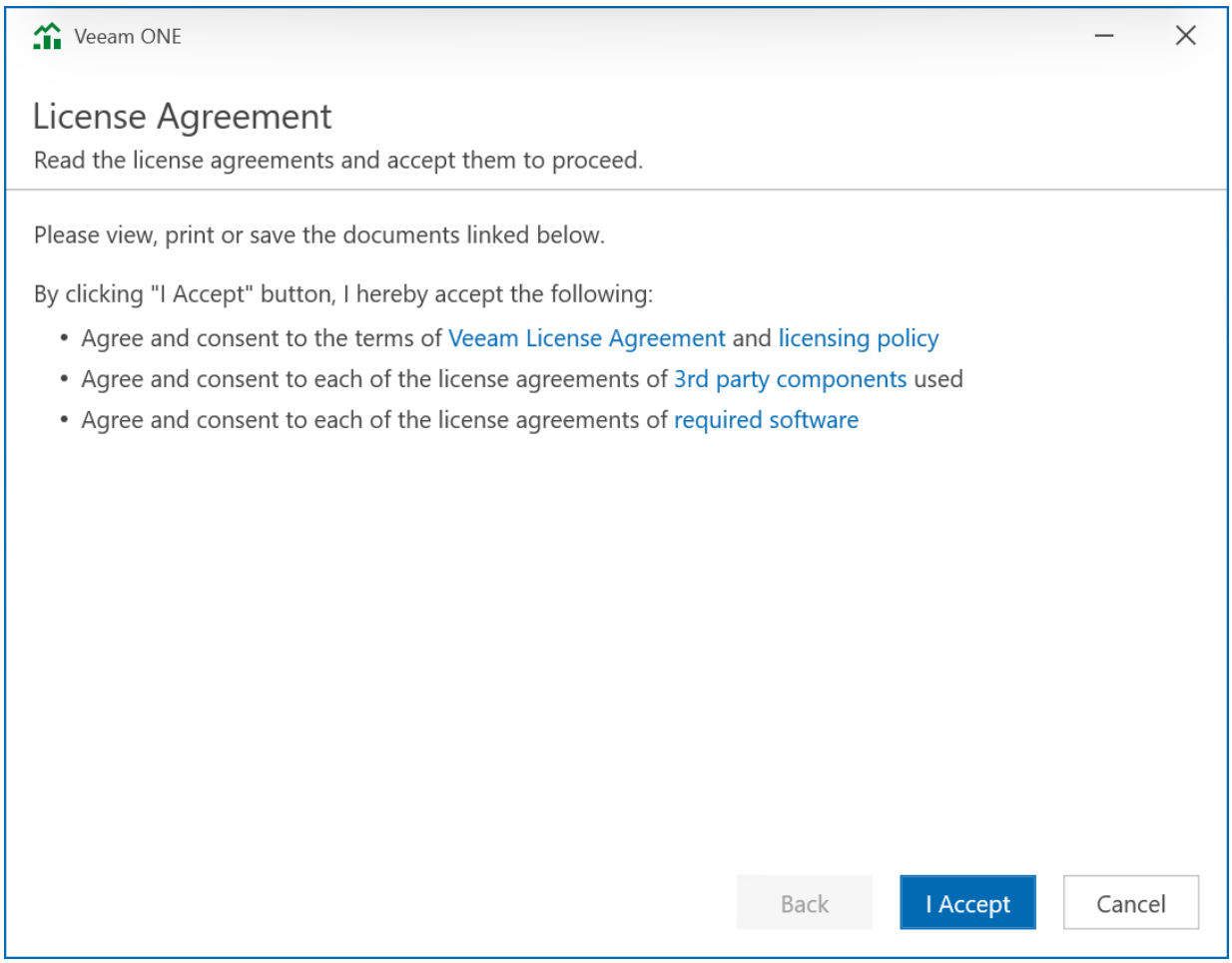
To open Veeam Help Center from the setup wizard, click **View Documentation**.



Step 3. Accept License Agreements

At the **License Agreement** step of the wizard, read and accept Veeam license agreement, licensing policy, 3rd party components and required software license agreements. You will not be able to continue installation until you accept license agreements.

To read the terms of the license agreements, click the individual links.

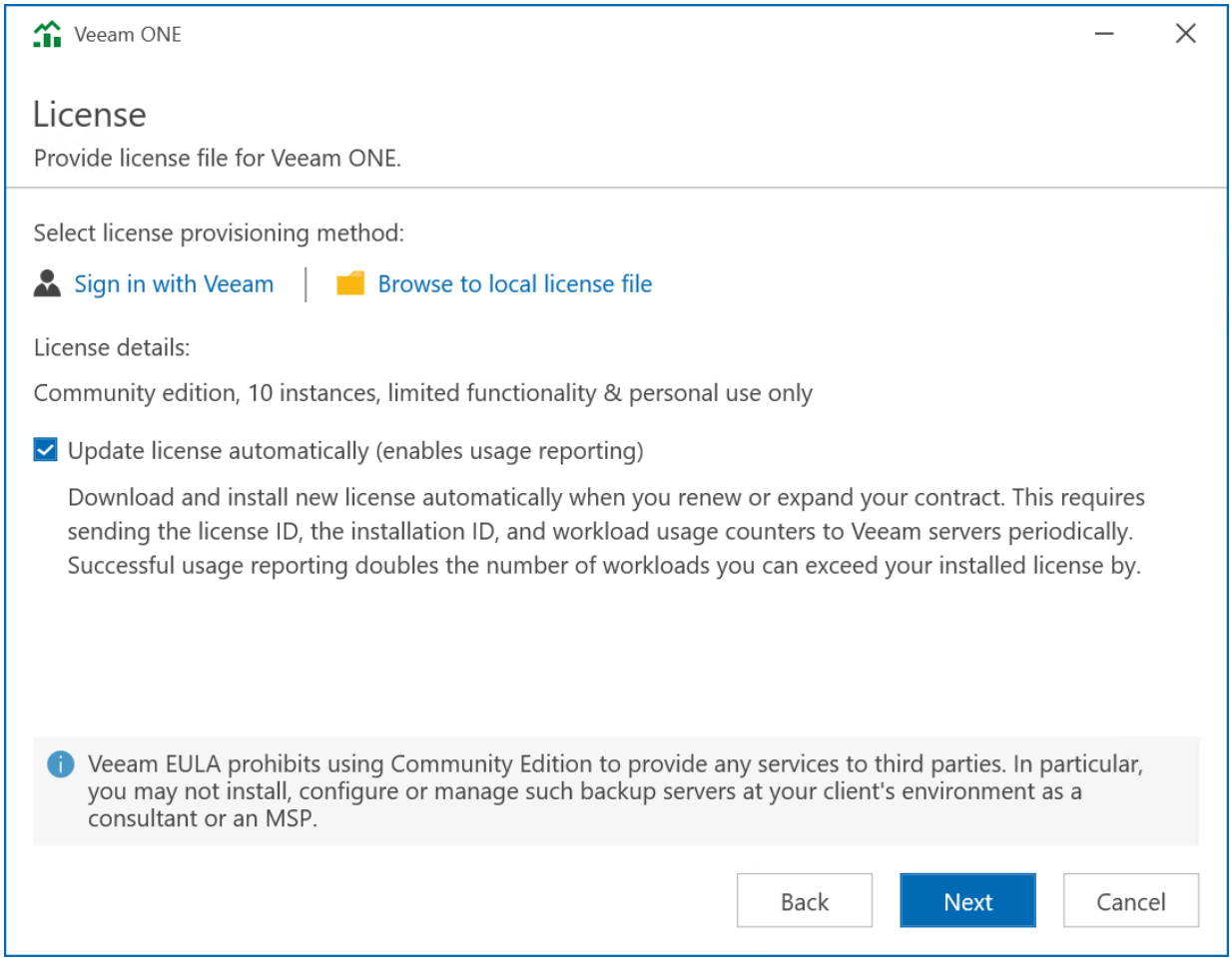


Step 4. Provide License

At the **License** step of the wizard, click one of the two options to provide a license:

- **Sign in with Veeam** – open the Veeam account Sign in screen to log in with your Veeam account credentials if you already have a registered license on your account.
- **Browse to local license file** – specify the local path to the license file.

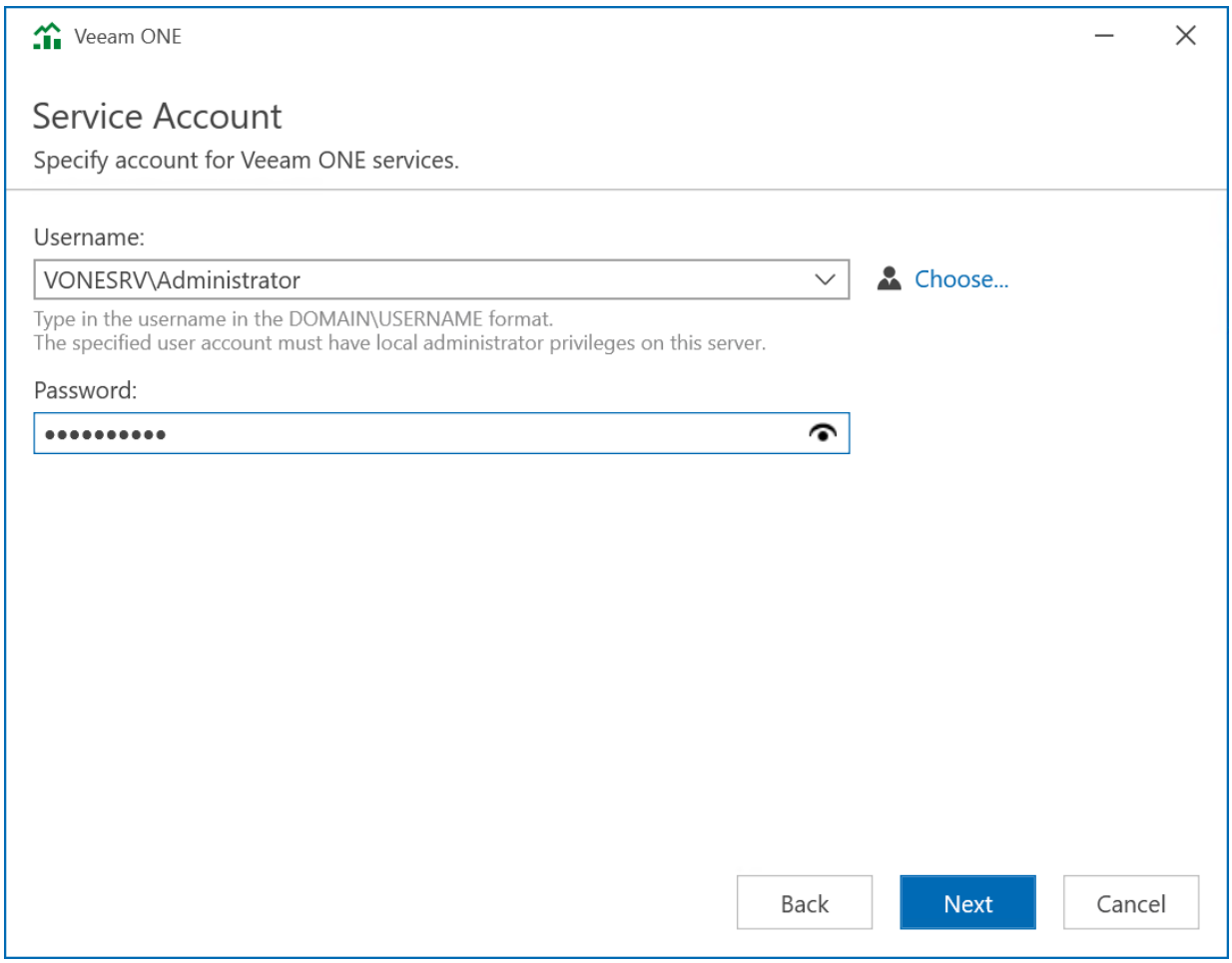
To install new licenses automatically when you renew or expand your contract, select the **Update license automatically** check box. If you enable the automatic license update, and therefore enable usage reporting, you will double the number of workloads by which you can exceed your installed license. Note that for *Evaluation* and *NFR* licenses automatic license update must be enabled.



Step 5. Specify Service Account

At the **Service Account** step of the wizard, specify credentials of the account under which the Veeam ONE services will run. The user name must be specified in the *DOMAIN|USERNAME* format. Alternatively click **Choose** to select an existing user account.

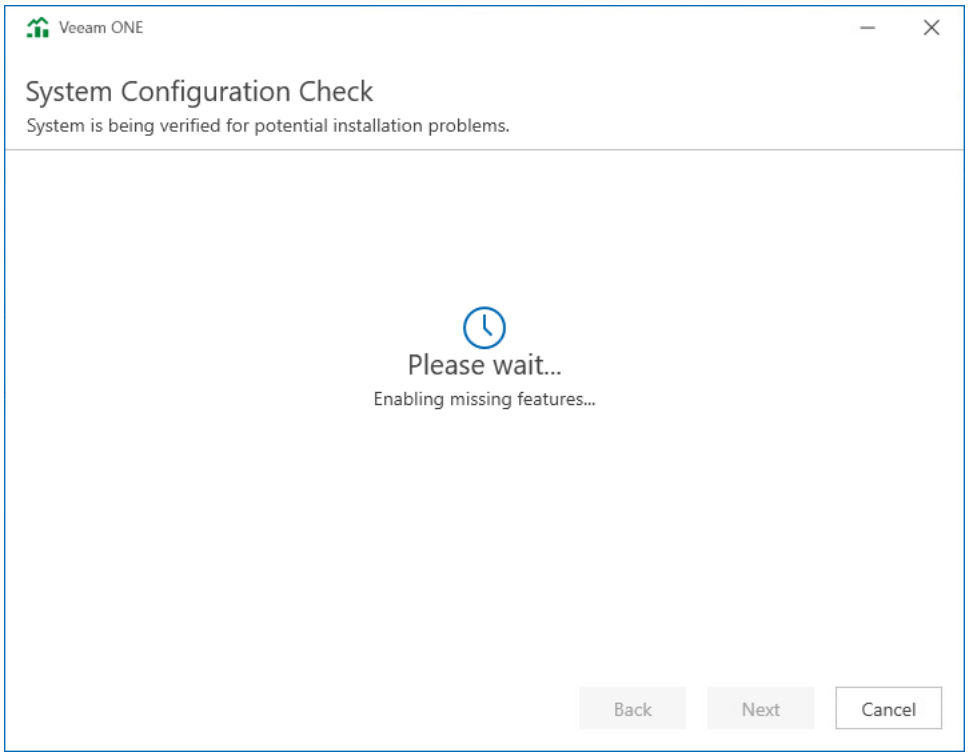
For details on required permissions for the service account, see Veeam ONE Service Account.



Step 6. Perform System Configuration Check

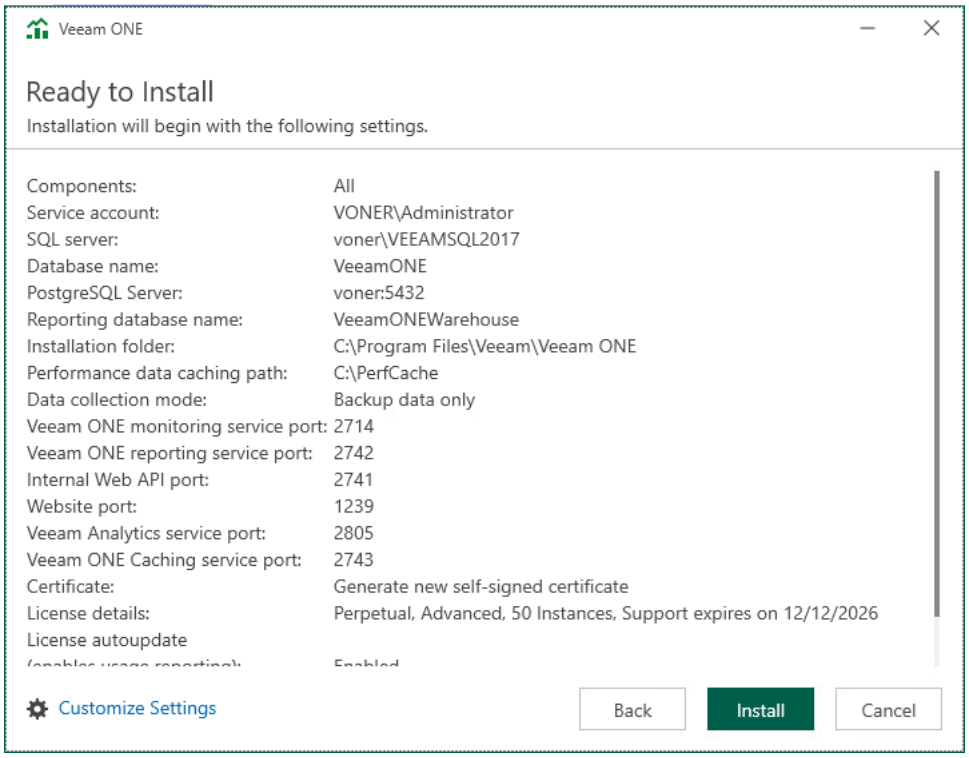
Before proceeding with the installation, the installer will perform system configuration check to determine if all prerequisite software is available on the machine. To learn what software is required for Veeam ONE, see System Requirements.

If some of the required software components are missing, the setup wizard will enable the missing software components and features automatically.



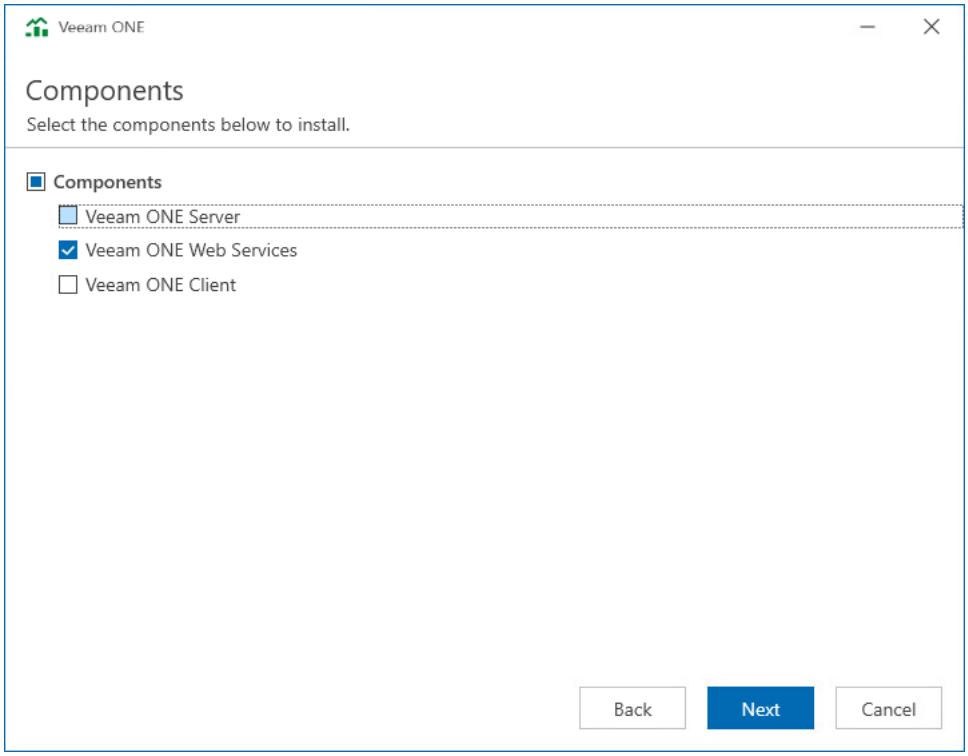
Step 7. Review Installation Summary

At the **Ready to Install** step of the wizard, review installation configuration and click **Customize Settings**.



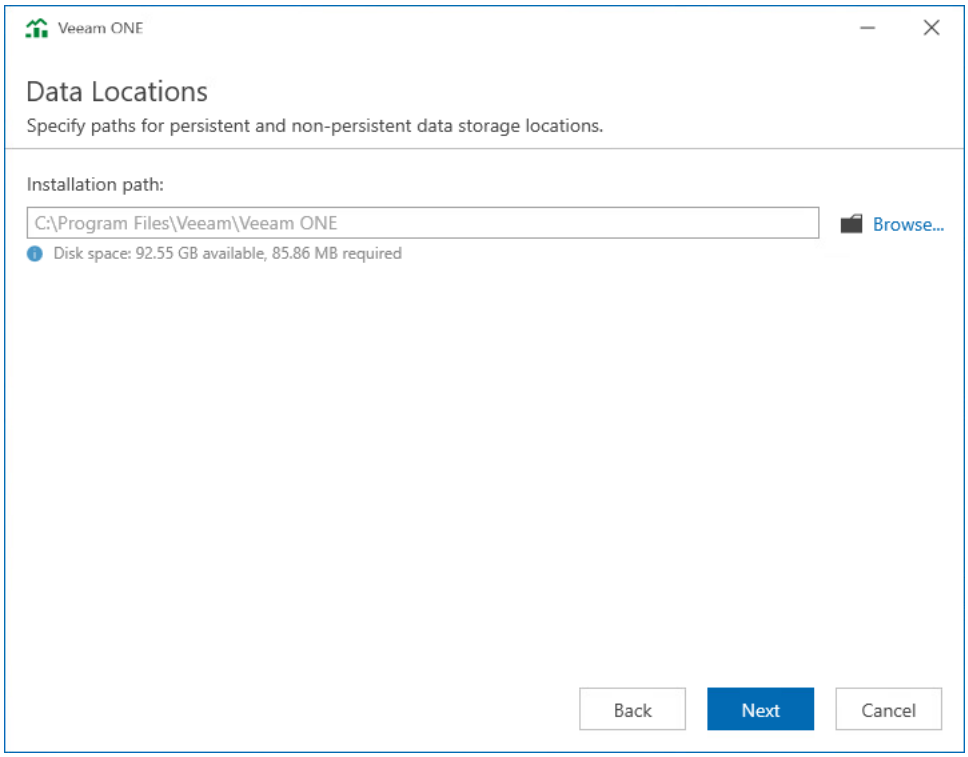
Step 8. Select Architectural Components

At the **Components** step of the wizard, choose to install **Veeam ONE Web Services** only.



Step 9. Choose Data Location

To change the installation directory, click **Browse** and select the location where you want to install Veeam ONE Web Services.



Step 10. Specify Connection Ports

At the **Port Configuration** step of the wizard, specify connection settings for Veeam ONE Web Client:

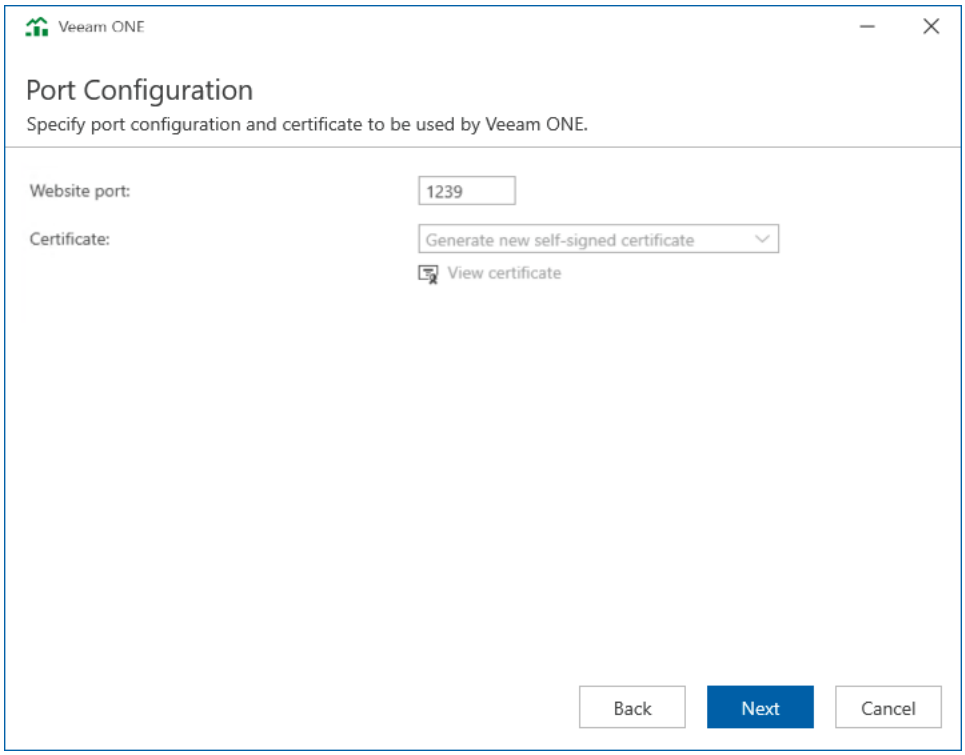
- In the **Website port** field, type a number of the port that will be used to access the Veeam ONE Web Client through a web browser.

  The default port number is `1239`.

- In the **Certificate** list, choose a certificate that will be used to secure traffic between the Veeam ONE Web Client and a web browser.

  You can choose an existing certificate installed on the machine or select the setup wizard to generate a self-signed certificate.

  > **NOTE:**
  > - If you generate or choose a self-signed certificate, you must configure a trusted connection between the Veeam ONE Web Client and a web browser later. For details, see Accessing Veeam ONE Components.
  > - You can change the selected certificate after installation. For details, see Change Default Certificate.



Step 11. Specify Veeam ONE Server Connection Details

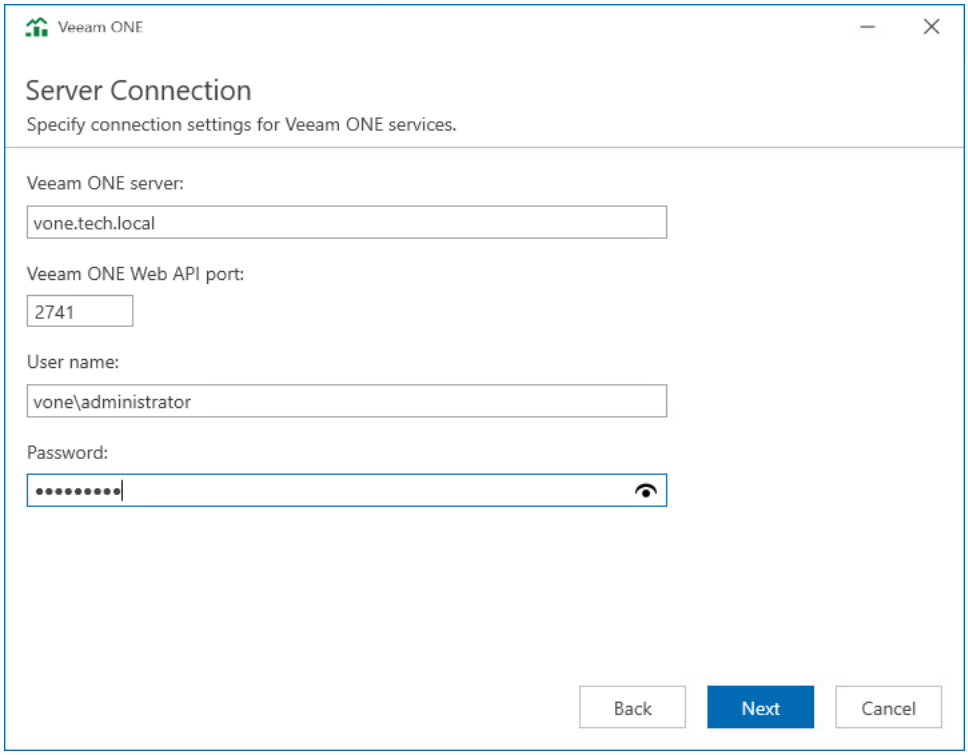
At the **Server Connection** step of the wizard, specify settings that the Web Services component must use to connect to the Server component:

- In the **Veeam ONE server** field, specify a FQDN of a machine on which you have installed the Veeam ONE Server component.
- In the **Veeam ONE Web API port** field, specify the number of a port that the Web Services component will use to communicate with the Veeam ONE Web API component.

  The default port number is `2741`.
- In the **Username** and **Password** fields, specify credentials of a user under which Veeam ONE Web Services will connect to Veeam ONE Server and configure it during installation.

  The user must be a member of *Veeam ONE Administrators* security group on the machine where Veeam ONE Server is installed.

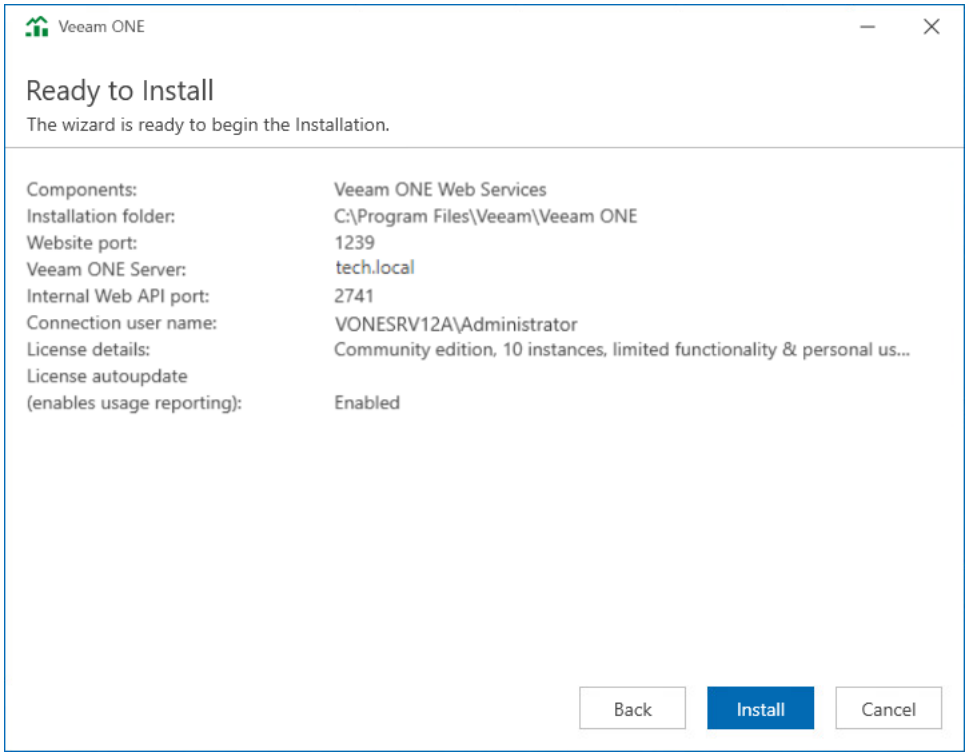
  The user name must be specified in the *DOMAIN|USERNAME* format.



Step 12. Review Installation Summary

At the **Ready to Install** step of the wizard, review installation configuration to ensure that you have provided correct settings.

Click **Install** to begin the installation.



When the installation completes, click **Finish** to close the wizard.

Installing Veeam ONE Client

Veeam ONE Client is the client part that allows users to access Veeam ONE monitoring functionality and work with alarms, dashboards and performance charts.

- In the course of all-in-one installation, Veeam ONE Client is installed with other Veeam ONE components. If you want to provide remote access to Veeam ONE monitoring functionality, you can install additional instances of Veeam ONE Client on user workstations.
- In the course of custom installation, Veeam ONE Client is not installed. To be able to access Veeam ONE monitoring functionality, you must install one or more instances of Veeam ONE Client.

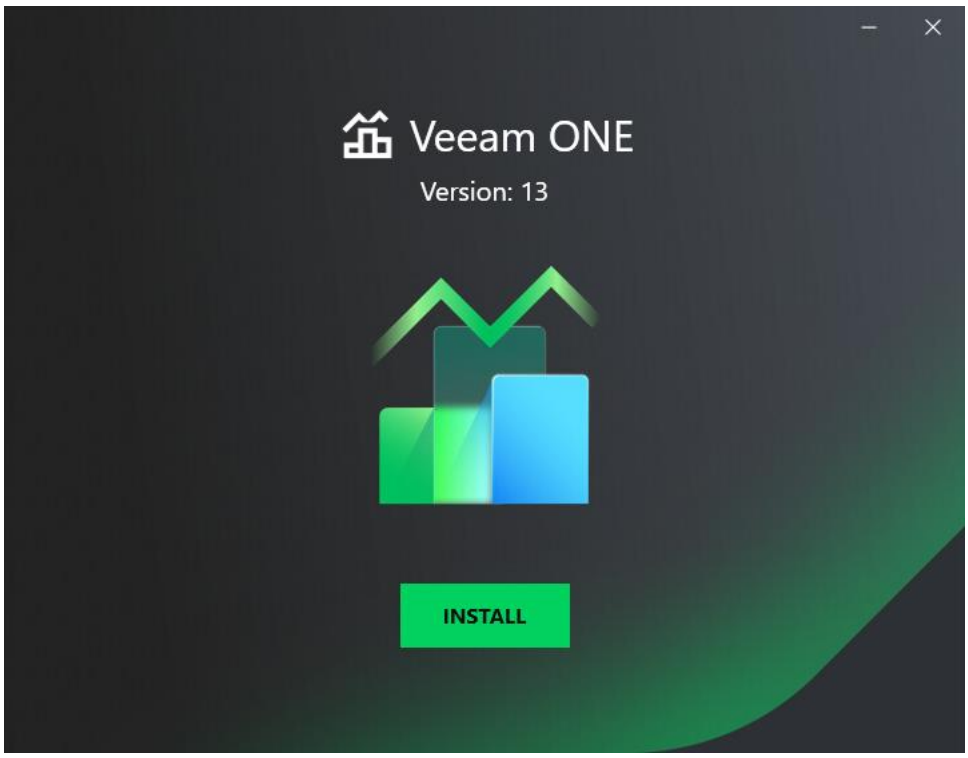
> **NOTE:**
>
> Mind the following:
>
> - Before installing Veeam ONE Client, make sure that you have already installed the Veeam ONE Server component.
> - You cannot install Veeam ONE Client using GPO or System Center Configuration Manager (SCCM).

To install Veeam ONE Client, follow these steps.

Step 1. Launch Splash Window

After you mount or insert the disk with Veeam ONE installation image, **Autorun** will open a splash screen with installation options. On the splash window, click **Install** to launch the **Veeam ONE Setup** wizard.

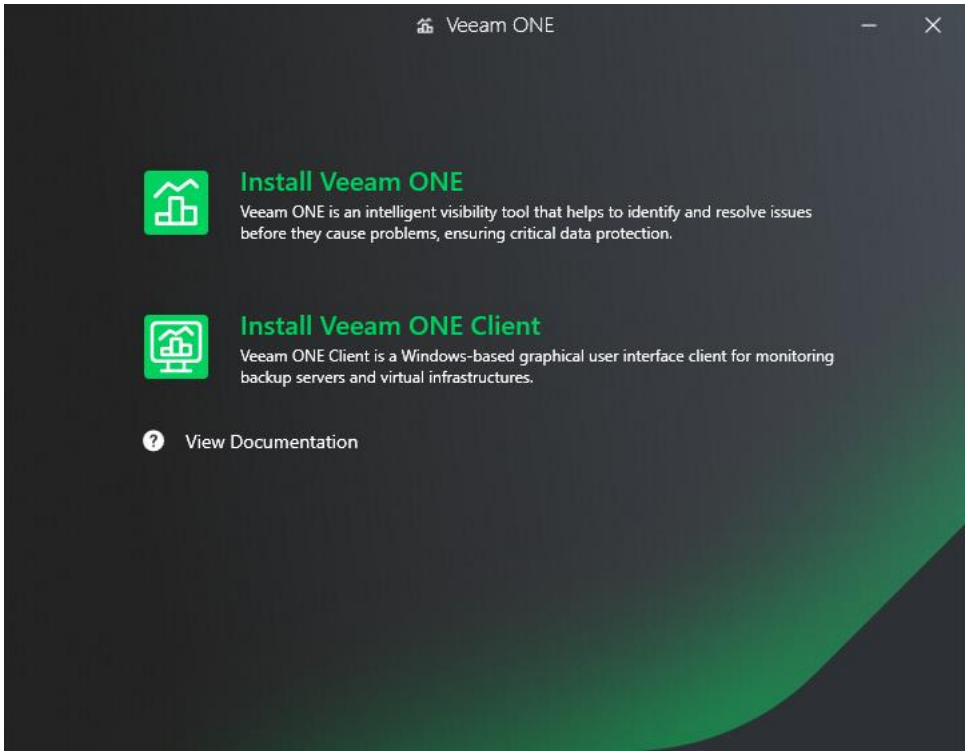
If **Autorun** is disabled, run the `Setup.exe` file from the installation image. Alternatively, you can right-click the new disk in **My Computer** and select **Execute Veeam ONE Autorun**.



Step 2. Select Component

At the select Veeam ONE component step of the wizard, select **Install Veeam ONE Client**.

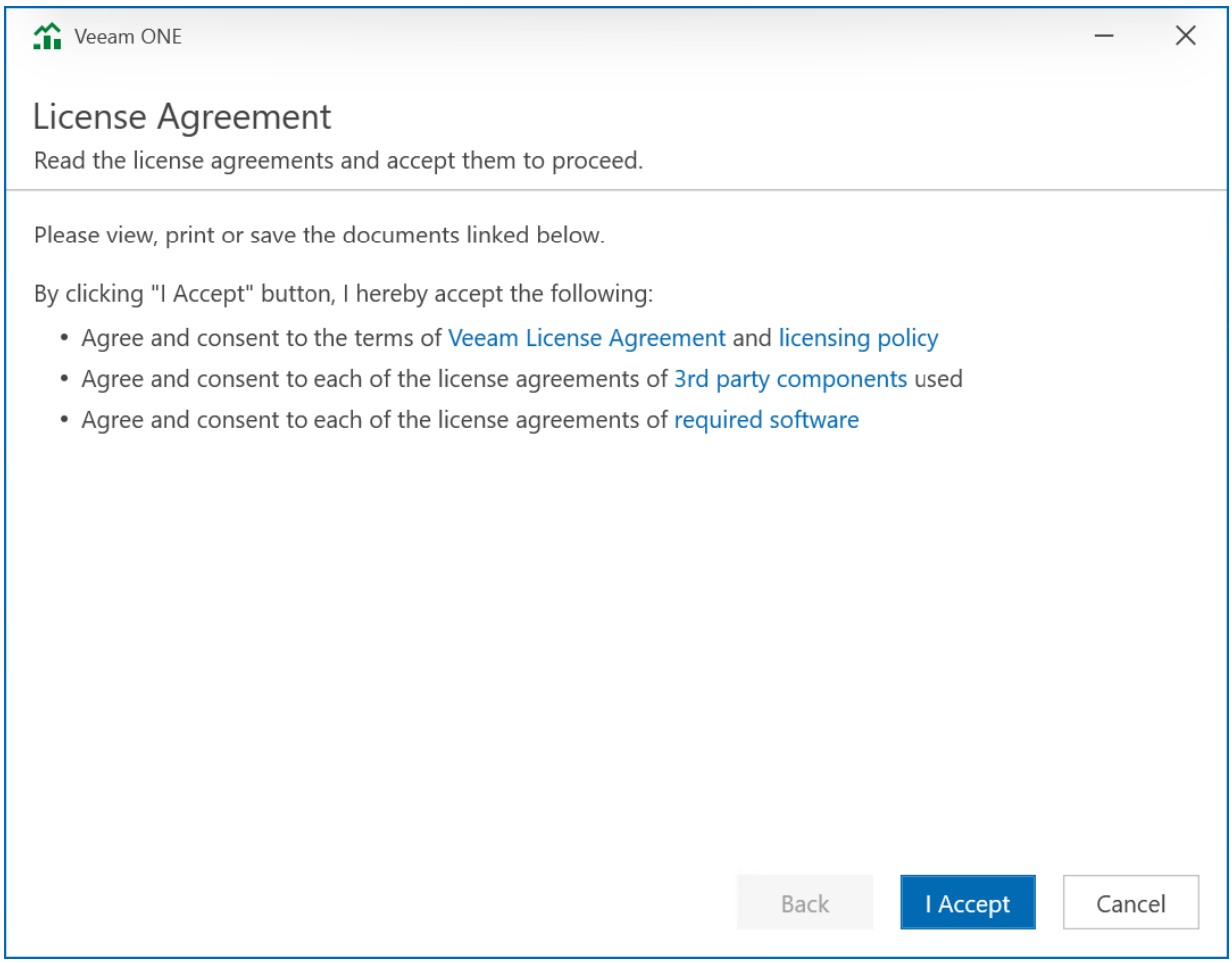
To open Veeam Help Center from the setup wizard, click **View Documentation**.



Step 3. Accept License Agreements

At the **License Agreement** step of the wizard, read and accept Veeam license agreement, licensing policy, 3rd party components and required software license agreements. You will not be able to continue installation until you accept license agreements.

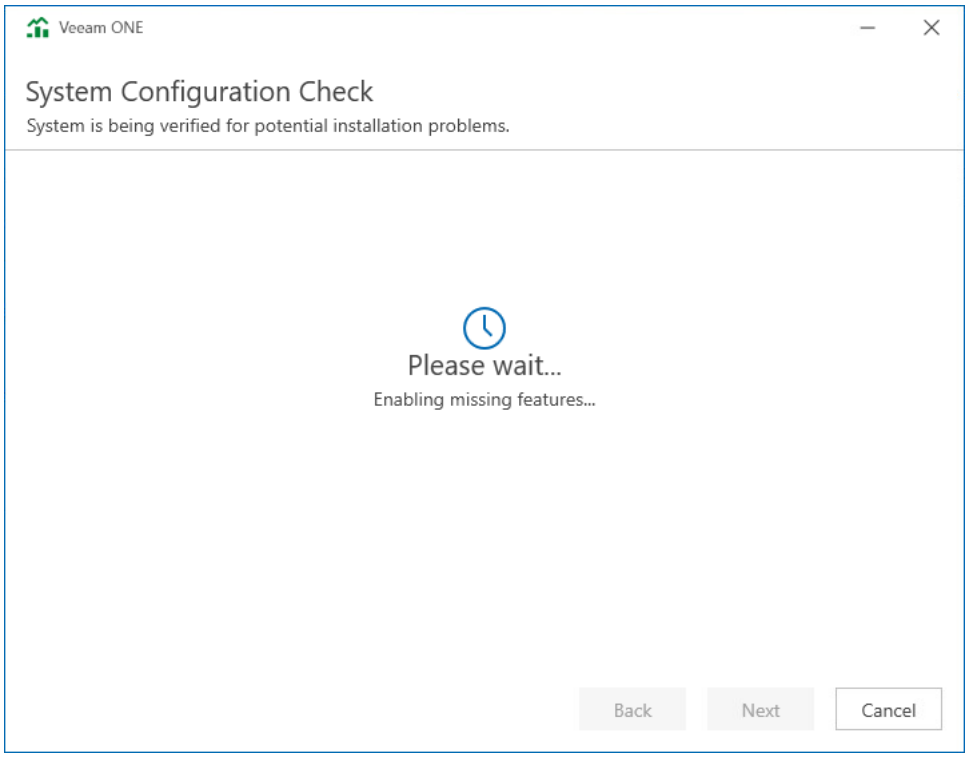
To read the terms of the license agreements, click the individual links.



Step 4. Perform System Configuration Check

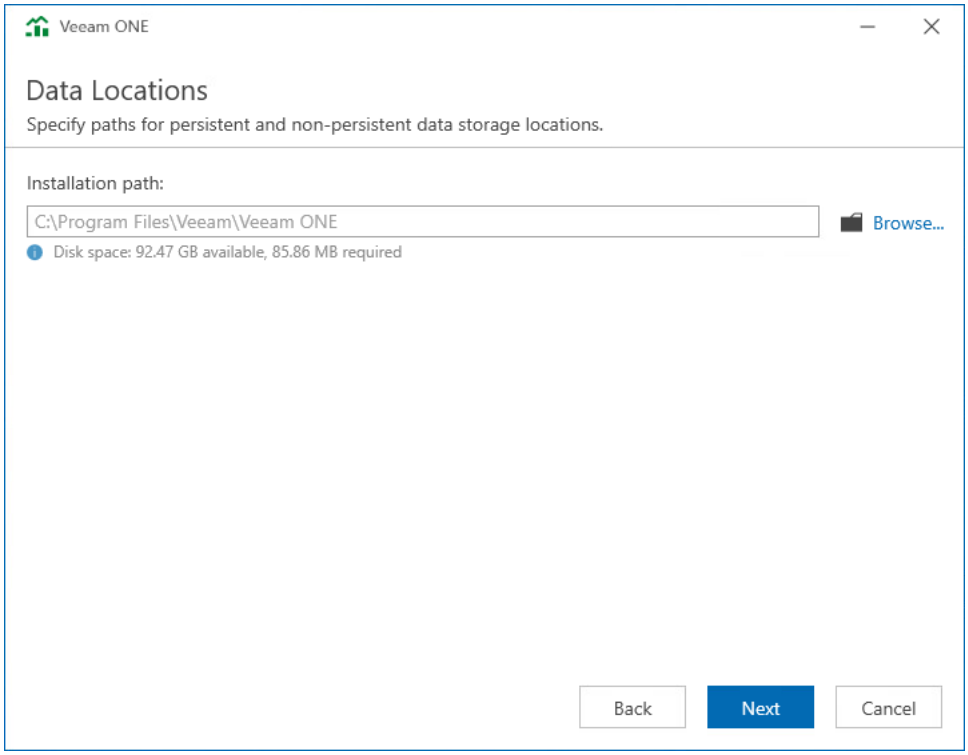
Before proceeding with the installation, the installer will perform system configuration check to determine if all prerequisite software is available on the machine. To learn what software is required for Veeam ONE, see System Requirements.

If some of the required software components are missing, the setup wizard will enable the missing software components and features automatically.



Step 5. Choose Installation Path

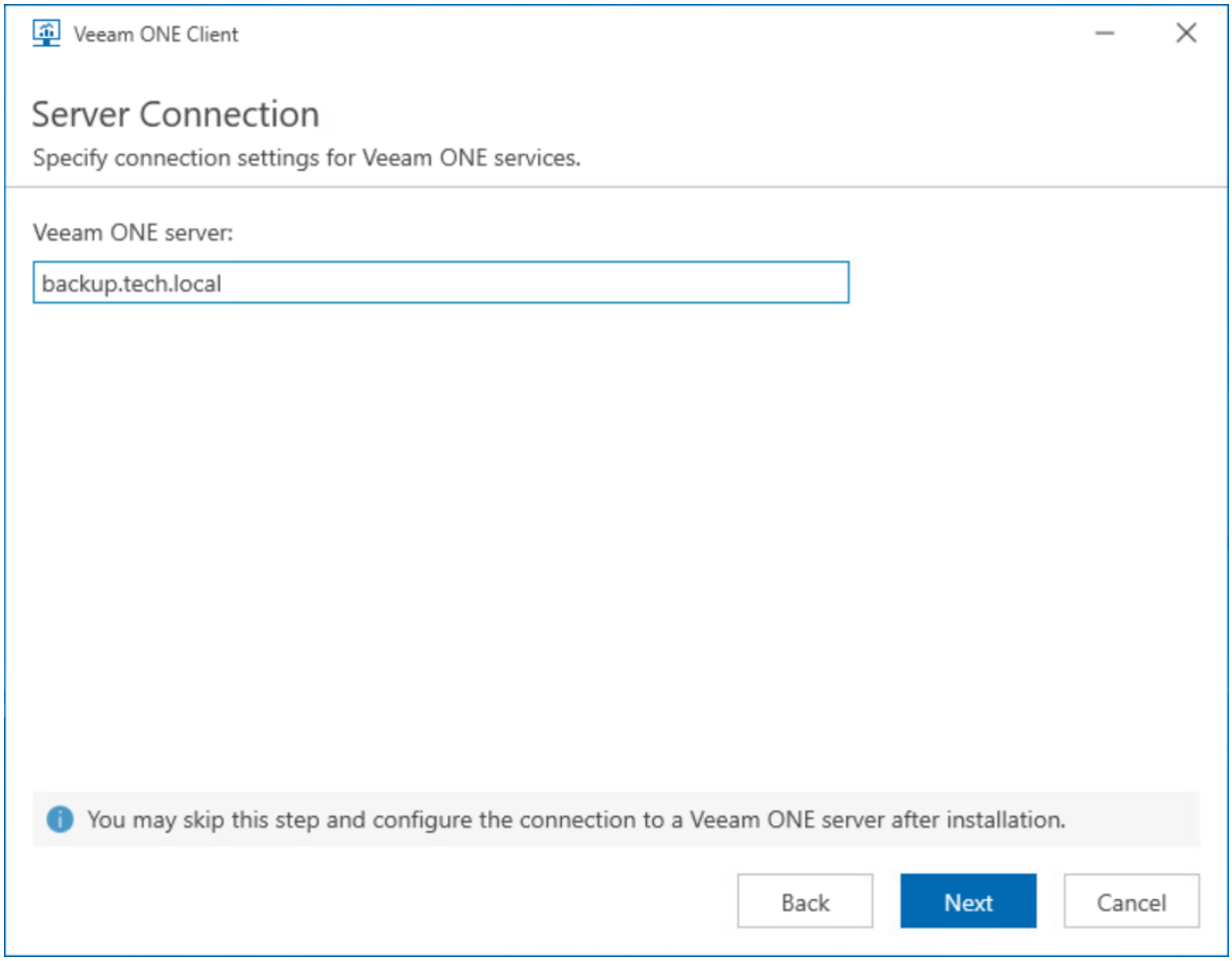
To change the installation directory, click **Browse** and select the location where you want to install Veeam ONE Client.



Step 6. Specify Veeam ONE Server Name

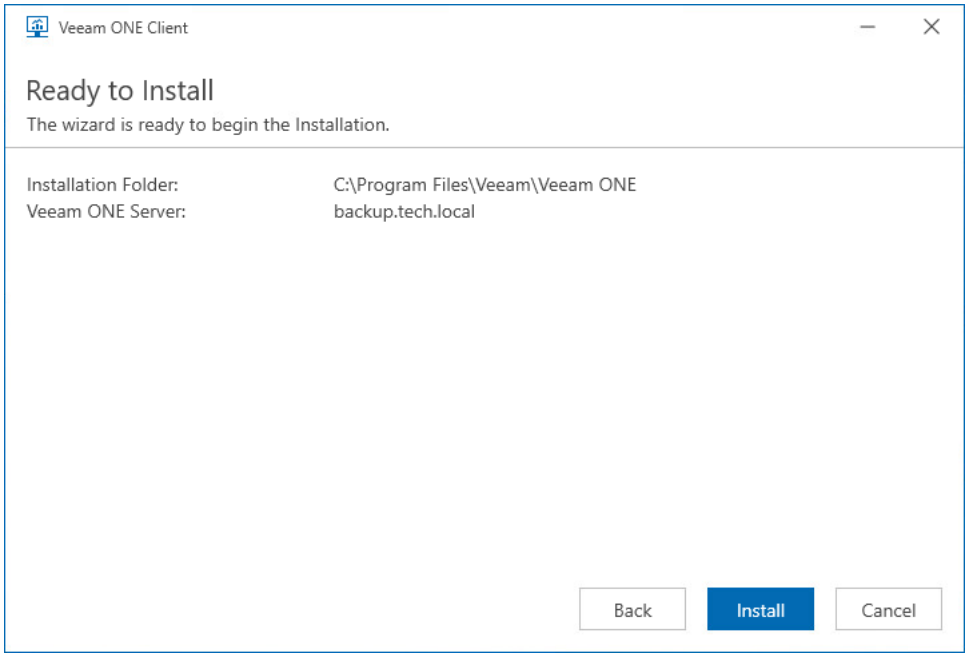
At the **Server Connection** step of the wizard, specify the FQDN or IP address of a machine where the Veeam ONE Server component is installed.

You can skip this step. In this case, you will be prompted to specify Veeam ONE Server name when you launch Veeam ONE Client for the first time.



Step 7. Review Installation Summary

At the **Ready to Install** step of the wizard, carefully review installation configuration to ensure that you specified correct settings. Click **Install** to begin the installation process.

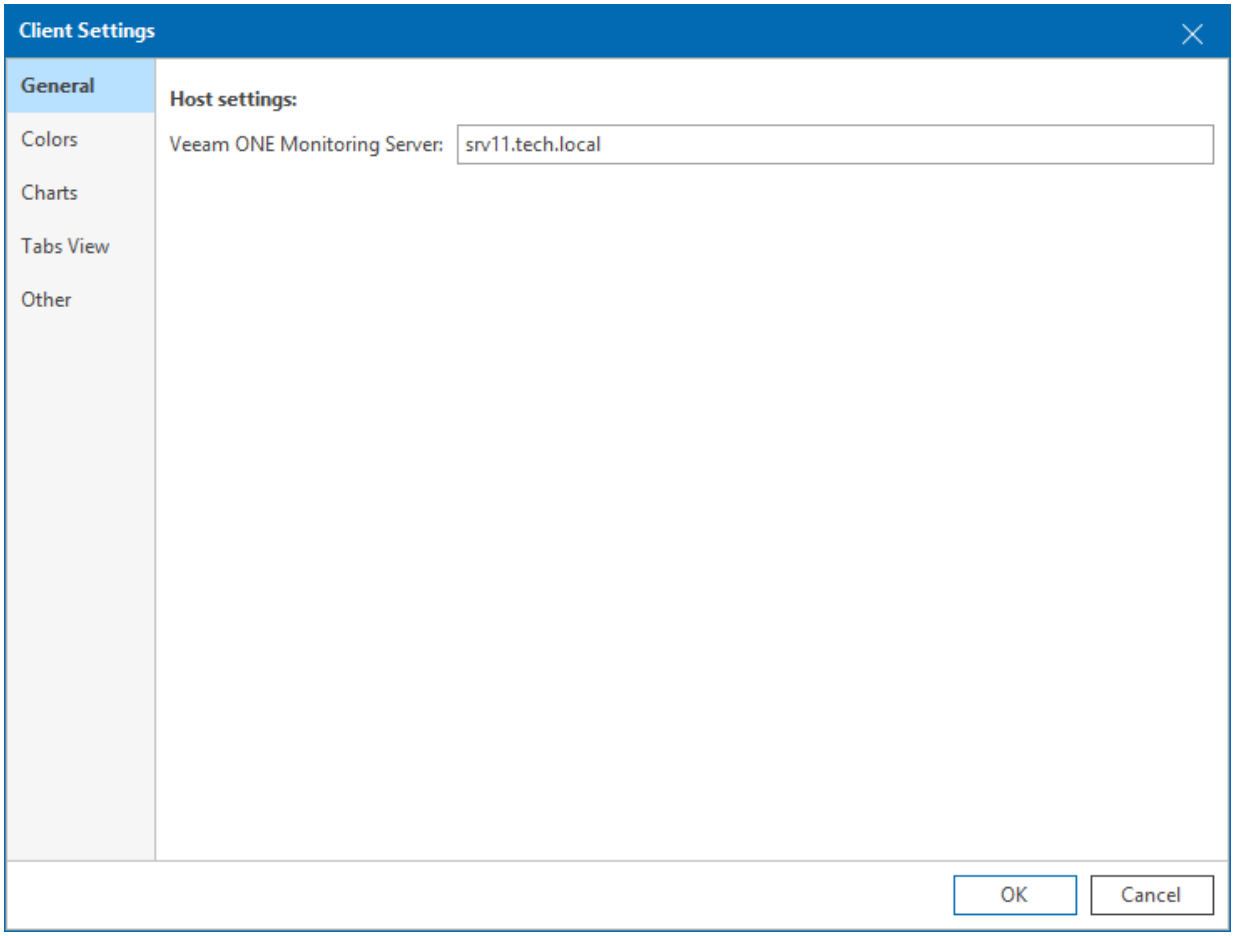


When the installation completes, click **Finish** to close the wizard.

Step 8. Check Veeam ONE Client Settings

If Veeam ONE Client is installed separately from the Veeam ONE Server component, make sure that Veeam ONE Client can communicate with the Veeam ONE Server part.

On the machine where you installed Veeam ONE Client, start the Veeam ONE Client. If during installation you did not specify the name of a machine where Veeam ONE Server runs, you will be prompted to provide the server name. If, for some reason, you cannot see a window prompting for the Veeam ONE Server name, in Veeam ONE Client main menu select **Settings** > **Client Settings** > **General**, and specify the name of a machine hosting Veeam ONE Server.



Installing Veeam ONE in Unattended Mode

You can install Veeam ONE in the unattended mode using the command line interface. The unattended installation mode does not require user interaction. You can use it to automate the installation process in large deployments.

Before You Begin

Before you start unattended installation, make sure that you perform the following steps:

1. Download the Veeam ONE installation image from the Veeam website. You can burn the downloaded image to a CD/DVD or mount the image to the target machine using disk image emulation software.
2. Check the system requirements. For details, see System Requirements.
3. Log on to the target machine under the account that has the Local Administrator permissions on the machine. For details, see Permissions.
4. Obtain a license file. If you do not specify a path to the license file during installation, Veeam ONE will operate in the Community Edition mode.
5. Define required and optional parameters in either the `VoAnswerFile_install.xml` or `VoClientAnswerFile_install.xml` file found in the `\Setup\Silent\AnswerFiles` folder of the Veeam ONE installation image:
   - To install all Veeam ONE components use `VoAnswerFile_install.xml` located in the `/Setup/Silent/AnswerFiles/VO` folder.

     To upgrade or uninstall all Veeam ONE components, use the `_uninstall.xml` and `_upgrade.xml` files located in the same folder.
   - To install Veeam ONE Client use `VoClientAnswerFile_install.xml` located in the `/Setup/Silent/AnswerFiles/VOClient` folder.

     To upgrade or uninstall Veeam ONE Client, use the `_uninstall.xml` and `_upgrade.xml` files located in the same folder.

Running Unattended Installation

To install Veeam ONE in unattended mode:

1. Open the product installation image file.
2. Navigate to the `Setup\Silent\AnswerFiles` folder.
3. Depending on what components you want to install, open `VO for Veeam ONE` or `VOCLient for Veeam ONE Client`.
4. In the relevant folder, open the `VoAnswerFile_install.xml` file in your preferred text editor.

   The file contains all the relevant information, including optional and required parameters for you to complete based on your installation requirements.
5. Once all parameters are complete, save the file and close.
6. Navigate back to the folder where the `Veeam.Silent.Install.exe` file exists (typically the `setup\silent` path of your root folder) and open the command line tool.
7. To check that all parameters are correct, run the `Veeam.Silent.Install.exe /?` command. This will display any unspecified parameters that must be completed before running unattended installation.
8. To run the install, enter `Veeam.Silent.Install.exe /AnswerFile C:\YourDesiredLogFolderPath_install.xml` where `YourDesireLogFolderPath` is the installation log files location.

   During installation the command line will return any error messages that need to be fixed.

NOTE:

You cannot use your Veeam account log in to verify your license, you can only specify the path to the license file. For details on Step 4. Provide License.

Installation Command-Line Syntax

You can install the following Veeam ONE components in the unattended mode:

- Monitoring Service
- Reporting Service
- Web Services
- Veeam ONE Client
- Veeam Analytics Service

NOTE:

You must install server components first to create Veeam ONE database. Installation of UI components (Veeam ONE Web Client and Veeam ONE Client) requires reference to an existing database.

Monitoring Service

To install Veeam ONE Monitoring service, use a command with the following syntax:

```
msiexec.exe [/L*v "<path_to_log>"] /qn /i "<path_to_msi>" [ACCEPT_THIRDPARTY_LI
CENSES="1"][ACCEPT_EULA="1"][ACCEPT_REQUIRED_SOFTWARE="1"][ACCEPT_LICENSING_POL
ICY="1"][VM_MN_SERVICEACCOUNT="<Veeam_One_Service_Account>"][VM_MN_SERVICEPASSW
ORD="<Veeam_One_Service_Account_Password>"][VM_MN_SQL_SERVER="<SQL_server>"][VM
_MN_SQL_DATABASE="<database_name>"] [VM_MN_SQL_AUTHENTICATION="0"] [VM_MN_SQL_U
SER="<SQL_auth_username>"] [VM_MN_SQL_PASSWORD="<SQL_auth_password>"] [EDITLICF
ILEPATH="<path_to_license_file>"] [VO_LICENSE_AUTOUPDATE="1"] [PF_VEEAMONE="<pa
th_to_installdir >"][VM_GRPC_SERVER_PORT="<port_number>"][VM_MN_CACHE="<path_to
_cache_folder>"] [VO_INSTALLATION_TYPE="0"] [VM_MN_SERVER_AUTOUPDATE_ENABLED="1
"]
```

The command has the following parameters:

Option	Parameter	Required	Description
/L	*v logfile	No	Creates an installation log file with the verbose output. Specify an existing path to the log file as the parameter value. A setup log file created during the previous installation is cleared. Example: */L*v "C:\ProgramData\Veeam\Setup\Temp\Logs\MonitorServerSetup.txt"*
/q	n	Yes	Sets the user interface level to "no", which means no user interaction is needed during installation.

Option	Parameter	Required	Description
/i	setup file	Yes	Installs Veeam ONE Monitoring service. Specify a full path to the setup file as the parameter value. Example: */i "C:\Veeam\Monitor\VeeamONE.Monitor.Server.x64.msi"*
ACCEPT_THIRDPARTY_LICENSES	0/1	Yes	Specifies if you want to accept the terms of the license agreement for the 3rd party components. Specify 1 if you want to accept the terms and proceed with installation. Example: *ACCEPT_THIRDPARTY_LICENSES="1"*
ACCEPT_EULA	0/1	Yes	Specifies if you want to accept the terms of the Veeam license agreement. Specify 1 if you want to accept the terms and proceed with installation. Example: *ACCEPT_EULA="1"*
ACCEPT_LICENSING_POLICY	0/1	Yes	Specifies if you want to accept the terms of the Veeam licensing policy. Specify 1 if you want to accept the terms and proceed with installation. Example: *ACCEPT_LICENSING_POLICY="1"*
ACCEPT_REQUIRED_SOFTWARE	0/1	Yes	Specifies if you want to accept the terms of the required software license agreements. Specify 1 if you want to accept the terms and proceed with installation. Example: *ACCEPT_REQUIRED_SOFTWARE="1"*
VM_MN_SERVICEACCOUNT	user	Yes	Specifies a user account under which the Veeam ONE Services will run and that will be used to access Veeam ONE database in the Microsoft Windows authentication mode. Example: *VM_MN_SERVICEACCOUNT="ONESERVER\Administrator"*

Option	Parameter	Required	Description
VM_MN_SERVICEPASSWORD	password	Yes	This parameter must be used if you have specified the *VM_MN_SERVICEACCOUNT* parameter. Specifies a password for the account under which the Veeam ONE Services will run and that will be used to access Veeam ONE database. Example: *VM_MN_SERVICEPASSWORD="p@ssw0rd"*
VM_MN_SQL_SERVER	SQL server\instance	No	Specifies a Microsoft SQL server and instance on which the Veeam ONE database will be deployed. By default, Veeam ONE uses the *LOCALHOST|VEEAMSQL2016* server. Example: *VM_MN_SQL_SERVER="ONESERVER|VEEAMSQL2016_MY"*
VM_MN_SQL_DATABASE	database	No	Specifies a name of the Veeam ONE database, by default, VeeamOne. Example: *VM_MN_SQL_DATABASE="VeeamOneDB"*
VM_MN_SQL_AUTHENTICATION	0/1	No	Specifies if you want to use the Microsoft SQL Server authentication mode to connect to the Microsoft SQL Server where the Veeam ONE database is deployed. Specify 1 to use the SQL Server authentication mode. If you do not use this parameter, Veeam ONE will connect to the Microsoft SQL Server in the Microsoft Windows authentication mode (default value, 0). Together with this parameter, you must specify the following parameters: *VM_MN_SQL_USER* and *VM_MN_SQL_PASSWORD.* Example: *VM_MN_SQL_AUTHENTICATION="1"*
VM_MN_SQL_USER	user	No	This parameter must be used if you have specified the *VM_MN_SQL_AUTHENTICATION* parameter. Specifies a LoginID to connect to the Microsoft SQL Server in the SQL Server authentication mode. Example: *VM_MN_SQL_USER="sa"*
VM_MN_SQL_PASSWORD	password	No	This parameter must be used if you have specified the *VM_MN_SQL_AUTHENTICATION* parameter. Specifies a password to connect to the Microsoft SQL Server in the SQL Server authentication mode. Example: *VM_MN_SQL_PASSWORD="p@ssw0rd"*

Option	Parameter	Required	Description
EDITLICFILEPATH	license path	No	Specifies a full path to the license file. If this parameter is not specified, Veeam ONE Community Edition will be installed. Example: *EDITLICFILEPATH="C:\Users\Administrator\Desktop\veeam_one_subscription_100_100.lic"*
VO_LICENSE_AUTOUPDATE	0/1	No	Specifies if you want to enable automatic license update and usage reporting. By default, license auto update is enabled. Example: VO_LICENSE_AUTOUPDATE="0"
PF_VEEAMONE	path	No	Installs the component to the specified location. By default, Veeam ONE uses the `Veeam ONE Monitor Server` subfolder of the `C:\Program Files\Veeam\Veeam ONE` folder. Example: *PF_VEEAMONE="C:\Veeam\"* The component will be installed to the `C:\Veeam\Veeam ONE Monitor Server` folder.
VM_GRPC_SERVER_PORT	port number	No	Specifies the port number used for communication between Veeam ONE Monitoring service and Veeam ONE Web Client. If you do not use this parameter, Veeam ONE Monotoring service will use the default port 2714. Example: *VM_GRPC_SERVER_PORT="2714"*
VM_MN_CACHE	path	No	Specifies a path to the folder where Performance Cache will be stored. If you do not use this parameter, the performance cache will be stored to the `C:\PerfCache` folder (default). Example: *VM_MN_CACHE="D:\Veeam\PerfCache"*

Option	Parameter	Required	Description
VO_INSTALLATION_TYPE	0, 1 or 2	No	Specifies the mode in which Veeam ONE will collect data from virtualization and Veeam Backup & Replication servers. Specify 1 to use the **Veeam backup data and large-scale virtual infrastructure performance monitoring** mode. Specify 2 to use the **Veeam backup data only** mode. If you do not use this parameter, Veeam ONE will collect data in the **Veeam backup data and virtual infrastructure performance monitoring mode** (default value, 0). For details, see Choose Data Collection Mode. Example: *VO_INSTALLATION_TYPE="2"*
VM_MN_SERVER_AUTOUPDATE_ENABLED	0/1	No	Specifies if you want to enable automatic updates after Veeam ONE installation. Specify 1 to enable automatic updates. Example: *VM_MN_SERVER_AUTOUPDATE_ENABLED="1"*

Example

Suppose you want to install Monitoring service with the following configuration:

- Installation log location: *C:|ProgramData|Veeam|Setup|Temp|Logs|MonitorServerSetup.txt*
- No user interaction
- Path to the MSI file: *C:|Veeam|Monitor|VeeamONE.Monitor.Server.x64.msi*
- Accept 3rd party license agreement
- Accept Veeam license agreement
- Accept required software license agreements
- Accept Veeam licensing policy
- Service user account: *ONESERVER|Administrator*
- Service user account password: *p@ssw0rd*
- License file location: *C:|Users|Administrator|Desktop|veeam_one_subscription_100_100.lic*
- Automatic license update: default
- Installation folder: default
- Path to Performance Cache folder: *D:|Veeam|PerfCache*
- SQL Server instance and database name: default
- Data collection mode: Veeam backup data and virtual infrastructure performance monitoring
- Automatic updates: enabled

The command to install Monitoring service with such configuration will have the following parameters:

```
msiexec.exe /L*v "C:\ProgramData\Veeam\Setup\Temp\Logs\MonitorServerSetup.txt"
/qn /i "C:\Veeam\Monitor\VeeamONE.Monitor.Server.x64.msi" ACCEPT_THIRDPARTY_LIC
ENSES="1" ACCEPT_EULA="1" ACCEPT_REQUIRED_SOFTWARE="1" ACCEPT_LICENSING_POLICY=
"1" VM_MN_SERVICEACCOUNT="ONESERVER\Administrator" VM_MN_SERVICEPASSWORD="p@ssw
0rd" EDITLICFILEPATH="C:\Users\Administrator\Desktop\veeam_one_subscription_100
_100.lic" VM_MN_CACHE="D:\Veeam\PerfCache" VO_INSTALLATION_TYPE="0" VM_MN_SERVE
R_AUTOUPDATE_ENABLED="1"
```

Reporting Service

To install Veeam ONE Reporting service, use a command with the following syntax:

```
msiexec.exe [/L*v "<path_to_log>"] /qn /i "<path_to_msi>" [ACCEPT_THIRDPARTY_LI
CENSES="1"][ACCEPT_EULA="1"][ACCEPT_REQUIRED_SOFTWARE="1"][ACCEPT_LICENSING_POL
ICY="1"][INSTALLDIR="<path_to_installdir >"][VO_REPORTER_SERVICE_ACCOUNT_NAME="
<Veeam_One_Service_Account>"][VO_REPORTER_SERVICE_ACCOUNT_PASSWORD="<Veeam_One_
Service_Account_Password>"][VO_REPORTER_SQL_SERVER_NAME="<SQL_server>"][VO_REPO
RTER_DATABASE_NAME="<database_name>"] [VO_REPORTER_AUTHENTICATION_MODE="0"] [VO
_REPORTER_SQL_USER_NAME="<SQL_auth_username>"] [VO_REPORTER_SQL_PASSWORD="<SQL_
auth_password>"] [EDITLICFILEPATH="<path_to_license_file>"] [VO_INSTALLATION_TY
PE="0"][VO_REPORTER_SERVER_WEB_API_CERTIFICATE_NAME="<certificate_name>"] [VO_R
EPORTER_SERVER_COMMUNICATION_PORT="<port_number>"] [VO_REPORTER_SERVER_WEB_API_
PORT="<port_number>"]
```

The command has the following parameters:

Option	Parameter	Required	Description
/L	*v logfile	No	Creates an installation log file with the verbose output. Specify an existing path to the log file as the parameter value. A setup log file created during the previous installation is cleared. Example: */L*v "C:\ProgramData\Veeam\Setup\Temp\Logs\ReporterServerSetup.txt"*
/q	n	Yes	Sets the user interface level to "no", which means no user interaction is needed during installation.
/i	setup file	Yes	Installs Veeam ONE Reporting Server. Specify a full path to the setup file as the parameter value. Example: */i "C:\Veeam\Reporter\VeeamONE.Reporter.Server.x64.msi"*

Option	Parameter	Required	Description
ACCEPT_THIRDPARTY_LICENSES	0/1	Yes	Specifies if you want to accept the terms of the license agreement for the 3rd party components. Specify 1 if you want to accept the terms and proceed with installation. Example: *ACCEPT_THIRDPARTY_LICENSES="1"*
ACCEPT_EULA	0/1	Yes	Specifies if you want to accept the terms of the Veeam license agreement. Specify *yes* if you want to accept the terms and proceed with installation. Example: *ACCEPT_EULA="1"*
ACCEPT_LICENSING_POLICY	0/1	Yes	Specifies if you want to accept the terms of the Veeam licensing policy. Specify 1 if you want to accept the terms and proceed with installation. Example: *ACCEPT_LICENSING_POLICY="1"*
ACCEPT_REQUIRED_SOFTWARE	0/1	Yes	Specifies if you want to accept the terms of the required software license agreements. Specify 1 if you want to accept the terms and proceed with installation. Example: *ACCEPT_REQUIRED_SOFTWARE="1"*
INSTALLDIR	path	No	Installs the component to the specified location. By default, Veeam ONE uses the `Veeam ONE Reporter Server` subfolder of the `C:\Program Files\Veeam\Veeam ONE` folder. Example: *INSTALLDIR="C:|Veeam|"* The component will be installed to the `C:\Veeam\Veeam ONE Reporter Server` folder.
VO_REPORTER_SERVICE_ACCOUNT_NAME	user	Yes	Specifies a user account under which the Veeam ONE Services will run and that will be used to access Veeam ONE database in the Microsoft Windows authentication mode. Example: *VO_REPORTER_SERVICE_ACCOUNT_NAME="ONESERVER|Administrator"*

Option	Parameter	Required	Description
VO_REPORTER_SERVICE_ACCOUNT_PASSWORD	password	Yes	This parameter must be used if you have specified the *VO_REPORTER_SERVICE_ACCOUNT_NAME* parameter. Specifies a password for the account under which the Veeam ONE Services will run and that will be used to access Veeam ONE database. Example: *VO_REPORTER_SERVICE_ACCOUNT_PASSWORD="p@sswOrd"*
VO_REPORTER_SQL_SERVER_NAME	SQL server\instance	No	Specifies a Microsoft SQL server and instance on which the Veeam ONE database will be deployed. By default, Veeam ONE uses the *LOCALHOST|VEEAMSQL2016* server. Example: *VO_REPORTER_SQL_SERVER_NAME="ONESERVER|VEEAMSQL2016_MY"*
VO_REPORTER_DATABASE_NAME	database	No	Specifies a name of the Veeam ONE database, by default, VeeamOne. Example: *VO_REPORTER_DATABASE_NAME="VeeamOneDB"*
VO_REPORTER_AUTHENTICATION_MODE_NAME	0/1	No	Specifies if you want to use the Microsoft SQL Server authentication mode to connect to the Microsoft SQL Server where the Veeam ONE database is deployed. Specify 1 to use the SQL Server authentication mode. If you do not use this parameter, Veeam ONE will connect to the Microsoft SQL Server in the Microsoft Windows authentication mode (default value, 0). Together with this parameter, you must specify the following parameters: *VO_REPORTER_SQL_USER_NAME* and *VO_REPORTER_SQL_PASSWORD*. Example: *VO_REPORTER_AUTHENTICATION_MODE_NAME="1"*
VO_REPORTER_SQL_USER_NAME	user	No	This parameter must be used if you have specified the *VO_REPORTER_AUTHENTICATION_TYPE_NAME* parameter. Specifies a LoginID to connect to the Microsoft SQL Server in the SQL Server authentication mode. Example: *VO_REPORTER_SQL_USER_NAME="sa"*

Option	Parameter	Required	Description
VO_REPORTER_SQL_PASSWORD	password	No	This parameter must be used if you have specified the *VO_REPORTER_AUTHENTICATION_TYPE_NAME* parameter. Specifies a password to connect to the Microsoft SQL Server in the SQL Server authentication mode. Example: *VO_REPORTER_SQL_PASSWORD="p@ssw0rd"*
EDITLICFILEPATH	license path	No	Specifies a full path to the license file. If this parameter is not specified, Veeam ONE Free Edition will be installed. Example: *EDITLICFILEPATH="C:\Users\Administrator\Desktop\veeam_one_subscription_100_100.lic"*
VO_REPORTER_SERVER_COMMUNICATION_PORT	port number	No	Specifies the port number used for communication between Veeam ONE Reporting service and Veeam ONE Web Client. If you do not use this parameter, Veeam ONE Reporting service will use the default port 2742. Example: *VO_REPORTER_SERVER_COMMUNICATION_PORT="2742"*
VO_REPORTER_SERVER_WEB_API_PORT	port number	No	Specifies the port number used for communication with Veeam ONE Web API. If you do not use this parameter, Veeam ONE Reporting service will use the default port 2741. Example: *VO_REPORTER_SERVER_WEB_API_PORT="2741"*
VO_REPORTER_SERVER_WEB_API_CERTIFICATE_NAME	certificate name	No	Specifies the certificate to be used by Veeam ONE Web API. The certificate must be installed to the Certificate Store on the machine where you run installation. If this parameter is not specified, a new self-signed certificate will be generated by `openssl.exe`.

Option	Parameter	Required	Description
VO_INSTALLATION_TYPE	0, 1 or 2	No	Specifies the mode in which Veeam ONE will collect data from virtualization and Veeam Backup & Replication servers. Specify 1 to use the **Optimized for Advanced Scalability Deployment** mode. Specify 2 to use **The Backup Data Only** mode. If you do not use this parameter, Veeam ONE will collect data in the **Optimized for Typical Deployment** mode (default value, 0). For details, see Choose Data Collection Mode. Example: *VO_INSTALLATION_TYPE="2"*

Example

Suppose you want to install Veeam ONE Web Client server with the following configuration:

- Installation log location: *C:|ProgramData|Veeam|Setup|Temp|Logs|ReporterServerSetup.txt*
- No user interaction
- Path to the MSI file: *C:|Veeam|Reporter|VeeamONE.Reporter.Server.x64.msi*
- Accept 3rd party license agreement
- Accept Veeam license agreement
- Accept required software license agreements
- Accept Veeam licensing policy
- Installation folder: default
- Service user account: *ONESERVER|Administrator*
- Service user account password: *p@ssw0rd*
- SQL Server instance and database name: default
- License file location: *C:|Users|Administrator|Desktop|veeam_one_subscription_100_100.lic*
- Data collection mode: Optimized for Typical Deployment
- Communication port: default
- Web API port: default
- Web API certificate: generate new self-signed certificate

The command to install Veeam ONE Web Client server with such configuration will have the following parameters:

```
msiexec.exe /L*v "C:\ProgramData\Veeam\Setup\Temp\Logs\ReporterServerSetup.txt"
/qn /i "C:\Veeam\Reporter\VeeamONE.Reporter.Server.x64.msi" ACCEPT_THIRDPARTY_L
ICENSES="1" ACCEPT_EULA="1" ACCEPT_REQUIRED_SOFTWARE="1" ACCEPT_LICENSING_POLIC
Y="1" VO_REPORTER_SERVICE_ACCOUNT_NAME="ONESERVER\Administrator" VO_REPORTER_SE
RVICE_ACCOUNT_PASSWORD="p@ssw0rd" EDITLICFILEPATH="C:\Users\Administrator\Deskt
op\veeam_one_subscription_100_100.lic" VO_INSTALLATION_TYPE="0"
```

Web Services

To install Veeam ONE Web Services, use a command with the following syntax:

```
msiexec.exe [/L*v "<path_to_log>"] /qn /i "<path_to_msi>" [ACCEPT_THIRDPARTY_LI
CENSES="1"][ACCEPT_EULA="1"][ACCEPT_REQUIRED_SOFTWARE="1"][ACCEPT_LICENSING_POL
ICY="1"][INSTALLDIR="<path_to_installdir >"][VO_REPORTER_WEB_SERVER_NAME="<Veea
m_One_Server_Name>"][VO_REPORTER_WEB_CONNECTION_ACCOUNT_NAME="<Veeam_One_Servic
e_Account>"][VO_REPORTER_WEB_CONNECTION_ACCOUNT_PASSWORD="<Veeam_One_Service_Ac
count_Password>"][VO_REPORTER_WEB_SERVER_WEB_API_PORT="<port_number>"] [VO_REPO
RTER_WEB_SITE_PORT="<reporter_site_port>"] [VO_REPORTER_WEB_SITE_CERTIFICATE_TH
UMBPRINT="reporter_site_certificate"]
```

The command has the following parameters:

Option	Parameter	Required	Description
/L	*v logfile	No	Creates an installation log file with the verbose output. Specify an existing path to the log file as the parameter value. A setup log file created during the previous installation is cleared. Example: */L*v "C:|ProgramData|Veeam|Setup|Temp|Logs|ReporterWEBSetup.txt"*
/q	n	Yes	Sets the user interface level to "no", which means no user interaction is needed during installation.
/i	setup file	Yes	Installs Veeam ONE Web Client Web UI. Specify a full path to the setup file as the parameter value. Example: */i "C:|Veeam|Reporter|VeeamONE.Reporter.WebUI.x64.msi"*

Option	Parameter	Required	Description
ACCEPT_THIRDPARTY_LICENSES	0/1	Yes	Specifies if you want to accept the terms of the license agreement for the 3rd party components. Specify 1 if you want to accept the terms and proceed with installation. Example: *ACCEPT_THIRDPARTY_LICENSES="1"*
ACCEPT_EULA	0/1	Yes	Specifies if you want to accept the terms of the Veeam license agreement. Specify *1* if you want to accept the terms and proceed with installation. Example: *ACCEPT_EULA="1"*
ACCEPT_LICENSING_POLICY	0/1	Yes	Specifies if you want to accept the terms of the Veeam licensing policy. Specify 1 if you want to accept the terms and proceed with installation. Example: *ACCEPT_LICENSING_POLICY="1"*
ACCEPT_REQUIRED_SOFTWARE	0/1	Yes	Specifies if you want to accept the terms of the required software license agreements. Specify 1 if you want to accept the terms and proceed with installation. Example: *ACCEPT_REQUIRED_SOFTWARE="1"*
INSTALLDIR	path	No	Installs the component to the specified location. By default, Veeam ONE uses the `Veeam ONE Reporter Web` subfolder of the `C:\Program Files\Veeam\Veeam ONE` folder. Example: *INSTALLDIR="C:|Veeam|"* The component will be installed to the `C:\Veeam\Veeam ONE Reporter Web` folder.
VO_REPORTER_WEB_SERVER_NAME	server name	Yes	Specifies FQDN of the server where Veeam ONE Reporting Service is installed. Example: *VO_REPORTER_WEB_SERVER_NAME="oneserver.tech.local"*

Option	Parameter	Required	Description
VO_REPORTER_WEB_CONNECTION_ACCOUNT_NAME	user	Yes	Specifies a user account that will be used to access and configure Veeam ONE Reporting Service from the Web Client in the Microsoft Windows authentication mode. Example: *VO_REPORTER_WEB_CONNECTION_ACCOUNT_NAME="ONESERVER\Administrator"*
VO_REPORTER_WEB_CONNECTION_ACCOUNT_PASSWORD	password	Yes	This parameter must be used if you have specified the *VO_REPORTER_WEB_CONNECTION_ACCOUNT_NAME* parameter. Specifies a password for the account that will be used to access Veeam ONE Reporting Service from the Web UI. Example: *VO_REPORTER_WEB_CONNECTION_ACCOUNT_PASSWORD="p@ssw0rd"*
VO_REPORTER_WEB_SITE_PORT	port	No	Specifies a port that will be used by the Veeam ONE Web Client website. By default, port number 1239 is used. Example: *VO_REPORTER_WEB_SITE_PORT="1239"*
VO_REPORTER_WEB_SITE_CERTIFICATE_THUMBPRINT	hash	No	Specifies the certificate to be used by the Veeam ONE Web Client website. If this parameter is not specified, a new certificate will be generated by `openssl.exe`. Example: *RP_THUMBPRINT="0677d0b8f27caccc966b15d807b41a101587b488"*
VO_REPORTER_WEB_SERVER_WEB_API_PORT	port	No	Specifies the port number used for communication with Veeam ONE Web API. If you do not use this parameter, Veeam ONE Web Client will use the default port 2741. Example: *VO_REPORTER_WEB_SERVER_WEB_API_PORT="2741"*

Example

Suppose you want to install Veeam ONE Web Client with the following configuration:

- Installation log location: *C:|ProgramData|Veeam|Setup|Temp|Logs|ReporterWEBSetup.txt*
- No user interaction
- Path to the MSI file: *C:|Veeam|Reporter|VeeamONE.Reporter.WebUI.x64.msi*
- Accept 3rd party license agreement
- Accept Veeam license agreement
- Accept required software license agreements
- Accept Veeam licensing policy
- Installation folder: default
- Veeam ONE Server name: oneserver.tech.local
- Service user account: *ONESERVER|Administrator*
- Service user account password: *p@ssw0rd*
- Website port: default
- Website certificate: generate new
- Web API port: default

The command to install Veeam ONE Web Client with such configuration will have the following parameters:

```
msiexec.exe /L*v "C:\ProgramData\Veeam\Setup\Temp\Logs\ReporterWEBSetup.txt" /q
n /i "C:\Veeam\Reporter\VeeamONE.Reporter.WebUI.x64.msi" ACCEPT_THIRDPARTY_LICE
NSES="1" ACCEPT_EULA="1" ACCEPT_REQUIRED_SOFTWARE="1" ACCEPT_LICENSING_POLICY="
1" VO_REPORTER_WEB_SERVER_NAME="ONESERVER.TECH.LOCAL" VO_REPORTER_WEB_CONNECTIO
N_ACCOUNT_NAME="ONESERVER\Administrator" VO_REPORTER_WEB_CONNECTION_ACCOUNT_PAS
SWORD="p@ssw0rd"
```

Veeam ONE Client

To install Veeam ONE Client, use a command with the following syntax:

```
msiexec.exe [/L*v "<path_to_log>"] /qn /i "<path_to_msi>" [ACCEPT_THIRDPARTY_LI
CENSES="1"][ACCEPT_EULA="1"][ACCEPT_REQUIRED_SOFTWARE="1"][ACCEPT_LICENSING_POL
ICY="1"][INSTALLDIR="<path_to_installdir >"][VM_CLN_SERVER_NAME="<one_server_ad
dress>"]
```

The command has the following parameters:

Option	Parameter	Required	Description
/L	*v logfile	No	Creates an installation log file with the verbose output. Specify an existing path to the log file as the parameter value. A setup log file created during the previous installation is cleared. Example: */L*v "C:\ProgramData\Veeam\Setup\Temp\Logs\MonitorClientSetup.txt"*
/q	n	Yes	Sets the user interface level to "no", which means no user interaction is needed during installation.
/i	setup file	Yes	Installs Veeam ONE Client. Specify a full path to the setup file as the parameter value. Example: */i "C:\Veeam\Monitor\VeeamONE.Monitor.Client.x64.msi "*
ACCEPT_THIRDPARTY_LICENSES	0/1	Yes	Specifies if you want to accept the terms of the license agreement for the 3rd party components. Specify 1 if you want to accept the terms and proceed with installation. Example: *ACCEPT_THIRDPARTY_LICENSES="1"*
ACCEPT_EULA	0/1	Yes	Specifies if you want to accept the terms of the Veeam license agreement. Specify *1* if you want to accept the terms and proceed with installation. Example: *ACCEPT_EULA="1"*
ACCEPT_LICENSING_POLICY	0/1	Yes	Specifies if you want to accept the terms of the Veeam licensing policy. Specify 1 if you want to accept the terms and proceed with installation. Example: *ACCEPT_LICENSING_POLICY="1"*
ACCEPT_REQUIRED_SOFTWARE	0/1	Yes	Specifies if you want to accept the terms of the required software license agreements. Specify 1 if you want to accept the terms and proceed with installation. Example: *ACCEPT_REQUIRED_SOFTWARE="1"*

Option	Parameter	Required	Description
INSTALLDIR	path	No	Installs the component to the specified location. By default, Veeam ONE uses the `Veeam ONE Monitor Client` subfolder of the `C:\Program Files\Veeam\Veeam ONE` folder. Example: *INSTALLDIR="C:\Veeam\"* The component will be installed to the `C:\Veeam\Veeam ONE Monitor Client` folder.
VM_CLN_SERVER_NAME	server name or address	No	Specifies FQDN or IP address of the server where Veeam ONE Client is deployed. Example: *VM_CLN_SERVER_NAME="oneserver.tech.local"*

Example

Suppose you want to install Veeam ONE Client with the following configuration:

- Installation log location: *C:\ProgramData\Veeam\Setup\Temp\Logs\MonitorClientSetup.txt*
- No user interaction
- Path to the MSI file: *C:\Veeam\Monitor\VeeamONE.Monitor.Client.x64.msi*
- Accept 3rd party license agreement
- Accept Veeam license agreement
- Accept required software license agreements
- Accept Veeam licensing policy
- Installation folder: default
- Veeam ONE server: *oneserver.tech.local*

The command to install Veeam ONE Client with such configuration will have the following parameters:

```
msiexec.exe /L*v "C:\ProgramData\Veeam\Setup\Temp\Logs\MonitorClientSetup.txt"
/qn /i "C:\Veeam\Monitor\VeeamONE.Monitor.Client.x64.msi" ACCEPT_THIRDPARTY_LIC
ENSES="1" ACCEPT_EULA="1" ACCEPT_REQUIRED_SOFTWARE="1" ACCEPT_LICENSING_POLICY=
"1" VM_CLN_SERVER_NAME="oneserver.tech.local"
```

Veeam Analytics Service

To install Veeam Analytics service, use a command with the following syntax:

```
msiexec.exe [/L*v "<path_to_log>"] /qn /i "<path_to_msi>" [ACCEPT_THIRDPARTY_LI
CENSES="1"][ACCEPT_EULA="1"][ACCEPT_REQUIRED_SOFTWARE="1"][ACCEPT_LICENSING_POL
ICY="1"][INSTALLDIR="<path_to_installdir >"][VO_AGENT_TYPE="1"][VO_AGENT_SERVIC
E_ACCOUNT_NAME="<Veeam_One_Service_Account>"][VO_AGENT_SERVICE_ACCOUNT_PASSWORD
="<Veeam_One_Service_Account_Password>"][VO_BUNDLE_INSTALLATION="1"] [VO_AGENT_
SERVICE_PORT="<agent_port>"]
```

IMPORTANT!

Veeam Analytics service server component must be installed on the machine that runs Veeam ONE server components.

The command has the following parameters:

Option	Parameter	Required	Description
/L	*v logfile	No	Creates an installation log file with the verbose output. Specify an existing path to the log file as the parameter value. A setup log file created during the previous installation is cleared. Example: */L*v "C:\ProgramData\Veeam\Setup\Temp\Logs\AgentSetup.txt"*
/q	n	Yes	Sets the user interface level to "no", which means no user interaction is needed during installation.
/i	setup file	Yes	Installs Veeam ONE Client Client. Specify a full path to the setup file as the parameter value. Example: */i "C:\Veeam\Monitor\VeeamONE.Agent.x64.msi"*
ACCEPT_THIRDPARTY_LICENSES	0/1	Yes	Specifies if you want to accept the terms of the license agreement for the 3rd party components. Specify 1 if you want to accept the terms and proceed with installation. Example: *ACCEPT_THIRDPARTY_LICENSES="1"*

Option	Parameter	Required	Description
ACCEPT_EULA	0/1	Yes	Specifies if you want to accept the terms of the Veeam license agreement. Specify 1 if you want to accept the terms and proceed with installation. Example: *ACCEPT_EULA="1"*
ACCEPT_LICENSING_POLICY	0/1	Yes	Specifies if you want to accept the terms of the Veeam licensing policy. Specify 1 if you want to accept the terms and proceed with installation. Example: *ACCEPT_LICENSING_POLICY="1"*
ACCEPT_REQUIRED_SOFTWARE	0/1	Yes	Specifies if you want to accept the terms of the required software license agreements. Specify 1 if you want to accept the terms and proceed with installation. Example: *ACCEPT_REQUIRED_SOFTWARE="1"*
INSTALLDIR	path	No	Installs the component to the specified location. By default, Veeam ONE uses the `Veeam ONE Agent` subfolder of the `C:\Program Files\Veeam\Veeam ONE` folder. Example: *INSTALLDIR="C:|Veeam|"* The component will be installed to the `C:\Veeam\Veeam ONE Agent` folder.
VO_AGENT_TYPE	0/1	Yes	Specifies the mode in which Veeam Analytics service will run. Specify 1 if you want to install Veeam Analytics service server. Specify 0 if you want to install Veeam Analytics service client. Example: *VO_AGENT_TYPE ="1"*
VO_AGENT_SERVICE_ACCOUNT_NAME	user	Yes	Specifies a user account under which the Veeam ONE Agent service will run. Example: *VO_AGENT_SERVICE_ACCOUNT_NAME="ONESERVER|Administrator"*

Option	Parameter	Required	Description
VO_AGENT_SERVICE_ACCOUNT_PASSWORD	password	Yes	This parameter must be used if you have specified the *VO_AGENT_SERVICE_ACCOUNT_NAME* parameter. Specifies a password for the account that will be used to run Veeam ONE Agent. Example: *VO_AGENT_SERVICE_ACCOUNT_PASSWORD="p@sswOrd"*
VO_BUNDLE_INSTALLATION	0/1	Yes	This parameter must be used if you have specified 1 for the VO_AGENT_TYPE parameter. Specify 1 to let Veeam ONE Monitor Service know about the installed Veeam ONE agent server.
VO_AGENT_SERVICE_PORT	port	No	Specifies a port that will be used by Veeam ONE to communicate with Veeam ONE Agent. By default, port number 2805 is used. Example: *VO_AGENT_SERVICE_PORT="2805"*

Example

Suppose you want to install Veeam ONE Client with the following configuration:

- Installation log location: *C:|ProgramData|Veeam|Setup|Temp|Logs|AgentSetup.txt*
- No user interaction
- Path to the MSI file: *C:|Veeam|Monitor|VeeamONE.Agent.x64.msi*
- Accept 3rd party license agreement
- Accept Veeam license agreement
- Accept required software license agreements
- Accept Veeam licensing policy
- Installation folder: default
- Agent mode: server
- Service user account: *ONESERVER|Administrator*
- Service user account password: *p@sswOrd*
- Veeam ONE Agent communication port: default

The command to install Veeam ONE Agent with such configuration will have the following parameters:

```
msiexec.exe /L*v "C:\ProgramData\Veeam\Setup\Temp\Logs\AgentSetup.txt" /qn /i "
C:\Veeam\Monitor\VeeamONE.Agent.x64.msi" ACCEPT_THIRDPARTY_LICENSES="1" ACCEPT_
EULA="1" ACCEPT_REQUIRED_SOFTWARE="1" ACCEPT_LICENSING_POLICY="1" VO_AGENT_TYPE
="1" VO_BUNDLE_INSTALLATION="1" VO_AGENT_SERVICE_ACCOUNT_NAME="ONESERVER\Admini
strator" VO_AGENT_SERVICE_ACCOUNT_PASSWORD="p@ssw0rd"
```

Upgrading to Veeam ONE 13

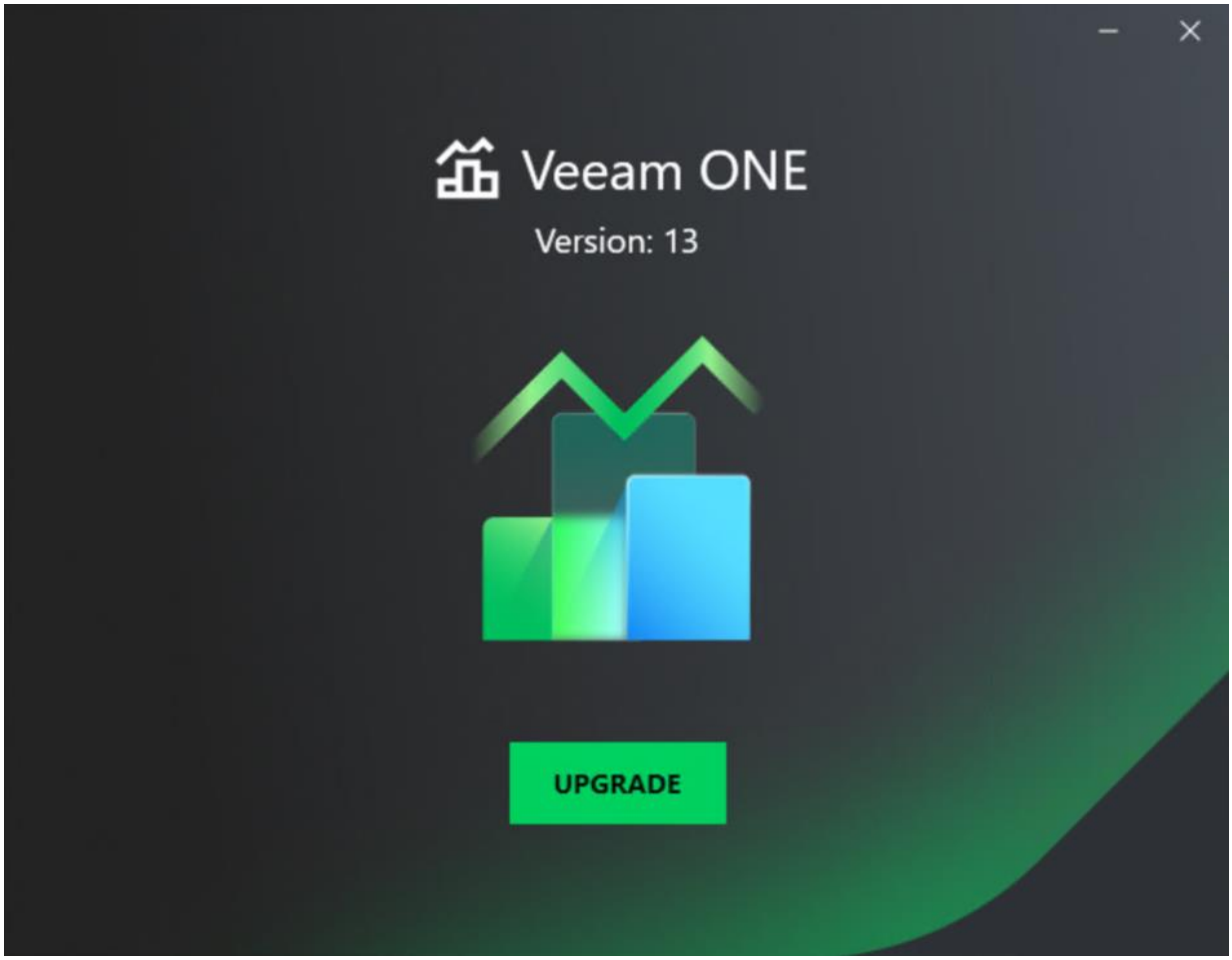
Upgrade to version 13 is supported starting from Veeam ONE version 12 (build #12.0.0.2498).

To upgrade to Veeam ONE 13, follow these steps.

Step 1. Launch Splash Window

After you mount or insert the disk with Veeam ONE installation image, Autorun will open a splash screen with installation options. On the splash window click **Upgrade**.

If Autorun is not available or disabled, run the `Setup.exe` file from the installation image or disk.



Step 2. Select Component

At the **Upgrade Veeam ONE Component** step of the wizard, select **Upgrade Veeam ONE**.

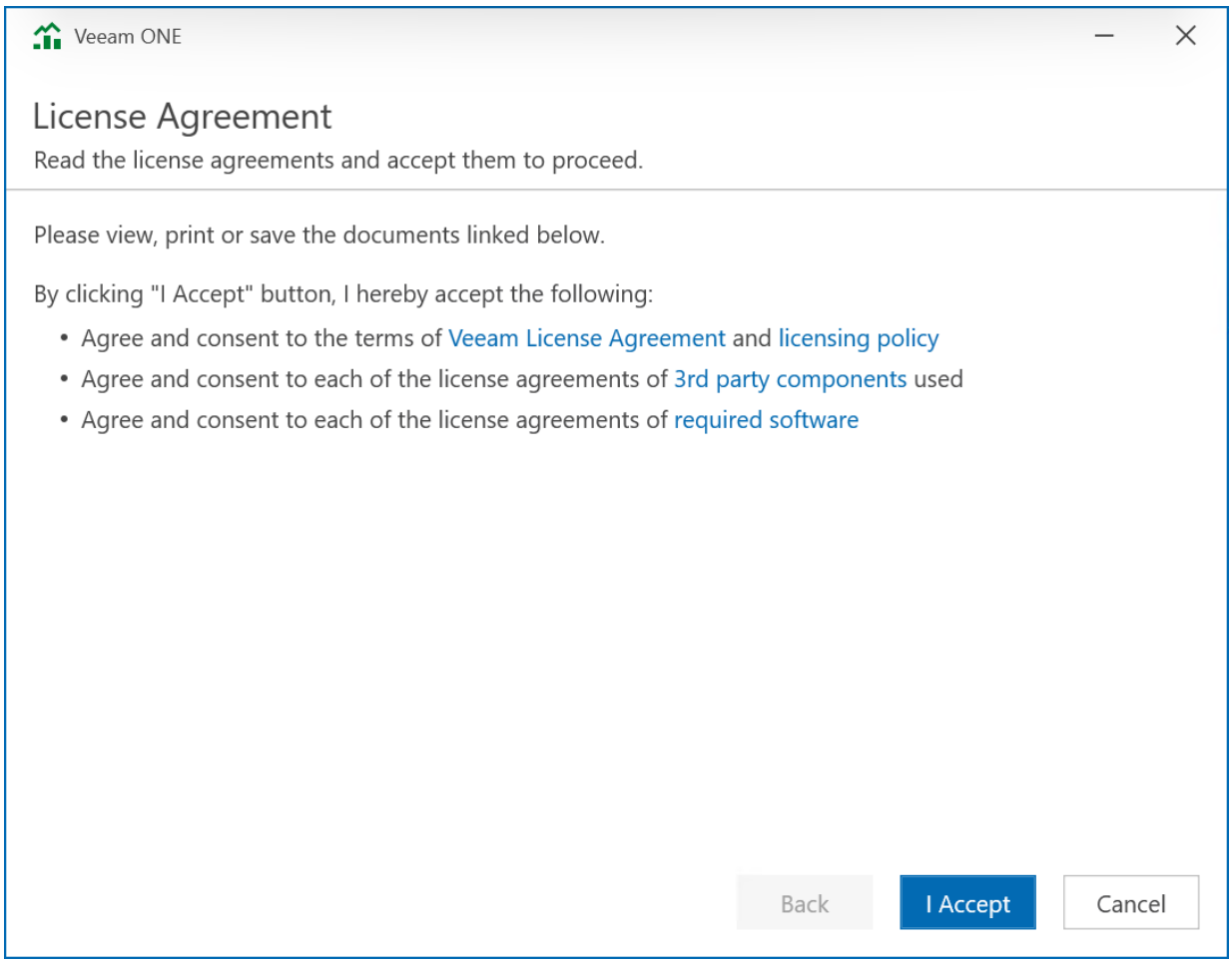
To open Veeam Help Center from the setup wizard, click **View Documentation**.



Step 3. Accept License Agreements

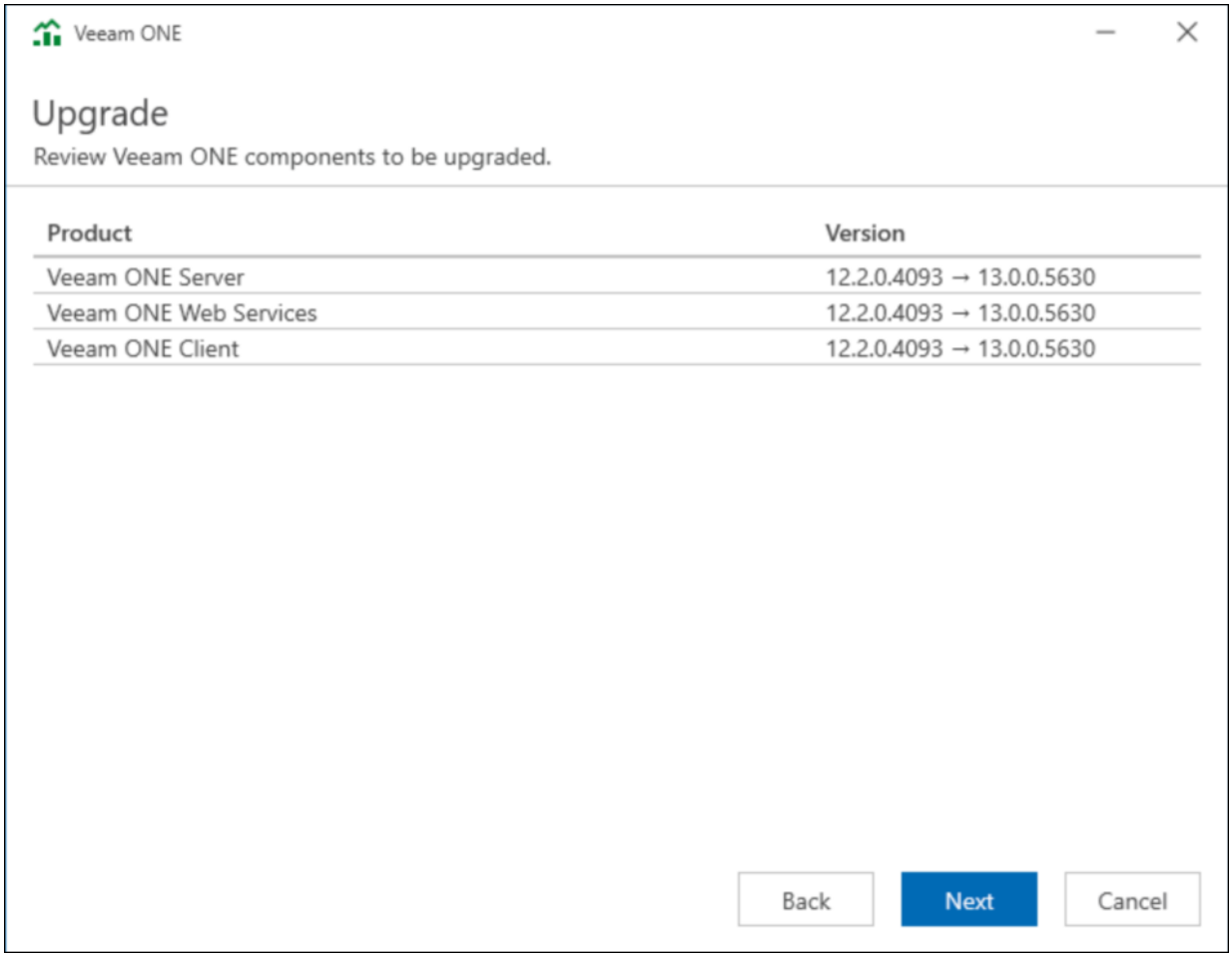
At the **License Agreements** step of the wizard, read and accept Veeam license agreement, licensing policy, 3rd party components and required software license agreements. You will not be able to continue upgrade until you accept license agreements.

To read the terms of the license agreements, click the individual links.



Step 4. Review Components to Upgrade

Veeam ONE Setup wizard will automatically detect components of the previous version installed on the machine. At the **Upgrade** step of the wizard, review the components to upgrade.

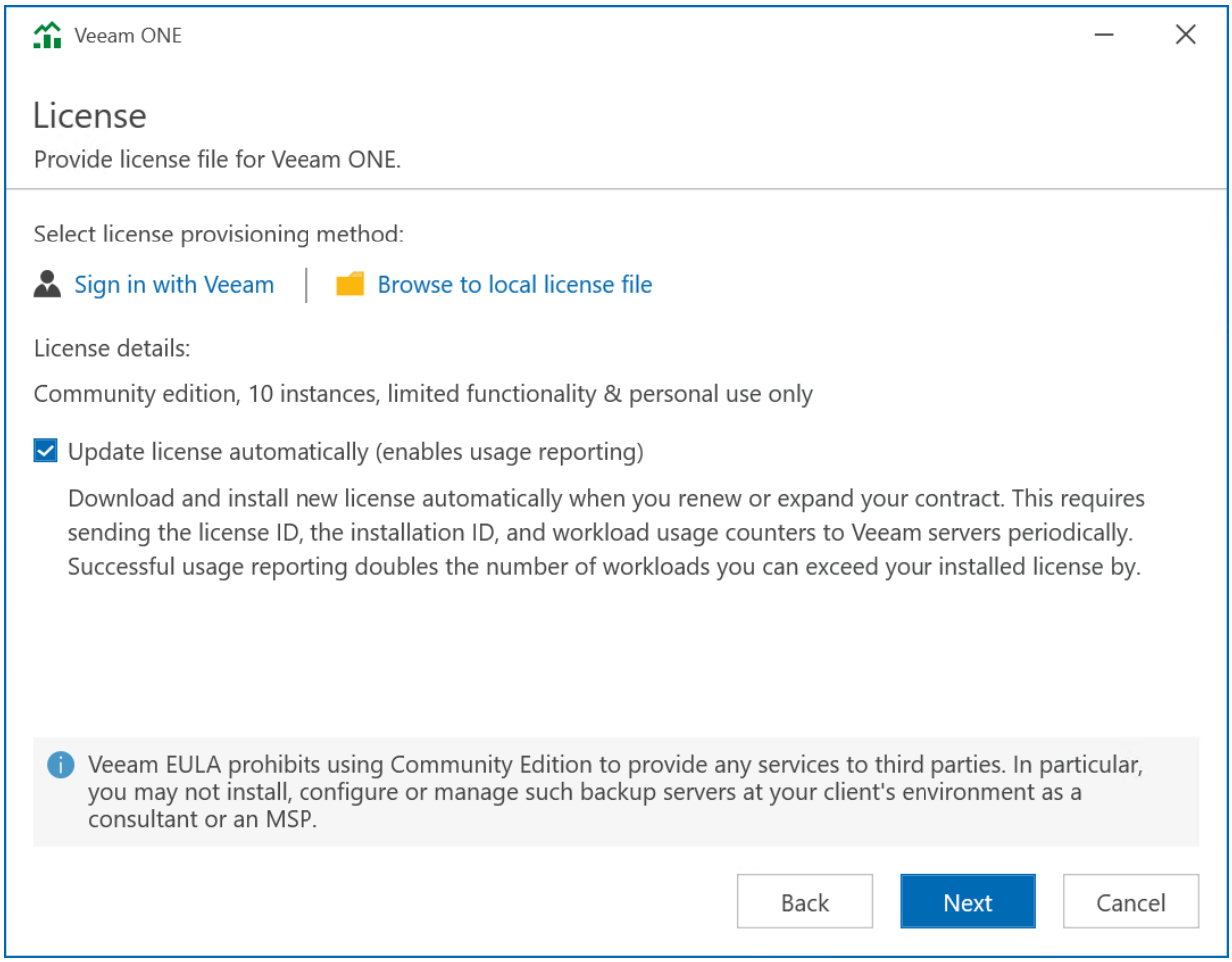


Step 5. Provide License

At the **License** step of the wizard, click one of the two options to provide a license:

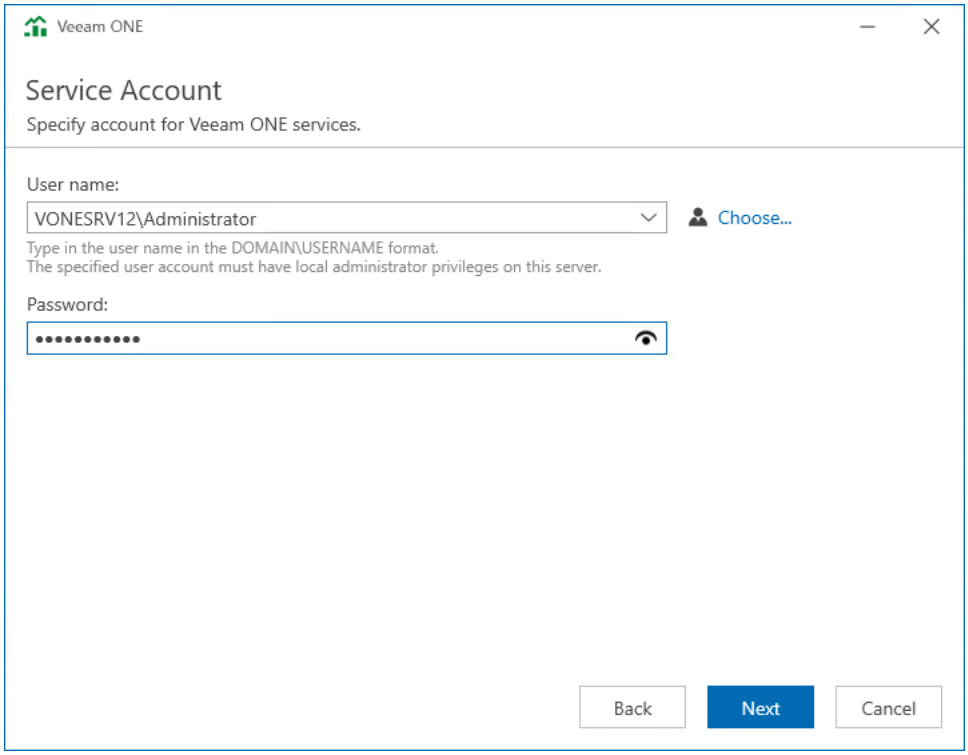
- **Sign-in with Veeam** – open the Veeam account Sign in screen to log in with your Veeam account credentials if you already have a registered license on your account.
- **Browse licence file locally** – specify the local path to the license file.

To install new licenses automatically when you renew or expand your contract, select the **Update license automatically** check box. If you enable the automatic license update, and therefore enable usage reporting, you will double the number of workloads by which you can exceed your installed license. Note that for *Evaluation* and *NFR* licenses automatic license update must be enabled.



Step 6. Specify Service Account Credentials

At the **Service Account** step of the wizard, specify the password of the account under which Veeam ONE Service runs.

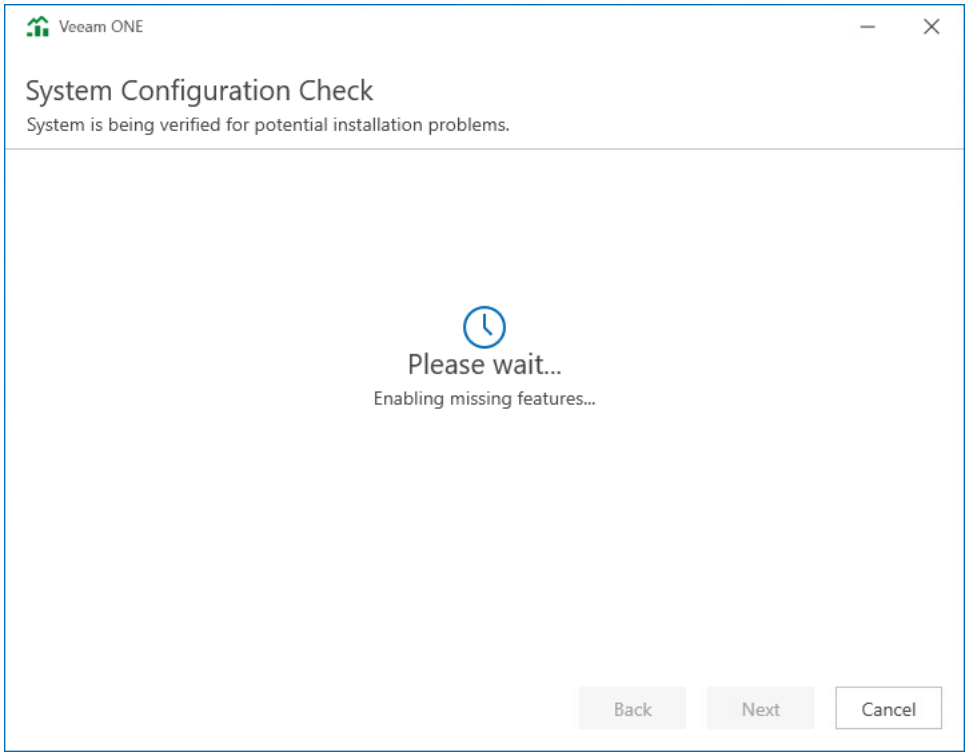


Step 7. Perform System Configuration Check

At the **System Configuration Check** step of the wizard, check what prerequisite software is missing.

Before proceeding with the upgrade, the installer will perform system configuration check to determine if all prerequisite software is available on the machine. To learn what software is required for Veeam ONE, see System Requirements.

If some of the required software components are missing, the setup wizard will enable the missing software components and features automatically.



Step 8. Choose Reporting Database

At the **Reporting Database** step of the wizard, choose a PostgreSQL Server instance that will host the Veeam ONE database.

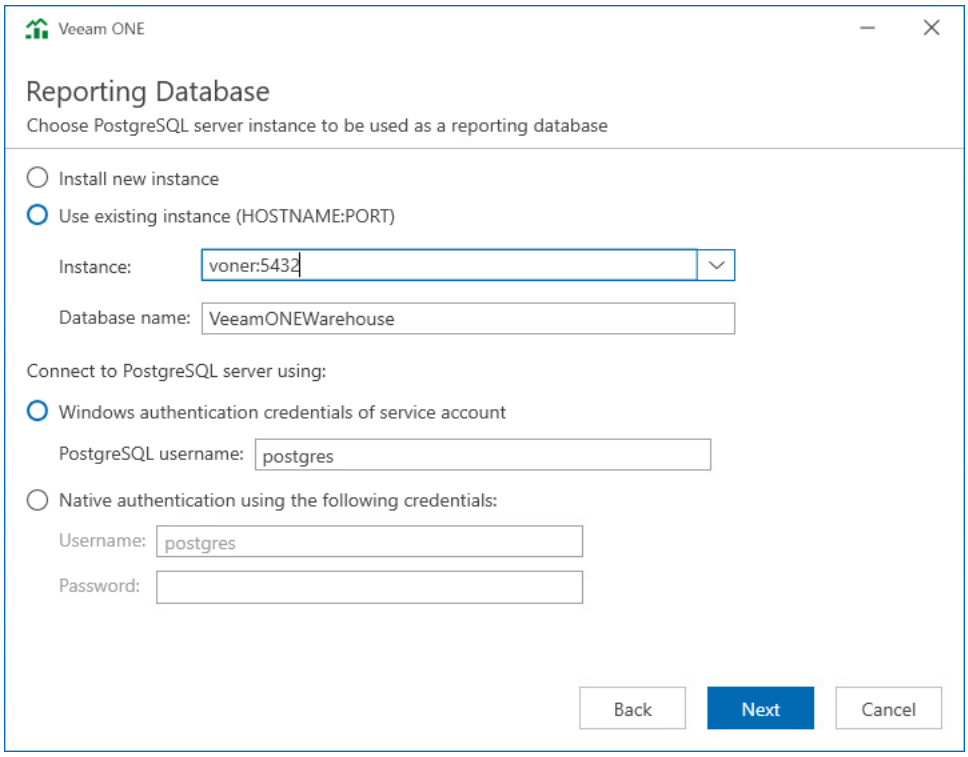
The reporting database is a dedicated database that stores PostgreSQL logs and metrics related to system activities, performance, and other relevant data for analysis and reporting purposes.

- If you do not have a PostgreSQL instance that you can use for Veeam ONE database, select the **Install new instance** option.

  If this option is selected, the setup will install PostgreSQL locally, on the computer where you are installing Veeam ONE.

- If you want to use an existing local or remote PostgreSQL instance, select the **Use existing instance** option and enter the instance and database name.

- In the **Connect to PostgreSQL server using** section, select an authentication mode to connect to the database server instance: Microsoft Windows authentication or native database server authentication. If you select the native authentication, enter credentials of the PostgreSQL database account.

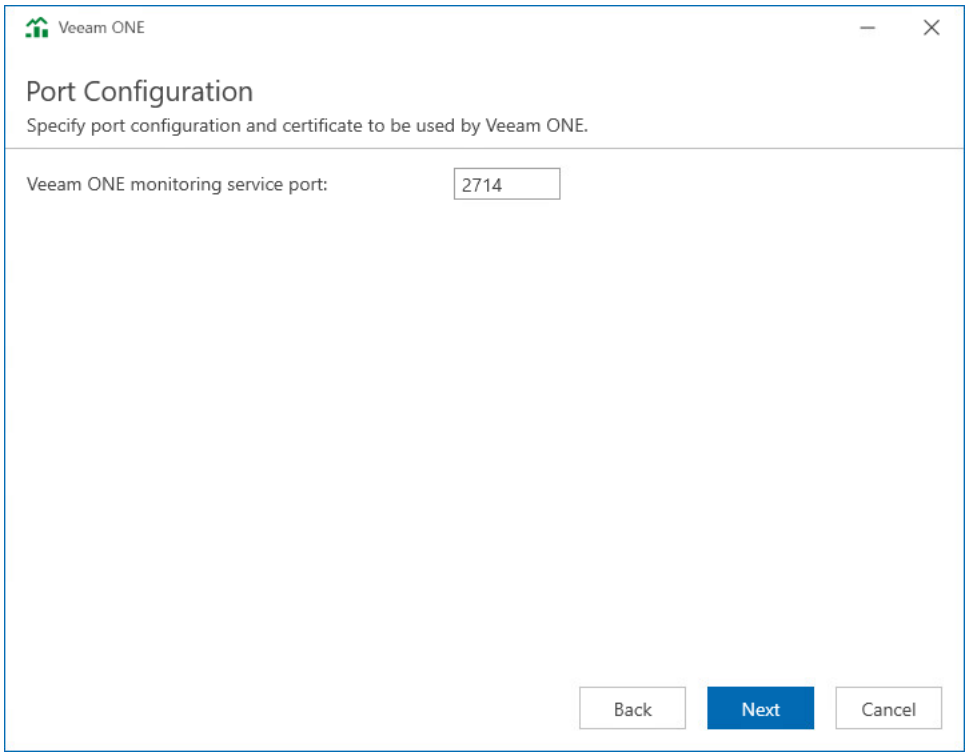


Step 9. Specify Connection Ports

At the **Port Configuration** step of the wizard, specify connection settings for Veeam ONE Monitoring Service.

In the **Veeam ONE monitoring service port** field, type a number of the port that will be used to interact with Veeam ONE Monitoring service.

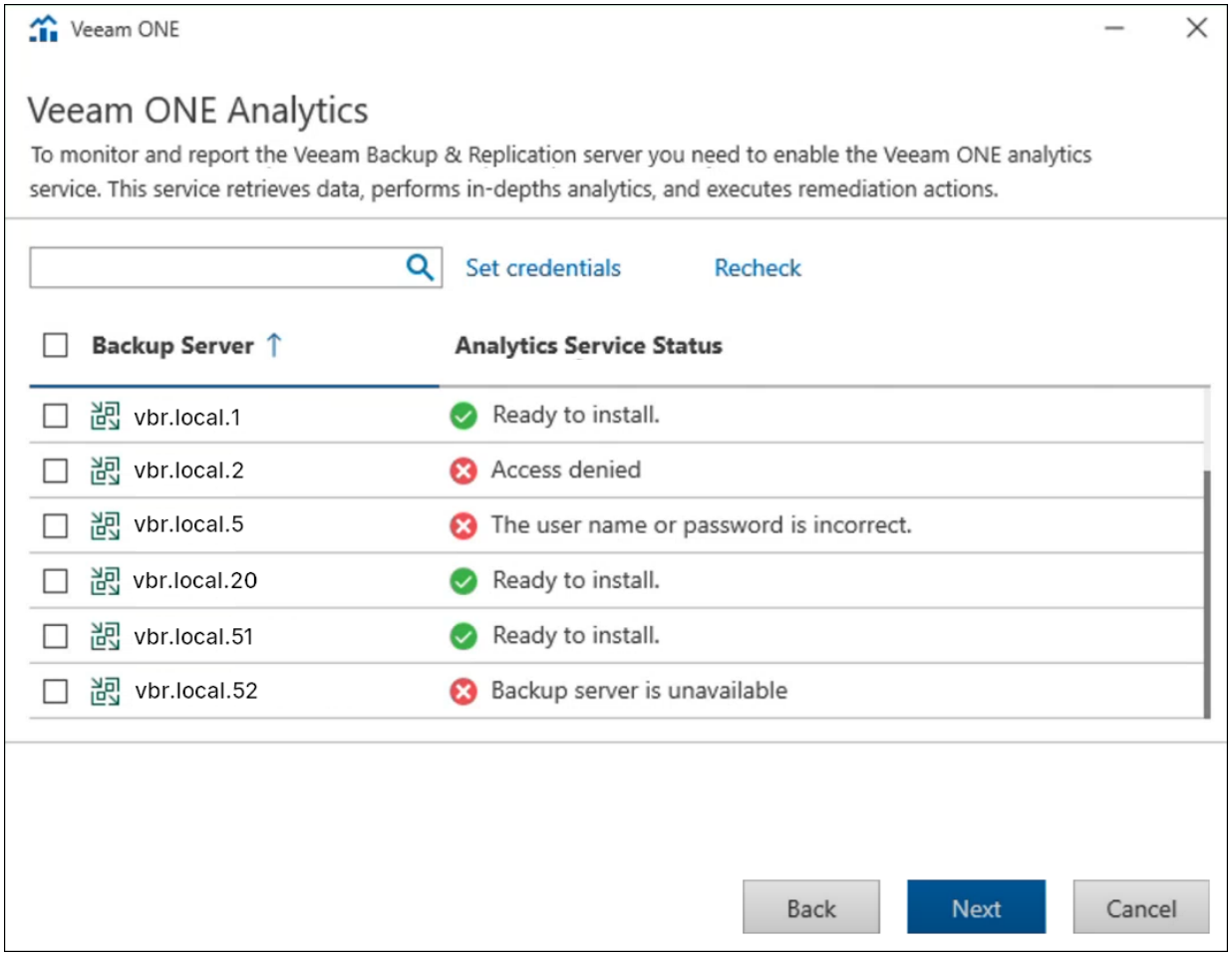
The default port number is `2714`.



Step 10. Upgrade Analytics Service Agents

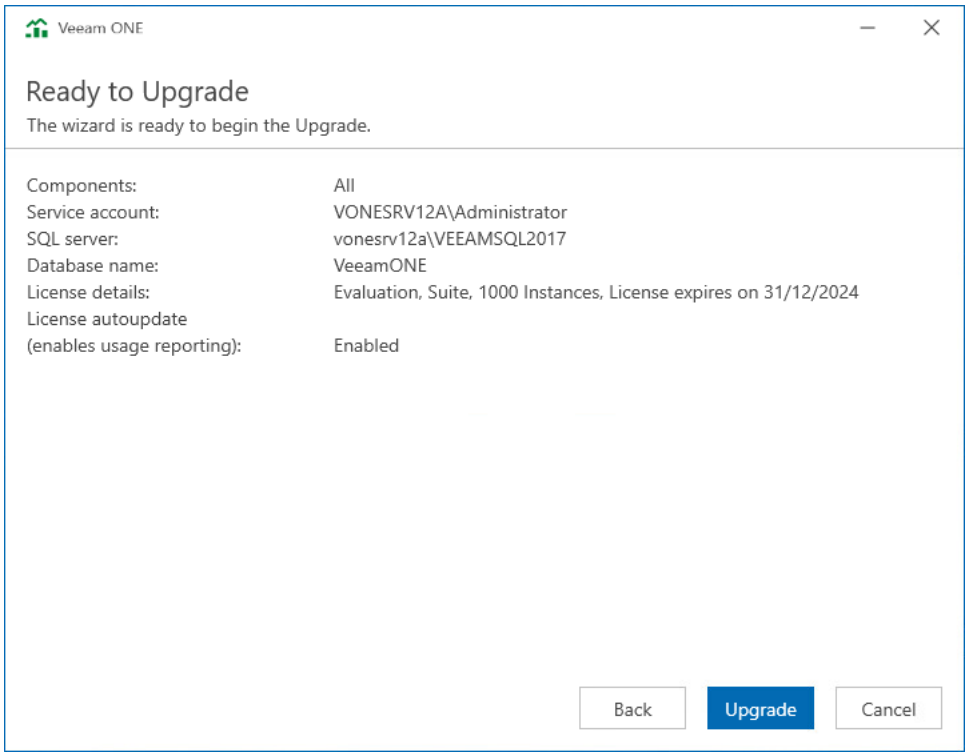
At the **Veeam ONE Analytics** step, the install wizard checks for your connected Veeam Backup & Replication servers and returns the statues of each Veeam Backup & Replication Server's Veeam Analytics service agent.

If any individual server requires credentials to access that instance, click **Set credentials**, enter the credentials and click **Recheck** to perform the server agent check again.



Step 11. Begin Upgrade

At the **Ready to Upgrade** step of the wizard, click **Upgrade** to begin the upgrade process.



If you installed Veeam ONE using the custom installation, repeat this upgrade procedure on every machine where the Veeam ONE components are installed.

Depending on the size of the Veeam ONE database, the upgrade procedure may take up to several hours.

Step 12. Change Default Certificate

Veeam ONE uses TLS to ensure secure data communication between Veeam ONE Web Client and a web browser. That is, the Veeam ONE Web Client is available over HTTPS.

During upgrade, Veeam ONE generates a self-signed certificate that is used to secure traffic. You can replace this default certificate with your own self-signed certificate or a certificate that was obtained from a Certificate Authority. This step is optional, and is not required if you want to keep the default certificate generated during the upgrade procedure.

For details on Veeam ONE certificates, see Veeam ONE Certificates.

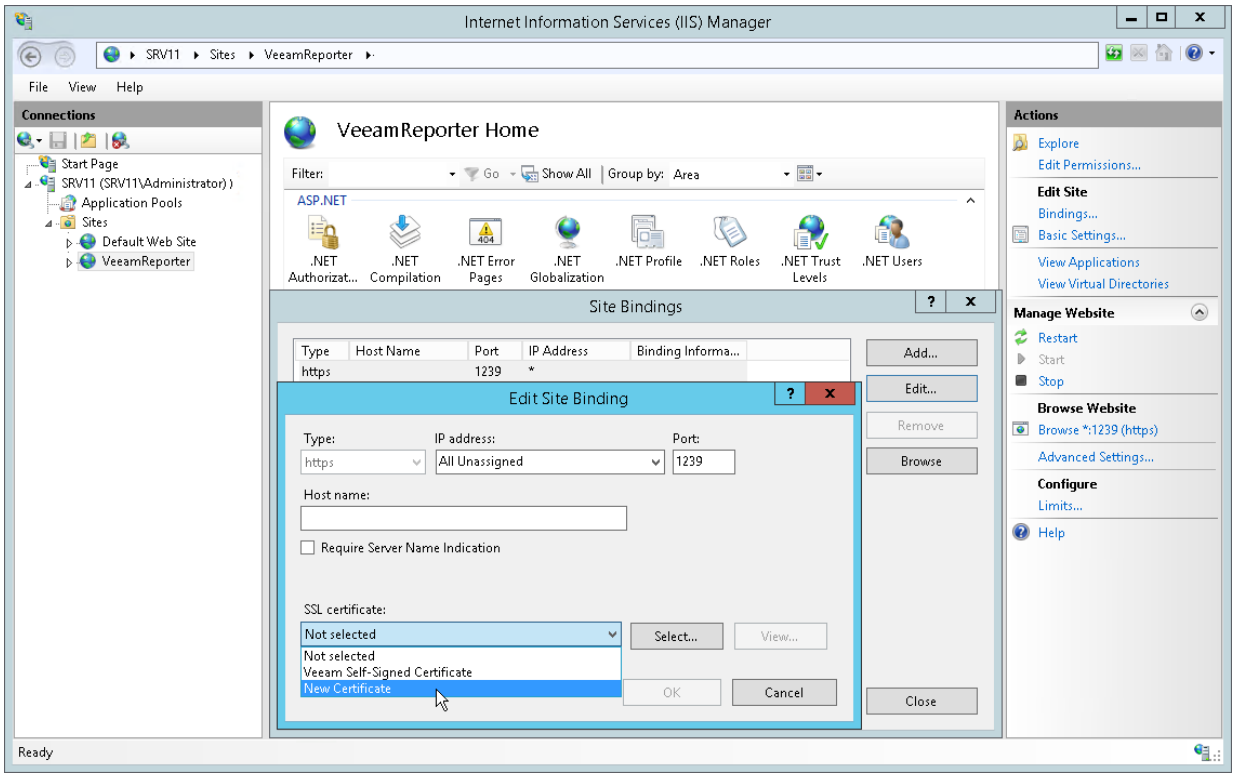
> **NOTE:**
>
> If you replace the default certificate with another self-signed certificate, you must configure a trusted connection between the Veeam ONE Web Client and a web browser later. For details, see Configuring Trusted Connection.

Assigning Certificate to the Veeam ONE Web Client Website

To assign a new certificate to the Veeam ONE Web Client:

1. Log on to the machine where the Veeam ONE Web Service component is installed.
2. Open the Internet Information Services (IIS) Manager, expand the *localhost* node and navigate to **Sites**.
3. In the **Connections** pane, select *VeeamReporter*.
4. In the **Actions** > **Edit Site** pane on the right, click **Bindings**.
5. In the **Site Bindings** window, select the existing binding and click **Edit**.
6. From the **SSL certificate** list, select the necessary certificate and click **OK**.

7. In the **Site Bindings** window, click **Close**.



Step 13. Specify Guest OS Credentials for Microsoft Hyper-V VMs

After you upgrade to Veeam ONE 13, you must specify credentials of an account that will be used to collect data from Windows guest OSes on Microsoft Hyper-V VMs. If you do not specify guest OS credentials, Veeam ONE will not display guest OS data (in particular, data about guest disks) in monitoring dashboards, alarms and reports.

For details, see Step 6. Specify VM Guest OS Credentials.

Step 14 Apply Available Updates

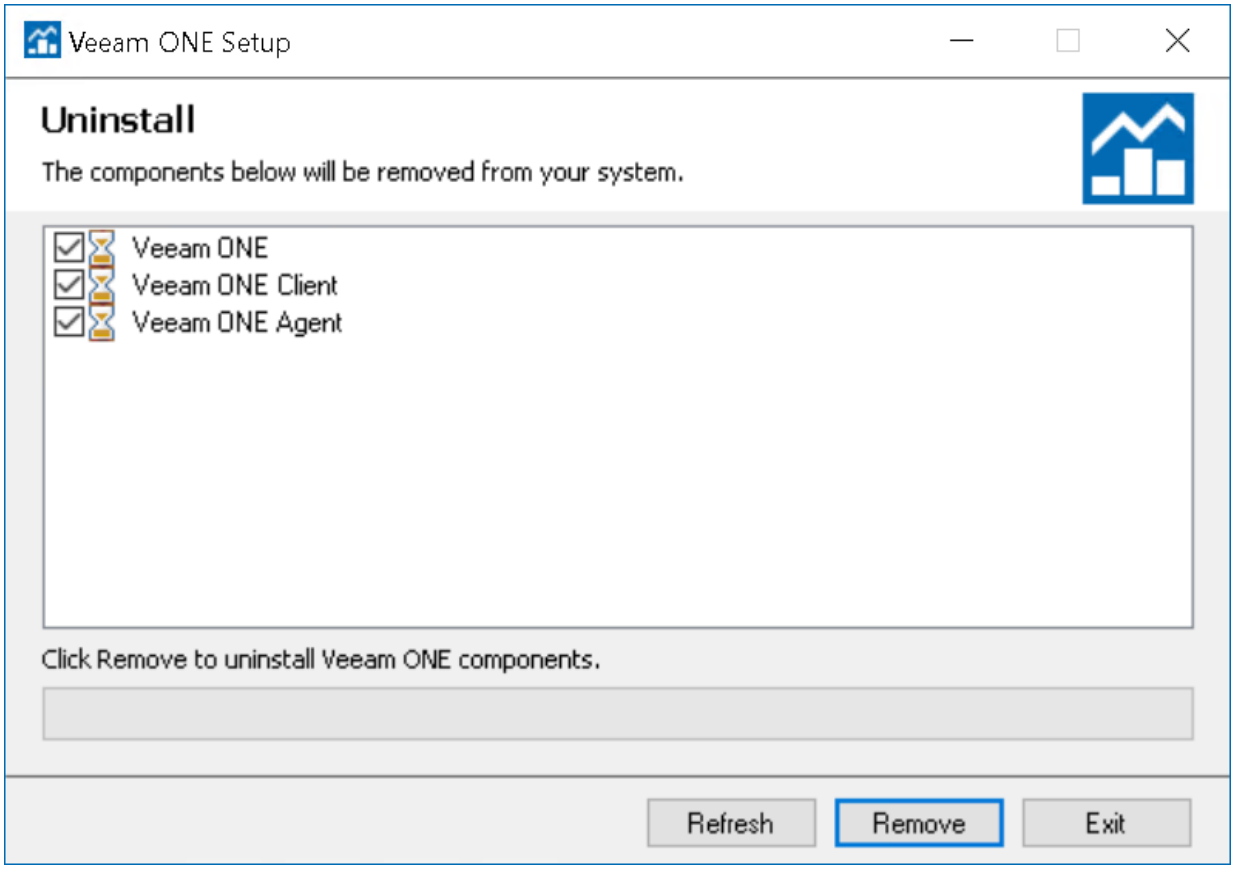
We recommend that you periodically check for Veeam ONE updates and install them as available. You can download product updates at Latest Updates.

Upgrading Veeam ONE Client

If you have additionally installed several standalone instances of Veeam ONE Client, you must upgrade them as well. The upgrade procedure is identical to Veeam ONE Client installation. For details, see Installing Veeam ONE Client.

Uninstalling Veeam ONE

To uninstall Veeam ONE, open the **Start** menu, go to **Control Panel** > **Uninstall a program**, choose Veeam ONE components you want to uninstall and click **Remove**.



If you installed Veeam ONE using the custom installation, repeat this procedure on every machine where the Veeam ONE components are installed.

The SQL Server instance installed and used by Veeam ONE is not removed during the uninstall of Veeam ONE. It needs to be removed separately using the standard **Add or Remove Programs** feature in **Control Panel**. Veeam ONE database and its data is retained until you manually remove the database or uninstall the SQL Server instance.

Getting Started with Veeam ONE

Veeam ONE Client and Veeam ONE Web Client user interfaces are designed to let you quickly locate the required commands, facilitate monitoring of your infrastructure and speed up the investigation and troubleshooting process. You can also access REST API to query information about Veeam ONE entities and perform basic operations with these entities using HTTP requests and standard HTTP methods. This section describes the basic elements and features of the Veeam ONE Client and Veeam ONE Web Client user interface.

Accessing Veeam ONE Components

You can interact with Veeam ONE using Veeam ONE Client, Veeam ONE Web Client and REST API:

Veeam ONE Client

To access Veeam ONE Client:

1. Log on to the machine where Veeam ONE Client is installed.
2. From the **Microsoft Windows Start** menu, choose **Veeam ONE Client**.
3. In the authentication window, specify the FQDN or IP address of a server where the Veeam ONE Server component runs and enter the credentials of the account used to connect to Veeam ONE Client. To connect using credentials of the account under which you are logged on to the machine, select the **Log in as current user** check box.

   The user account must either:

   - Be a member of the *Veeam ONE Administrators* or *Veeam ONE Read-Only Users* group. For details on user groups, see Security Groups.

     Members of the *Power User* group can also access the Veeam ONE Client, but receive only the *Read-Only* role.

   - Have permissions assigned to objects in the vCenter Server or VMware Cloud Director inventory hierarchy. For details on assigning permissions to objects, see Multi-Tenant Monitoring and Reporting.

     This prerequisite applies to the VMware vSphere platform only.
4. Click **Connect**.
5. If Veeam ONE is configured to display a consent banner, read the banner content and click **I Agree**.

   For details on configuring consent banner, see Banners.

To create a shortcut for the connection, click **Save Shortcut**. You can create one shortcut for every Veeam ONE server. The server name will be saved after the first successful login.

> **NOTE**
>
> If you want to save credentials for a connection in a shortcut, you must agree to save these credentials in the Windows Credentials Manager.

Other Ways to Access Veeam ONE Client

To gain a faster access to Veeam ONE Client, you can launch it without providing user credentials in the authentication window.

- To launch Veeam ONE Client under the account of a user that is currently logged to the machine, in the command shell call the `Monitor.exe` file that resides in the installation directory and pass the `/currentuser` parameter. For example:

  ```
  "C:\Program Files\Veeam\Veeam ONE\Veeam ONE Monitor Client\Monitor.exe"
  /currentuser
  ```

- To launch Veeam ONE Client with explicit user credentials, in the command shell call the `Monitor.exe` file that resides in the installation directory and pass the `/username` and `/password` parameters. For example:

  ```
  "C:\Program Files\Veeam\Veeam ONE\Veeam ONE Monitor Client\Monitor.exe"
  /username tech\john.smith /password PaSSw0rd
  ```

You can save this set of commands as a Windows shortcut and use it to quickly access Veeam ONE Client.

Veeam ONE Web Client

To access Veeam ONE Web Client:

1. Open the Veeam ONE Web Client website using one of the following options:
   - Access Veeam ONE Web Client from the Veeam ONE Client. To do this, in the main menu, click **Reports**.
   - Access Veeam ONE Web Client locally, on the machine where the Veeam ONE Web UI component is installed. To do this choose **Veeam ONE Web Client** in the Microsoft Windows Programs menu.
   - Access Veeam ONE Web Client remotely using your web browser. To do this, browse to the URL of the Veeam ONE Web Client website. This website runs on the machine where the Veeam ONE Web UI component is installed. The URL must look similar to the following one (assuming you use the default website port `1239`):

     ```
     https://webserver.domain.tld:1239
     ```

     Note that Veeam ONE Web Client is available over HTTPS.
2. If Veeam ONE is configured to display a consent banner, read the banner content and click **I Agree**.
3. Type credentials of a user account under which you want to connect to Veeam ONE Web Client.

   The user account must either:

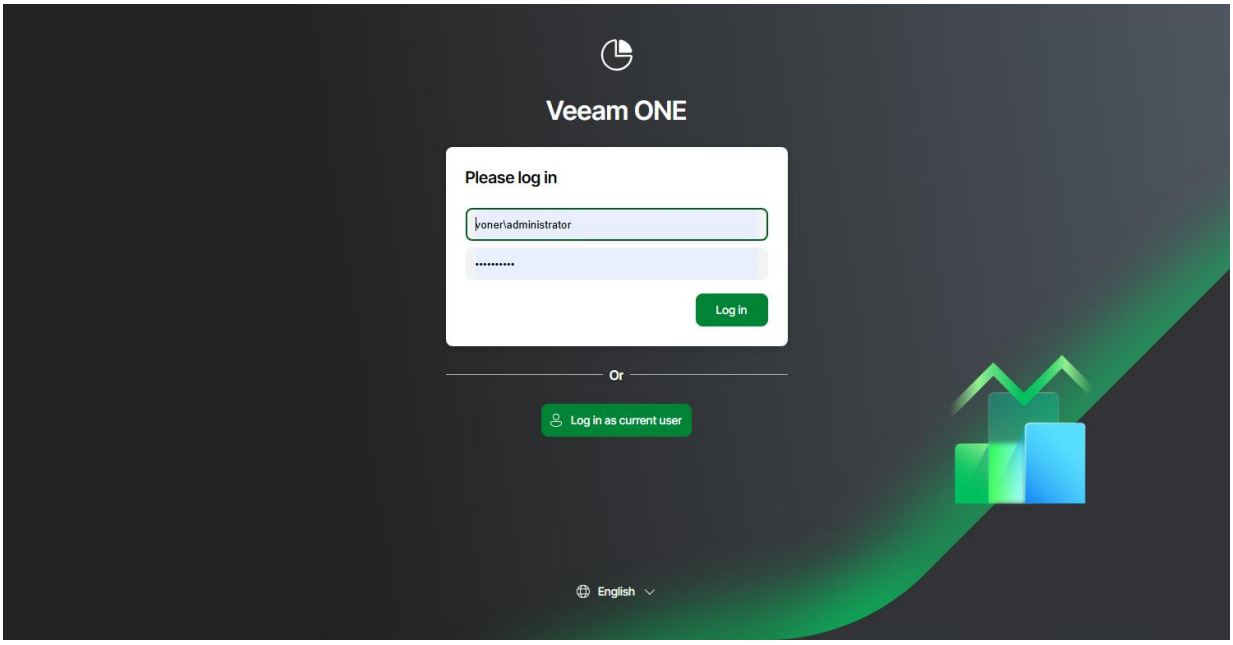
   - Be a member of the *Veeam ONE Administrators*, *Veeam ONE Power Users* or *Veeam ONE Read-Only Users* group. For details on user groups, see Security Groups.
   - Have permissions assigned on objects in the vCenter Server or VMware Cloud Director inventory hierarchy. For details on, see Multi-Tenant Monitoring and Reporting.

     This prerequisite applies to the VMware vSphere and VMware Cloud Director platforms.

   To connect using credentials of a Microsoft Windows user account under which you are logged on to the machine, click **Log in as current user**.

   If multi-factor authentication (MFA) is enabled through certificate authentication, select **Log in with your certificate**. For details on, see Veeam ONE Web Settings.

4. Click **Log In**.



5. In the displayed **Welcome** pop-up window, click **Start** to view all updates.

   If you do not want to view updates, click **Skip**.

   If you do not want Veeam ONE Web Client to display the **Welcome** window, select the **Don't show again** check box.

> **NOTE:**
>
> If you log in for the first time, make sure that pop-up windows are allowed for the Veeam ONE Web Client website.

If you used a self-signed certificate and try to access Veeam ONE Web Client from a remote machine, the browser will display a warning notifying that the connection is untrusted (although it is secured with TLS).

Veeam ONE REST API

To access Veeam ONE REST API Swagger UI see section Evaluation with Swagger UI of the REST API Reference guide.

Navigating Veeam ONE Web Client

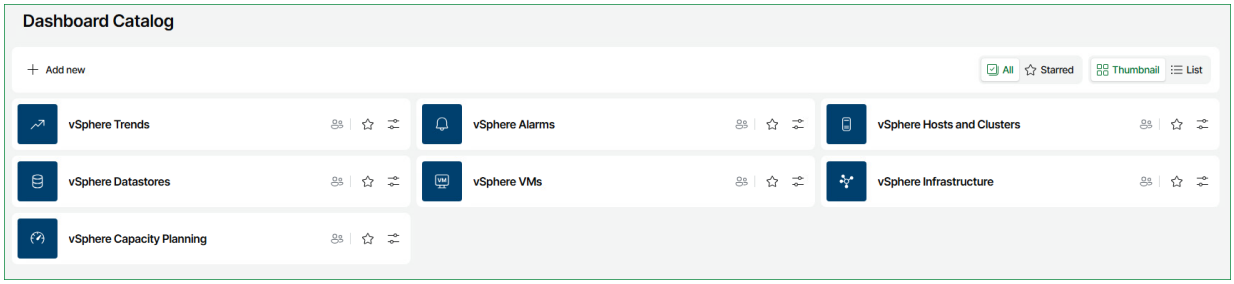
Veeam ONE Web Client interface includes the following elements:

- Threat Center
- Dashboards
- Jobs Calendar
- Report Catalog
- Saved Reports
- Alarms Overview
- Scheduling (Reports and Dashboards)
- Deployment Projects
- Global Search
- Veeam Intelligence
- Language
- Downloads
- Notification bell
- Configuration

Dashboards

In the **Dashboard Catalog** section, you can work with predefined and custom dashboards. Veeam ONE dashboards provide at-a-glance view on the state of the Veeam Backup & Replication infrastructure and virtual environment, and present information on the health state, performance, configuration and other aspects of the managed environment.

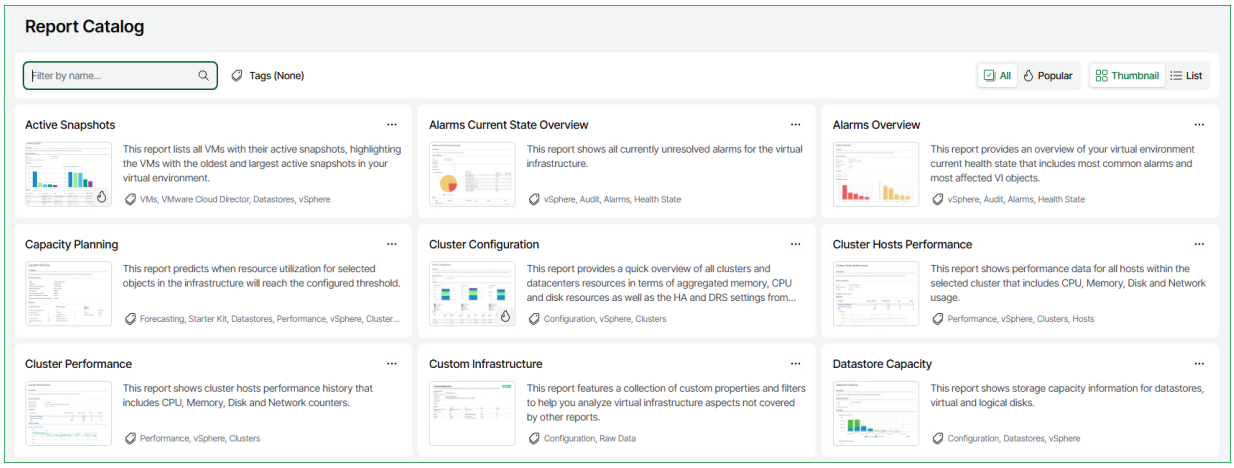
For details, see Dashboards.



Report Catalog

In the **Report Catalog** section, you can work with predefined and custom reports. Reports provide an insight into performance, health state, configuration and efficiency aspects of the Veeam Backup & Replication infrastructure and virtual environment.

For details, see Reports.



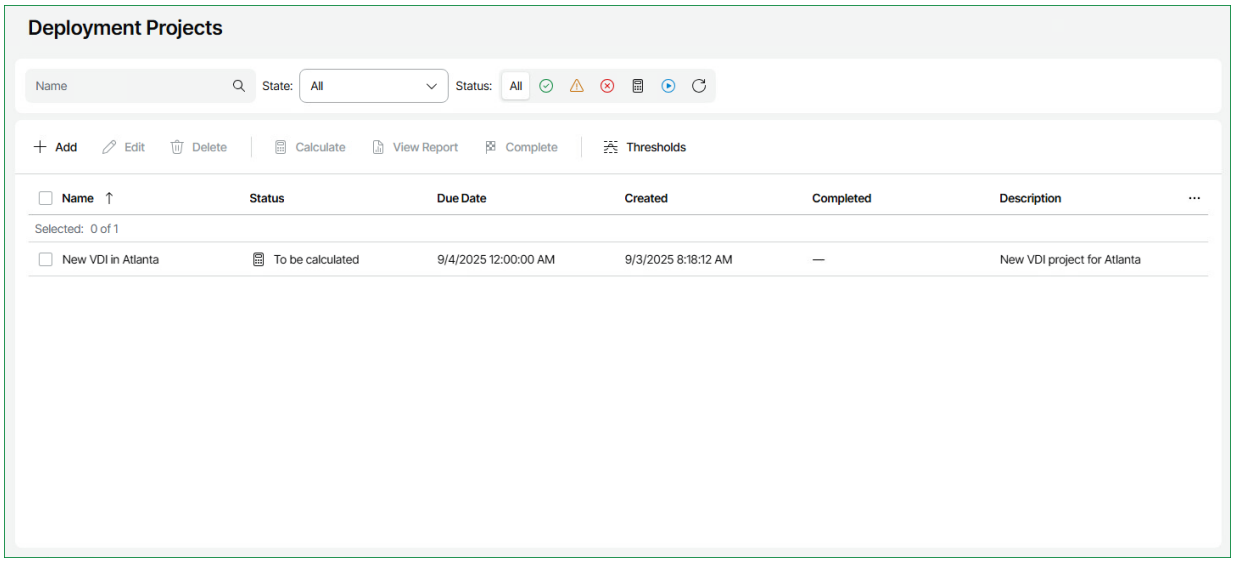
Saved Reports

In the **Saved Reports** section, you can work with your configured report projects. Saved reports allow you to track future resource utilization and monitor trends and issues in the virtual environment.

Deployment Projects

In the **Deployments Projects** section, you can work with deployment projects. Deployment projects allow you to predict future resource utilization and plan resource reservations in the virtual environment.

For details, see Deployment Projects.



Language

The language button allows you to select the display language for Veeam ONE Web Client (English, Japanese).

Downloads

The Downloads button displays all recent report downloads over the last 24 hours.

For details, see Reports.

Notifications

Veeam ONE Web Client generates notifications about important internal events such as data collection failure, Veeam ONE license expiration and so on.

To view the notifications, at the top right corner, click the button with the bell icon. The drop-down list of notifications will open.

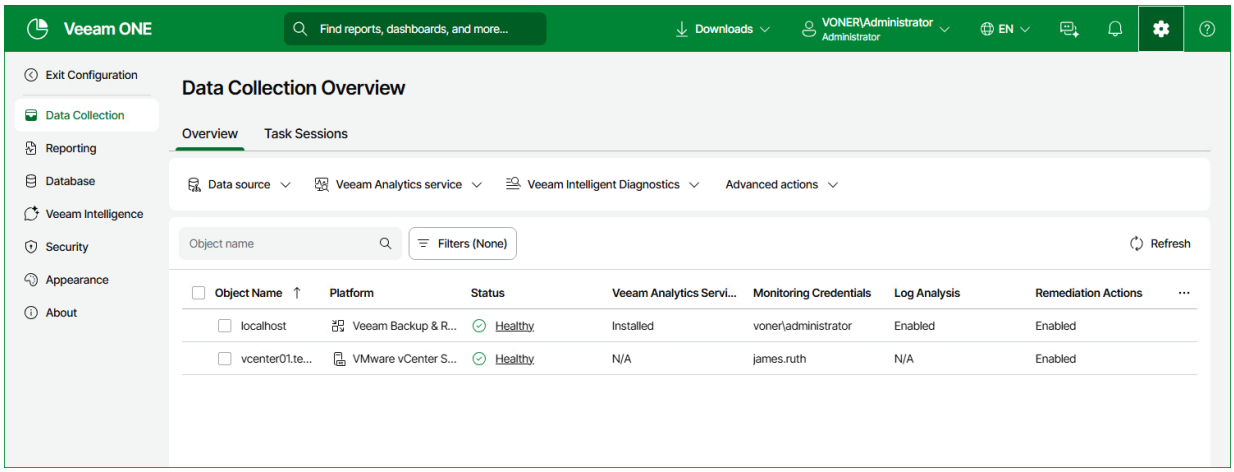
To clear the list of notifications, click **Clear All**.

By default, new notifications are displayed automatically. To disable this, turn off the **Auto-display new message** toggle to the left. When a new notification is generated, the number on the notification button increases.

Configuration

In the **Configuration** section, you can configure Veeam ONE Web Client settings and perform administrative tasks, such as scheduling data collection for reports and dashboards.

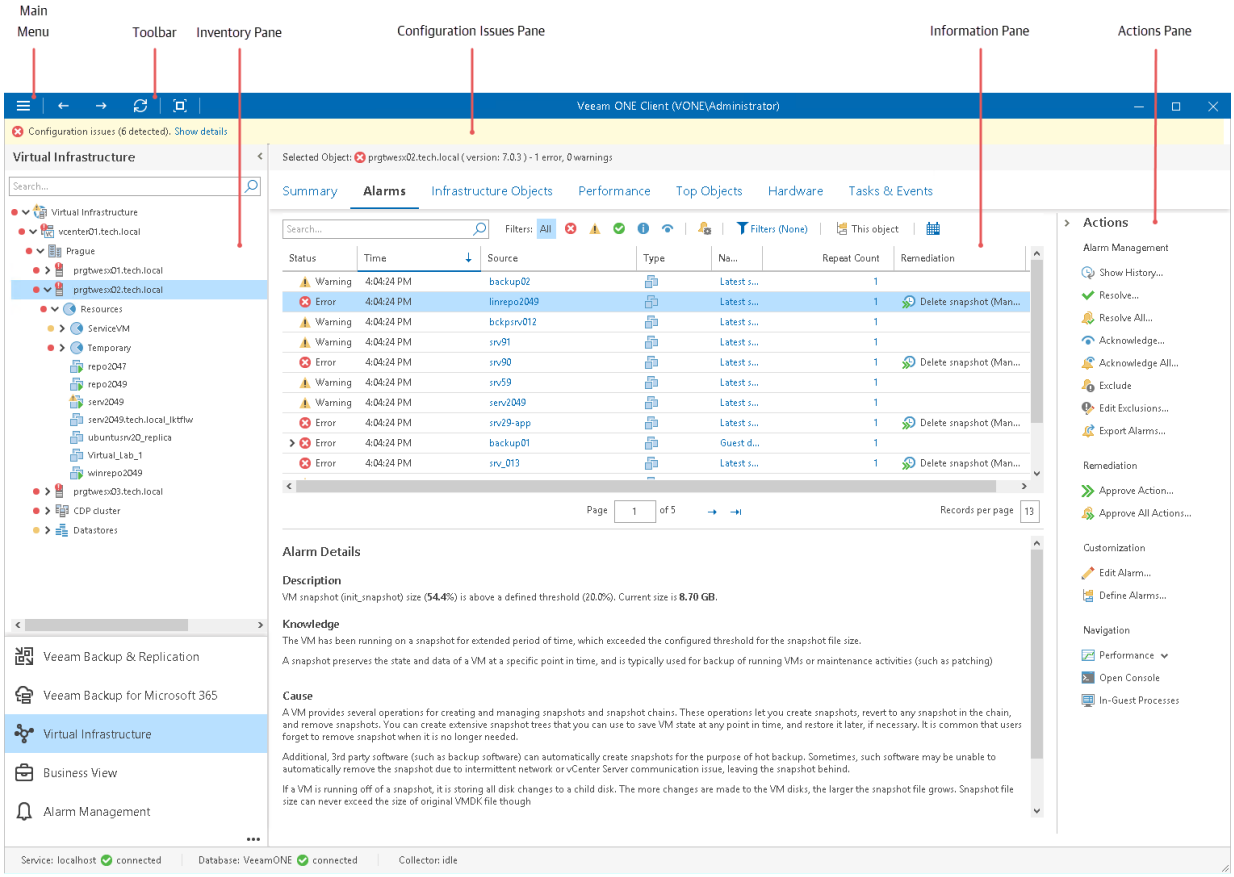
For details, see Configuring Veeam ONE.



Navigating Veeam ONE Client

Veeam ONE Client interface includes the following elements:

- Toolbar and Main Menu
- Inventory Pane
- Configuration Issues Pane
- Information Pane
- Actions Pane



Toolbar and Main Menu

Toolbar

Veeam ONE Client toolbar provides access to frequently used commands.

- **Back/Forward** — navigate to the previous/next visited view in the Veeam ONE Client.
- **Refresh** — retrieve the latest collected data from the Veeam ONE Monitoring Service to show up-to-date information in the Veeam ONE Client. To perform this command, you can also press `[F5]` on the keyboard.
- **Full Screen** — switch to the full screen mode. To perform this command, you can also press `[F11]` on the keyboard.
- **Get Full Version** (present in Community Edition Mode or if the current license is outdated) — access the webpage where you can download Veeam free trial that allows you to use Veeam ONE with no functionality restrictions for a limited period of time.



Main Menu

Veeam ONE Client main menu provides access to the following commands and features:

- **Add Server** — connect a new virtualization server, VMware Cloud Director, or Veeam Backup & Replication server. To perform this command, you can also press `[CTRL+I]` on the keyboard.

  For details on connecting servers, see Add Data Source.
- **Notifications** — open the **Notification Settings** wizard.

  For details on configuring notifications, see Configuring Notification Settings.
- **Reports** — create a report for an infrastructure object selected in the inventory pane.

  For details on creating reports, see View Reports.
- **Alarm Modeling** — forecast the number of alarms that will be triggered for an infrastructure object selected in the inventory pane.

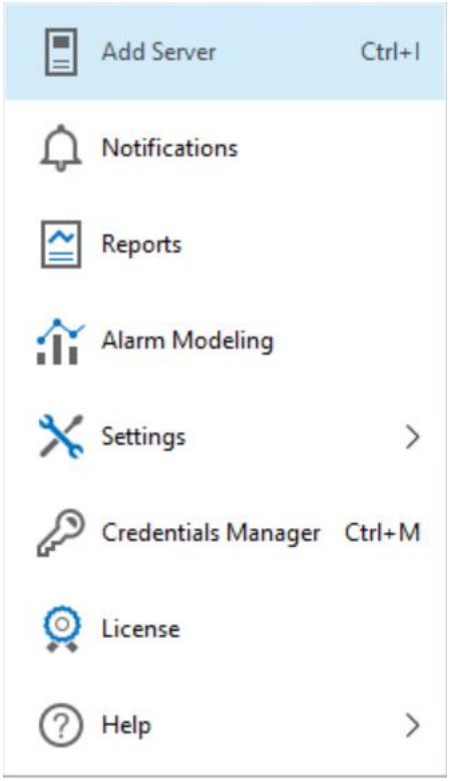
  For details on alarm modeling, see Modeling Alarm Number.
- **Settings** — view or change Veeam ONE client and server settings.

  For details on customizing settings, see Configuring Veeam ONE.
- **Credentials Manager** — view and manage credentials records.

  For details on working with credentials, see Credentials Manager.
- **License** — view license information, change and update the license file, and send license usage reports.

  For details on Veeam ONE licensing, see Licensing Veeam ONE.

- **Help** — open Veeam ONE Client help, export log files and check the current version of Veeam ONE Client. To open help topics, you can also press `[F1]` on the keyboard.



Inventory Pane

The inventory pane on the left shows a hierarchical list of infrastructure objects. The buttons at the bottom of the inventory pane allow you to switch between Veeam ONE Client views.

Each node in the hierarchy tree reflects the state of a corresponding infrastructure object. If there exist unresolved alarms for the object, Veeam ONE Client displays on the node an icon of an alarm with the highest severity.

Veeam ONE reflects the state of child objects on parent nodes to let you easily find problematic objects. For example, if an error alarm was triggered for a host, the error icon displays on the host node. In addition, a red downward error is shown on the parent cluster node and on the parent management server node to indicate that an error has occurred on the child host. If necessary, you can change Veeam ONE Client settings to display icons next to affected objects only.

- To search for a Veeam Backup & Replication, Veeam Backup for Microsoft 365, virtual infrastructure, VMware Cloud Director or Business View infrastructure component, use the search field at the top of the inventory tree.

  Search results depend on the selected view.

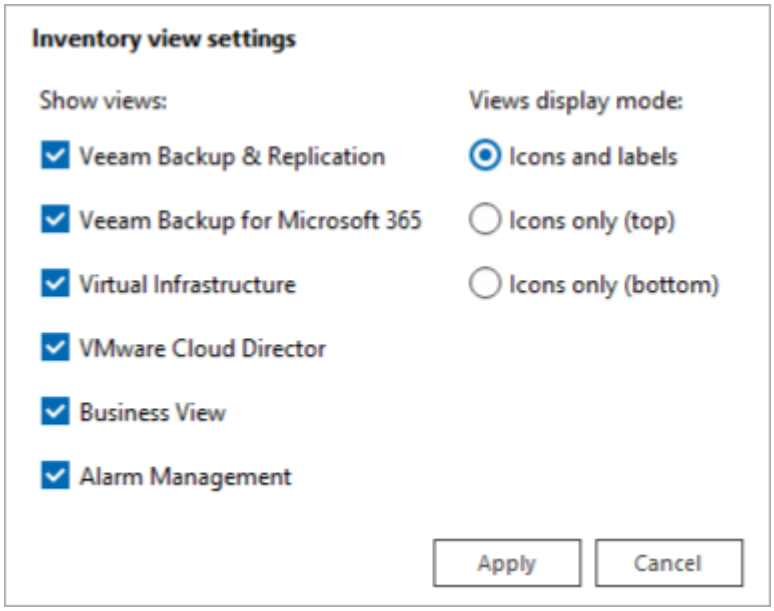
- To expand/collapse all tree nodes, right-click the root node in the inventory pane and choose **Expand all/Collapse all** from the shortcut menu.

- To show all objects with errors and warnings in the hierarchy, right-click the root node in the inventory pane and choose **Show all error objects** from the shortcut menu.

  Veeam ONE Client expands all nodes that have child objects with registered errors or warnings.

- To hide and show the inventory pane, use the collapse/expand arrow at the top right corner of the inventory pane.

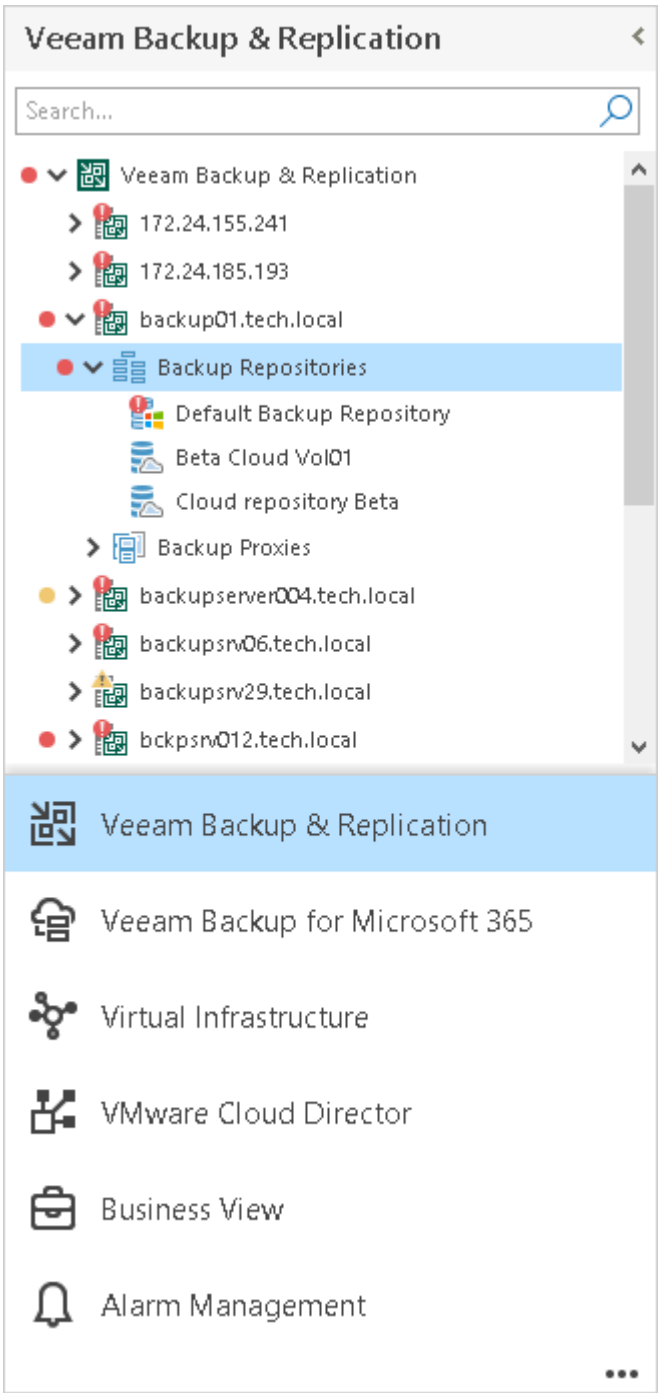
- To change the inventory view display settings, click the ellipsis at the bottom right corner of the inventory pane and select the necessary options.



For details on changing display settings, see Other Settings.

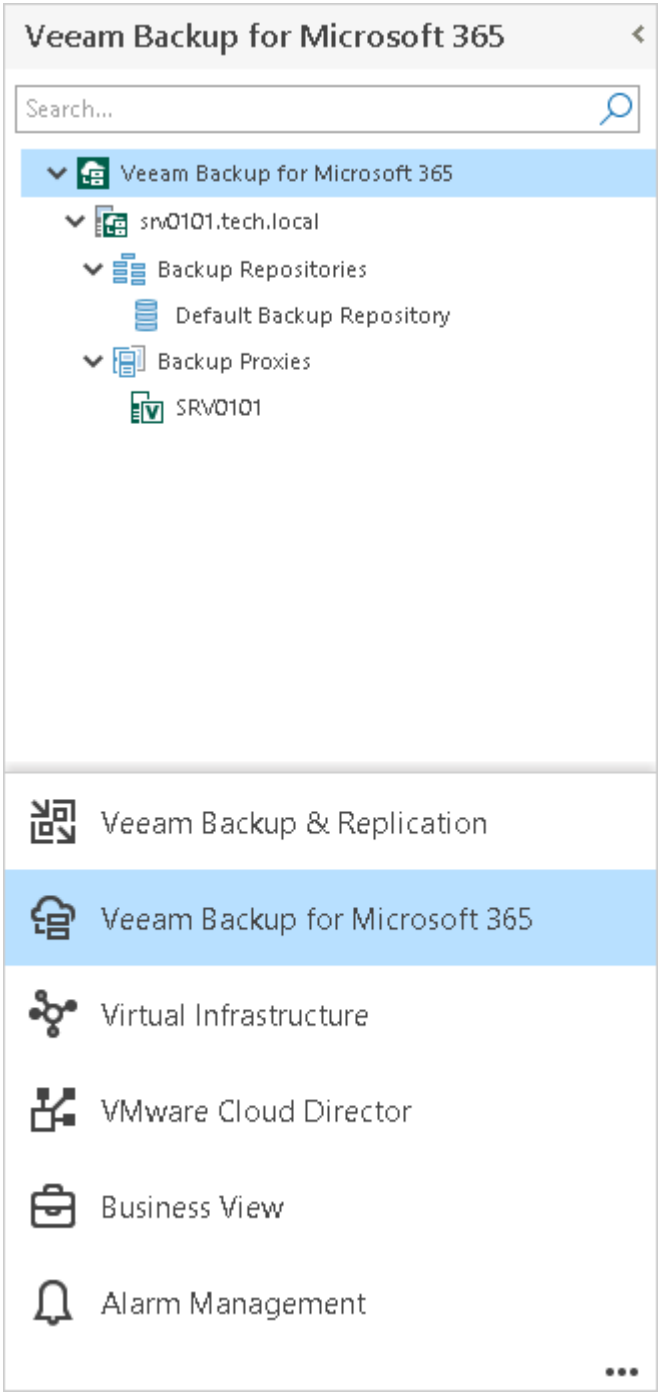
Veeam Backup & Replication

The **Veeam Backup & Replication** tree displays a hierarchical list of connected Veeam Backup Enterprise Manager servers, Veeam Backup & Replication servers, and components of the backup infrastructure — backup proxies, backup repositories, WAN Accelerators, tape servers, cloud repositories, and cloud gateways.



Veeam Backup for Microsoft 365

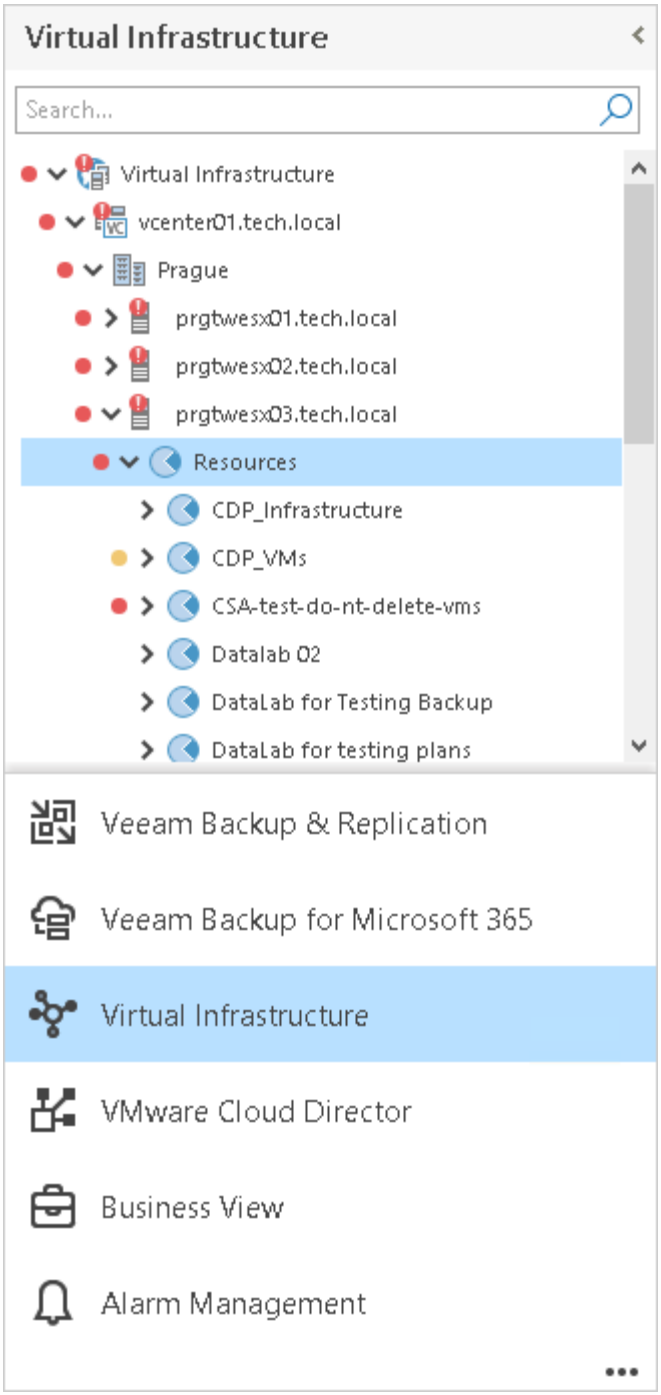
The **Veeam Backup for Microsoft 365** tree displays a hierarchical list of connected Veeam Backup for Microsoft 365 servers and components of the backup infrastructure — backup proxies and backup repositories.



Virtual Infrastructure

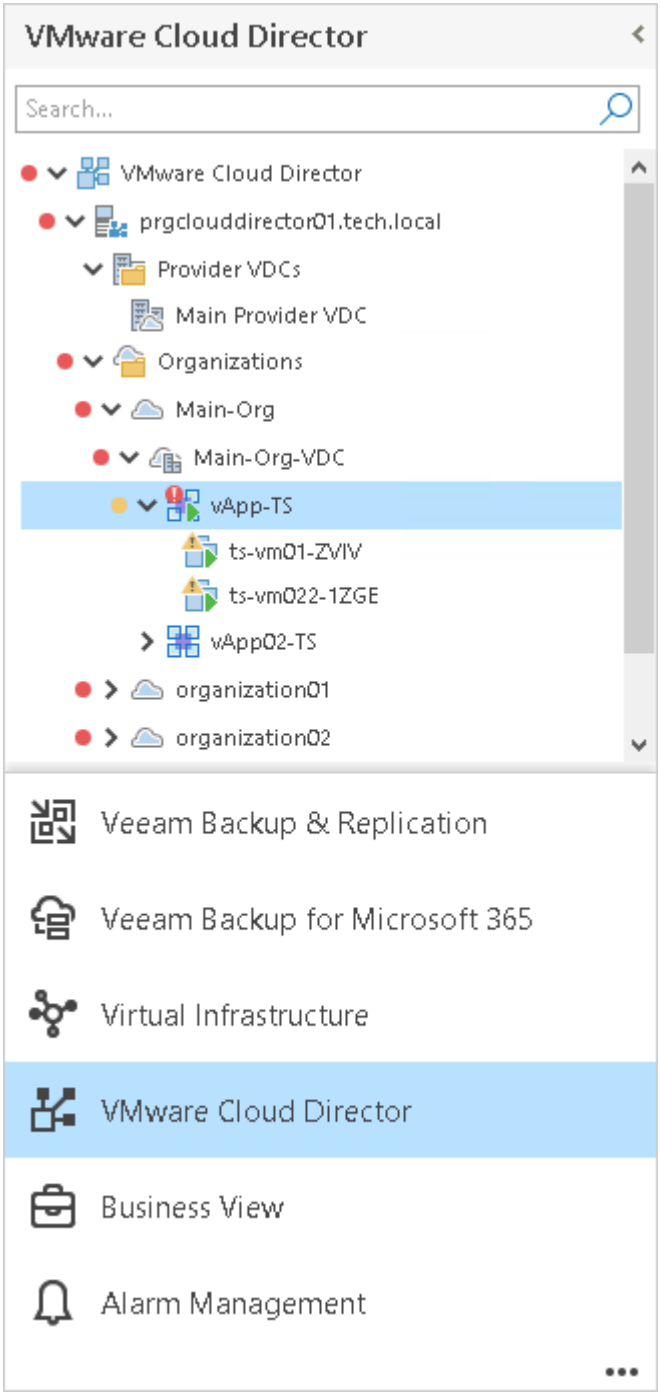
The **Virtual Infrastructure** tree displays a hierarchical list of virtual infrastructure objects — vCenter Servers/SCVMM servers, clusters, hosts, folders, VMs, storage objects and so on. It shows the virtual infrastructure in inventory terms, similar to vCenter Server/SCVMM topology presentation.

If you connect a VMware Cloud Director server to Veeam ONE, the Virtual Infrastructure inventory tree displays vCenter Servers attached to VMware Cloud Director and VMware Cloud Director VMs. To hide VMware Cloud Director VMs from the Virtual Infrastructure inventory, enable the **Hide VMware Cloud Director VMs from Virtual Infrastructure tree** option in Veeam ONE server settings. For details on the VMware Cloud Director display settings, see Other Settings.



VMware Cloud Director

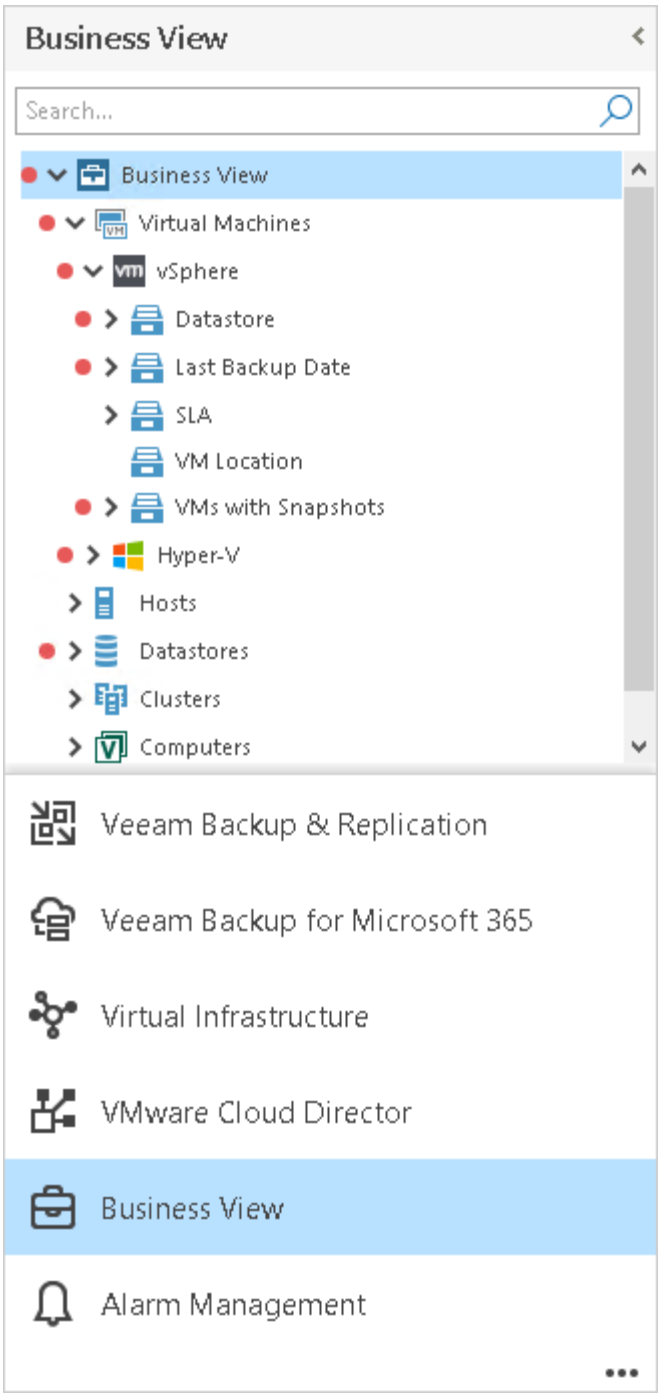
The VMware Cloud Director tree displays a hierarchical list of VMware Cloud Director objects — provider VDCs, organizations, organization VDCs, vApps, and VMs.



Business View

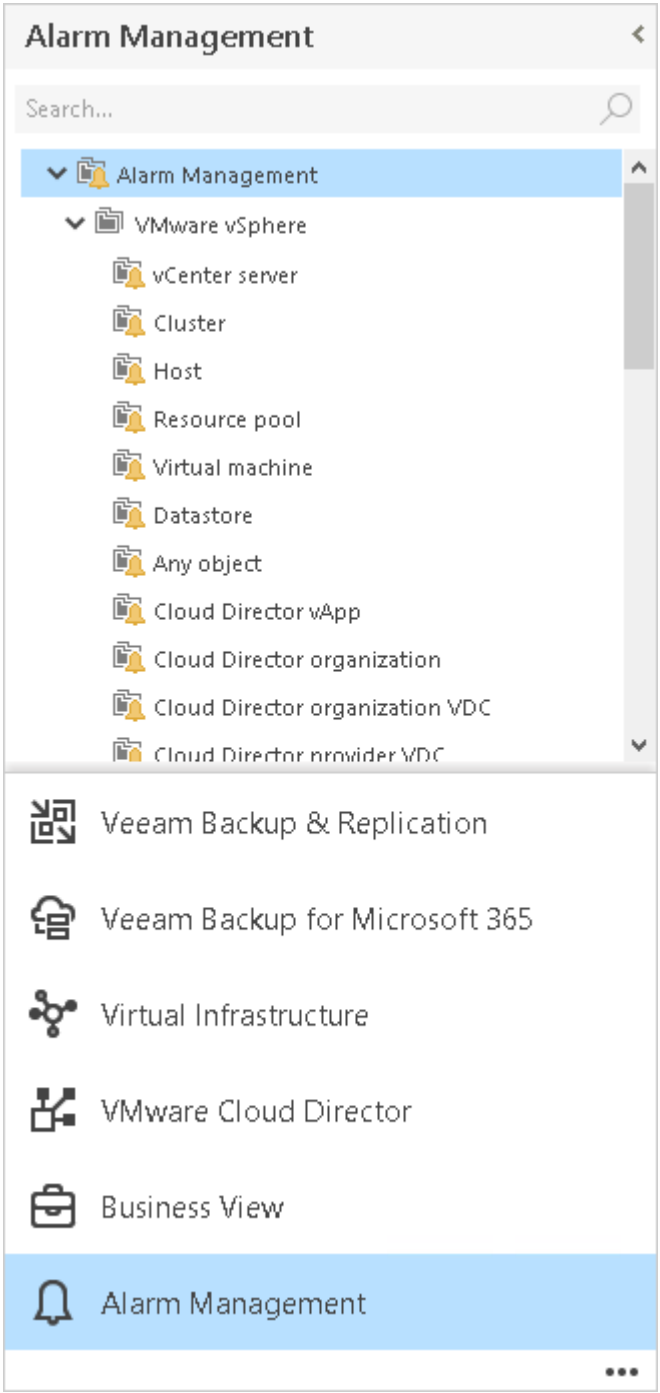
The **Business View** tree displays a hierarchical list of categorization groups configured in Business View. It presents the infrastructure topology in business terms and allows you to monitor, alert and report on custom categorization units in your environment.

By default, Veeam ONE Client hides the *Uncategorized* group for all Business View categories in the inventory tree. To make it available in the Business View hierarchy, disable the **Hide ungrouped objects from Business View tree** option in Veeam ONE Client server settings. For details on changing Business View display settings, see Hiding Ungrouped Objects.



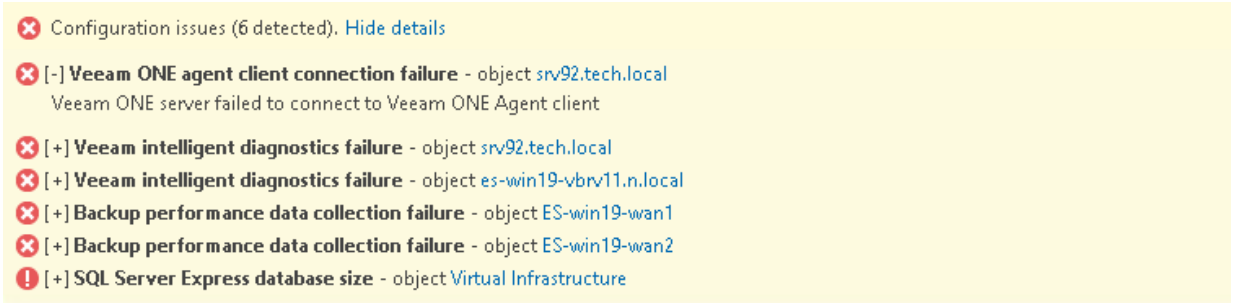
Alarm Management

The **Alarm Management** tree displays the list of available alarm types. Use the **Alarm Management** view to manage predefined alarms or create new alarms.



Configuration Issues Pane

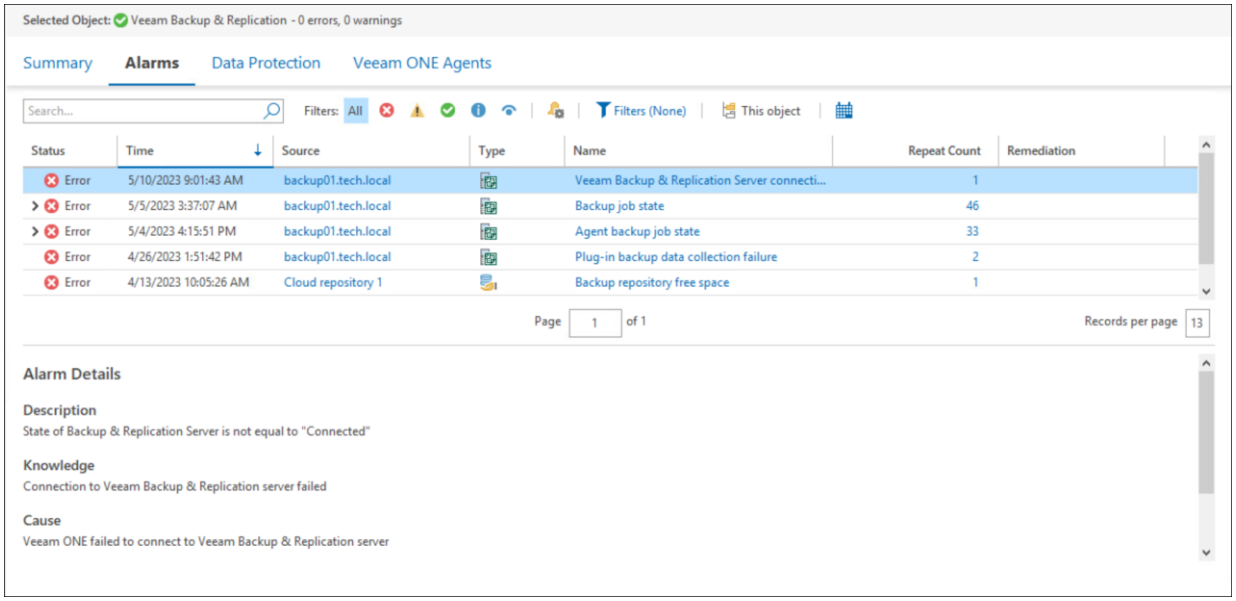
The **Configuration issues** pane displays information on alarms triggered as a result of internal Veeam ONE configuration issues (such as lost connection to a virtual server, data collection failure, license expiration and so on). To view details of internal alarms, click the **Show details** link on the pane. For details on working with internal configuration alarms, see Working with Internal Alarms.



Information Pane

The information pane is the main working area used for managing alarms, viewing performance data and accomplishing other operations for monitoring your virtual and data protection environment.

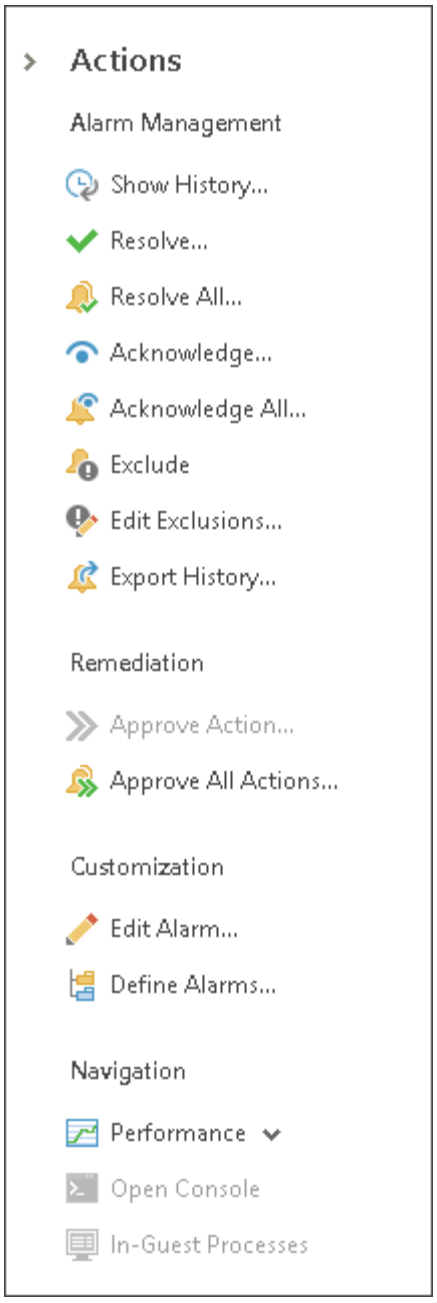
Tabs in the information pane allow you to switch between Veeam ONE Client dashboards. The set of available dashboards varies depending on the object selected in the inventory tree.



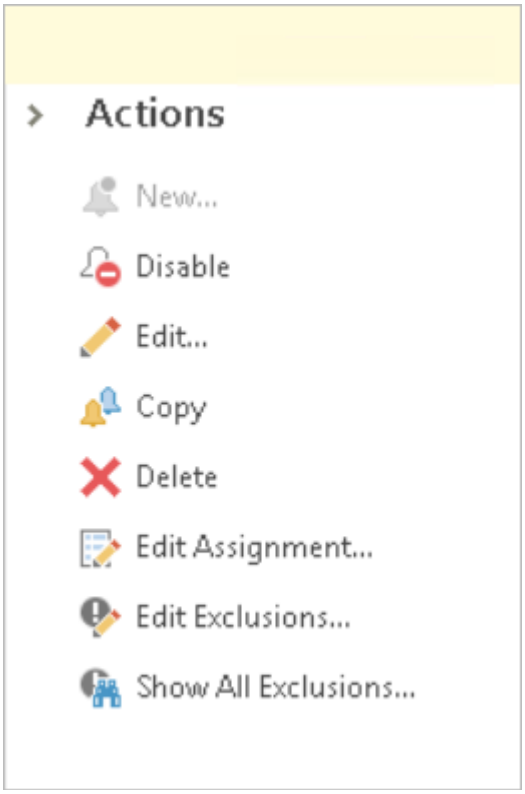
Actions Pane

The **Actions** pane on the right displays links to tasks and commands that can be initiated by the user. The pane becomes available when you open the **Veeam ONE Agents** or **Alarms** tabs, or switch to the **Alarm Management** view. You can hide and show the pane using the collapse/expand arrows.

Options displayed on the pane depend on the object type selected in the information pane. For example, if you select a VM in the inventory pane and open the list of triggered alarms for this VM, all alarm actions, object actions, and navigation actions will be available in the **Actions** pane. If you select a storage object in the inventory pane, some navigation actions will become unavailable as they do not apply to storage objects. For details on working with alarm actions, see Working with Alarms.



In a similar manner, if you open the **Alarm Management** section and select the **Alarm Management** node in the inventory pane, the **New** action will become unavailable, as you must select a particular object to create a new alarm.



Configuring Notification Settings

When you open Veeam ONE Client for the first time, you will be prompted to configure notification settings in the **Notification Settings** wizard.

> **TIP:**
>
> If you want to configure notification settings later, click **Cancel**.
>
> To access the wizard later, in the main menu, select **Notifications**. Alternatively, you can configure notifications by changing server settings. For details, see Veeam ONE Server Settings.

To configure notification settings, take the following steps.

Step 1. Configure SMTP Server Settings

At the **Mail Server Settings** tab, configure SMTP server settings or integration with Google Gmail or Microsoft 365. Veeam ONE will use provided settings for notifications generated by both Veeam ONE Monitoring Service and Veeam ONE Reporting Service.

Configuring SMTP Server Settings

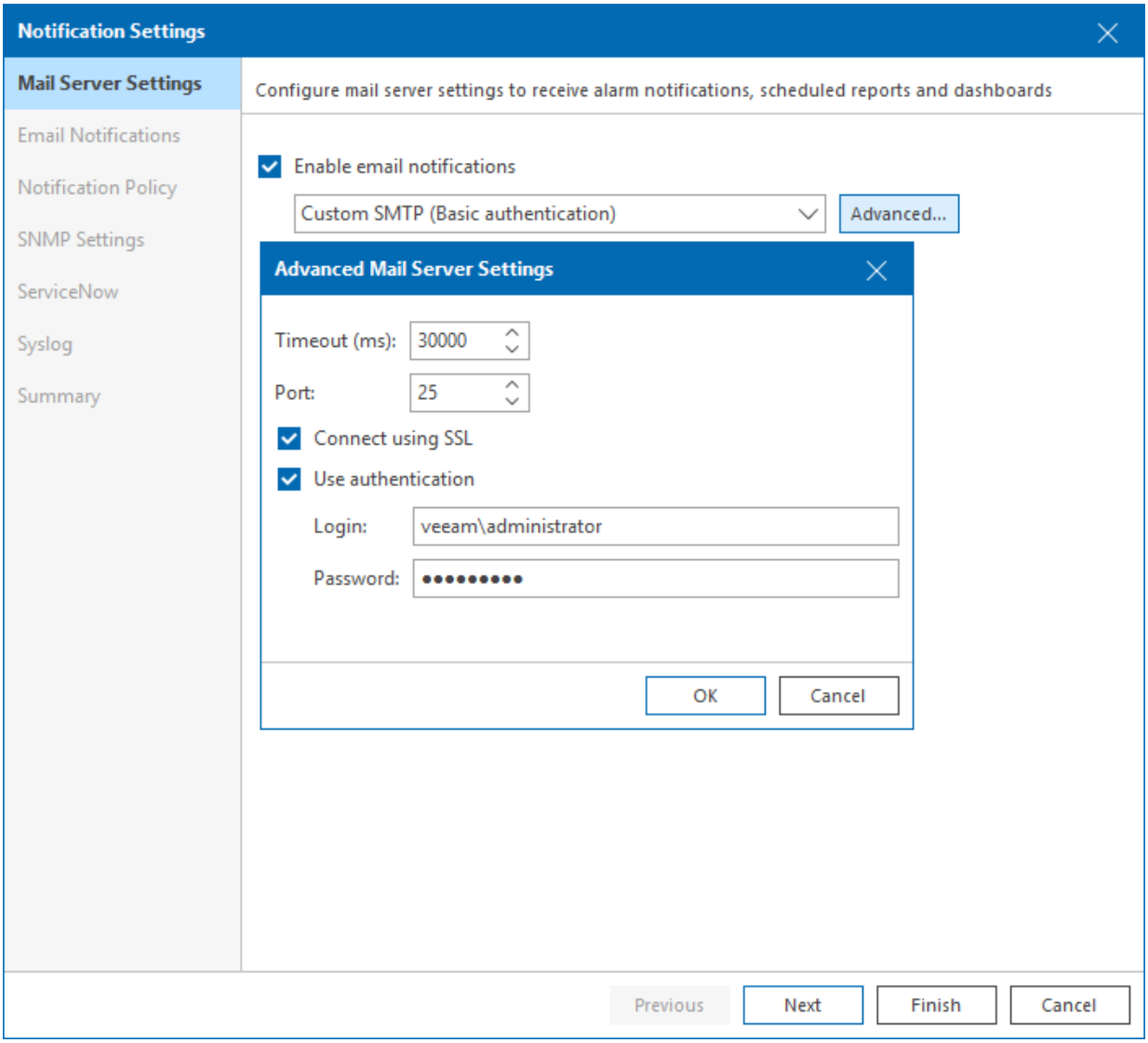
To configure SMTP server settings:

1. Select the **Enable email notifications** check box.
2. From the drop-down list, select **Custom SMTP (Basic authentication)**.
3. In the **SMTP server** field, enter DNS name or IP address of the SMTP server that will be used to send email notifications. All Veeam ONE email notifications (including test messages), automatically generated reports and dashboards will be sent by this SMTP server.

   The default SMTP port is 25.
4. In the **From** field, enter the email address of the notification sender.

   This email address will be displayed in the **From** field of notifications.
5. To configure additional settings, click **Advanced**:
   a. In the **Timeout** field, specify server connection timeout in milliseconds.
   b. In the **Port** field, change the default SMTP communication port if required.
   c. For SMTP server with SSL support, select **Connect using SSL** to enable SSL data encryption.
   d. If your SMTP server requires authentication, select the **Use authentication** check box and specify authentication credentials in the **Login** and **Password** fields.

e. Click **OK**.



Configuring Mail Service Integration

To configure mail service integration:

1. Select the **Enable email notifications** check box.
2. From the drop-down list, select **Microsoft 365** or **Google Gmail**.
3. Click Authorize now.

   You will be redirected to your mail service provider page. After you complete the authentication, you will be redirected to Veeam ONE web portal and the mail server settings will be saved automatically.
4. In the **From** field, enter the email address of the notification sender.

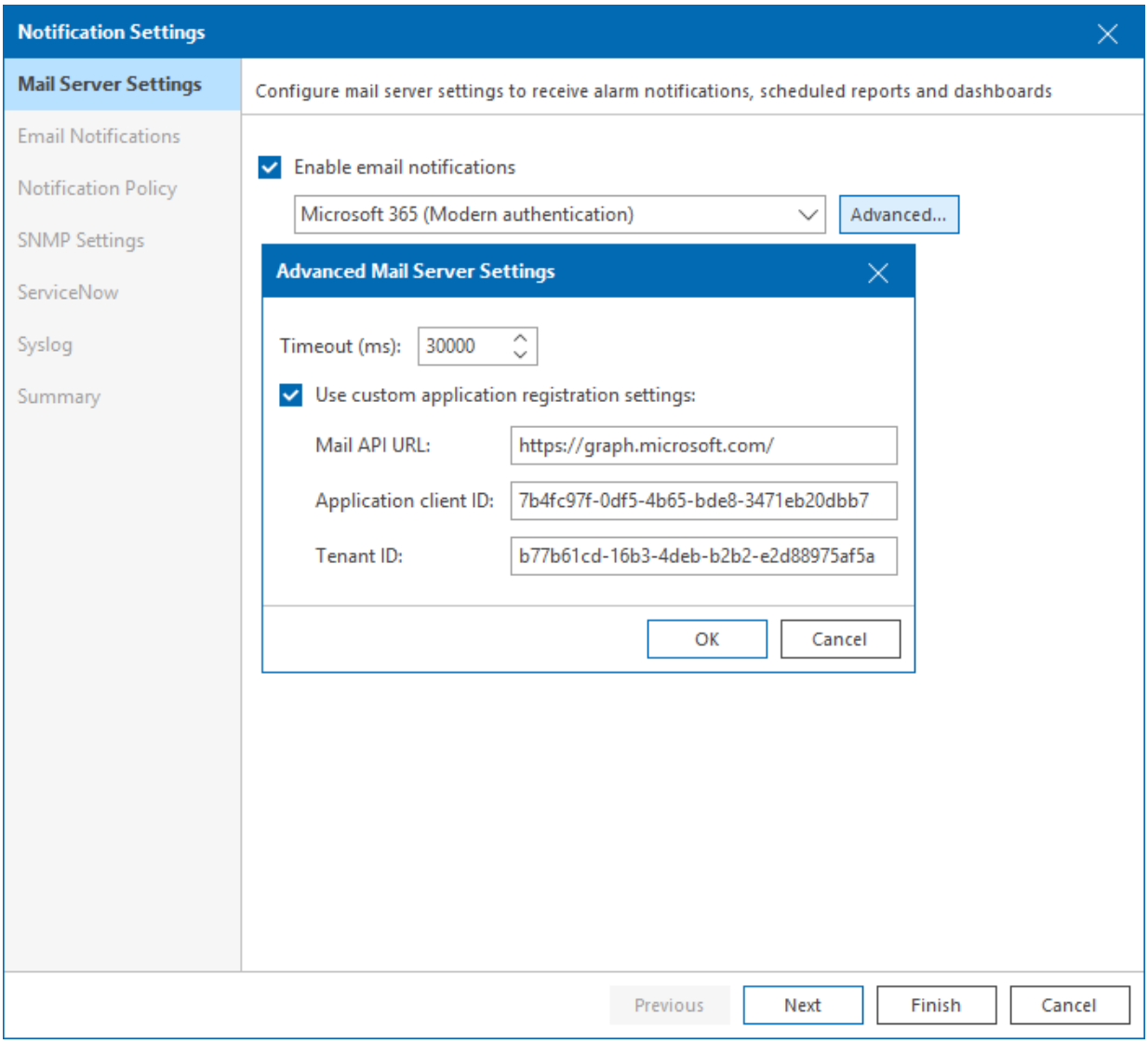
   This email address will be displayed in the **From** field of notifications.
5. To configure additional settings, click **Advanced**:

6. In the **Timeout** field, specify server connection timeout in milliseconds.

   a. Select the **Use custom application registration settings** check box and specify Veeam ONE identification parameters in the mail service:

      - [For Microsoft 365] Specify **Mail API URL, Application client ID** and **Tenant ID**.
      - [For Google Gmail] Specify **Application client ID** and **Client secret**.

   b. Click **OK**.



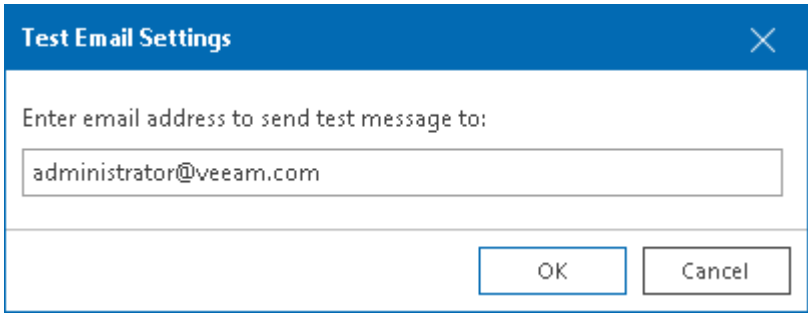
Testing Mail Server Settings

You can send out a test email to make sure that mail server settings are configured correctly:

1. Click **Send Test Email**.
2. Enter an email address at which a test notification should be sent.

3. Click **OK**.

   A test email will be sent to the specified email address.



For details on alarm notification settings, see Configuring Alarm Notifications.

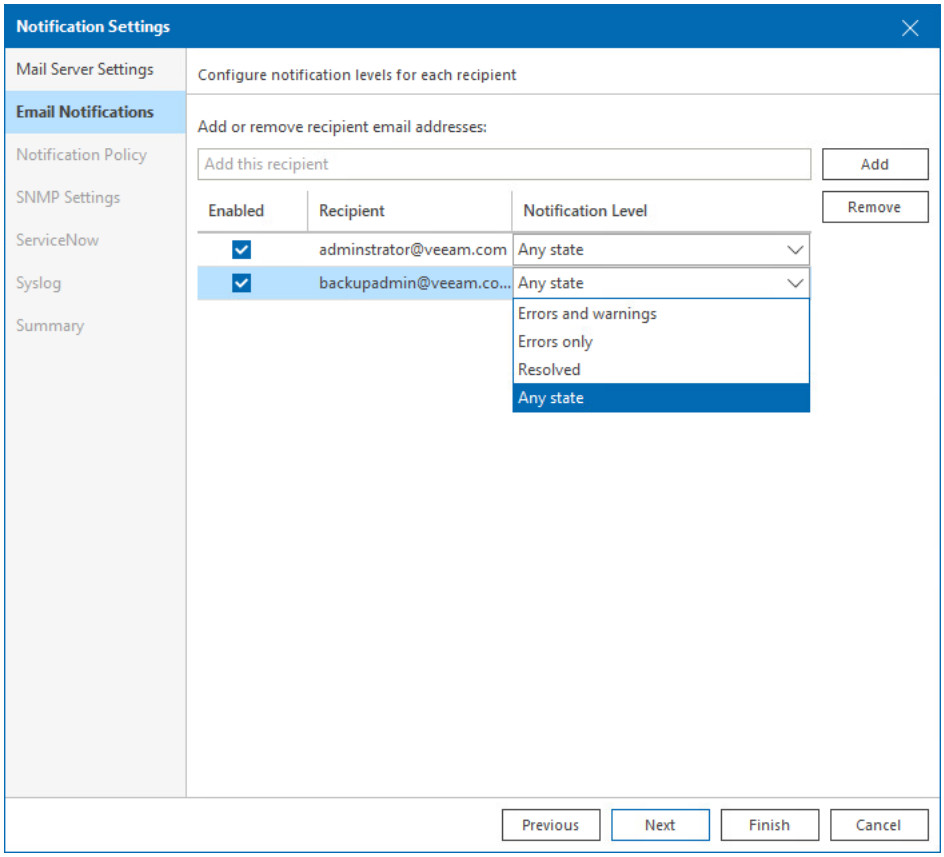
Step 2. Configure Email Notification Settings

At the **Email Notifications** step of the wizard, create a list of recipients to include in the default notification group. For every recipient in the group, specify notification conditions.

The default notification group allows you to simplify the process of configuring alarm notification settings. Instead of specifying notification recipients for every alarm, you can create a group of recipients (for example, monitoring operators and administrators) and notify the whole group when an alarm is triggered or when an alarm changes its status.

To add a recipient to the default notification group:

1. In the **Add or remove recipient email addresses** field, enter an email address of a recipient and click **Add**.
2. From the **Notification Level** list, choose the severity of notifications that the recipient will receive:
   - **Any state** – an email notification will be sent every time when an alarm status changes to *Error*, *Warning* or *Info*.
   - **Errors and warnings** – an email notification will be sent every time when an alarm status changes to *Error* or *Warning*.
   - **Errors only** – an email notification will be sent every time when an alarm status changes to *Error*.
   - **Resolved** – an email notification will be sent every time when an alarm status changes to *Resolved*.



To remove a recipient from the list, select an email address in the list and click **Remove**.

To temporarily disable notifications for specific recipients, clear check boxes next to necessary email addresses in the list.

IMPORTANT!

By default, all predefined alarms are configured to notify members of the default notification group in accordance with the specified notification level. After you add recipients to the default notification group, you might need to change alarm settings or adjust the default email notification frequency. For details on alarm settings, see Specify Alarm Notification Options.

Step 3. Configure Email Frequency

At the **Notification Policy** step of the wizard, specify how often Veeam ONE must send email notifications about alarms.

The frequency at which email notifications are sent is defined with the help of notification policies. Veeam ONE offers two notification policies:

- **Mission Critical** – if this notification policy is used, Veeam ONE creates a new email notification for every alarm. You get an instant email notification once a new alarm is triggered, or once alarm status is changed.
- **Other** – if this notification policy is used, Veeam ONE sends out an email notification about alarms once in a specific time interval (by default, once in 30 minutes). You do not receive a separate email notification for every alarm. Instead, every 30 minutes you receive one email notification about all alarms that were triggered or that changed their status since the latest notification.

By default, the **Mission Critical** policy is applied to all objects in your virtual infrastructure, VMware Cloud Director infrastructure and all objects in your backup infrastructure. If necessary, you can apply different notification policy settings to infrastructure objects or Business View groups:

1. Remove effective notification policy settings for chosen infrastructure objects.
2. Apply new notification policy settings to chosen infrastructure objects or Business View groups.

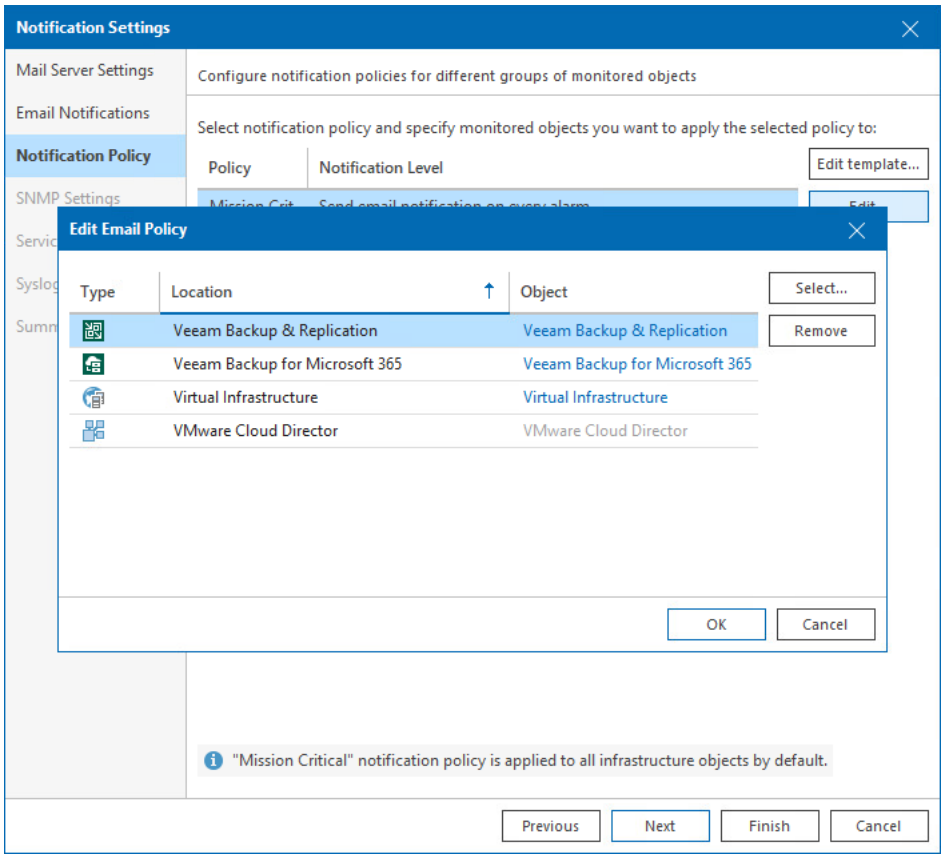
For example, if you want to receive email notifications about problems in the backup environment once within 30 minutes, you must first remove the **Mission Critical** policy settings for backup infrastructure objects, and then apply the **Other** policy settings to backup infrastructure objects.

Removing Effective Notification Policy Settings

Before applying new notification policy settings, you must remove the effective settings for the chosen type of infrastructure objects:

1. Select the necessary policy in the list and click **Edit**.

2. In the **Edit Email Policy** window, select the necessary type of infrastructure objects and click **Remove**.

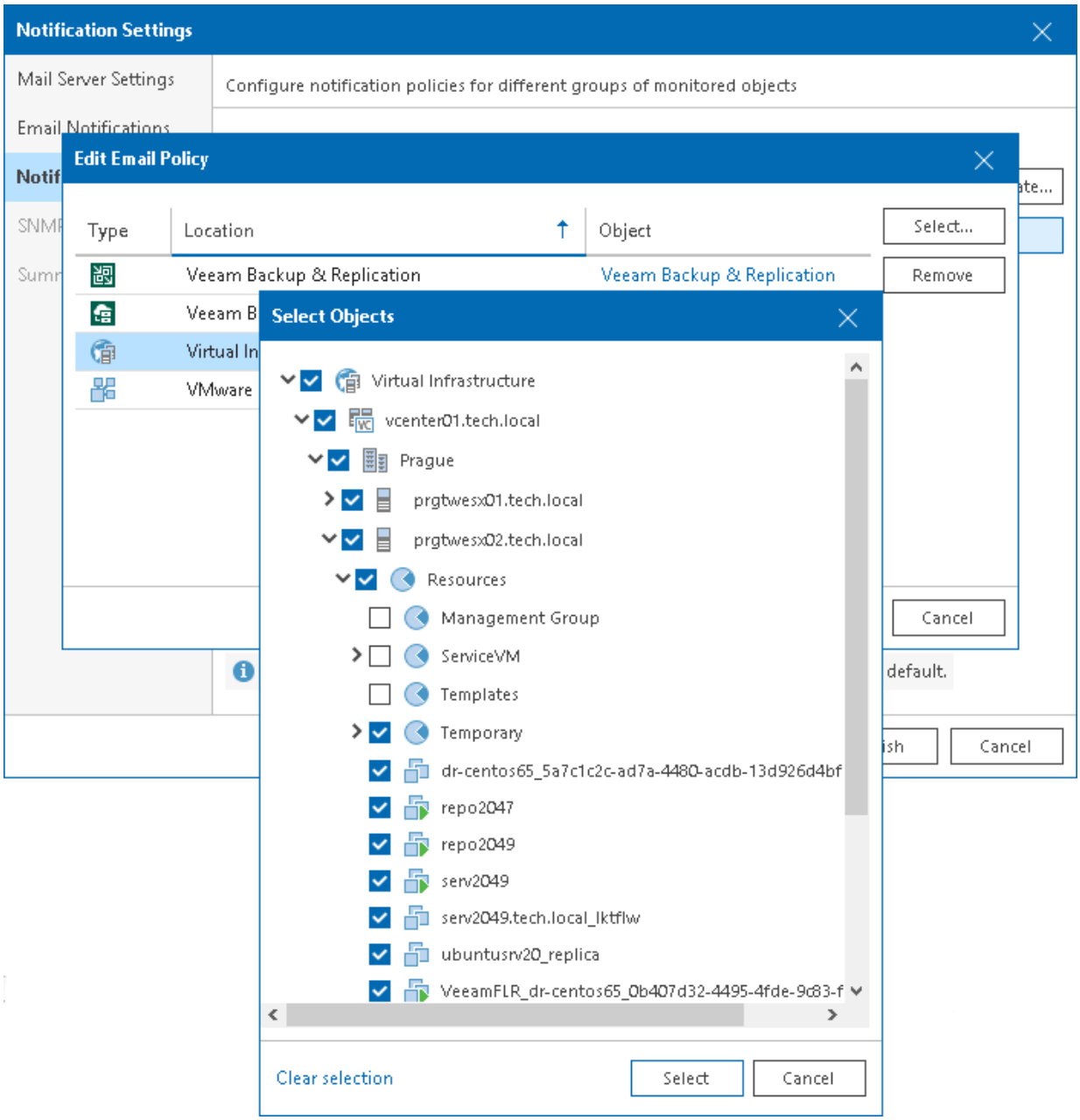


Applying Notification Policy Settings

To apply new notification policy settings to infrastructure objects or Business View groups:

1. Select the necessary policy in the list and click **Edit**.
2. In the **Edit Email Policy** window, click **Select** and choose one of the following options:
   - **Virtual Infrastructure** — browse the virtual infrastructure hierarchy and select check boxes next to objects or infrastructure segments to which the policy settings must apply.
   - **Business View** — browse the Business View hierarchy and select check boxes next to groups or infrastructure objects to which the policy settings must apply.
   - **VMware Cloud Director** — browse the VMware Cloud Director infrastructure and select check boxes next to infrastructure components to which the policy settings must apply.
   - **Veeam Backup & Replication** — browse the backup infrastructure and select check boxes next to infrastructure components to which the policy settings must apply.
   - **Veeam Backup for Microsoft 365** — browse the Veeam Backup for Microsoft 365 infrastructure and select check boxes next to infrastructure components to which the policy settings must apply.
3. Click **Select**.
4. [Only for the **Other** policy] In the **Time interval to send summary email (minutes)** field, specify how often Veeam ONE must send a summary email informing about triggered alarms.

5. Click **OK**.



TIP:

You can also change the notification policy settings by adjusting server settings. For details, see Veeam ONE Server Settings.

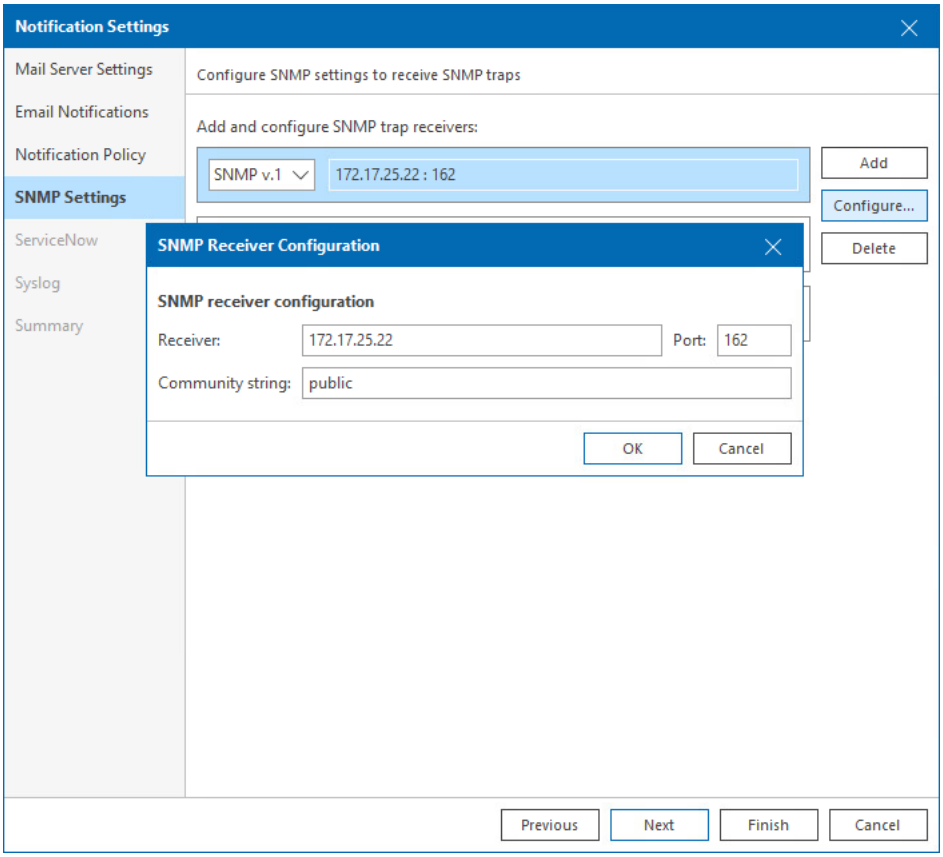
Step 4. Configure SNMP Settings

At the **SNMP Settings** step of the wizard, specify trap notification settings that can be used for sending notifications about alarms.

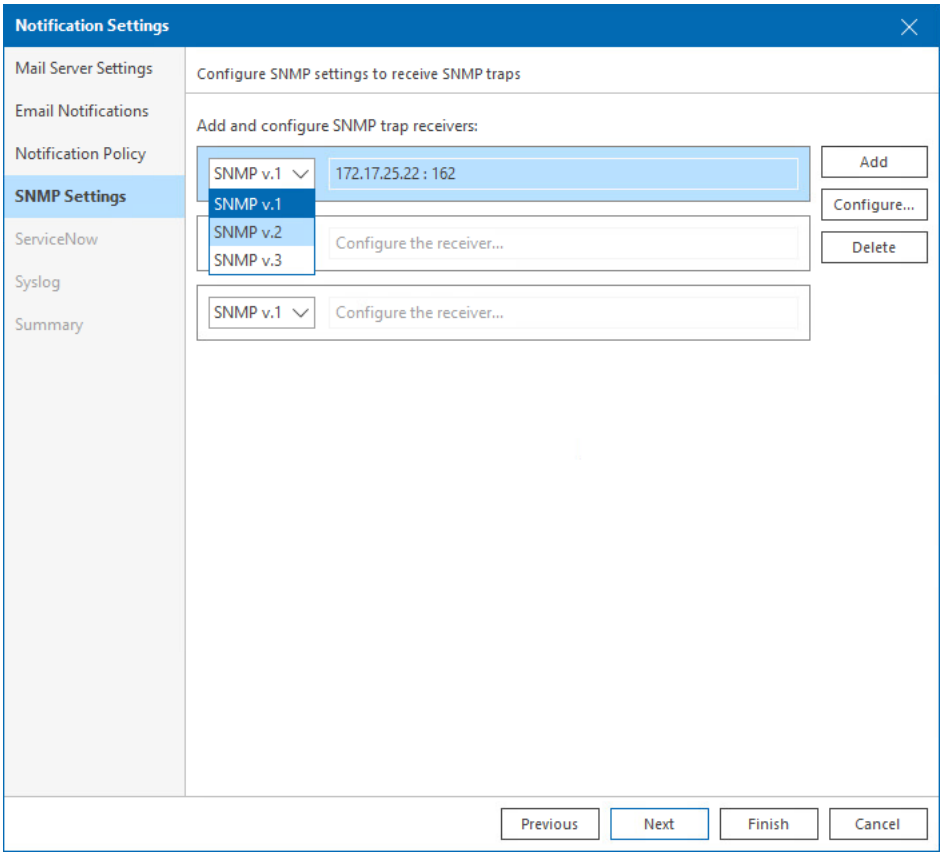
To specify SNMP receiver configuration settings:

1. Click **Add**.
2. Click **Configure** to open the **SNMP Receiver Configuration** window.
3. In the **Receiver** field, specify DNS name or IP address of the SNMP receiver.
4. In the **Port** field, specify the port number to be used.

   The default SNMP port is 162.
5. In the **Community string** field, enter the community identifier.
6. Click **OK** to apply the specified settings.



7. In the list of SNMP receivers, choose the version of the SNMP protocol to be used.



To add a new receiver to the list, click **Add** and repeat steps 2-7 described above.

Note that after you configure notification settings, you must configure SNMP service properties on the trap recipient computers:

1. Install a standard Microsoft SNMP agent from the Windows distribution.
2. From the Start menu, select **Control Panel** > **Administrative Tools** > **Services**.
3. Double-click **SNMP Service** to open the **SNMP Service Properties** window.
4. Click the **Traps** tab.
5. Add the public string to the **Community name** list and the host name to the **Trap destinations** list.
6. Click the **Security** tab.
7. Make sure the **Send authentication trap** option is selected.
8. Add the public string to the **Accepted community names** list.
9. Select the **Accept SNMP packets from any hosts** option.
10. Click **Apply** and then **OK** to accept changes.

> **NOTE:**
>
> By default, Veeam ONE alarms are not configured to send SNMP traps when the alarm state changes. To enable SNMP traps for an alarm, you should change alarm action settings. For details, see Enable SNMP Notification for Alarms.

Step 5. Configure ServiceNow Integration

The ServiceNow integration provides Veeam ONE with enhanced visibility and faster alerts triggered directly as ServiceNow incidents.

At the **ServiceNow** step of the wizard, specify your ServiceNow settings used for ServiceNow integration.

To specify ServiceNow integration details:

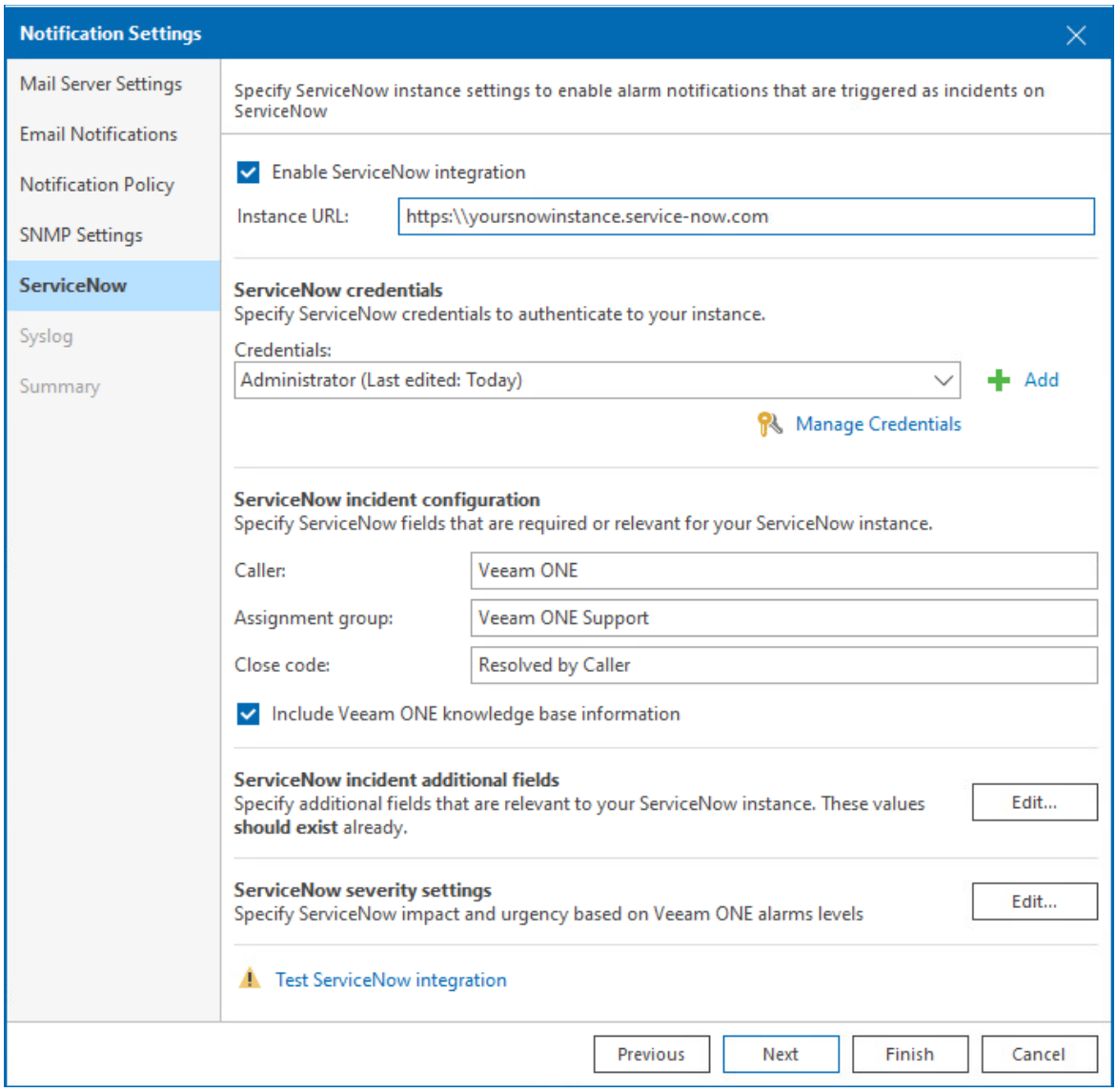
1. Select the **Enable ServiceNow integration** check box.
2. In the **Instance URL** field, specify the ServiceNow instance URL, for example `https:\\yourinstancename.service-now.com`.
3. Specify **ServiceNow credentials** used to authenticate your ServiceNow instance administration.

   For details on permissions required for connection, see Connection to ServiceNow.

   For details on adding credentials records, see Credentials Manager.
4. [Optional] If your organization policy requires additional ServiceNow credentials, click **Add** and enter your additional credentials.
5. In the **ServiceNow incident configuration** section, specify the following details:
   - **Caller** — defines the caller name assigned for the purposes to create, update, and resolve incidents. *Veeam ONE* is the default value, alternatively you can define a custom name if it already exists on your ServiceNow instance.
   - **Assignment group** — defines the name for the assignment group for the purposes to create, update, and resolve incidents. *Veeam ONE Support* is the default value, alternatively you can define a custom name if it already exists on your ServiceNow instance.
   - **Close code** — defines the close code for resolved incidents. Use only the close code defined on your ServiceNow instance.
   - [Optional] Select the **Include Veeam ONE Knowledge Base** information check box to mark incidents for knowledge base articles.
6. [Optional] In the **ServiceNow incident additional fields** section, click **Edit** and add additional **Name** and **Value** parameters to add additional fields relevant to your company's ServiceNow requirements. You must provide both the **Name** and **Value** in the same form as found in the ServiceNow REST API.
7. [Optional] In the **ServiceNow severity settings** section, click **Edit** and configure the ServiceNow impact and urgency levels that correspond to each Veeam ONE *Error*, *Warning* and *Information* alarm. To test that the severity settings match the correct values in your ServiceNow instance, click **Check available values**. To return the severity settings to their default values click **Back to default values**.
8. To test the connection settings, click **Test ServiceNow Integration**.

   Veeam ONE will establish a connection to ServiceNow, create and resolve a test incident.

If you select the **Enable ServiceNow integration** check box and do not test the connection, Veeam ONE will verify it before saving the notification settings. Additionally, the connection is checked when each *Notification Settings* item (*Mail Server Settings*, *Email Notifications* and so on) changes.



For details on alarm notification settings, see Configuring Alarm Notifications.

Step 6. Configure Syslog Integration

Syslog integration allows you to send pre-built Veeam ONE alarms and data for audit events for reuse within your Syslog server environment.

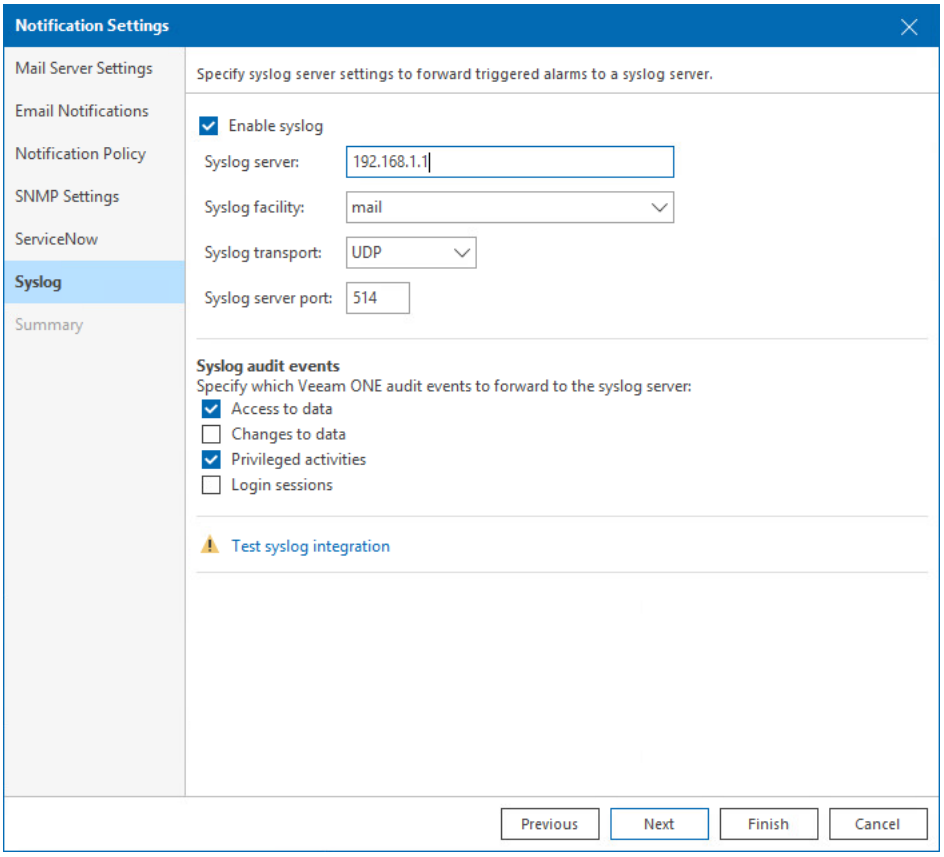
At the **Syslog** step of the wizard, specify your Syslog settings used to return alarms to your Syslog instance.

To specify your Syslog integration details:

1. Click the **Enable syslog** check box.
2. Enter **Syslog server** details::
   - **Syslog server** — define the IPv4 or IPv6 address of your Syslog instance.
   - **Syslog facility** — define the value used to identify the source of the alarm. By default this is set to mail.
   - **Syslog transport** — define TCP, TCP with TLS, or UDP. By default this is UDP.
   - **Syslog server port** — the port used to connect to your Syslog integration instance. By default this is 514.
3. Select your required **Syslog audit events** to send to your Syslog integration:
   - Access to data
   - Changes to data
   - Privileged activities
   - Login sessions

4. To test the connection settings, click **Test syslog integration**. This creates a test connection to Syslog and returns a signal confirming a successful connection.

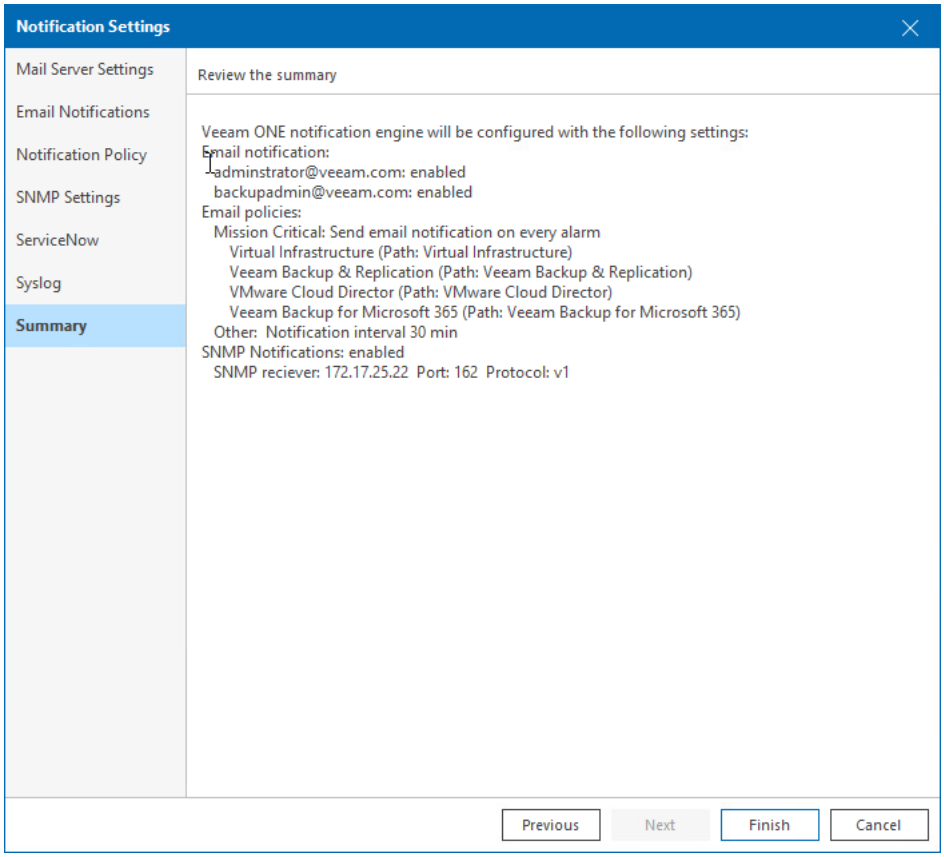
   If you select the **Enable syslog** check box and do not test the connection, Veeam ONE will verify it before saving the notification settings. Additionally, the connection is checked when each Notification Settings item (*Mail Server Settings*, *Email Notifications* and so on) changes.



For details on alarm notification settings, see Configuring Alarm Notifications.

Step 7. Review Summary

Review configured notification settings and click **Finish**.



Configuring Veeam ONE

To start working with Veeam ONE, perform a number of steps for its initial configuration:

1. Add data sources.

   Connect Veeam Backup & Replication, Veeam Backup for Microsoft 365, VMware vSphere, VMware Cloud Director and Microsoft Hyper-V servers.

2. Choose objects to monitor and report on.

   By default, Veeam ONE collects data for all child objects of connected servers. You can change the data collection scope and choose to monitor and report on only specific hosts, datastores and VMs.

3. Configure notification settings.

   Specify notification settings to stay aware of all important events and changes that happen in the virtual and backup environment.

4. Check data collection schedule for Veeam ONE Reporting Service.

   Check and if necessary adjust data collection schedule for Veeam ONE reporting capabilities.

5. Add users to Veeam ONE security groups.

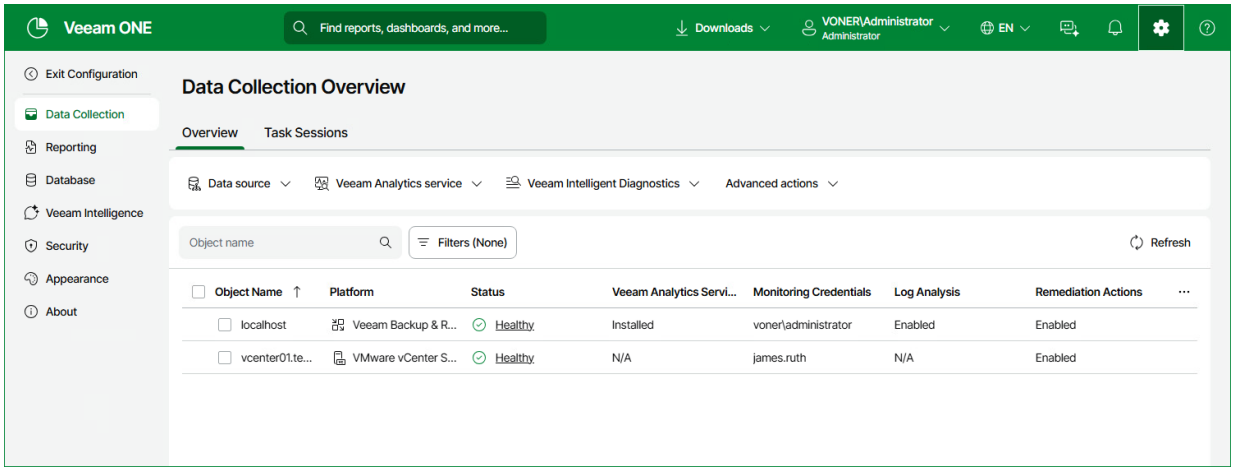
   Add to Veeam ONE security groups users who must have access to Veeam ONE Client and Veeam ONE Web Client functionality.

Data Collection

In the **Data Collection Overview** tab you can configure server connections, **Veeam Analytics service** settings, **Veeam Intelligent Diagnostics** settings and perform **Advanced actions**.

The **Overview** tab shows overall health status of the connected servers based on collection session and connection status results. In the case of Veeam Backup & Replication servers, it also displays additional information based on the Veeam Analytics service status and state.

If you do not have any connected servers yet, connect them in the Veeam ONE Web Client. For details, see Add Data Source.



For each server in the list, the following details are available:

- Object name
- Platform type
- Status of data source:
  - *Healthy* — no errors detected
  - *Unhealthy* — indicates a problem with data source collection or connection to the server or in the case of Veeam Backup & Replication or Veeam Backup Enterprise Manager, the Veeam Analytics Service is not installed or has connection problems
  - *Processing* — initial data collection is running or status of the data source is synchronizing after services restart
- Veeam Analytics Service state
- Version
- Monitoring Credentials
- Log Analysis Session State
- Log Analysis (enabled or disabled)
- Remediation Actions (enabled or disabled)

Additionally, you can click the **Filters** button to filter the list by additional details and the **Show or hide columns** button to broaden or narrow the information displayed. You can also click an individual entry's status to open the **Task Details** window.

In This Section

- Adding Data Source
- Veeam Analytics Service
- Veeam Intelligent Diagnostics
- Advanced Actions
- Task Sessions

Adding Data Source

To collect information about your virtual infrastructure and track the efficiency of VM data protection, you must configure connections to VMware vSphere, VMware Cloud Director, Microsoft Hyper-V virtual management servers and Veeam Backup for Microsoft 365 and Veeam Backup & Replication servers in Veeam ONE. Configured connection settings are automatically propagated to all Veeam ONE components.

You can connect the following types of servers:

- Veeam Backup & Replication
- Veeam Backup for Microsoft 365
- VMware vSphere
- VMware Cloud Director
- Microsoft Hyper-V

Before You Begin

Before you configure server connections, check these requirements:

- Supported versions of virtual platforms
- Supported versions and editions of Veeam Backup & Replication and Veeam Backup for Microsoft 365
- Requirements to accounts used for collecting data
- Ports that must be open to allow Veeam ONE collect data from connected servers

For details, see Deployment Planning and Preparation.

Connecting Veeam Backup & Replication Servers

To collect data about your backup infrastructure and data protection operations, you must configure connections to Veeam Backup & Replication servers in Veeam ONE Web Client. You can connect the following types of servers:

- Veeam Backup & Replication server to monitor standalone backup servers
- Veeam Backup Enterprise Manager to monitor all backup servers federated under Veeam Backup Enterprise Manager

NOTE:

- Before you connect a Veeam Backup & Replication server to Veeam ONE check that product licenses are compatible. For details on license compatibility, see Compatibility with Veeam Backup & Replication Licenses.
- To install the Veeam Analytics Service package on Veeam Software Appliance, you must enable remote data collection in the Host Management Interface. For more information, see section Enabling Remote Data Collection of the Veeam Backup & Replication User Guide.

To configure a connection to a Veeam Backup & Replication server, take the following steps.

Step 1. Launch Data Source Wizard

To launch the **Add Server** wizard:

1. Open Veeam ONE Web Client.

   For details on accessing Veeam ONE components, see Veeam ONE Web Client.

2. At the top right corner of the Veeam ONE Web Client window, click **Configuration**.
3. In the **Data Collection** section of the configuration menu, click **Data source**.
4. Click **Add server**.

You can also launch the **Add Server** wizard from Veeam ONE Client, to do so:

1. Open Veeam ONE Client.

   For details on accessing Veeam ONE components, see Veeam ONE Client.

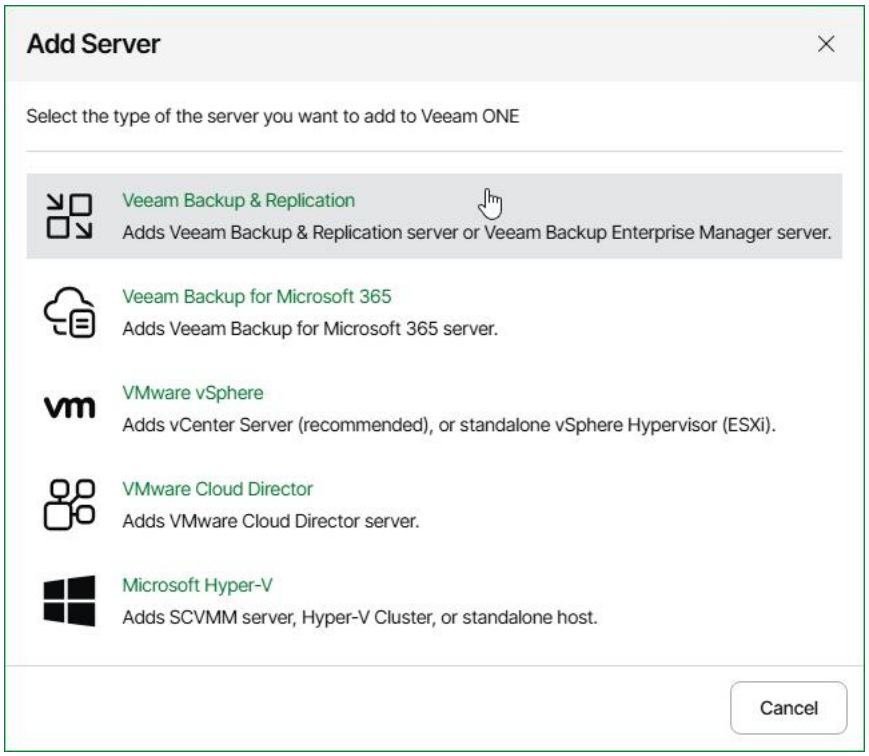
2. In the main menu, click **Add Server**. You will be redirected to Veeam ONE Web Client to follow the wizard steps.

Alternatively, to access the **Add Server** wizard from Veeam ONE Client you can:

- Press [CTRL+I] on the keyboard.
- At the bottom of the inventory pane, open the **Veeam Backup & Replication** view, right-click the **Veeam Backup & Replication** node and choose **Add Server** from the shortcut menu.

Step 2. Choose Server Type

At the first step of the wizard, click **Veeam Backup & Replication**.



Step 3. Specify Server Name and Role

At the **Connection** step of the wizard:

1. Enter DNS name or IP address of the backup server you want to connect.

   If you are adding a high availability cluster, use the IP address or hostname of the primary node.

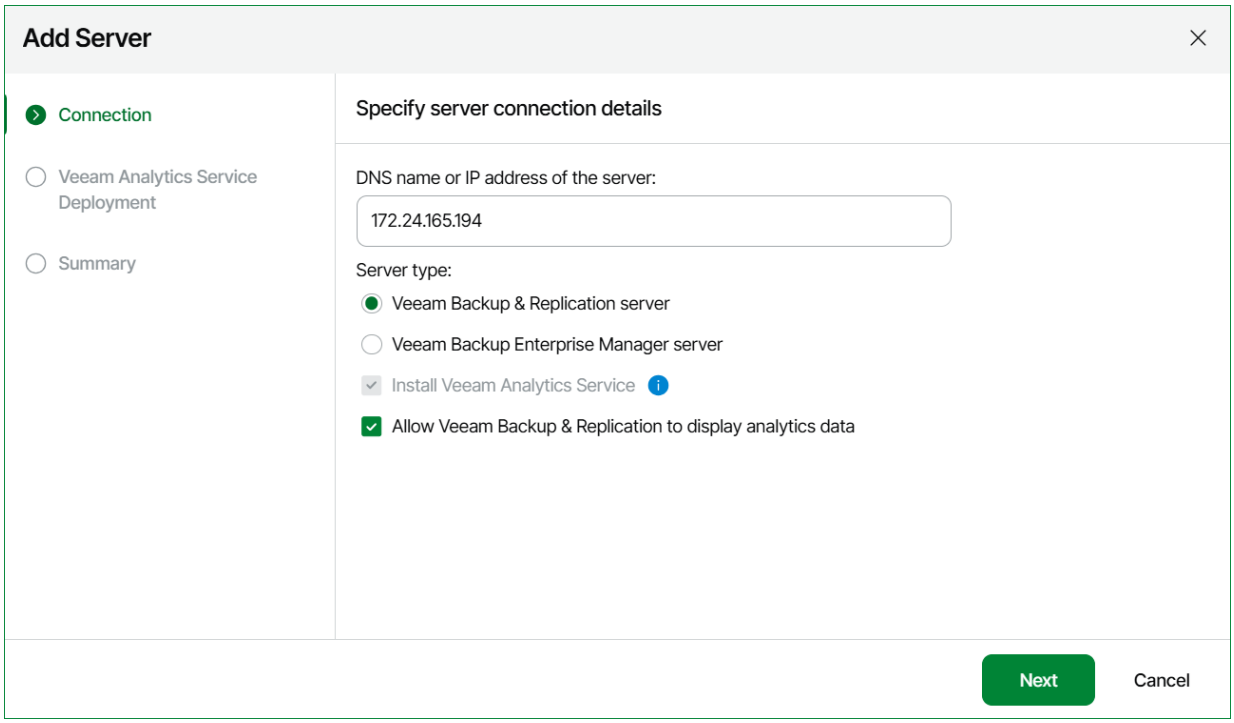
2. Specify the server role — Veeam Backup & Replication server or Veeam Backup Enterprise Manager.

   If you choose to add Veeam Backup Enterprise Manager, Veeam ONE will automatically connect all Veeam Backup & Replication servers added to the Veeam Backup Enterprise Manager.

3. If you want to enable Veeam ONE dashboard and report integration in Veeam Backup & Replication, select the **Allow Veeam Backup & Replication to display analytics data** check box. For details, see Veeam Backup & Replication Web UI.

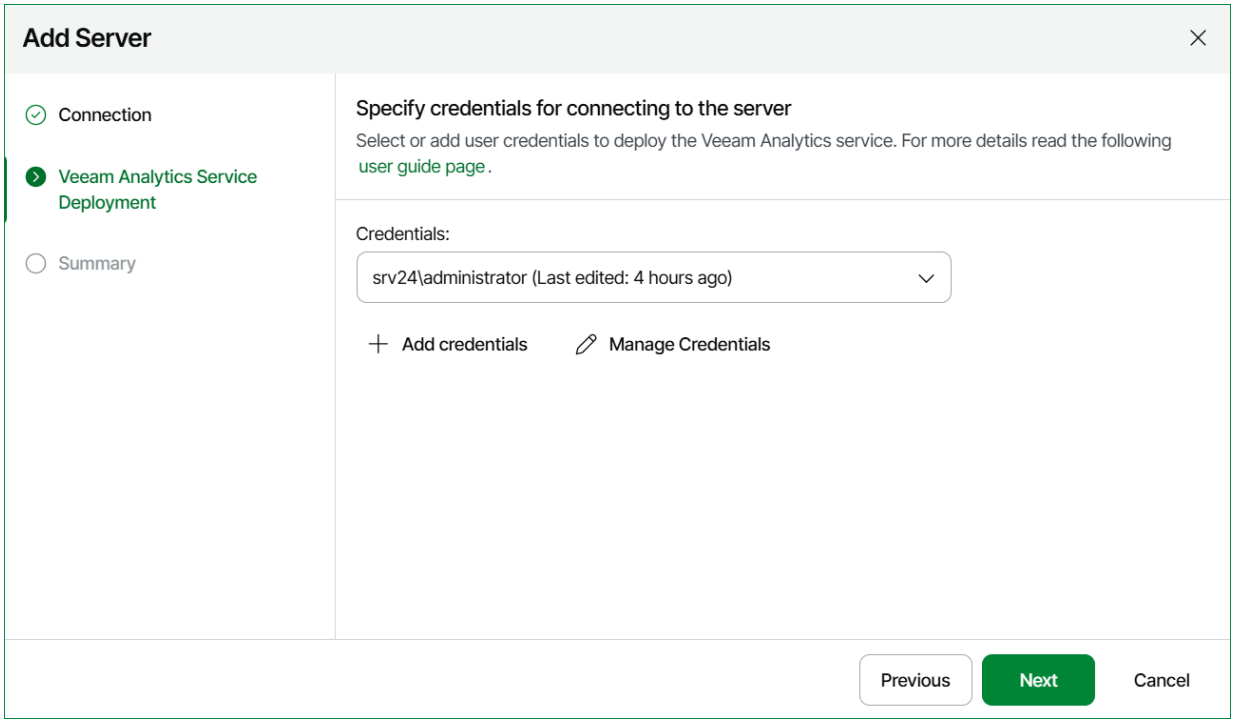
NOTE

- Veeam Analytics service must be installed when adding Veeam Backup & Replication servers.



Step 4. Specify Veeam Analytics Service Deployment Credentials

At the **Veeam Analytics Service Deployment** step of the wizard, specify credentials to install Veeam Analytics service. For details on account permissions, see Veeam Analytics Service Permissions. For details on adding credentials records, see Security.



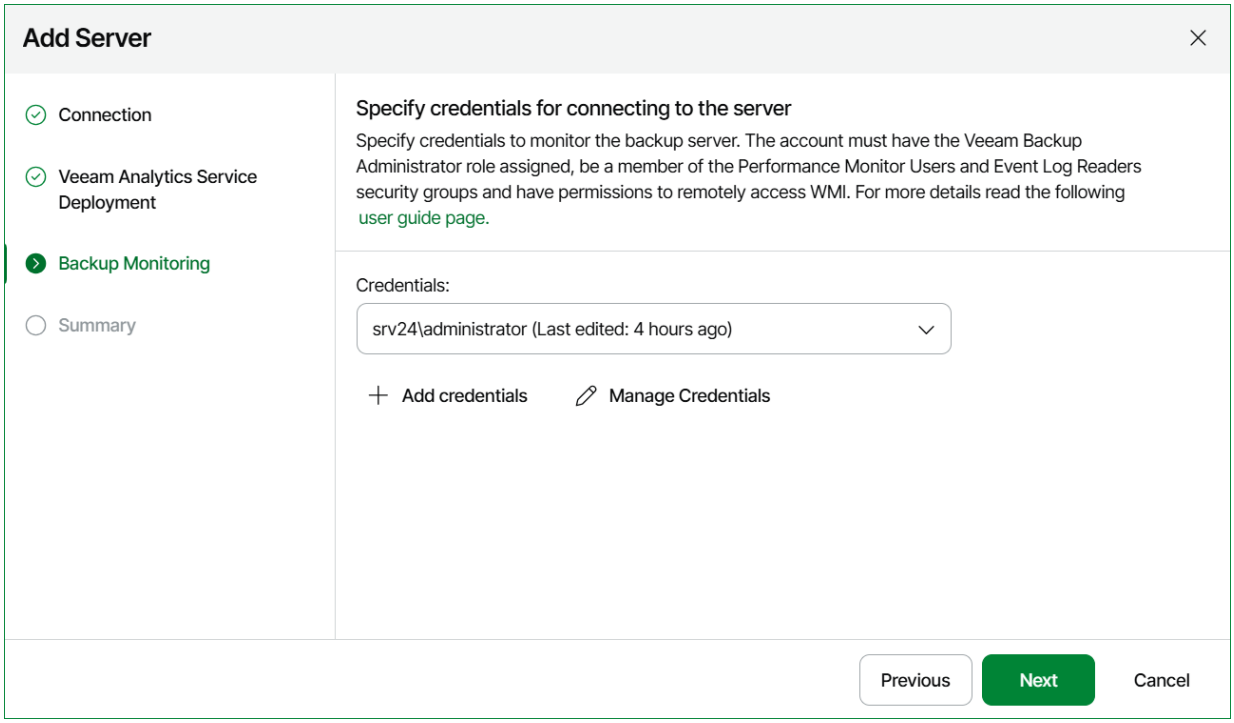
When you add a Veeam Backup & Replication host, Veeam ONE saves to the configuration database a thumbprint of the TLS certificate installed on the Veeam Backup & Replication host. During every subsequent connection to the server, Veeam ONE uses the saved thumbprint to verify the server identity and avoid the man-in-the-middle attack.

If the certificate installed on the server is not trusted, Veeam ONE displays a warning.

- To view detailed information about the certificate, click **View Certificate**.
- If you trust the server, click **Trust and Continue**.
- If you are installing on a high availability cluster, you may need to trust multiple certificates depending on the administration setup of each node within the cluster.
- If you are adding a high availability cluster, Veeam Analytics service must be installed on all nodes in the cluster where it is not already present. It is recommended to use the same user credentials on each node in the cluster. Otherwise, Veeam Analytics service may not install correctly on all secondary nodes, and you may need to perform a manual installation. For details on For details about setting up high availability clusters in Veeam Backup & Replication, see Assembling High Availability Cluster.
- If you do not trust the server, click **Cancel**. Veeam ONE will display an error message, and you will not be able to connect to the server.

Step 5. Specify Backup Monitoring Credentials

If you are adding a Veeam Backup & Replication deployed on Microsoft Windows, at the **Backup Monitoring** step of the wizard, specify credentials to connect to the backup server. For details on account permissions, see Connection to Veeam Backup & Replication Servers. For details on adding credentials records, see Security.

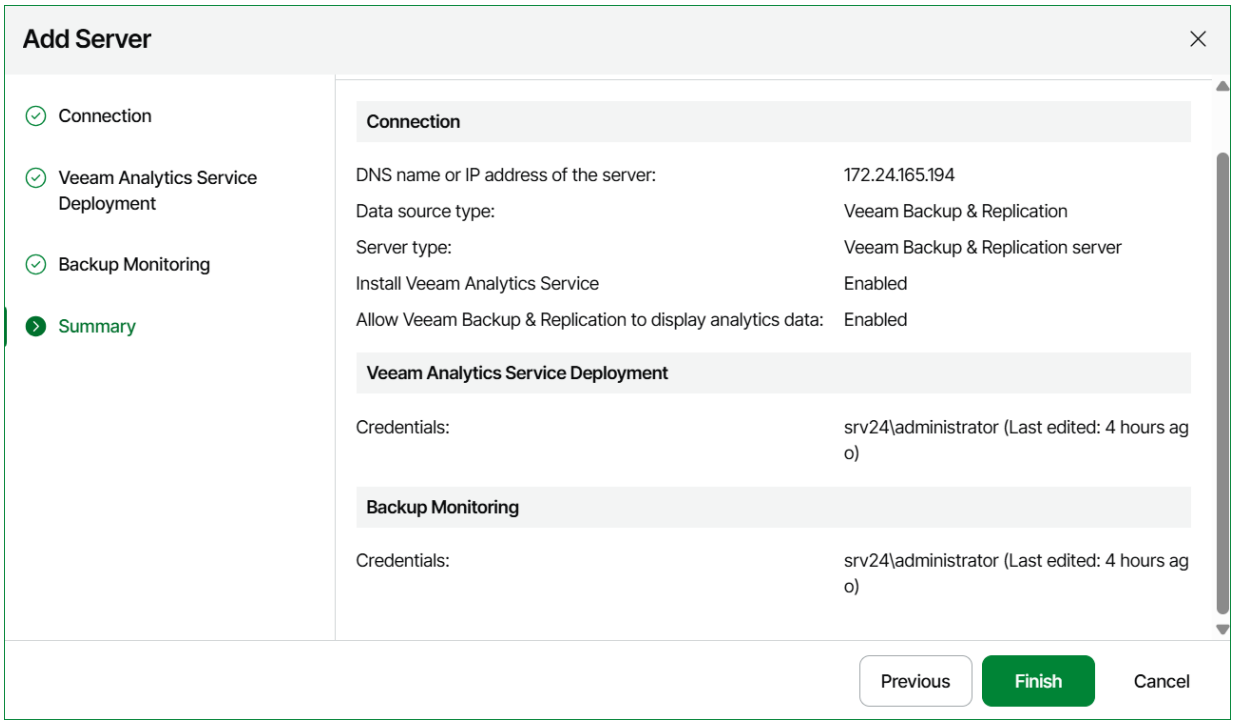


The provided credentials will be used to connect the backup server and all managed servers in the backup infrastructure:

- Veeam Backup & Replication servers (if you connect Veeam Backup Enterprise Manager)
- Backup proxies
- Backup repositories
- WAN Accelerators
- Tape servers
- Cloud Gateways

Step 6. Review Connection Settings

At the **Summary** step of the wizard, review the connection details and click **Finish**.



Keep in mind that it may take a while for Veeam ONE to collect and display configuration and performance data for the newly added backup server and managed backup infrastructure components.

- After you connect a Veeam Backup & Replication server, Veeam ONE imports all historical data that is stored on the backup server.
- After you connect a Veeam Backup Enterprise Manager server, Veeam ONE automatically builds the hierarchy of all managed backup servers. Next, it connects managed backup servers and imports from these servers data on job sessions.

Connecting Veeam Backup for Microsoft 365 Servers

To collect data about your Veeam Backup for Microsoft 365 infrastructure and data protection operations, you must configure connections to Veeam Backup for Microsoft 365 servers in Veeam ONE Web Client.

> **NOTE:**
> - Before you connect a Veeam Backup for Microsoft 365 server to Veeam ONE check that product licenses are compatible. For details on license compatibility, see Compatibility with Veeam Backup for Microsoft 365 Licenses.
> - Veeam ONE monitors cloud Organizations protection only, monitoring of hybrid and on-premise (Exchange) platform protection is not supported.

To configure a connection to a Veeam Backup for Microsoft 365 server, take the following steps.

Step 1. Launch Data Source Wizard

To launch the **Add Server** wizard:

1. Open Veeam ONE Web Client.

   For details on accessing Veeam ONE components, see Veeam ONE Web Client.

2. At the top right corner of the Veeam ONE Web Client window, click **Configuration**.
3. In the **Data Collection** section of the configuration menu, click **Data source**.
4. Click **Add server**.

You can also launch the **Add Server** wizard from Veeam ONE Client, to do so:

1. Open Veeam ONE Client.

   For details on accessing Veeam ONE components, see Veeam ONE Client.

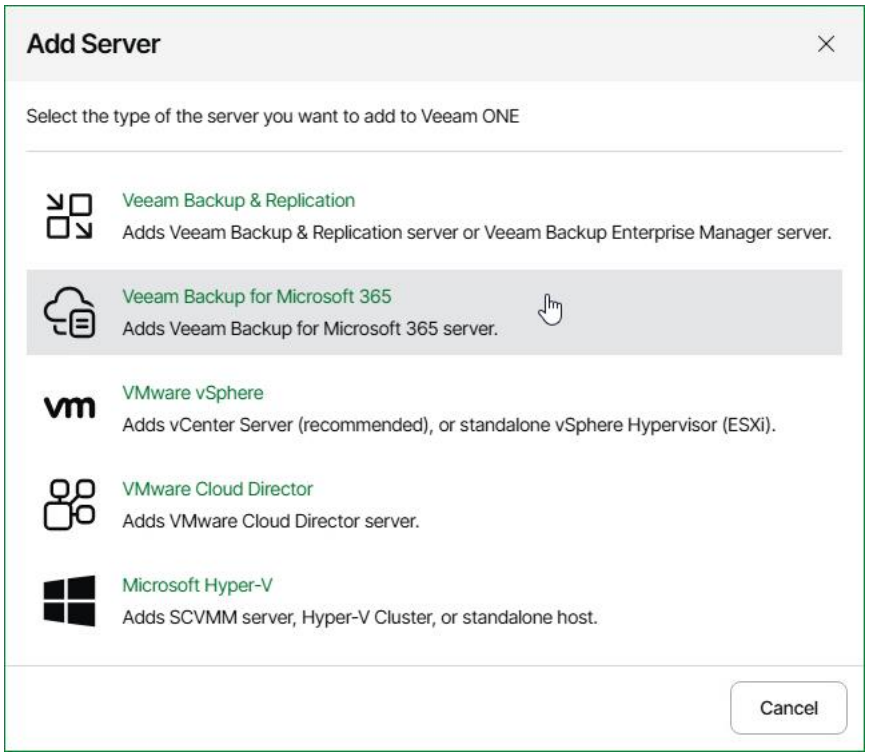
2. In the main menu, click **Add Server**. You will be redirected to Veeam ONE Web Client to follow the wizard steps.

Alternatively, to access the **Add Server** wizard from Veeam ONE Client you can:

- Press [CTRL+I] on the keyboard.
- At the bottom of the inventory pane, open the **Veeam Backup for Microsoft 365** view, right-click the **Veeam Backup for Microsoft 365** node and choose **Add Server** from the shortcut menu.

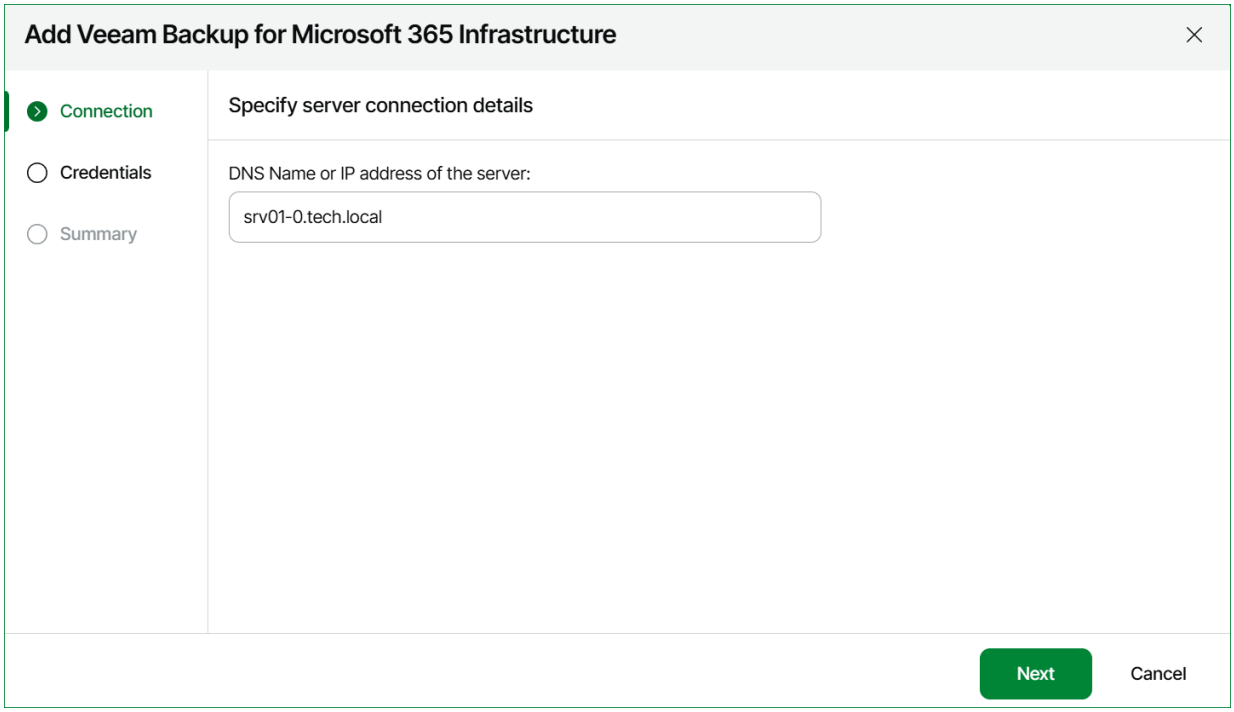
Step 2. Choose Server Type

At the first step of the wizard, click **Veeam Backup for Microsoft 365**.



Step 3. Specify Server Name

At the **Connection** step of the wizard, enter DNS or IP address of the Veeam Backup for Microsoft 365 server that you want to connect.



Step 4. Specify Credentials

At the **Credentials** step of the wizard:

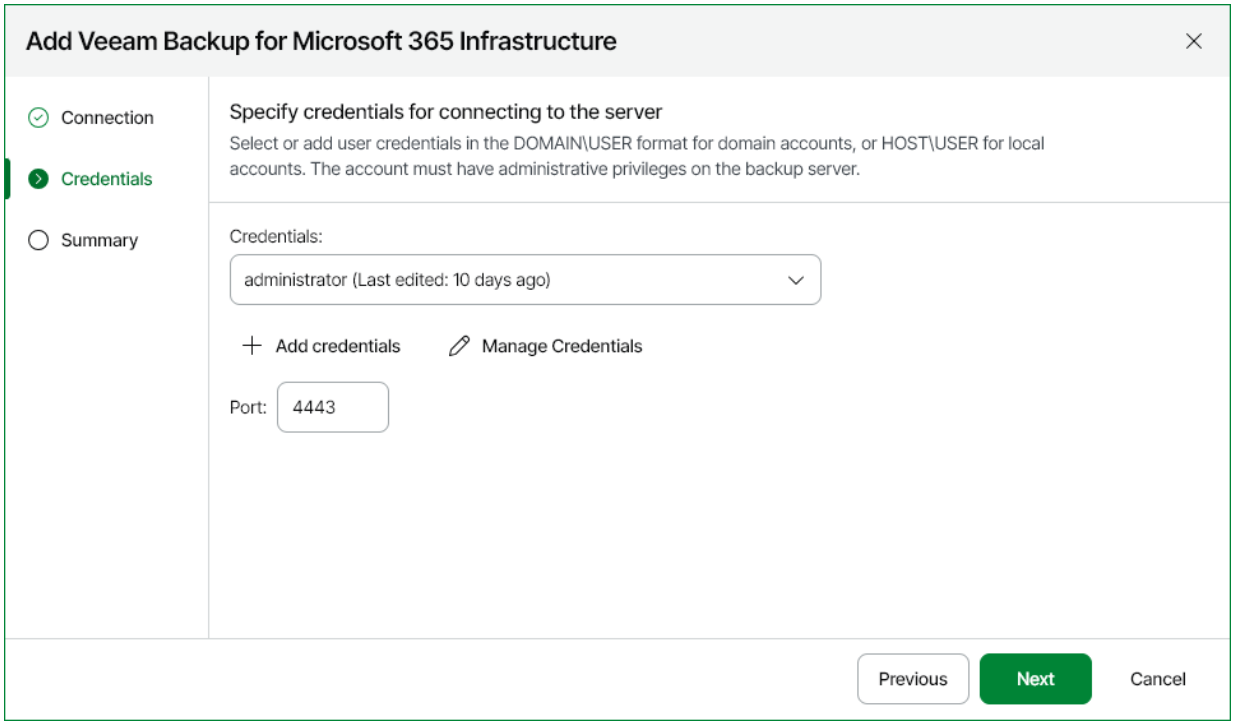
1. Click **Add credentials** and specify credentials of the user account for connecting to the server.

   For details on adding credentials records, see Security.

   For details on permissions required to connect to Veeam Backup for Microsoft 365, see Connection to Veeam Backup for Microsoft 365 Servers.

2. Change the port number if required.

   By default, port 4443 is used for communication with Veeam Backup for Microsoft 365 servers.

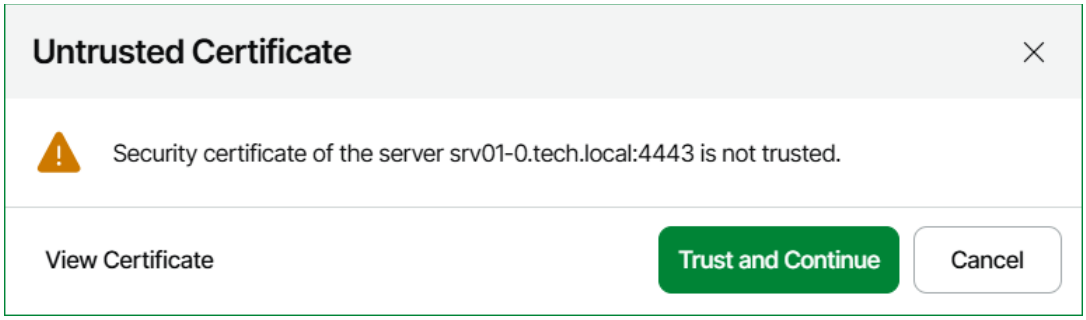


3. When you add a Veeam Backup for Microsoft 365 server, Veeam ONE saves to the configuration database a thumbprint of the TLS certificate installed on the server. During every subsequent connection to the server, Veeam ONE uses the saved thumbprint to verify the server identity and avoid the man-in-the-middle attack.

   If the certificate installed on the server is not trusted, Veeam ONE displays a warning.

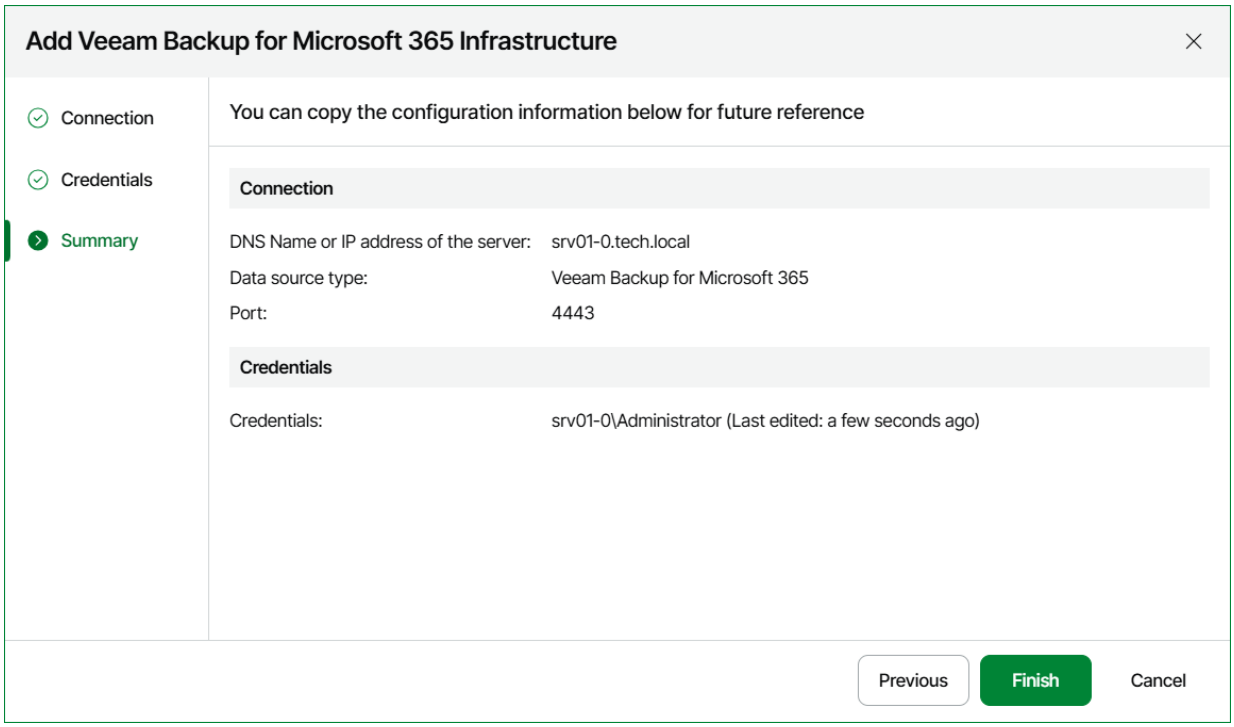
   - To view detailed information about the certificate, click **View Certificate**.
   - If you trust the server, click **Trust and Continue**.

- If you do not trust the server, click **Cancel**. Veeam ONE will display an error message, and you will not be able to connect to the server.



Step 5. Review Connection Settings

At the **Summary** step of the wizard, review the connection details and click **Finish**.



Keep in mind that it may take a while for Veeam ONE to collect and display configuration and performance data for the newly added Veeam Backup for Microsoft 365 server and managed backup infrastructure components. The approximate collection rate is around 600 000 protected Microsoft 365 objects per hour.

Connecting VMware vSphere Servers

To collect data about VMware vSphere infrastructure objects, you must configure connections to infrastructure servers in Veeam ONE Web Client. You can connect the following types of servers:

- vCenter Servers
- Standalone ESXi hosts

To configure a connection to a VMware vSphere server, take the following steps.

Step 1. Launch Data Source Wizard

To launch the **Add Server** wizard:

1. Open Veeam ONE Web Client.

   For details on accessing Veeam ONE components, see Veeam ONE Web Client.

2. At the top right corner of the Veeam ONE Web Client window, click **Configuration**.
3. In the **Data Collection** section of the configuration menu, click **Data source**.
4. Click **Add server**.

You can also launch the **Add Server** wizard from Veeam ONE Client, to do so:

1. Open Veeam ONE Client.

   For details on accessing Veeam ONE components, see Veeam ONE Client.

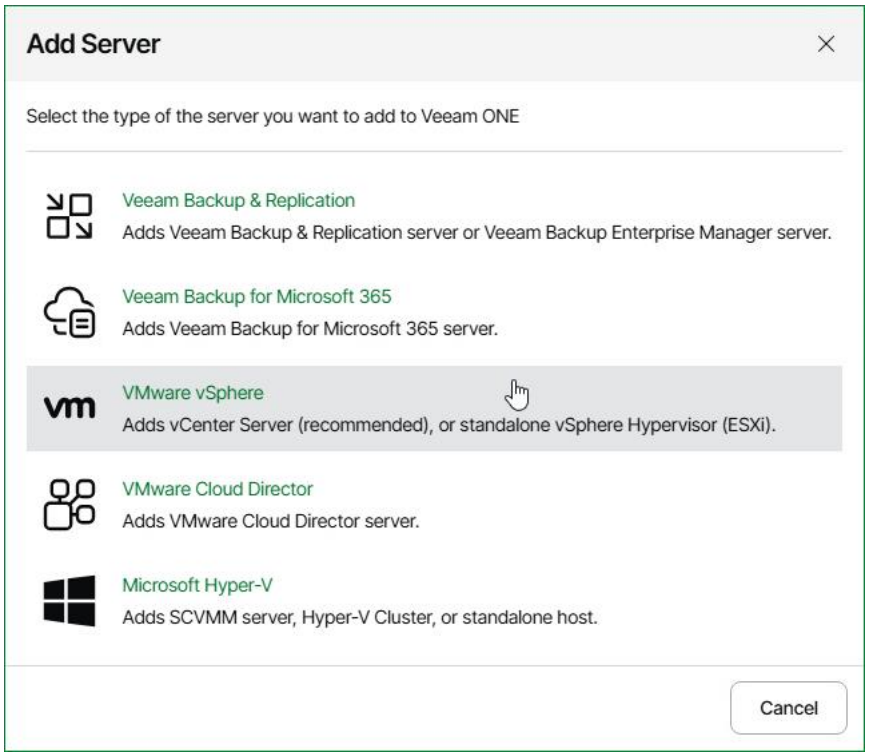
2. In the main menu, click **Add Server**. You will be redirected to Veeam ONE Web Client to follow the wizard steps.

Alternatively, to access the **Add Server** wizard from Veeam ONE Client you can:

- Press [CTRL+I] on the keyboard.
- At the bottom of the inventory pane, open the **Virtual Infrastructure** view, right-click the **Virtual Infrastructure** node and choose **Add Server** from the shortcut menu.

Step 2. Choose Server Type

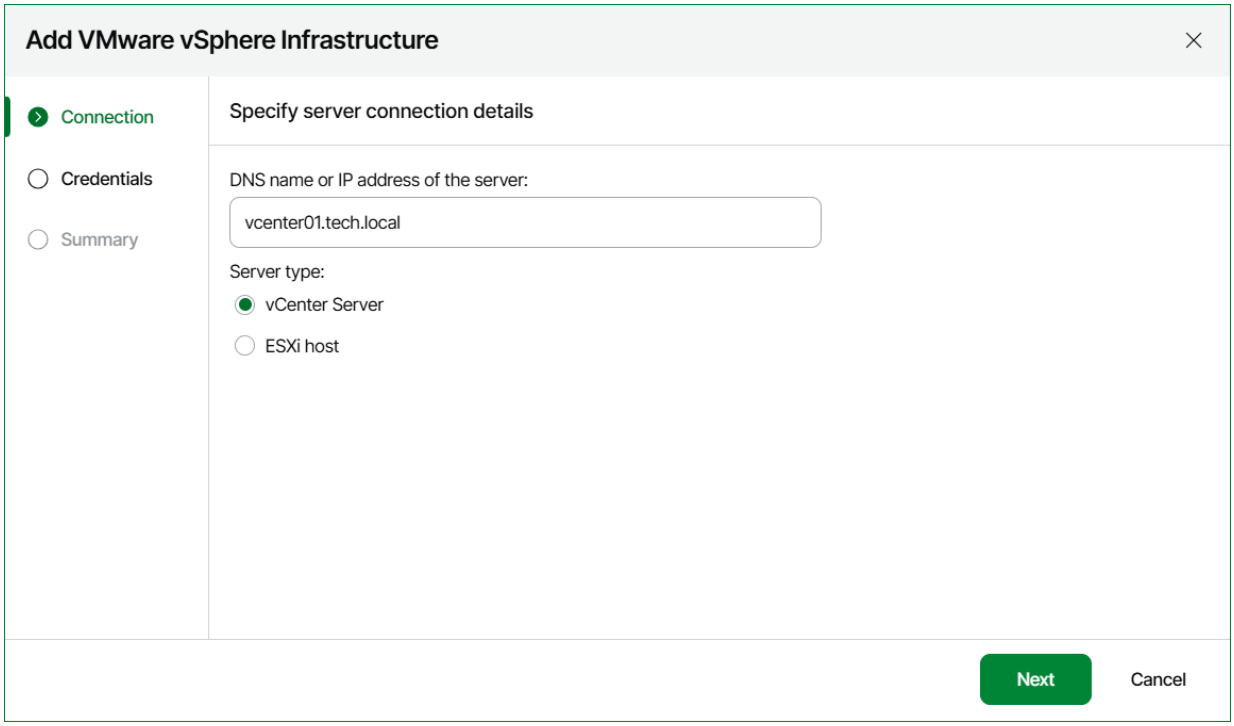
At the first step of the wizard, click **VMware vSphere**.



Step 3. Specify Server Name and Role

At the **Connection** step of the wizard:

1. Specify DNS name or IP address of the server that you want to connect.
2. Specify the server role — vCenter Server or a standalone ESXi host.



Step 4. Specify Credentials

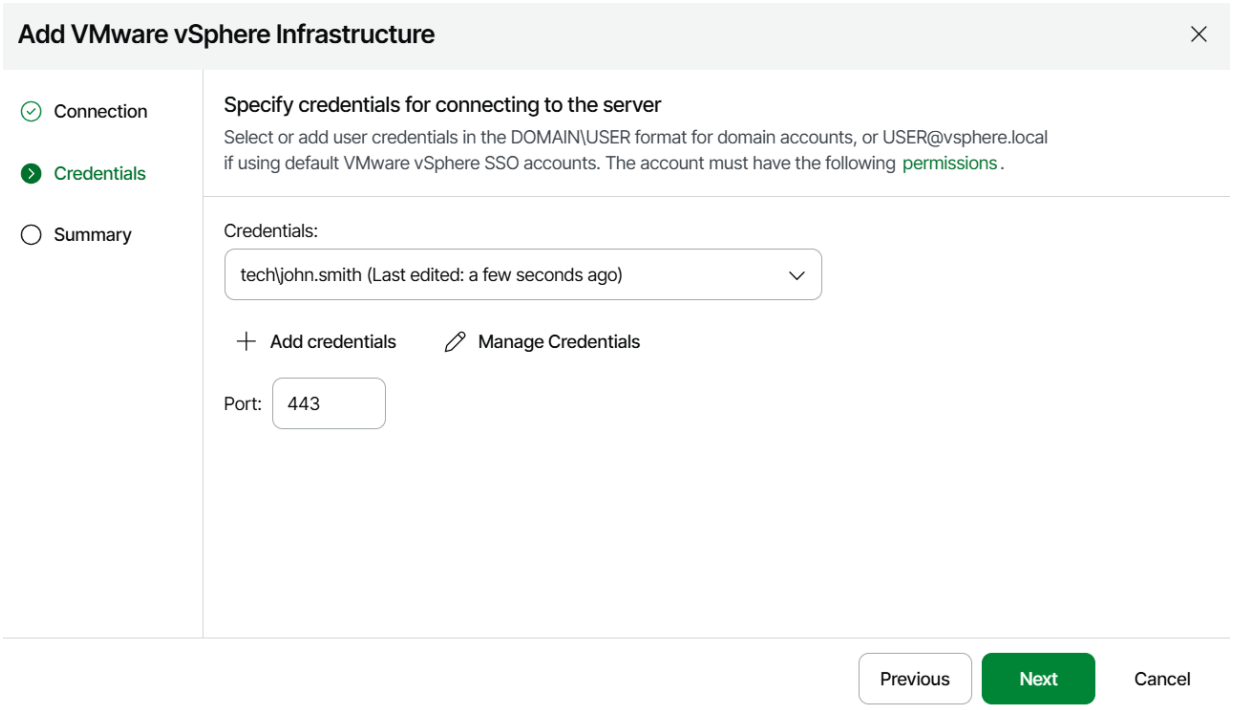
At the **Credentials** step of the wizard:

1. Click **Add credentials** and specify credentials of the user account for connecting to the server.

   For details on adding credentials records, see Security. For details on account permissions, see VMware vSphere Servers.

2. Change the port number if required.

   By default, port 443 is used for communication with VMware vSphere servers.



3. When you add a vCenter Server or ESXi host, Veeam ONE saves to the configuration database a thumbprint of the TLS certificate installed on the vCenter Server or ESXi host. During every subsequent connection to the server, Veeam ONE uses the saved thumbprint to verify the server identity and avoid the man-in-the-middle attack.

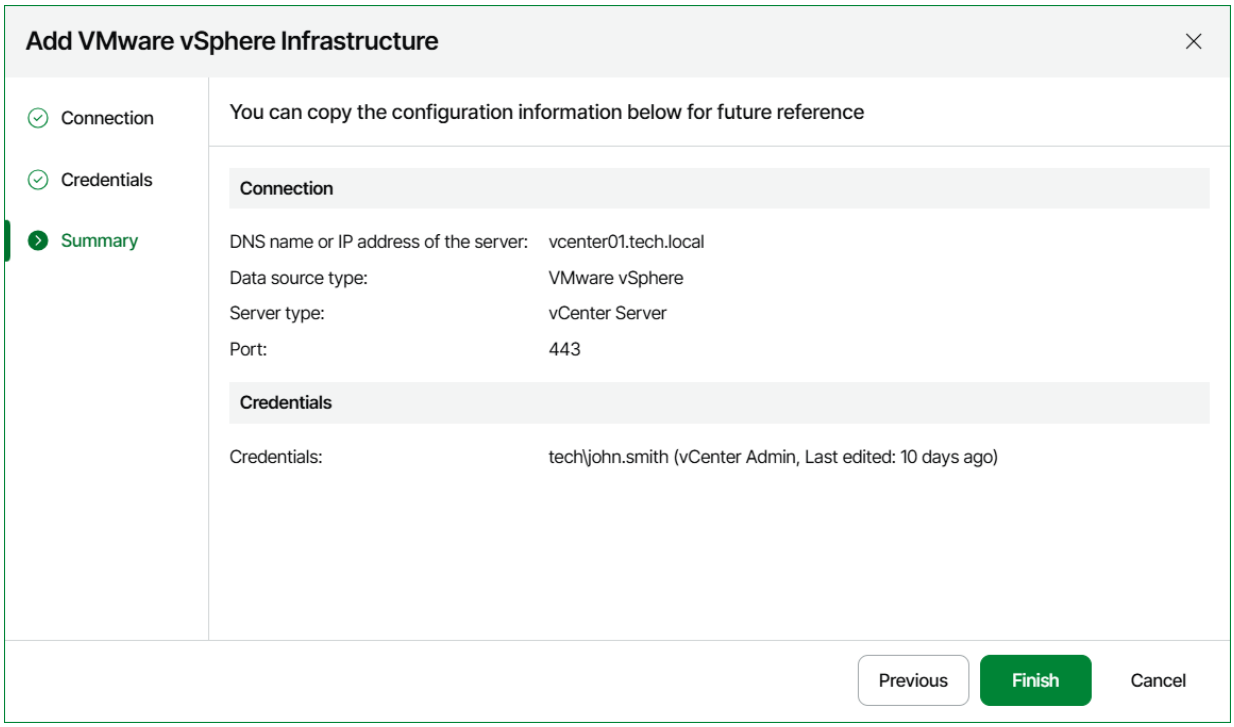
   If the certificate installed on the server is not trusted, Veeam ONE displays a warning.

   - To view detailed information about the certificate, click **View Certificate**.
   - If you trust the server, click **Trust and Continue**.
   - If you do not trust the server, click **Cancel**. Veeam ONE will display an error message, and you will not be able to connect to the server.

Step 5. Review Connection Settings

At the **Summary** step of the wizard, review the connection details and click **Finish**.

Note that it may take a while for Veeam ONE to collect and display data for the connected server and its child objects.



Step 6. Specify VM Guest OS Credentials

After you connect one or more VMware vSphere servers, you must specify credentials of an account that will be used to collect data from Windows-based guest OSes on VMs. If you do not specify guest OS credentials, Veeam ONE will use connection credentials to display guest OS data in monitoring dashboards, alarms and reports.

You can specify the account credentials for VM guest OS at the following levels of the VMware vSphere infrastructure:

- VMware vSphere infrastructure
- VM containers, such as hosts and clusters
- Individual VMs

If you specify guest OS account credentials at multiple levels, Veeam ONE will use the following order of priority: VM > VM containers > VMware vSphere infrastructure. For example, if account credentials are specified both at the VM and VM container level, Veeam ONE will collect guest OS data using an account set at the VM level.

Specifying Account Credentials for VMware vSphere Infrastructure

You can specify account credentials at the level of the VMware vSphere infrastructure. Veeam ONE will use this account to connect to all VMs running on VMware vSphere hosts unless you specify other credentials for specific VMs or VM containers.

To specify account credentials for all VMs in the VMware vSphere infrastructure:

1. Open Veeam ONE Client.
2. In the main menu, click **Settings** and select **Server Settings**.

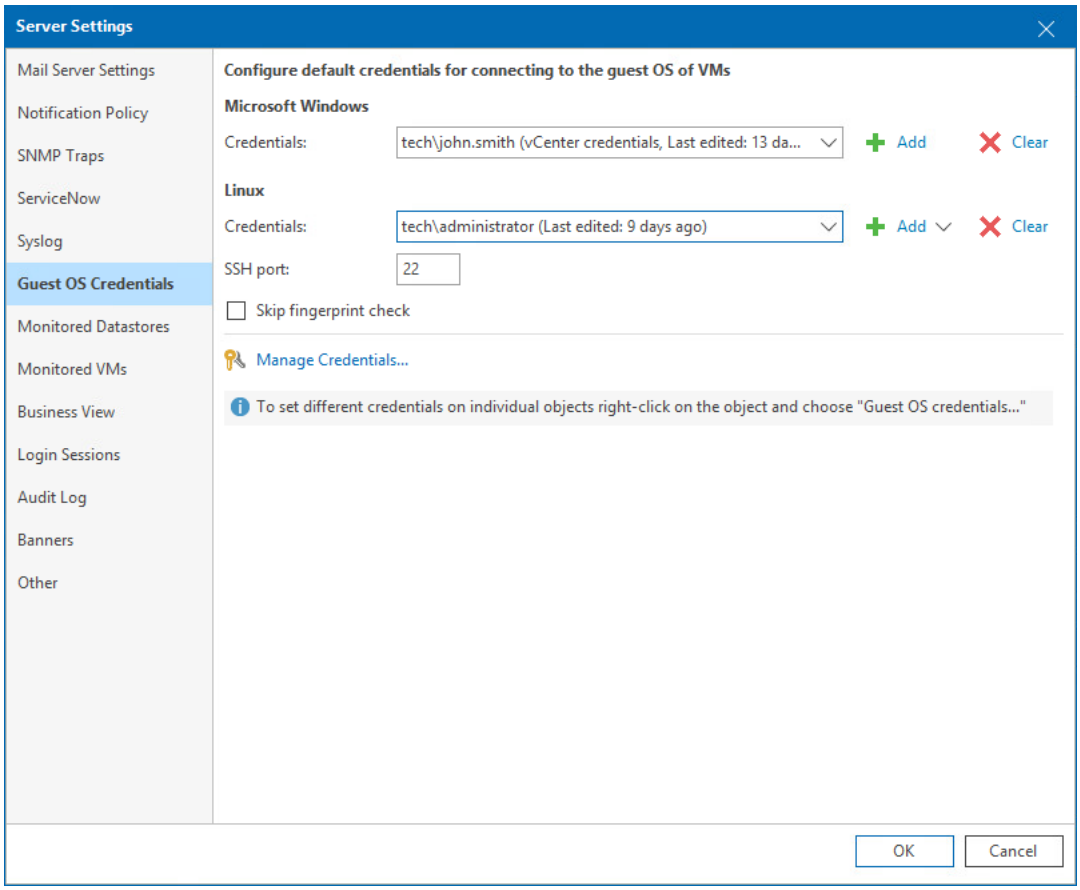
   Alternatively, press the `[CTRL+S]` on the keyboard.
3. In the **Server Settings** window, open the **Guest OS Credentials** tab.
4. Specify guest OS credentials:
   - In the **Microsoft Windows** section, select credentials of an account that will be used to collect data from the guest OS of Windows-based VMs. To create a new credentials record, click **Add**.
   - In the **Linux** section, select credentials of an account that will be used to collect data from the guest OS of Linux-based VMs. To create a new credentials record, click **Add** and select **Standard account** or **Linux private key**.

     In the **SSH port** field, change the default connection port if required.

     To disable fingerprint validation for Linux VMs, select **Skip fingerprint check**.

   To access credentials manager, click the **Manage Credentials** link. For more information on working with credentials, see Security.

5. Click **OK**.



Specifying Account Credentials for Containers and VMs

You can specify account credentials at the level of specific VMs or VM containers. This can be helpful if an account specified at the level of the VMware vSphere infrastructure does not have enough permissions on specific VMs or VM containers.

To specify account credentials for individual VMs or VM containers:

1. Open Veeam ONE Client.
2. At the bottom of the inventory pane, click **Virtual Infrastructure**.
3. Right-click the necessary VM and select **Guest OS Credentials** from the shortcut menu.
4. In the **Guest OS Credentials** window, specify credentials of a Windows or Linux account that will be used to collect guest OS data from VMware vSphere VMs.
5. Select **Propagate credentials to child objects** to use the specified account credentials to connect to child objects of a container.
6. Click **OK**.

Connecting VMware Cloud Director Servers

To collect data about VMware Cloud Director infrastructure objects, you must configure connections to VMware Cloud Director servers in Veeam ONE Web Client.

To configure a connection to a VMware Cloud Director server, take the following steps.

Step 1. Launch Data Source Wizard

To launch the **Add Server** wizard:

1. Open Veeam ONE Web Client.

   For details on accessing Veeam ONE components, see Veeam ONE Web Client.

2. At the top right corner of the Veeam ONE Web Client window, click **Configuration**.
3. In the **Data Collection** section of the configuration menu, click **Data source**.
4. Click **Add server**.

You can also launch the **Add Server** wizard from Veeam ONE Client, to do so:

1. Open Veeam ONE Client.

   For details on accessing Veeam ONE components, see Veeam ONE Client.

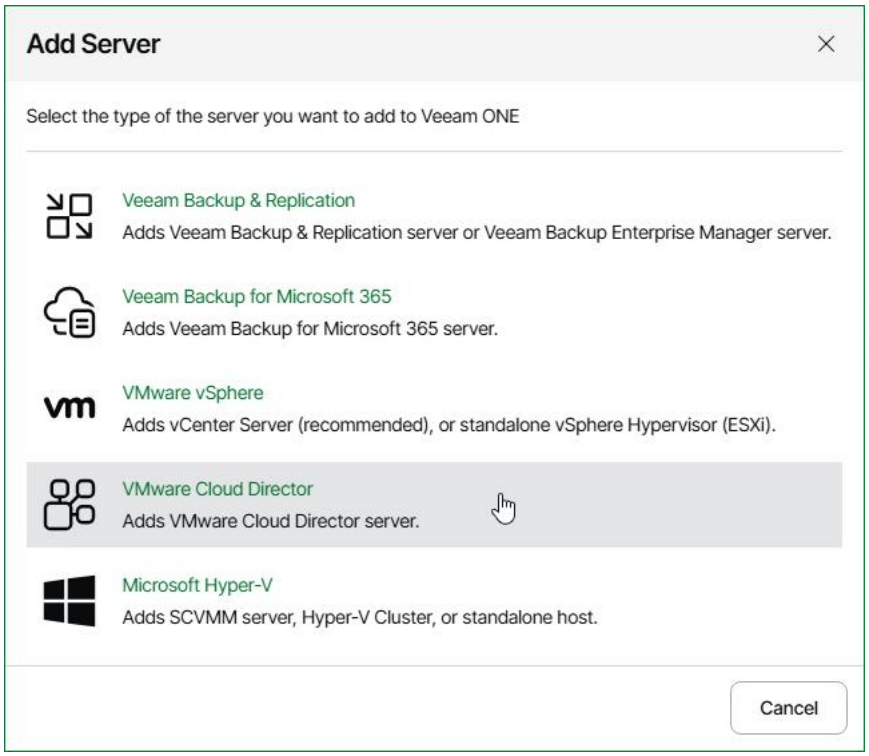
2. In the main menu, click **Add Server**. You will be redirected to Veeam ONE Web Client to follow the wizard steps.

Alternatively, to access the **Add Server** wizard from Veeam ONE Client you can:

- Press [CTRL+I] on the keyboard.

Step 2. Choose Server Type

At the first step of the wizard, click **VMware Cloud Director**.

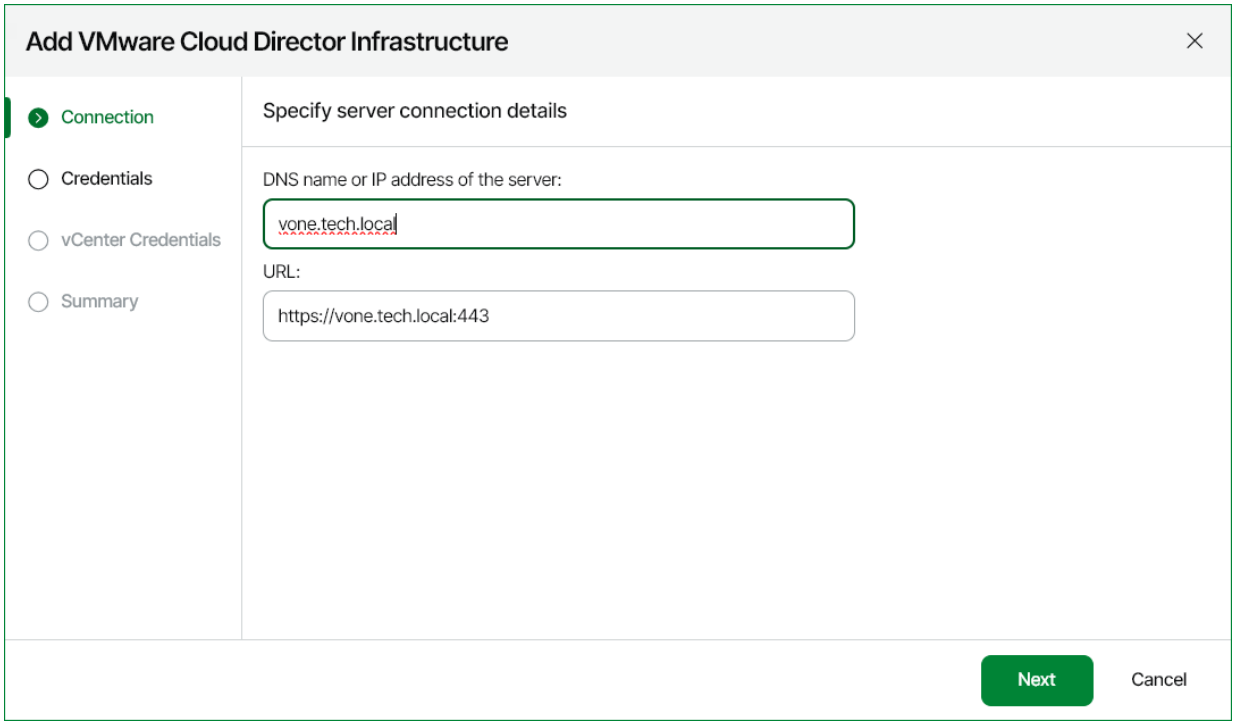


Step 3. Specify Server Name

At the **Connection** step of the wizard:

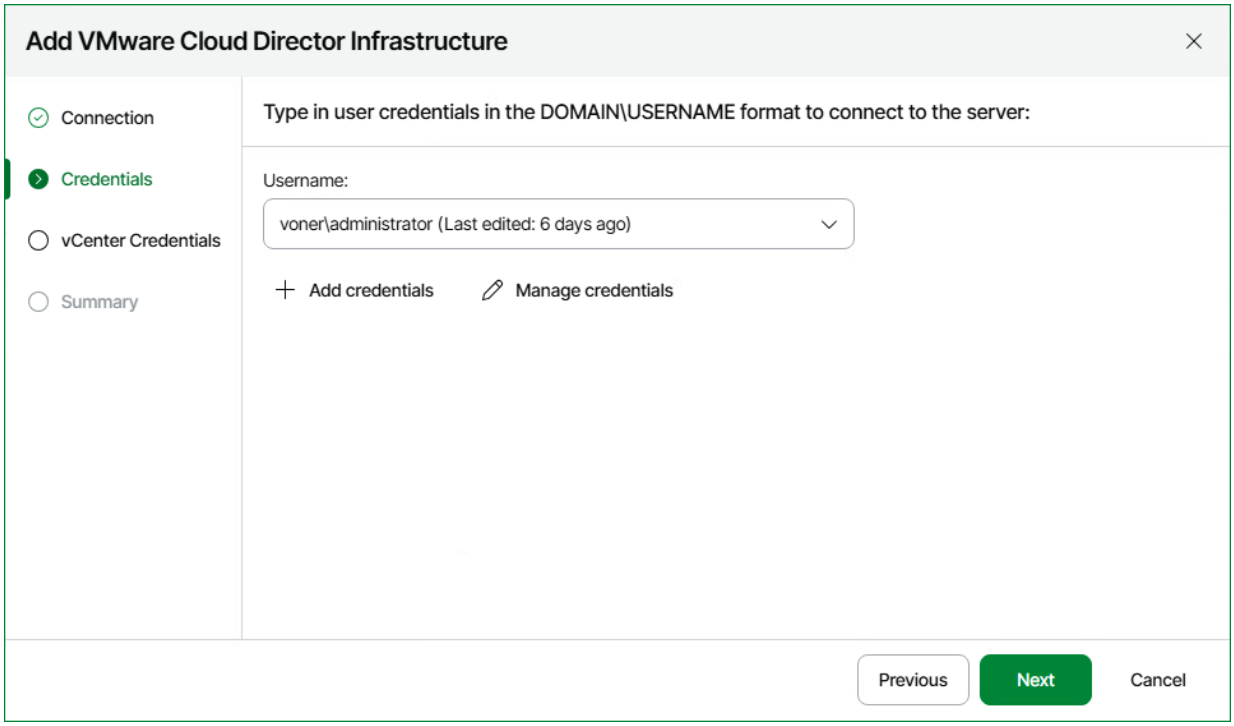
1. Enter DNS or IP address of the VMware Cloud Director server that you want to connect.
2. Change VMware Cloud Director URL if required.

   Veeam ONE populates the **URL** field with a URL used for connecting to the VMware Cloud Director server. The URL format is `https://<vcdservername>:443`, where `<vcdservername>` is the DNS name or IP address of the VMware Cloud Director server, and 443 is the default port. If you use port number other than `443`, you can change it in the **URL** field.



Step 4. Specify Credentials for VMware Cloud Director

At the **Credentials** step of the wizard, click **Add credentials** and specify credentials of the user account for connecting to VMware Cloud Director. For details on adding credentials records, see Security.



3. When you add a VMware Cloud Director host, Veeam ONE saves to the configuration database a thumbprint of the TLS certificate installed on the VMware Cloud Director host and all vCenter servers under it. During every subsequent connection to the server, Veeam ONE uses the saved thumbprint to verify the server identity and avoid the man-in-the-middle attack.

   If the certificate installed on the server is not trusted, Veeam ONE displays a warning.

   - To view detailed information about the certificate, click **View Certificate**.
   - If you trust the server, click **Trust and Continue**.
   - If you do not trust the server, click **Cancel**. Veeam ONE will display an error message, and you will not be able to connect to the server.

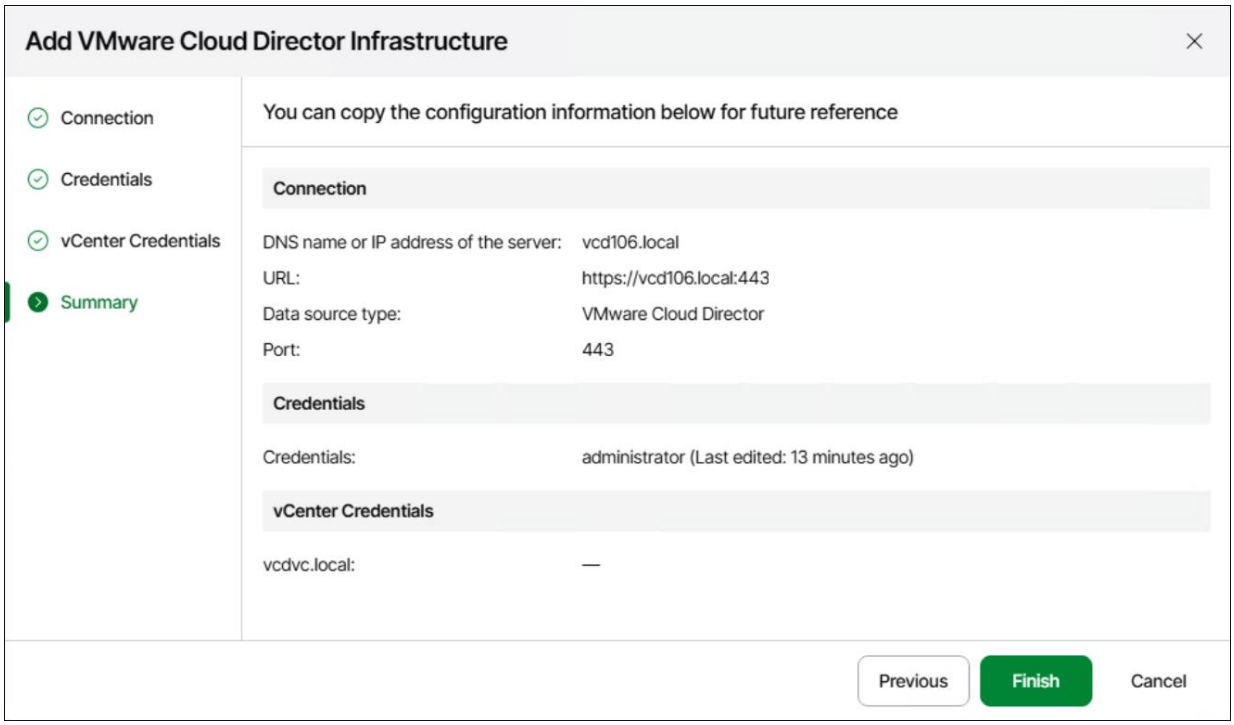
Step 5. Specify Credentials for Underlying vCenter Servers

At the **vCenter Credentials** step of the wizard, specify credentials for each vCenter Server attached to VMware Cloud Director. By default, Veeam ONE uses the same credentials that you have specified at the Credentials step of the wizard. However, if the underlying vCenter Servers must be connected under another user account, you can set the credentials for each vCenter Server manually:

1. Select the necessary vCenter Server in the list.
2. Click **Set User** and specify credentials to connect to the vCenter Server.
3. Repeat steps 1-2 for all vCenter Servers attached to VMware Cloud Director.
4. To test if connection settings are configured correctly, click the **Check Connection** button. Veeam ONE will attempt to establish connection with the vCenter Servers using the provided credentials.

Step 6. Review Connection Settings

At the **Summary** step of the wizard, review the connection details and click **Finish**.



The VMware Cloud Director hierarchy will become available in the VMware Cloud Director view. Note that it may take a while for Veeam ONE to collect and display data for the newly added VMware Cloud Director and its child objects.

When you connect VMware Cloud Director, Veeam ONE also connects underlying vCenter Servers and initiates data import. vCenter Servers become available on the Data Collection Overview page and in the Infrastructure View, and you can work with them as with regular VMware vSphere infrastructure servers. If the vCenter Server attached to VMware Cloud Director is already connected, Veeam ONE will only create an association between the VMware Cloud Director hierarchy and the vCenter Server.

Connecting Microsoft Hyper-V Servers

To collect data about Microsoft Hyper-V infrastructure objects, you must configure connections to Microsoft Hyper-V servers in Veeam ONE Web Client. You can connect the following types of servers:

- SCVMM server
- Failover clusters
- Standalone Hyper-V hosts

> **NOTE:**
>
> If you plan to connect an SCVMM server, make sure that SCVMM Admin Console is installed on the machine where you installed the Veeam ONE Server component. The version of the SCVMM Admin Console must be the same as the version of SCVMM server you are adding. For details, see System Requirements.

To configure a connection to a Microsoft Hyper-V server, take the following steps.

Step 1. Launch Data Source Wizard

To launch the **Add Server** wizard:

1. Open Veeam ONE Web Client.

   For details on accessing Veeam ONE components, see Veeam ONE Web Client.

2. At the top right corner of the Veeam ONE Web Client window, click **Configuration**.
3. In the **Data Collection** section of the configuration menu, click **Data source**.
4. Click **Add server**.

You can also launch the **Add Server** wizard from Veeam ONE Client, to do so:

1. Open Veeam ONE Client.

   For details on accessing Veeam ONE components, see Veeam ONE Client.

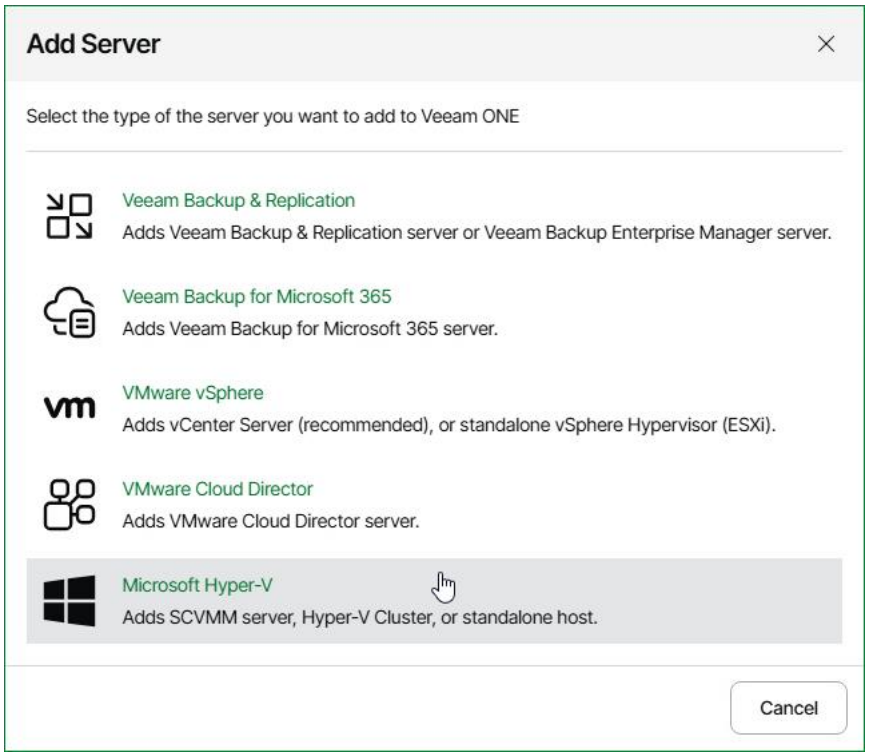
2. In the main menu, click **Add Server**. You will be redirected to Veeam ONE Web Client to follow the wizard steps.

Alternatively, to access the **Add Server** wizard from Veeam ONE Client you can:

- Press [CTRL+I] on the keyboard.
- At the bottom of the inventory pane, open the **Virtual Infrastructure** view, right-click the **Virtual Infrastructure** node and choose **Add Server** from the shortcut menu.

Step 2. Choose Server Type

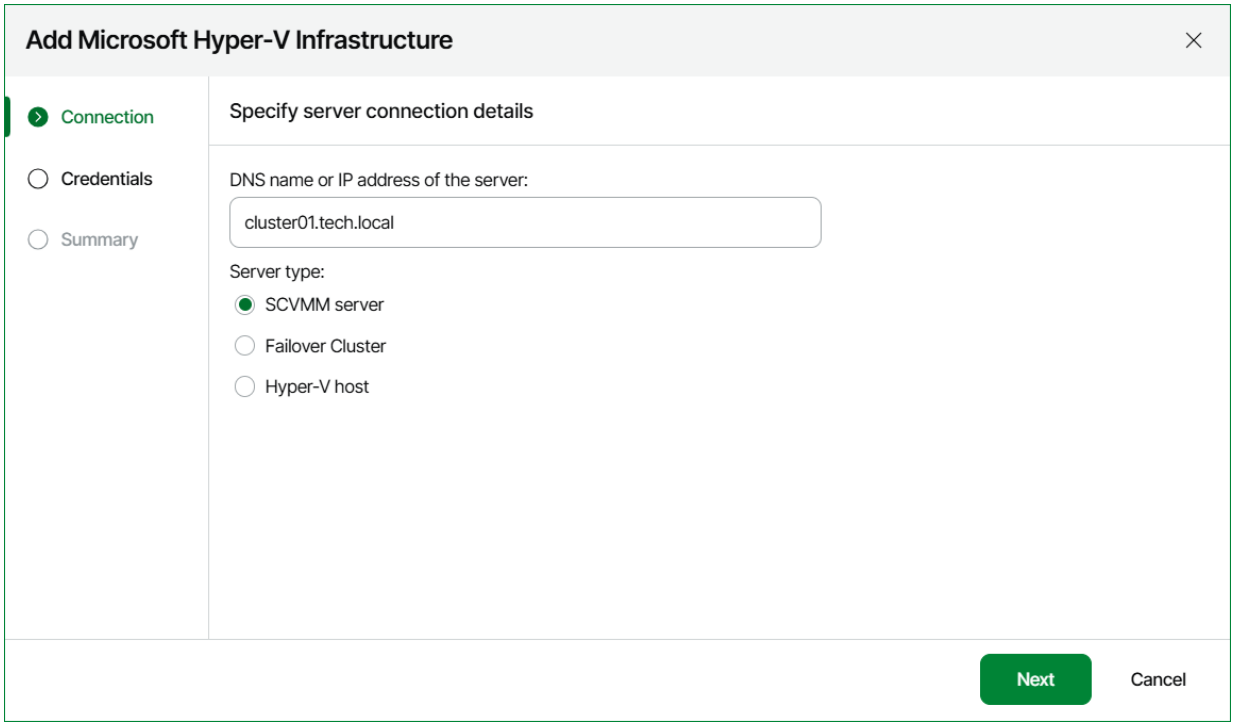
At the first step of the wizard, click **Microsoft Hyper-V**.



Step 3. Specify Server Name and Role

At the **Connection** step of the wizard:

1. Enter DNS name or IP address of the server that will be connected to Veeam ONE.
2. Specify the server type — SCVMM server, failover cluster or standalone host.



Step 4. Specify Credentials

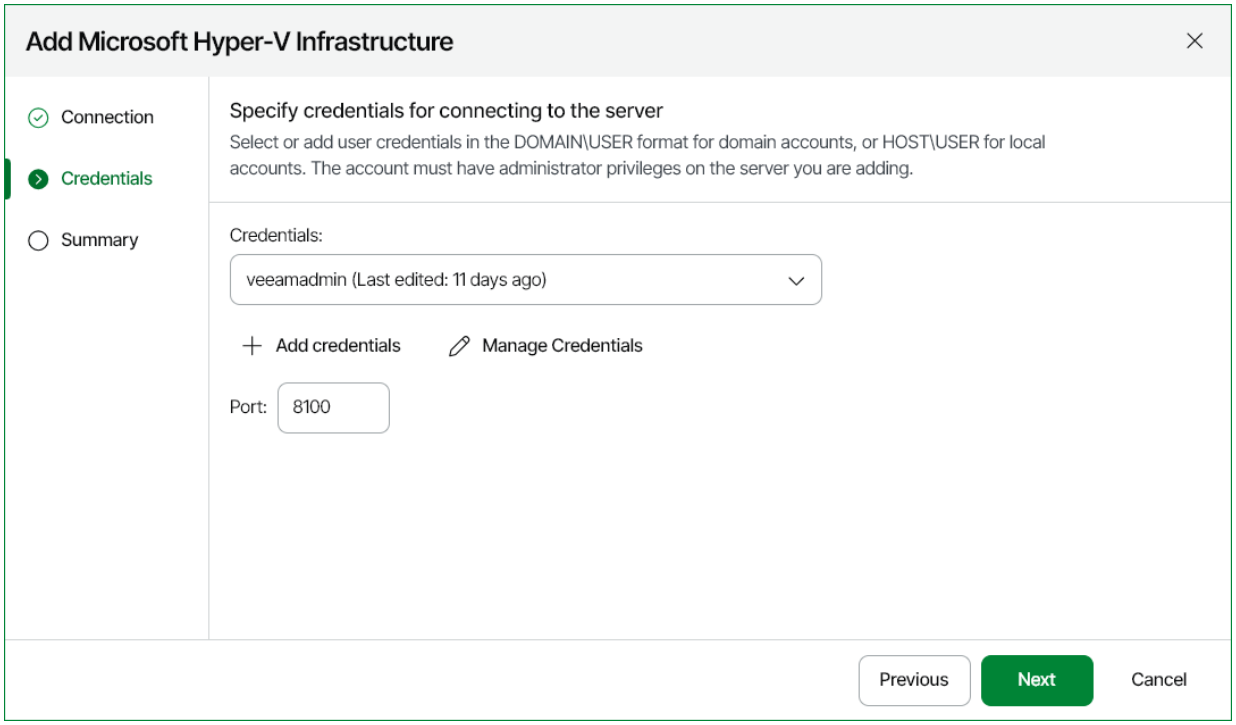
At the **Credentials** step of the wizard:

1. Click **Add credentials** and specify credentials of the user account for connecting to the server.

   For details on adding credentials records, see Security.

2. [For SCVMM connection] Change the port number if required.

   By default, port `8100` is used as the VMM Administrator Console to VMM server port.



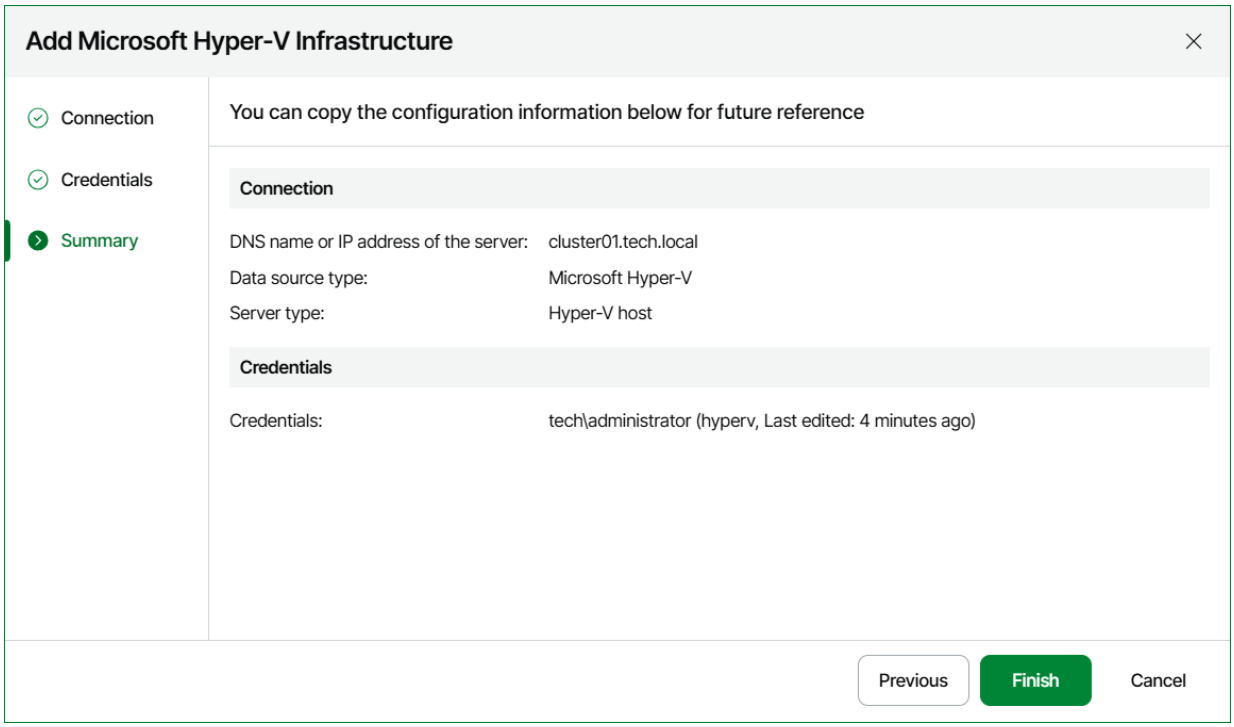
> **NOTE**
>
> VM guest OS credentials are specified in **Server Settings**.

For details, see Step 6. Specify VM Guest OS Credentials.

Step 5. Review Connection Settings

At the **Summary** step of the wizard, review the connection details and click **Finish**.

Note that it may take a while for Veeam ONE to collect and display the collected data for the newly added SCVMM server, failover cluster or host and its child objects.



Step 6. Specify VM Guest OS Credentials

After you connect one or more Microsoft Hyper-V servers, you must specify credentials of an account that will be used to collect data from Windows-based guest OSes on VMs. If you do not specify guest OS credentials, Veeam ONE will use connection credentials to display guest OS data (in particular, data about guest disks) in monitoring dashboards, alarms and reports.

You can specify the account credentials for VM guest OS at the following levels of the Microsoft Hyper-V infrastructure:

- Microsoft Hyper-V infrastructure
- VM containers, such as hosts and clusters
- Individual VMs

If you specify guest OS account credentials at multiple levels, Veeam ONE will use the following order of priority: VM > VM container > Microsoft Hyper-V infrastructure. For example, if account credentials are specified both at the VM and VM container level, Veeam ONE will collect guest OS data using an account set at the VM level.

Specifying Account Credentials for Microsoft Hyper-V Infrastructure

You can specify account credentials at the level of the Microsoft Hyper-V infrastructure. Veeam ONE will use this account to connect to all VMs running on Microsoft Hyper-V hosts unless you specify other credentials for specific VMs or VM containers.

To specify account credentials for all VMs in the Microsoft Hyper-V infrastructure:

1. Open Veeam ONE Client.
2. In the main menu, click **Settings** and select **Server Settings**.

   Alternatively, press the `[CTRL+S]` on the keyboard.
3. In the **Server Settings** window, open the **Guest OS Credentials** tab.
4. Specify guest OS credentials:
   - In the **Microsoft Windows** section, select credentials of an account that will be used to collect data from the guest OS of Windows-based VMs. To create a new credentials record, click **Add**.

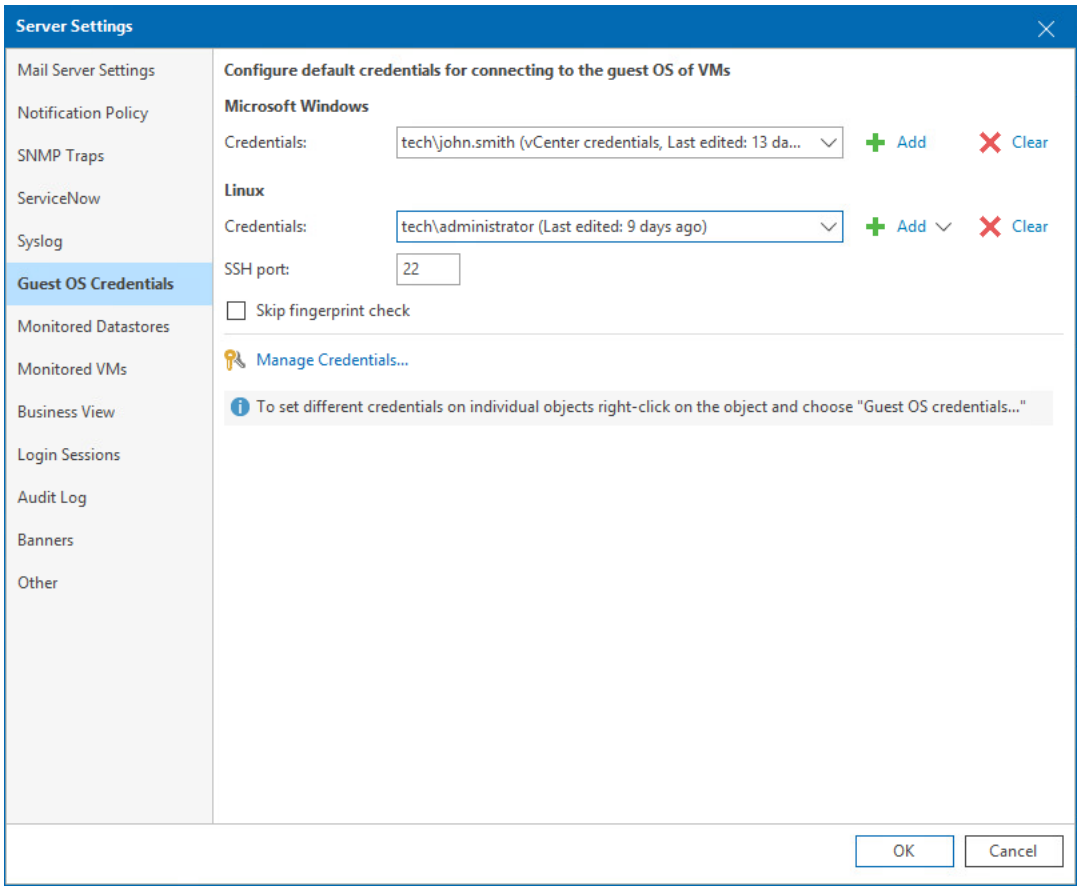
     For details on requirements to the account, see Connection to VM Guest OS.
   - In the **Linux** section, select credentials of an account that will be used to collect data from the guest OS of Linux-based VMs. To create a new credentials record, click **Add** and select **Standard account** or **Linux private key**.

     In the **SSH port** field, change the default connection port if required.

     To disable fingerprint validation for Linux VMs, select **Skip fingerprint check**.

   To access credentials manager, click the **Manage Credentials** link. For more information on working with credentials, see Security.

5. Click **OK**.



Specifying Account Credentials for Containers and VMs

You can specify account credentials at the level of specific VMs or VM containers. This can be helpful if an account specified at the level of the Microsoft Hyper-V infrastructure does not have enough permissions on specific VMs or VM containers.

To specify account credentials for individual VMs or VM containers:

1. Open Veeam ONE Client.
2. At the bottom of the inventory pane, click **Virtual Infrastructure**.
3. Right-click the necessary VM or VM container and select **Guest OS Credentials** from the shortcut menu.
4. In the **Guest OS Credentials** window, select the **Use these credentials** option and specify credentials of an account that will be used to collect guest OS data from Microsoft Hyper-V VMs.
5. Click **OK**.

Changing Server Connection Settings

In some situations, you might need to change connection settings for a monitored server. Consider the following examples:

- If you need to reconnect a server with another user name and/or password, you can change connection settings for this server.

- If the account you provided for a Veeam backup server does not have sufficient permissions to collect data from all backup infrastructure components, you can set custom connection settings for specific servers in your backup infrastructure.

To change connection settings for a server:

1. Open Veeam ONE Web Client.
2. At the top right corner of the Veeam ONE Web Client window, click **Configuration**.
3. In the **Data Collection** section of the configuration menu, select your server name.

   To narrow down the list, you can either search or apply the following filters:

   - In the **Status** field specify the current operational state of the platform.
   - In the **Platform type** field specify the type of platform in use.
   - In the **Veeam Analytics service state** field specify whether the Veeam Analytics service is running, stopped, or in another state.
4. Click **Data source**.
5. Click **Connection settings**.
6. Edit the user name, enter the password and/or change the port number (if applicable).
7. (Optional) If you want to enable Veeam ONE dashboard and report integration in Veeam Backup & Replication, select the **Allow Veeam Backup & Replication to display analytics data** check box. For details, see Veeam Backup & Replication Web UI.

You can also change connection settings for a server from Veeam ONE Client, to do so:

1. Open Veeam ONE Client.
2. At the bottom of the inventory pane, click **Veeam Backup & Replication**, **Veeam Backup for Microsoft 365**, **Virtual Infrastructure** or **VMware Cloud Director**.
3. In the inventory pane, right-click the server and choose **Connection Settings** from the shortcut menu.
4. Edit the user name, enter the password and/or change the port number (if applicable).
5. (Optional) If you want to enable Veeam ONE dashboard and report integration in Veeam Backup & Replication, select the **Allow Veeam Backup & Replication to display analytics data** check box.

NOTE:

When changing connection settings, mind the following:

- When you change connection settings for a virtualization server, Veeam ONE disconnects the server and re-connects it with the new settings. When a virtual server is disconnected, previously discovered VMs remain available in the inventory tree. After the server is re-connected, its performance data will be updated. If the connection is not restored, only the history of performance data will be available in Veeam ONE.
- When you change connection settings for a backup server in the Veeam Backup Enterprise Manager hierarchy, a new job is automatically configured in Veeam ONE Reporting Sevice to collect data from this backup server.

Removing Server Connections

If you no longer want to monitor a virtualization or a backup server, you can remove a connection to it in Veeam ONE Client.

To change connection settings for a server:

1. Open Veeam ONE Web Client.
2. At the top right corner of the Veeam ONE Web Client window, click **Configuration**.
3. In the **Data Collection** section of the configuration menu, select your server name.

   To narrow down the list of servers, you can either search or apply the following filters:

   - In the **Status** field specify the current operational state of the platform.
   - In the **Platform type** field specify the type of platform in use.
   - In the **Veeam Analytics service state** field specify whether the Veeam Analytics service is running, stopped, or in another state.
4. Click **Data source**.
5. Click **Remove server**.

You can also remove data sources from Veeam ONE Client, to do so:

1. Open Veeam ONE Client.
2. At the bottom of the inventory pane, click **Veeam Backup & Replication**, **Veeam Backup for Microsoft 365**, **Virtual Infrastructure** or **VMware Cloud Director**.
3. In the inventory pane, right-click the server you want to remove and choose **Remove Server** from the shortcut menu.

After you remove a server connection in Veeam ONE Client, connection to this server will be automatically removed in Veeam ONE Reporting Service.

> **NOTE:**
>
> When removing server connection, mind the following:
>
> - When you remove a server, historical performance and configuration data for the server and its child objects is deleted from the Veeam ONE database.
> - When you remove VMware Cloud Director, Veeam ONE withdraws connection to VMware Cloud Director server only. Connections to underlying vCenter Servers are not removed automatically — you must remove these connections manually.
> - When you delete Veeam Backup & Replication, Veeam ONE becomes unregistered on Veeam Backup & Replication for dashboards and reports integrations and additionally reports saved from Veeam Backup & Replication Analytics nodes are also removed. For details on Veeam Backup & Replication Analytics, see Veeam Backup & Replication Web UI.

Veeam Analytics Service

Veeam Analytics service is a component that enables communication with Veeam Backup & Replication servers, collects monitoring and reporting data, and sends remediation commands.

By default, Veeam ONE installs Veeam Analytics service automatically when you connect Veeam Backup & Replication servers. However, you might need to install Veeam Analytics service manually in specific situations. For example, if you did not approve the request for data collection in the Veeam Host Management console or if there was an error during installation.

You can install, configure, repair and monitor Veeam Analytics service on the Veeam Backup & Replication servers that are connected to Veeam ONE.

Considerations and Limitations

Consider the following:

- DNS resolution must work in both directions. Veeam ONE Server should be able to resolve the Veeam Backup & Replication Server using reverse DNS (PTR record), and the Veeam Backup & Replication Server should be able to resolve the FQDN of the Veeam ONE Server.

  To edit the Hosts file on Veeam Analytics service, use the Configuration Files Import/Export feature. For details on file import and export, see Performing Maintenance Tasks.

- Veeam Analytics service only collects performance data from the Veeam Backup & Replication server itself. Data from proxies, repositories, or remote hosts is not collected.

- Each Veeam Analytics service is owned by a single Veeam ONE server. If you connect Veeam Backup & Replication server to another Veeam ONE instance, the ownership will be overwritten.

- [For high availability clusters] Veeam Analytics service must be installed on each node in the cluster. Veeam Analytics service is typically installed automatically during setup; however, depending on your cluster configuration, you may need to install it manually (`.msi` for Windows and `.bndl` for Linux). When configured, performance data is collected only from the primary node.

- [For Microsoft Windows servers] Veeam Analytics service can be automatically installed on Veeam Backup & Replication servers managed by Enterprise Manager if their credentials match. Otherwise, you must install Veeam Analytics service on such servers in Veeam ONE Web Client or manually.

- [For Linux servers] To install and repair the Veeam Analytics Service package on Linux, you must enable remote data collection in the Veeam Host Management console on Veeam Backup & Replication. For more information, see section Configuring Backup Infrastructure Settings of the Veeam Backup & Replication User Guide.

- [For Linux servers] Veeam Analytics service cannot be automatically installed on Veeam Backup & Replication servers managed by Enterprise Manager. You must install Veeam Analytics service on such servers in Veeam ONE Web Client or manually.

- [For Linux servers] When using a user account other than the default `veeamadmin`, it is recommended to assign the Service Account role in Veeam Host Management and also Backup Administrator permissions in Veeam Backup & Replication. For details on roles and permissions, see Configuring Users and Configuring Roles in the Veeam Backup & Replication User Guide.

  For newly created local users in Veeam Host Management with a role other than Service Account, the user must first log in to the Veeam Software Appliance Web Client to change the password. Otherwise, an error occurs when connecting to the backup server to deploy Veeam Analytics service.

Installing Veeam Analytics Service in Veeam ONE Web Client

To install Veeam Analytics service on Veeam Backup & Replication in Veeam ONE Web Client:

1. Open Veeam ONE Web Client.

   For details, see Accessing Veeam ONE Components.

2. At the top right corner of the Veeam ONE Web Client screen, click the **Configuration** icon.

3. In the **Data Collection Overview** section, select the Veeam Backup & Replication servers on which you want to install Veeam Analytics service.

   To find the servers on which Veeam Analytics service is not installed, you can use the **Veeam Analytics service state** filter at the top of the servers list.

4. In the **Veeam Analytics service** menu, select **Management** and click **Install**.

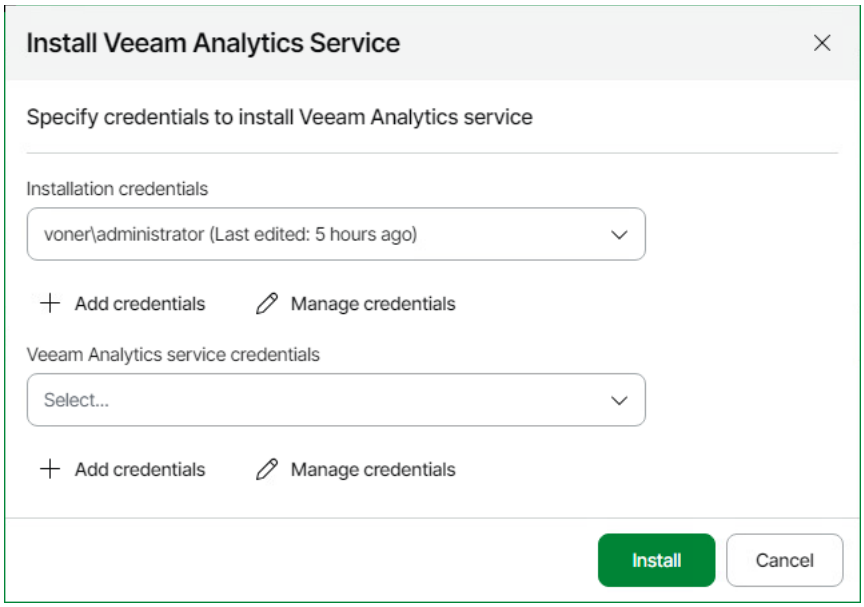
5. Specify credentials to install Veeam Analytics service.

   For details on account permissions, see Veeam Analytics Service Permissions.

6. [For Microsoft Windows servers] Specify credentials to run Veeam Analytics service.

   For details on account permissions, see Connection to Veeam Backup & Replication Servers.

7. Click **Install**.



Installing Veeam Analytics Service on Microsoft Windows Manually

By default, Veeam ONE Web Client installs Veeam Analytics service when you connect Veeam Backup & Replication servers in the **Add Server** wizard.

To install Veeam Analytics service on Windows manually:

1. Open Veeam ONE Web Client.

   For details, see Accessing Veeam ONE Components.

2. At the top right corner of the Veeam ONE Web Client screen, click the **Configuration** icon.

3. Navigate to the **Data Collection Overview** section.
4. At the top of the servers list, open the **Veeam Analytics service** drop-down menu and select **Download package** > **Microsoft Windows**.

   Veeam Analytics service package file will be saved to the default download folder on your local machine.
5. Run the installation package on the machine with Veeam Backup & Replication server and follow the installation wizard instructions.

Installing Veeam Analytics Service on Linux Manually

By default, Veeam ONE Web Client installs Veeam Analytics service when you connect Veeam Backup & Replication servers in the **Add Server** wizard.

To install Veeam Analytics service on Linux manually:

1. Open Veeam ONE Web Client.

   For details, see Accessing Veeam ONE Components.
2. At the top right corner of the Veeam ONE Web Client screen, click the **Configuration** icon.
3. Navigate to the **Data Collection Overview** section.
4. At the top of the servers list, open the **Veeam Analytics service** drop-down menu and select **Download package** > **Linux**.

   Veeam Analytics service package file will be saved to the default download folder on your local machine.
5. Open Veeam Updater.

   For details on accessing Veeam Updater on Veeam Backup & Replication server, see section Installing Private Hotfixes of the Veeam Backup & Replication User Guide.
6. Click **Upload a local file** and select the Veeam Analytics service package.
7. Click **Upload**.

Configuring Veeam Analytics Service Settings

You can configure settings of Veeam Analytics service installed on Veeam Backup & Replication servers:

1. Open Veeam ONE Web Client.

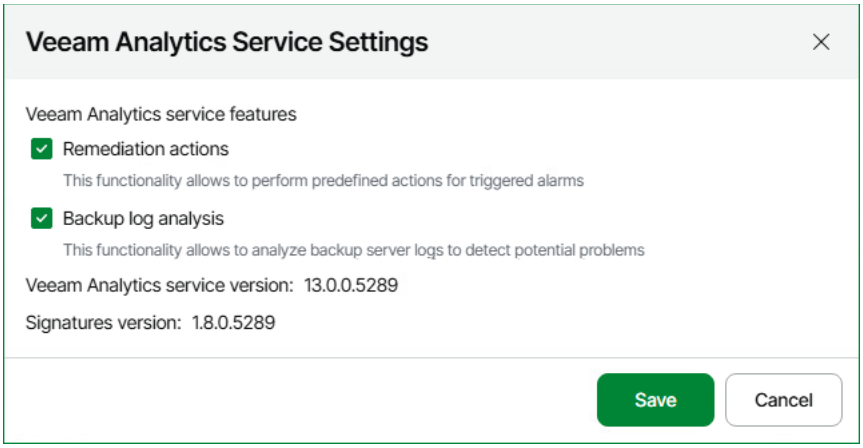
   For details, see Accessing Veeam ONE Components.
2. At the top right corner of the Veeam ONE Web Client screen, click the **Configuration** icon.
3. Navigate to the **Data Collection Overview** section.
4. From the list of connected Veeam Backup & Replication servers, select the server that you want to configure Veeam Analytics service .
5. At the top of the servers list, open the **Veeam Analytics service** drop-down menu and click **Settings**.
6. Configure Veeam Analytics service features:
   - **Remediation actions** – keep this check box selected if you want to allow Veeam Analytics service perform remediation actions on alarms.

     For details on alarm remediation actions, see Alarm Remediation Actions.

- **Backup log analysis** — keep this this check box selected if you want to allow Veeam Analytics service perform analysis of Veeam Backup & Replication logs.

  For details on log analysis, see Performing Log Analysis.

7. Click **Save**.



Repairing Veeam Analytics Service

If the connection to Veeam Analytics service is lost, you may try to perform a repair. When you repair Veeam Analytics service, Veeam ONE re-installs the package on Veeam Backup & Replication server and re-establishes connection.

To repair Veeam Analytics service:

1. Open Veeam ONE Web Client.

   For details, see Accessing Veeam ONE Components.

2. At the top right corner of the Veeam ONE Web Client screen, click the **Configuration** icon.
3. In the configuration menu on the left, click **Data Collection**.
4. From the list of connected Veeam Backup & Replication servers, select servers on which you want to repair Veeam Analytics service.

   Additionally you can press and hold the `[CTRL]` or `[SHIFT]` key to select multiple servers.

5. At the top of the servers list, open the **Veeam Analytics service** drop-down menu and click **Management** > **Repair**.
6. Edit Veeam Analytics service credentials if required and click **Install**.

Downloading Veeam Analytics Service Logs

To download Veeam Analytics service logs:

1. Open Veeam ONE Web Client.

   For details on accessing Veeam ONE components, see Veeam ONE Web Client.

2. Click **Configuration** on the top right of the Veeam ONE Web Client screen.
3. Navigate to the **Data Collection Overview** section.

4. From the list of connected Veeam Backup & Replication servers, select servers on which you want to repair Veeam Analytics service.

   Additionally you can press and hold the [CTRL] or [SHIFT] key to select multiple servers.

5. At the top of the servers list, open the Veeam Analytics service drop-down menu and click **Management** > **Download logs**.
6. Define the time period for which you want to collect logs.
7. To download service database information, select the **Include service data base** check box.
8. Click **Start**.

   The logs package will be saved to the default download folder on your local machine.

Advanced Actions

The following advanced actions are available for all data collection tasks on connected Veeam ONE servers:

- Scheduling Data Collection
- Running Data Collection Manually

Scheduling Data Collection

By default, data for Veeam ONE Web Client and Business View reporting data is collected automatically, according to a predefined schedule. Data collection runs on weekdays at 3:00 a.m. This schedule applies to all Veeam Backup & Replication, Veeam Backup for Microsoft 365 and virtualization servers that are managed by Veeam ONE. For details on data collection sessions, see Viewing Data Collection Session Details.

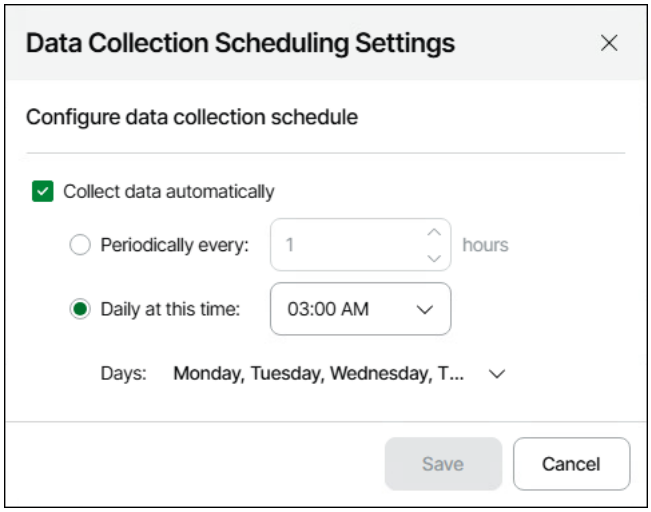
You can change the default data collection schedule or disable the schedule.

Changing Data Collection Schedule

To change the schedule according to which data collection will start:

1. Open Veeam ONE Web Client.
2. At the top right corner of the Veeam ONE Web Client window, click **Configuration**.
3. In the configuration menu on the left, click **Data Collection**.
4. Click **Advanced Actions** and choose **Schedule report data collection**.
5. Make sure the **Collect data automatically** check box is selected.
6. Set the schedule according to which data collection must start.
    - To run data collection with specific time intervals, select the **Periodically every N hours** option and specify the interval at which data collection must start. If you choose to run data collection periodically, make sure that the interval between data collection sessions is long enough to collect data from all connected servers.
    - To run data collection every day at specific time, select the **Daily at this time** option and specify the time of the day when data collection must start. In the **Days** section, select days of week on which data collection must run.
7. Click **Save**.

After you schedule automatic data collection, the schedule type for the *Object properties collection task* will be set to *Daily* or *Periodic*. The task will start data collection according to the specified schedule.



Disabling Data Collection

You can disable automatic data collection for Veeam ONE Web Client, and perform data collection manually. To learn how to perform data collection manually, see Running Data Collection Manually.

To disable automatic data collection:

1. Open Veeam ONE Web Client.
2. At the top right corner of the Veeam ONE Web Client window, click **Configuration**.
3. In the configuration menu on the left, click **Data Collection**.
4. Click **Advanced Actions** and choose **Schedule report data collection**.
5. Clear the **Collect data automatically** check box.
6. Click **Save**.

Running Data Collection Manually

You can run data collection for Veeam ONE Web Client manually. This can be required if you disabled automatic data collection, or if you want to collect data between scheduled collection sessions. Data collection runs on all data sources added to Veeam ONE Web Client. For details on data collection sessions, see Viewing Data Collection Session Details.

Starting Data Collection

When you start data collection manually, Veeam ONE will collect data from all connected servers.

1. Open Veeam ONE Web Client.
2. At the top right corner of the Veeam ONE Web Client window, click **Configuration**.
3. In the configuration menu on the left, click **Data Collection**.
4. Click **Advanced actions** and choose **Start report data collection**.

Stopping Data Collection

You can stop a data collection session that was started either manually or by the schedule:

1. Open Veeam ONE Web Client.
2. At the top right corner of the Veeam ONE Web Client window, click **Configuration**.
3. In the configuration menu on the left, click **Data Collection**.
4. Click **Advanced actions** and choose **Stop report data collection**.

Viewing Data Collection Session Details

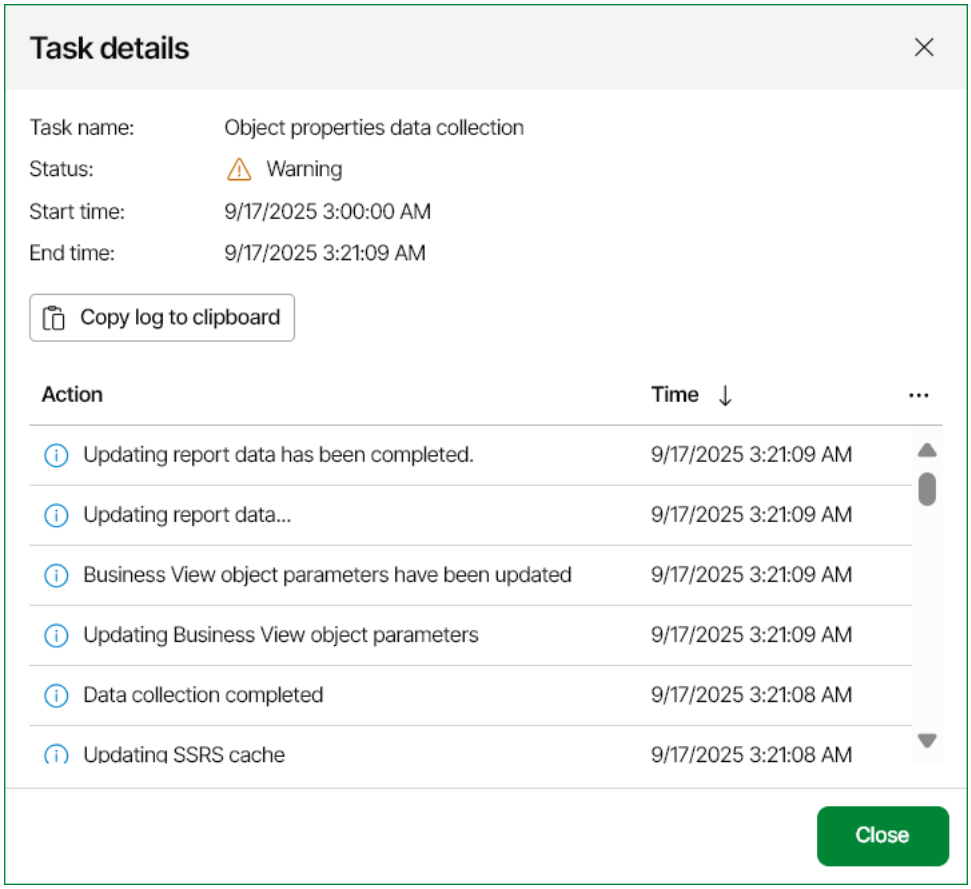
Every run of data collection initiates a new data collection session. Veeam ONE keeps record of tasks performed during data collection sessions and stores this information, so that you can view session details.

To view data collection session details:

1. Open Veeam ONE Web Client.
2. At the top right corner of the Veeam ONE Web Client window, click **Configuration**.
3. Click **Data Collection**.
4. Open **Task Sessions** and click on the required **Object properties data collection** session from the **Task Name** list.

   To easily find the necessary session, you can apply the following filters:

   - **Filter by name** – search the list of sessions by name.
   - **Status** – limit the list of sessions by status (*Success*, *Warning*, *Failed*, *Processing*, *Stopped*).
   - **Filter** – limit the list of sessions by session type.
   - **Time period** – limit the list of sessions by a defined time period.



Every session is described with the following details:

- Session type
- Session result

- Session start and end date and time
- Details on operations performed during the session

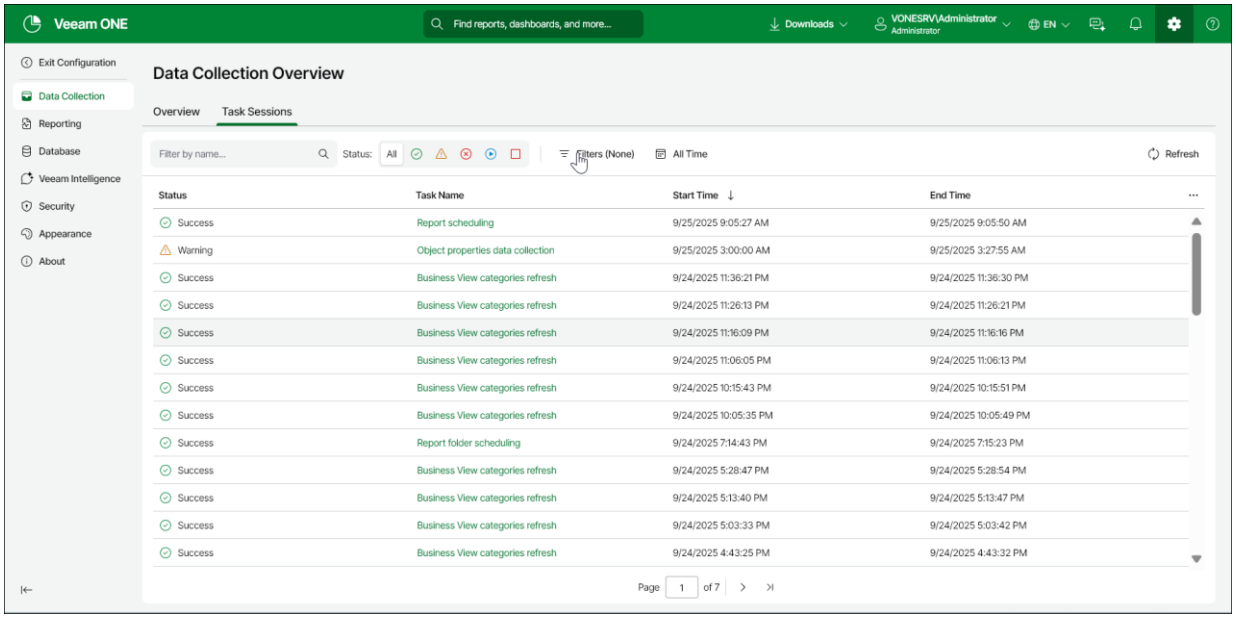
Database Maintenance Tasks

In addition to data collection, Veeam ONE periodically runs database maintenance tasks to delete data that must no longer be kept in the database according to the retention policy. Database maintenance tasks run every Sunday at 3:00 a.m.

Database maintenance task details are stored in the list of sessions. You can view details of database maintenance tasks similarly to viewing data collection session details.

Task Sessions

Task sessions provide a detailed record of ongoing and completed operations within the system, enabling effective monitoring and management of various tasks.



To view **Task Sessions**:

1. Open Veeam ONE Web Client.

   For details on accessing Veeam ONE components, see Veeam ONE Web Client.

2. In the configuration menu, click **Data Collection**.
3. Click **Task Sessions**.
4. Click the required session from the **Task Name** list.

   To easily find the necessary session, you can apply the following filters:

   - **Filter by name** — search the list of sessions by name.
   - **Status** — limit the list of sessions by status (*Success*, *Warning*, *Failed*, *Processing*, *Stopped*).
   - **Filter** — filter the list of sessions by session type including:
     - Object properties data collection
     - Business view categories refresh
     - Database maintenance
     - Report scheduling
     - Dashboard scheduling
     - Report folder scheduling
     - Deployment projects calculation
   - **Time period** — limit the list of sessions by a defined time period.

Related Topics

- Viewing Data Collection Session Details
- Business View
- Scheduling Reports
- Scheduling Dashboards
- Scheduling Delivery for Multiple Reports
- Calculating Deployment Projects

Reporting Settings

In the **Reporting** section, you can customize miscellaneous settings of the Veeam ONE Web Client configuration:

- Customizing Report Branding

  In this section, you can replace the default report header with a custom image.

- Configuring SSRS Server Settings

  In this section, you can specify settings of the Microsoft SQL Server Reporting Services server. These settings will be used for integration with Veeam ONE Web Client.

Customizing Report Branding

To customize appearance of reports according to your company branding, you can replace the default report header with a custom image, such as your company logo.

Branding applies to both legacy reports and reports generated by Veeam ONE version 13's the new report engine. Custom branding for these reports is only visible in scheduled or downloaded PDF reports.

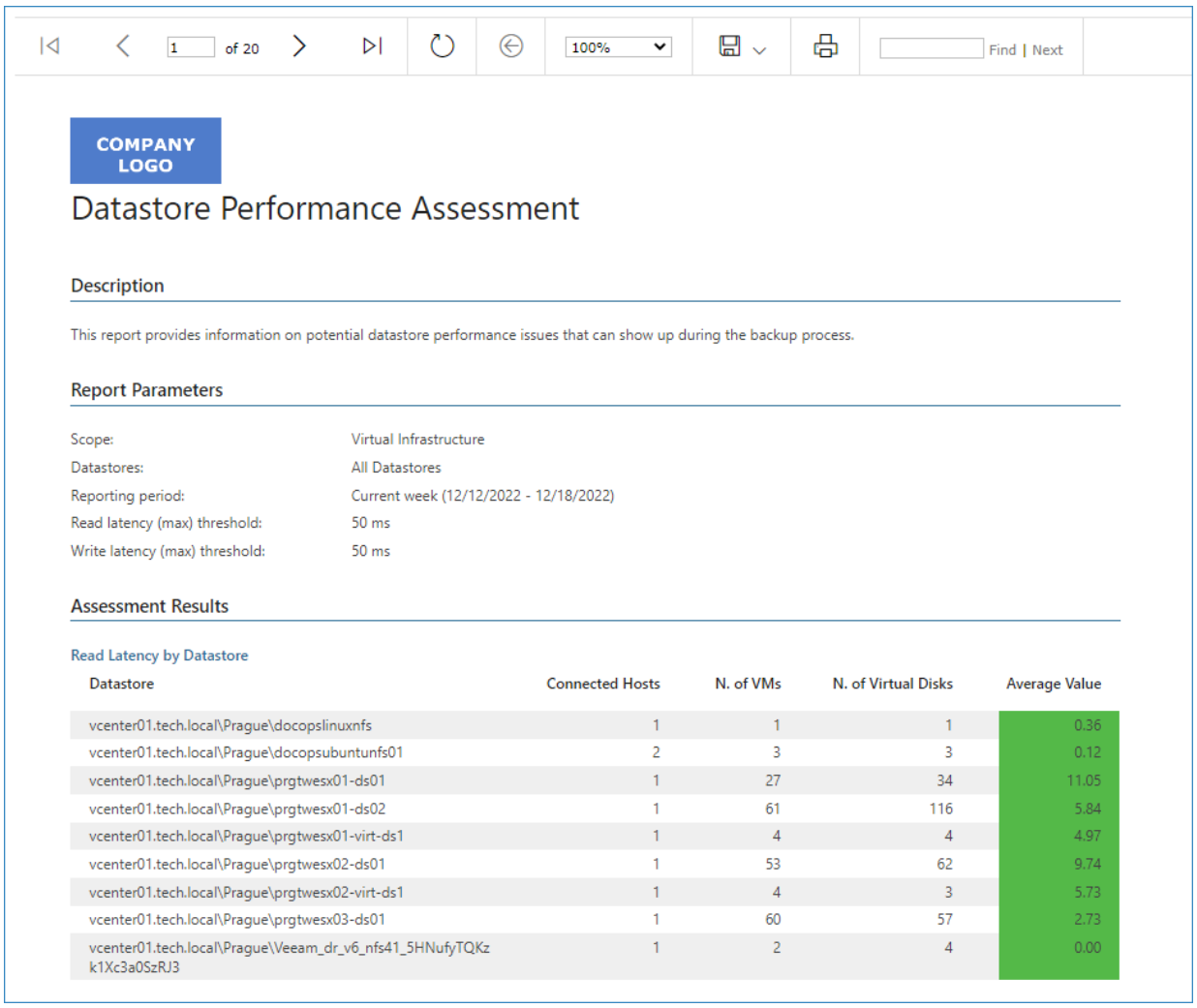


Image Requirements

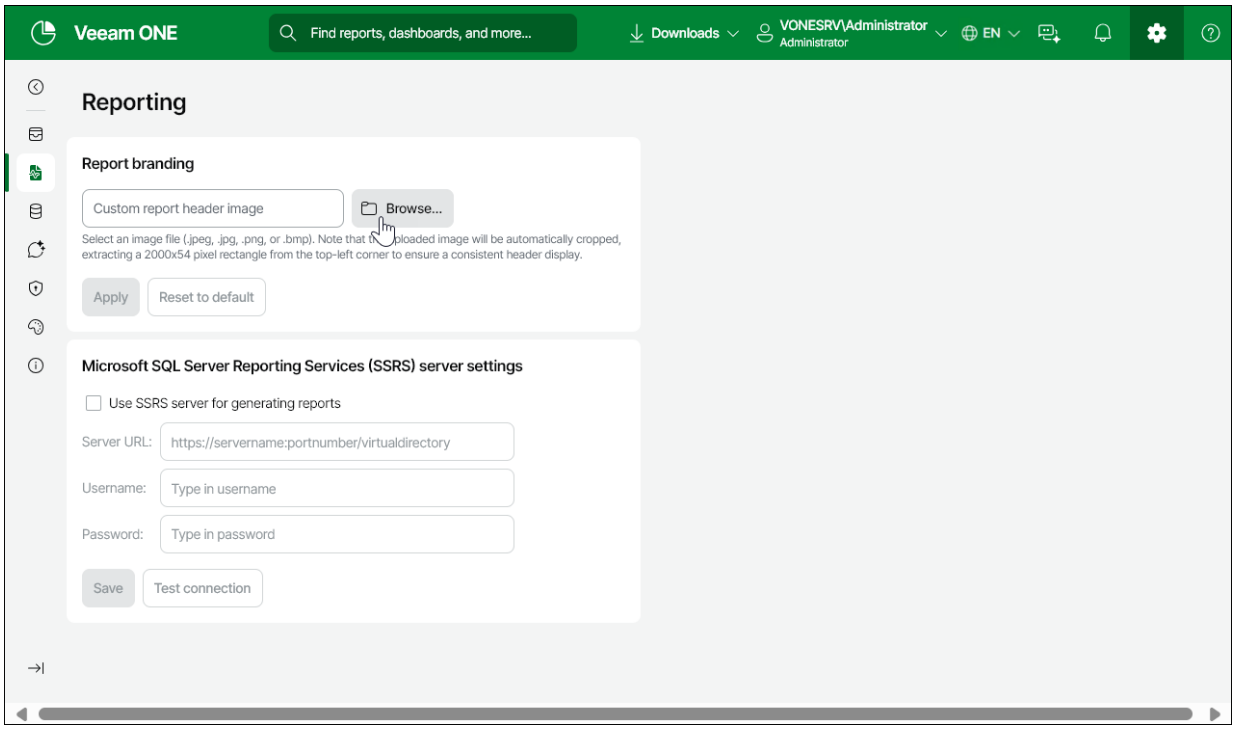
Before creating an image that will replace the default report header, make sure that the image file is saved in the PNG, JPEG, JPG or BMP formats.

Replacing Default Report Header

To replace the default report header with a custom image:

1. Open Veeam ONE Web Client.
2. At the top right corner of the Veeam ONE Web Client window, click **Configuration**.
3. In the configuration menu on the left, click **Reporting**.
4. In the **Report branding** section, click **Browse** and specify path to the custom report image file.

5. Click **Apply**.



Restoring the Default Report Header

To restore the default report header:

1. Open Veeam ONE Web Client.
2. At the top right corner of the Veeam ONE Web Client window, click **Configuration**.
3. In the configuration menu on the left, click **Reporting**.
4. In the **Report branding** section, click **Reset to Default**.
5. In the **Reset Report Header Image** window, click **Reset**.

Configuring SSRS Server Settings

When you report on a large virtual infrastructure, you may experience slowdowns with generating reports. In this case, you can integrate an SSRS server with Veeam ONE Web Client and use this SSRS server as an alternative to the default Veeam ONE report viewer.

> **NOTE**
>
> SSRS server is not used for generating Veeam Backup & Replication and Veeam Backup for Microsoft 365 reports that work with Veeam ONE version 13's new report engine. Reports that currently use the legacy engine including VMware, Hyper-V and vCD still require SSRS server configuration.

To configure SSRS server settings you must have the following permissions:

- *System User* role in SSRS site settings
- *Content Manager* role in SSRS Home folder settings
- User mapping to Veeam ONE database with *public* role
- *Select* and *Execute* permissions on Veeam ONE database

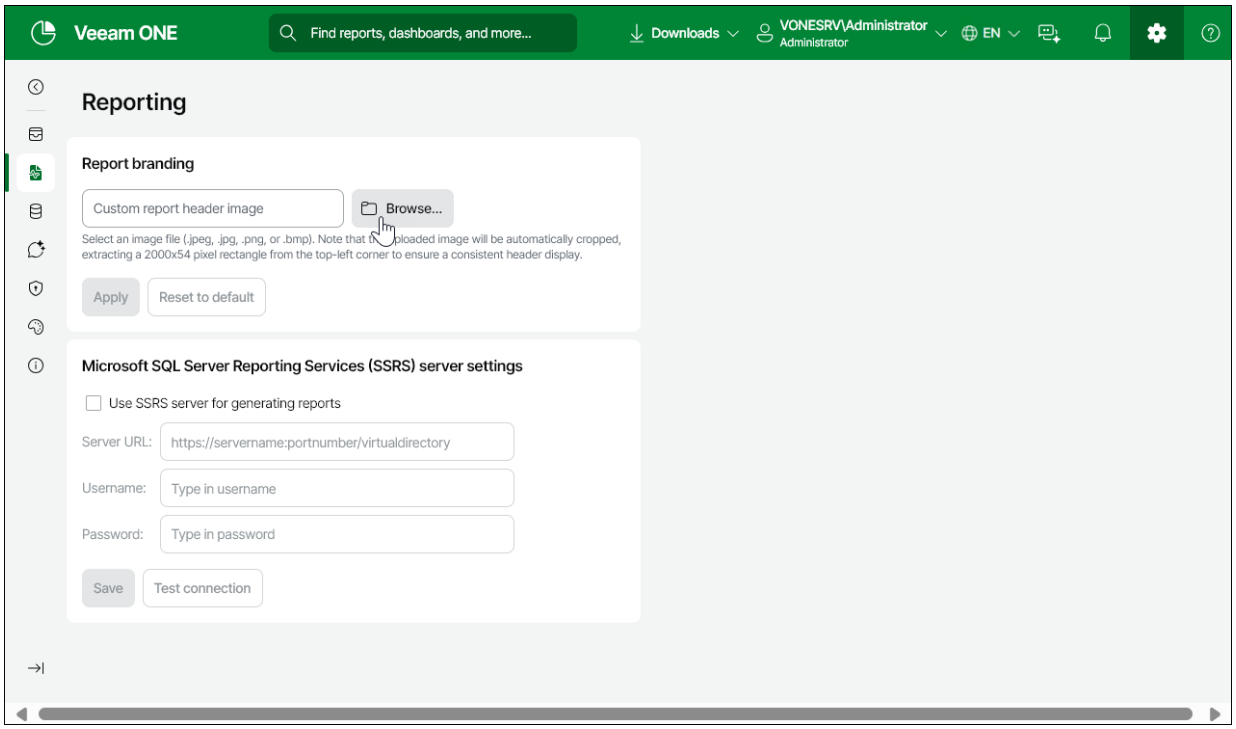
You can specify access settings to the Microsoft SQL Reporting Services server that will be used for integration with Veeam ONE Web Client:

1. Open Veeam ONE Web Client.
2. At the top right corner of the Veeam ONE Web Client window, click **Configuration**.
3. In the configuration menu on the left, click **Reporting Settings**.
4. In the **Microsoft SQL Server Reporting Services (SSRS) Server Settings** section, select the **Use SSRS server for generating reports** check box.
5. In the **Server URL** field, enter the address of the SSRS hosting server.

   The URL must be specified in the following format: `https://servername:port/virtualdirectory`. To check if this URL is correct, launch the Reporting Services Configuration Manager and check the **Web Service URL** section.
6. Specify a user name and a password to connect to the SSRS server.

   The user name must be specified in the `DOMAIN\USERNAME` format.
7. To verify SSRS server settings, click **Test Connection**. Veeam ONE Web Client will display verification results on a summary screen.

8. Click **Save** to save SSRS server settings.



Database

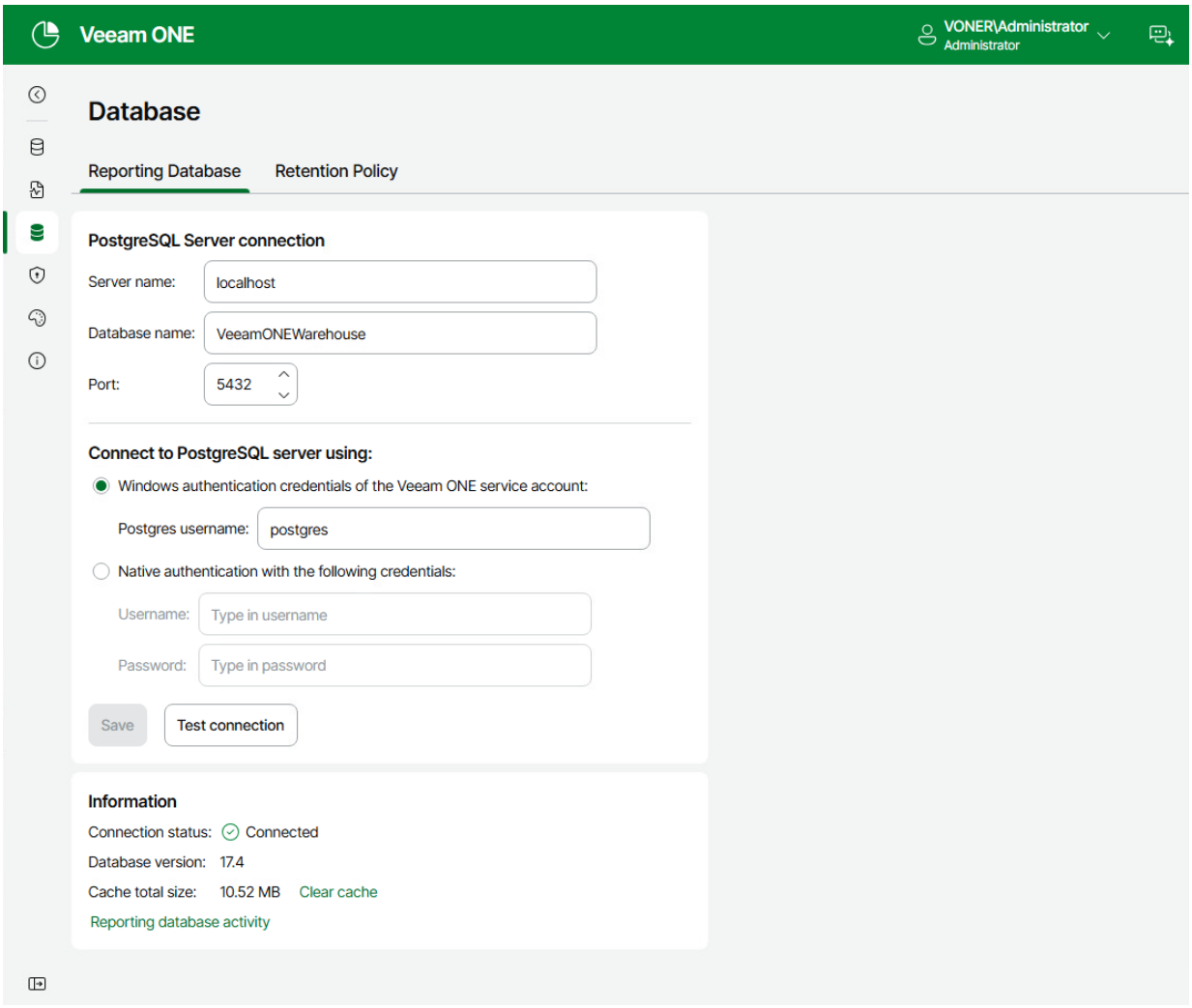
The reporting database is a dedicated database that stores PostgreSQL logs and metrics related to system activities, performance, and other relevant data for analysis and reporting purposes.

PostgreSQL server connection is configured during installation, but you can edit and configure your PostgreSQL server connection to Veeam ONE after installation.

To do that:

1. Open Veeam ONE Web Client.
2. At the top right corner of the Veeam ONE Web Client window, click **Configuration**.
3. In the configuration menu on the left, click **Database**.
4. On the **Reporting Database** tab, specify the database settings:
   - In the **Server name** field, specify the hostname or IP address of the PostgreSQL server that hosts the Veeam ONE reporting database.
   - In the **Database name** field, specify the name of the database that stores the Veeam ONE reporting data you wish to connect to.
   - In the **Port** field, specify the port number used for the PostgreSQL connection. The default number is 5432.
5. In the **Connect to PostgreSQL server using** section, select an authentication mode to connect to the database server instance: Microsoft Windows authentication or native database server authentication. If you select the native authentication, enter credentials of the PostgreSQL database account.
6. (Optional) Click **Test connection** to test whether your configured settings are correct. The **Information** section displays details of your connection.
7. (Optional) Click **Reporting database activity** to display the audit logs of your PostgreSQL connection including connection status, name and associated run time information.
8. (Optional) Click **Clear cache** if you encounter issues with report data or if any issue is affecting PostgreSQL as the first step when troubleshooting connections.

9. Click **Save** to save your configuration settings.



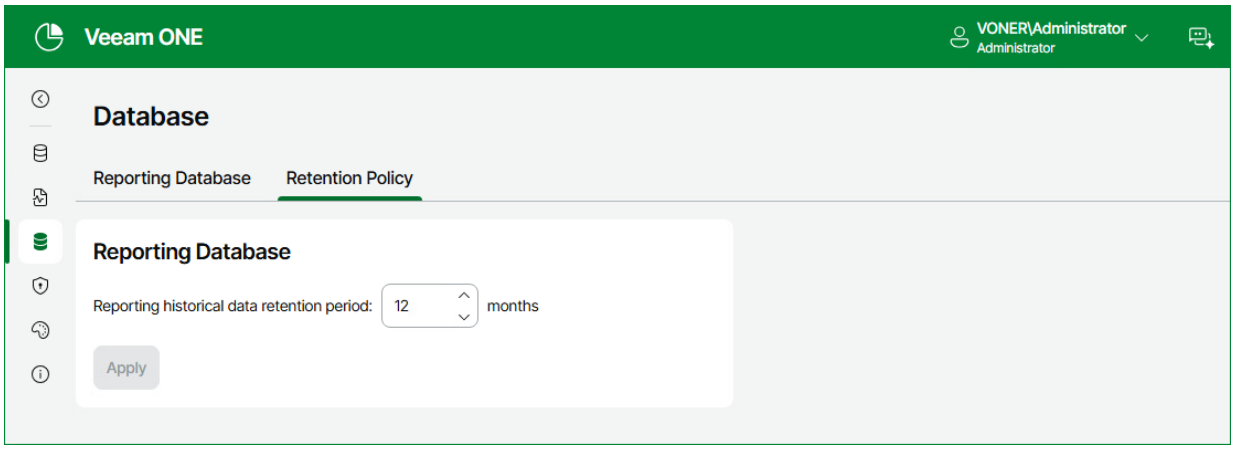
Retention Policy

On the **Retention Policy** tab, you can modify the time period during which reporting historical data is stored in the Veeam ONE reporting database. By default, reporting data is retained for 12 months.

To modify the retention period:

1. Navigate to the **Retention Policy** tab.
2. Define **Reporting historical data retention period** (in months).

3. Click **Apply**.



Veeam Intelligence Settings

Veeam Intelligence is an Artificial Intelligence based solution integrated into Veeam ONE Web Client.

For details on the Veeam Intelligence feature, see Veeam Intelligence.

To disable Veeam Intelligence or select its operation mode, follow these steps:

1. Open Veeam ONE Web Client.
2. At the top right corner of the Veeam ONE Web Client window, click **Configuration**.
3. In the configuration menu on the left, click **Veeam Intelligence**.
4. Select one of the following options:
   - **Disabled** – disables Veeam Intelligence. The feature is immediately removed from the top bar.
   - **Basic mode** – enables Veeam Intelligence basic mode. The feature icon appears in the top bar, allowing administrators to ask questions about Veeam ONE and receive AI-generated answers based on technical documentation, knowledge base articles and Veeam forums.
   - **Advanced** – activates Veeam Intelligence in the advanced mode. Administrators can inquire about Veeam ONE functionality and settings as well as data protection operations and infrastructure state. For details on Advanced mode, see Veeam Intelligence Advanced Mode.

Security

You can use the **Security** screen to create and maintain a list of credentials records that you plan to use to connect to components in the virtual and backup infrastructure, configure your integration with Recon for Veeam Infrastructure and adjust the login session settings to optimize the process of accessing Veeam ONE Web Client.

- Credentials Manager
- Integration with Recon for Veeam Infrastructure
- Login Sessions

Credentials Manager

The Credentials Manager lets you create the following types of credentials records:

- Standard account
- Linux private key

Adding Standard Accounts

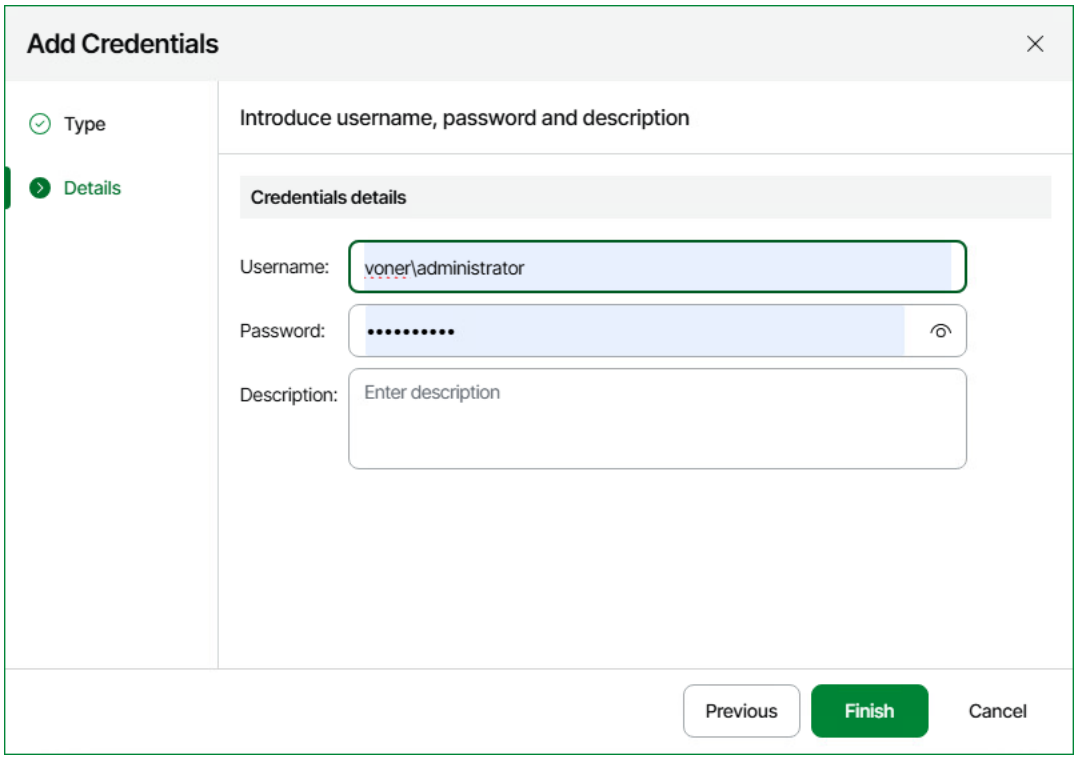
You can create a credentials record for an account that you plan to use to connect to infrastructure objects and their guest OS.

1. Open Veeam ONE Web Client.

   For details, see Accessing Veeam ONE Components.
2. At the top right corner of the Veeam ONE Web Client window, click **Configuration**.
3. In the configuration menu on the left, click **Security**.
4. Navigate to the **Credentials Manager** tab.
5. Click **Add credentials**.
6. At the **Type** step of the wizard, select **Standard account**.
7. At the **Details** step of the wizard:
   a. In the **Username** field, enter a user name for the account that you want to add. You can also click **Browse** to select an existing user account.
   b. In the **Password** field, enter a password for the account that you want to add. To view the entered password, click and hold the eye icon on the right of the field.
   c. In the **Description** field, enter a description for the created credentials record.

      As there can be a number of similar account names, for example, Administrator, it is recommended that you provide a meaningful unique description for the credentials record so that you can distinguish it in the list. The description is shown in brackets, following the user name.

8. Click **Finish**.



Adding Linux Private Keys

You can add a credentials record to connect to Linux machines using the Identity/Pubkey authentication method.

> **NOTE:**
>
> To use this method, you must first generate a pair of keys using a key generation utility, for example, ssh-keygen. Place the public key on a Linux server. To do this, add the public key to the `authorized_keys` file in the `.ssh/` directory in the home directory on the Linux machine. Place the private key in some folder on the Veeam ONE server or in a network shared folder.

To create a new credentials record using the Identity/Pubkey authentication method:

1. Open Veeam ONE Web Client.

   For details, see Accessing Veeam ONE Components.
2. At the top right corner of the Veeam ONE Web Client window, click **Configuration**.
3. In the configuration menu on the left, click **Security**.
4. Navigate to the **Credentials Manager** tab.
5. Click **Add credentials**.
6. At the **Type** step of the wizard, select **Linux private key**.
7. At the Details step of the wizard:
   a. In the **Username** field, specify a user name for the created credentials record.
   b. In the **Password** field, specify the password for the user account.

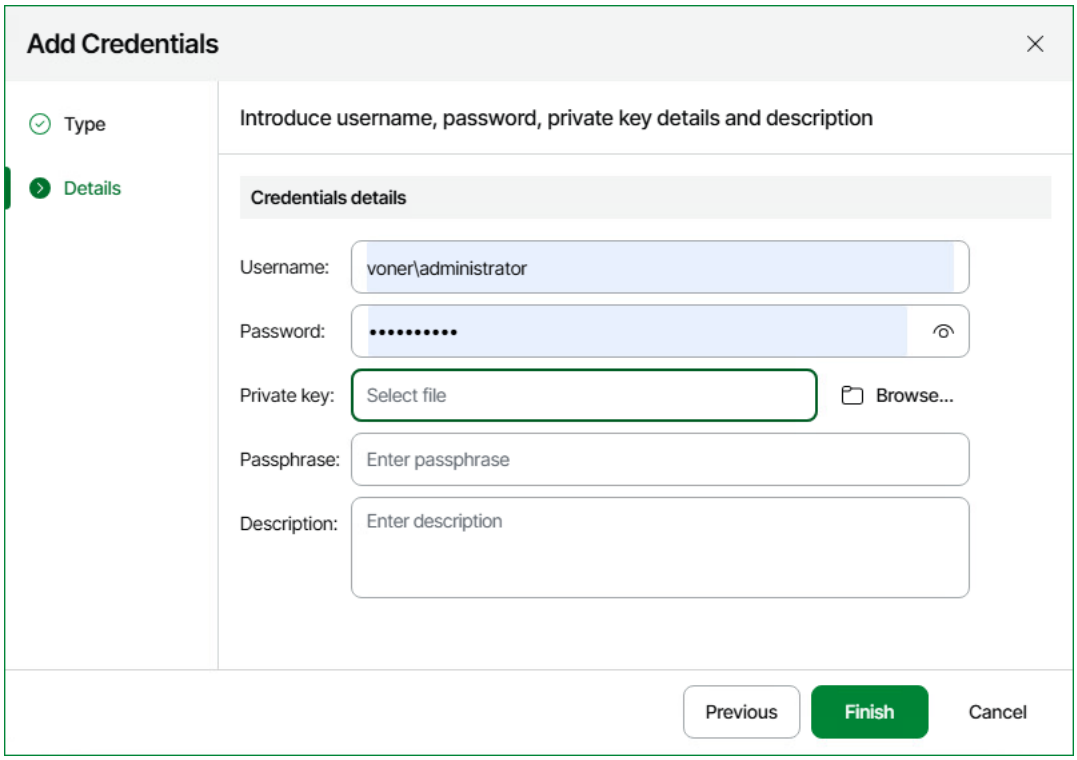
c. Click **Browse** next to the **Private key** field to select a private key file.

d. In the **Passphrase** field, specify a passphrase for the private key on the backup server.

e. In the **Description** field, enter a description for the created credentials record.

As there can be a number of similar account names, for example, Root, it is recommended that you supply a meaningful unique description for the credentials record so that you can distinguish it in the list.

8. Click **Finish**.



Editing and Deleting Credentials Records

You can edit or delete credentials records that you have created.

1. Open Veeam ONE Web Client.

   For details, see Accessing Veeam ONE Components.

2. At the top right corner of the Veeam ONE Web Client window, click **Configuration**.

3. In the configuration menu on the left, click **Security**.

4. Navigate to the **Credentials Manager** tab.

5. Select the credentials record and click **Edit credentials**.

6. If the credentials record is already used for any component in the infrastructure, Veeam ONE will display a warning. Click **Edit** to confirm your intention.

7. Edit settings of the credentials record as required and click **Finish**.

To delete a credentials record:

1. Open Veeam ONE Web Client.

   For details, see Accessing Veeam ONE Components.

2. At the top right corner of the Veeam ONE Web Client window, click **Configuration**.

3. In the configuration menu on the left, click **Security**.

4. Navigate to the **Credentials Manager** tab.

5. Select the credentials record and click **Delete credentials**.

   If the credentials record is already used for any component in the infrastructure, Veeam ONE will display a warning. In this case, you need to connect to an infrastructure object with new credentials before deleting current credentials record.

Adding Credentials in Veeam ONE Client

Alternatively you can create credential records in Veeam ONE Client.

To create a new standard credentials record:

1. Open Veeam ONE Web Client.

   For details, see Accessing Veeam ONE Components.

2. In the main menu, click **Credentials Manager**.

   Alternatively, press `[CTRL + M]` on the keyboard.

3. Click **Add** > **Standard account**.

4. In the **Username** field, enter a user name for the account that you want to add. You can also click **Browse** to select an existing user account.

5. In the **Password** field, enter a password for the account that you want to add. To view the entered password, click and hold the eye icon on the right of the field.

6. In the **Description** field, enter a description for the created credentials record.

   As there can be a number of similar account names, for example, Administrator, it is recommended that you provide a meaningful unique description for the credentials record so that you can distinguish it in the list. The description is shown in brackets, following the user name.

7. Click **Save**.

Adding Linux Private Keys in Veeam ONE Client

You can add a credentials record to connect to Linux machines using the Identity/Pubkey authentication method.

> **NOTE:**
>
> To use this method, you must first generate a pair of keys using a key generation utility, for example, ssh-keygen. Place the public key on a Linux server. To do this, add the public key to the `authorized_keys` file in the `.ssh/` directory in the home directory on the Linux machine. Place the private key in some folder on the Veeam ONE server or in a network shared folder.

To create a new credentials record using the Identity/Pubkey authentication method:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. In the main menu, click **Credentials Manager**.

   Alternatively, press [CTRL + M] on the keyboard.

3. Click **Add** > **Linux private key**.

4. In the **Username** field, specify a user name for the created credentials record.

5. In the **Password** field, specify the password for the user account.

6. Click **Browse** next to the **Private key** field to select a private key file.

7. In the **Passphrase** field, specify a passphrase for the private key on the backup server.

8. In the **Description** field, enter a description for the created credentials record.

   As there can be a number of similar account names, for example, Root, it is recommended that you supply a meaningful unique description for the credentials record so that you can distinguish it in the list.

9. Click **Save**.

Editing and Deleting Credentials Records on Veeam ONE Client

You can edit or delete credentials records that you have created.

To edit a credentials record:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. In the main menu, click **Credentials Manager**.

   Alternatively, press [CTRL + M] on the keyboard.

3. Select the credentials record in the list and click **Edit**.

4. If the credentials record is already used for any component in the infrastructure, Veeam ONE will display a warning. Click **Edit** to confirm your intention.

5. Edit settings of the credentials record as required and click **Save**.

To delete a credentials record:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. In the main menu, click **Credentials Manager**.

   Alternatively, press [CTRL + M] on the keyboard.

3. Select the credentials record in the list and click **Delete**.

   If the credentials record is already used for any component in the infrastructure, Veeam ONE will display a warning. In this case, you need to connect to an infrastructure object with new credentials before deleting current credentials record.

Integration with Recon for Veeam Infrastructure

You can optionally integrate Recon for Veeam Infrastructure into Veeam ONE to provide the following information:

- Suspicious ransomware activities detected by Recon and displayed in the Threat Center dashboard.
- Internal alarms triggered by Recon and displayed in the Alarms Overview dashboard.

For more information on the solution, see Recon for Veeam Infrastructure User Guide.

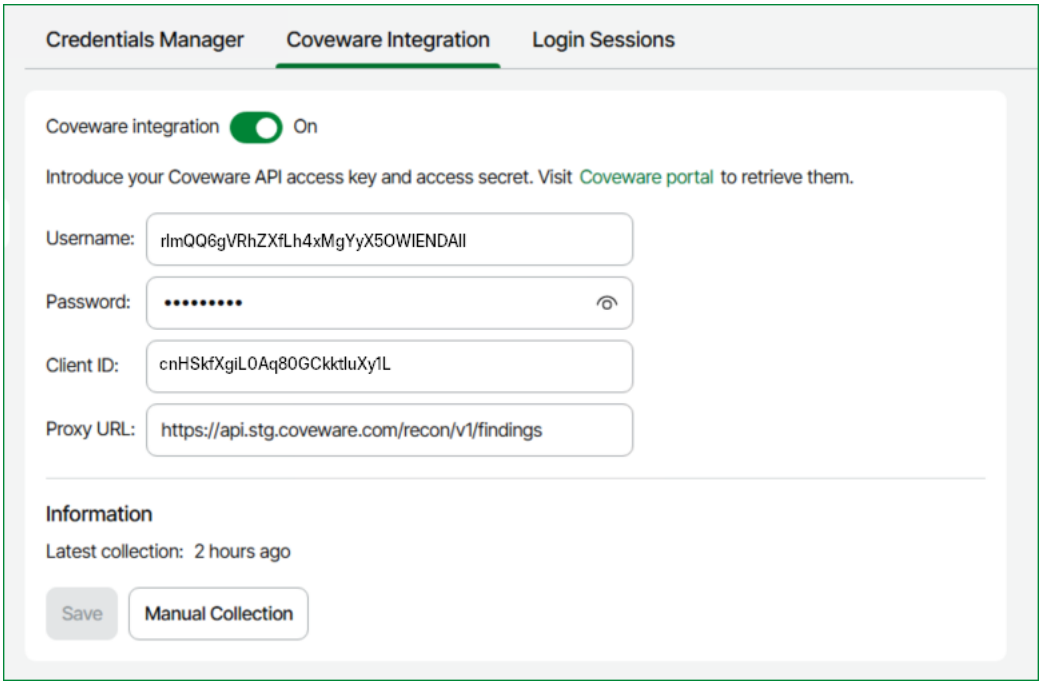
To configure integration with Recon for Veeam Infrastructure:

1. Open Veeam ONE Web Client.

   For details, see Accessing Veeam ONE Components.
2. At the top right corner of the Veeam ONE Web Client window, click **Configuration**.
3. In the configuration menu on the left, click **Security**.
4. In the main menu, navigate to the **Coveware Integration** tab.
5. Switch the **Coveware integration** toggle to **On**.
6. Specify parameters to connect to the Recon REST API:
   - Username
   - Password
   - Client ID
   - Proxy URL

   To get these parameters, log in to the Coveware portal and enable API integration. For more information, see Integrations in the Recon for Veeam Infrastructure User Guide.
7. Click **Save**.

8. (Optional) To manually collect data from your Coveware instance, click **Manual Collection**.



Login Sessions

You can adjust the login session settings to optimize the process of accessing Veeam ONE Web Client. To do that:

1. Open Veeam ONE Web Client.
2. At the top right corner of the Veeam ONE Web Client window, click **Configuration**.
3. In the configuration menu on the left, click **Security**.
4. Navigate to the **Login Sessions** tab.
5. Specify login session settings:
   - In the **Idle user login session timeout, minutes**, specify the time period in minutes after which an idle user must be automatically logged out.
   - In the **Idle administrator login session timeout, minutes**, specify the time period in minutes after which an idle administrator must be automatically logged out.
   - In the **Maximum number of concurrent login sessions per user**, specify the maximum allowed number of simultaneously processed login attempts performed by a single user.
   - To view information on previous login sessions, select the **Show previous login attempts after logging in** check box. The information will be displayed on an additional page that opens after you log in.
6. Click **Save**.

Veeam ONE Web Client Appearance

You can change the color scheme, color mode and menu display to suit your work environment.

To change the color scheme, color mode and menu display:

1. At the top right corner of the Veeam ONE Web Client window, click **Configuration**.
2. In the Appearance section of the configuration menu, click:
   - **Color scheme** – choose from green, blue or gray.
   - **Color mode** – choose from **Light**, **Dark** or **System**.
   - **Left menu** – **Automatic**, **Expanded** or **Collapsed**.
3. Click **Apply**.

General Configuration Details

To access Veeam ONE Web Client configuration details:

1. Open Veeam ONE Web Client.
2. At the top right corner of the Veeam ONE Web Client window, click **Configuration**.
3. In the configuration menu on the left, click **About**.

In the **About** section, you can view **Server information**: Veeam ONE version, the machine where the Veeam ONE Server component runs and the location of the log files on the machine where Veeam ONE Server component is installed. Additionally you can download logs in the **Support Information** section when required for debugging or support analysis.

Veeam ONE Client Settings

Veeam ONE client settings include:

- General settings
- Color settings
- Charts settings
- Tabs view settings
- Other settings

General Settings

In client general settings, you can specify an FQDN name or IP address of a machine where the Veeam ONE Server component is installed.

To specify client general settings:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

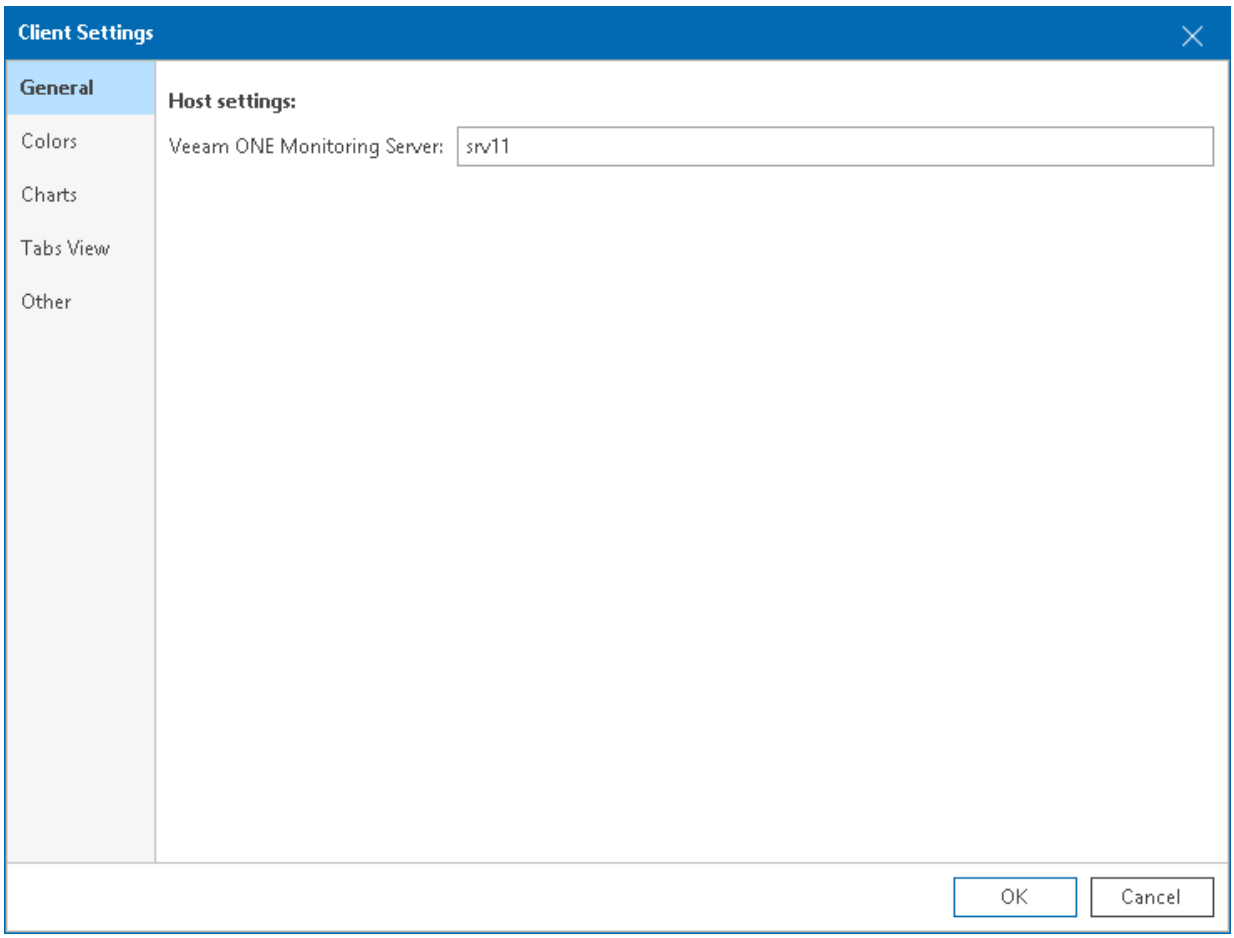
2. In the main menu, click **Settings** > **Client Settings**.

   Alternatively, press `[CTRL + O]` on the keyboard.

3. In the **Client Settings** window, open the **General** tab.

4. In the **Host settings** section, specify an FQDN or IP address of a machine where the Veeam ONE Server component is installed.

   - If the connection to the Veeam ONE Server component is successful, the **Veeam ONE Monitoring Server** field is filled automatically with the name of the machine where Veeam ONE Server component is installed or localhost.
   - If Veeam ONE Server component is not found on the specified machine, Veeam ONE will prompt you to specify the correct name in the client settings.



Color Settings

In color settings, you can create a custom color scheme that will be used to display graphs on performance charts.

To specify color settings:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

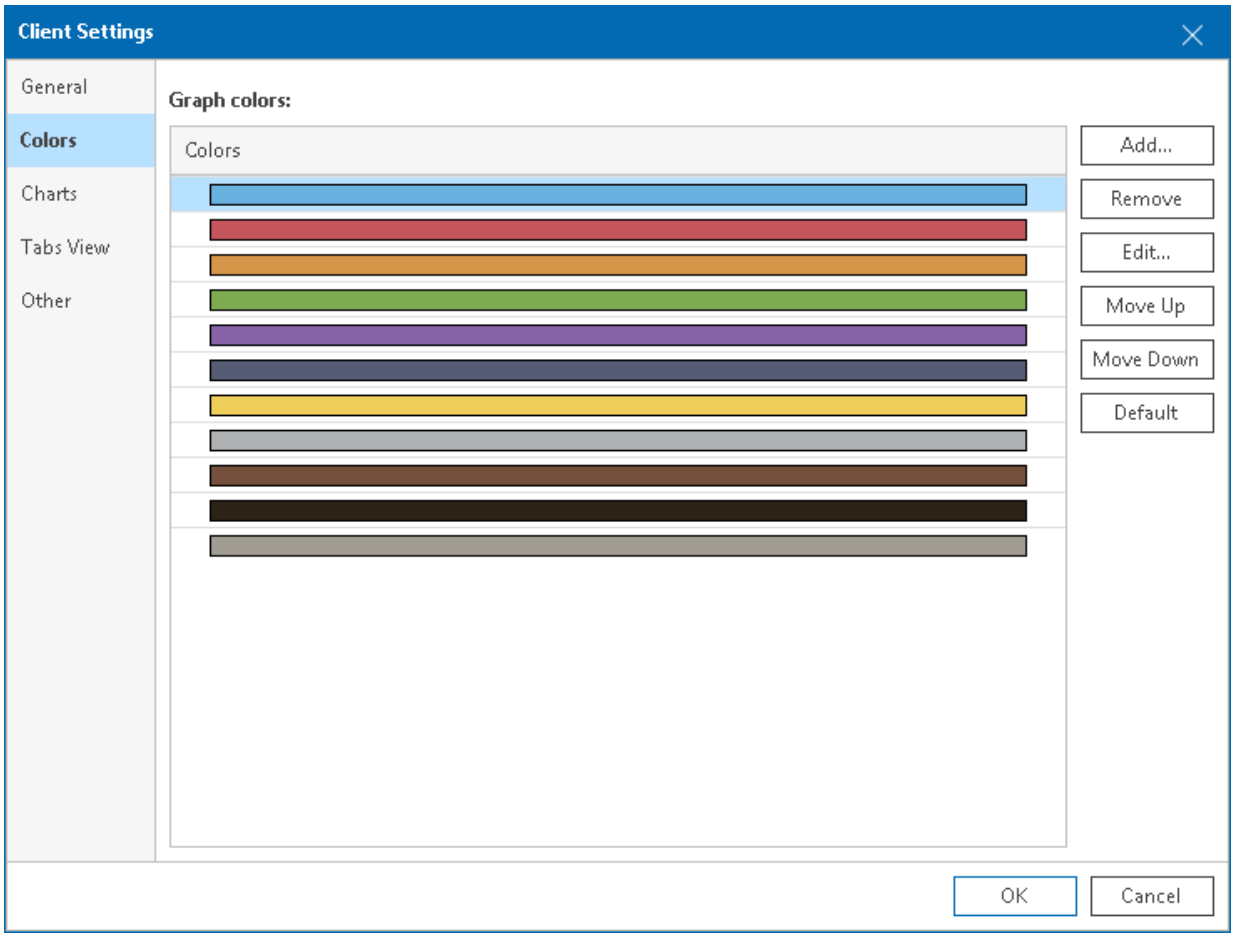
2. In the main menu, click **Settings** > **Client Settings**.

   Alternatively, press `[CTRL + O]` on the keyboard.

3. In the **Client Settings** window, open the **Colors** tab.

4. Create a custom color scheme that must be used to display graphs on performance charts.

   You can add colors from the color palette, remove and edit existing colors, as well as sort them as required. Colors at the top are used first for graphs on performance charts.



Charts Settings

In charts settings, you can customize display preferences for graphs on performance charts.

To specify charts settings:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. In the main menu, click **Settings** > **Client Settings**.

   Alternatively, press `[CTRL + O]` on the keyboard.

3. In the **Client Settings** window, open the **Charts** tab.

4. In the **Chart options** section, configure display preferences for graphs in performance charts:

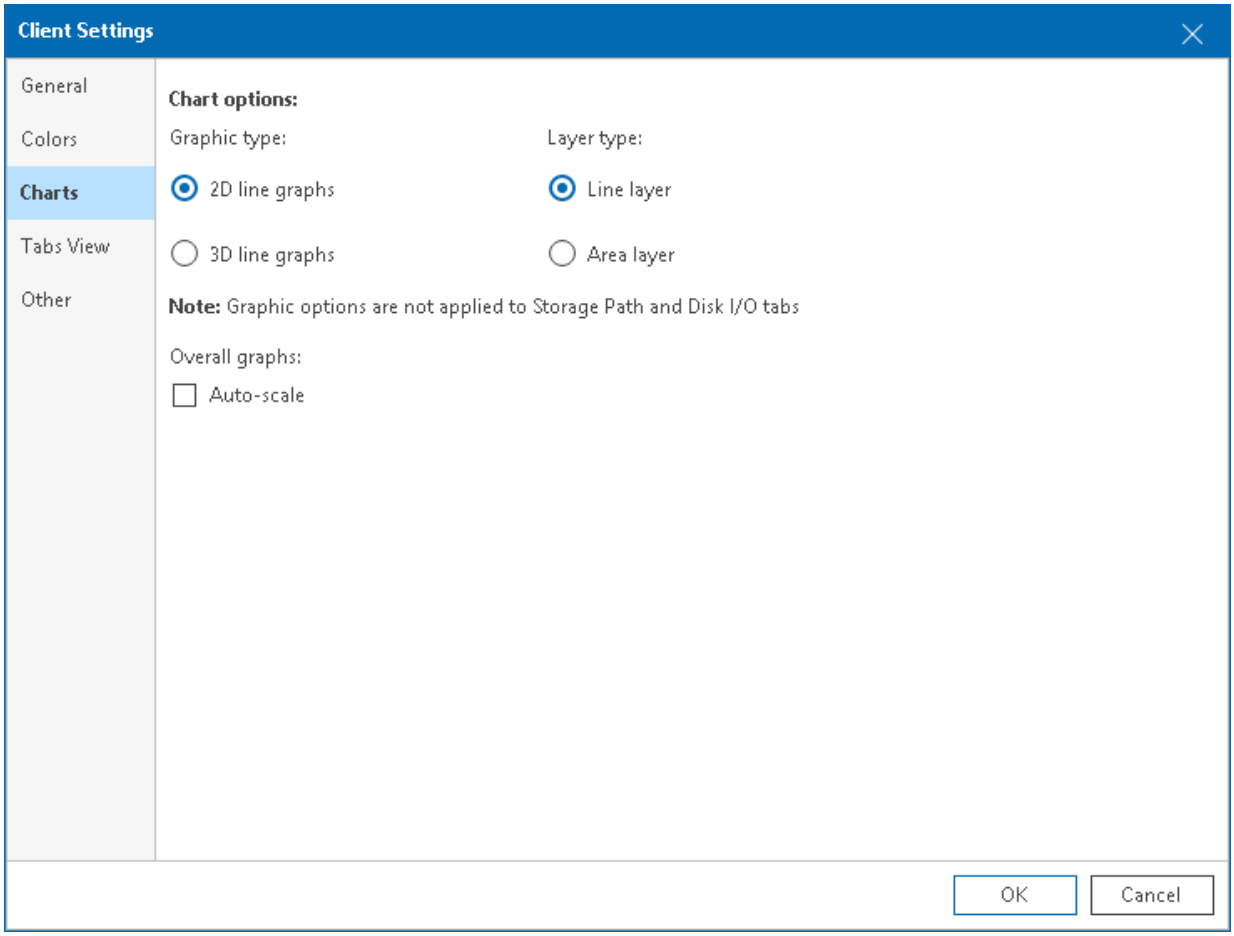
   - In the **Graphic type** section, choose how line graphs must be presented in charts — as 2D or 3D line graphs.
   - In the **Layer type** section, choose how graphs layer must be presented in charts — as line layer or area layer.

   For samples of graphic type and layer type combinations, see Graphic and Layer Type Samples.

5. In the **Overall** graphs section, specify whether top line thresholds must be present on the **Overview** tab.

   If the **Auto-scale** check box is enabled, the Y-axis will scale automatically to match the range of the displayed data.

For samples of the **Overview** tabs with the **Auto-scale** option enabled and disabled, see Auto-Scale Samples.

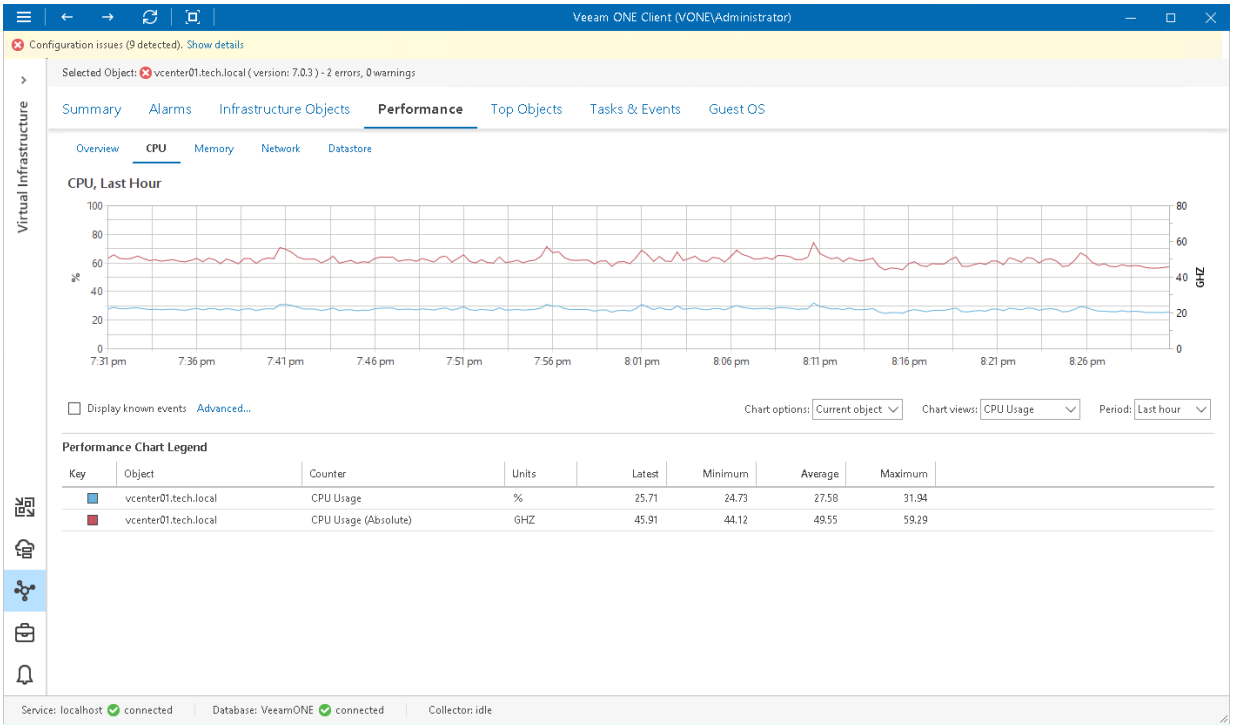


Graphic and Layer Type Samples

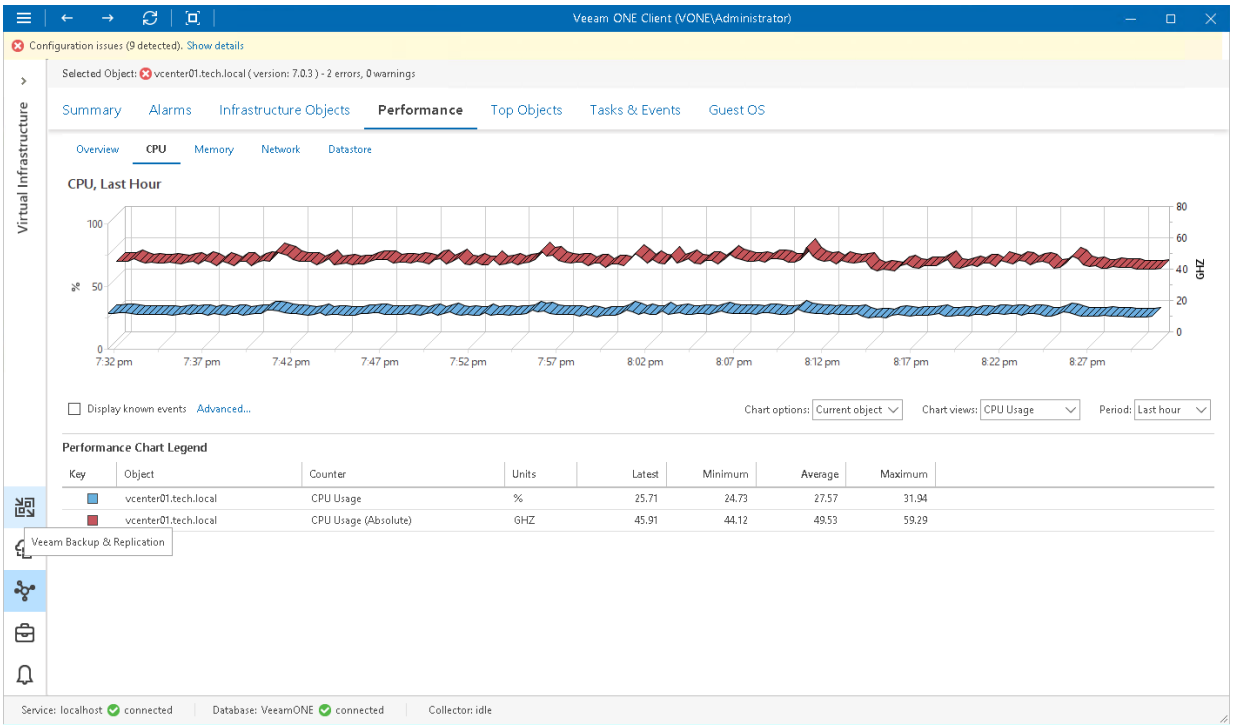
You can choose to show graphs in 2D or 3D, as plain lines or filled areas.

The following images illustrate how different combinations of line graphs and layer types will be reflected on performance charts:

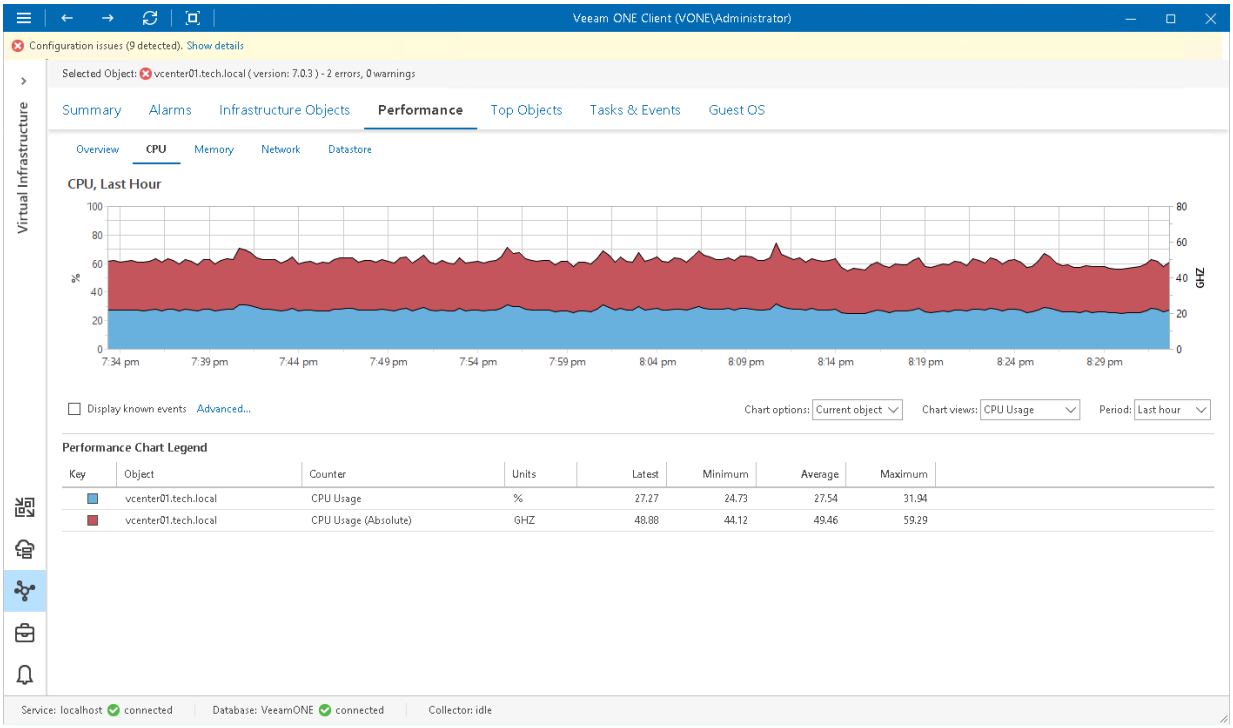
- 2D line graphs with line layer



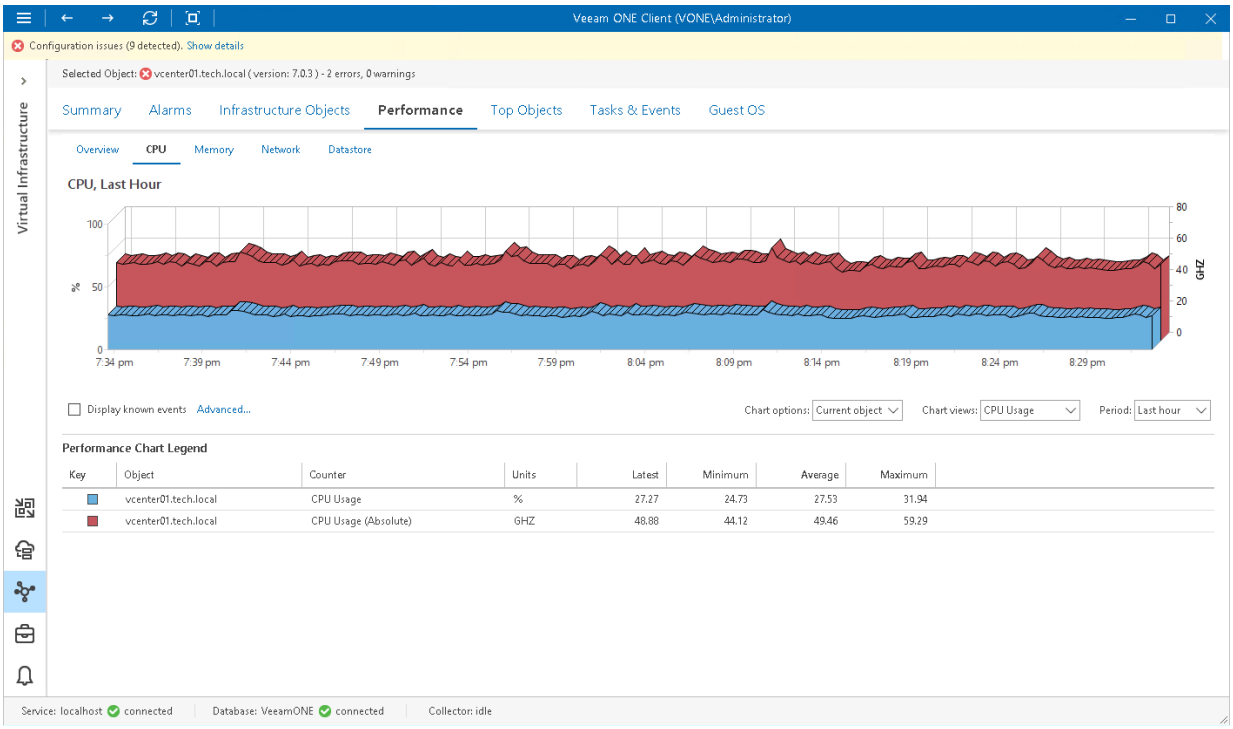
- 3D line graphs with line layer



- 2D line graphs with area layer



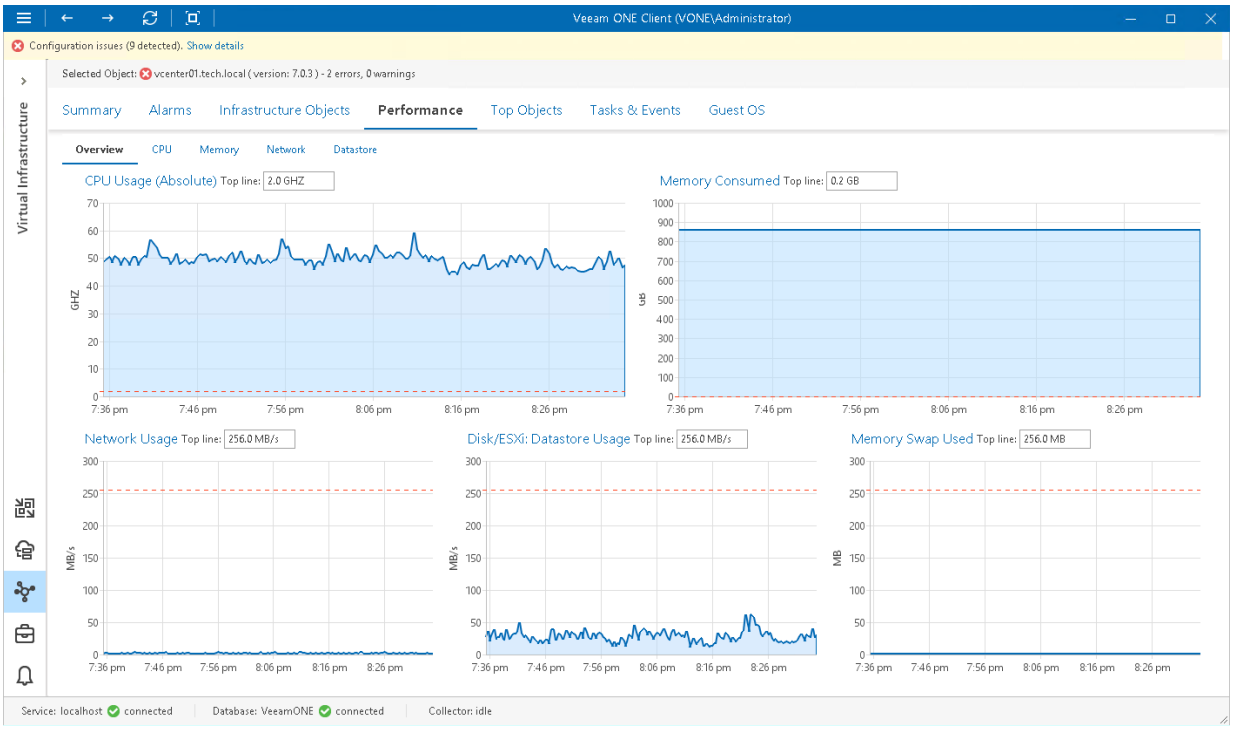
- 3D line graphs with area layer



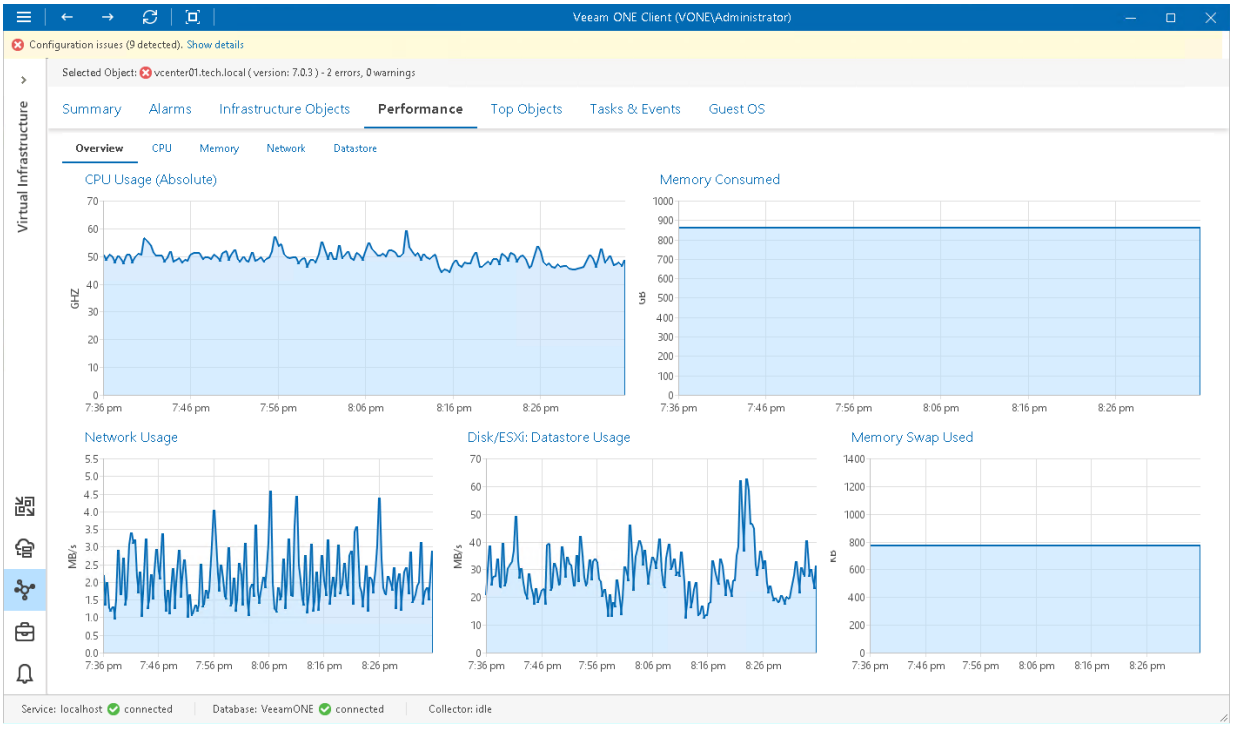
Auto-Scale Samples

The **Auto-scale** option allows you to enable auto-scaling if you want to remove top line thresholds from performance charts on the **Overview** tab. With auto-scale enabled, the Y-axis scales automatically, to match the range of the displayed data.

- Auto-scale disabled



- Auto-scale enabled



Tabs View Settings

In the tabs view settings, you can enable the automatic switching between the tabs in Veeam ONE Client.

Automatic switching is intended for screens and monitors in a network operations center (NOC). With this option enabled, Veeam ONE automatically switches between its tabs (dashboards) at a certain time interval, and displays dashboards similarly to a slideshow. An administrator can view the whole picture without interacting with Veeam ONE, and can be sure not to miss critical situations in case they occur.

If automatic switching is enabled, Veeam ONE starts switching tabs only if there is no user input from a keyboard, mouse, and so on. Once the user starts interacting with Veeam ONE Client, Veeam ONE Client stops switching tabs.

Automatic switching is disabled by default. You can enable it and create rules that Veeam ONE will use to switch tabs.

There are two types of rules for the automatic switching of tabs:

- You can choose to switch tabs for an object that is selected in the navigation tree. This rule will be useful if you want to monitor the state of one critical object.
- You can choose to switch specific tabs for a predefined scope of objects. This view will be useful if you want to monitor certain aspects of a critical infrastructure segment.

Switching Tabs for One Infrastructure Object

To enable automatic switching of tabs and create a rule that switches tabs for one infrastructure object:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. In the inventory pane, click the necessary view — Veeam Backup & Replication, Veeam Backup for Microsoft 365, Virtual Infrastructure, VMware Cloud Director, or Business View.

3. In the inventory pane, select the necessary infrastructure object.

4. In the main menu, click **Settings** > **Client Settings**.

   Alternatively, press `[CTRL + O]` on the keyboard.

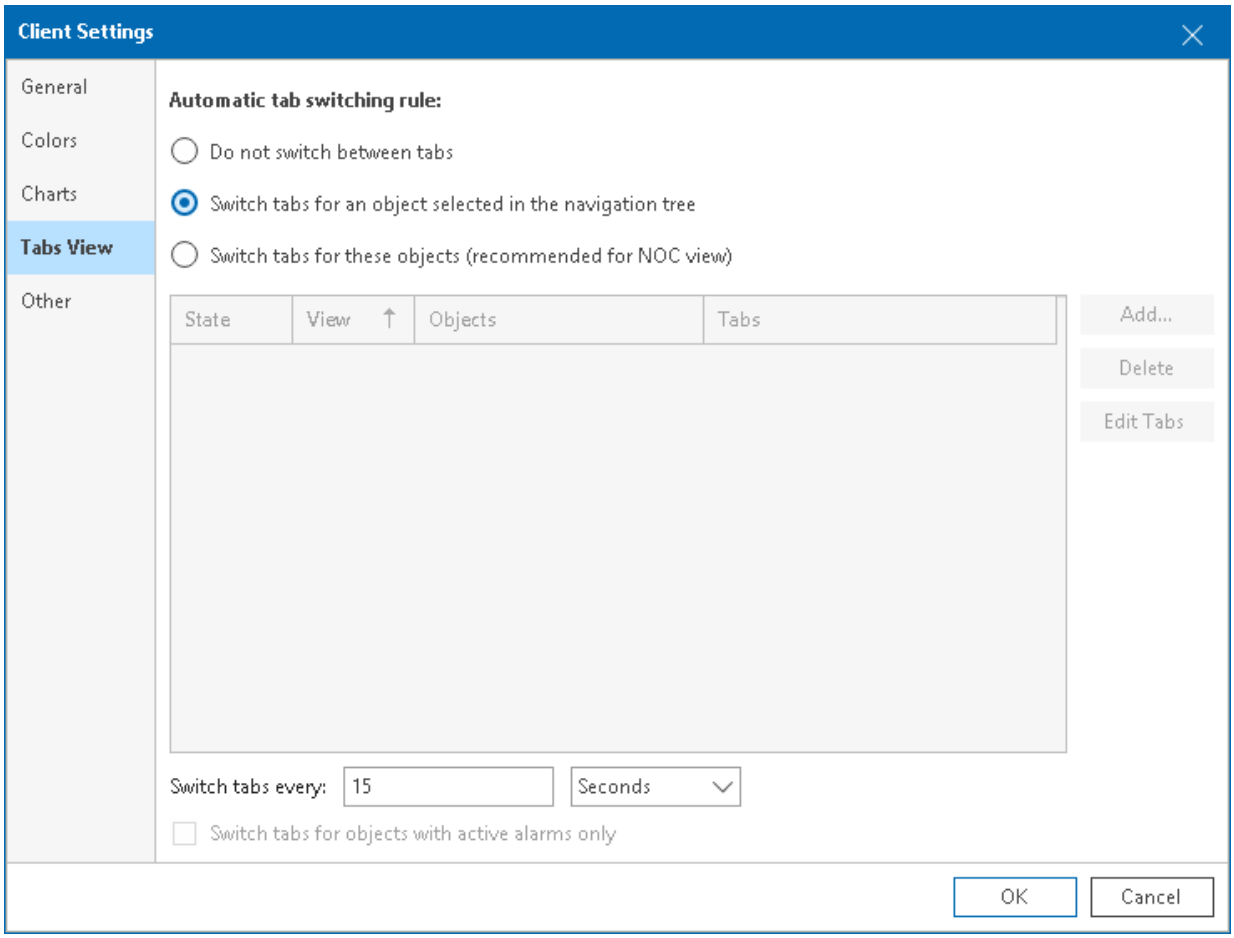
5. In the **Client Settings** window, navigate to the **Tabs View** tab.

6. In the **Automatic tab switching rule** section, select **Switch tabs for an object selected in the navigation tree**.

7. In the **Switch tabs every <time interval>** section, specify a time interval at which tabs must be switched.

   You can specify an interval in seconds, minutes, or hours.

8. Click **OK**.



Switching Tabs for Multiple Infrastructure Objects

To enable automatic switching of tabs and create a rule that switches tabs for specific objects:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. In the main menu, click **Settings** > **Client Settings**.

   Alternatively, press `[CTRL + O]` on the keyboard.

3. In the **Client Settings** window, navigate to the **Tabs View** tab.

4. In the **Automatic tab switching rule** section, select **Switch tabs for these objects (recommended for NOC view)**.

5. Choose objects to include in the scope, and specify tabs that must be displayed.

   a. Click **Add** and choose the type of infrastructure objects to add — Veeam Backup & Replication, Veeam Backup for Microsoft 365, Virtual Infrastructure, VMware Cloud Director, or Business View.

   b. In the **Select scope** window, select check boxes next to objects you want to add to the scope and click **OK**.

      To select an object together with its child objects, click it with the left mouse button.

If you select several objects of different types, Veeam ONE will create a new rule for each object type. For example, if you select a resource pool with VMs, Veeam ONE will add a rule for the resource pool, and a rule for VMs inside it.

c. Select the added object in the list and click **Edit Tabs**.

Alternatively, you can click the **All tabs** link next to the added object.

d. In the **Select tabs** window, select check boxes next to tabs that must be displayed for an object and click **OK**.

e. Make sure that the **State** check box is selected for the newly added object. If the check box is cleared, the object will not be added to the scope of automatic tab switching.

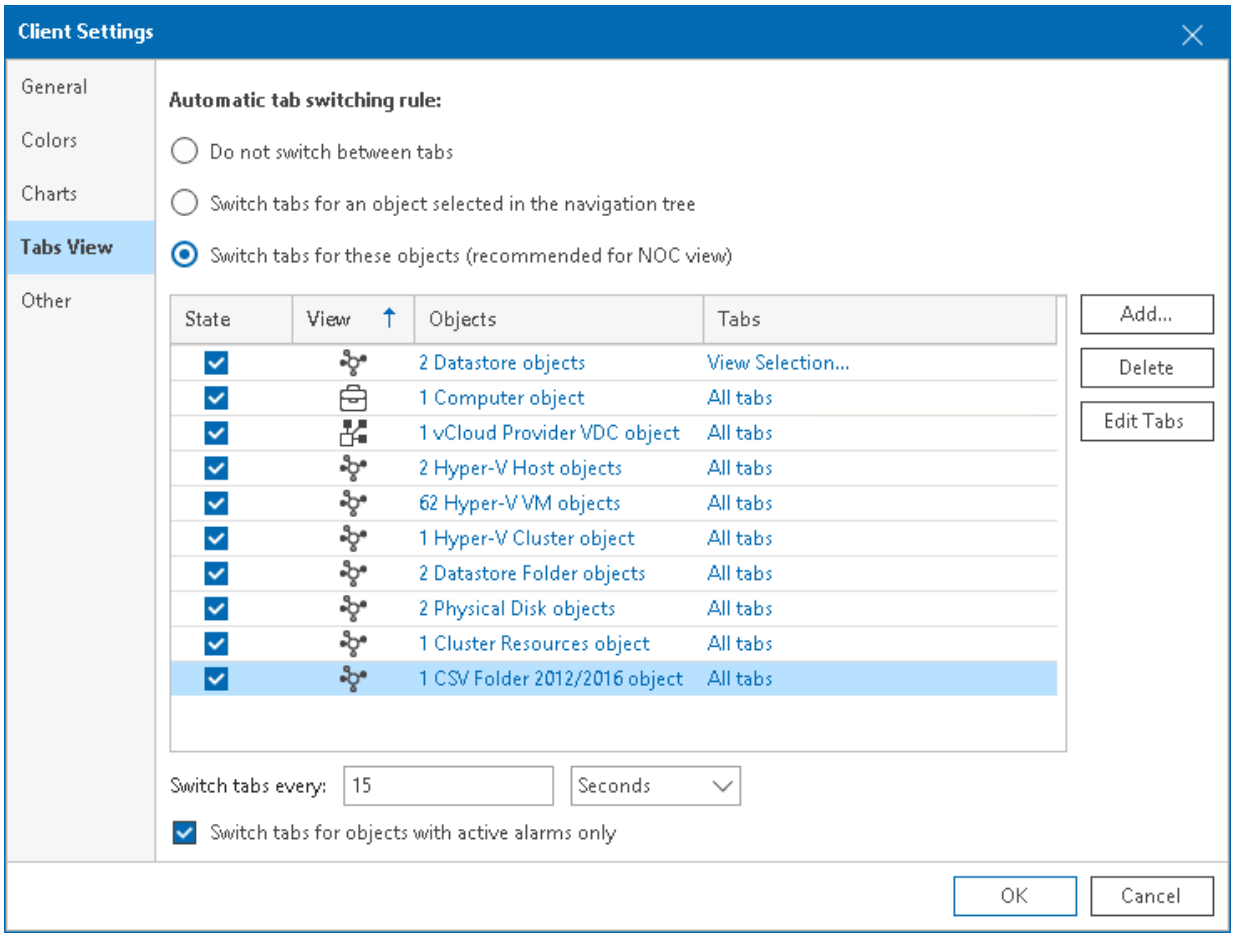
f. Repeat steps **a–e** for all objects that you want to add to the scope.

6. In the **Switch tabs every <time interval>** section, specify a time interval at which tabs must be switched.

You can specify an interval in seconds, minutes, or hours.

7. Select the **Switch tabs for objects with active alarms only** check box if Veeam ONE must switch tabs for infrastructure objects that have unresolved alarms — that is, only for objects that have potential problems and that may need your attention.

8. Click **OK**.



Other Settings

To specify miscellaneous client settings:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. In the main menu, click **Options** > **Client Settings**.

   Alternatively, press `[CTRL + O]` on the keyboard.

3. In the **Client Settings** window, navigate to the **Other** tab.

4. In the **Miscellaneous** section, specify the following settings:

   - From the **Logging level** list, choose the level of detail for logging:
     - **High** – includes events with the *Info*, *Warning* and *Error* status.
     - **Low** – includes events with the *Warning* and *Error* status.
     - **Off** – disables logging.
   - Select the **Minimize to tray** check box if you want to hide Veeam ONE Client to a system tray icon when the Veeam ONE Client window is minimized.
   - Clear the **Show child object status on a parent node in the Infrastructure tree** check box if every object in the inventory tree must reflect its own state only.

     If this check box is cleared, the state of child objects with errors and warnings will not be reflected on parent nodes. If this check box is selected, Veeam ONE will show downward arrows on parent nodes to reflect the problematic state of child objects. For details on displaying the infrastructure inventory tree, see Inventory Pane.

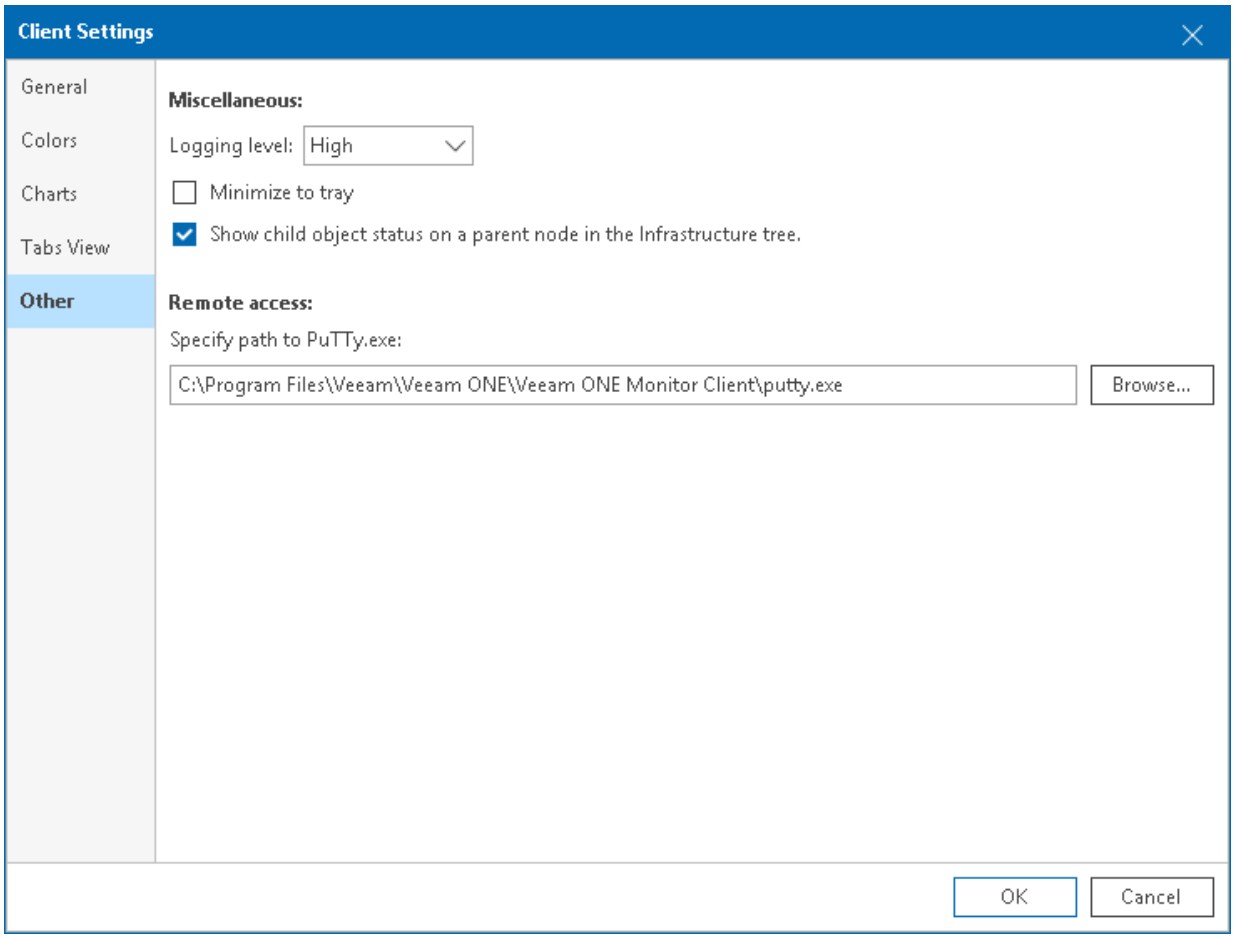
5. In the **Remote access** section, specify the path to the `PuTTy.exe` file.

   Veeam ONE requires PuTTy to provide easy access to consoles of Linux VMs.

   For details on PuTTY, see PuTTY Documentation Page.

   For details on accessing VM console for VMware vSphere, see VMware Remote Console (VMRC).

For details on accessing VM console for Microsoft Hyper-V, see Microsoft Hyper-V VM Console.



Veeam ONE Server Settings

Veeam ONE server settings include:

- Mail Server Settings
- Notification Policy
- SNMP Traps
- ServiceNow Integration
- Syslog Integration
- Guest OS Credentials
- Monitored Datastores
- Monitored VMs
- Business View
- Login Sessions
- Audit Log
- Banners
- Other Settings

Mail Server Settings

In mail server settings, you can configure email settings that will be used for sending alarm notifications, dashboards and reports by email.

To specify SMTP server settings:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. In the main menu, click **Settings** > **Server Settings**.

   Alternatively, press `[CTRL + S]` on the keyboard.

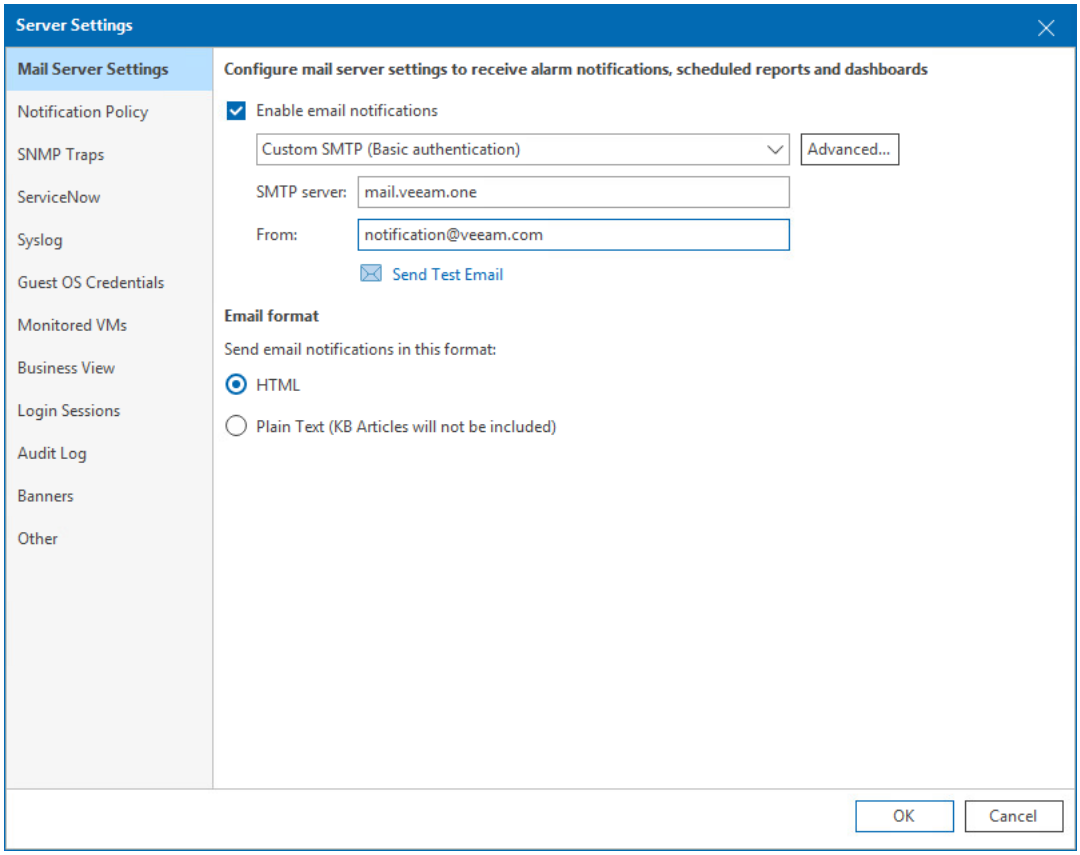
3. In the **Server Settings** window, open the **Mail Server Settings** tab.

4. To configure email notification settings, select the **Enable email notifications** check box.

   For details on configuring mail server settings, see Configuring Notification Settings.

5. In the **Email format** section, choose the format of email messages notifying about Veeam ONE alarms.

   For details on configuring format of alarm email notifications, see Configuring Email Notifications.



Notification Policy

In notification policy settings, you can configure the default email notification group, set the necessary notification policies, and specify other notification settings.

To specify notification policy settings:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. In the main menu, click **Settings** > **Server Settings**.

   Alternatively, press `[CTRL + S]` on the keyboard.

3. In the **Server Settings** window, open the **Notification Policy** tab.

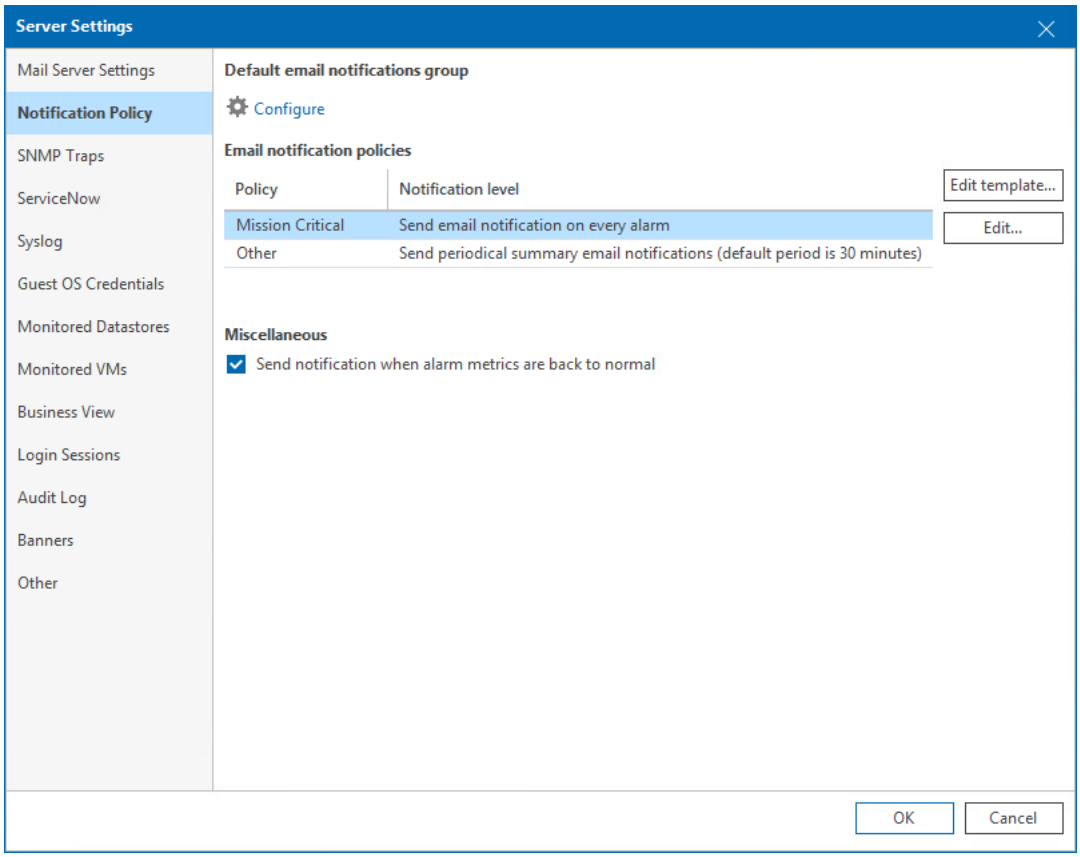
4. Configure email notifications:

   a. In the **Default email notification group** section, configure a list of recipients who must receive email notifications about Veeam ONE alarms.

   b. In the **Email notification policies** section, specify how often email notifications about Veeam ONE alarms must be sent.

   c. In the **Miscellaneous** section, choose whether you want to send email notifications when conditions that triggered alarms return to normal.

For details on configuring alarm notification options, see Configuring Email Notifications.



SNMP Traps

In SNMP settings, you can specify trap notification settings for sending notifications about alarms.

To specify SNMP settings:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

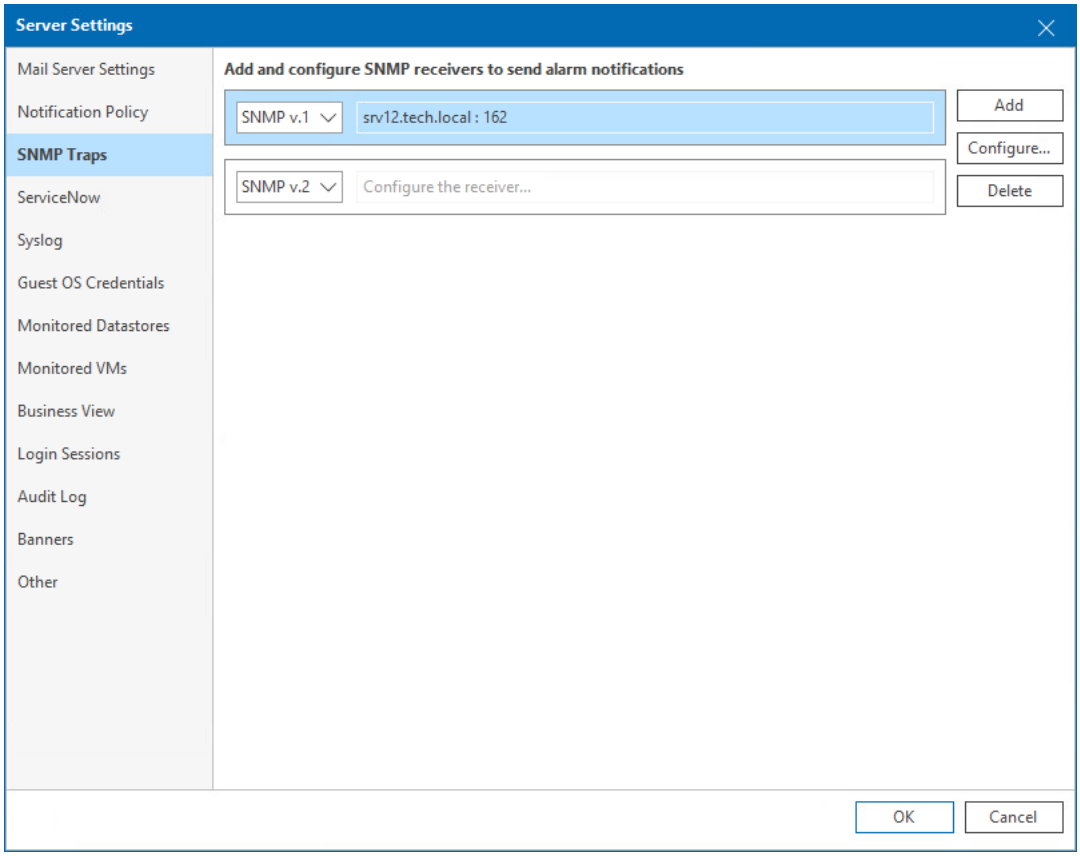
2. In the main menu, click **Settings** > **Server Settings**.

   Alternatively, press `[CTRL + S]` on the keyboard.

3. In the **Server Settings** window, open the **SNMP Traps** tab.

4. Configure SNMP settings for sending trap notifications about alarms.

For details on configuring SNMP notification options, see Configuring SNMP Traps.



ServiceNow Integration

The ServiceNow integration provides Veeam ONE with enhanced visibility and faster alerts triggered directly as ServiceNow incidents. For each triggered alarm, Veeam ONE creates a ServiceNow incident. When the alarm is resolved in Veeam ONE, the corresponding incident is also resolved in ServiceNow.

At the **ServiceNow** step of the wizard, specify your ServiceNow settings used for ServiceNow integration.

To specify ServiceNow integration details:

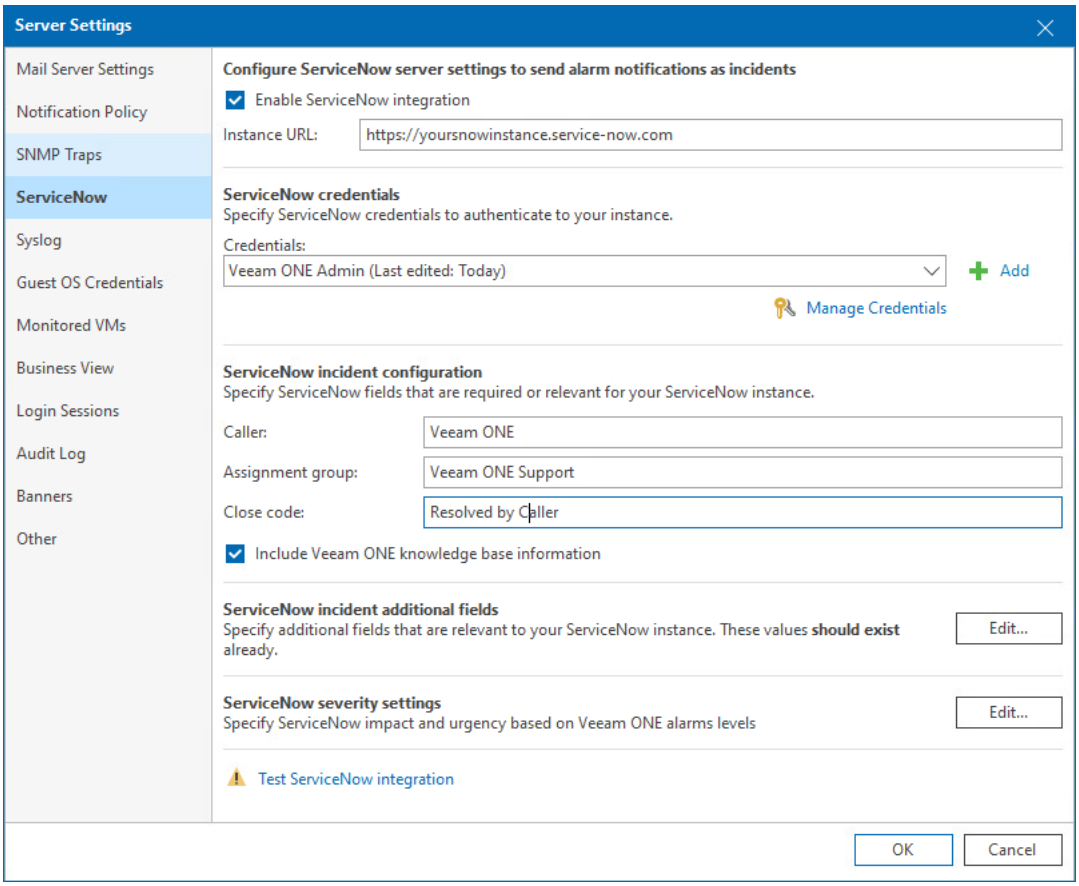
1. Select the **Enable ServiceNow integration** check box.
2. In the **Instance URL** field, specify the ServiceNow instance URL, for example `https:\\yourinstancename.service-now.com`.
3. Specify **ServiceNow credentials** used to authenticate your ServiceNow instance administration.

   For details on permissions required for connection, see Connection to ServiceNow.

   For details on adding credentials records, see Credentials Manager.
4. [Optional] If your organization policy requires additional ServiceNow credentials, click **Add** and enter your additional credentials.
5. In the **ServiceNow incident configuration** section, specify the following details:
   - **Caller** — defines the caller name assigned for the purposes to create, update, and resolve incidents. *Veeam ONE* is the default value, alternatively you can define a custom name if it already exists on your ServiceNow instance.
   - **Assignment group** — defines the name for the assignment group for the purposes to create, update, and resolve incidents. *Veeam ONE Support* is the default value, alternatively you can define a custom name if it already exists on your ServiceNow instance.
   - **Close code** — defines the close code for resolved incidents. Use only the close code defined on your ServiceNow instance.
   - [Optional] Select the **Include Veeam ONE Knowledge Base** information check box to mark incidents for knowledge base articles.
6. [Optional] In the **ServiceNow incident additional fields** section, click **Edit** and add additional **Name** and **Value** parameters to add additional fields relevant to your company's ServiceNow requirements. You must provide both the **Name** and **Value** in the same form as found in the ServiceNow REST API.
7. [Optional] In the **ServiceNow severity settings** section, click **Edit** and configure the ServiceNow impact and urgency levels that correspond to each Veeam ONE *Error*, *Warning* and *Information* alarm. To test that the severity settings match the correct values in your ServiceNow instance, click **Check available values**. To return the severity settings to their default values click **Back to default values**.
8. To test the connection settings, click **Test ServiceNow integration**.

   Veeam ONE will establish a connection to ServiceNow, create and resolve a test incident.

If you select the **Enable ServiceNow integration** check box and do not test the connection, Veeam ONE will verify it before saving the server settings. Additionally, the connection is checked when each Server Settings item (*Mail Server Settings*, *Email Notifications* and so on) changes.



For details on ServiceNow alarm server settings, see Configuring Alarm Notifications.

Syslog Integration

Syslog integration allows you to send pre-built Veeam ONE alarms and data for audit events for reuse within your Syslog server environment.

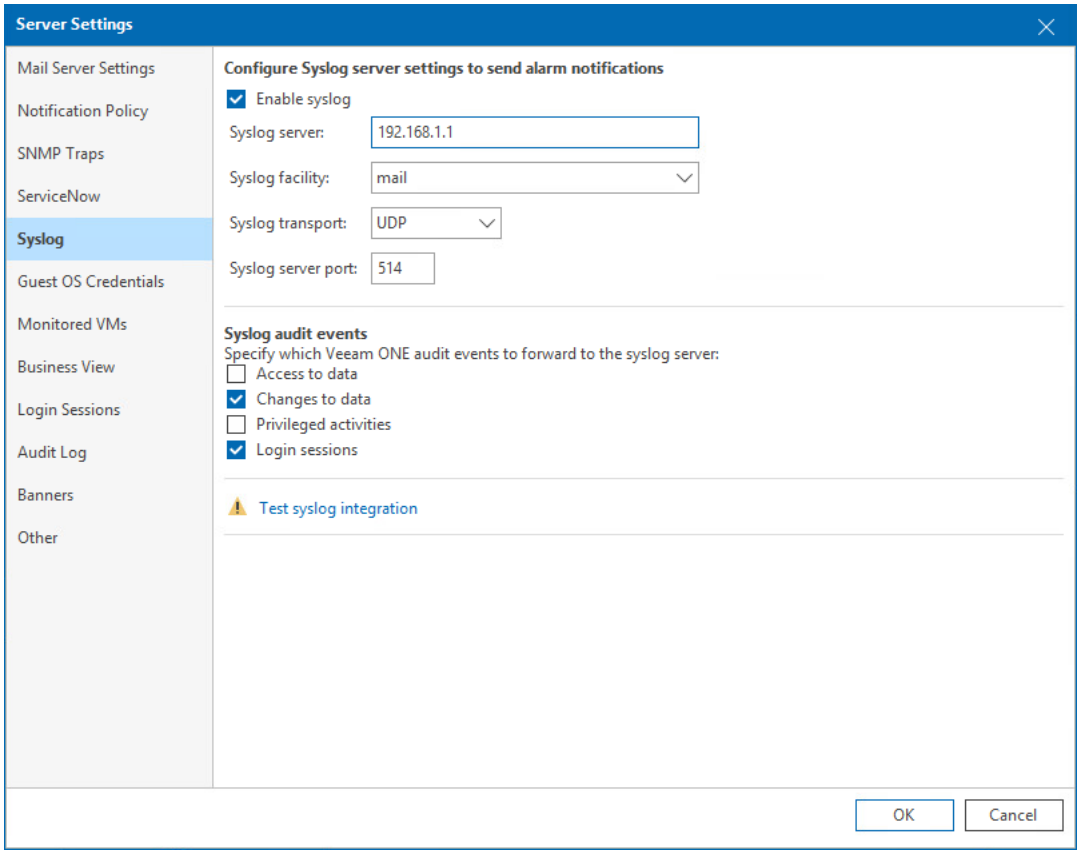
At the **Syslog** step of the wizard, specify your Syslog settings used to return alarms to your Syslog instance.

To specify your Syslog integration details:

1. Click the **Enable syslog** check box.
2. Enter **Syslog server** details:
   - **Syslog server —** define the IPv4 or IPv6 address of your Syslog instance.
   - **Syslog facility —** define the value used to identify the source of the alarm. By default this is set to **mail**.
   - **Syslog transport** — define TCP, TCP with TLS, or UDP. By default this is UDP.
   - **Syslog server port** — the port used to connect to your Syslog integration instance. By default this is 514.
3. Select your required **Syslog Audit events** to send to your Syslog integration:
   - Access to data
   - Changes to data
   - Privileged activities
   - Login sessions

4. To test the connection settings, click **Test syslog integration**. This creates a test connection to Syslog and returns a signal confirming a successful connection.

   If you select the **Enable syslog** check box and do not test the connection, Veeam ONE will verify it before saving the server settings. Additionally, the connection is checked when each Server Settings item (*Mail Server Settings*, *Email Notifications* and so on) changes.



For details on Syslog alarm server settings, see Configuring Alarm Notifications.

Guest OS Credentials

In guest OS credentials settings, you can set an account that will be used to collect data from the guest OS of Windows and Linux-based VMs.

To access **Guest OS Credentials** settings:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. In the main menu, click **Settings** > **Server Settings**.

   Alternatively, press `[CTRL + S]` on the keyboard.

3. In the **Server Settings** window, open the **Guest OS Credentials** tab.

4. Specify guest OS credentials:

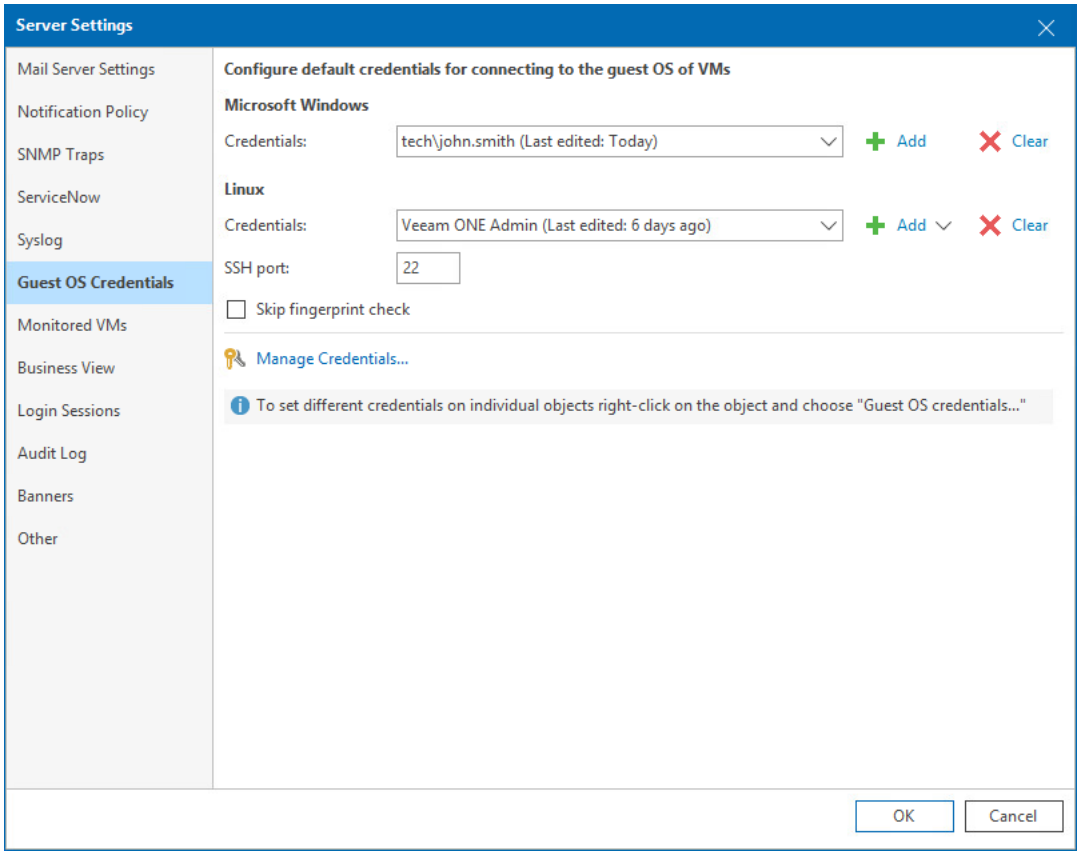
   a. In the **Microsoft Windows** section, select credentials of an account that will be used to collect data from the guest OS of Windows-based VMs. To create a new credentials record, click **Add**.

   b. In the **Linux** section, select credentials of an account that will be used to collect data from the guest OS of Linux-based VMs. To create a new credentials record, click **Add** and select **Standard account** or **Linux private key**.

      In the **SSH Port** field, change the default connection port if required.

      To disable fingerprint validation for Linux VMs, select **Skip fingerprint check**.

   To access credentials manager, click the **Manage Credentials** link. For details on working with credentials, see Credentials Manager.



TIP:

You can set guest OS credentials on individual VMs. To do this, right-click a VM and choose **Guest OS Credentials** from the shortcut menu.

Monitored Datastores

You can manage the list of datastores that must be included in the reporting scope:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

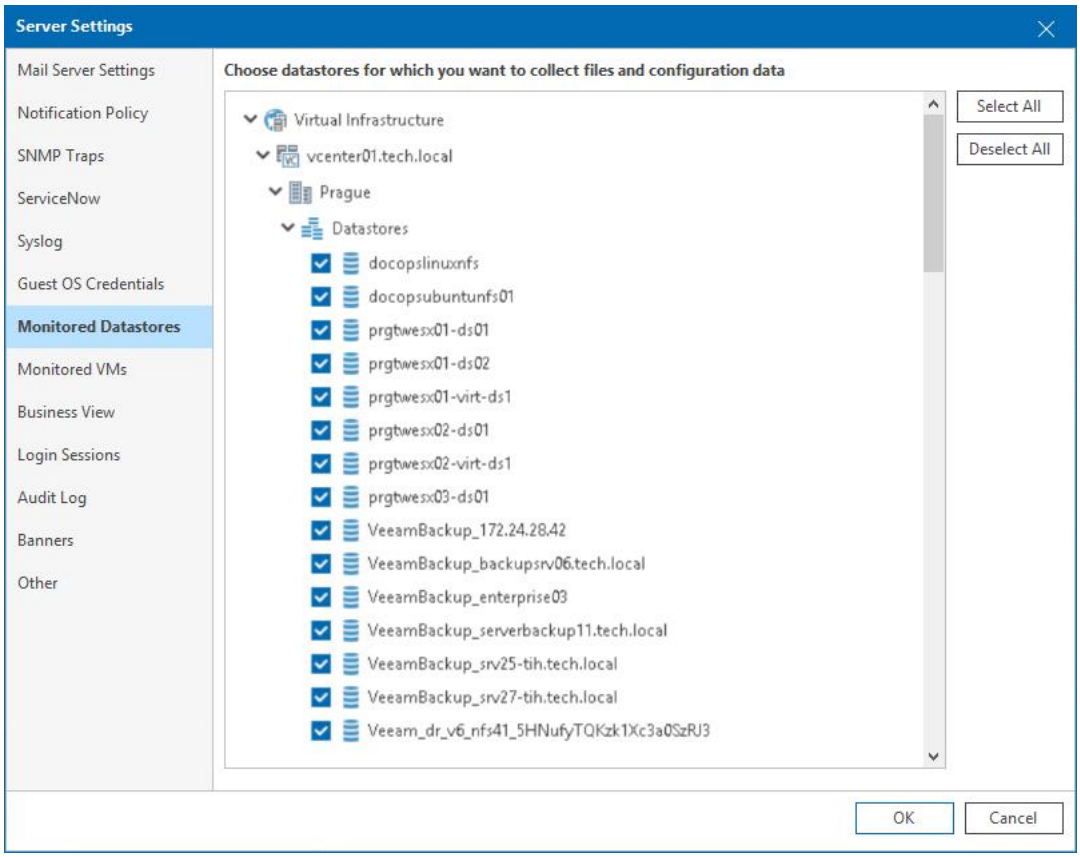
2. In the main menu, click **Settings** > **Server Settings**.

   Alternatively, press `[CTRL + S]` on the keyboard.

3. In the **Server Settings** window, open the **Monitored Datastores** tab.

4. Expand the virtual infrastructure tree and select check boxes next to datastores that you want to include in reporting.

For details on choosing datastores to report on, see Choosing Datastores to Report On.



Monitored VMs

On the **Monitored VMs** tab, you can manage the list of VMs and VM containers (hosts, clusters, datastores and so on) that must be included in the monitoring and reporting scope.

To choose what VMs and VM containers must be included in the monitoring and reporting scope:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

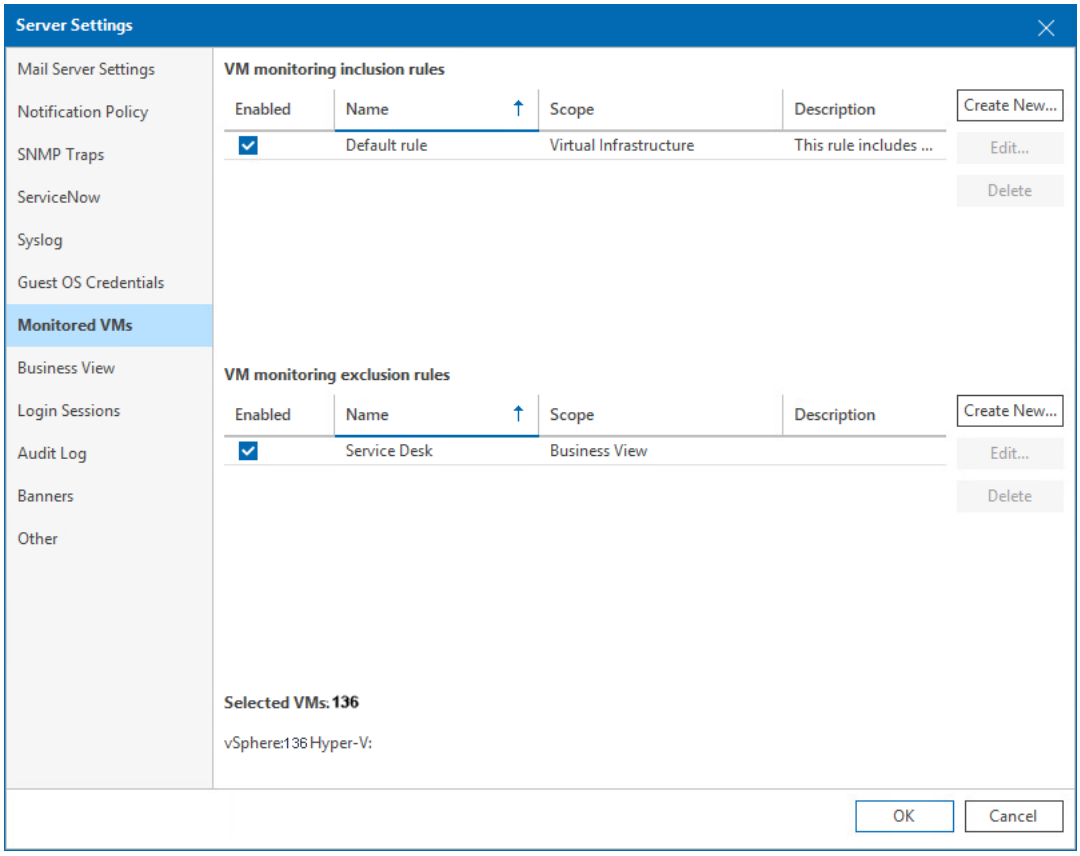
2. In the main menu, click **Settings** > **Server Settings**.

   Alternatively, press `[CTRL + S]` on the keyboard.

3. In the **Server Settings** window, open the **Monitored VMs** tab.

4. Create rules that will be used to include VMs and VM containers to and exclude VMs and VM containers from monitoring and reporting.

For details on choosing objects to monitor and report on, see Choosing VMs and VM Containers to Monitor and Report On.



Business View

On the **Business View** tab, you can define the following settings:

- Categorization model — choose whether you want to import an existing categorization model or create your own categories and groups.
- Ungrouped objects — hide ungrouped objects from the Business View inventory tree.
- Defining Exclusions — define objects that must be excluded from categorization.

For details on Business View categorization, see Business View.

Selecting Categorization Model

To select a categorization model:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. In the main menu, click **Settings** > **Server Settings**.

   Alternatively, press `[CTRL + S]` on the keyboard.

3. In the **Server Settings** window, open the **Business View** tab.

4. Select one of the following categorization options:

   - **From vCenter Server and System Center Virtual Machine Manager** — select this option if you have vCenter Server tags or System Center Virtual Machine Manager properties assigned to virtual infrastructure objects, and you want to use these tags and properties to categorize objects in Veeam ONE Client.
   - **From CSV file** — select this option if you want to synchronize categorization data between Business View and a 3rd party application using a CSV file.

     For details on configuring data synchronization, see Importing Categorization Data Automatically.
   - **Do not import** — select this option if you want to create a custom categorization model in Business View.

     For details on creating Business View categories, see Creating Business View Categories and Groups.
   - **Import categorization model from CSV file once** — select this option if you want to map categorization data from a 3rd party application to Business View groups using a CSV file.

     For details on manual import from, see Importing Categorization Data Manually.

NOTE:

- You cannot enable synchronization with vCenter Server and System Center Virtual Machine Manager tags and properties and a CSV file at the same time. When you switch between these options or disable import, Veeam ONE Client deletes all previously imported categories.
- Categorization model settings do not affect tags collection. For example, if you select the **Do not import** option, Veeam ONE will still collect vCenter Server tags or System Center Virtual Machine Manager properties, but will not use them for building categories and groups.

Hiding Ungrouped Objects

To hide ungrouped objects from the Business View inventory tree:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. In the main menu, click **Settings** > **Server Settings**.

   Alternatively, press `[CTRL + S]` on the keyboard.

3. In the **Server Settings** window, open the **Business View** tab.

4. In the **Ungrouped objects** section, select **Hide ungrouped objects from Business View tree**.

   If you select **Hide ungrouped objects from Business View tree** check box, Veeam ONE Client will hide the Uncategorized group and all objects within this group from the Business View inventory tree.

For details on displaying the Business View inventory tree, see Business View.

Defining Exclusions

To exclude objects from Business View categorization:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. In the main menu, click **Settings** > **Server Settings**.

   Alternatively, press `[CTRL + S]` on the keyboard.

3. In the **Server Settings** window, open the **Business View** tab.

4. In the **Exclusion rules** section, select an object type and click **Edit**.

5. [For virtual infrastructure objects] Choose platform for which you want to define exclusions (*VMware*, *Hyper-V*).

6. In the **Edit Global Exclusion Rule** window, click **Add Condition** and specify exclusion conditions:

   - From the **Property** drop-down list, select an object property.

     The list contains all object properties that Veeam ONE collects from virtual and backup infrastructure servers.

   - From the **Operator** drop-down list, select a conditional operator.

     The list contains the following operators: *Equals*, *Does not equal*, *Starts with*, *Ends with*, *Contains*, *Does not contain*, *Wildcard*.

   - In the **Value** field, specify a value that will be checked in the condition.

   The condition will be evaluated against discovered objects. To add another condition, click **Add Condition**.

   By default, conditions are linked by the **AND** operator. That is, an object is excluded when all specified conditions are met. You can change this behavior by linking conditions with the **OR** operator. In this case, Veeam ONE will exclude an object from categorization when a condition for any of the linked rules is met.

For example, you can exclude VMs based on their power state, datacenter name, and guest OS. If you want to exclude all powered on VMs that reside in datacenter Atlanta or run Linux as their guest OS, you must link these conditions. The second and the third conditions will be linked to each other with the OR operator. The first condition will be linked to them with the AND operator.

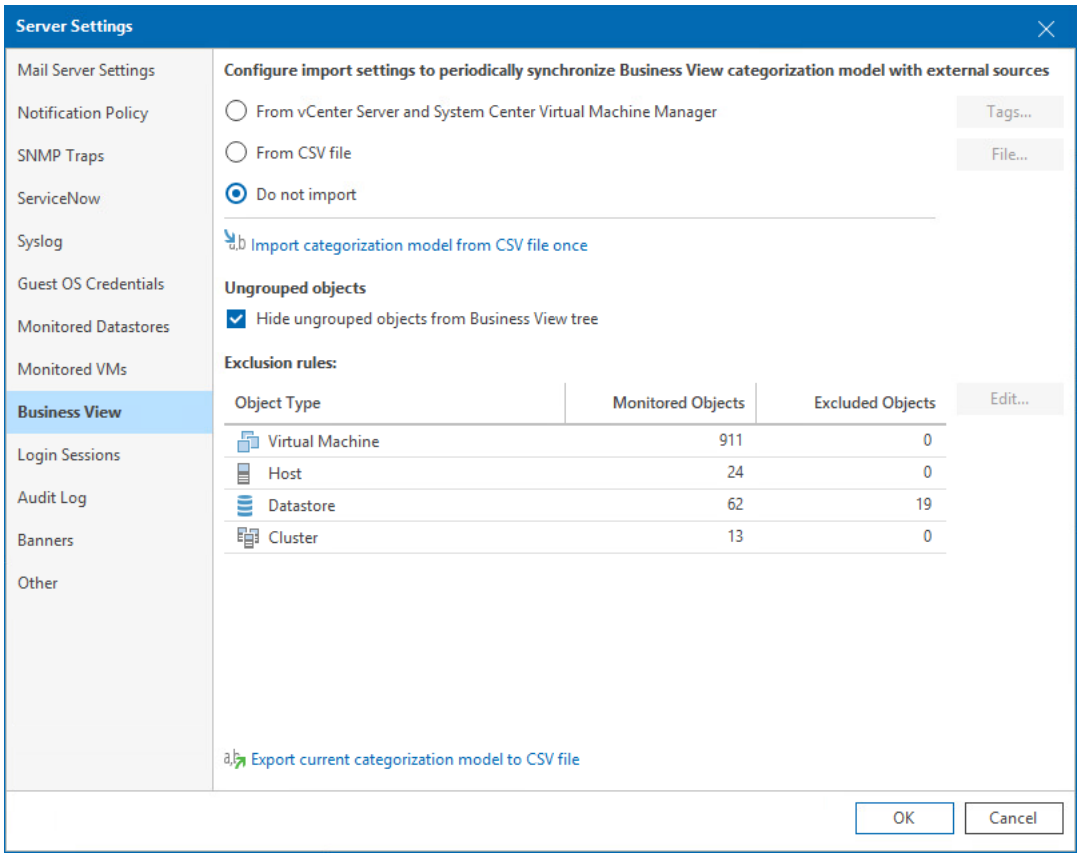
To link conditions:

a. Select check boxes next to the necessary conditions and click **Link**.

b. In the **Rule Condition** window, select a link operator and click **OK**.

Linking supports 3 levels of nesting.

6. Click **Save**.



Login Sessions

On the **Login Sessions** tab, you can define user session settings and timeouts.

To configure Veeam ONE Client login sessions settings:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. In the main menu, click **Settings** > **Server Settings**.

   Alternatively, press `[CTRL + S]` on the keyboard.

3. In the **Server Settings** window, open the **Login Sessions** tab.

4. To limit the duration of an idle session:

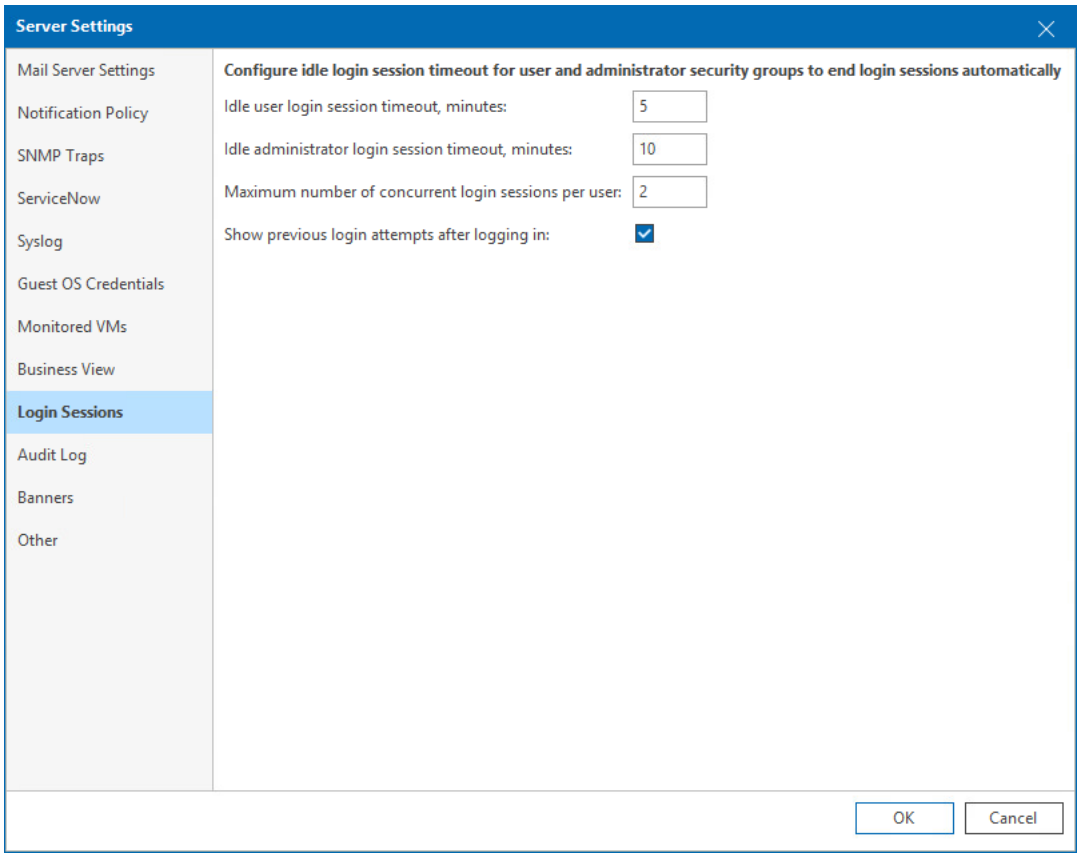
   - [For users included in the *Veeam ONE Power Users* and *Veeam ONE Read-Only Users* security groups] specify the value in the **Idle user login session timeout, minutes** field.
   - [For users included in the *Veeam ONE Administrators* security group] specify the value in the **Idle administrator login session timeout, minutes** field.

   For details on Veeam ONE security groups, see Security Groups.

5. To limit the number of simultaneous login sessions under the same user credentials, specify the value in the **Maximum number of concurrent login sessions per user** field.

   To allow unlimited number of login sessions, specify 0.

6. To display date and time of the last successful or failed authentication to a user, select the **Show previous login attempts after logging in** check box.



Audit Log

In the audit log settings, you can select which user activities in Veeam ONE Client and Veeam ONE Web Client must be logged and enable automatic shutdown of Veeam ONE services.

To configure audit log settings:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. In the main menu, click **Settings** > **Server Settings**.

   Alternatively, press `[CTRL + S]` on the keyboard.

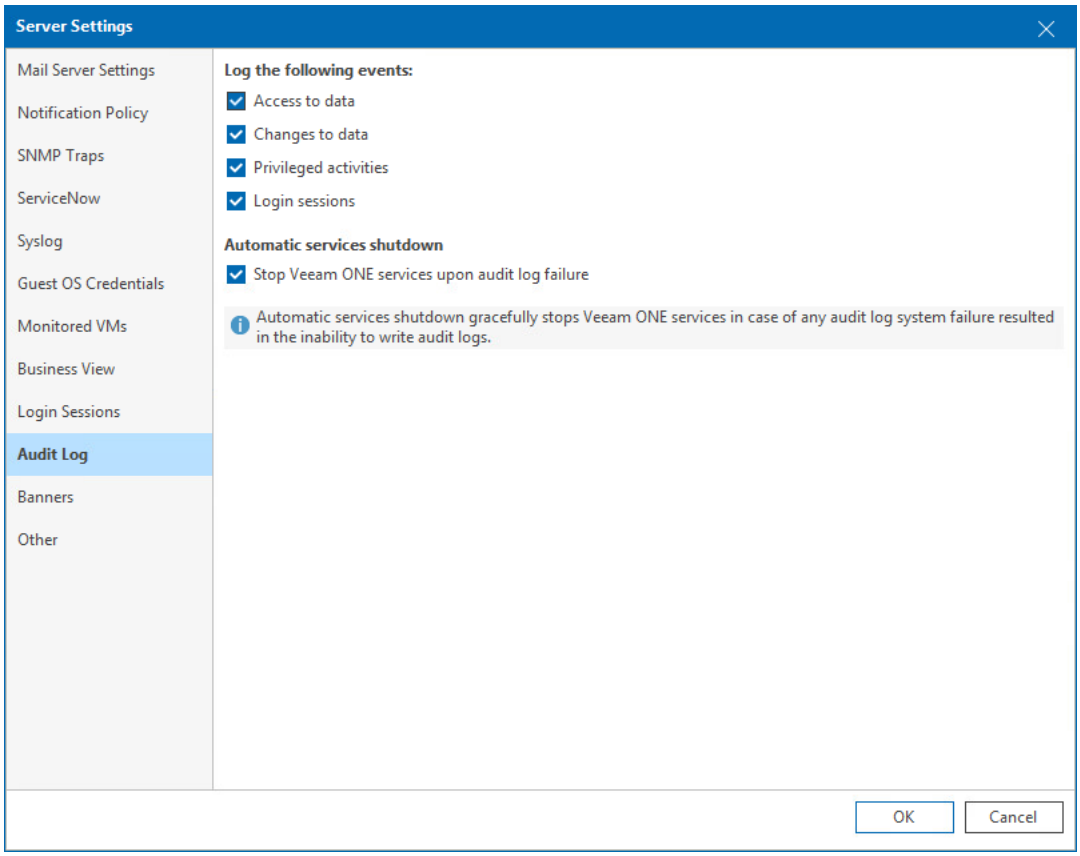
3. In the **Server Settings** window, open the **Audit Log** tab.

4. Select which events you want to log:

   - **Access to data** — fill this check box to log data access events, for example, switching tabs or opening dialogs.
   - **Changes to data** — fill this check box to log data modification events, for example, changing Veeam ONE Server settings, report parameters or modifying tree view settings.
   - **Privileged activities** — fill this check box to log administrative events, for example, managing Veeam Analytics service, updating a license or starting data collection.
   - **Login sessions** — fill this check box to log user sessions in Veeam ONE Client and Veeam ONE Web Client.

5. If you want to shut down Veeam ONE services in case Veeam ONE is unable to write audit logs, fill the **Stop Veeam ONE services upon audit log failure** check box.

   If events cannot be written to Windows Event Log, Veeam ONE will trigger the *Audit log failure* alarm and gracefully shut down Veeam ONE services.



Banners

On the **Banners** tab, you can configure consent and classified data banners to comply with data protection policies and regulations.

To configure banners:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. In the main menu, click **Settings** > **Server Settings**.

   Alternatively, press `[CTRL + S]` on the keyboard.

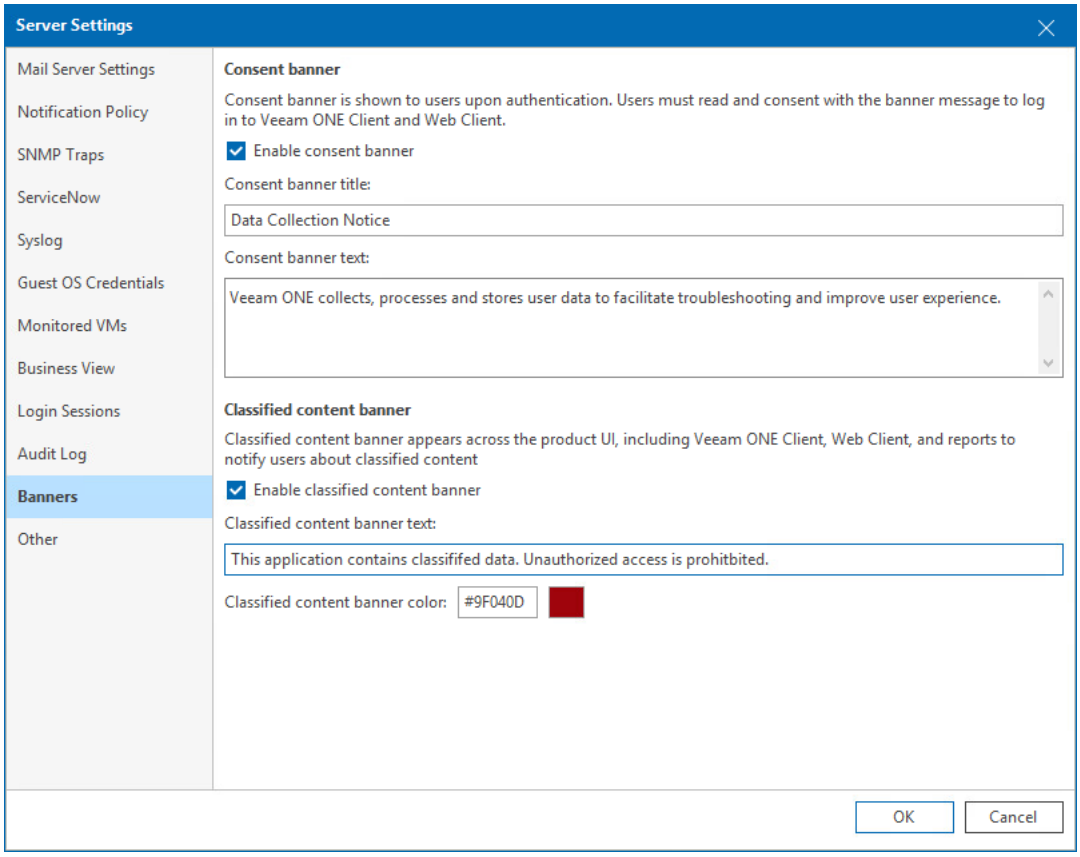
3. In the **Server Settings** window, open the **Banners** tab.

4. Select **Enable consent banner** and specify banner title and text.

   The banner will be shown to all users who log in to Veeam ONE Client and Veeam ONE Web Client. A user must click **I Agree** to continue working with Veeam ONE.

5. Select **Enable classified content banner** and specify text that will be shown to all users in Veeam ONE Client, Veeam ONE Web Client and generated reports.

   In the **Classified content banner color** field, specify banner color in HEX format.



Other Settings

To specify miscellaneous server settings:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. In the main menu, click **Settings** > **Server Settings**.

   Alternatively, you can press `[CTRL + S]` on the keyboard.

3. In the **Server Settings** window, open the **Other** tab.

4. In the **VMware Cloud Director** section, choose whether VMware Cloud Director VMs must be shown in the Virtual Infrastructure inventory tree:

   - If you select the **Hide VMware Cloud Director VMs from Virtual Infrastructure tree** check box, VMware Cloud Director VMs will be shown in the VMware Cloud Director inventory tree only.
   - If you select the **Hide expired VMware Cloud Director vApps from Cloud Infrastructure tree** check box, expired VMware Cloud Director vApps will not be shown in the VMware Cloud Director inventory tree.

   For details on displaying the virtual infrastructure inventory tree, see Virtual Infrastructure.

5. In the **Notifications** section, you can disable and enable notification messages about support contract expiration.

   If you select the **Disable support contract expiration notifications** check box, Veeam ONE will not display notification messages in the UI and notification emails.

   > **NOTE:**
   >
   > This option does not disable internal alarms notifying about support expiration. It only controls whether notification messages must be displayed in the UI and notification emails. For details on working with internal alarms, see Working with Internal Alarms.

6. In the **Support utility** section, click **Launch**, to run the Veeam ONE Settings Utility.

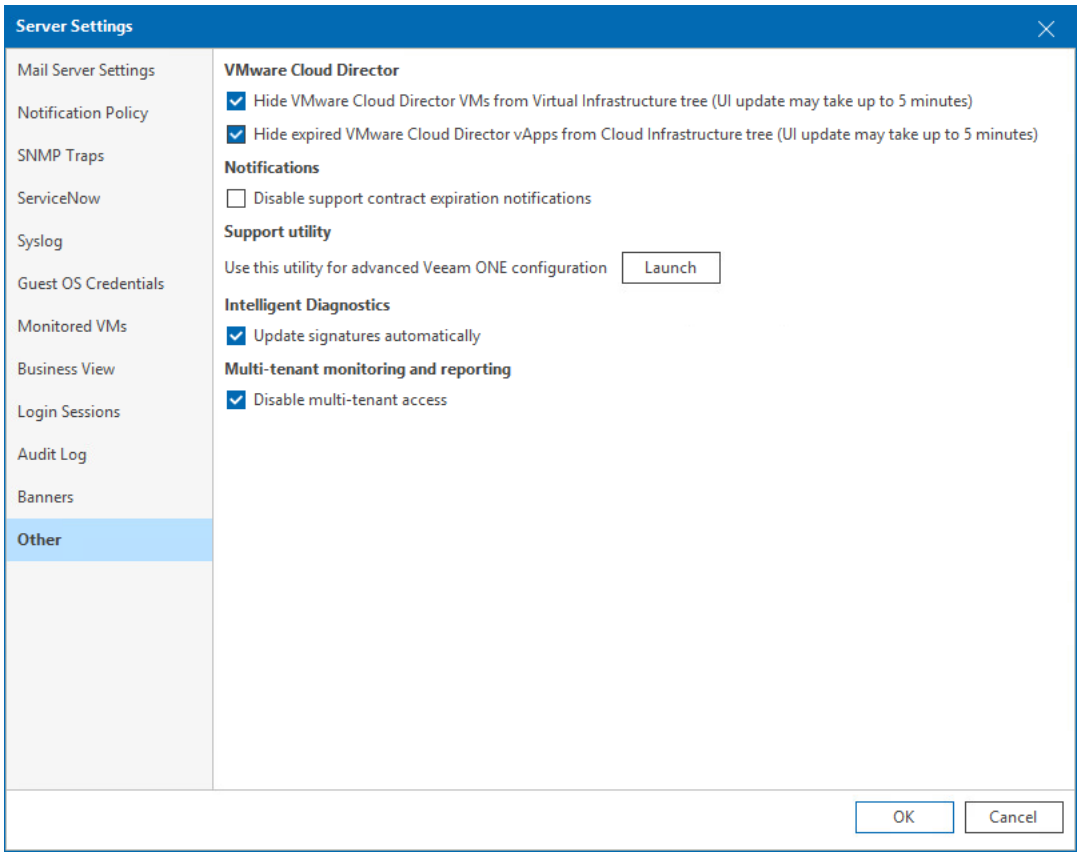
   The utility allows you to change configuration settings of the Veeam ONE software components. For details on working with Veeam ONE Settings Utility, see Veeam ONE Settings Utility.

   > **IMPORTANT!**
   >
   > The Veeam ONE Settings utility must be used only under the guidance of Veeam Support. It is strongly recommended that you obtain detailed instructions from the Veeam Support team before changing any configuration settings in your Veeam ONE deployment.

7. In the **Intelligent Diagnostics** section, you can disable and enable automatic update of Veeam Intelligent Diagnostics signatures:

   If you fill the **Update signatures automatically** check box, Veeam ONE will connect to the Veeam Technical Support web server and update signatures once a day. For details on working with signatures, see Managing Signatures.

8. In the **Multi-tenant monitoring and reporting** section, fill the **Disable multi-tenant access** check box to restrict access to Veeam ONE Client and Veeam ONE Web Client for users who have permissions on monitored infrastructure, but not included in Veeam ONE security groups. For details on multi-user access, see Multi-Tenant Monitoring and Reporting.



Choosing Objects to Monitor and Report On

After you connect Veeam Backup & Replication, Veeam Backup for Microsoft 365, VMware vSphere, VMware Cloud Director or Microsoft Hyper-V servers, Veeam ONE automatically includes in the data collection scope all child objects managed by these servers. If you do not need to monitor and report on all managed objects, you can exclude them from the data collection scope.

Choosing VMs and VM Containers to Monitor and Report On

By default, Veeam ONE collects data about all VMs and VM containers (hosts, clusters, datastores and so on) on connected virtualization servers. If you do not want to monitor and report on specific VMs or VM containers, you can configure rules to include and exclude VMs and VM containers from the data collection scope.

You can refine the data collection scope with the following types of rules:

- **Inclusion rules** define VMs and VM containers that must be monitored and reported on. Out-of-the-box, Veeam ONE includes a default inclusion rule that adds to the data collection scope all VMs and VM containers on connected servers.
- **Exclusion rules** define VMs and VM containers that must not be monitored and reported on.

> **NOTE:**
>
> If you exclude all child objects of a container from monitoring, Veeam ONE will not collect monitoring and reporting data for the parent container.

To configure an inclusion or exclusion rule, perform the following steps.

Step 1. Disable or Delete the Default Inclusion Rule

If you want to create one or more VM inclusion rules, you must delete or disable the default inclusion rule. Otherwise Veeam ONE will keep collecting data about all VMs and VM containers.

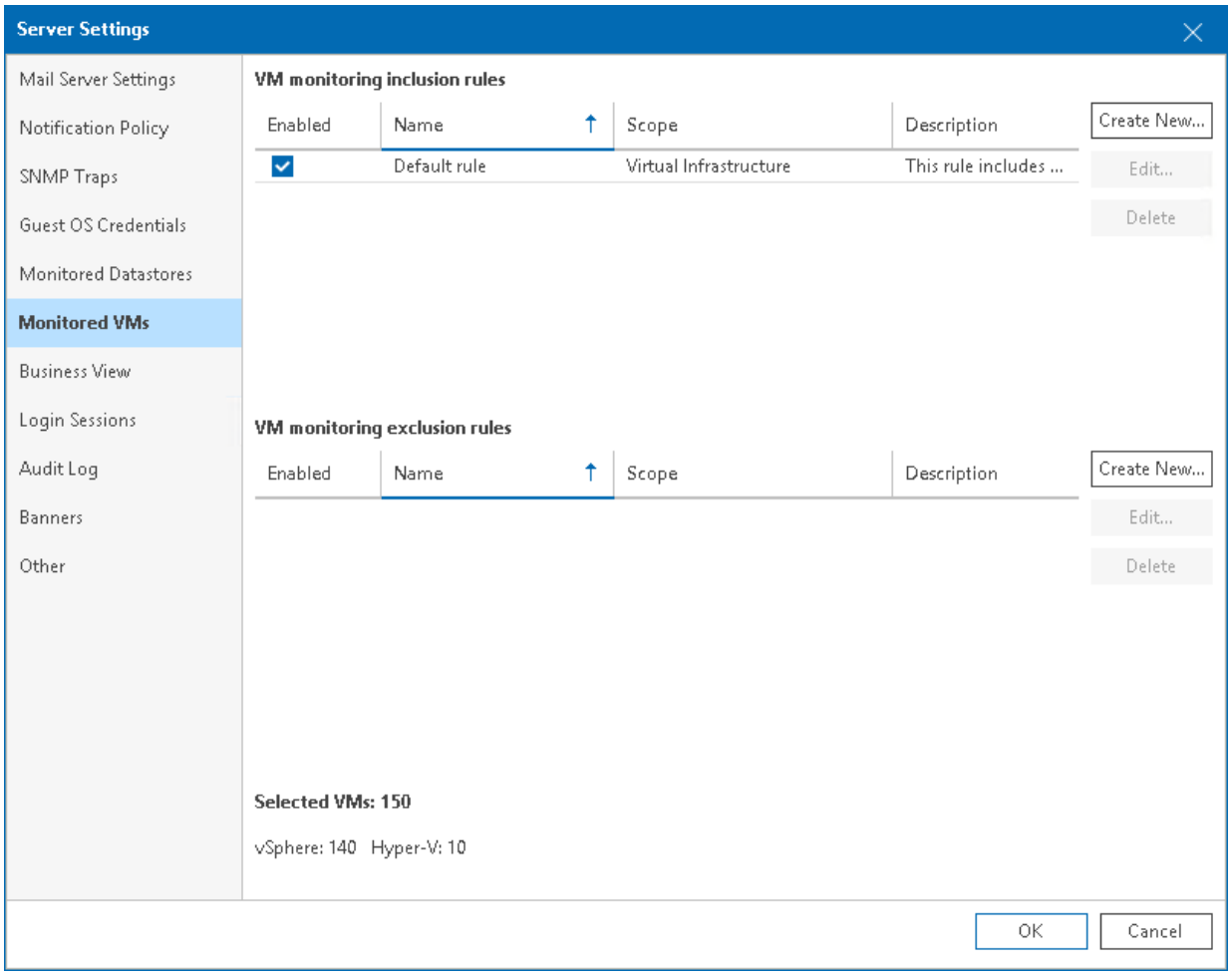
> **NOTE:**
>
> This step is not required if you want to create exclusion rules only.

To delete or disable the default inclusion rule:

1. Open Veeam ONE Client.
2. In the main menu, click **Settings** and select **Server Settings**.

   Alternatively, press the `[CTRL+S]` on the keyboard.
3. In the **Server Settings** window, open the **Monitored VMs** tab.
4. In the **VM Monitoring Inclusion Rules** section, delete or disable the default inclusion rule:
   - To disable the default inclusion rule, clear the **Enabled** check box next to the rule.

- To delete the default inclusion rule, select the rule and click **Delete** on the right.

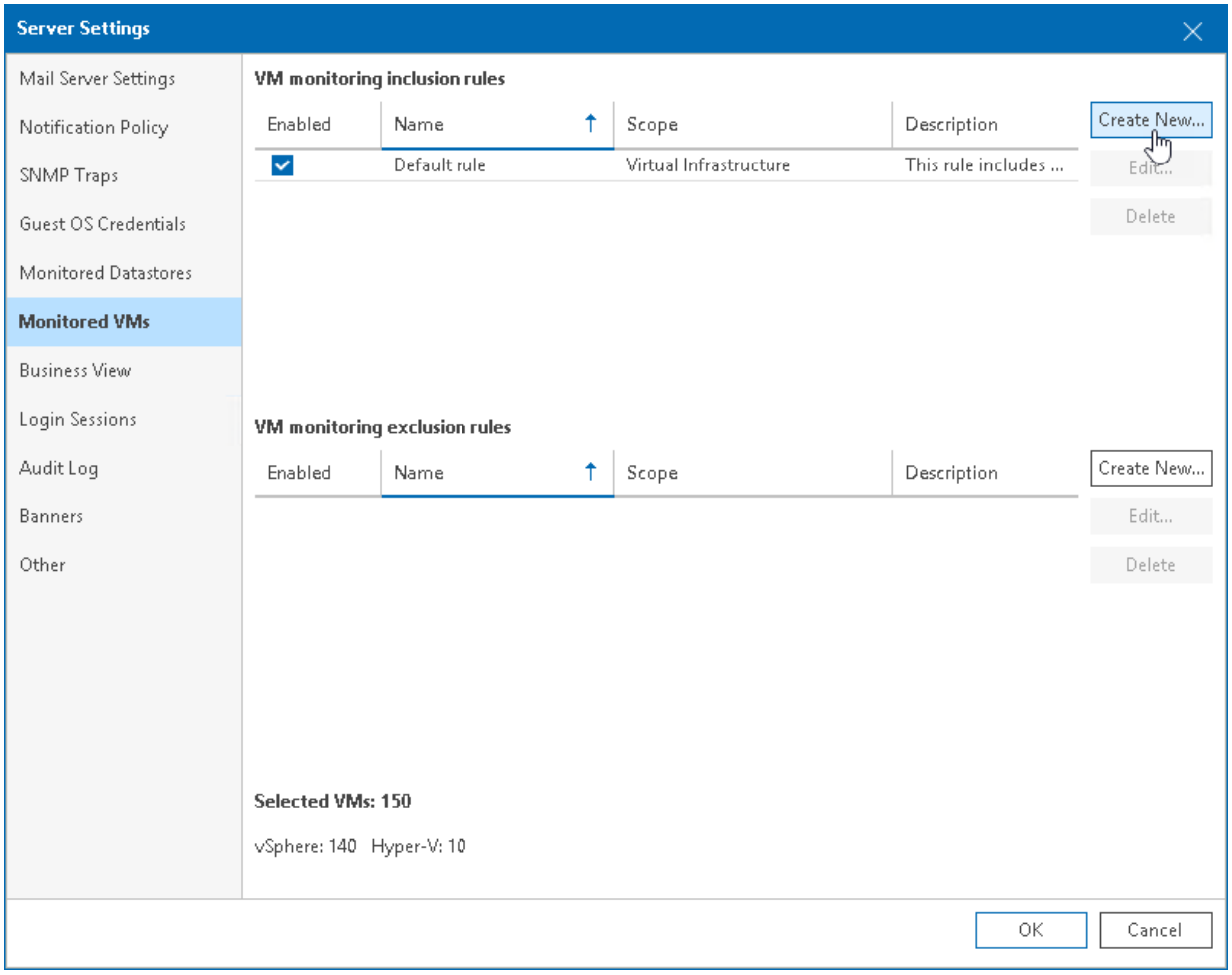


Step 2. Launch the Monitoring Rule Wizard

Launch the **Monitoring Rule** wizard:

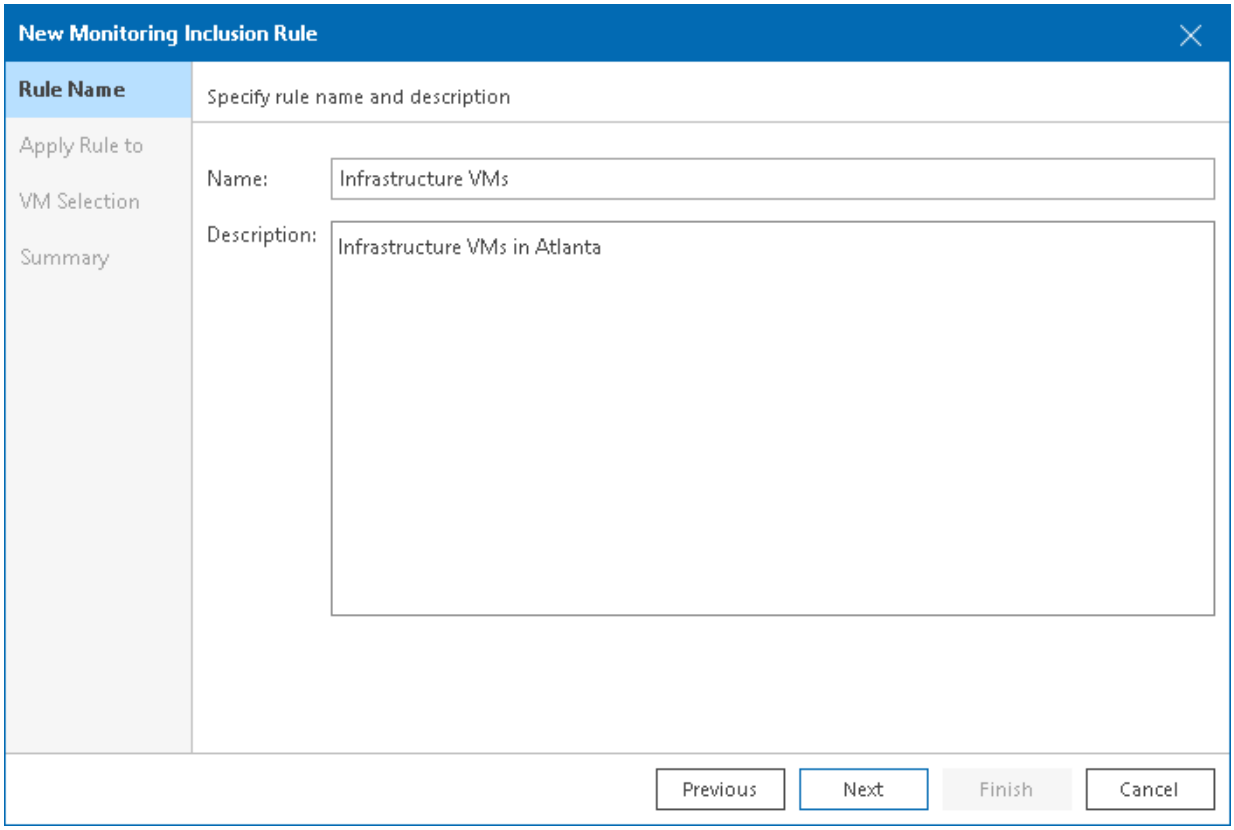
- To create an inclusion rule, in the **VM Monitoring Inclusion Rules** section, click **Create New**.

- To create an exclusion rule, in the **VM Monitoring Exclusion Rules** section, click **Create New**.



Step 3. Specify Rule Name and Description

At the **Rule Name** step of the wizard, specify a name and description for the new rule.

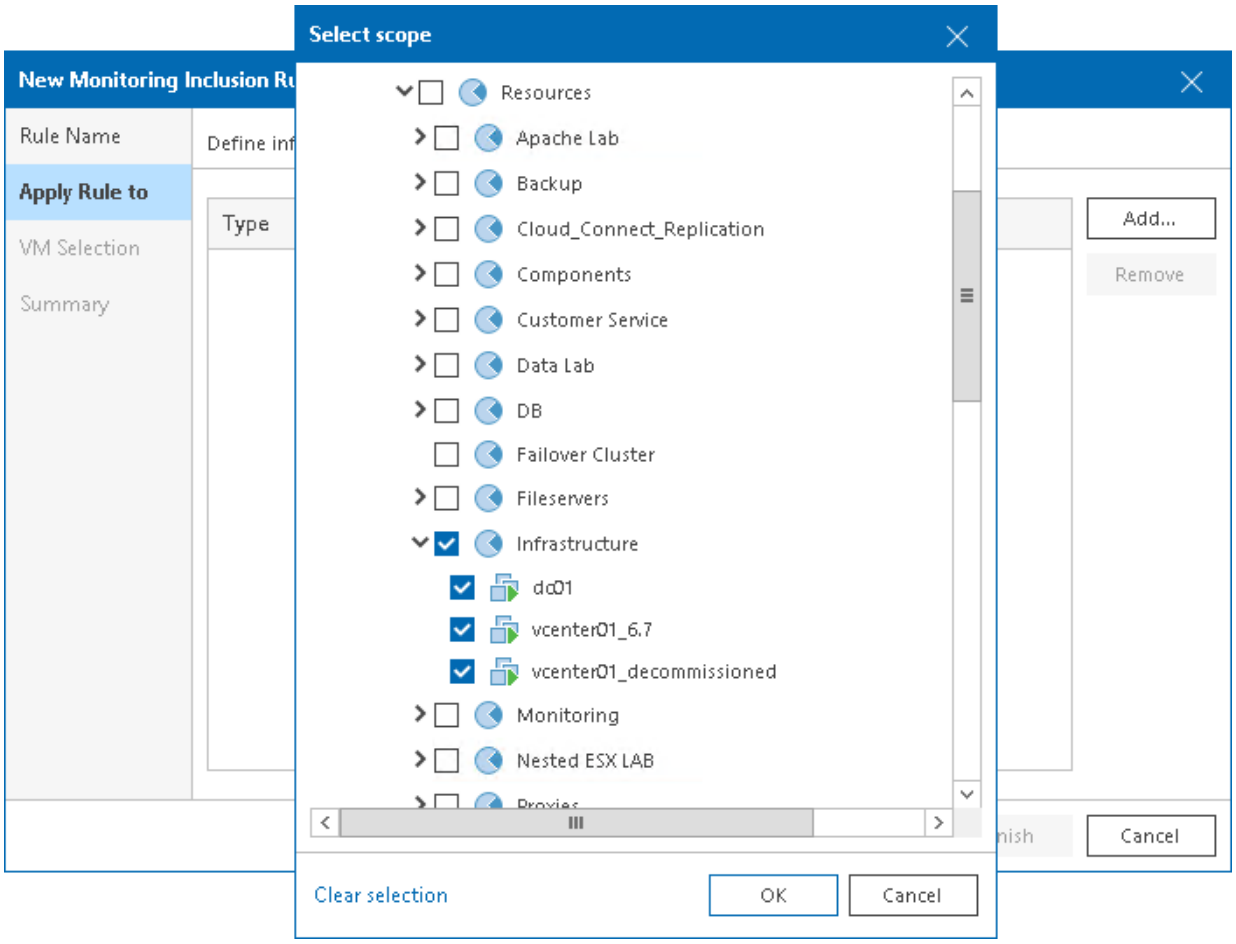


Step 4. Add Objects to the Rule

At the **Apply Rule to** step of the wizard, specify the scope of the virtual infrastructure to which the rule must apply:

1. Click **Add** and select *Infrastructure View*, *Business View* or *VMware Cloud Director View*.
2. In the **Select scope** window, select check boxes next to VM containers to which the rule must apply.

3. Click **OK**.



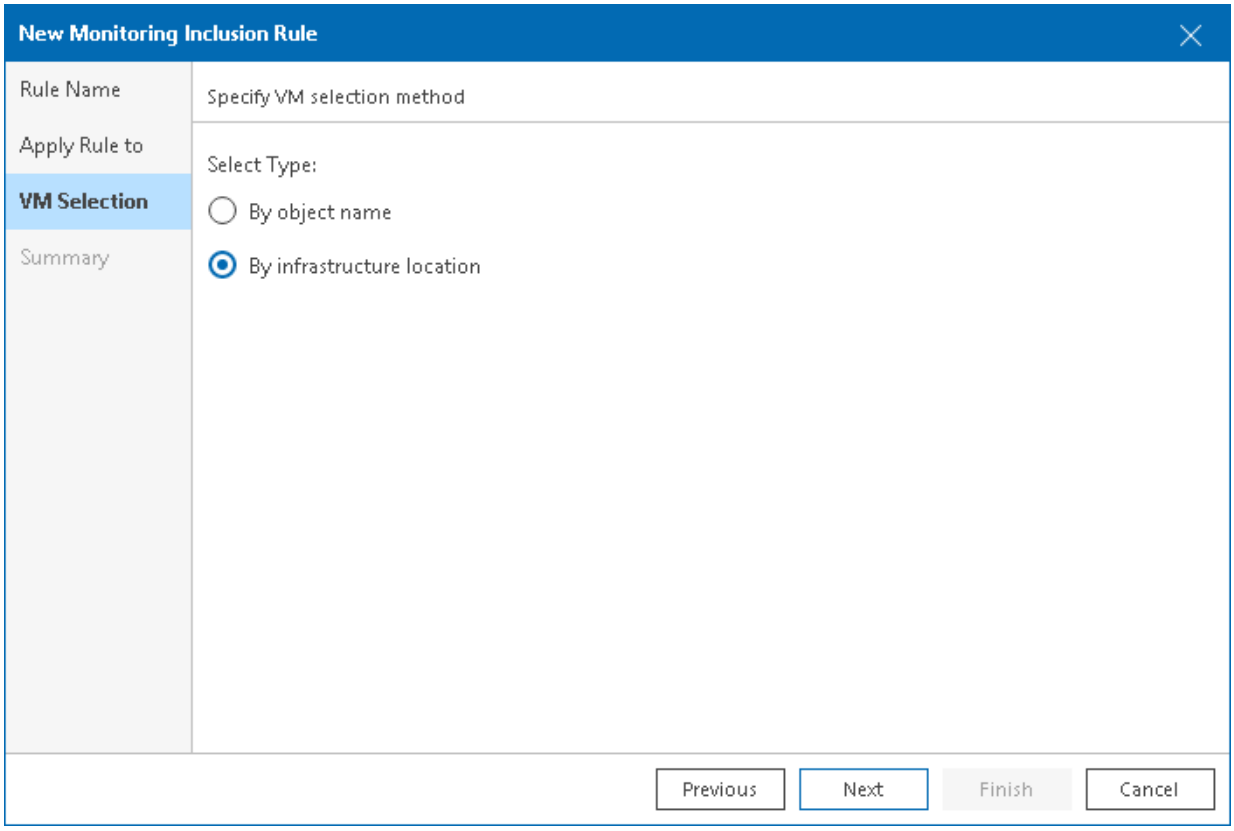
Step 5. Choose VM Selection Criterion

At the **VM Selection** step, choose a criterion according to which VMs and VM containers must be added to the rule:

- **By object name** — select this option if you want to add VMs to the rule based on VM names.

- **By infrastructure location** — select this option if you want to add to the rule VMs that belong to a specific level of the virtual infrastructure hierarchy (the level you specified at the **Apply Rule to** step of the wizard).

  You can use this selection criterion to find VMs that belong to a specific cluster, host, datastore or other VM container in the virtual infrastructure hierarchy.



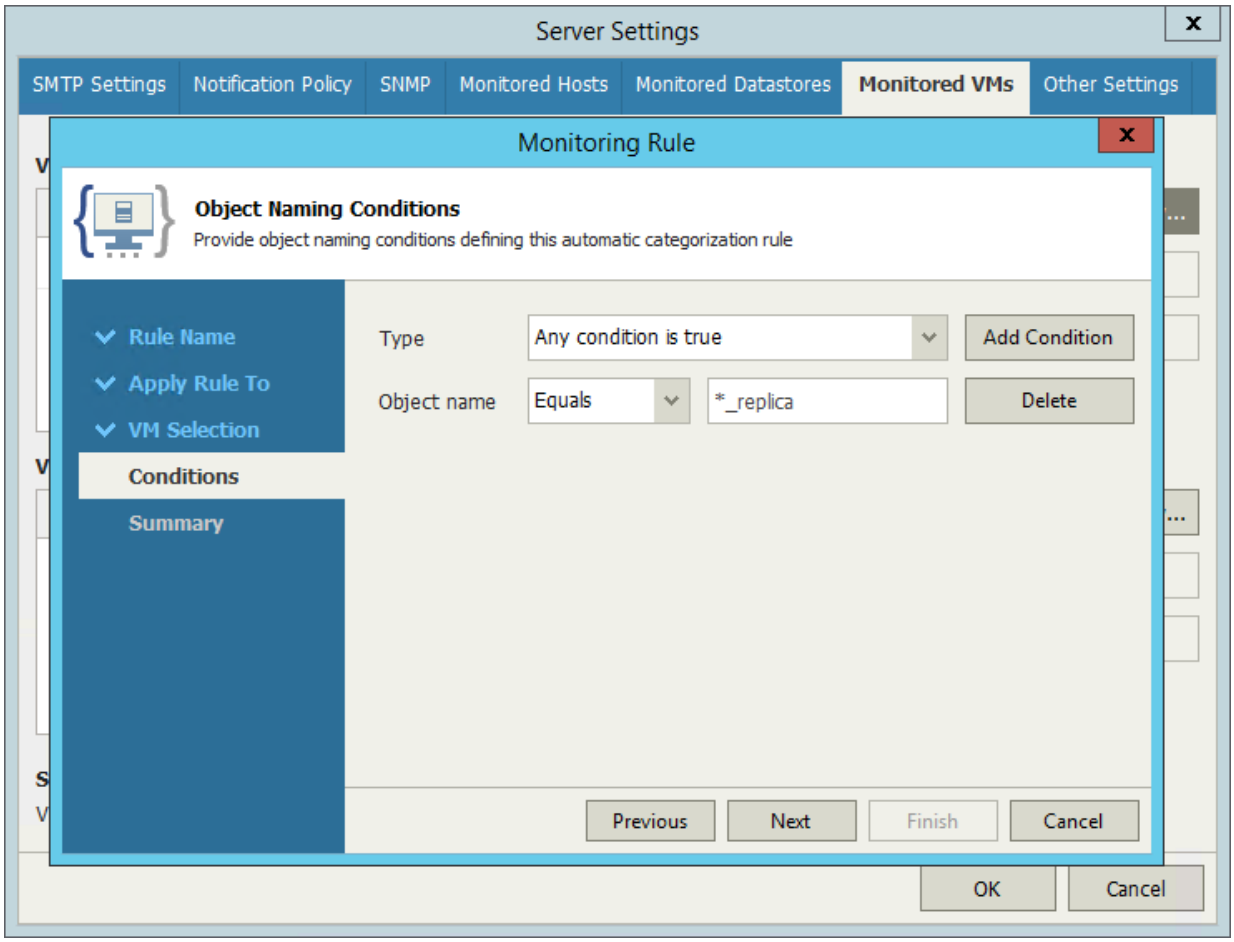
Step 6. Specify Rule Conditions

The **Conditions** step of the wizard appears only if you have selected the **By object name** option at the **VM Selection** step. At this step, configure conditions for adding VMs to the rule by name:

1. Click **Add Condition**.
2. From the **Object name** list, select a condition for adding VMs — *Equals* or *Not Equals*.
3. In the field next to the selected condition, specify the name of VMs to add to the rule.

   You can use the '*' (asterisk) and '?' (question mark) wildcards. The '*' (asterisk) character stands for zero or more characters. The '?' (question mark) stands for a single character. For example, if you want to find VM replicas created with Veeam Backup & Replication, you can create a rule with the '*_replica' name query.
4. If you add two or more conditions, link them with Boolean operators. From the **Type** list, select a Boolean operator to link the conditions:
   - **Any condition is true** — if at least one of the specified conditions is met, a VM will be added to the rule.

- **All conditions are true** – if all specified conditions are met, a VM will be added to the rule.



Step 7. Review the Configuration

At the **Summary** step, review the rule configuration and click **Finish** to exit the wizard.

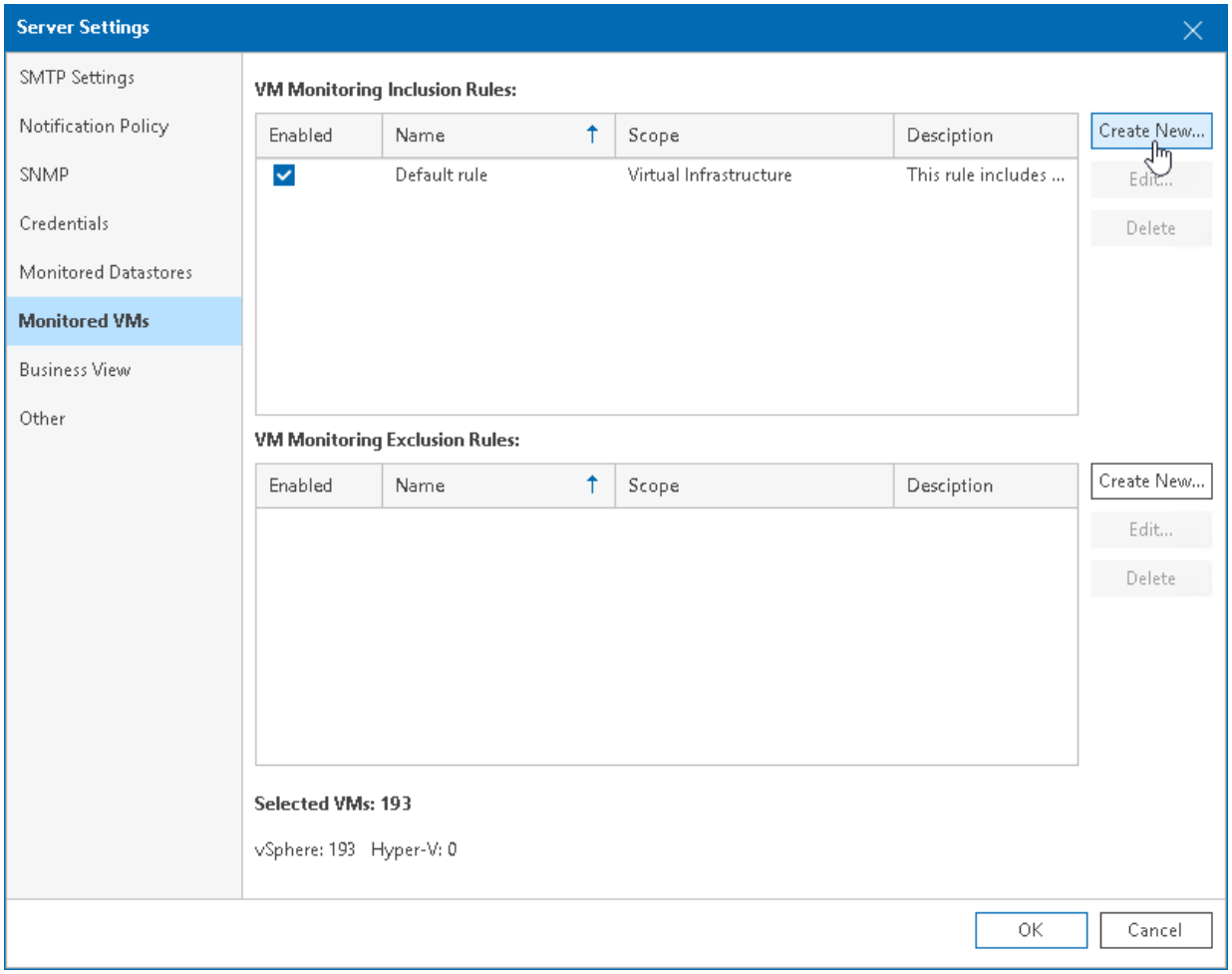
How to Create Inclusion Rule and Add VMs by Name

You can create a rule to include VMs in the data collection scope VMs whose names end with *'_srv'*:

1. Open Veeam ONE Client.
2. In the main menu, click **Settings** and select **Server Settings**.

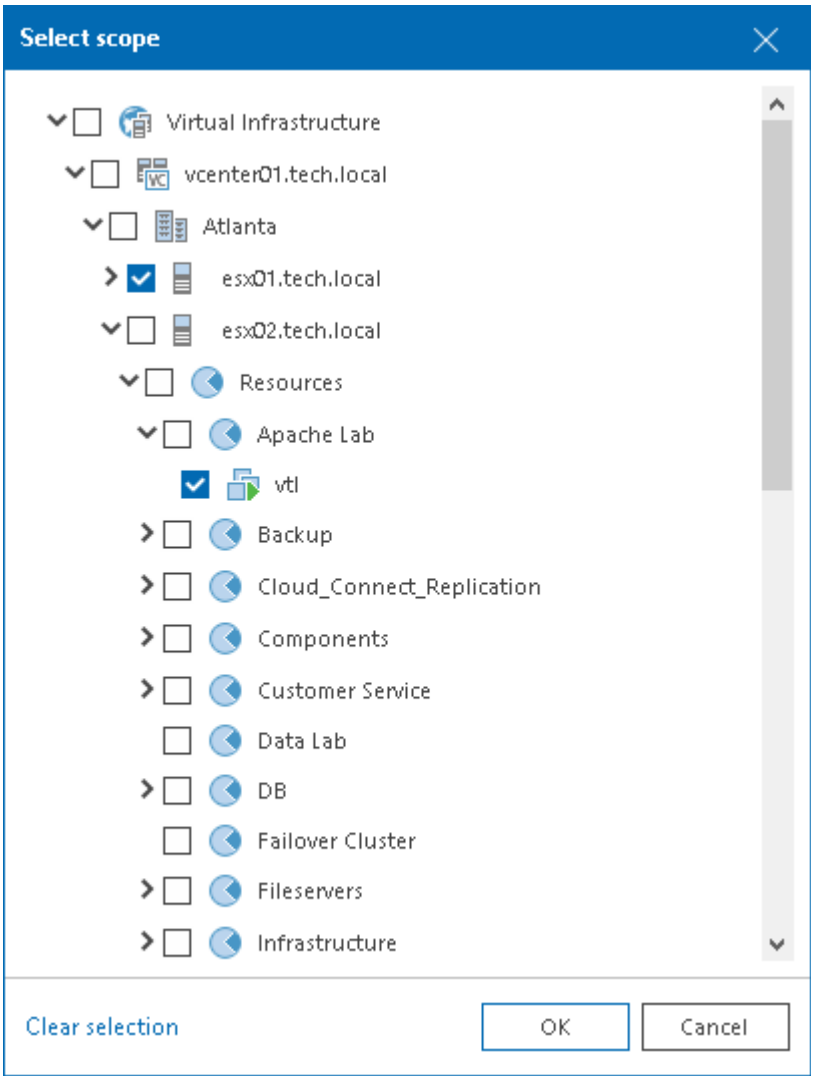
   Alternatively, press the `[CTRL+S]` on the keyboard.
3. In the **Server Settings** window, open the **Monitored VMs** tab.

4. On the **Monitored VMs** tab, in the **VM Monitoring Inclusion Rules** section, click **Create New**.



5. At the **Rule Name** step of the **Monitoring Rule** wizard, type the rule name. In the **Description** field, type the rule description.

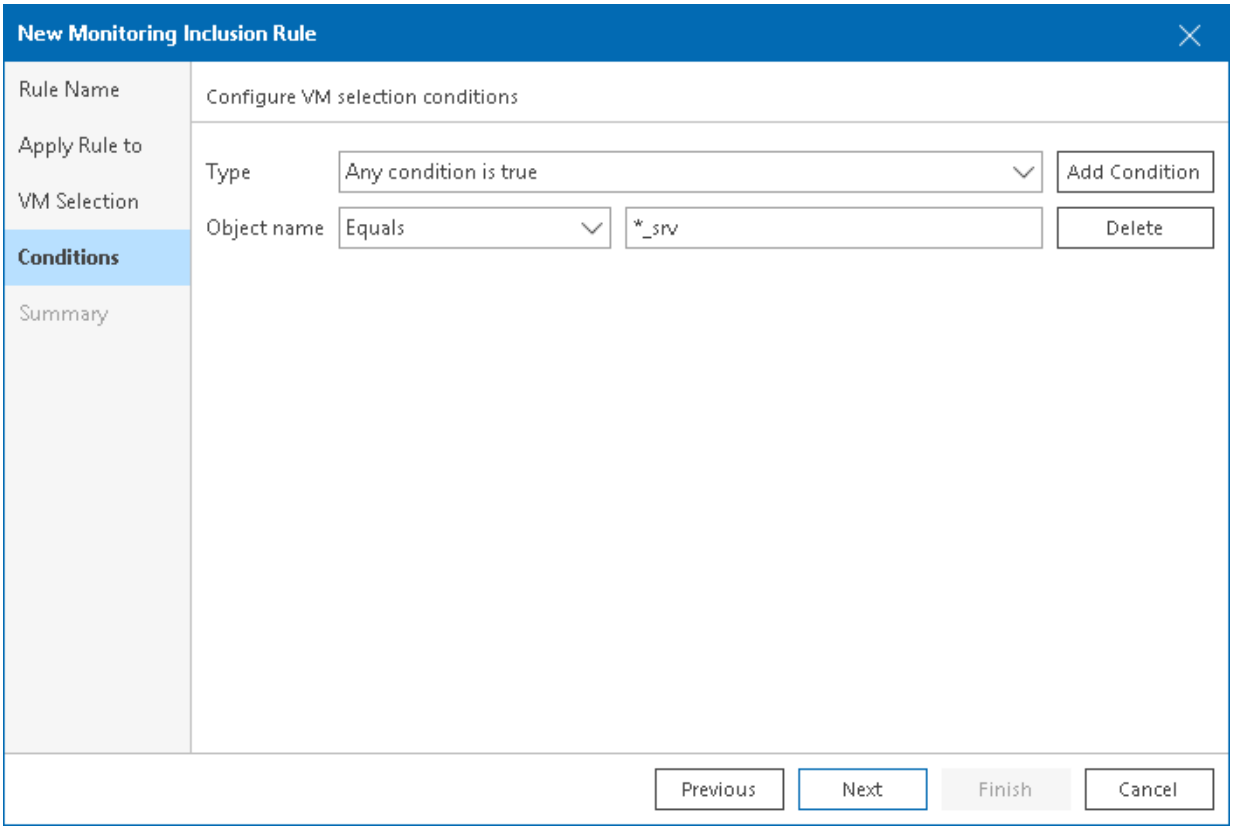
6. At the **Apply Rule To** step of the wizard, click **Add** and select *Infrastructure View*, *Business View* or *VMware Cloud Director View*. In the **Select scope** window, select check boxes next to containers to which the rule must apply.



7. At the **VM Selection** step of the wizard, choose **By object name**.
8. At the **Conditions** step of the wizard, perform the following steps:
   a. Click **Add Condition**.
   b. From the **Object name** list, select the *Equals* condition.

c. In the value field, type the *'*_srv'* query.

This will include in the data collection scope all VMs whose name ends with *'_srv'*.



9. At the **Summary** step of the wizard, review rule configuration and click **Finish**.

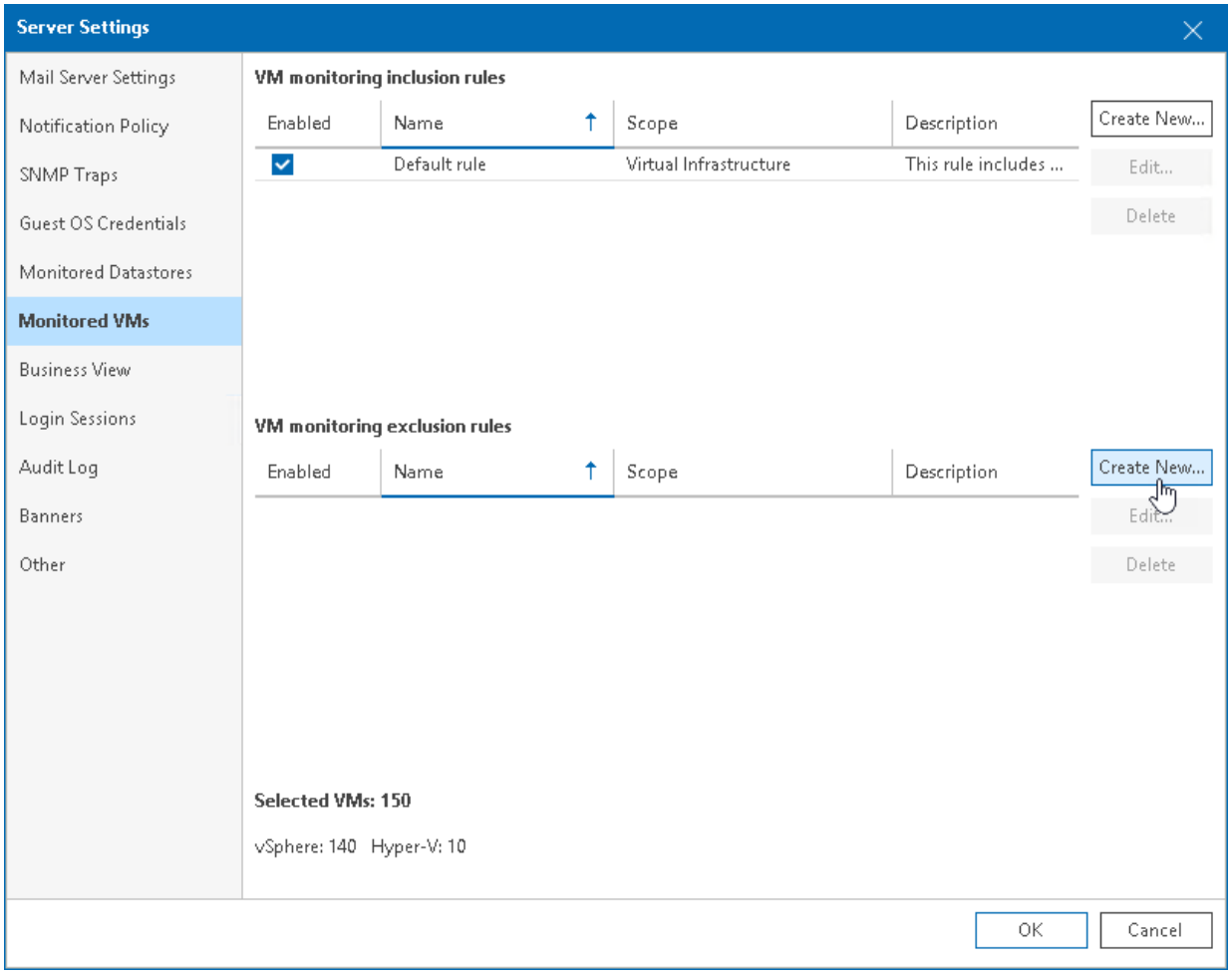
How to Create Exclusion Rule and Add VMs by Location

You can create a rule to exclude from the data collection scope VMs residing on a specific host:

1. Open Veeam ONE Client.
2. In the main menu, click **Settings** and select **Server Settings**.

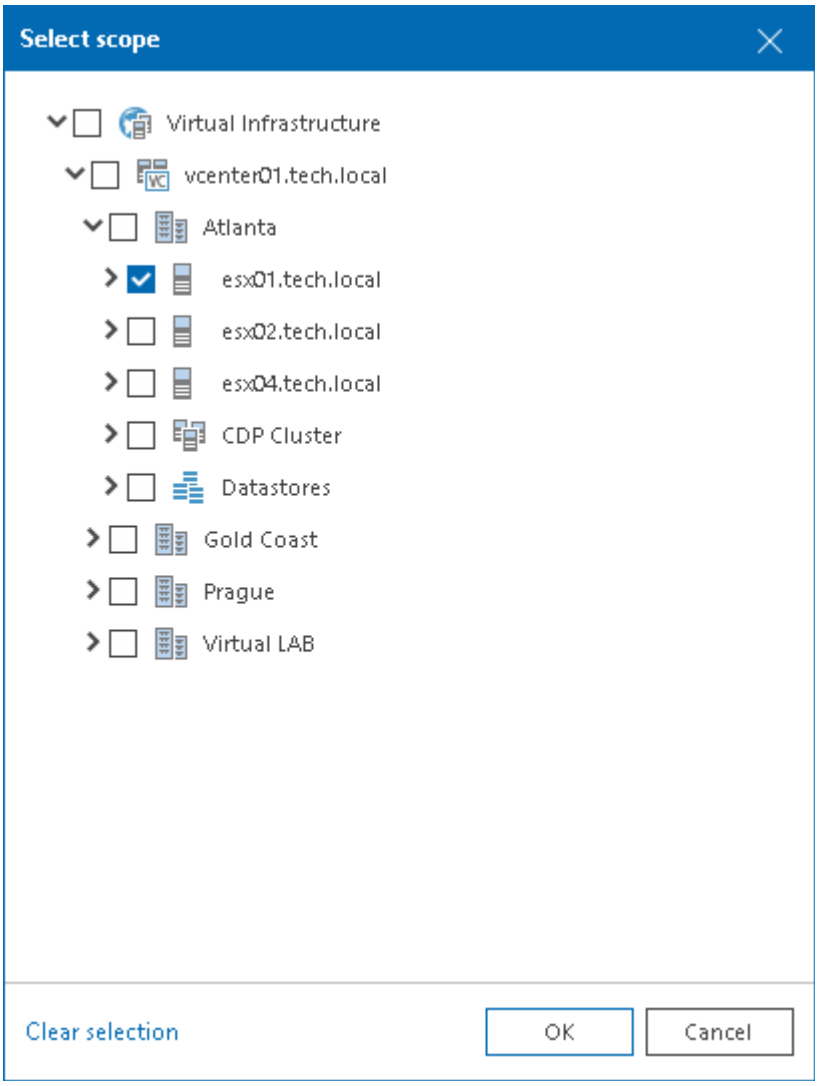
   Alternatively, press the `[CTRL+S]` on the keyboard.
3. In the **Server Settings** window, open the **Monitored VMs** tab.

4. On the **Monitored VMs** tab, in the **VM Monitoring Exclusion Rules** section, click **Create New**.

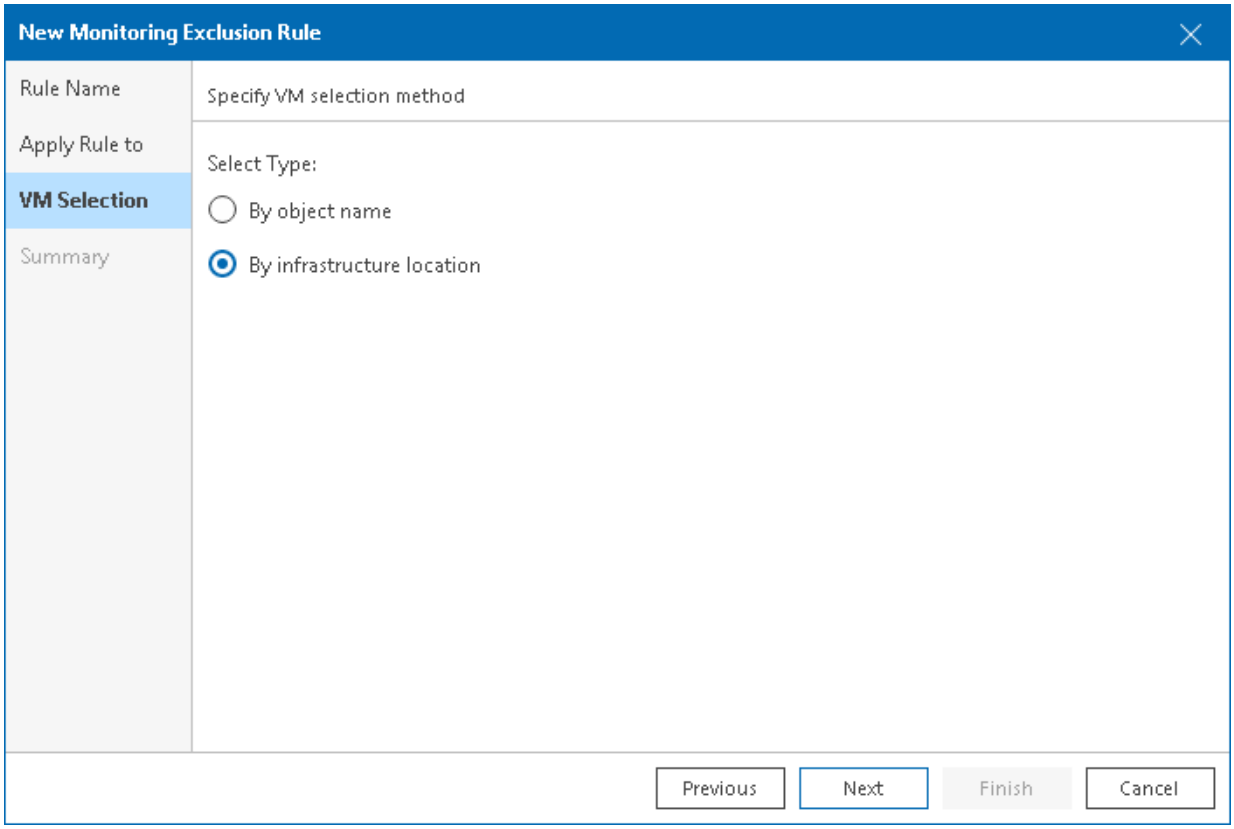


5. At the **Rule Name** step of the **Monitoring Rule** wizard, type the rule name. In the **Description** field, type the rule description.

6. At the **Apply Rule to** step of the wizard, click **Add** and select **Infrastructure View**. In the **Select scope** window, select the check box next to the host that must be excluded from the data collection scope.



7. At the **VM Selection** step of the wizard, choose **By infrastructure location**.



8. At the **Summary** step of the wizard, review rule configuration and click **Finish**.

Choosing Datastores to Report On

After you connect a VMware vSphere server in Veeam ONE Client, all datastores attached to this server are added to the data collection scope. If you do not need to collect data about specific datastores (for example, local datastores or datastores with ISO images), you can exclude these datastores from the collection scope.

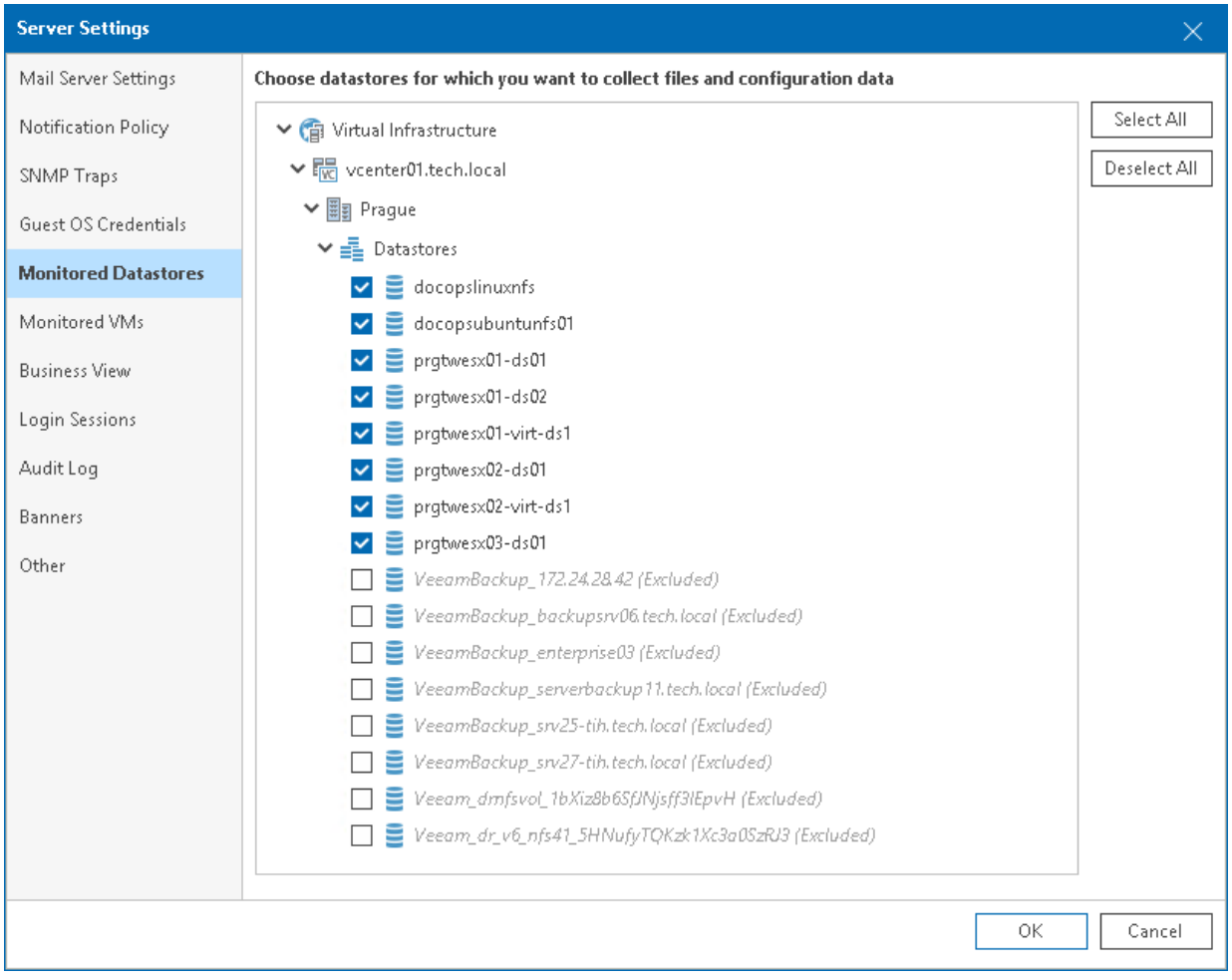
Excluding datastores will accelerate completion of a data collection sessions. Excluded datastores will not be reflected in reports that analyze and list the files residing on datastores (such as the *Garbage Files* and *Idle Templates* reports).

> **IMPORTANT!**
>
> Excluding datastores available for the VMware vSphere platform only.

To exclude one or more datastores from the data collection scope:

1. Open Veeam ONE Client.
2. In the main menu, click **Settings** and select **Server Settings**.

   Alternatively, press the `[CTRL+S]` on the keyboard.
3. In the **Server Settings** window, open the **Monitored Datastores** tab.
4. Expand the virtual infrastructure hierarchy and clear check boxes next to datastores that must be excluded from the data collection scope.
5. Click **OK** to apply changes.



Data Collection Schedule

After you connect VMware vSphere, Microsoft Hyper-V, Veeam Backup & Replication and Veeam Backup for Microsoft 365 servers, Veeam ONE will propagate the provided connection settings to all its components and will set up the following default data collection configuration:

- In Veeam ONE Client, the connected servers will be added to the list of monitored objects. Data from the servers will be collected in the real-time mode.
- In Veeam ONE Web Client, the connected servers will be added to the list of objects targeted for data collection. Data collection will be scheduled to run on weekdays, at 3:00 a.m. The first data collection session will start immediately after installation. You can customize the schedule according to which reporting data is collected in the Veeam ONE Web Client console. For details on changing data collection schedule, see Scheduling Data Collection.

Security Groups

Veeam ONE creates the following security groups on the machines where Veeam ONE Server and Veeam ONE Web Services components are installed:

- **Veeam ONE Administrators**: members of this group can access monitoring data, generate reports and modify all Veeam ONE configuration settings.

  This group must include the Veeam ONE service account.

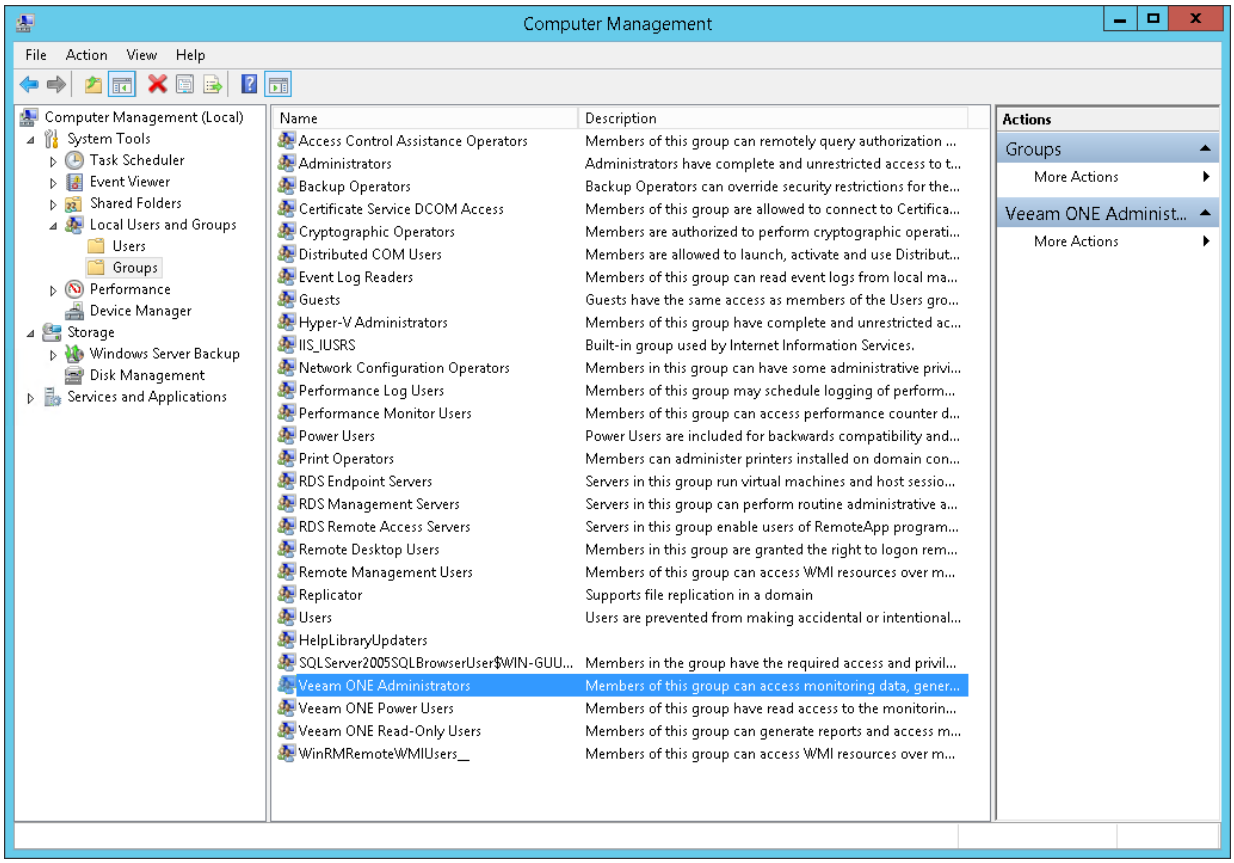
  > **NOTE:**
  >
  > If the Windows security policy *Deny access to this computer from the network* is set to deny network logon for local accounts and members of the Administrators group, local administrator accounts may be assigned the *Limited Scope* user role in Veeam ONE Web Client.
  >
  > In this situation, Veeam ONE Web Client cannot validate local administrator group membership because it relies on a Windows network logon (Logon Type 3).
  >
  > To ensure proper validation and access, we recommend using only domain accounts or groups for Veeam ONE administration.

- **Veeam ONE Power Users:** members of this group have full access to all Veeam ONE Web Client tabs except configuration settings and read access in Veeam ONE Client.

  > **NOTE:**
  >
  > Members of the *Power Users* security group can run report and dashboard scheduling scripts on the machine on which the Veeam ONE Web Services component is installed. Include users into this group with caution.

- **Veeam ONE Read-Only Users**: members of this group can generate reports and access monitoring data in read-only mode, but cannot modify any Veeam ONE configuration settings.

You can access and manage security groups in the Computer Management console.



To provide access to Veeam ONE functionality for an administrator or operator, you must include this user either in the *Veeam ONE Administrators*, *Veeam ONE Read-Only Users* or *Veeam ONE Power Users* group. Member of these groups have access to:

- All Veeam ONE consoles (Veeam ONE Client and Veeam ONE Web Client)
- All objects of the infrastructure inventory

> **NOTE:**
>
> To apply the changes after a user has been included to a Security Group, this user must log out and log back on to the machines where Veeam ONE Server and Veeam ONE Web Services components are installed.

Multi-Tenant Monitoring and Reporting

Veeam ONE supports multi-user access to its monitoring and reporting capabilities. Authorized users can concurrently access the same instance of Veeam ONE to monitor the health state of the virtual infrastructure and create reports.

To restrict access to sensitive infrastructure data, you can limit the scope of virtual infrastructure objects and associated data that must be available to a Veeam ONE user. Thus you can control what subset of the managed virtual infrastructure the user can see and work with. In multi-tenant environments, you can configure restricted access to Veeam ONE for owners of virtualized systems or responsible personnel and delegate monitoring and reporting tasks.

NOTE:

Do not use security groups to enable for users possibilities of self-service monitoring and reporting on a restricted scope of the virtual infrastructure. Instead, configure permissions for multi-tenant access. For details, see Multi-Tenant Monitoring and Reporting.

Data Retention

Data collected from virtual and backup servers is organized to the Veeam ONE database. Veeam ONE retains data in the database as follows:

- For categorization data, Veeam ONE retains one sample in the database. This data is updated with every new data collection.
- For topology, configuration, audit and performance data, Veeam ONE keeps multiple samples based on the retention policy. Performance data is aggregated in the database according to the scheme described below.
- For events collected from backup and virtual servers, Veeam ONE keeps all collected instances.

Performance Data Aggregation

As the performance data ages, Veeam ONE aggregates it for long-term storage. Data aggregation helps save disk space on the database server and speed up generation of performance reports and charts.

Veeam ONE uses the following aggregation scheme for performance data:

Period	Optimized for Veeam backup data and virtual infrastructure performance monitoring	Optimized for Veeam backup data and large-scale virtual infrastructure performance monitoring	Veeam Backup Data Only
Hour	20 seconds for VMware vSphere 30 seconds for Microsoft Hyper-V	15 minutes	20 seconds
Week	5 minutes	30 minutes	5 minutes
Year	2 hours	2 hours	2 hours

Sampling intervals at which data is stored to the database depend on Veeam ONE data collection mode. For example, for the Veeam backup data only mode, raw data (data with 20-second resolution) is stored for 1 hour. After 1 hour, raw data is aggregated to 5-minute resolution data. After 1 week, data with 5-minute resolution is aggregated to 2-hour resolution data. Data with this level of detail is stored in the database for up to 1 year.

To draw performance charts, Veeam ONE uses data with various aggregation levels, depending on the period for which performance data is shown. For example, for Veeam backup data only mode, performance charts for the past hour use samples with 20-second resolution, charts for the past day use data with 5-minute resolution and so on.

To generate performance reports, Veeam ONE uses data with 2-hour resolution.

If you use Veeam ONE for monitoring and reporting in large environments, the Veeam ONE database can grow quickly. To support large virtual and backup infrastructures and reduce the size of the Veeam ONE database, you can increase aggregation intervals for performance data. To learn how to change aggregation intervals, contact Veeam Support at https://www.veeam.com/support.html.

Changing Veeam ONE Service Account

You can change Veeam ONE service account or the service account password that you provided during the product installation. For example, changing Veeam ONE service account properties can be required if you use a domain account as the Veeam ONE service account. When you update the domain account password, you must manually update the service account password for Veeam ONE.

To change the Veeam ONE service account or service account password:

1. Log on as Administrator to the machine where the Veeam ONE Server component is installed.
2. Change accounts of *Veeam ONE Caching Service, Veeam ONE Monitoring Service*, *Veeam ONE Error Reporting Service, Veeam ONE Reporting Service* and *Veeam Analytics service*:
   a. Click **Start**, go to **Programs > Administrative Tools**, and then click **Services**.
   b. Right-click *Veeam ONE Monitoring Service* and choose **Stop**.
   c. Right-click *Veeam ONE Monitoring Service*, choose **Properties** and open the **Log on** tab.
   d. In the **This account** filed, specify the user name of the service account.
   e. In the **Password** and **Confirm password** fields, type a password of the service account.
   f. Click **OK**.
   g. Repeat steps a-f for *Veeam ONE Reporting Service*, *Veeam Analytics service, Veeam ONE caching Service* and *Veeam ONE Error Reporting Service*.
3. Start *Veeam ONE Caching Service, Veeam ONE Monitoring Service*, *Veeam ONE Error Reporting Service, Veeam ONE Reporting Service* and *Veeam Analytics service*:
   a. Click **Start**, go to **Programs > Administrative Tools**, and then click **Services**.
   b. Right-click the necessary service and choose **Start**.

IMPORTANT!

If you want to use *Local System* as the service account, consider the following:

- SQL Server Authentication is required for the account used to connect to the Microsoft SQL Server hosting the Veeam ONE database.
  For details on modifying database connection settings, see Database.
- You cannot install the license using the POST `/license/install` method of the Veeam ONE REST API.

Other Ways to Change Service Account

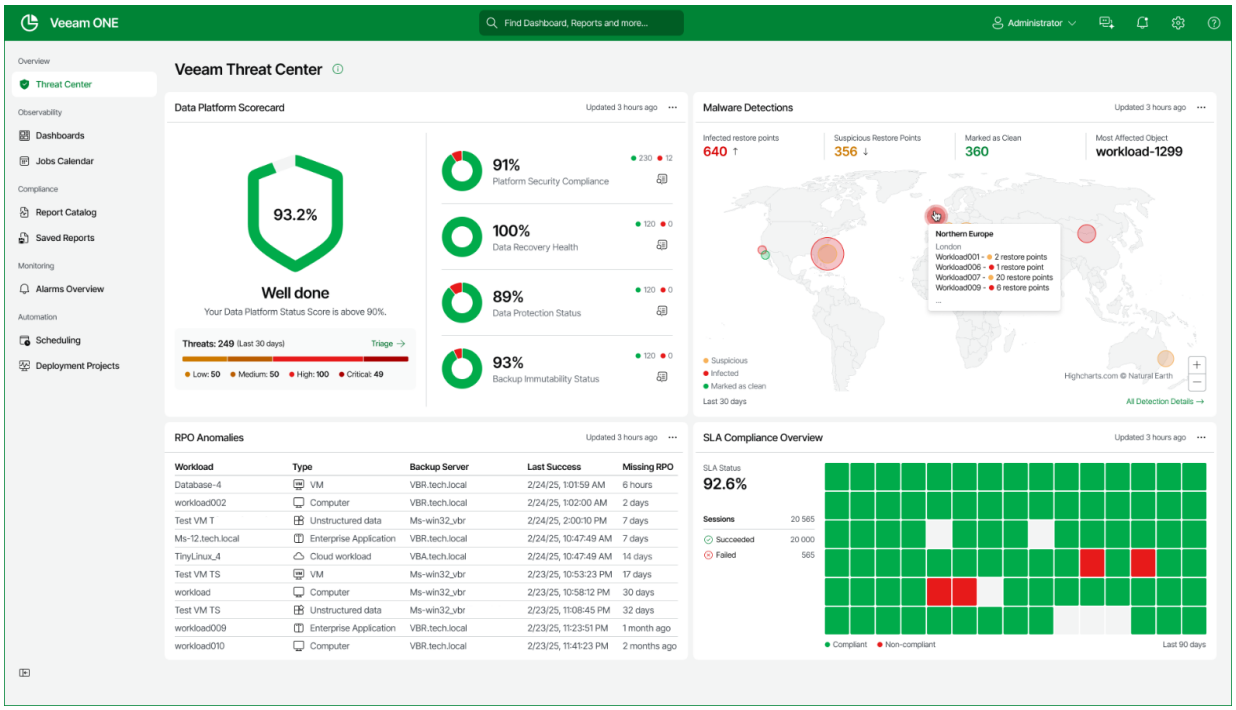
To change Veeam ONE service account, you can also perform the following steps:

1. Uninstall Veeam ONE.
2. Re-install Veeam ONE and specify a new service account during installation.
   Note that when you re-install Veeam ONE, you must point it to the existing Veeam ONE database.

Veeam Threat Center

The **Veeam Threat Center** dashboard displays Veeam Backup & Replication infrastructure security state and helps you assess the overall security and compliance of your infrastructure objects.

Veeam Threat Center provides all the required data protection visibility at a glance, allowing you to quickly and easily access all the threats, best practices and SLA data you need to operate securely and safely.



Widgets Included

Data Platform Scorecard

This widget summarizes and displays data platform scores for Platform Security Compliance, Data Recovery Health, Data Protection Status and Backup Immutability Status. This display provides all the required data protection visibility at a glance, allowing you to quickly and easily identify the information you need to action solutions to threats to your backup infrastructure.

You can configure the information displayed in the scorecard in the settings panel. You can edit the scorecard widget to display information on infrastructure objects as well as *Data Recovery Health*, *Data Protection Status*, *Backup Immutability Status* and *Platform Security Compliance* mini-widgets.

You can also configure and generate reports directly from the *Platform Security Compliance*, *Data Protection Status* and *Backup Immutability Status* and *Data Recovery Health* mini-widgets. Click the relevant report icon to the right of each section. For details on predefined Veeam ONE reports, see Predefined Veeam ONE Reports.

If you have configured integration with Coveware, the *Data Platform Scorecard* widget contains a *Threats* mini-widget that displays the number of potentially detected malware incidents depending on detected severity (*low, medium, high, critical*). To review incidents in the Coveware portal, click **Triage**. For details on Coveware integration, see Security.

NOTE:

- To analyze data about protected VMs in the Data Protection Status mini-widget, you must connect the target virtualization servers to Veeam ONE. For details on, see Add Data Source.
- This widget inherits exclusions along with virtualization servers. Virtual Machines are hidden if they are excluded from the Monitoring Rules set in Veeam ONE Client.

To configure the **Data Platform Scorecard** widget:

1. Open Veeam ONE Web Client.
2. Navigate to the **Veeam Threat Center** section.
3. At the top right corner of the **Data Platform Scorecard** widget, click the settings icon.
4. In the **Platform Security Compliance** step:
   - Infrastructure objects — Select the infrastructure objects you want to include in the mini-widget scope.
   - Include suppressed — Click the **Include suppressed** check box to include suppressed best practices objects in the mini-widget scope.
5. In the **Data Recovery Health** step:
   - Infrastructure objects — Select the infrastructure objects you want to include in the mini-widget scope.
6. In the **Data Protection Status** step:
   - Infrastructure objects — Select the infrastructure objects you want to include in the mini-widget scope.
   - Protected workload types — Select the protected workload types that you want to include in the mini-widget scope: *Virtual machines*, *Computers*, *Unstructured data*, *Cloud instances* and *Enterprise applications*.
   - RPO — Define the Recovery Point Objective period.
   - Workload exclusion rule — Specify a list of workloads that should be excluded from the widget scope. You can enter workload names explicitly or create a wildcard mask by using the asterisk (*) to replace any number of characters or question mark (?) to replace a single character. Multiple entries are separated by semicolon. Usage example: the following string will exclude workloads with the _R&D suffix from appearing in the widget: *_R&D.
7. In the **Backup Immutability Status** step:
   - **Scope** — Click the corresponding option button to switch between Business View and Infrastructure objects.
   - **Protected workload types** — Select the protected workload types that you want to include in the mini-widget scope: *Virtual machines*, *Computers*, *Unstructured data*, *Cloud instances* and *Enterprise applications*.
   - **Job types** — Select the job types to display on mini-widget.
   - **Threshold analysis** — To set immutability thresholds, click the **Use these immutability thresholds for analysis** check box and define the immutability period and the number of immutable restore points.
8. Click **Finish** to save the changes.

Malware Detections

This widget shows malware detections by geographic location based on infection severity and infection suspicion. It also displays clean restore points and most affected objects. You can configure the time range to display malware detection over your desired defined time period.

The Malware Detections widget displays only detections in the defined time period and does not display any backup that has received no detection.

To configure a **Malware Detections** widget:

1. Open Veeam ONE Web Client.
2. Open the **Veeam Threat Center** section.
3. At the top right corner of the **Malware Detections** widget, click the settings icon.
4. In the **Settings** step:
   - Infrastructure objects — Select the objects you want to include in the widget scope.
   - Period — Define the time period in which detected malware is displayed.
   - Show most affected — Define the most affected types of objects to display including backup repositories, backup servers or locations.
5. Click **Assign Location** in the **Location** tab to add location to each your backup repositories.
6. Select the required backup repository check boxes and click **Assign location** to assign a location to several objects. You can also assign a location to individual backup repositories. To do this click on the entry in the location column. If currently unassigned this displays as **Unselected**.

   Additionally to create your own custom locations click **Add custom location** to define city, sub-region, region and geographic co-ordinates to display on the malware map.
7. Click **Finish** to save the changes.

Recovery Point Objective (RPO) Anomalies

This widget shows all objects in your infrastructure that have missed their defined RPO period. You can configure the widget settings to display your desired backup infrastructure objects, protected workload types, time period to display RPOs and Top N workloads.

> **NOTE:**
>
> - To analyze data about protected VMs in the RPO Anomalies widget, you must connect the target virtualization servers to Veeam ONE. For details on, see Add Data Source.
> - This widget inherits exclusions along with virtualization servers. Virtual machines are also hidden if they are excluded by Monitoring Rules in Veeam ONE Client and have no restore points.

To configure the **RPO Anomalies** widget:

1. Open Veeam ONE Web Client.
2. Open the **Veeam Threat Center** section.
3. At the top right corner of the **RPO Anomalies** widget, click the settings icon.

4. In the **Edit Widget** wizard, change the widget settings:
    - Infrastructure objects — Select the infrastructure objects you want to include in the widget scope.
    - Protected workload types — Select the protected workload types to monitor including *Virtual machines*, *Computers*, *Unstructured data*, *Cloud instances* and *Enterprise applications*.
    - RPO — Define the Recovery Point Objective period.
    - Top N workloads — Define the number of workloads to display on the widget.
    - Workload exclusion rule — Specify a list of workloads that should be excluded from the widget scope. You can enter workload names explicitly or create a wildcard mask by using the asterisk (*) to replace any number of characters or question mark (?) to replace a single character. Multiple entries are separated by semicolon. Usage example: the following string will exclude workloads with the _R&D suffix from appearing in the widget: *_R&D.
5. Click **Finish** to save the changes.

SLA Compliance Overview

This widget displays a heatmap for your SLA success compliance allowing you to deep dive into success percentages over a defined time period. You can configure the widget settings to display infrastructure objects, job types, SLA period and SLA percentage threshold.

To configure the **SLA Compliance Overview** widget:

1. Open Veeam ONE Web Client.
2. Open the **Veeam Threat Center** section.
3. At the top right corner of the **SLA Compliance Overview** widget, click the settings icon.
4. In the **Edit Widget** wizard, change the widget settings:
    - Infrastructure objects — Select the infrastructure objects you want to include in the widget scope.
    - Job types — Select the job types to display on your widget.
    - Period — Define the time period in which SLA data is displayed.
    - Target SLA — Define the service level agreement threshold in percentage.
5. Click **Finish** to save the changes.

Veeam Intelligence

Veeam Intelligence is an advanced Artificial Intelligence solution designed to assist customers with Veeam products. It searches for up-to-date information in the technical documentation and analyzes product data to provide recommendations using natural language. You can interact with Veeam Intelligence in any language, whether for simple queries or complex inquiries.

By default Veeam Intelligence is enabled in the Basic mode. In this mode, Veeam Intelligence assists users with technical questions about Veeam ONE based on official documentation. You can switch Veeam Intelligence to the Advanced mode which provides deeper insights into your infrastracture using Veeam ONE REST API.

For details on disabling or changing Veeam Intelligence, see Veeam Intelligence Settings.

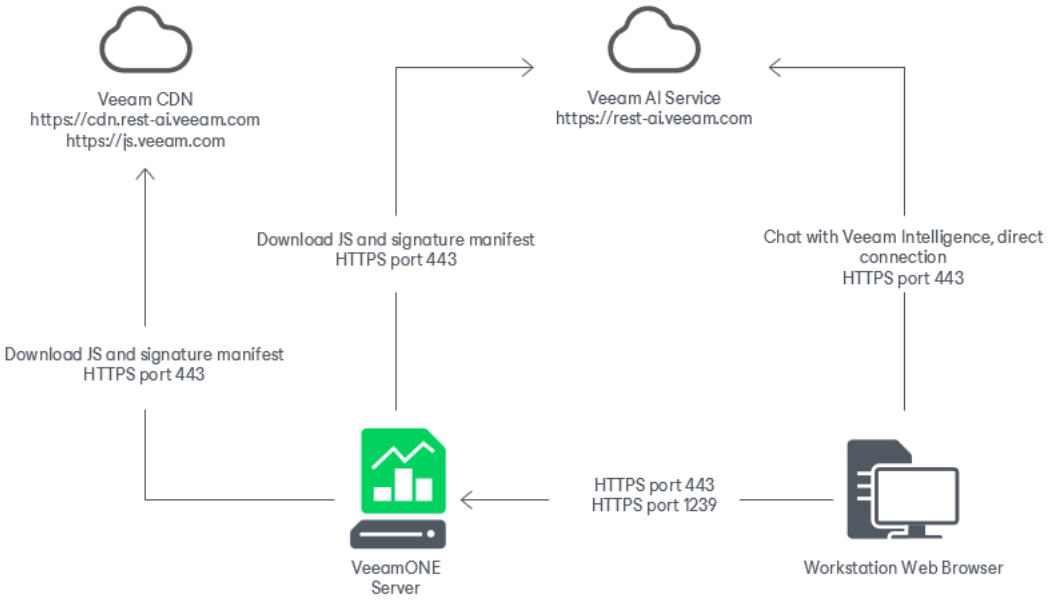
> **IMPORTANT!**
>
> Consider the following:
>
> - Only a currently installed license is used for authentication. If the license is changed, you must close Veeam Intelligence window and open it again.
> - Veeam Intelligence sends your queries outside of your organization. Be aware of this when writing queries related to private or confidential information.
> - Veeam takes no responsibility for the accuracy of the information that Veeam Intelligence provides.
> - Veeam Intelligence accepts only text input.
> - The Veeam Intelligence bot considers the context of all previous messages and may affect its consequent responses. If you need to clear the context of your conversation, refresh the page.
> - Veeam Intelligence is under constant development. Make sure to monitor additional improvements and features in future Veeam ONE releases and release notes.

Limitations of Veeam Intelligence

Veeam Intelligence has the following limitations:

- The machine on which Veeam ONE Web Services runs must have internet access.
- Veeam Intelligence is only available to Veeam ONE Administrators. For all other user types, the Veeam Intelligence button is not available.
- Community and Perpetual (with expired support) licenses are not supported.
- Network access with the following conditions is required for the machine on which your workstation web browser and Veeam ONE Server runs:
  - An open connection to *rest-ai.veeam.com*, *cdn.rest-ai.veeam.com* and *js.veeam.com*
  - Port: 443
  - Protocols used to communicate Veeam Intelligence queries: HTTPS and WSS (transport level: TCP)

Network communication between your workstation web browser, Veeam ONE Server and the Veeam AI Service is displayed in the following schema:



Veeam Intelligence Advanced Mode

Advanced mode allows additional searches of Veeam ONE API GET queries to provide additional answers specific to your environment. In Advanced mode, Veeam Intelligence has access to the following information to generate the answers you receive for your infrastructure:

- Veeam ONE Server and installation information
- Predefined and triggered alarms, including alarms for child objects
- Protected VMs, computers, storage and applications protected with Veeam Backup & Replication
- Cloud VMs, file share, database and network policies
- Cloud VMs, cloud file shares and cloud databases
- Veeam Backup & Replication servers and best practices
- All monitored Veeam Backup & Replication jobs

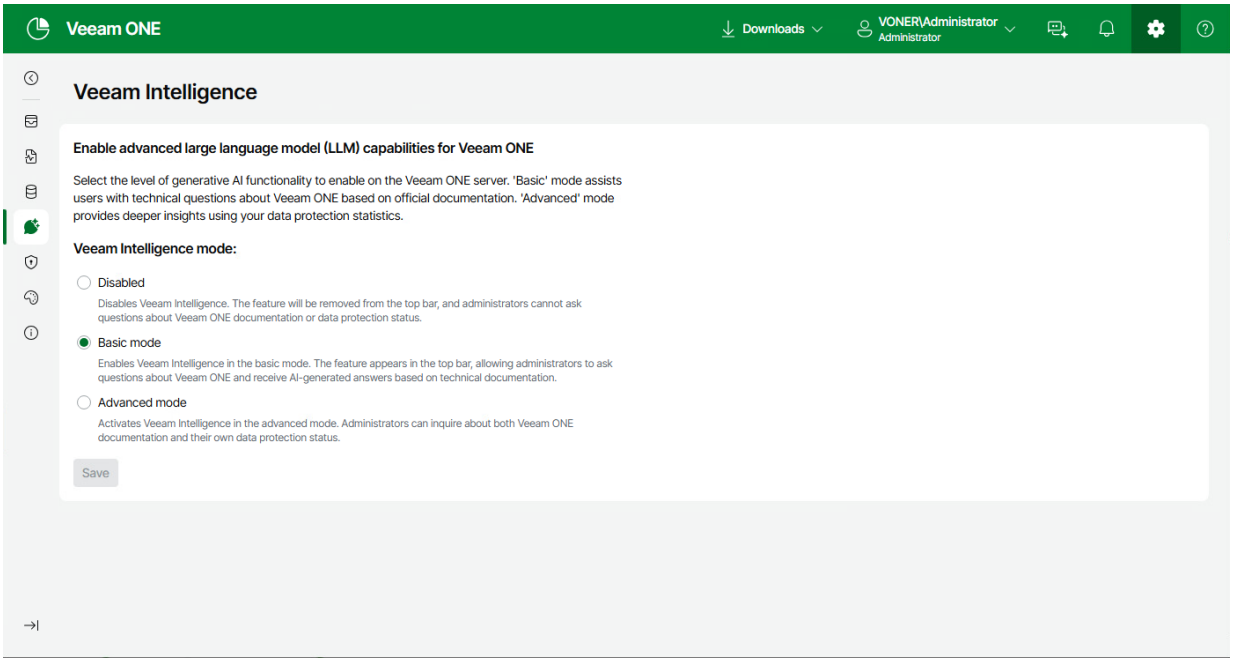
Using Veeam Intelligence

To start a new conversation:

1. Click **Veeam Intelligence** button located in the upper right corner of the Veeam ONE window.
2. In the chat window, type the question. Alternatively, click prompt to provide a short list of suggested questions. Consider the following examples:
    - How to create an alarm notification?
    - Where are Veeam ONE logs stored?

- How to change license?
- How can I use Veeam ONE to make sure my VMs are regularly checked?

3. Click **Send** or press **Enter** to send your question.
4. When you do not need Veeam Intelligence click the **Close** button to close the Veeam Intelligence window. The context and entire history is still saved when closed. If you refresh the page your conversation history is cleared.



Responses from Veeam Intelligence are generated in real-time, token-by-token, allowing users to begin reading as the AI continues writing the answer. Relevant links to Veeam documentation and Knowledge Base articles are integrated within the text. Note that screenshots and images are not supported in the current version.

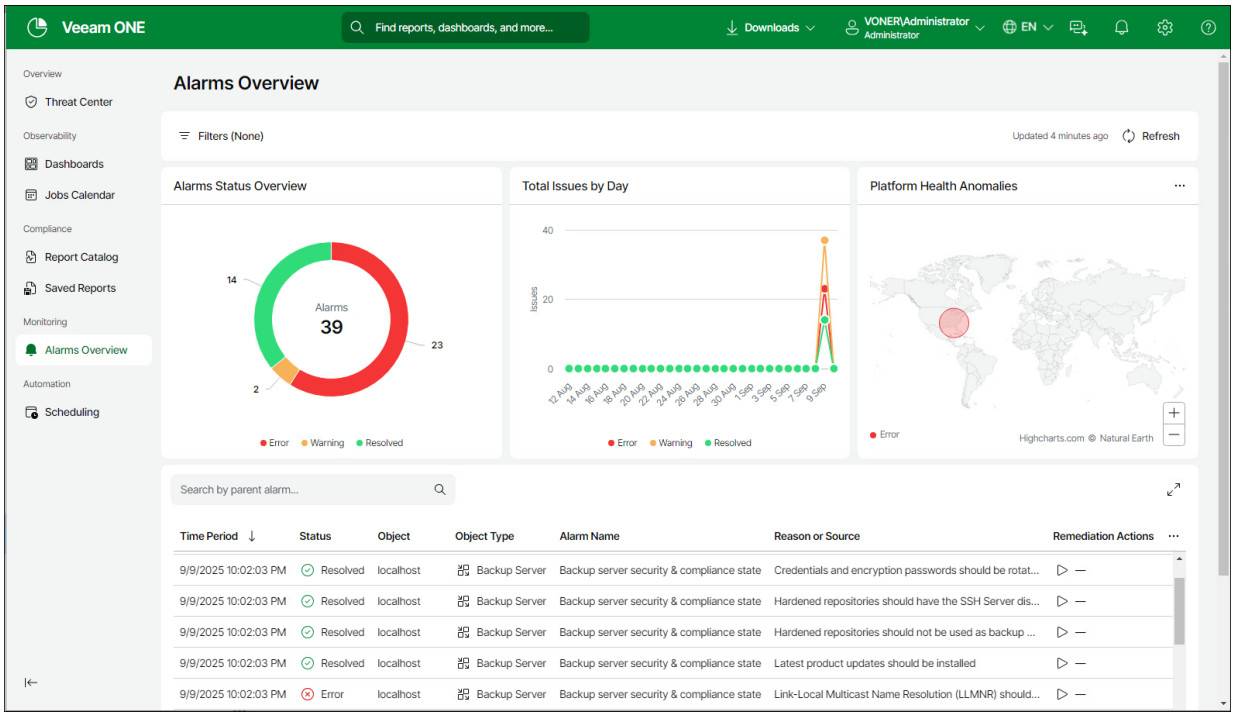
If you find the answer to be insufficient, you can add more details. The bot retains the conversation context and previous questions within a current session, so you do not have to repeat anything. If you close the session, Veeam Intelligence restarts and loses the context of your previous conversation.

Alarms Overview

The Alarms Overview dashboard provides a centralized overview of all active and historical Veeam Backup & Replication alarms within the system, allowing users to quickly assess the current health and status of monitored resources. It displays key metrics such as the number of *error*, *warning*, *resolved*, *information* and *acknowledged* alarms, along with their timestamps, affected components, and severity levels.

To improve your alarm data displayed you can also use the filter panel to refine the information displayed by filtering alarms by status, object type and remediation action as well as specifying the time period to display all associated data. Applied filters are immediately reflected in the displayed data.

You can access the **Alarms Overview** dashboard from the main navigation bar in Veeam ONE Web Client.



Widgets Included

Alarms Status Overview

This widget shows all currently triggered alarms within the system, providing real-time visibility into ongoing issues that require attention. The chart is broken down into details of all current alarms that have the status of *Error*, *Warning*, *Resolved*, *Information* and *Acknowledged.*

Total Issues by Day

This widget shows a daily summary of all issues detected within the system over a selected time period. This view helps users track trends and patterns in system health by displaying the number of new issues identified each day.

Platform Health Anomalies

This widget shows alarms detected by geographic location based on alarm severity. This view helps users track alarm trends in system health by displaying the number of issues identified in each configured geographic location.

Alarms list

This table provides a detailed, filterable list of all alarms. It displays essential information for each alarm in the following columns: *Time Period*, *Status*, *Object*, *Object Type*, *Alarm Name*, and *Reason or Source*. You can also click on any alarm entry to provide additional details and acknowledge, resolve and approve alarms. For details, see Resolving Individual Alarms, Acknowledging Individual Alarms and Approving Actions for Individual Alarms.

Jobs Calendar

Jobs Calendar visually represents jobs scheduled for a specified time period. It shows both upcoming and finished job sessions arranged in the calendar format. With the help of Jobs Calendar, you can analyze job history and plan job schedule avoiding previously occurred issues and without the risk of overloading the server.

Limitations

Jobs Calendar does not provide information on the following types of jobs:

- Veeam Backup for AWS jobs
- Veeam Backup for Google Cloud jobs
- Veeam Backup for Microsoft Azure jobs
- CDP policies
- Transaction log backups
- Veeam Backup for Microsoft 365 jobs

Accessing Jobs Calendar

To view Jobs Calendar:

1. Open Veeam ONE Web Client.
2. Open the **Jobs Calendar** section on the left.
3. From the **Backup server** drop-down list, select a backup server or Veeam Backup & Replication high availability cluster.

   The protection calendar will display data on completed and jobs configured on the selected server.
4. To narrow down the list of jobs:
   - Click **Filters** and select protected workload types and job types that you want to display.
   - Click the **Job Status** icons to narrow the the jobs displayed based on status (*Success*, *Warning*, *Error*).
   - Create a custom list of jobs:
     i. Click **Jobs**.
     ii. Select **Manual selection**.
     iii. Select check boxes of the jobs that you want to display.
5. To specify time period:
   - Click **Day**, **Week** or **Month** button.
   - Click the date link and select the day, week or month that you want to be displayed.

     To select the current day, week or month, click the **Today** button.

Viewing Jobs Calendar

Jobs Calendar marks the monitored job types with the following colors:

- *Green* — backup job.
- *Blue* — replication job.
- *Aquamarine* — backup copy job.
- *Beige* — tape job.
- *Brown* — VM and file copy job.
- *Dark green* — SureBackup.

Jobs Calendar represents completed and scheduled job sessions differently:

- Completed job sessions are transparent.

  In the **Month** view, completed sessions are filled with color.

- Scheduled job sessions are filled with color.

  In the **Month** view, scheduled sessions are transparent.

- Continuous job sessions scheduled for backup window periods are fully colored and connected with dashes.

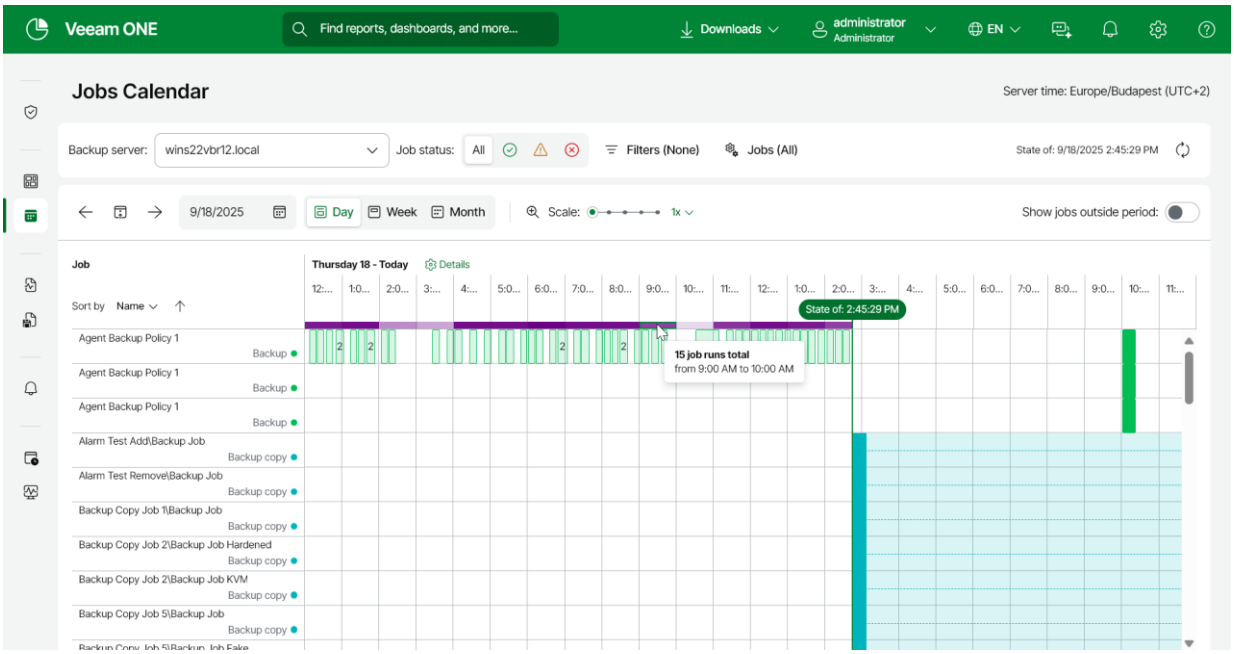
  If a continuous job schedule is split into smaller schedules, the job band will also be split.

To get brief information on a specific job, do one of the following:

- In the **Month** view, hover the cursor over the job name in the calendar.
- In the **Day** and **Week** view, hover the cursor over the job name in the **Job** column.
- In the **Day** and **Week** view, hover the cursor over the colored band of the job.

> **NOTE:**
>
> For backup copy jobs, the job list will include a separate line for each source job. The job name is presented in the *Backup copy job*|*Source job* format.
>
> For backup agent jobs, the job list will include a separate line for each backup agent. The job name is presented in the *Backup agent job - backup agent name* format.

The purple band above the calendar indicates how many jobs sessions ran simultaneously during the time period. The more parallel job sessions, the more saturated the band becomes. To see the exact number of job sessions for a specific period, hover the pointer over the purple band. Note that the purple band is available in the **Day** and **Week** view only.



By default, jobs are sorted by name. You can change that by selecting the **Job types** or **Earliest job session / Job schedule** option in the **Sort by** drop-down list. Note that sorting is available in the **Day** and **Week** view only.

Chained jobs are marked with a chain-like sign. To see information on a job after which a chained job starts, hover the cursor over the chained job color band.

The currently running job sessions are marked with a right-pointing triangle in a circle.

Disabled jobs are marked with horizontal line in a circle.

TIP:

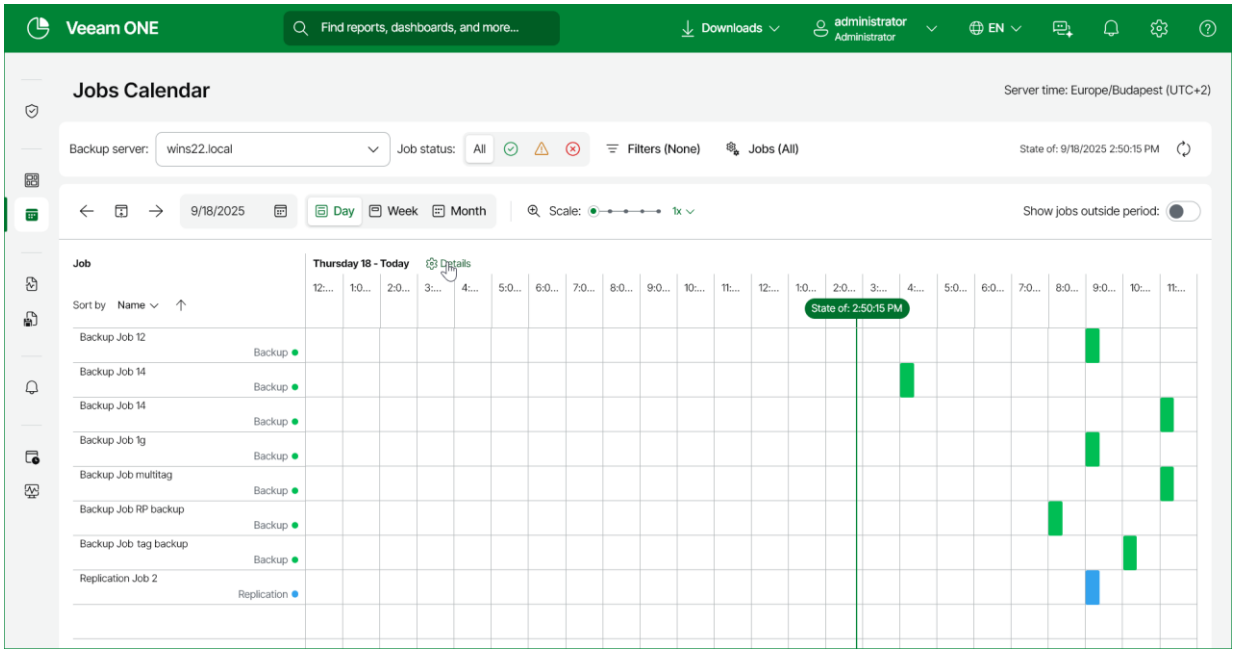
- You can include jobs that do not have any job sessions during the selected period into Jobs Calendar. To do that, switch the **Show jobs outside period** toggle to *On*.
  Note that the toggle is available in the **Day** and **Week** view only.
- If you want to zoom in the time period and all scheduled jobs, use **Scale**.
  Note that the **Scale** slider is available in the **Day** and **Week** view only.

Viewing Job Details

The protection calendar allows you to view detailed information on all jobs sessions for a specific day. To open day details, do one of the following:

- In the **Day** view, click **Details**.
- In the **Week** view, hover the cursor over the column associated with the necessary day and click **Details**.

- In the **Month** view, select the cell associated with the necessary day and click **Details**.



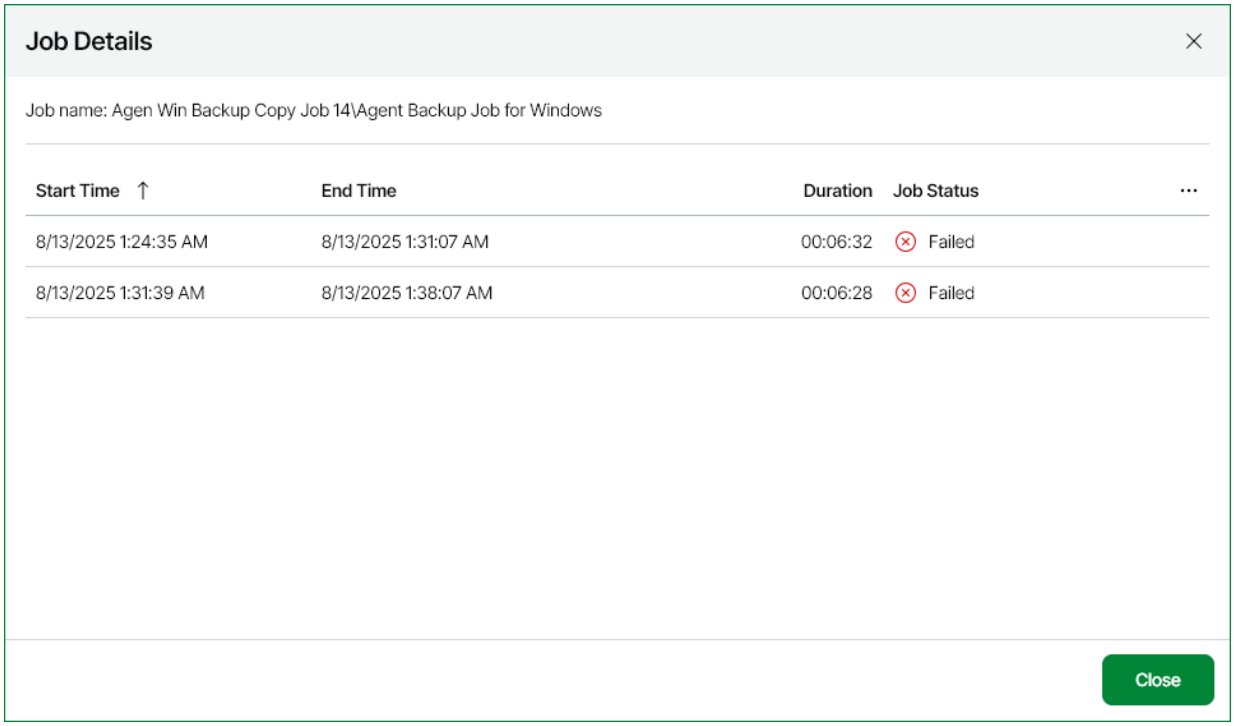
Each scheduled job session is described with the following set of properties:

- **Job** – name of a job.
- **Job Type** – type of job (*Backup*, *Replication*, *Backup copy*, *Tape job*, *VM and file copy*, *SureBackup*).
- **Start Time** – date and time when the job session will start.
- **Average Duration** – average time a job session takes to complete. Only the latest 5 sessions are considered.

Each completed job session is described with the following set of properties:

- **Job** – name of a job.
- **Job Type** – type of a job (*Backup*, *Replication*, *Backup copy*, *Tape job*, *VM and file copy*, *SureBackup*).
- **Job Status** – status of the job session (*Success*, *Warning*, *Failed*, *Running*).
- **Start Time** – date and time when the job session started.
- **End Time** – date and time when the job session ended.
- **Duration** – duration of the job session.
- **Average Duration** – average time a job session takes to complete. Only the latest 5 sessions are considered.
- **Data Transferred, GB** – total amount of data transferred during the a job session.

Some colored band segments include data on multiple sessions. Usually, those segments are marked with the number of aggregated sessions. To view the sessions data, click the related segment.



Dashboards

Veeam ONE Web Client dashboards provide at-a-glance view on the managed Veeam Backup & Replication and Veeam Backup for Microsoft 365 infrastructure, VMware vSphere and Microsoft Hyper-V environments. You can view dashboards in the web browser, schedule automatic dashboard delivery or integrate dashboards into the intranet web portals, such as Microsoft SharePoint.

Every dashboard includes a set of visual components called *widgets*. Widgets are visual modules that portray various aspects of the managed environment in the form of charts, graphs or tables. By aggregating several widgets on a single screen, dashboards allow you to focus on critical areas of the managed environment, track dependencies and interrelated aspects.

Veeam ONE Web Client includes a set of predefined dashboards. For detailed description of predefined dashboards, see Predefined Veeam ONE Dashboards.

In addition to predefined dashboards, you can create custom dashboards to meet your requirements. In custom dashboards, you can choose the necessary widgets and specify widget properties.

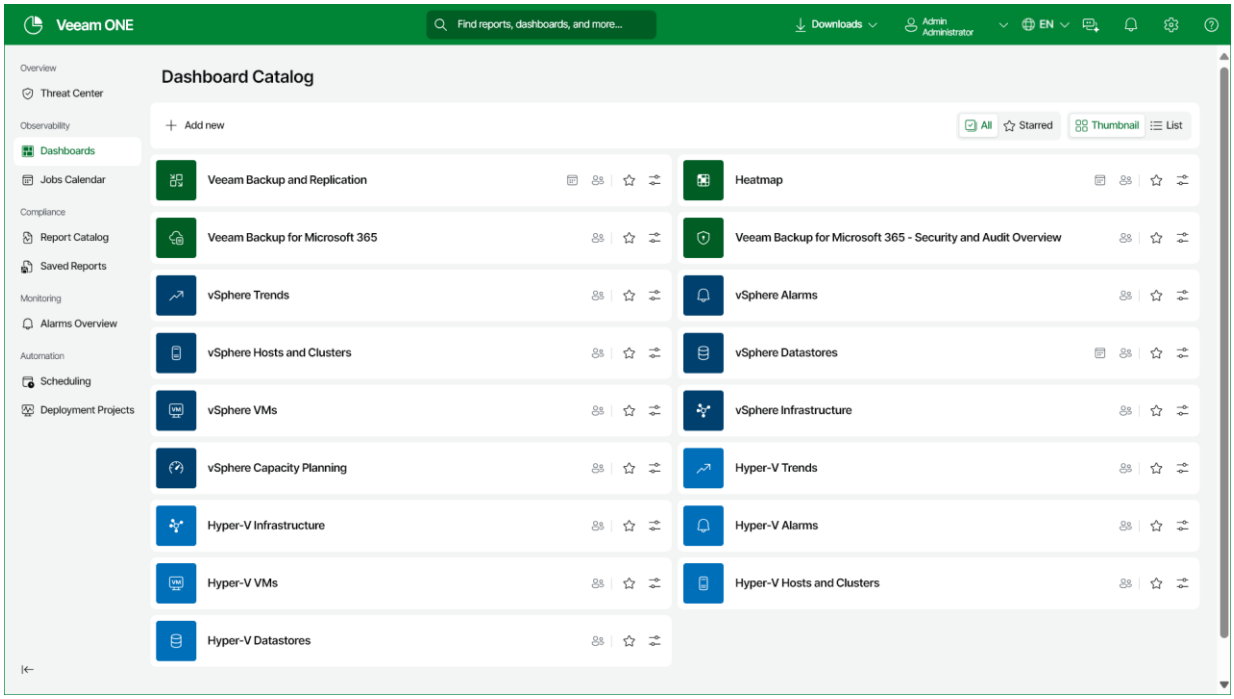
Viewing Dashboards

Veeam ONE Web Client dashboards are available in the **Dashboards** section.

The **Dashboards** section displays preview images for available dashboards (dashboards for which data has been collected from connected servers). You can re-arrange the dashboards by dragging their preview images to the necessary position in the **Dashboards** section.

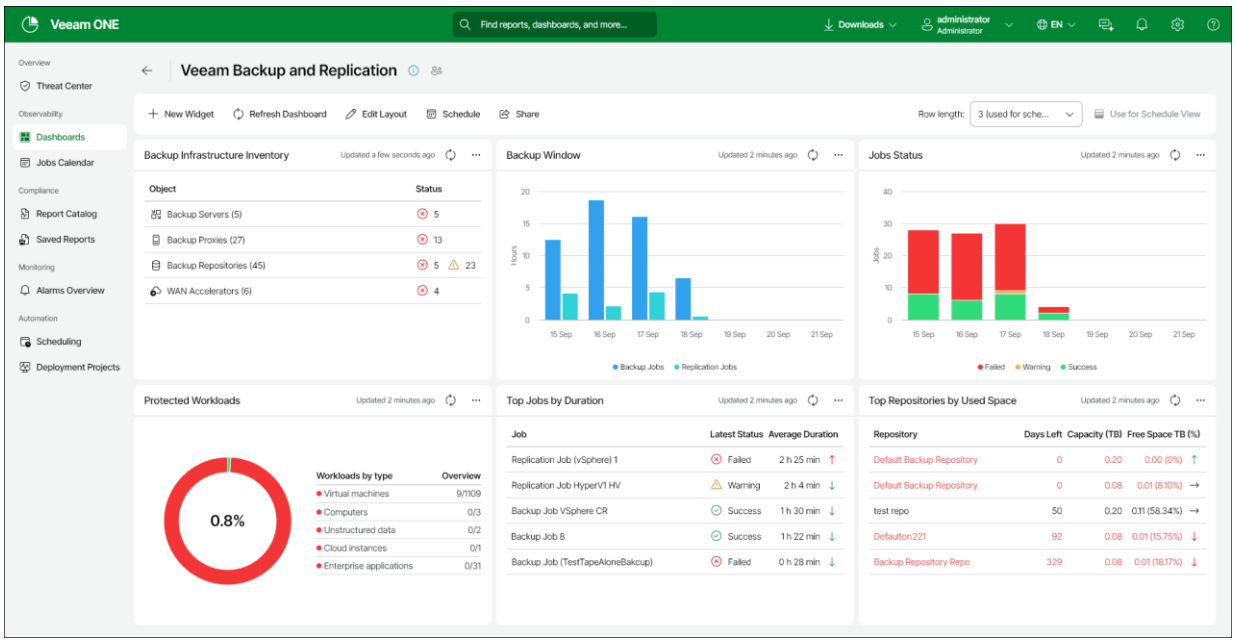
To view a dashboard:

1. Open Veeam ONE Web Client.
2. Open the **Dashboards** section.
   - (Optional) Toggle between **Thumbnail** and **List** view to display.
   - (Optional) Click the star on each dashboard to create a personalized list of you favorite dashboards accessible by the **Starred** button.
3. Click the dashboard preview image.



Dashboard Details

Dashboards are composed of widgets that display various aspects of the managed environment. Every widget is located in a separate cell, or entry, in the dashboard.



To get back to the list of dashboards, click the **Dashboards** tab on the left of the page, click the **Go back** button at the top left corner or use the browser **Back** button.

Creating Custom Dashboards

In addition to predefined dashboards, you can create custom dashboards and add custom widgets to this dashboard. To create a custom dashboard, perform the following steps:

1. Create a dashboard and specify its settings.

   Create a new dashboard, specify its name and description.

2. Add widgets to the dashboard.

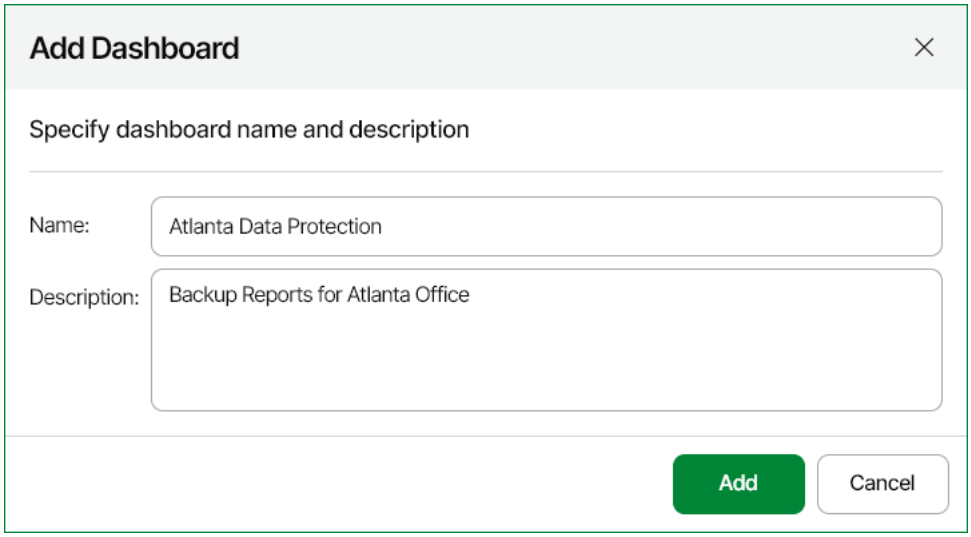
   Add custom widgets to the new dashboard and specify widget settings.

Step 1. Create Dashboard

To create a new dashboard:

1. Open Veeam ONE Web Client.
2. Open the **Dashboards** section.
3. At the top left corner of the **Dashboards** section, click **Add New**.
4. In the **Add dashboard** window, specify dashboard settings:
   - In the **Name** field, specify the name that will be displayed at the top of the dashboard.
   - In the **Description** field, specify a brief dashboard description.
5. Click **Add**.

A new empty dashboard will be created and added to the **Dashboards** section.



Step 2. Add Widgets to Dashboard

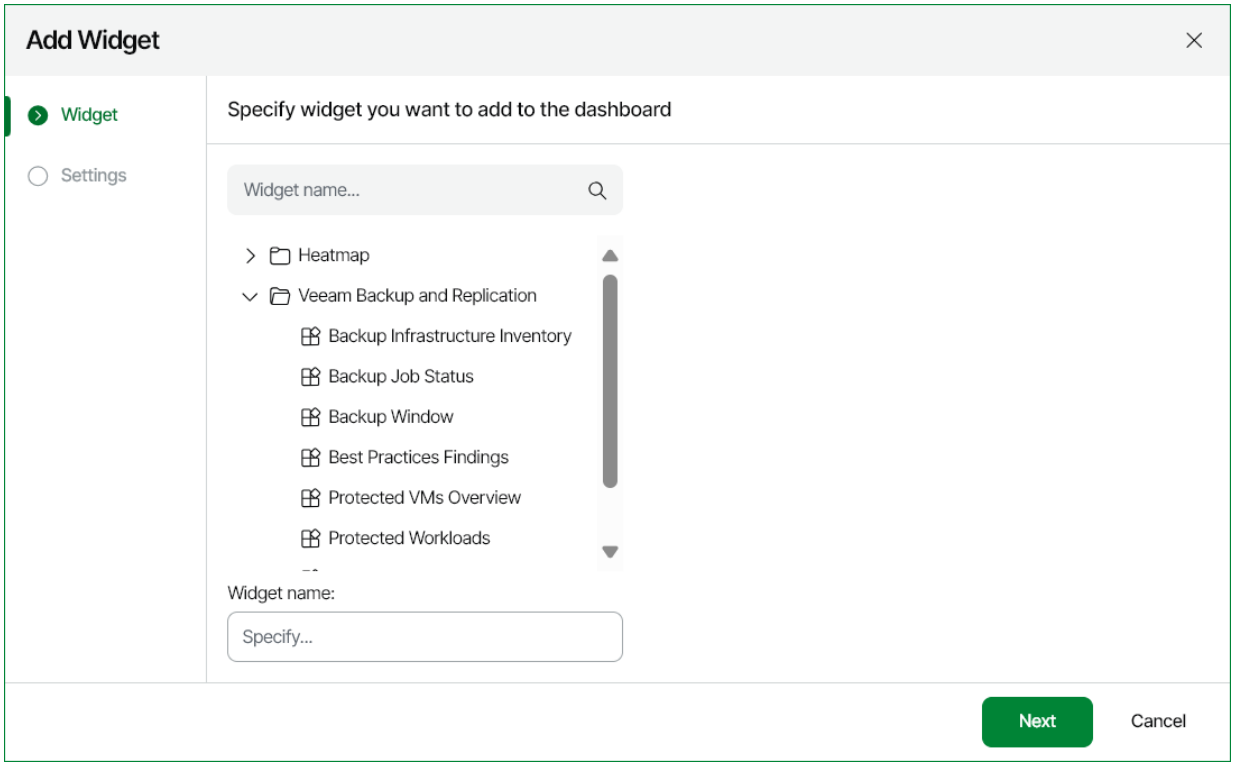
After you create a new dashboard, you must add widgets to it.

Veeam ONE Web Client comes with a set of widgets packs for Veeam Backup & Replication, Veeam Backup for Microsoft 365, VMware vSphere and Microsoft Hyper-V. Widget packs include ready-to-use widgets that portray various aspects of the managed environment. You can add widgets from widget packs to custom dashboards.

To add a widget to a dashboard:

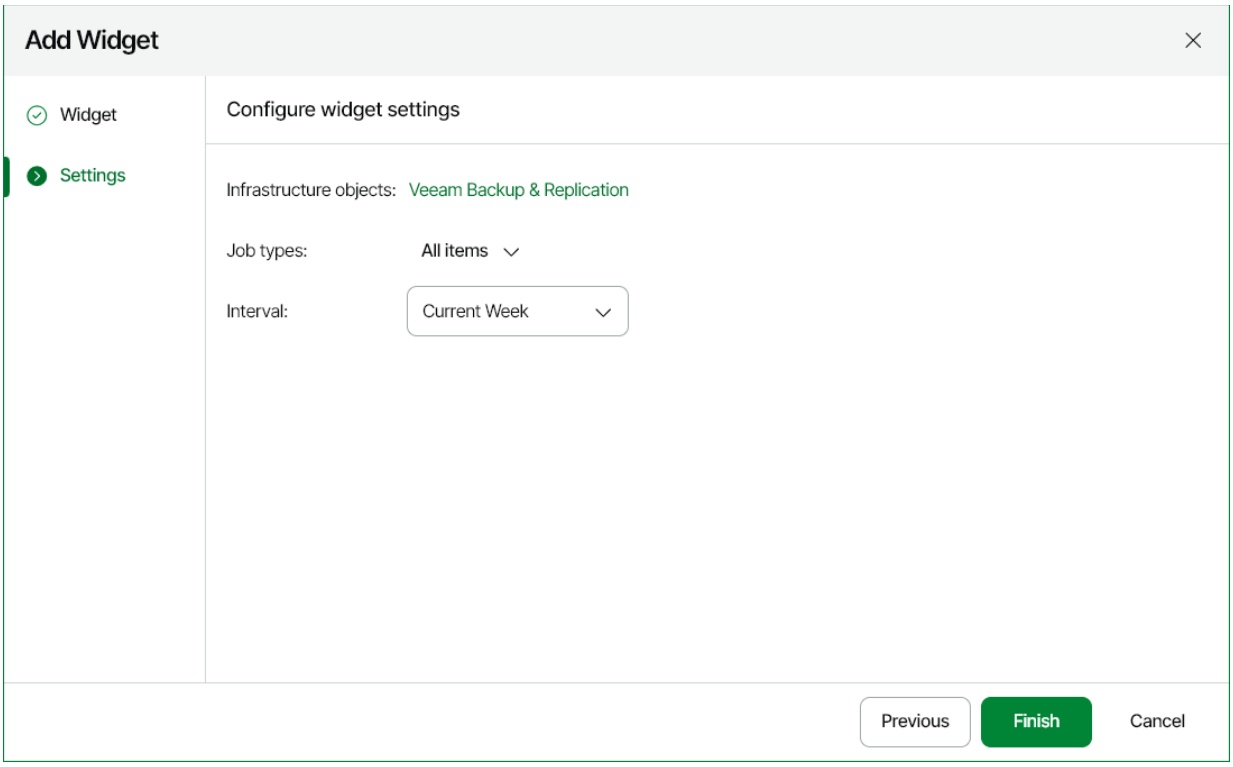
1. Open Veeam ONE Web Client.
2. Open the **Dashboards** section.
3. Click the dashboard preview image.
4. At the top left corner of the dashboard window, click **New Widget**.

   Veeam ONE Web Client will launch the **Add Widget** wizard.
5. At the **Widget** step of the wizard, select a widget to add on the dashboard and specify the widget name in the **Widget name** field. The widget name will be displayed at the top of the widget on the dashboard.

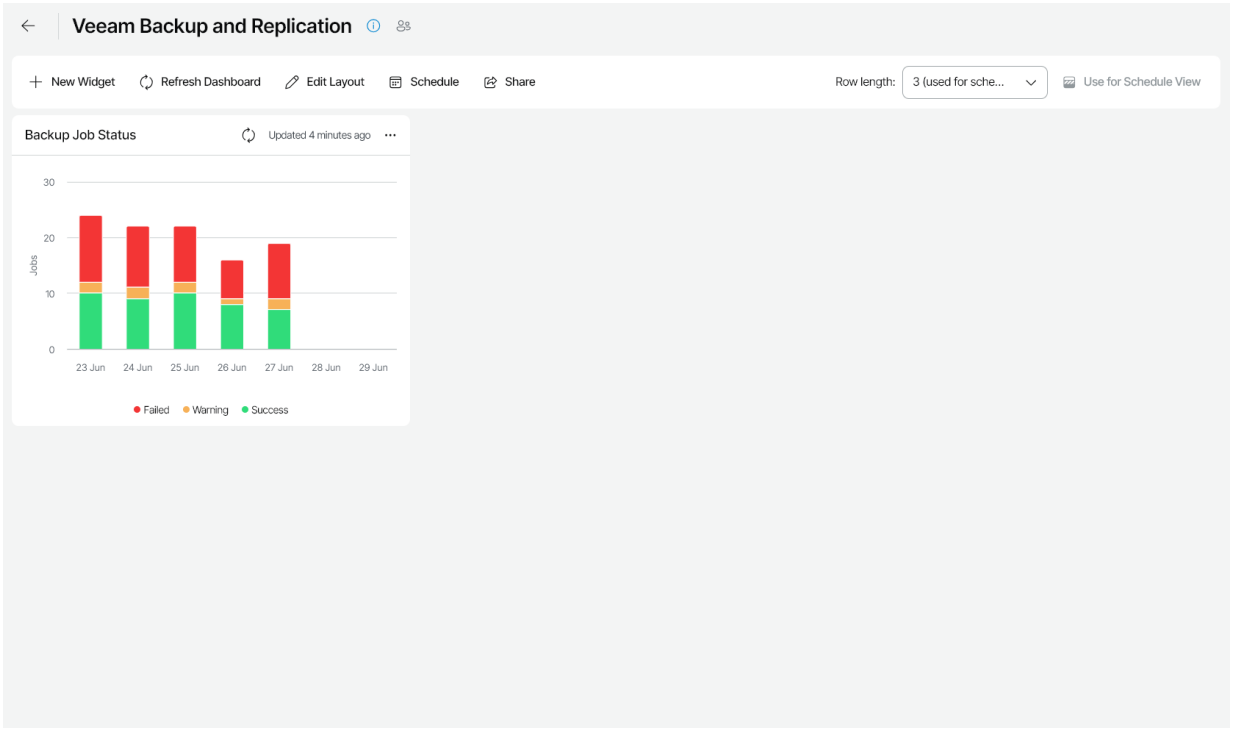


6. At the **Settings** step of the wizard, define widget options, such as the scope, time interval, number of objects to display in the widget and so on.

   Availability of widget options depends on the type of the selected widget.



7. Click **Finish** to add the widget to the dashboard.



8. Repeat steps **4–8** for each new widget you want to add to the dashboard.

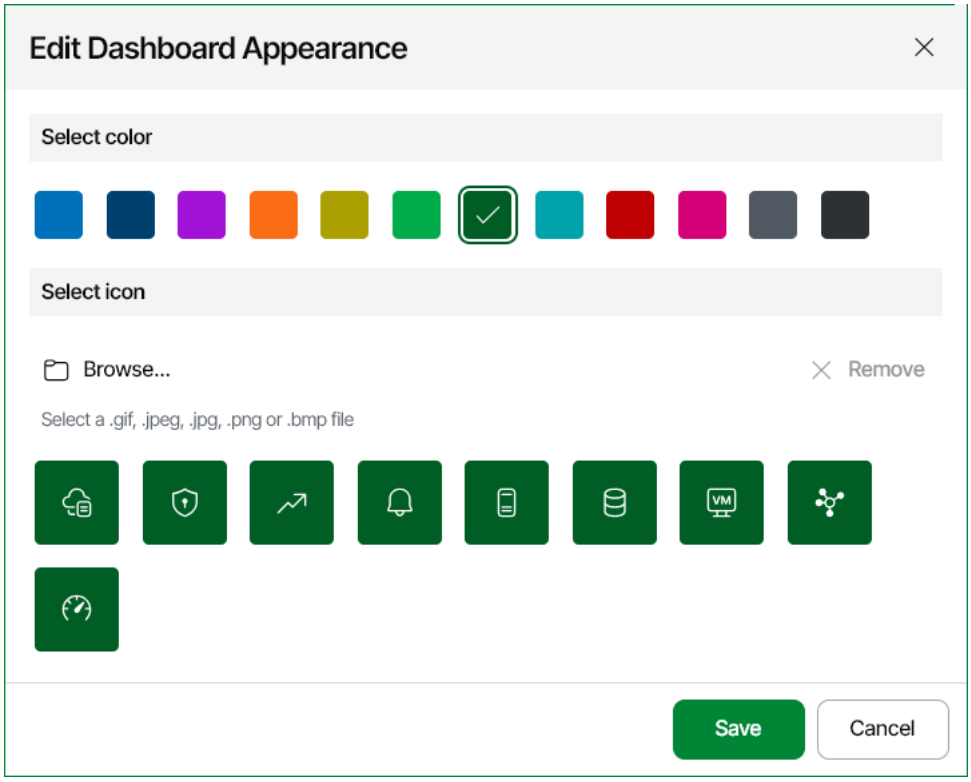
Setting Dashboard Preview Image and Color

You can select the preview image and background color that will be used to depict the dashboard in the **Dashboards** section.

To set a preview image and background color for a dashboard:

1. Open Veeam ONE Web Client.
2. Open the **Dashboards** section.
3. At the right edge of the dashboard thumbnail, expand the **Settings** menu and click **Edit Appearance**.
4. In the **Select color** palette, choose the necessary background color.
5. In the **Select icon** list, choose an image that must depict the dashboard.

   You can select a custom image preview image. To do so, click the **Browse** link at the top of the list and select the necessary image file. The image must be in GIF, JPEG, JPG, PNG, BMP or SVG format.
6. Click **Save**.



Managing Dashboard Layout

You can arrange widgets in a dashboard, change the number of widget columns and select a row length for dashboard schedule.

Changing Dashboard Layout

To change the arrangement of dashboard widgets:

1. Open Veeam ONE Web Client.
2. Open the **Dashboards** section.
3. Click the necessary dashboard to open it.
4. At the top left corner of dashboard window, click **Edit Layout**.
5. Change the arrangement of widgets by dragging them to the necessary dashboard cells.
6. Click **Save**.

Changing Dashboard Row Length

To change the number of widget columns:

1. Open Veeam ONE Web Client.
2. Open the **Dashboards** section.
3. Click the necessary dashboard to open it.
4. In the **Row length** list, choose the number of widget columns.
5. To assign the selected number of columns to automatically delivered dashboards, click **Use for Schedule View**.

   For details on dashboard delivery, see Scheduling Dashboards.

Scheduling Dashboards

You can schedule automatic dashboard delivery. You can choose to receive dashboards by email, save dashboards to a disk or network share.

To schedule automatic dashboard delivery:

1. Open Veeam ONE Web Client.
2. Open the **Dashboards** section.
3. At the right edge of the dashboard preview image, expand the **Settings** menu and click **Schedule**.

   Alternatively, you can click the dashboard preview image to open the dashboard and click **Schedule** at the top left corner of the dashboard window.
4. In the **Dashboard Scheduling Settings** window, click **Add**.

   Veeam ONE Web Client will launch the **Add Dashboard Schedule** wizard.
5. Configure dashboard delivery schedule as described in section Scheduling.
6. Click **Close**.

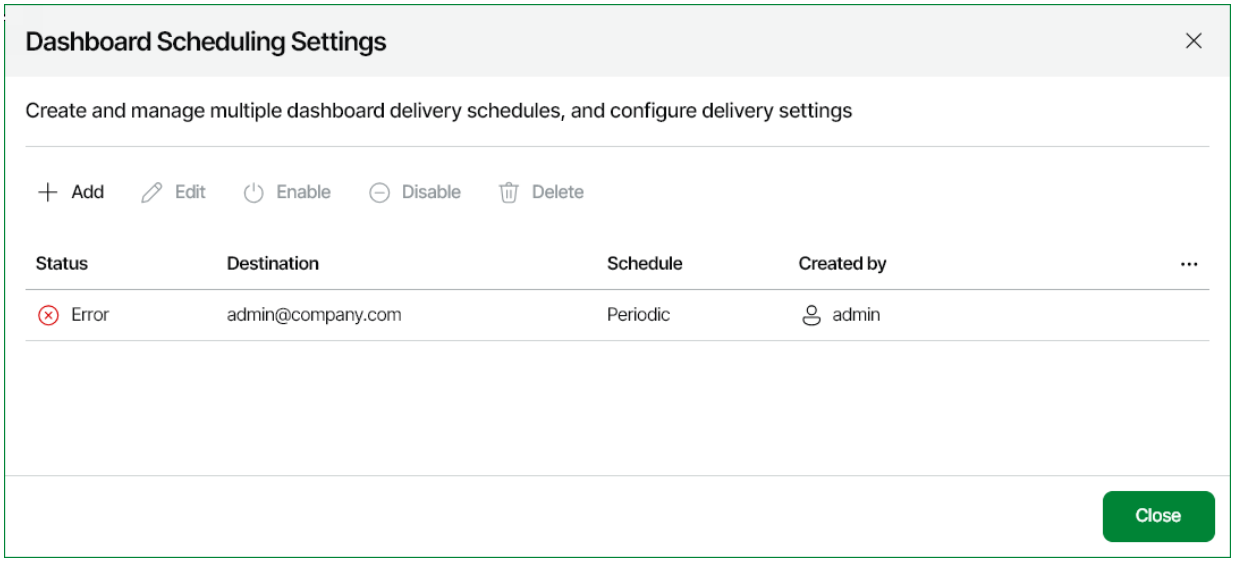
Managing Dashboard Schedules

You can create multiple schedules for a dashboard. Configuring multiple schedules allows you to set up complex scheduling and delivery method settings for the same dashboard.

To manage dashboard schedules:

1. Open Veeam ONE Web Client.
2. Open the **Dashboards** section.
3. At the right edge of the dashboard preview image, expand the **Settings** menu and click **Schedule**.

   Alternatively, you can click the dashboard preview image to open the dashboard and click **Schedule** at the top left corner of the dashboard window.
4. Use buttons in the **Dashboard Scheduling Settings** window to manage the schedules that you added for the dashboard:
   - To create a new dashboard schedule, click **Add**.
   - To edit scheduling settings, select a schedule in the list and click **Edit**.
   - To enable a previously disabled schedule, select the schedule in the list and click **Enable**.
   - To temporarily disable a schedule, select the schedule in the list and click **Disable**.
   - To delete a schedule from the list, select the schedule in the list and click **Delete**.
5. To finish working with the schedules, click **Close**.

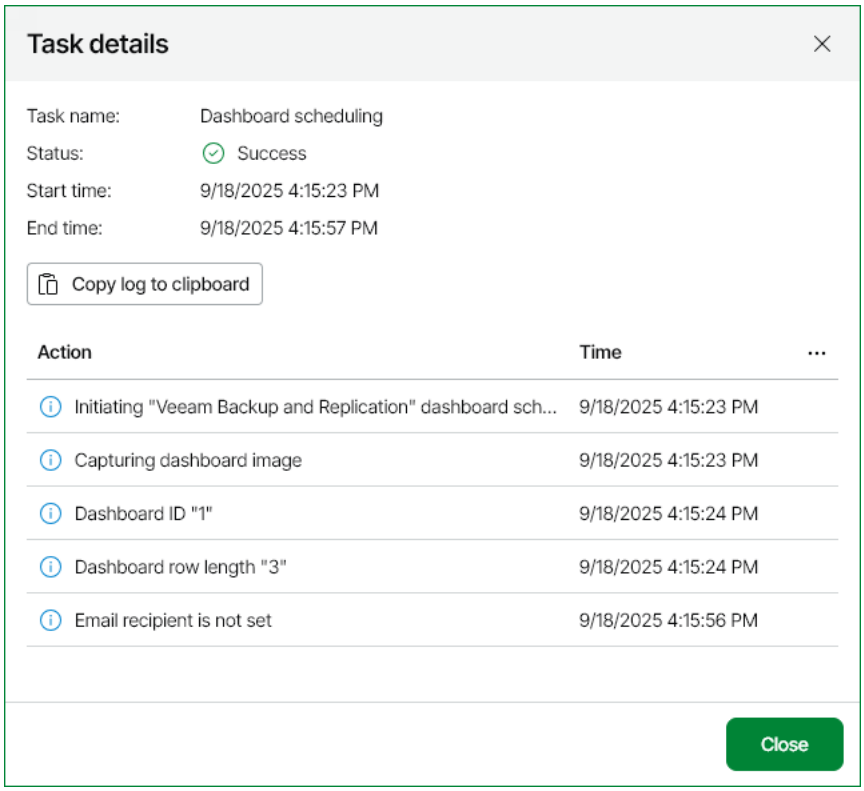


Viewing Dashboard Delivery Results

Every dashboard delivery initiates a new delivery session.

To view details of dashboard delivery sessions:

1. Open Veeam ONE Web Client.
2. At the top right corner of the Veeam ONE Web Client window, click **Configuration**.
3. In the **Data Collection** tab, click **Task Sessions**.
4. To display all dashboard delivery sessions, click **Filters**, select *Dashboard scheduling*, and click **Apply**.
5. Click the necessary session in the list to display detailed information about it.



Cloning Dashboards

If you need a custom dashboard, you can create a clone of an existing dashboard and modify its settings and widgets.

To clone a dashboard:

1. Open Veeam ONE Web Client.
2. Open the **Dashboards** section.
3. At the right edge of the dashboard preview image, expand the **Settings** menu and click **Clone**.
4. In the **Clone Dashboard** window, change the name and description of a dashboard clone.
5. Modify dashboard widgets as described in Managing Widgets.
6. If necessary, modify dashboard preview image and color as described in Setting Dashboard Preview Image and Color.
7. If necessary, modify dashboard layout as described in Managing Dashboard Layout.

Sharing Dashboards

To share a dashboard with other users, you can enable public access to the dashboard or generate a direct dashboard link.

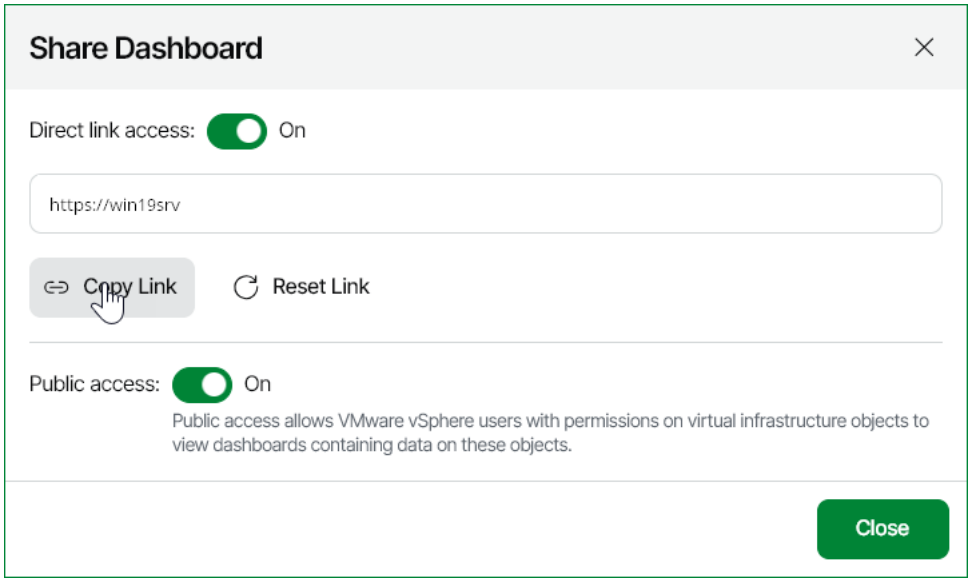
Generating Direct Dashboard Link

To share a dashboard with other users, or integrate a dashboard to a web portal, you can generate a direct dashboard link:

1. Open Veeam ONE Web Client.
2. Open the **Dashboards** section.
3. At the right edge of the dashboard preview image, expand the **Settings** menu and click **Share**.

   Alternatively, you can click the dashboard preview image to open the dashboard and click **Share** at the top left corner of the dashboard window.
4. In the **Share Dashboard** window, switch the **Direct link access** toggle to *On*.
5. Click **Copy Link** to copy the link and use it to share with other users or integrate to web portals.
6. If you need to generate a new direct link, click **Reset Link**.

   Note that after you change the direct link, the previous link will become invalid.
7. Click **Close**.



Enabling and Disabling Public Access

To share a dashboard with other users, you can enable public access to this dashboard. Veeam ONE users, including VMware vSphere and VMware Cloud Director users who have permissions assigned on virtual infrastructure objects, can access published dashboards in the Veeam ONE Web Client.

> **NOTE:**
>
> Predefined dashboards are available for public access by default.

To enable or disable public access to a dashboard:

1. Open Veeam ONE Web Client.
2. Open the **Dashboards** section.
3. At the top right corner of the dashboard preview image, expand the menu and click **Share**.

   Alternatively, you can click the dashboard preview image to open the dashboard and click **Share** at the top left corner of the dashboard window.
4. In the **Share Dashboard** window, switch the **Public access** toggle to *On* to enable public access, or to *Off* to disable public access.
5. Click **Close**.

Modifying Dashboards

You can modify the name, description, layout and widgets of dashboards.

Changing Dashboard Name and Description

To modify the name or description of a dashboard:

1. Open Veeam ONE Web Client.
2. Open the **Dashboards** section.
3. At the right edge of the dashboard preview image, expand the **Settings** menu and click **Edit Information**.
4. In the **Edit Dashboard Information** window, change the dashboard name and description.
5. Click **Save**.

Changing Dashboard Widgets

To modify widgets of a dashboard:

1. Open Veeam ONE Web Client.
2. Open the **Dashboards** section.
3. Click the dashboard preview image.
4. Change properties of dashboard widgets.

   For details, see Managing Widgets.
5. Change the arrangement of dashboard widgets.

   For details on, see Managing Dashboard Layout.

Deleting Dashboards

You can delete dashboards if you no longer need them:

1. Open Veeam ONE Web Client.
2. Open the **Dashboards** section.
3. At the right edge of the dashboard preview image, expand the **Settings** menu and click **Delete**.
4. In the displayed dialog box, click **Delete** to confirm deletion.

Managing Widgets

You can edit settings of dashboard widgets, create reports based on widgets and remove widgets from dashboards.

Changing Widget Properties

You can change the way your widgets look on dashboards:

1. Open Veeam ONE Web Client.
2. Open the **Dashboards** section.
3. Click the necessary dashboard to open it.
4. On the dashboard, select the widget you want to modify.
5. At the top right corner of the widget, expand the menu and click **Edit**.
6. In the **Edit Widget** wizard, change the widget settings.

   For details, see Add Widgets to Dashboard.
7. Save changes.

Creating a Widget Report

You can create reports associated with dashboard widgets:

1. Open Veeam ONE Web Client.
2. Open the **Dashboards** view.
3. Click the necessary dashboard to open it.
4. On the dashboard, select the widget for which you want to create a report.
5. At the top right corner of the widget, expand the menu and click **View Full Report**.
6. In the report window, specify report parameters.
7. Click **Preview** to open the report.

Deleting Widgets

You can delete widgets from dashboards:

1. Open Veeam ONE Web Client.
2. Open the **Dashboards** section.
3. Click the necessary dashboard to open it.
4. On the dashboard, select the widget you want to delete.
5. At the top right corner of the widget, expand the menu and click **Delete**.
6. In the displayed window, click **Delete** to confirm deletion.

Predefined Veeam ONE Dashboards

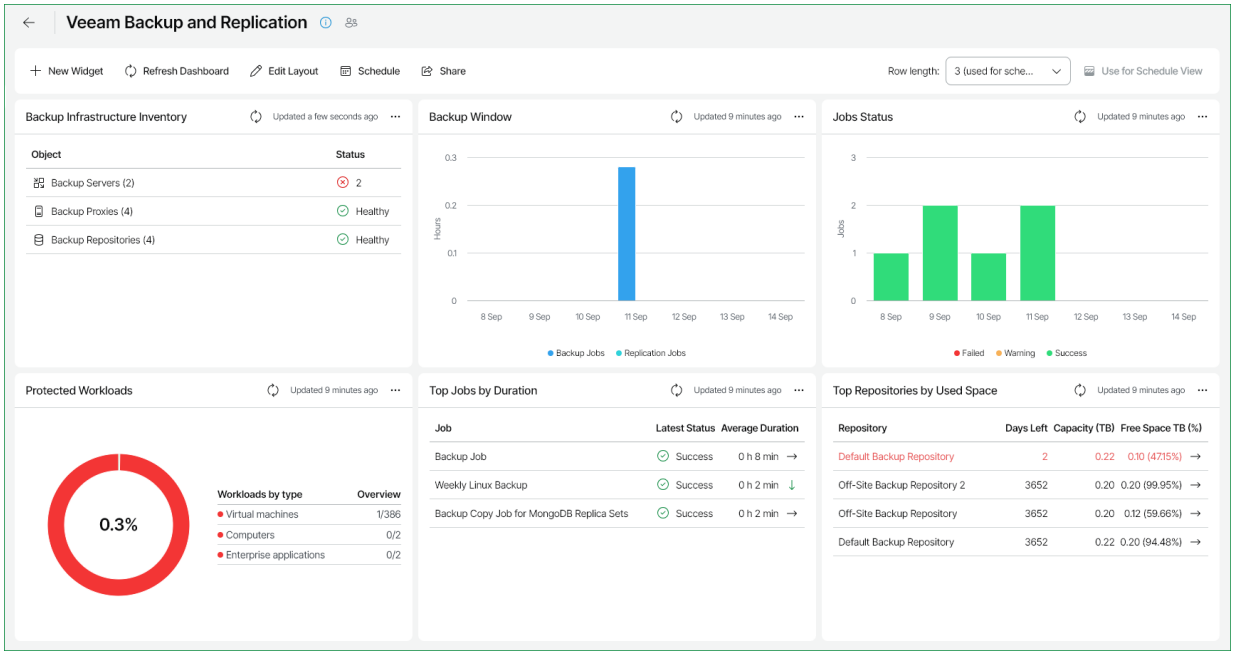
Veeam ONE Web Client features a set of preconfigured dashboards Veeam Backup & Replication, Veeam Backup for Microsoft 365, VMware vSphere and Microsoft Hyper-V.

> **NOTE:**
>
> Some predefined dashboards can represent incomplete data, contain Veeam watermark, or be unavailable due to licensing limitations.

Veeam Backup & Replication Dashboard

The **Veeam Backup & Replication** dashboard provides information on the state of the key backup infrastructure components. The built-in widgets display a list of important events and help focus on the core efficiency indicators.

You can access the **Veeam Backup & Replication** dashboard from the **Dashboard** tab in Veeam ONE Web Client.



Widgets Included

Backup Infrastructure Inventory

This widget describes your backup infrastructure inventory and shows how many backup components of each type are deployed. The widget reflects the health state of backup infrastructure and displays healthy objects (green), objects with warnings (yellow), objects with errors (red).

Best Practices Findings

This widget displays the status of security and compliance checks for each backup server. The widget displays healthy for all checks passed (green), warning for Unable to detect (yellow), error for Not implemented (red), and other for Not checked or Suppressed (gray). This provides a quick overview of your backup infrastructure's compliance and health.

Backup Window

This widget shows the total duration of daily backup and replication job sessions. It allows you to track the efficiency of backup jobs, to detect issues occurred in the backup process and to check whether jobs completed within the prescribed backup window.

Jobs Status

This widget provides information on the completion state of scheduled backup and replication jobs. It displays a daily summary of successfully completed jobs, and shows the number of jobs that completed with warnings and errors during the past week.

The widget helps you assess the efficiency of your data protection operations.

Protected VMs Overview

This widget displays information on VMware vSphere and Microsoft Hyper-V VMs protected with backup and replication jobs, specifically:

- *Protected VMs* — the total number of VMs protected with backups or replicas.
- *Backed Up VMs* — the total number of VMs for which backups are available.
- *Replicated VMs* — the total number of VMs for which replicas are available.
- *Unprotected VMs* — the total number of VMs not protected with backups or replicas.
- *Restore Points* — the total number of available restore points for protected VMs.
- *Full Backups Size* — the amount of storage space consumed by full backups.
- *Increments Size* — the amount of storage space consumed by incremental backups.
- *Source VMs Size* — the total size of storage space consumed by source VMs on production storage.
- *Successful VMs Backup Ratio* — the percentage of latest backup and replication sessions that completed successfully over the previous week against the total number of latest sessions for protected VMs.

Protected Workloads

This widget displays information on all protected workloads in your infrastructure: *VMs* (*VMware*, *Hyper-V*, *AHV*, *Proxmox VE*, *KVM)*, *Computers*, *Cloud instances*, *Enterprise Applications*, *Unstructured Data*.

Top Jobs by Duration

This widget displays top 5 jobs in terms of the longest duration, job completion status and the value of the average weekly duration. The widget helps you assess the backup infrastructure health and efficiency.

Arrows on the right show how job duration has changed over the previous week*.

Top Repositories by Used Space

This widget displays 5 repositories that will run out of free space sooner than other repositories, as well as total capacity and free space left on these repositories. The widget also forecasts how many days remain before the repositories will run out of free space.

Arrows on the right show how the repository free space value has changed over the previous week*.

NOTE:

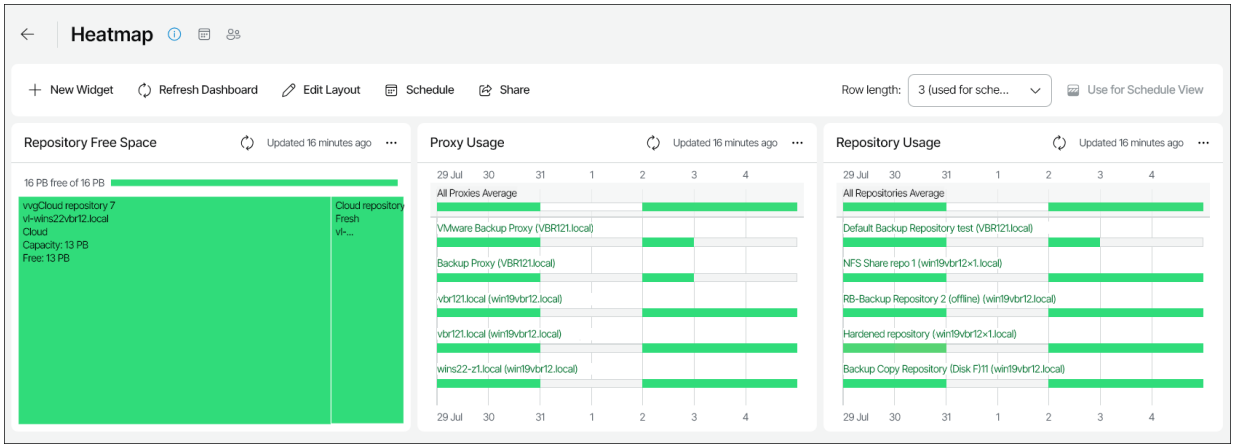
- Veeam ONE Web Client displays file backup copy jobs together with other backup copy jobs.
- Veeam ONE Web Client displays CDP Proxy servers together with other proxy servers.
- Infrastructure topology view in Veeam ONE and Veeam Backup & Replication must match. Otherwise, Veeam ONE Web Client may show invalid data for Veeam Backup & Replication reports and dashboards.

*The arrows allow you to compare the results of this week to the results of the previous week and to track how the trend has evolved. For example, a grey arrow pointing right next to the Duration value means that duration of the job has not changed over the past week, a green arrow pointing down means that job duration has decreased, while a red arrow pointing up means that job duration has increased.

Heatmap

The **Heatmap** dashboard visually represents key resource utilization in your backup infrastructure. The dashboard allows real-time monitoring of free space on repositories as well as repository and proxy usage.

You can access the **Heatmap** dashboard from the **Dashboard** tab in Veeam ONE Web Client.



Widgets Included

Repository Free Space

This widget shows the amount of total and free disk space on each of your backup repositories in a form of a treemap.

Each section of the treemap contains information about a single repository. To see detailed information, hover the pointer over a section. Color of a section is determined by the amount of free space relative to the total space: green color means repository disk space is mostly free while red color means repository disk space is mostly used.

Click a section associated with a scale-out repository to see detailed information about its extents.

Proxy Usage

This widget shows concurrent tasks that backup proxy servers processed during the week.

Each row of the diagram contains information about a single proxy server.

To see details on hourly proxy server usage, click a row. In the section dedicated to a specific proxy server, each cell represents server activity during 1-hour time periods.

To open the section with detailed information about proxy server settings and activity during specific hour, click the cell. This section includes the following elements:

- **Backup server** — host name of the backup server.
- **CPU count** — number of CPU cores.
- **Concurrent tasks limit** — number of maximum concurrent tasks.
- **Max concurrent tasks processed** — configured number of concurrent tasks processed.
- **CPU usage** — CPU resources consumed, in percent.

- **Memory usage** — memory resources consumed, in percent.
- **Related jobs** — list of the concurrent jobs.

Color of a cell is determined by number of processed concurrent tasks relative to maximum number of concurrent tasks: green color means none or few concurrent tasks were processed while red color means number of concurrent tasks is close to or reaches maximum.

Repository Usage

This widget shows concurrent tasks that backup repositories processed during the week.

Each row of the diagram contains information about a single repository.

To see details on hourly repository usage, click a row. In the section dedicated to a specific repository, each cell represents server activity during 1-hour time periods.

To open the section with detailed information about repository settings and activity during specific hour, click the cell. This section includes the following elements:

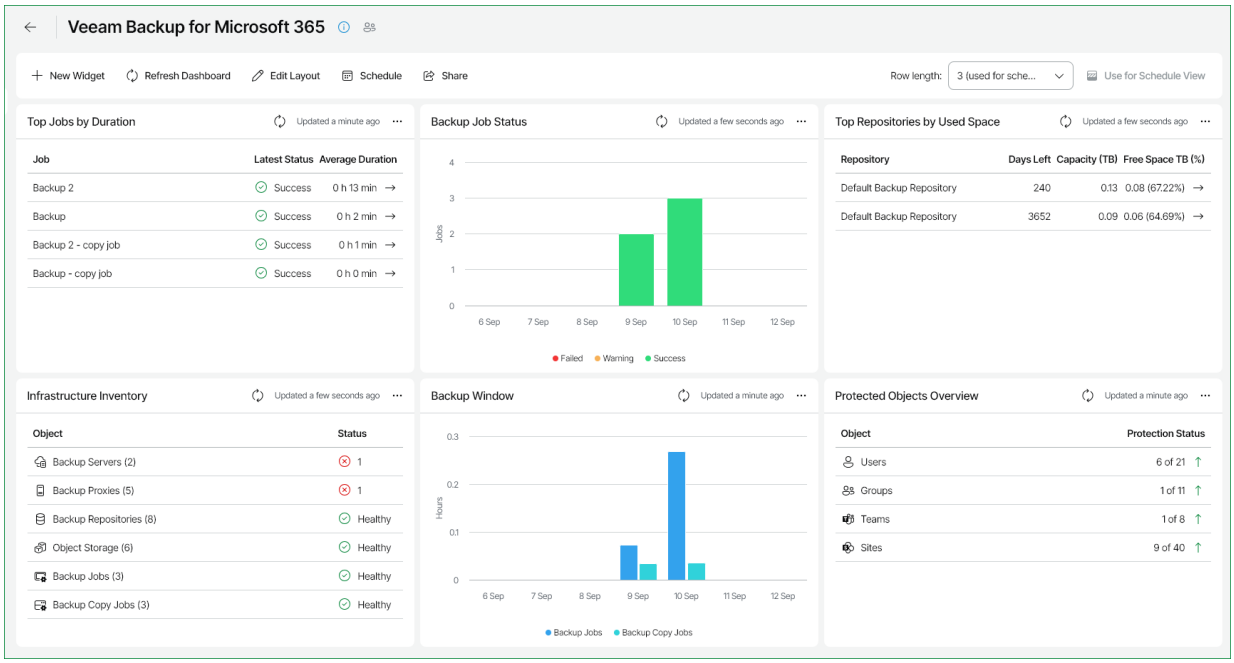
- **Repository type** — type of the repository.
- **Backup server** — host name of the backup server.
- **Concurrent tasks limit** — configured number of maximum concurrent tasks.
- **Max concurrent tasks processed** — number of concurrent tasks processed.
- **Disk Bytes/sec** — operation speed of the repository disk.
- **Related jobs** — list of the concurrent jobs.

Color of the section is determined by the number of processed concurrent tasks relative to the maximum number of concurrent tasks: green color means none or few concurrent tasks were processed while red color means the number of concurrent tasks is close to or reaches maximum.

Veeam Backup for Microsoft 365

The **Veeam Backup for Microsoft 365** dashboard provides information on the state of the key Veeam Backup for Microsoft 365 infrastructure components. The built-in widgets display a list of important events and help focus on the core efficiency indicators.

You can access the **Veeam Backup for Microsoft 365** dashboard from the **Dashboard** tab in Veeam ONE Web Client.



Widgets Included

Top Jobs by Duration

This widget displays top 5 jobs in terms of the longest duration, job completion status and the value of the average weekly duration. The widget helps you assess the backup infrastructure health and efficiency.

Arrows on the right show how job duration has changed over the previous week*.

Backup Job Status

This widget provides information on the completion state of scheduled backup and backup copy jobs. It displays a daily summary of successfully completed jobs, and shows the number of jobs that completed with warnings and errors during the past week.

The widget helps you assess the efficiency of your data protection operations.

Top Repositories by Used Space

This widget displays 5 repositories that will run out of free space sooner than other repositories, as well as total capacity and free space left on these repositories. The widget also forecasts how many days remain before the repositories will run out of free space.

Arrows on the right show how the repository free space value has changed over the previous week*.

To display object storage data in this widget, you must first set the capacity limit for these repositories in your Veeam Backup for Microsoft 365 configuration. To do this, select the **Limit object storage consumption to** check box and specify the limit value in GB, TB or PB. For details on see Adding Object Storage Repositories.

Infrastructure Inventory

This widget describes your Veeam Backup for Microsoft 365 infrastructure inventory and shows how many backup components of each type are deployed. The widget reflects the health state of backup infrastructure and displays how many objects have the *Warning* and *Error* statuses.

Backup Window

This widget shows the total duration of daily backup and backup copy job sessions. It allows you to track the efficiency of jobs, detect issues occurred in the backup process and to check whether jobs completed within the prescribed backup window.

Protected Objects Overview

This widget displays information on Microsoft 365 objects protected with backup jobs, specifically:

- *Users* — the total number of protected user accounts.

  Note that shared mailboxes are counted as separate users.
- *Groups* — the total number of protected user groups.
- *Teams* — the total number of protected Microsoft Teams teams.
- *Sites* — the total number of protected Microsoft 365 organization sites.

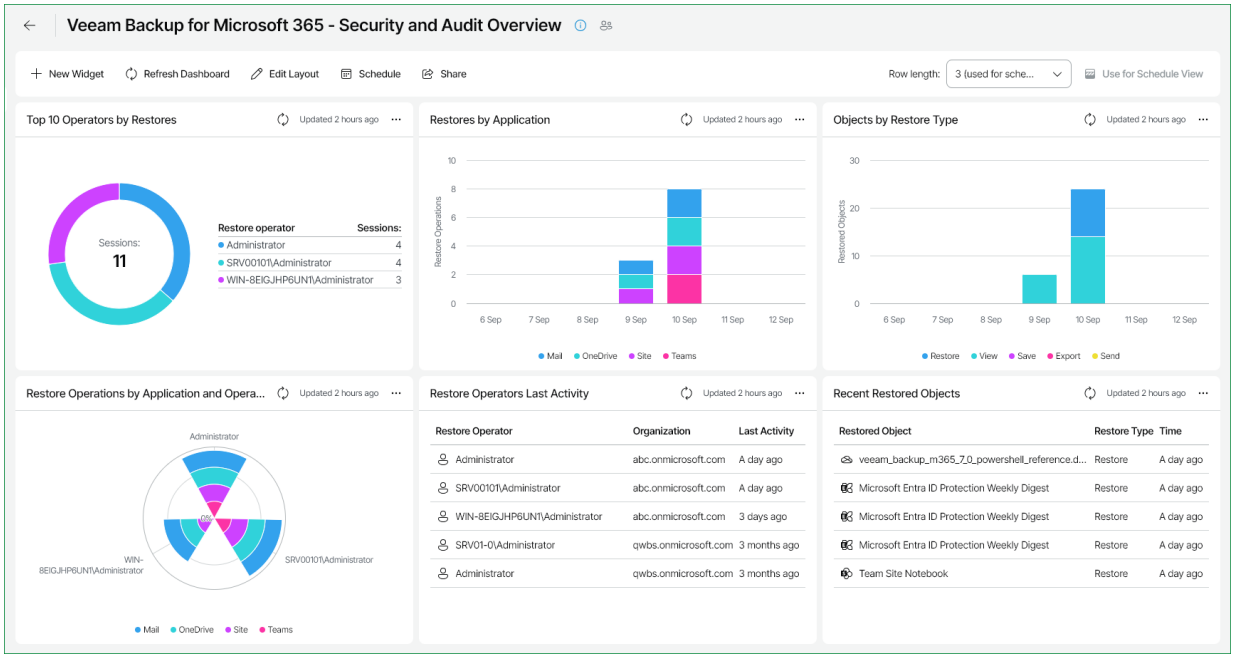
To display only objects with at least one restore point on the widget, select the **Show only objects with at least 1 restore point** check box.

*The arrows allow you to compare the results of this week to the results of the previous week and to track how the trend has evolved. For example, a grey arrow pointing right next to the Duration value means that duration of the job has not changed over the past week, a green arrow pointing down means that job duration has decreased, while a red arrow pointing up means that job duration has increased.

Veeam Backup for Microsoft 365 - Security and Audit Overview

The **Veeam Backup for Microsoft 365 - Security and Audit Overview** dashboard provides detailed information on the state of Veeam Backup for Microsoft 365 restore operations. The built-in widgets display a list of important events and help focus on security and audit indicators. This allows you to monitor all restore activities performed by any authorized user and arrange this information by the type of performed restore actions.

> **NOTE:**
>
> Veeam ONE only collects information about restores from Veeam Backup for Microsoft 365 versions 8 and above. Restore data from versions below 8 is not presented in this dashboard.



Widgets Included

Top 10 Restore Operators by Operations

This widget displays the top 10 users who have initiated the largest number of restore sessions or who have restored the largest number of objects. For details on operator roles, see Data Restore Using Restore Portal.

Hover over the chart segment to break down information about each operator in your organization and the number of restore operations performed on the servers added to the widget scope.

This widget helps you assess the largest number of executed restore operations* by operator in your organization.

Restore Operations by Application

This widget displays the number of restore operations* by application type performed over a defined time period.

This widget helps you assess the most commonly restored applications in your organization.

Objects by Restore Type

This widget displays the number of restored objects by type of restore.

This widget helps you view the number of objects restored with a specific restore type. You can filter out restore type by clicking on the relevant restore type name at the bottom of the widget.

Restore Operations by Application and Operator

This widget allows you to filter and display a composite pie chart of your restore operations and applications for your Veeam Backup for Microsoft 365 infrastructure by user. Hover over the chart to provide additional details for each operator and their restored applications types*.

You can filter out restores for a specific application by clicking on the relevant application name in the widget.

Restore Operators Last Activity

This widget displays a list of operators who performed the most recent restores in your infrastructure.

You can define the number of restore activity entries to display on the widget up to a maximum of 25 entries.

Recent Restored Objects

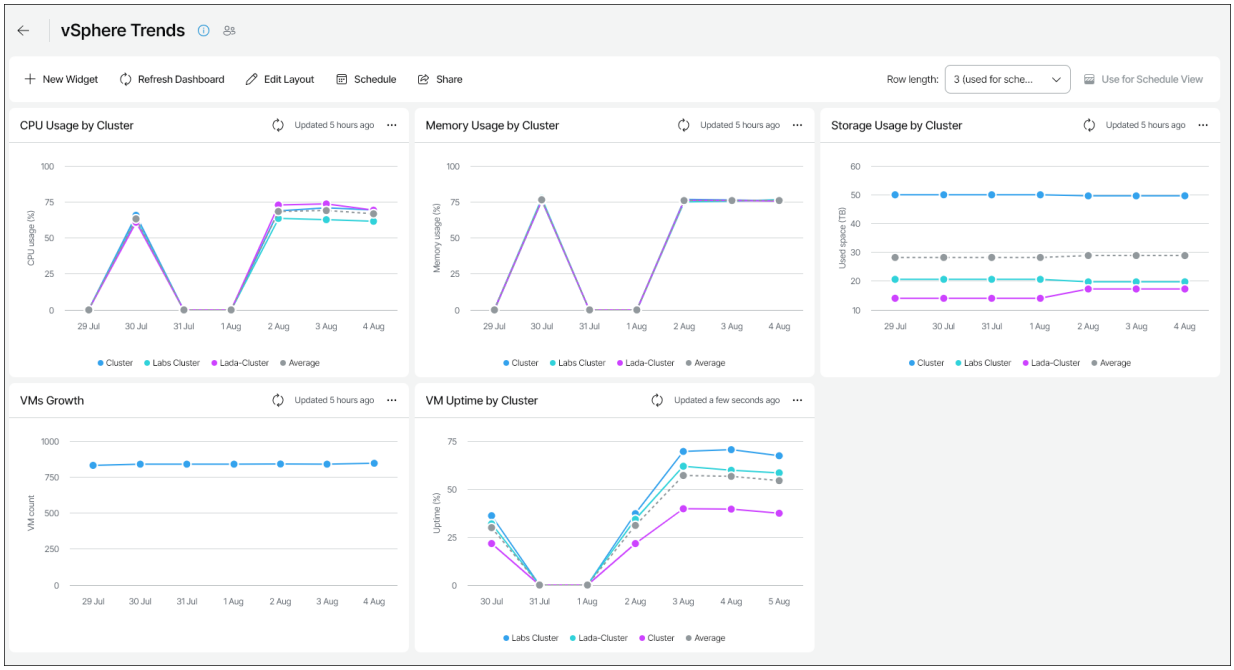
This widget displays the last 5 objects restored in your infrastructure. It provides the following information on each object: object name, type of restore (*View, Save, Send, Export, Restore*) and how long ago the operation was performed.

*You can also configure the widget to display the number of restored objects. To do this, change the **Group by** parameter in the widget settings. For more information on editing widgets, see Managing Widgets.

vSphere Trends

The **vSphere Trends** dashboard helps you track resource utilization in your VMware vSphere infrastructure by displaying growth trends for the previous week.

You can access the **vSphere Trends** dashboard from the **Dashboard** tab in Veeam ONE Web Client.



Widgets Included

CPU Usage by Cluster

This widget shows how CPU utilization in a cluster has been changing during the week.

Memory Usage by Cluster

This widget shows how memory utilization in a cluster has been changing during the week.

Storage Usage by Cluster

This widget shows how storage utilization in a cluster has been changing during the week.

VMs Growth

This widget shows how the number of VMs in your virtual infrastructure has been changing during the week.

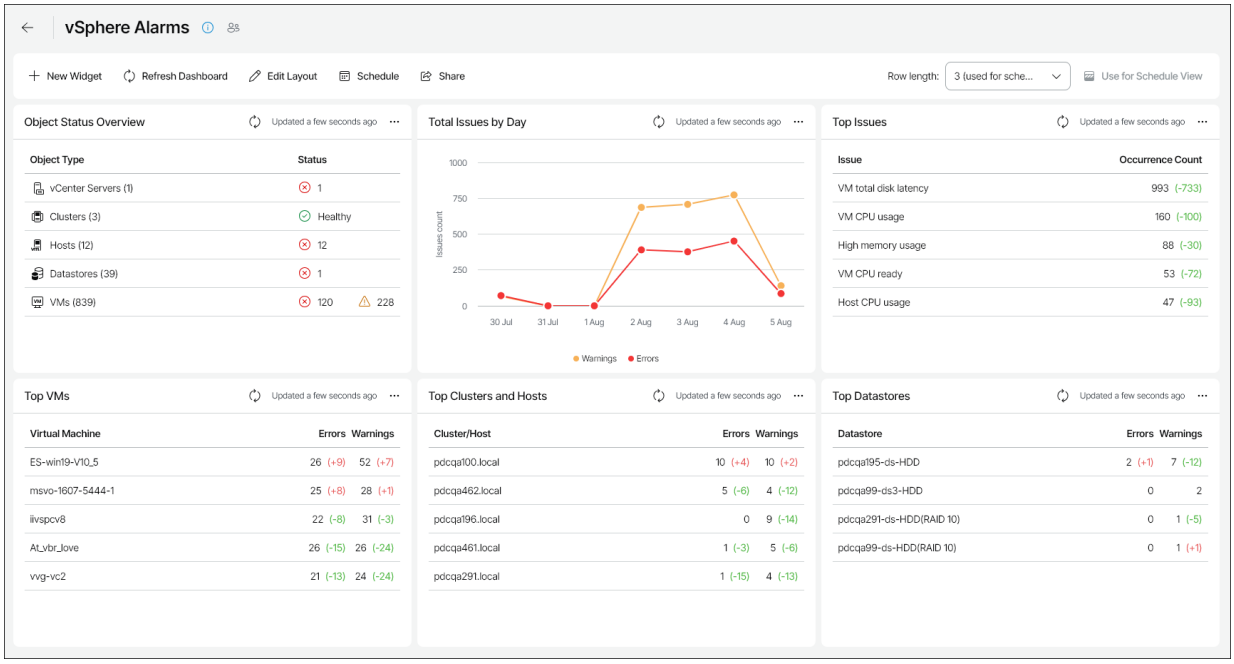
VM Uptime by Cluster

This widget shows how the average uptime value for VMs in a cluster has been changing during the week.

vSphere Alarms

The **vSphere Alarms** dashboard provides an overview of alarms triggered by Veeam ONE Client during the past week. The dashboard allows you to identify the most typical issues that occur in your environment and to simplify troubleshooting.

You can access the **vSphere Trends** dashboard from the **Dashboard** tab in Veeam ONE Web Client.



Widgets Included

Object Status Overview

This widget shows the number of healthy objects, objects with warnings and objects with errors for each infrastructure component type.

Total Issues by Day

This widget displays the daily number of warnings and errors that were triggered during the week.

Top Issues

This widget provides a list of 5 most typical alarms in your environment and shows the number of times each alarm was triggered.

Values in parentheses show how the alarm repeat count has changed over the previous week*.

Top VMs

This widget provides a list of VMs with the highest number of registered errors and warnings.

Values in parentheses show how the number of alarms has changed over the previous week*.

Top Clusters and Hosts

This widget provides a list of virtual infrastructure objects (clusters and hosts) with the highest number of registered errors and warnings.

Values in parentheses show how the number of alarms has changed over the previous week*.

Top Datastores

This widget provides a list of datastores with the highest number of registered errors and warnings.

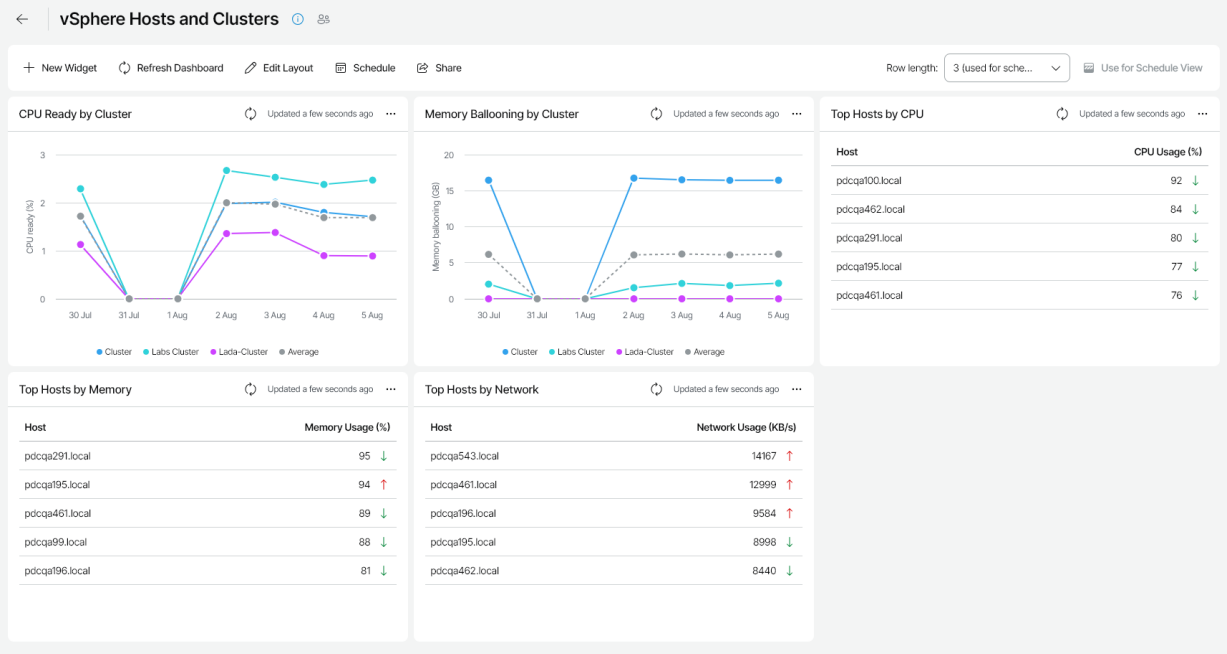
Values in parentheses show how the number of alarms has changed over the previous week*.

*The value in parentheses stands for the amount by which the number of alarms has changed compared to the value of the previous week. For example, the 11 (+5) value means that the number of alarms has increased by 5 over the past week (while the previous value equaled 6), and the 11(-7) value means that the number of alarms has decreased by 7 (while the previous value equaled 18).

vSphere Hosts and Clusters

The **vSphere Hosts and Clusters** dashboard helps you evaluate host and cluster performance in your VMware vSphere infrastructure. The dashboard displays statistics on CPU, memory and network utilization, and helps you identify hosts and clusters with performance issues.

You can access the **vSphere Hosts and Clusters** dashboard from the **Dashboard** tab in Veeam ONE Web Client.



Widgets Included

CPU Ready by Cluster

This widget shows how the average CPU ready time for all VMs on all hosts in the cluster has been changing during the week.

Memory Ballooning by Cluster

This widget shows how the amount of memory processed by the VM memory control driver for all VMs on all hosts in the cluster has been changing during the week.

Top Hosts by CPU

This widget displays weekly CPU utilization data for the top 5 most loaded hosts in your infrastructure.

Arrows on the right show how the average CPU usage value has changed over the previous week*.

Top Hosts by Memory

This widget displays a list of hosts with the highest level of memory consumption.

Arrows on the right show how the average memory usage value has changed over the previous week*.

Top Hosts by Network

This widget displays a list of hosts with the highest level of network usage.

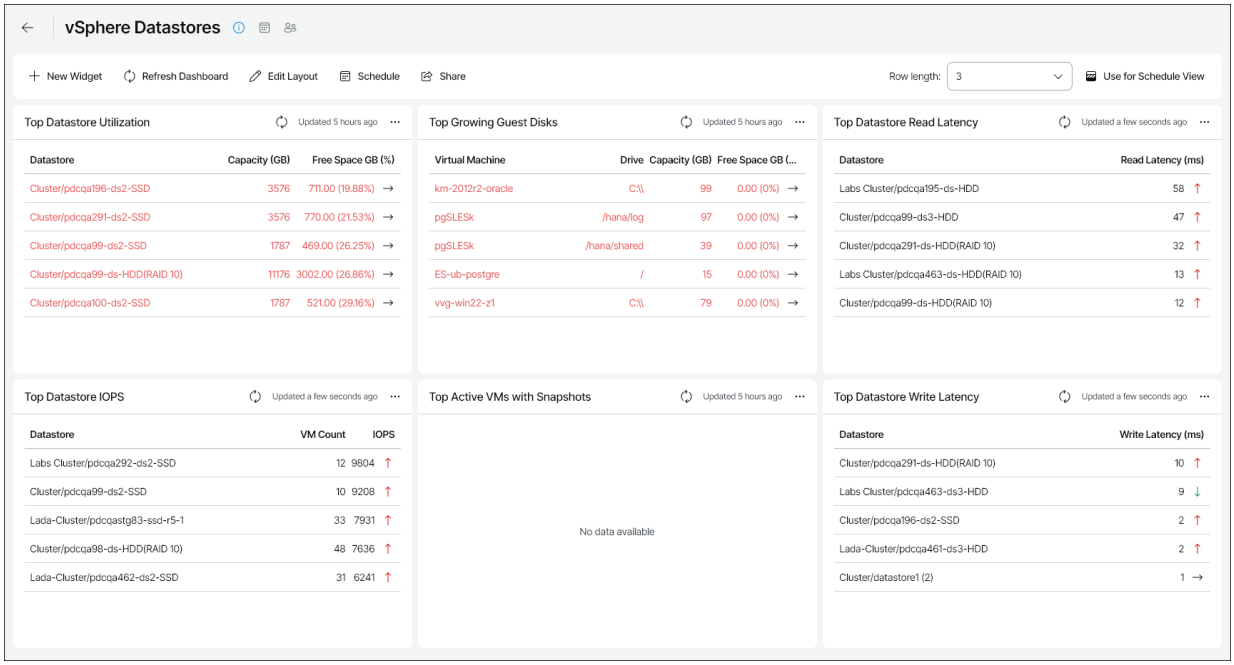
Arrows on the right show how the average network throughput value has changed over the previous week*.

*The arrows allow you to compare the results of this week to the results of the previous week, and to track how the trend has evolved. For example, a grey arrow pointing right next to the CPU Usage value means that CPU utilization has not changed over the past week, a green arrow pointing down means that CPU utilization has decreased, while a red arrow pointing up means that CPU utilization has increased.

vSphere Datastores

The **vSphere Datastores** dashboard is designed to provide at-a-glance view on resource usage and performance of datastores in the VMware vSphere infrastructure. The dashboard helps you assess disk capacities and prevent potential performance bottlenecks.

You can access the **vSphere Datastores** dashboard from the **Dashboard** tab in Veeam ONE Web Client.



Widgets Included

Top Datastore Utilization

This widget displays a list of datastores that will run out of free space sooner than other datastores.

A datastore is highlighted with red if the amount of free space is less than 50% of the capacity value.

Values in parentheses show free space values for the previous week.

Arrows on the right show how the amount of free space has changed over the previous week*.

Top Growing Guest Disks

This widget displays a list of VMs with the least amount of free guest disk space. For each VM in the list, the widget provides information on the logical disk volume and total capacity.

A disk is highlighted with red if the amount of free space is less than 50% of the capacity value.

Values in parentheses show free space values for the previous week.

Arrows on the right show how the amount of free space has changed over the previous week*.

Top Datastore Read Latency

This widget displays a list of datastores with the highest average Read Latency metric values.

Arrows on the right show how the average read latency value has changed over the previous week*.

Top Datastore IOPS

This widget displays a list of datastores with the highest number of IOPS. For each datastore in the list, the widget provides the total number of VMs residing on the datastore.

Arrows on the right show how the number of IOPS has changed over the previous week*.

Top Active VMs with Snapshots

This widget displays a list of VMs with the largest snapshots. For each VM in the list, the widget provides the name of the datastore where the VM snapshots are located.

A VM is highlighted with red if the total size of all VM snapshots is greater than 20% of the VM size.

Top Datastore Write Latency

This widget displays a list of datastores with the highest Write Latency metric values.

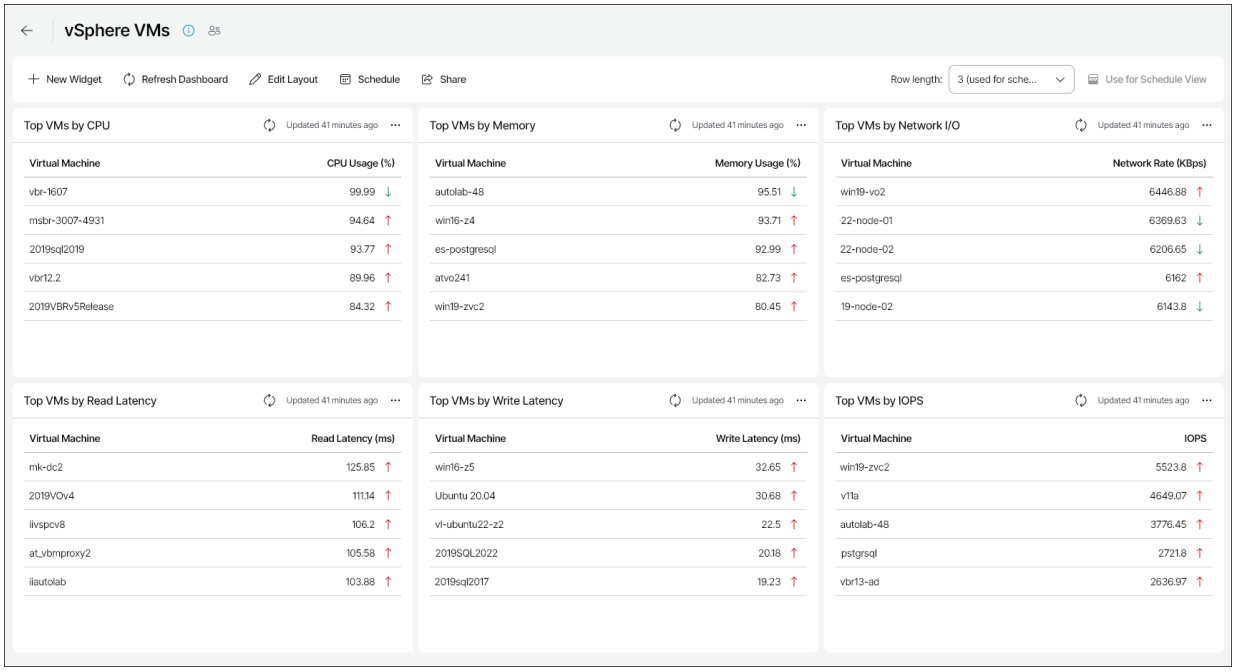
Arrows on the right show how the average write latency value has changed over the previous week*.

*The arrows allow you to compare the results of this week to the results of the previous week, and to track how the trend has evolved. For example, a grey arrow pointing right next to the Write Latency value means that the average latency has not changed over the past week, a green arrow pointing down means that the average latency has decreased, while a red arrow pointing up means that the average latency has increased.

vSphere VMs

The **vSphere VMs** dashboard provides information about health and performance of VMs in the VMware vSphere infrastructure, and shows general VM statistics on CPU, memory and network usage for the past week.

You can access the **vSphere VMs** dashboard from the **Dashboard** tab in Veeam ONE Web Client.



Widgets Included

Top VMs by CPU

This widget displays a list of VMs with the highest average level of CPU utilization.

Arrows on the right show how the CPU usage value has changed over the previous week*.

Top VMs by Memory

This widget displays a list of VMs with the highest average level of memory utilization. The memory utilization value is calculated as a percentage of total memory allocated for the VM.

Arrows on the right show how the memory utilization value has changed over the previous week*.

Top VMs by Network I/O

This widget displays a list of VMs with the highest average network throughput values.

Arrows on the right show how the throughput value has changed over the previous week*.

Top VMs by Read Latency

This widget displays a list of VMs with the highest average Read Latency metric values.

Arrows on the right show how the average read latency value has changed over the previous week*.

Top VMs by Write Latency

This widget displays a list of VMs with the highest average Write Latency metric values.

Arrows on the right show how the average write latency value has changed over the previous week*.

Top VMs by IOPS

This widget displays a list of VMs with the highest average number of IOPS.

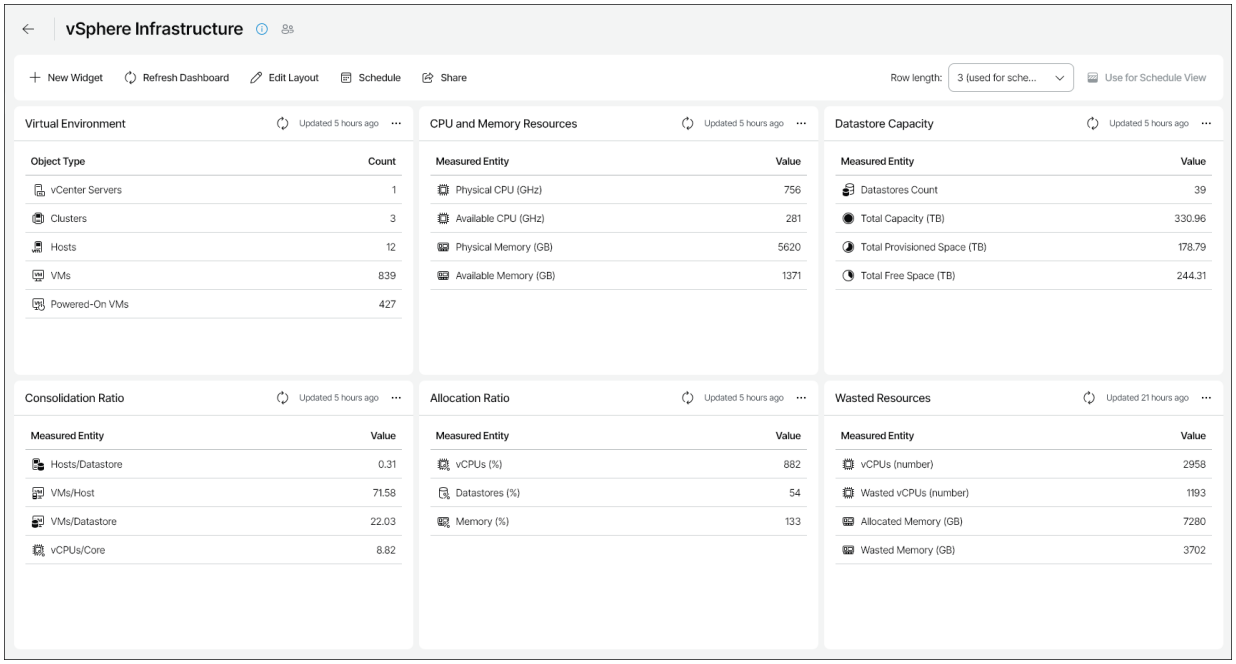
Arrows on the right show how the number of IOPS has changed over the previous week*.

*The arrows allow you to compare the results of this week to the results of the previous week, and to track how the trend has evolved. For example, a grey arrow pointing right next to the CPU Usage value means that CPU utilization has not changed over the past week, a green arrow pointing down means that CPU utilization has decreased, while a red arrow pointing up means that CPU utilization has increased.

vSphere Infrastructure

The **vSphere Infrastructure** dashboard is designed to provide at-a-glance view of configuration of the VMware vSphere infrastructure and to help you assess the overall performance and resource usage efficiency.

You can access the **vSphere Infrastructure** dashboard from the **Dashboard** tab in Veeam ONE Web Client.



Widgets Included

Virtual Environment

This widget shows the total number of vCenter servers, clusters, ESXi hosts and VMs in your environment, as well as the number of currently running VMs.

CPU and Memory Resources

This widget assesses physical CPU and memory resources installed on ESXi hosts and shows the amount of available resources allocated to VMs.

Datastore Capacity

This widget provides information on the number of datastores in your environment, their total capacity, the amount of provisioned and free space left on the datastores.

Consolidation Ratio

The widget tracks the amount of virtual hardware placed on physical hardware:

- Hosts/Datastore ratio shows the average number of hosts connected to a single datastore.
- VMs/Host ratio shows the average number of VMs running on a single physical host.
- VMs/Datastore ratio shows the average number of VMs that store data on a single datastore.

- vCPUs/Core ratio shows the average number of virtual processors operating on a single physical CPU core.

Allocation Ratio

The widget tracks the amount of virtual and physical resources allocated to VMs:

- vCPU allocation ratio shows the number of virtual processors operating on a single physical CPU core (in percentage).
- Datastores allocation ratio shows the amount of datastore space allocated to VMs (in percentage).
- Memory allocation ratio shows the amount of physical RAM allocated to VMs (in percentage).

Wasted Resources

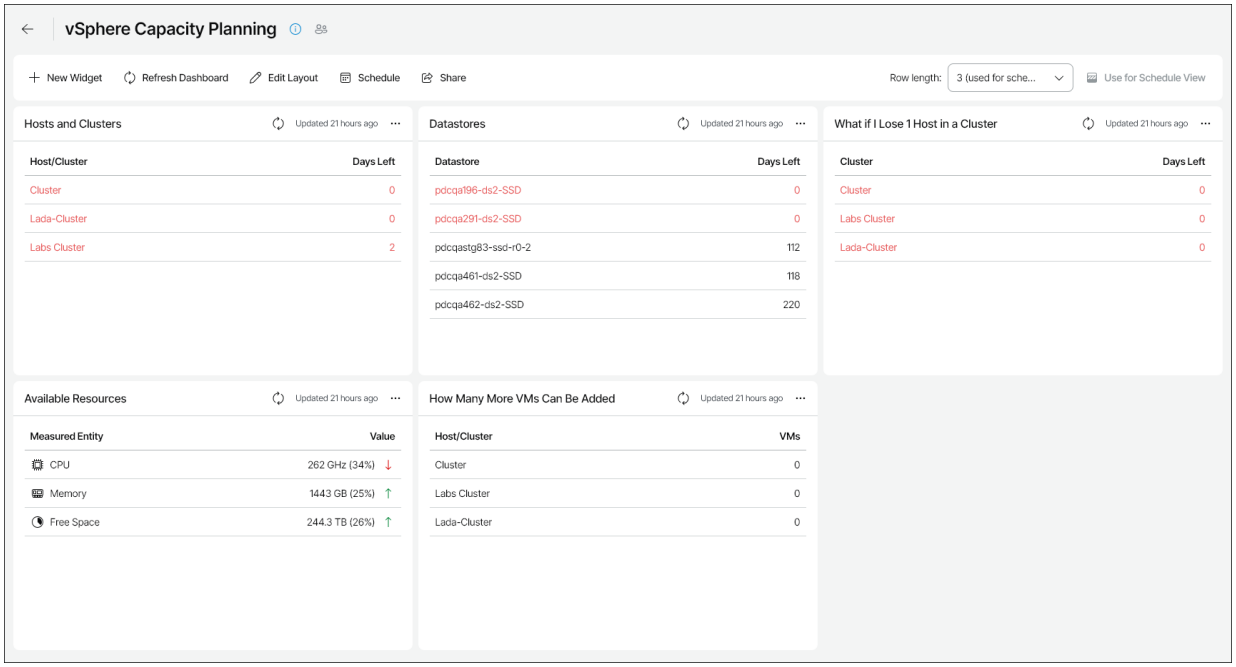
The widget tracks the amount of over-provisioned resources in your environment, based on data gathered by the Oversized VMs report:

- vCPU value shows the total number of provisioned vCPUs.
- vCPU Wasted value shows the total number of over-provisioned vCPUs. Use this value as a measure of compute resources that you can reclaim and allocate to other VMs.
- Allocated Memory value shows the total amount of provisioned virtual memory.
- Memory Wasted value shows the amount of over-provisioned virtual memory. Use this value as a measure of compute resources that you can reclaim and allocate to other VMs.

vSphere Capacity Planning

The **vSphere Capacity Planning** dashboard helps you analyze performance of virtual infrastructure objects, forecast resource shortages, optimize resource provisioning and maintain high availability for VMware clusters.

You can access the **vSphere Capacity Planning** dashboard from the **Dashboard** tab in Veeam ONE Web Client.



Widgets Included

To estimate future resource utilization and forecast resource shortages, the dashboard analyzes historical performance data for the previous 90 days and calculates the performance utilization trend.

Hosts and Clusters

The widget forecasts how many days remain before hosts and clusters start experiencing resource shortages, given the performance utilization trend. The widget analyzes CPU, memory, storage space and storage I/O performance data.

The days left value is highlighted with red if the number of remaining days is less than 30. The infinity sign implies that a host or a cluster will not run out of CPU and memory resources in the foreseeable future.

Datastores

The widget forecasts how many days remain before datastores will run out of free space, given the performance utilization trend.

The days left value is highlighted with red if the number of remaining days is less than 30. The infinity sign implies that a datastore will not run out of free space in the foreseeable future.

What if I Lose 1 Host in a Cluster

A host may unexpectedly go down or enter a maintenance mode, which will increase workloads across failover hosts in a cluster. The widget simulates a failure of one host in a HA cluster and forecasts how many days remain before the cluster starts experiencing resource shortages.

The days left value is highlighted with red if the number of remaining days is less than 30. The infinity sign implies that a cluster will not run out of CPU and memory resources in the foreseeable future.

Available Resources

The widget shows the amount of available CPU, memory and storage resources for the previous week.

The number in parentheses represents available resources as a percentage of total physical resources.

Arrows on the right show whether the amount of CPU, memory and free space has changed since the previous day. For example, a green arrow pointing up next to the Free Space value means that the available storage space has increased since yesterday, while a red arrow pointing down next to the CPU value means that the amount of available CPU resources has decreased since yesterday.

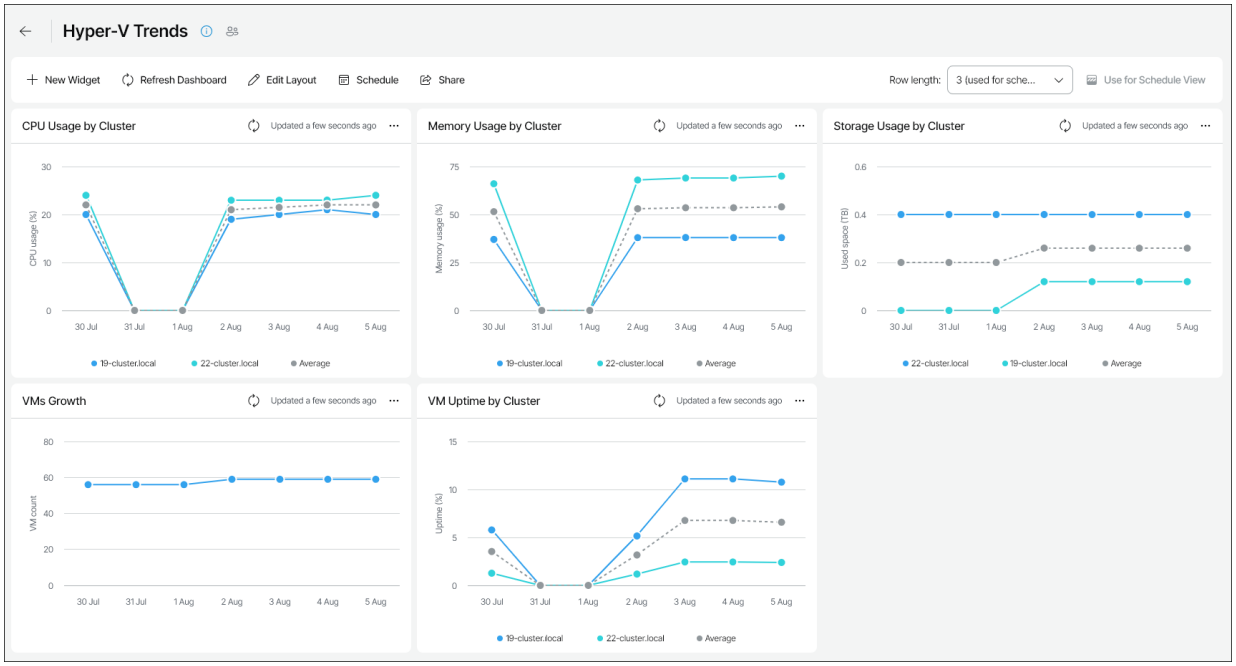
How Many More VMs Can Be Added

The widget analyzes the current workload, assesses average VM configuration in your clusters and hosts, and calculates the number of additional VMs with the average configuration that your existing infrastructure can support without experiencing significant resource shortages.

Hyper-V Trends

The **Hyper-V Trends** dashboard helps you track resource utilization in the Microsoft Hyper-V infrastructure by displaying growth trends for the previous week.

You can access the **Hyper-V Trends** dashboard from the **Dashboard** tab in Veeam ONE Web Client.



Widgets Included

CPU Usage by Cluster

This widget shows how CPU utilization in a cluster has been changing during the week.

Available Memory by Cluster

This widget shows how memory utilization in a cluster has been changing during the week.

Storage Usage by Cluster

This widget shows how storage utilization in a cluster has been changing during the week.

VMs Growth

This widget shows how the number of VMs in your virtual infrastructure has been changing during the week.

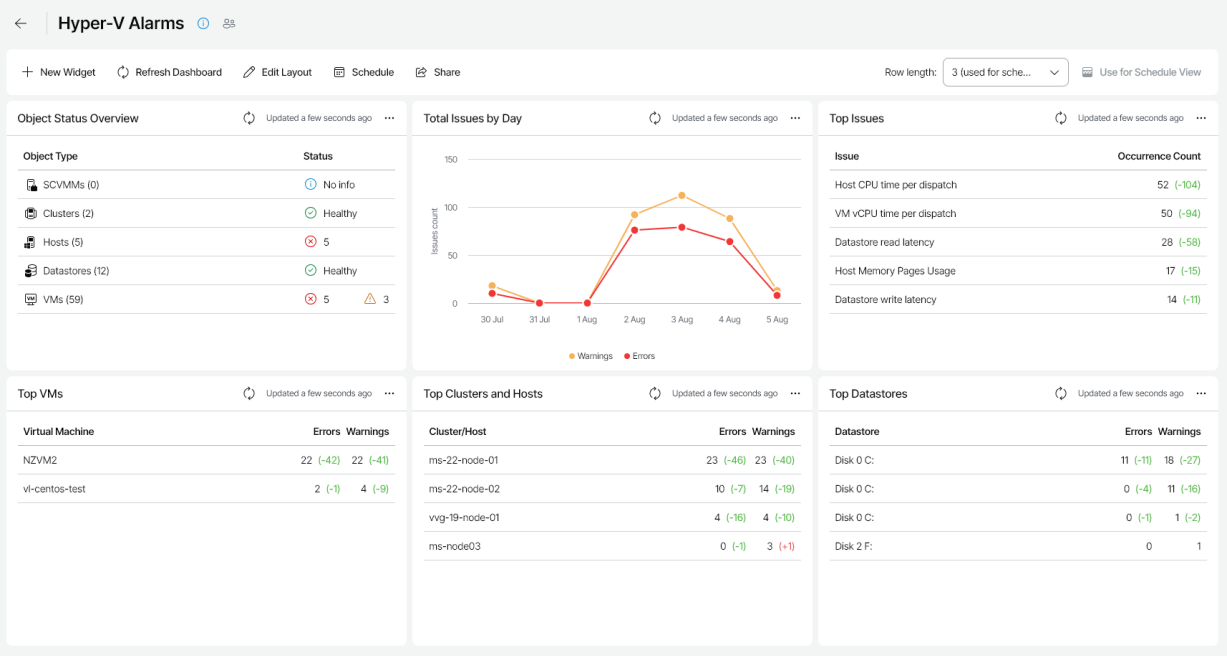
VM Uptime by Cluster

This widget shows how the average uptime value for VMs in a cluster has been changing during the week.

Hyper-V Alarms

The **Hyper-V Alarms** dashboard provides an overview of alarms triggered for Microsoft Hyper-V infrastructure objects by Veeam ONE Client during the past week. The dashboard allows you to identify the most typical issues that occur in your environment and to simplify troubleshooting.

You can access the **Hyper-V Alarms** dashboard from the **Dashboard** tab in Veeam ONE Web Client.



Widgets Included

Object Status Overview

This widget shows the number of healthy objects, objects with warnings and objects with errors for each infrastructure component type.

Total Issues by Day

This widget displays the daily number of warnings and errors that were triggered during the week.

Top Issues

This widget provides a list of 5 most typical alarms in your environment and shows the number of times each alarm was triggered.

Values in parentheses show how the alarm repeat count has changed over the previous week*.

Top VMs

This widget provides a list of VMs with the highest number of registered errors and warnings.

Values in parentheses show how the number of alarms has changed over the previous week*.

Top Clusters and Hosts

This widget provides a list of virtual infrastructure objects (clusters and hosts) with the highest number of registered errors and warnings.

Values in parentheses show how the number of alarms has changed over the previous week*.

Top Datastores

This widget provides a list of volumes and disks with the highest number of registered errors and warnings.

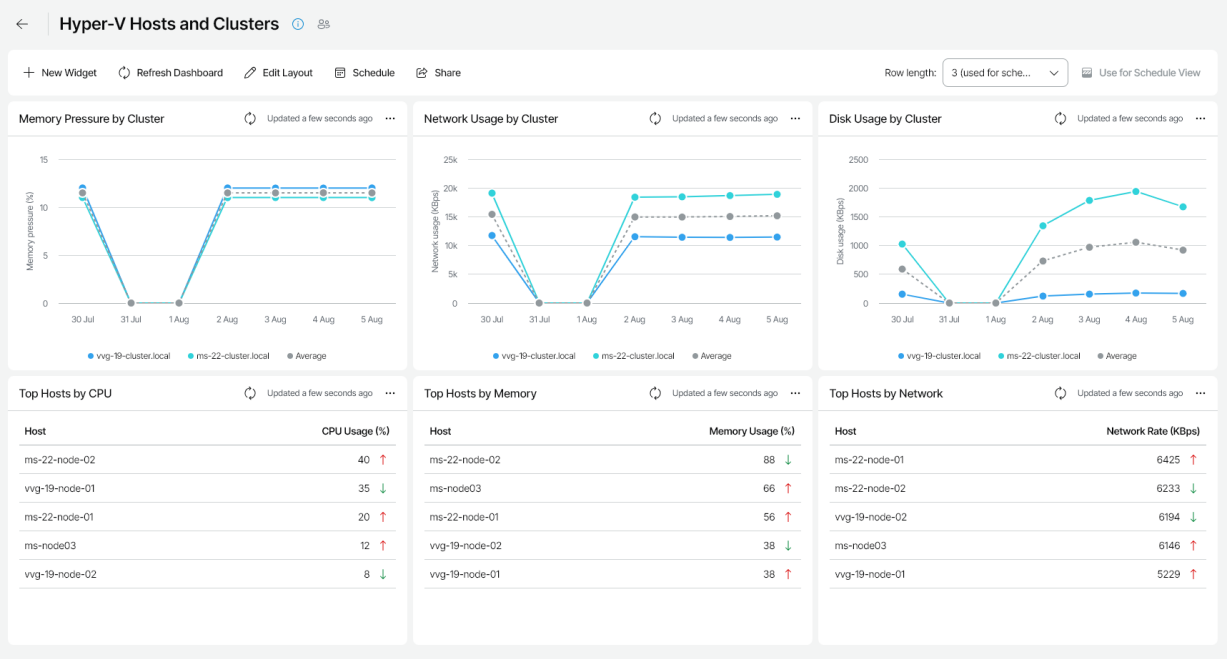
Values in parentheses show how the number of alarms has changed over the previous week*.

*The value in parentheses stands for the amount by which the number of alarms has changed compared to the value of the previous week. For example, the 11 (+5) value means that the number of alarms has increased by 5 over the past week (while the previous value equaled 6), and the 11(-7) value means that the number of alarms has decreased by 7 (while the previous value equaled 18).

Hyper-V Hosts and Clusters

The **Hyper-V Hosts and Clusters** dashboard helps you evaluate host and cluster performance in the Microsoft Hyper-V infrastructure. The dashboard displays statistics on CPU, memory, disk and network utilization, and helps you identify hosts and clusters with performance issues.

You can access the **Hyper-V Hosts and Clusters** dashboard from the **Dashboard** tab in Veeam ONE Web Client.



Widgets Included

Memory Pressure by Cluster

This widget shows how the average memory pressure for all VMs on all hosts in the cluster has been changing during the week.

Network Usage by Cluster

This widget shows how the average rate at which bytes are transferred to and from the cluster disk during I/O operations has been changing during the week.

Disk Usage by Cluster

This widget shows how the average rate at which data is read from and written to the cluster disk has been changing during the week.

Top Hosts by CPU

This widget displays weekly CPU utilization data for the top 5 most loaded hosts in your infrastructure.

Arrows on the right show whether the average CPU usage value has changed over the previous week*.

Top Hosts by Memory

This widget displays a list of hosts with the highest level of memory consumption.

Arrows on the right show whether the average memory usage value has changed over the previous week*.

Top Hosts by Network

This widget displays a list of hosts with the highest level of network usage.

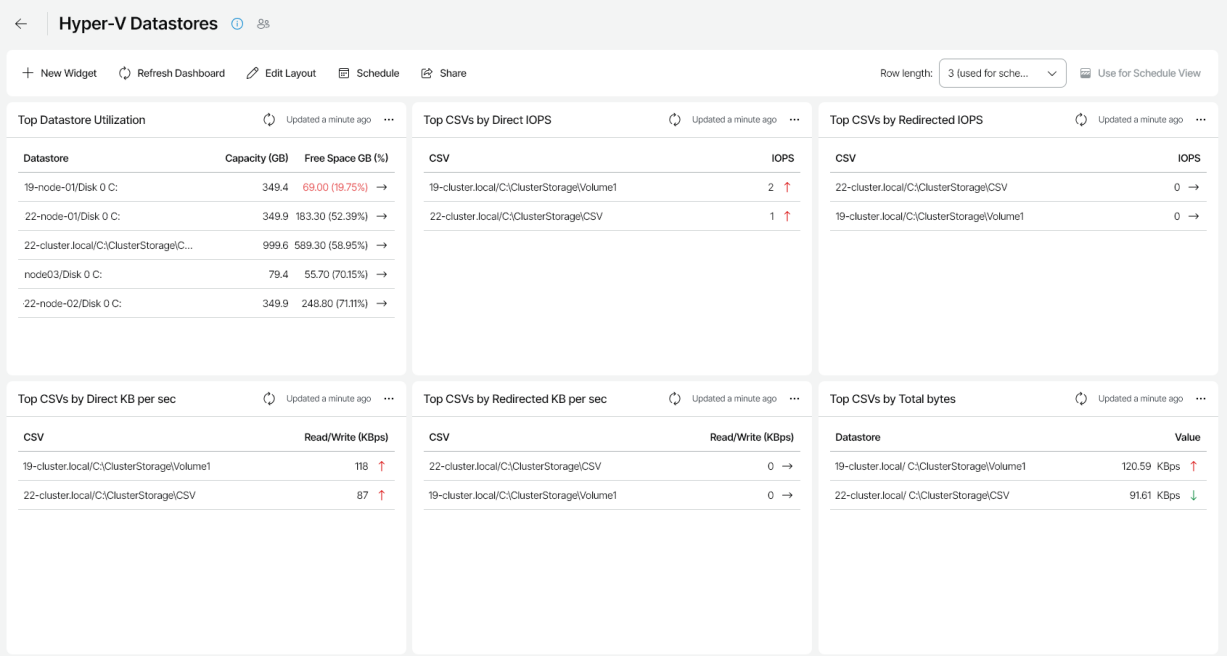
Arrows on the right show whether the average network throughput value has changed over the previous week*.

*The arrows allow you to compare the results of this week to the results of the previous week, and to track how the trend has evolved. For example, a grey arrow pointing right next to the CPU Usage value means that CPU utilization has not changed over the past week, a green arrow pointing down means that CPU utilization has decreased, while a red arrow pointing up means that CPU utilization has increased.

Hyper-V Datastores

The **Hyper-V Datastores** dashboard provides at-a-glance view on resource usage and performance of disks and Cluster Shared Volumes in the Microsoft Hyper-V environment. The dashboard helps you assess disk capacities and prevent potential performance bottlenecks.

You can access the **Hyper-V Datastores** dashboard from the **Dashboard** tab in Veeam ONE Web Client.



Widgets Included

Top Datastore Utilization

This widget displays a list of disks that will run out of free space sooner than other disks.

A datastore is highlighted with red if the amount of free space is less than 5% of the capacity value.

Values in parentheses show free space values for the previous week.

Top CSVs by Direct IOPS

This widget displays a list of Cluster Shared Volumes with the highest number of I/O operations performed in the direct access mode.

Arrows on the right show how the number of IOPS has changed over the previous week*.

Top CSVs by Redirected IOPS

This widget displays a list of Cluster Shared Volumes with the highest number of I/O operations performed in the redirected access mode.

Arrows on the right show how the number of IOPS has changed over the previous week*.

Top CSVs by Direct KB per Sec

This widget displays a list of Cluster Shared Volumes with the highest rate at which bytes were transferred to/from the CSV during write/read operations in the direct access mode.

Arrows on the right show how the *Direct Bytes/sec* metric value has changed over the previous week*.

Top CSVs by Redirected KB per Sec

This widget displays a list of Cluster Shared Volumes with the highest rate at which bytes were transferred to/from the CSV during write/read operations in the redirected access mode.

Arrows on the right show how the *Redirected Bytes/sec* metric value has changed over the previous week*.

Top CSVs by Total bytes

This widget displays a list of Cluster Shared Volumes with the highest rate at which data was read from and written to the volume in the direct and redirected access modes.

Arrows on the right show how the *Total Bytes/sec* metric value has changed over the previous week*.

Top CSVs by IOPS

This widget displays a list of Cluster Shared Volumes with the highest rate at which reads and writes were performed directly on the volume.

Arrows on the right show how the *IOPS* metric value has changed over the previous week*.

Top CSVs by Latency

This widget displays a list of Cluster Shared Volumes with the highest average latency for completing read and write requests on the volume.

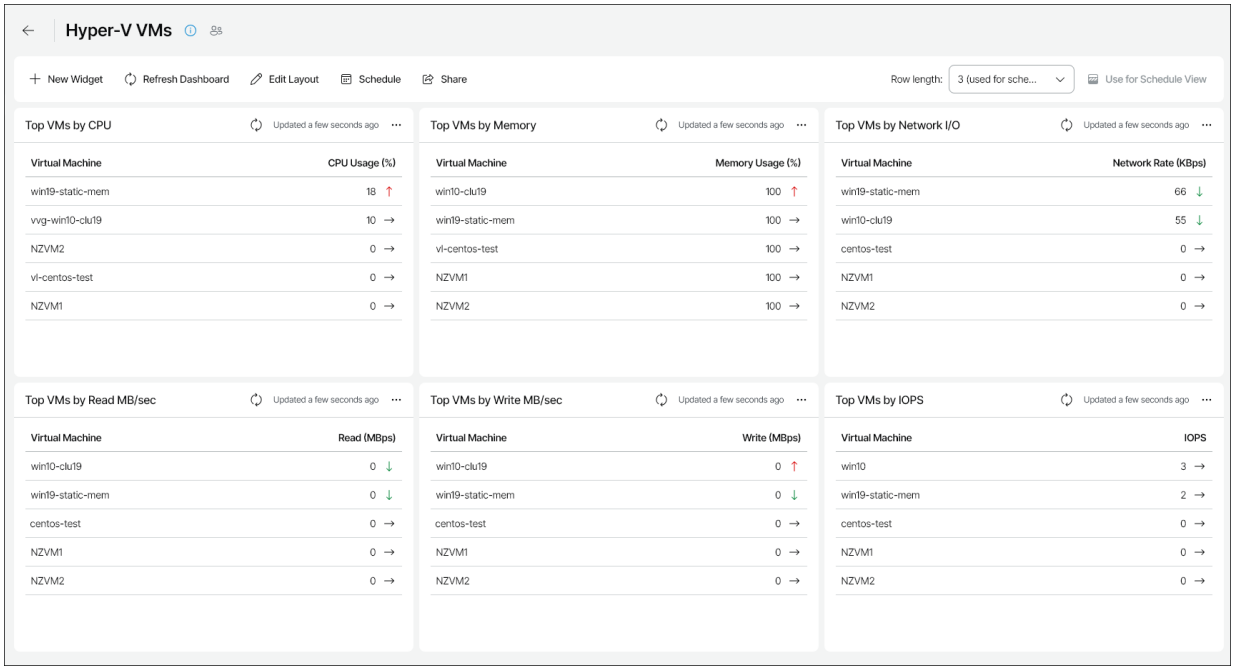
Arrows on the right show how the *Latency* metric value has changed over the previous week*.

*The arrow allows you to compare the results of the current week to the results of the previous week, and to track how the trend has evolved. For example, a grey arrow pointing right next to the IOPS value means that the average number of IOPS has not changed over the past week, a green arrow pointing down means that the average number of IOPS has decreased, while a red arrow pointing up means that the average number of IOPS has increased.

Hyper-V VMs

The **Hyper-V VMs** dashboard provides information about health and performance of VMs in the Microsoft Hyper-V infrastructure, and shows general VM statistics on CPU, memory and network usage for the past week.

You can access the **Hyper-V VMs** dashboard from the **Dashboard** tab in Veeam ONE Web Client.



Widgets Included

Top VMs by CPU

This widget displays a list of VMs with the highest average level of CPU utilization.

Arrows on the right show whether the CPU usage value has changed over the previous week*.

Top VMs by Memory

This widget displays a list of VMs with the highest average level of memory utilization. The memory utilization value is calculated as a percentage of total memory allocated for the VM.

Arrows on the right show whether the memory utilization value has changed over the previous week*.

Top VMs by Network I/O

This widget displays a list of VMs with the highest average network throughput values.

Arrows on the right show whether the throughput value has changed over the previous week*.

Top VMs by Read MB/sec

This widget displays a list of VMs with the highest average Read metric values.

Arrows on the right show whether the average read latency value has changed over the previous week*.

Top VMs by Write MB/sec

This widget displays a list of VMs with the highest average Write metric values.

Arrows on the right show whether the average write latency value has changed over the previous week*.

Top VMs by IOPs

This widget displays a list of VMs with the highest average number of IOPS.

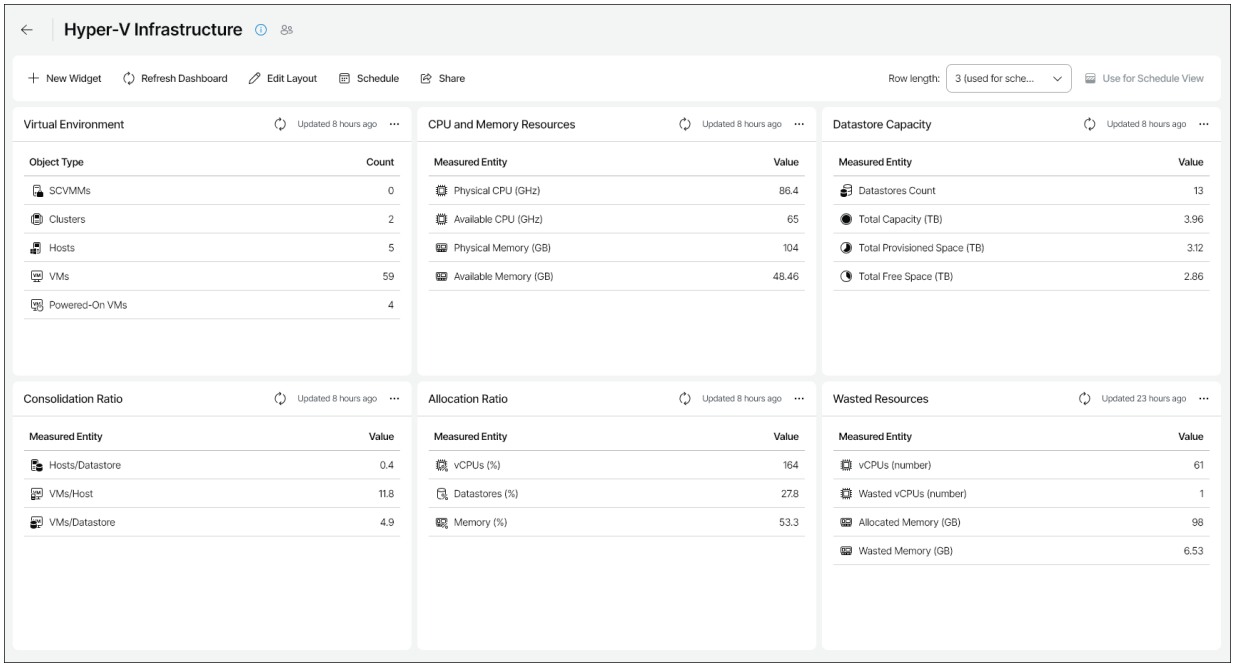
Arrows on the right show whether the number of IOPS has changed over the previous week*.

*The arrows allow you to compare the results of this week to the results of the previous week, and to track how the trend has evolved. For example, a grey arrow pointing right next to the CPU Usage value means that CPU utilization has not changed over the past week, a green arrow pointing down means that CPU utilization has decreased, while a red arrow pointing up means that CPU utilization has increased.

Hyper-V Infrastructure

The **Hyper-V Infrastructure** dashboard provides at-a-glance view of configuration of the Microsoft Hyper-V infrastructure and helps you assess the overall performance and resource usage efficiency.

You can access the **Hyper-V Infrastructure** dashboard from the **Dashboard** tab in Veeam ONE Web Client.



Widgets Included

Virtual Environment

This widget shows the total number of SCVMM servers, clusters, Hyper-V hosts and VMs in your environment, as well as the number of currently running VMs.

CPU and Memory Resources

This widget assesses physical compute resources deployed across Hyper-V hosts and shows the amount of available resources.

Datastores Capacity

This widget provides information on the number of volumes in the virtual environment, their total capacity, the amount of provisioned and free space left.

Consolidation Ratio

The widget tracks the amount of virtual hardware placed on physical hardware:

- Hosts/Datastore ratio shows the average number of hosts connected to a single volume.
- VMs/Host ratio shows the average number of VMs running on a single physical host.
- VMs/Datastore ratio shows the average number of VMs that store data on a single volume.

Allocation Ratio

The widget tracks the amount of resources allocated to VMs (allocated resources against physical resources, in percent):

- vCPU allocation ration shows the amount of CPU resources allocated to VMs.
- Datastores allocation ratio shows the amount of volume space allocated to VMs.
- Memory allocation ratio shows the amount of RAM allocated to VMs.

Wasted Resources

The widget tracks the amount of available and wasted resources:

- vCPU value shows the number of vCPUs configured for VMs.
- vCPU Wasted value shows the number of vCPUs that can be reclaimed from oversized VMs.
- Allocated Memory shows the amount of memory allocated to VMs.
- Memory Wasted value shows the amount of memory that can be reclaimed from oversized VMs.

Reports

Veeam ONE reports analyze data collected from VMware vSphere, Microsoft Hyper-V, Veeam Backup & Replication and Veeam Backup for Microsoft 365 servers. Reports provide structured information to help you examine historical data for the managed backup infrastructure and virtual environment. You can view reports in the web browser, export them to various formats, or schedule automatic report delivery by email, to disk or a network share.

Veeam ONE Web Client includes a set of predefined reports that analyze the managed environment from various aspects. For detailed description of predefined reports, see Predefined Veeam ONE Reports.

In addition to predefined reports, you can create custom reports, and save these reports for future use. In custom reports, you can choose the necessary report parameters, such as the scope of the backup and virtual infrastructure, reporting period and so on.

Introduced in Veeam ONE version 13, reports for Veeam Backup & Replication and Veeam Backup for Microsoft 365 are generated using an enhanced reporting engine. This updated engine offers improved sorting, grouping, filtering, and layout customization that can be dynamically adjusted without modifying report parameters directly. All other report types continue to use the legacy reporting engine.

Viewing Reports

Veeam ONE Web Client reports are available in the **Report Catalog** section.

The **Report Catalog** contains a list of all available reports on Veeam ONE. The **Saved Reports** tab contains your saved reports.

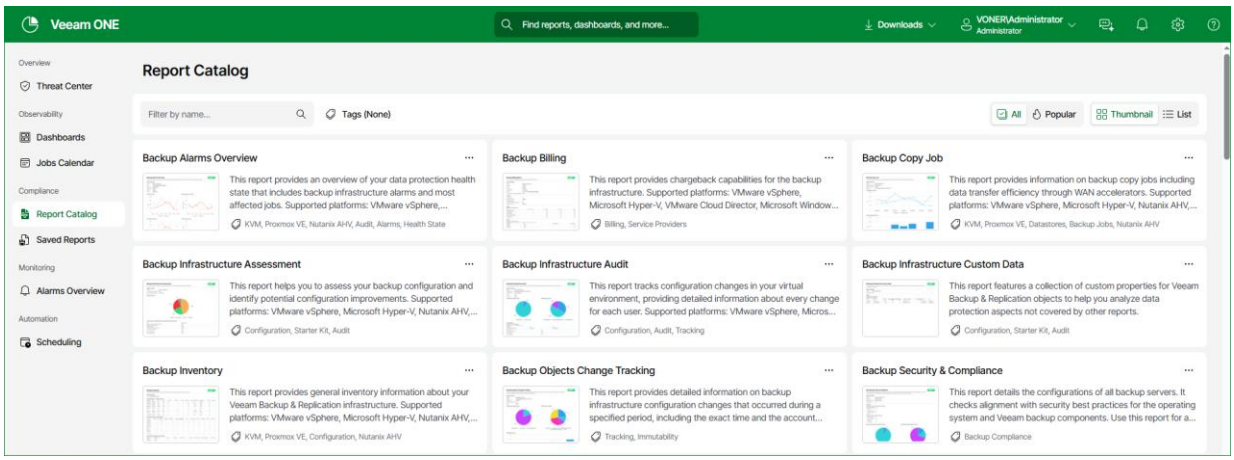
The *User reports* folder of the **Saved reports** tab contains reports created by users who have permissions assigned on objects in the vCenter Server or VMware Cloud Director inventory hierarchy. For details on, see Multi-Tenant Monitoring and Reporting.

> **NOTE:**
>
> Veeam ONE reports that use the legacy reporting engine are displayed in the browser pop-up windows. Before you create a report, make sure that pop-up windows are allowed from the Veeam ONE Web Client.

To create a report:

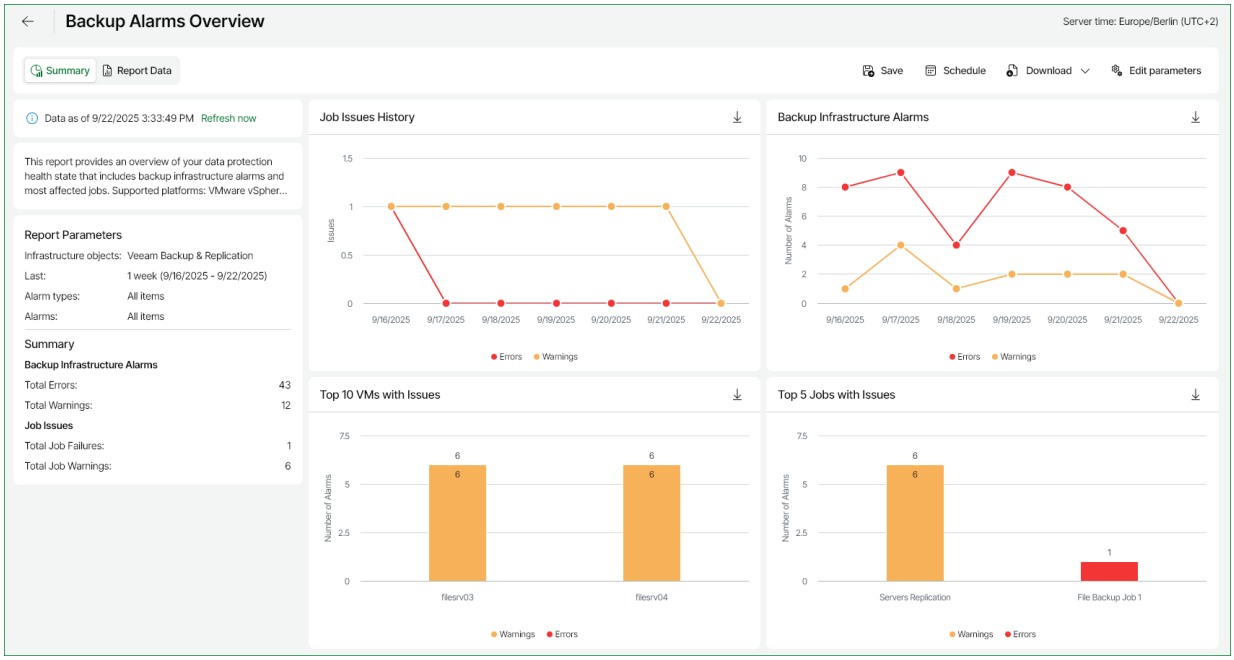
1. Open Veeam ONE Web Client.
2. Open the **Report Catalog** section.
3. In the main screen, select the necessary report. You can also search for any particular report by adding a keyword into the *Filter by name* field.
4. In the displayed list of reports, click the necessary report.
5. Specify report parameters, such as the virtual or backup infrastructure scope, reporting period and so on.
6. At the bottom of the report parameters, click the **Preview** button.

   The report will open in a pop-up browser window.
7. (Optional) Click the **Popular** tab to display the most popular reports selected on your system.
8. (Optional) Click **Tags** to open a list report name tags to further filter your search.



Navigating Reports

Veeam ONE reports vary depending on the type and input parameters. They can be short or span to several pages. Report data can be presented as graphs, charts, tables or text entries.



The navigation menu at the top of a report allows you to navigate the report and can include the following controls:

For reports supported by Veeam ONE version 13's new reporting engine (Veeam Backup & Replication and Veeam Backup for Microsoft 365 reports):

- Summary button — shows a summary of the report's details and associated charts and tables.
- Report Data button — shows additional tables and details of the report for further analysis.
- Filters — creates and applies logic filters to refine report displays.
- Save button — opens the **Save Report** window.
- Schedule button — opens the **Add Report Schedule** window.
- Download button — downloads the report in CSV or PDF format.
- Edit parameters button — opens the **Report Settings** panel to alter your report settings.
- Export chart button — downloads individual report charts in PNG, SVG, JPEG or CSV formats.
- Columns in the **Report Data** display allow you to:
  - Drag columns to resize.
  - Click **Auto-size all** to automatically organize columns.
  - Click **Group by** to select displayed columns.
  - Click **Columns** to in include or filter out columns.

For reports supported by Veeam ONE legacy reporting engine:

- Left/right arrow buttons — switch between the report pages.
- Fast forward/fast backward buttons — go to the last/first page of the report.
- Refresh button — update the report content with the latest collected data.
- Back button — return to the parent report from a drill-down report.
- Export menu (diskette icon) — save your report in one of the following file formats: Excel, Word or PDF.
- Go to page field — enter the necessary page number and press **Enter** on your keyboard to go to a specific page of the report.
- Zoom level field — zoom the report in/out.
- Print button — print the report.
- Search box — search for specific text within the report.

  If Veeam ONE Web Client is integrated with the Microsoft SQL Reporting Services server, the following additional report formats are available: CSV (comma delimited), XML, MS PowerPoint, TIFF, MHTML, Data Feed.

Date and Time Format in Reports

Most Veeam ONE reports include date and time details. The format of date and time in reports depends on the browser you use to work with Veeam ONE Web Client.

If you use Chrome, Firefox or Edge the date and time format will be determined by language preferences (locale) set in the browser.

To change the date and time format for those browsers, you must modify the language preferences in browser settings. To learn how to change the language in Chrome, see Change Chrome browser language settings. To learn how to change the language in Firefox, see Settings for web content, pop-ups, fonts, and languages. To learn how to change the language in Edge, see Use Microsoft Edge in another language.

Saving Reports

You can create reports with custom parameters and save them for future use:

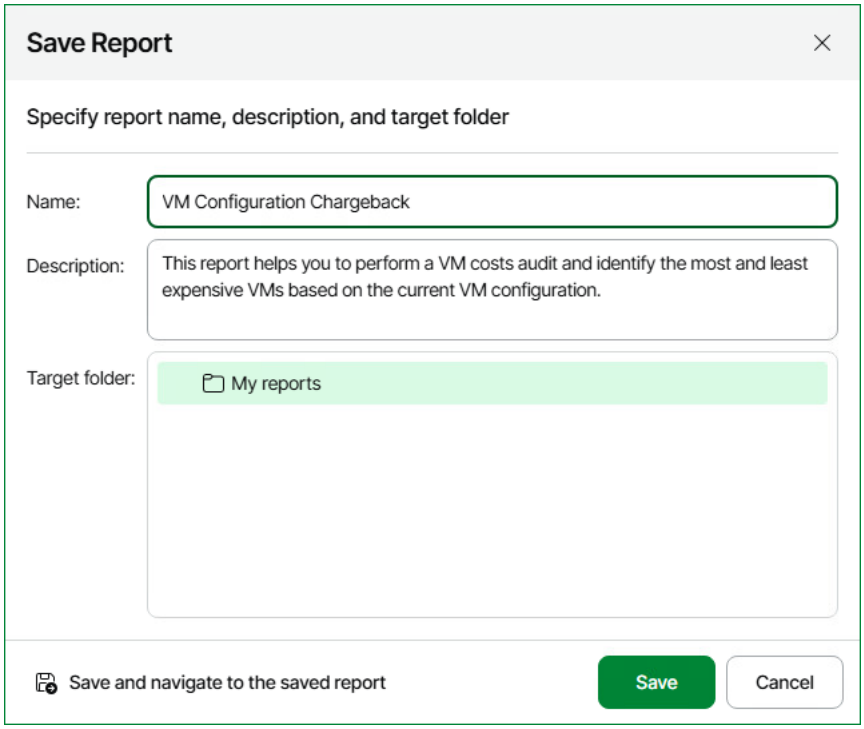
1. Open Veeam ONE Web Client.
2. Open the **Report Catalog** section.
3. In the displayed list of reports, click the necessary report.
4. Specify the report parameters, such as the virtual or backup infrastructure scope, reporting period and so on.
5. At the bottom of the report parameters, click **Save to**.
6. In the **Save Report** window, specify the report name and description and select a folder to which you want to place the report.

   You can only select the *My reports* folder or another folder that you have previously created. You cannot save reports to folders that include predefined reports. For details on working with folders, see Organizing Reports.
7. Click **Save**.

   If you want to open the report after saving, click **Save and navigate to the saved report**.

NOTE:

A saved report can become unavailable if you change the Veeam ONE license.



Modifying Reports

You can modify the name, description and parameters of reports that you have previously saved to *My Reports*.

> **NOTE**
>
> Report scopes saved from Veeam Backup & Replication servers cannot be changed. For details, see Veeam Backup & Replication Web UI and Configuring Analytics View.

Modifying Report Name and Description

To modify the name of a saved report:

1. Open Veeam ONE Web Client.
2. Open the **Saved Reports** tab.
3. In the displayed list of reports, click a saved report whose name and description you want to modify.
4. At the top of the report parameters, click **Report Actions** and select **Edit Information**.

   Alternatively, you can right-click the necessary report and select **Edit Information** in the context menu.
5. In the **Edit Report Information** window, modify report name and description.
6. Click **Save**.

Changing Report Parameters

To change parameters of a saved report:

1. Open Veeam ONE Web Client.
2. Open the **Saved Reports** tab.
3. In the displayed list of reports, click a saved report whose parameters you want to modify.
4. Change the report parameters.
5. At the top of the report parameters, click **Save**.

Organizing Reports

You can organize your reports with the help of report folders. Similar to file system folders, Veeam ONE Web Client folders are used to group reports in a way that is convenient for you. Veeam ONE Power Users and Administrators have a common root *My reports* folder. Reports saved by limited scope users appear to Veeam ONE Power Users and Administrators in a separate folder named after the limited scope username. For details on user roles, see Permissions and Security Groups and Multi-Tenant Monitoring and Reporting.

In Veeam ONE 13 or later, all reports saved from the reports node in Veeam Backup & Replication 13 or later appear in Veeam ONE in a separate folder under the name of the Veeam Backup & Replication server. For details on Veeam Backup & Replication, see Veeam Backup & Replication Web UI and Configuring Analytics View.

In addition to grouping reports, folders allow you to perform operations over a group of reports at once. For example, if you want to schedule automatic report delivery for a set of reports, you can place the necessary reports to the same folder and then specify delivery settings for the whole folder.

You can create custom folders under *My reports* folder of the **Saved Reports** tab.

Creating Folders

To create a new folder:

1. Open Veeam ONE Web Client.
2. Open the **Saved Reports** tab.
3. In the reports screen, select *My reports*.

   You can also choose any folder that you have previously created under the *My reports* node.
4. At the top right of the hierarchy, click the **Settings** button and choose **New folder**.

   Alternatively, you can right-click the necessary folder name and select **New Folder** in the context menu.
5. In the **New Folder** window, specify the name of a new folder and click **Create**.

The new folder will be added to the *My reports* hierarchy.

Renaming Folders

To change a folder name:

1. Open Veeam ONE Web Client.
2. Open the **Saved Reports** tab.
3. In the report screen, under *My reports*, select the necessary folder.
4. At the top right of the hierarchy, click **Settings** button and choose **Rename**.

   Alternatively, you can right-click the necessary folder name and select **Rename** in the context menu.
5. In the **Rename Folder** window, specify a new folder name and click **Rename**.

Deleting Folders

If you no longer need a folder, you can delete it. When you delete a folder with content, such as reports and subfolders, you can move child items to another folder during the deletion procedure.

To delete a folder:

1. Open Veeam ONE Web Client.
2. Open the **Saved Reports** tab.
3. In the reports screen, under *My reports*, select the necessary folder.
4. At the top right of the hierarchy, click **Settings** button and choose **Delete**.

   Alternatively, you can right-click the necessary folder name and select **Delete** in the context menu.
5. If the folder you delete contains reports or subfolders, you can choose to move the folder content to another folder. To do so, select the **Delete folder and move contained reports to the following folder** option and choose the new destination folder from the list. If you want to delete the folder with its content, select the **Delete folder and all contained reports** option.
6. Click **Delete**.

Moving Reports

You can move saved reports from one folder to another folder in *My Reports*.

To move a saved report:

1. Open Veeam ONE Web Client.
2. Open the **Saved Reports** tab.
3. In the report screen, under *My reports*, select the necessary folder.
4. In the displayed list of reports, click a saved report that you want to move.
5. At the top right of the report parameters, click **Settings** button and choose **Move**.

   Alternatively, you can right-click the necessary report name and select **Move** in the context menu.
6. In the **Move Report** window, choose a new target folder for the report.
7. Click **Move**.

Scheduling Reports

You can schedule automatic report delivery for one report or for a number of reports included in a report folder. You can choose to receive reports by email, save reports to a disk or network share. Note that you can only schedule delivery for saved reports (that is, reports in the *My reports* folder and its subfolders).

To schedule automatic report delivery:

1. Open Veeam ONE Web Client.
2. Open the **Report Catalog** section.
3. In the displayed list of reports, click a report for which you want to enable scheduled delivery.
4. At the bottom of the report parameters, click **Schedule**.

   Veeam ONE Web Client will launch the **Add Report Schedule** wizard.
5. At the **General** step of the wizard, specify the report name and description and select a folder to which you want to place the report.
6. Configure report delivery schedule as described in section Scheduling.
7. Click **Close**.

Scheduling Saved Reports

To schedule automatic report delivery for saved reports:

1. Open Veeam ONE Web Client.
2. Open the **Saved Reports** tab.
3. In the reports screen, select the necessary folder.
4. In the displayed list of reports, click a report for which you want to enable scheduled delivery.
5. At the bottom of the report parameters, click **Schedule**.

   Alternatively, you can right-click the necessary report and select **Schedule** in the context menu.
6. In the **Report Scheduling Settings** window, click **Add**.

   Veeam ONE Web Client will launch the **Add Schedule** wizard.
7. Configure report delivery schedule as described in section Scheduling.
8. Click **Close**.

Scheduling Delivery for Multiple Reports

Instead of scheduling automatic report delivery for separate reports, you can configure scheduled delivery for a number of reports that are included in the same folder.

To schedule delivery for reports in the same folder:

1. Open Veeam ONE Web Client.
2. Open the **Saved Reports** tab.
3. In the report screen, select a folder for which you want to schedule delivery.
4. At the top right of the hierarchy, click **Settings** and choose **Schedule**.

   Alternatively, you can right-click the necessary folder and select **Schedule** in the context menu.
5. In the **Report Folder Scheduling Settings** window, click **Add**.

   Veeam ONE Web Client will launch the **Add Schedule** wizard.
6. Configure the schedule and delivery method as described in section Scheduling.
7. Click **Close**.

Managing Report Schedules

You can create multiple schedules for a report or a report folder. Maintaining multiple schedules allows you to set up complex scheduling and delivery method settings for the same report or folder.

To manage report or folder schedules:

1. Open Veeam ONE Web Client.
2. Open the **Saved Reports** tab.
3. In the report screen, select the necessary folder or click a saved report in the displayed list of reports.
4. Do one of following:
   - At the bottom of the report parameters, click **Schedule**.
   - To the right of the report hierarchy, click **Settings** and select **Schedule**.
   - Right-click the necessary folder and select **Schedule** in the context menu.

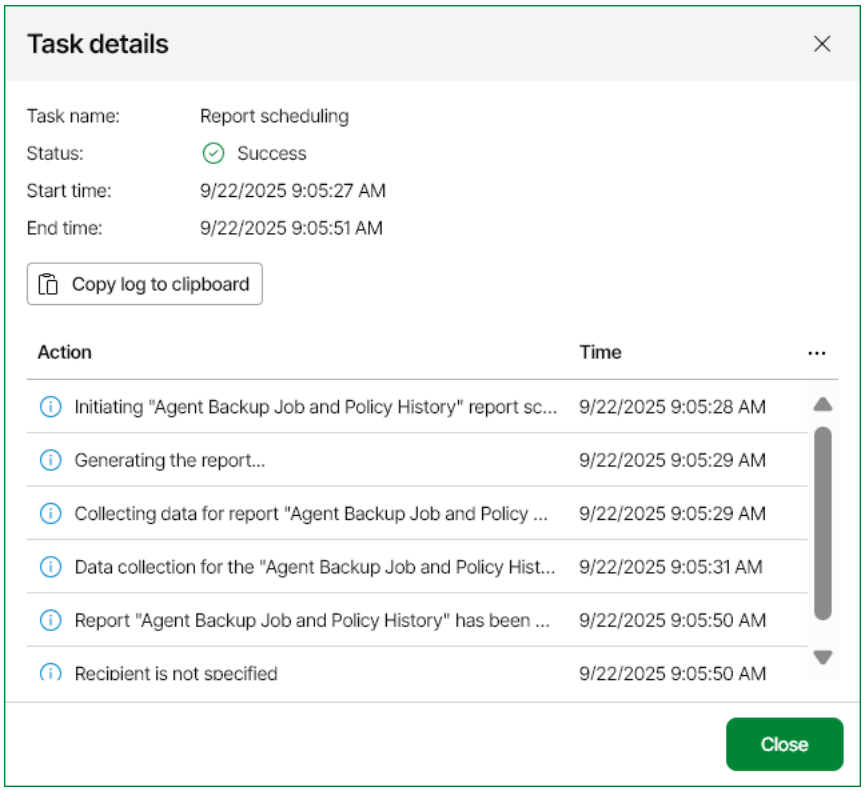
   The **Report Scheduling Settings** or **Report Folder Scheduling Settings** window will open.
5. Do one of the following:
   - To create a new schedule, click **Add**.
   - To modify scheduling settings, select a schedule in the list and click **Edit**.
   - To delete a schedule from the list, select the schedule in the list and click **Delete**.
   - To temporarily disable a schedule, select the schedule in the list and click **Disable**.
   - To enable a previously disabled schedule, select the schedule in the list and click **Enable**.
6. To finish working with the schedules, click **Close**.

Viewing Scheduled Report Delivery Results

Every run of a report or report folder scheduling job initiates a new scheduling session.

To view details on report or report folder scheduling sessions:

1. Open Veeam ONE Web Client.
2. At the top right corner of the Veeam ONE Web Client window, click **Configuration**.
3. In the configuration menu on the left, click **Data Collection**.
4. In the **Data Collection** screen click **Task Sessions**.
5. To display all report or report folder delivery sessions, click **Filter**, select *Report scheduling* or *Report folder scheduling* and click **Apply**.
6. Click the session in the list to display detailed information on it.



Cloning Reports

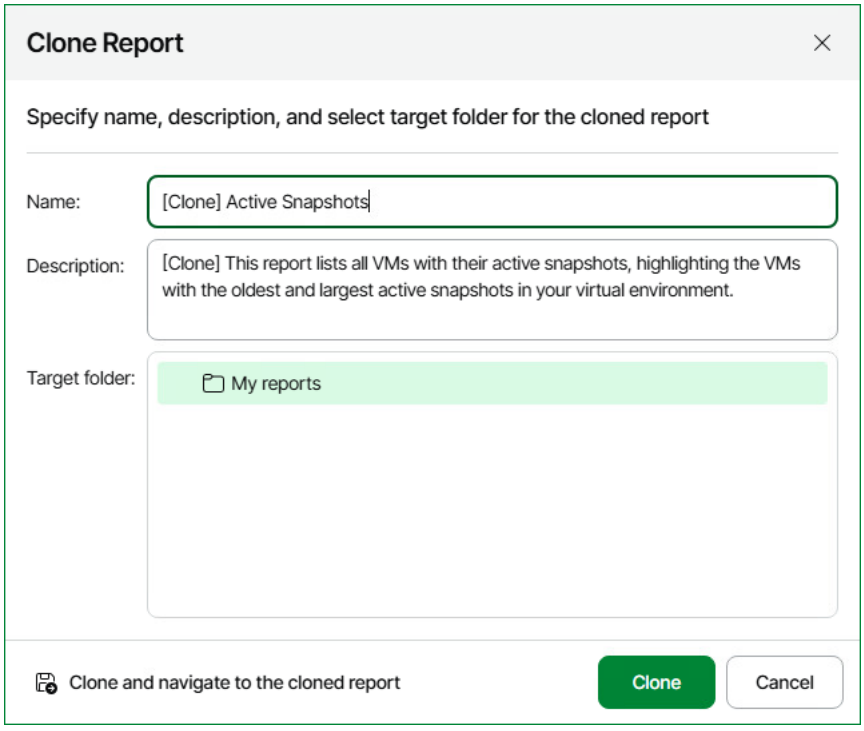
You can create clones of reports that you have previously saved to *My reports*.

Cloning may save time if you need to create multiple instances of the same report. For example, you have configured a report with complex parameters and need create a set of similar reports with minor changes. In this situation, you can create several clones of the saved report and change report parameters for each report clone.

To create a report copy:

1. Open Veeam ONE Web Client.
2. Open the **Saved Reports** tab.
3. In the displayed list of reports, right click a saved report that you want to clone and select **Clone** in the context menu.
4. In the **Clone Report** window, specify the name of the report, its description and select a folder to which the report clone should be saved. You can only choose a folder in the *My reports* hierarchy.
5. Click **Clone**.

After you create a report clone, modify the report parameters as described in Modifying Reports.



Deleting Reports

If you no longer need a report, you can delete it. Note that you can only delete reports that you have previously saved to *My Reports*.

To delete a report:

1. Open Veeam ONE Web Client.
2. Open the **Saved Reports** tab.
3. In the hierarchy on the left, select the necessary report.
4. In the displayed list of reports, click a saved report that you want to delete.
5. At the top of the report parameters, right-click the necessary report and select **Delete** in the context menu.
6. In the displayed dialog box, click **Delete** to confirm report deletion.

Sharing Reports

To share a saved report with other users or integrate the report to a web portal, you can enable public access to the report or generate a direct report link.

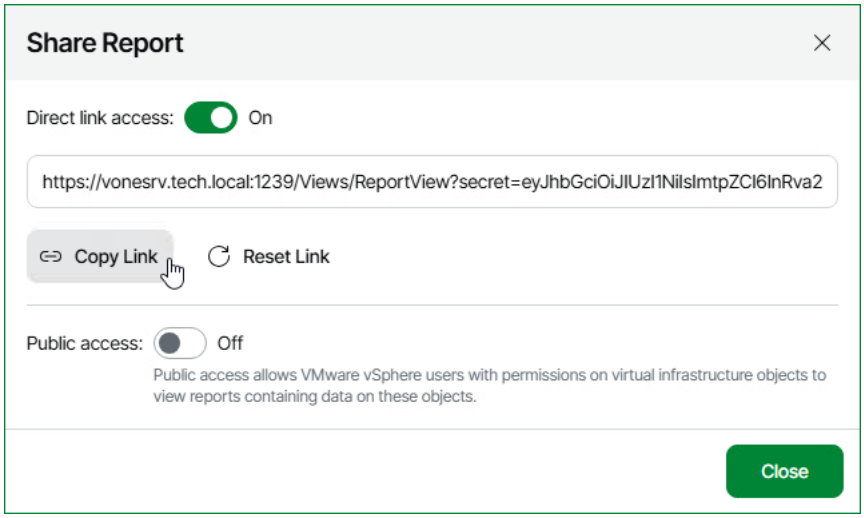
Before you share a report with other users, make sure that you have saved the report to *My Reports*. For details, see Saving Reports.

Generating Direct Report Link

To share a report with other users, or integrate a report to a web portal, you can generate a direct report link:

1. Open Veeam ONE Web Client.
2. Open the **Saved Reports** tab.
3. In the report screen, select the necessary report.
4. In the displayed list of reports, click a saved report for which you want to generate a direct link.
5. At the top of the report parameters, right-click the necessary report and select **Share** in the context menu.
6. In the **Share Report** window, switch the **Direct link access** toggle to *On*.
7. Click **Copy Link** to copy the link and use it to share with other users or integrate to web portals.
8. If you need to generate a new direct link, click **Reset Link**.

   Note that after you change the direct link, the previous link will become invalid.
9. Click **Close**.



Enabling Public Access

To share a report with other users, you must enable public access to this report. Veeam ONE users, including VMware vSphere users who have permissions assigned on virtual infrastructure objects, can access published reports in the Veeam ONE Web Client.

To enable public access to a report:

1. Open Veeam ONE Web Client.

2. Open the **Saved Reports** tab.
3. In the displayed list of reports, click a saved report for which you want to enable public access.
4. At the top of the report parameters, right-click the necessary report and select **Share** in the context menu.
5. In the **Share Report** window, switch the **Public access** toggle to *On*.
6. Click **Close**.

Disabling Public Access

To make a published report inaccessible, you can disable public access to the report:

1. Open Veeam ONE Web Client.
2. Open the **Saved Reports** tab.
3. In the report screen, select the necessary folder.
4. In the displayed list of reports, click a saved report for which you want to disable public access.
5. At the top of the report parameters, right-click the necessary report and select **Share** in the context menu.
6. In the **Share Report** window, switch the **Public access** toggle to *Off*.
7. Click **Close**.

Exporting and Importing Reports

You can export saved reports to a JSON file and import reports from a JSON file. Exporting and importing can be useful if you need to back up custom-designed reports, or if you want to copy saved reports from one Veeam ONE deployment to another.

> **NOTE**
>
> Reports cannot be imported into folders with reports saved from Veeam Backup & Replication. For details, see Veeam Backup & Replication Web UI and Configuring Analytics View.

Exporting Reports

To export saved user report to a JSON file:

1. Open Veeam ONE Web Client.
2. Open the **Saved Reports** tab.
3. In the displayed list of reports, right-click a saved report which you want to export.
4. At the top of the report parameters, select **Export parameters** in the context menu.

The selected report will be exported to a JSON file and saved to the download location on your machine.

Exporting Report Folders

To export report folders to a JSON file:

1. Open Veeam ONE Web Client.
2. Open the **Saved Reports** tab.
3. In the report screen, under *My reports*, select the necessary folder or report.
4. At the top of the hierarchy, right-click the necessary folder and select **Export parameters** in the context menu.
5. In the displayed window, click **Close**.

The selected folder and all contained objects will be exported to a JSON file and saved to the download location on your machine.

Importing Reports

To import saved user reports from a JSON file:

1. Open Veeam ONE Web Client.
2. Open the **Saved Reports** tab.
3. In the report screen, select the necessary folder or report.
4. At the top of the hierarchy, right-click the necessary folder and select **Import parameters** in the context menu.
5. In the Windows **Open** dialog box, select the JSON file that describes saved user reports, and click **Open**.

6. In the displayed window, click **Close**.

Reports from the JSON file will be installed to the selected folder.

Predefined Veeam ONE Reports

Veeam ONE Web Client features a set of preconfigured reports for Veeam Backup & Replication, Veeam Backup for Microsoft 365, VMware vSphere and Microsoft Hyper-V.

> **NOTE:**
>
> Some predefined reports can represent incomplete data, contain Veeam watermark, or be unavailable due to licensing limitations.

Active Checkpoints

This report shows a list of all VMs with checkpoints, including the oldest and the largest checkpoints in the virtual environment.

- The **Top VMs by Active Checkpoint Size (GB)** and **Top VMs by Active Checkpoints Age (Weeks)** charts display top 5 VMs with the oldest and the largest checkpoints in the virtual environment.
- The **Details** table provides the list of VMs with checkpoints and shows checkpoint name, location, date and time when the checkpoint was created, checkpoint size and VM state.

Report Parameters

You can specify the following report parameters:

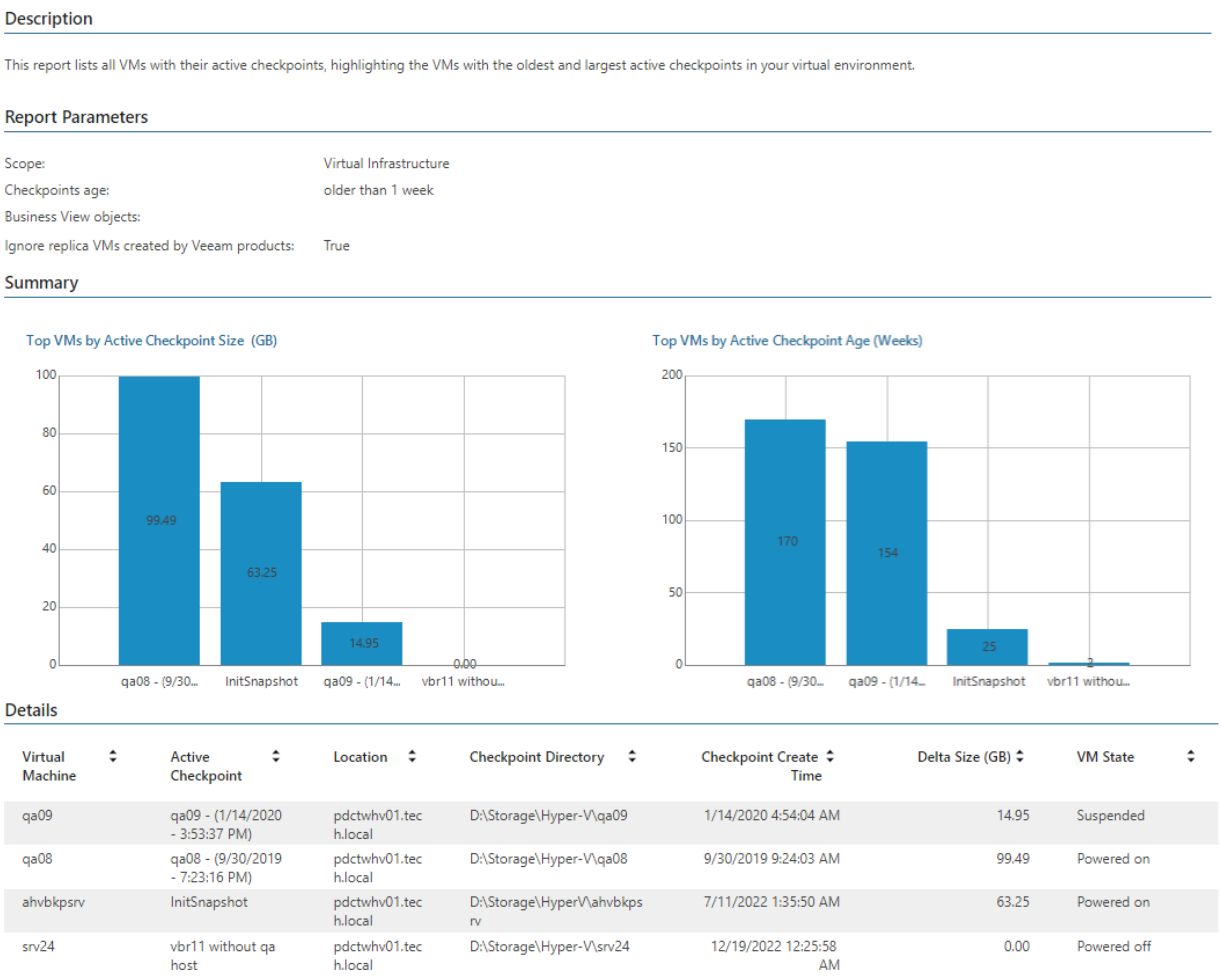
- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **Business View objects**: defines Business View groups to analyze in the report. The parameter options are limited to objects of the Virtual Machine type.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.
- **Checkpoint age, older than**: defines checkpoint age threshold. If a VM checkpoint is older than the specified age, the VM will be included in the report.

- **Ignore replica VMs created by Veeam products**: defines whether VM replicas created by Veeam Backup & Replication will be excluded from the report scope.

  Veeam Backup & Replication uses VM checkpoint as replica restore points. Such restore points may be large in size and remain on disk for a long period of time. If you have VM replicas created with Veeam Backup & Replication, select this check box to exclude VM replicas with checkpoint restore points from the report.

Active Checkpoints



Description

This report lists all VMs with their active checkpoints, highlighting the VMs with the oldest and largest active checkpoints in your virtual environment.

Report Parameters

Scope:	Virtual Infrastructure
Checkpoints age:	older than 1 week
Business View objects:	
Ignore replica VMs created by Veeam products:	True

Summary

Details

Virtual Machine	Active Checkpoint	Location	Checkpoint Directory	Checkpoint Create Time	Delta Size (GB)	VM State
qa09	qa09 - (1/14/2020 - 3:53:37 PM)	pdctwhv01.tech.local	D:\Storage\Hyper-V\qa09	1/14/2020 4:54:04 AM	14.95	Suspended
qa08	qa08 - (9/30/2019 - 7:23:16 PM)	pdctwhv01.tech.local	D:\Storage\Hyper-V\qa08	9/30/2019 9:24:03 AM	99.49	Powered on
ahvbkpsrv	InitSnapshot	pdctwhv01.tech.local	D:\Storage\HyperV\ahvbkpsrv	7/11/2022 1:35:50 AM	63.25	Powered on
srv24	vbr11 without qa host	pdctwhv01.tech.local	D:\Storage\Hyper-V\srv24	12/19/2022 12:25:58 AM	0.00	Powered off

Use Case

Orphaned checkpoints consume valuable storage resources. Best practices for checkpoints recommend that you delete checkpoints older than 3 days, since they no longer reflect recent VM changes.

The report helps you detect orphaned checkpoints and better address the problem of wasted storage space.

Active Snapshots

This report shows a list of all VMs with snapshots, including the oldest and the largest snapshots in the virtual environment.

- The **Top VMs by Active Snapshot Size (GB)** and **Top VMs by Active Snapshot Age (Weeks)** charts display top 5 VMs with the oldest and the largest snapshots in the virtual environment.
- The **Details** table provides the list of VMs with snapshots and shows snapshot name, its location, date and time when the snapshot was created, snapshot size and state of the VM.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **VMware Cloud Director objects**: defines VMware Cloud Director components to analyze in the report.
- **Business View objects**: defines Business View groups to analyze in the report. The parameter options are limited to objects of the Virtual Machine type.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.
- **Snapshot age, older than**: defines snapshot age threshold. If a VM snapshot is older than the specified age, the VM will be included in the report.
- **Ignore replica VMs created by Veeam products**: defines whether to include VM replicas created by Veeam Backup & Replication in the report.

  Veeam Backup & Replication uses VM snapshots as replica restore points. Such snapshot restore points may be large in size and remain on the datastore for a long period of time. If you have VM replicas created with Veeam Backup & Replication, select this check box to exclude VM replicas with snapshot restore points from the report.

> **NOTE:**
>
> If you run the Active Snapshots report with **Veeam backup data and large-scale virtual infrastructure performance monitoring** mode selected, the snapshot size data may be incorrect or absent. For more information on data collection modes, see Scalability and Choose Data Collection Mode.

View Report Example

Use Case

Outdated snapshots consume valuable storage resources. Best practices for snapshots recommend that you delete snapshots older than 3 days, since they no longer reflect recent VM changes.

The report helps you detect outdated snapshots and better address the problem of wasted storage space.

Agent Backup Job and Policy History

This report provides historical information for Veeam agent backup policies and job sessions results.

- The **Summary** display includes the following elements:
  - The **Top 5 Jobs and Policies by Restore Points Created** and **Top 5 Jobs and Policies by Backed up Data** charts display top 5 jobs and policies in terms of the greatest number of restore points and the largest amount of backed up data.
  - The **Agent Backup Jobs and Policies Result** chart shows the number of jobs and policies whose sessions completed successfully, the number of jobs and policies whose sessions completed with warnings and the number of jobs and policies whose sessions failed.
- The **Jobs and Policy - Overview** table provides information on each performed agent backup job: session date, number of backed up agents and created restore points, the completion state and total backup size.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a list of Veeam Backup & Replication servers to include in the report.
- **Backup jobs/policies**: defines a list of backup jobs and policies to include in the report.
- **Period**: defines the time period to analyze in the report.

View Report Example

Use Case

This report allows you to track historical statistics, amount of backed up data and created restore points for all agent backup jobs and policies.

Alarms Current State Overview (Hyper-V)

This report shows alarms triggered by Veeam ONE Client for the managed virtual infrastructure.

- The **Summary** section includes the following elements:
  - The **Total Issues Number** chart shows the number of triggered alarms.
  - The **Top 10 Alarms** table shows 10 most frequently triggered alarms.
- The **Details** section provides information on each triggered alarm, including affected object, location, alarm name, alarm type, trigger and date and time when the alarm was triggered.

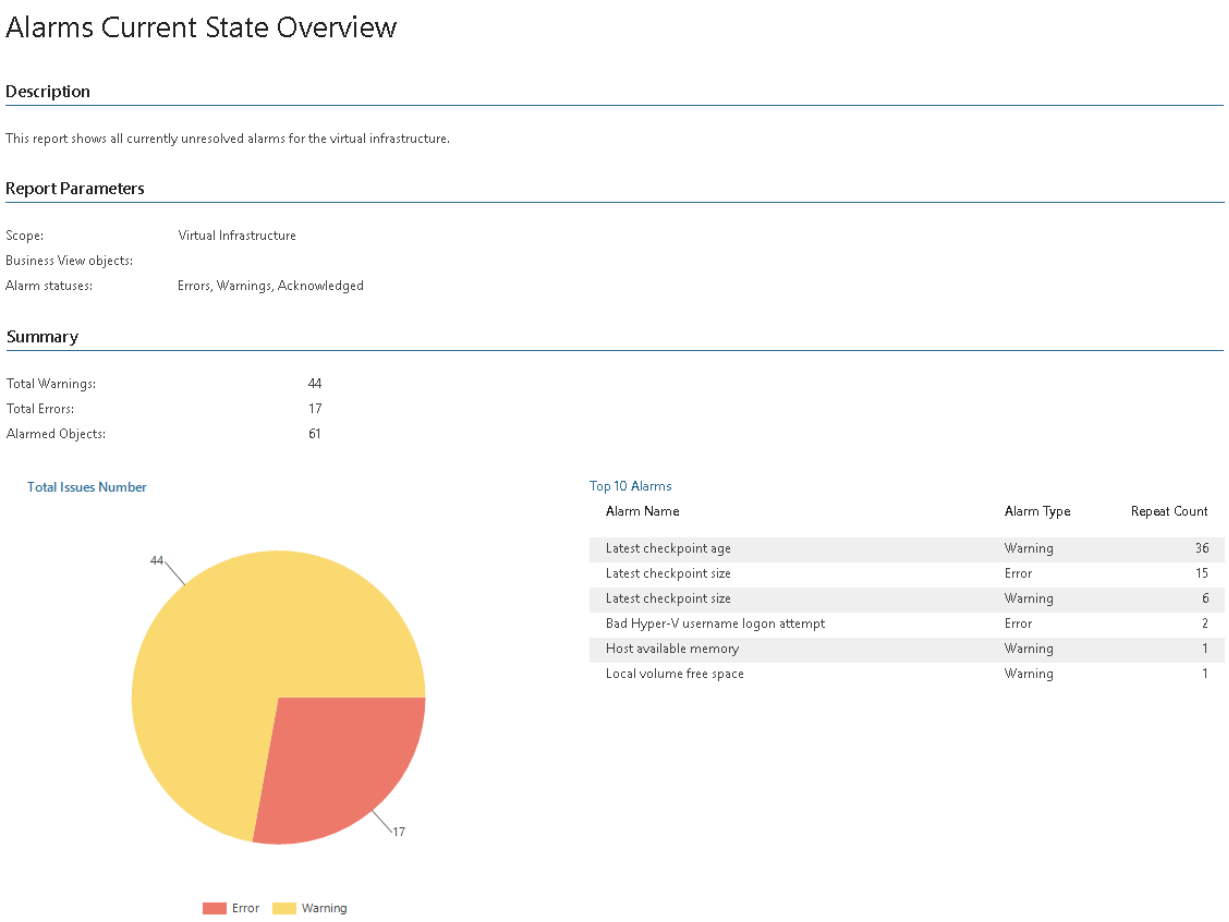
Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **Business View objects**: defines Business View groups to analyze in the report.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.

- **Alarm statuses**: defines the status of alarms that must be included in the report (*Error*; *Error and Warning*; *Error, Warning, Acknowledged*; *Acknowledged*).



Alarms Current State Overview

Description

This report shows all currently unresolved alarms for the virtual infrastructure.

Report Parameters

Scope:	Virtual Infrastructure
Business View objects:	
Alarm statuses:	Errors, Warnings, Acknowledged

Summary

Total Warnings:	44
Total Errors:	17
Alarmed Objects:	61

Total Issues Number

Top 10 Alarms

Alarm Name	Alarm Type	Repeat Count
Latest checkpoint age	Warning	36
Latest checkpoint size	Error	15
Latest checkpoint size	Warning	6
Bad Hyper-V username logon attempt	Error	2
Host available memory	Warning	1
Local volume free space	Warning	1

Details

Object	Location	Alarm Name	Type	Trigger	Time
Object Type: Host			3		
hyperv01	\Virtual Infrastructure\cluster01	Host available memory	Warning	"Hyper-V Services Memory Usage" (**80.0%**) is above a defined threshold (80.0%)	1/2/2019 8:59:27 PM
hyperv01	\Virtual Infrastructure\cluster01	Bad Hyper-V username logon attempt	Error	Fired by event: 4625 Microsoft-Windows-Security-Auditing Event description: An account failed to log on. Failure Reason: Unknown user name or bad password. Account Name: Administrator Account Domain: TECH Initiated by: n/a	12/29/2018 1:27:17 PM
hyperv02	\Virtual Infrastructure\cluster01	Bad Hyper-V username logon attempt	Error	Fired by event: 4625 Microsoft-Windows-Security-Auditing Event description: An account failed to log on. Failure Reason: Unknown user name or bad password. Account Name: mark.scissor Account Domain: TECH Initiated by: n/a	1/14/2019 1:47:25 PM
Object Type: Local storage			1		
Disk 1 F: G:	\Virtual Infrastructure\cluster01\hyperv01	Local volume free space	Warning	Amount of free space (**10.0%**) is below a defined threshold (10.0%). Current free space is **19.94 GB**.	12/29/2018 1:08:59 PM
Object Type: Virtual Machine			57		

Use Case

This report evaluates the health state of the managed infrastructure and helps you simplify troubleshooting. You can use the report to export details of triggered alarms.

Alarms Current State Overview (vSphere)

This report shows alarms triggered by Veeam ONE Client for the managed virtual infrastructure.

- The **Summary** section includes the following elements:
  - The **Total Issues Number** chart shows the number of triggered alarms.
  - The **Top 10 Alarms** table shows 10 most frequently triggered alarms.
- The **Details** section provides information on each triggered alarm, including affected object, object location, alarm name, alarm type, trigger and date and time when the alarm was triggered.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **Business View objects**: defines Business View groups to analyze in the report.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.
- **Alarm statuses**: defines the status of alarms that must be included in the report (*Errors and Warnings*; *Errors only*; *Errors, Warning, Acknowledged*; *Acknowledged only*).

View Report Example

Use Case

This report evaluates the health state of the managed infrastructure and helps you simplify troubleshooting. You can use the report to export details of triggered alarms.

Alarms Overview (Hyper-V)

Veeam ONE Client generates multiple alarms to inform you about important events in your environment. This report allows administrators to quickly review the health state of the environment and to track how the number of alarms has been changing during the reporting period.

- The **Summary** section includes the following elements:
  - The **Errors** and **Warnings** charts show top 5 objects that caused the greatest number of alarms.
  - The **Total Issues** chart shows alarm activity during the reporting period.
  - The **Top 10 Issues** table shows 10 most frequently triggered alarms.
- The **Details** section provides information on each affected object , including object type, location, object name, number of triggered alarms and alarm activity trend.

  Click a number in the **Alarms** column in the details table to drill down to details for alarms raised for the infrastructure object.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **Business View objects**: defines Business View groups to analyze in the report.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.
- **Period**: defines the time period to analyze in the report. Note that the reporting period must include at least one successfully completed *Object properties data collection* task for the selected scope. Otherwise, the report will contain no data.
- **Group by**: defines how data will be grouped in the report output (by *Issue type* or *Object type*).
- **Object types**: defines a list of virtual infrastructure object types to analyze in the report.

- **Alarms**: defines a list of alarms to analyze in the report.

  For details on alarms you can select in the list, see Microsoft Hyper-V Alarms.

Alarms Overview

Description

This report provides an overview of your virtual environment current health state that includes most common alarms and most affected VI objects.

Report Parameters

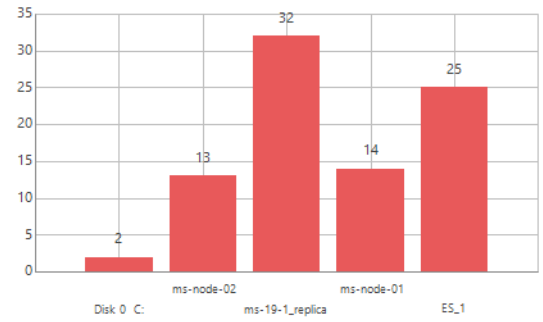
Scope:	Virtual Infrastructure
Reporting period:	1 week (12/23/2022 - 12/29/2022)
Group by:	Issue type
Business View objects:	
Object types:	All items
Alarms:	All items

Summary

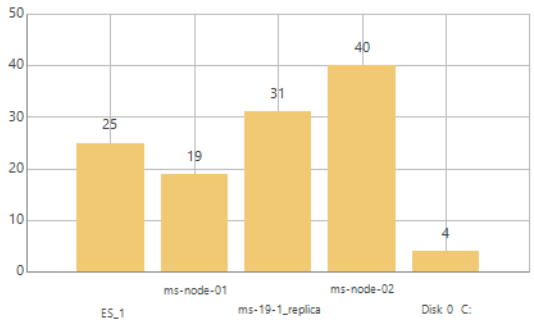
Total Errors:	90
Total Warnings:	122

Top Objects and Issues

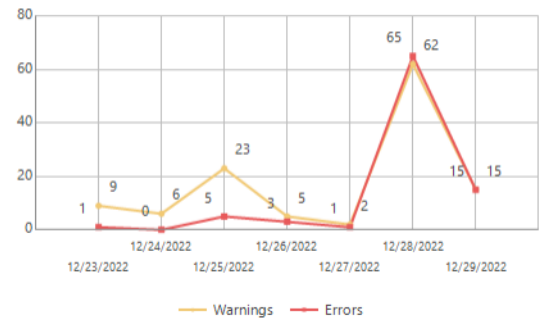
Errors



Warnings



Total Issues



Top 10 Issues

Name	Total Triggered	Total Objects
VM vCPU time per dispatch	116	4
Host available memory	53	1
Host Memory Pages Usage	29	1
Datastore read latency	6	1
Host CPU time per dispatch	4	1
Latest checkpoint age	2	2
Datastore write latency	1	1
Cluster memory overcommitment	1	1

Details

Issue Type: Error

Object Type	Location	Object	Alarms	Trend
Hyper-V Failover Cluster		1	1	
	\Virtual Infrastructure	ms-cluster.tech.local	1	Increasing
Hyper-V Host		2	27	
	\Virtual Infrastructure\ms-cluster.tech.local	ms-node-01	14	Increasing
	\Virtual Infrastructure\ms-cluster.tech.local	ms-node-02	13	Increasing
Hyper-V Storage		1	2	
	\Virtual Infrastructure\ms-cluster.tech.local\ms-node-02	Disk 0 C:	2	Increasing
Hyper-V Virtual Machine		4	60	
	\Virtual Infrastructure\ms-cluster.tech.local\ms-node-02	ES_1	25	Increasing
	\Virtual Infrastructure\ms-cluster.tech.local\ms-node-01	ms-19-1	2	Increasing
	\Virtual Infrastructure\ms-cluster.tech.local\ms-node-01	ms-19-1_replica	32	Increasing
	\Virtual Infrastructure\ms-cluster.tech.local\ms-node-02	Virtual_Lab_ES_Hyper-V	1	Increasing

Issue Type: Warning

Object Type	Location	Object	Alarms	Trend
Hyper-V Host		2	59	
	\Virtual Infrastructure\ms-cluster.tech.local	ms-node-02	40	Increasing
	\Virtual Infrastructure\ms-cluster.tech.local	ms-node-01	19	Increasing
Hyper-V Storage		2	5	
	\Virtual Infrastructure\ms-cluster.tech.local\ms-node-02	Disk 0 C:	4	Increasing
	\Virtual Infrastructure\ms-cluster.tech.local\ms-node-01	Disk 2 F:	1	Increasing
Hyper-V Virtual Machine		4	58	
	\Virtual Infrastructure\ms-cluster.tech.local\ms-node-02	ES_1	25	Increasing
	\Virtual Infrastructure\ms-cluster.tech.local\ms-node-01	ms-tape-01	1	Increasing
	\Virtual Infrastructure\ms-cluster.tech.local\ms-node-01	ms-19-1_replica	31	Increasing
	\Virtual Infrastructure\ms-cluster.tech.local\ms-node-01	node-1-vm1	1	Increasing

Use Case

The report provides an overview of the current health state of your virtual environment, shows the list of the most common alarms and identifies the most affected virtual infrastructure objects.

Alarms Overview (vSphere)

Veeam ONE Client generates multiple alarms to inform you about important events in your environment. This report allows administrators to quickly review the health state of the environment and to track how the number of alarms has been changing during the reporting period.

The report analyzes alerting activity across a time range, provides information on virtual infrastructure objects that caused the greatest number of alerts, and displays top 10 most frequently occurred issues.

- The **Summary** section includes the following elements:
  - The **Errors** and **Warnings** charts show top 5 objects that caused the greatest number of alarms.
  - The **Total Issues** chart shows alarm activity during the reporting period.
  - The **Top 10 Issues** table shows 10 most frequently triggered alarms.
- The **Details** section provides information on each affected object , including object type, location, object name, number of triggered alarms and alarm activity trend.

  Click a number in the **Alarms** column in the details table to drill down to details for alarms raised for the infrastructure object.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **Business View objects**: defines Business View groups to analyze in the report.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.
- **Period**: defines the time period to analyze in the report. Note that the reporting period must include at least one successfully completed *Object properties data collection* task for the selected scope. Otherwise, the report will contain no data.
- **Group by**: defines how data will be grouped in the report output (by *Issue type* or *Object type*).
- **Object types**: defines a list of virtual infrastructure object types to analyze in the report.
- **Alarms**: defines a list of alarms to analyze in the report.

  For details on alarms you can select in the list, see VMware vSphere Alarms.

View Report Example

Use Case

The report provides an overview of the current health state of your virtual environment, shows the list of the most common alarms and identifies the most affected virtual infrastructure objects.

Backup Alarms Overview

This report provides an overview of the data protection health state. It allows you to track Veeam Backup & Replication alarms triggered by Veeam ONE Client, and see most affected Veeam Backup & Replication jobs and components.

- The **Summary** display includes the following elements:
  - The **Job Issues History** chart displays the total number of warnings and errors for jobs for each day within a reporting period.
  - The **Backup Infrastructure Alarms** chart displays the total number of warnings and errors for infrastructure alarms for each day within a reporting period.
  - The **Top 10 VMs with Issues** table lists 10 most affected VMs and the number of alarms triggered for each machine.
  - The **Top 5 Jobs with Issues** chart displays top 5 jobs that caused more alarms than other jobs.
  - The **Top 10 Triggered Alarms** table shows 10 the most frequent alarms and how many times each alarm was triggered.
- The **Report Data** display shows the **Details** table that provides information on affected backup infrastructure objects and displays how many alarms were triggered.

  The report also calculates a trend for each object. It compares information on alarms triggered over the reporting period (day/week/month/year) with the number of alarms triggered during the day/week/month/year previous to the reporting period. For example, if the selected reporting period is one month, the trend will use the month previous to the reporting period to calculate the trend. By comparing two equal periods, the report shows whether the number of triggered alarms increased or reduced. Therefore, you can track data protection health state changes.

  Click a number in the **Alarms Triggered** column to drill down to alarm details.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines backup infrastructure objects to analyze in the report.
- **Period**: defines the time period to analyze in the report.
- **Alarm types**: defines a list of data protection object types to analyze and include in the report.
- **Alarms**: defines a list of alarms to analyze in the report. The options in the list depend on the selected *Alarm types* parameter.

  For details on alarms you can select in the list, see Veeam Backup & Replication Alarms.

View Report Example

Use Case

The report provides an overview of the data protection health state, shows the list of the frequently triggered alarms and displays the most affected backup infrastructure objects.

Backup Billing

This report allows you to assess storage costs for the backup infrastructure and to track the consumption of storage by backup files.

The report estimates storage resources required to store backups. The cost can be calculated based on the price of 1 GB or TB of consumed storage space or on the price of a single VM. If there is a repository that is more expensive than other ones, an administrator can also specify the price adjustment factor (or the multiplier) that characterizes the premium charged for access to the repository.

The report provides details on every backup job included into the report scope — the number of backed up VMs and computers, size of a restore point and total amount of gigabytes transferred to the storage.

- The **Summary** section provides an overview on the number of backup jobs, used repositories and backed up VMs and computers, total size of backups and total cost in selected currency.
- The **Details** section provides information on each backup job, including the number of backed up VMs and computers, restore points size, total amount of gigabytes transferred to the storage and total cost.

> **IMPORTANT!**
>
> If one restore point contains several VMs, the report will not provide detailed information on the size of individual backups for every VMs in this restore point. For details on, see Backup Chain Formats.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a list of backup repositories to analyze in the report.
- **Business View objects**: defines a list of Business View objects to analyze in the report.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.
- **Job type**: defines a job type to evaluate in the report (*VM backup*, *Backup copy*, *Agent backup policy*, *Agent backup*, *All types*).
- **Jobs**: defines a list of backup and backup copy jobs to include in the report.
- **Period**: defines the interval for which the billing statement is required.
- **Storage price**: defines a storage price for accommodating 1 GB/TB of backup files or a price for a single VM included in backup.
- **Individual repository price multipliers**: defines the price adjustment factor that characterizes the benefit (and the expense) of using the preferred repository storage. The resulting cost is calculated by multiplying the basic rate by the repository multiplier.

  To edit price multipliers:

  a. Click **Configure**.

  b. In the **Configure Individual Repository Price Multipliers** window, select the target repository and click **Edit**.

c. In the **Set Individual Repository Price Multiplier** window, specify the desired price adjustment multiplier and click **Save**.

d. For scale-out backup repositories:

   - To include capacity and archive tiers in the list of extents, select the **Count data stored on Capacity and Archive tier extents** check box.
   - To set a single multiplier for all extents of a scale-out backup repository, select the **Specify the same multiplier for each extent** check box and specify the multiplier.
   - To apply an individual multiplier to each extent, click the value in the **Multiplier** column next to an extent and specify the multiplier.

e. Repeat steps 2–3 for each repository price multiplier you want to edit.

- **Calculate price based on:** defines the value based on which prices will be calculated (*Latest value, Max value*).
- **Customer**: defines a customer name to display in the report output.
- **Show days with no backup activities**: defines whether the report will include days without backup activity.

View Report Example

Use Case

This report allows managed storage providers (MSP) to generate billing statements for customers and to charge them for the used storage.

The report can help administrators evaluate efficiency of the storage resources utilization.

Backup Copy Job

The main backup purpose is to protect your data against disasters and VM failures. Having only one copy of a backup file does not provide the necessary level of safety. To build a successful data protection and disaster recovery plan, you must have at least one independent copy of a backup file offsite, for example, in the remote site. To optimize data transfer between remote sites over the WAN, Veeam Backup & Replication offers the WAN acceleration technology.

To learn more about the 3-2-1 backup strategy and WAN acceleration, see the Veeam Blog article How to follow the 3-2-1 backup rule with Veeam Backup & Replication.

This report analyzes amount of traffic transmitted to target repository by backup copy jobs, evaluates the efficiency of backup data transfer through WAN accelerators and estimates the amount of network traffic savings.

- The **Summary** section includes the following elements:
  - The **Traffic Efficiency (GB)** chart shows the actual amount of traffic read from the source datastore and the amount of traffic transmitted over the network to the target repository.
  - The **Traffic Savings by Day (GB)** chart shows the amount of traffic saved on each day of the reporting interval (that is, the difference between the amount of read traffic and the amount of transferred traffic).
  - The **Savings Ratio by Day** chart shows daily fluctuations in the raw data to traffic savings ratio.
- The **Accelerators Details** table provides details for each pair of WAN accelerators used by backup copy jobs, backup server, job name, service size, actual amount of data transferred to the target repository, amount of saved traffic and savings ratio.

  Click a backup copy job name to drill down to details for the job.
- The **Job Details** table provides detailed information on, backup server, job names, session start time, source, status, source size (GB), backup file sizes, actual amount of data transferred, amount of saved traffic, savings ratio, WAN accelerator status, job type and copy mode.

> **NOTE:**
>
> For WAN accelerators used in Veeam Cloud Connect jobs, performance data is available only if the target WAN accelerator is present in the Veeam ONE infrastructure.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a list of Veeam Backup & Replication servers to include in the report.
- **WAN accelerators**: defines pairs of source-to-target WAN accelerators to include in the report.
- **Backup copy jobs**: defines a list of backup copy jobs to include in the report.
- **Period**: defines the time period to analyze in the report.

View Report Example

Use Case

WAN accelerators allow reducing the amount of network traffic transmitted to remote DR sites by leveraging the deduplication techniques.

This report helps you analyze traffic savings and raise the efficiency of your backup copy jobs.

Backup Infrastructure Assessment

This report evaluates how optimally your backup infrastructure is configured and suggests actions aimed at boosting its efficiency.

NOTE:

- This report is available for VMware vSphere environments only.
- Infrastructure topology view in Veeam ONE and Veeam Backup & Replication must match. Otherwise, Veeam ONE Web Client may show invalid data for Veeam Backup & Replication reports and dashboards.
- Veeam Cloud Connect service providers cannot see performance data for proxies used by tenant data protection jobs.

The report analyzes configuration of your virtual environment against a set of recommended baseline settings and implementations, identifies VMs that cannot be properly backed up due to configuration limitations, verifies problem areas and helps mitigate the issues.

- The **Summary** display contains the **Verification Results** chart that displays how many verification tests failed, passed or completed with warnings and how many criteria do not apply to your backup infrastructure (in percentage).
- The **Report Data** display shows whether verification tests for each criteria failed, passed or completed with warnings and marks criteria that does not apply to the infrastructure as *Not required*. It also shows a summary of recommendations for each test within the report infrastructure.

The report takes into account the following criteria when analyzing infrastructure configuration:

VM Configuration and Application-aware VM Processing

Criterion	Description
Application-aware image processing for Windows Servers	The report searches for jobs that do not have the **Enable application-aware image processing** option enabled. To create a transactionally consistent backup of a VM running VSS-aware applications (such as Active Directory, Microsoft SQL, Microsoft Exchange, Sharepoint) without shutting them down, Veeam Backup & Replication uses application-aware image processing. It is a proprietary technology that ensures successful VM recovery, as well as proper recovery of all applications installed on the VM without any data loss.
VMware tools quiescence for Linux/Unix VMs	The report searches for jobs that do not have the **Enable VMware Tools quiescence** option enabled. When taking snapshots of a running VM, VMware Tools will quiesce the VM file systems to ensure integrity of on-disk data. However, under heavy I/O load, this delay in I/O could become too long.

Criterion	Description
VMware tools status	The report analyzes your virtual infrastructure to find VMs that do not have VMware Tools installed, running or up-to-date. To enable backup with application-aware image processing, it is required that guest OS running inside your VMs have VMware Tools installed and running.
VMs verification	The report analyzes your virtual infrastructure to find VMs for which SureBackup jobs are not configured. SureBackup and SureReplica are technologies developed to automate and simplify the recovery verification process — one of the most crucial parts of data management and protection. SureBackup and SureReplica let users verify the recoverability of every VM backup and replica, without additional hardware or administrative time and effort.

Job Performance Optimization

Criterion	Description
Parallel virtual disk processing	The report searches for Veeam Backup servers that do not have the **Enable parallel VM and virtual disk processing** option enabled. Multiple VMs and VM disks can be processed in parallel, optimizing your backup infrastructure performance and increasing the efficiency of resource usage.
Virtual stand-by proxy server	The report analyzes your virtual infrastructure to find virtual backup proxy servers. For data retrieval,Veeam Backup & Replication offers the Virtual Appliance mode. The mode can only be used if the backup proxy is deployed on a VM. The Virtual Appliance mode uses the SCSI hot-add capability of ESXi hosts to attach disks of the backed up VM to the backup proxy VM. In this mode, VM data is retrieved directly from storage through the ESXi I/O stack, instead of going through the network stack, which improves performance.
Proxy server on the remote site	The report analyzes your virtual infrastructure to find backup proxy servers on the remote site. Storing backups offsite always involves moving large volumes of data between remote sites. To solve the problem of insufficient network bandwidth to support VM data traffic and optimize data transfer over the WAN, it is recommended to deploy a proxy server on the remote site.

Criterion	Description
Direct SAN access iSCSI performance tweaks	The report analyzes your infrastructure to find backup proxies configured to use the Direct SAN Access mode working with iSCSI storage. The Direct SAN Access mode is recommended if the ESXi host uses shared storage. The backup proxy leverages VADP to retrieve VM data directly from FC or iSCSI storage in the Storage Area Network (SAN). To retrieve data blocks from SAN LUN, the backup proxy uses metadata about the layout of VM disks on the SAN. Since data blocks are not retrieved over the Local Area Network (LAN), this mode minimizes disruptions to your production network during backup.
Meeting Backup Window	The report analyzes job sessions to find jobs whose duration exceeds the defined backup window. If job duration exceeds the backup window and the bottleneck is a proxy, the report will provide recommendations to deploy more proxies. This criterion is available only if you specified the **Required Backup Window** parameter.
Backup job processing mode optimizations	The report analyzes job statistics to find bottlenecks in the data flow. As any backup application handles a great amount of data, it is important to make sure the data flow is efficient and all resources engaged in the backup process are optimally used. To identify a bottleneck in the data path, Veeam Backup & Replication detects the component with the maximum workload: that is, the component that works for the most time of the job. In case the report discovers that a backup proxy is the weakest component in the data flow, it is recommended to deploy additional proxy servers.

Backup Infrastructure Configuration

Criterion	Description
VMs failed over to network processing mode	The report analyzes your virtual infrastructure to find VMs that failed over to the Network Processing mode. The Network Processing mode can be used with any infrastructure configuration. However, when an alternative transport mode is applicable, the Network mode is not recommended because of the lowest data retrieval speed.

Criterion	Description
Backup server protection	The report analyzes your virtual infrastructure to find backup servers that do not run configuration backups on their database. If a Veeam backup server fails, you can re-deploy the Veeam backup server, restore configuration data for the Veeam backup server from the backup and apply it to the re-built server. Alternatively, you can apply configuration data to any other Veeam backup server in your backup infrastructure. In terms of configuration, you get a replica of the Veeam backup server you had, without additional adjustments and fine-tuning.
SQL Server optimization	The report analyzes Veeam Backup & Replication databases hosted on SQL Server Express instances to check whether these instances need to be upgraded to the full version of SQL Server. If the amount of data stored in Veeam Backup & Replication databases exceeds SQL Server Express capabilities, it may cause slow operation of the Veeam Backup & Replication console.
Repository free space	The report analyzes your virtual infrastructure to find repositories that have run out of free space.
Storage latency control	The report searches for jobs that do not have the **Enable storage latency control** option enabled. Storage latency control should be enabled in the Veeam Backup & Replication console to ensure that running jobs do not impact storage availability to production workloads.
Proxy Server Configuration	The report analyzes your virtual infrastructure to find backup proxy servers for which the number of concurrent tasks is greater than the number of CPU cores.

File level restores

Criterion	Description
Indexing of Guest OS files (optional)	The report searches for jobs that do not have the **Enable guest file system indexing** option enabled. This criterion is available only if you selected the **1-Click file level restores** parameter.

Report Parameters

You can specify the following report parameters:

- **Scope**: defines a list of Veeam Backup & Replication servers to include in the report.

- **1-Click file restore sessions**: defines whether the report will analyze the 1-click file level restore capabilities.
- **Required backup window**: defines an interval for daily backup sessions that should be assessed.

View Report Example

Use Case

The size and complexity of modern geographically disperse backup infrastructures makes it difficult to manage and optimize them.

Following the report recommendations, backup administrators can improve job configuration and implement the necessary hardware and software optimizations. This will help you attain better efficiency, lower resource consumption and expedite backup time.

Backup Infrastructure Audit

This report tracks configuration changes in your backup environment, providing detailed information about every change for each object.

- The **Summary** section includes the following elements:
  - The **Modifications by Object Types** chart illustrates types of changed objects and shows the share of particular object type changes.
  - The **Modifications per User** chart illustrates which users made changes and shows the share of changes made by each user.
- The **Details** table lists descriptions of changes made to particular objects.

> **NOTE:**
> - For WAN accelerators used in Veeam Cloud Connect jobs, performance data is available only if the target WAN accelerator is present in the Veeam ONE infrastructure.
> - Veeam Cloud Connect service providers cannot see performance data for proxies used by tenant data protection jobs.
> - This report uses Windows Events collected from machines with Veeam Backup & Replication servers deployed and Events Data collection configured. Remote Event Log Management must also be enabled for this report. For details on Remote Event Log Management, see Firewall Rules.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a list of Veeam Backup & Replication servers to include in the report.
- **Period**: defines the time period to analyze in the report.
- **Object types**: defines a list of backup infrastructure objects to include in the report (*Backup Server*, *Backup Proxy*, *Backup Repository*, *Cloud Gateway*, *WAN Accelerator*, *Cloud Repository*).
- **Users**: defines a list of backup users, changes from whom to include in the report.

View Report Example

Use Case

The report allows backup administrators to get details on recent infrastructure changes made by authorized users so that any unwanted action can be quickly rolled back.

Backup Infrastructure Custom Data

This report features a collection of custom properties for Veeam Backup & Replication objects, including backup servers, backup jobs, VMs and computers. The report helps you analyze data protection aspects not covered by Veeam Backup & Replication reports.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a list of Veeam Backup & Replication servers to include in the report.
- **Object type**: defines a list of Veeam Backup & Replication objects to analyze in the report (*Backup server*, *Job*, *Virtual machine*, *Computer*, *Repository*, *Workload*).
- **Columns**: defines configuration properties to analyze in the report. The list of available properties will depend on the selected object type. Use the **Filter** field to search for the necessary properties by name. Note that the number of selected properties must not exceed 50.

> **NOTE:**
>
> To analyze data about protected VMs in the report, you must connect the target virtualization servers to Veeam ONE. For details on, see Add Data Source.

View Report Example

Use Case

Use the advanced collection of Veeam Backup & Replication object properties to create custom reports that display key aspects of the backup infrastructure and data protection operations.

Backup Inventory

This report provides inventory information on configuration of your Veeam Backup & Replication infrastructure.

- The **License Information** section shows product license details. The **Installed Licenses** subsection includes the license type, the number of licensed and used sockets and instances, support expiration and license expiration dates, the overall and used capacity. The **Instances Usage** subsection shows groups of managed objects, number of objects in each group, and number of instances consumed by each group.
- The **Veeam B&R Infrastructure** section provides information about backup servers, including the version of Veeam Backup & Replication installed, the number and type of backup proxies and backup repositories managed by backup servers.
- The **Backup Proxies** section provides information about backup proxy servers, including the type of transport mode chosen for proxy servers, the number of maximum allowable concurrent tasks, connected datastores, and shows whether throttling is enabled for these servers.

  Veeam Cloud Connect service providers cannot see performance data for proxies used by tenant data protection jobs.
- The **Veeam Plugins for Enterprise Applications** section provides information about protected data on enterprise databases, including version, type and number of objects.
- The **Tape Servers** section provides information about tape servers and tape libraries connected to the servers, and shows whether throttling is enabled for these servers.
- The **Backup Repositories** section shows a list of backup repositories and provides additional details including the repository capacity and free space, the amount of space used by full and incremental backups, the number of backup jobs utilizing a repository and the number of workloads residing in backups stored on a repository.
- The **Scale-Out Backup Repositories** section shows a list of scale-out backup repositories and provides additional details including the repository regular extents and capacity tiers, their capacities and free space, the amount of used space, the number of backup jobs utilizing a repository and the number of workloads residing in backups stored on a repository.
- The **WAN Accelerators** section provides information about WAN accelerators and their configuration, including a port number, the number of allowed concurrent connections, cache size, the amount of free space in cache, and cache location.

  For WAN accelerators used in Veeam Cloud Connect jobs, performance data is available only if the target WAN accelerator is present in the Veeam ONE infrastructure.
- The **Cloud Repositories** section provides information about cloud repositories available for cloud tenants, including physical repositories on which cloud storage is allocated, storage quota, free space remaining on the repositories, the number of workloads residing in backups stored on a repository, repository expiration date.
- The **Cloud Gateway Servers** section provides information about cloud gateways configured on Veeam Cloud Connect servers, including OS of a machine that performs the role of a cloud gateway, IP address or DNS name of this machine, a port that a cloud gateway uses to transport data, and related gateway pools.
- The **Cloud Gateway Pools** section provides information about number of gateways in each gateway pool.
- The **Jobs** section displays all backup jobs, their types and the number of workloads in each job.

> **NOTE:**
>
> Veeam ONE displays file backup copy jobs together with other backup copy jobs.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a list of Veeam Backup & Replication servers to include in the report.

View Report Example

Use Case

This report displays information on the state of backup infrastructure components and provides product licensing details.

Backup Objects Change Tracking

This report provides detailed information on backup infrastructure configuration changes performed within the reporting period. It includes the exact time of change and the name of the user who did the change.

- The **Summary** section includes the following elements:
  - The **Modifications by Object Types** chart illustrates types of changed objects and shows the share of particular object type changes.
  - The **Modifications per Initiator** chart illustrates which users made changes and shows the share of changes made by each user.
  - The **Modifications by Day** chart displays distribution of changes performed during report period.
- The **Details** table lists descriptions of changes made to particular objects.

> **NOTE:**
>
> Veeam Cloud Connect service providers cannot see performance data for proxies used by tenant data protection jobs.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a list of Veeam Backup & Replication servers to include in the report.
- **Period**: defines the time period to analyze in the report.
- **Object types**: defines a list of backup infrastructure objects to include in the report (*Backup Server*, *Backup Proxy*, *Backup Repository*, *All Items)*.
- **Object inclusion rule**: defines names of objects to include in the report. You can enter object names explicitly or create a wildcard mask by using the asterisk (*) to replace any number of characters. Multiple entries are separated by semicolon.
- **Users**: defines a list of backup users, changes from whom to include in the report.

View Report Example

Use Case

The report allows backup administrators to get details on recent infrastructure modifications made to target objects so that any unwanted action can be quickly rolled back.

Backup Security and Compliance

This report provides information about all backup server configurations to ensure they follow security best practices for the OS and Veeam backup infrastructure components.

- The **Summary** section includes the following elements:
  - The **Backup Server Security & Compliance Status** chart shows the status of your total backup servers based on success rate configured in the report's **Check result**,
  - The **Missed Security & Compliance Checks** chart shows the volume of missed best practices configured in the report's **Check result** including whether the security and compliance check missed, is not implemented, is not checked, is suppressed or is unable to detect.
  - The **Security & Compliance Last Check** chart shows how recently the best practice check was performed on each server.
- The **Overview** table provides information on security and compliance checks on individual server instances.
- The **Details** section provides information on best practice types, their status and recommendations on how to resolve best practice failures.

Report Parameters

You can specify the following report parameters to filter your Backup Security & Compliance report:

- **Infrastructure objects**: defines a list of Veeam Backup & Replication servers to include in the report.
- **Best practice types**: select the type of the best practice to check for on your servers.
- **Check result**: filter best practices with the selected states (Passed, Unable to detect, Not implemented, Suppressed, Not checked).

View Report Example

Use Case

This report helps you identify missed security and compliance checks and provides recommendations for rectifying them. Using this report, you can effectively monitor the current status of security and compliance checks within your infrastructure.

Backup SLA Compliance (Veeam Backup for Microsoft 365)

This report analyzes backups of Microsoft 365 infrastructure objects. The report examines whether these objects are compliant with SLA target.

- The **Summary** section includes the following elements:
  - Information on SLA compliance of different organization object types.
  - The **Organization Objects by Compliance State** chart shows the percentage of organization objects of each type that meet the target SLA.
- The **Organizations** table provides information on all types of protected objects for each organization.
- The **Organization Objects That Meet Target Backup SLA** and **Organization Objects That Breach Target Backup SLA** tables provide information on all organization objects, jobs that include the objects, number of available restore points and SLA compliance percentage.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a list of Veeam Backup for Microsoft 365 servers to include in the report.
- **Organizations**: defines Microsoft organizations to analyze in the report.
- **Object types**: defines Microsoft 365 infrastructure objects to analyze in the report.
- **Jobs**: defines backup jobs to analyze in the report.
- **Period**: defines the time period to analyze in the report.
- **Object exclusion rule**: defines a list of Microsoft 365 infrastructure objects that should be excluded from the report scope. You can enter object names either explicitly or input a part of the name. Multiple entries are separated by comma.
- **Target SLA**: defines the target SLA value (in percent).
- **Show organization objects that missed target SLA**: defines whether objects not compliant with the target SLA should be included in the report.

View Report Example

Use Case

This report helps you discover protected objects that breach the target SLA, and jobs that do not operate properly.

Backups on Repository

This report provides detailed information about files stored on backup repositories.

- The **Summary** section includes the following elements:
  - The **Top Repositories by Used Space, %** chart displays top 5 repositories in terms of the greatest amount of used space of restore points and the largest amount of backed up data.
  - The **Top Repositories by VM/Computer/File Object Storage/Application Backups, GB** charts display top repositories in terms of the greatest number of VMs, computers and file sources stored on the repository.
- The **Details** section provides information on repository type, capacity, free and used space as well as detailed information about backups stored on the repository.

> **IMPORTANT!**
>
> If one restore point contains several VMs, the report will not provide detailed information on the size of individual backups for every VMs in this restore point. For details on, see Backup Chain Formats.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a list of Veeam Backup & Replication servers to include in the report.
- **Backup repositories**: defines a list of backup repositories to include in the report.
- **Protected workloads**: defines types of objects to include in the report (*Virtual machine*, *Computer*, *File share, Unstructured Data*, *Enterprise Application*).

View Report Example

Use Case

This report helps you monitor space usage on backup repositories and the amount of VMs, computers and file sources stored on repositories.

Backups on Tape

This report provides detailed information about backup files stored on tapes.

- The **Details** section provides the **Details**, **Tape Details** and **Empty Tapes** tables which provide information on each tape, including the amount of used space and remaining free space, size of stored backups, the date until which the tape is protected, and detailed information on backups stored on the tape.

> **IMPORTANT!**
>
> If one restore point contains several VMs, the report will not provide detailed information on the size of individual backups for every VMs in this restore point.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a list of Veeam Backup & Replication servers to include in the report.
- **Media pools**: defines a list of media pools to include in the report.
- **Tapes**: defines a list of tapes to include in the report.

View Report Example

Use Case

This report helps you monitor tape space usage and the number of VMs, computers and unstructured data files stored on tapes.

Capacity Planning (Hyper-V)

This report forecasts how many days remain before the level of resource utilization reaches the specified threshold values. The report allows you to analyze the following resource utilization parameters: CPU, memory, datastore free space, read and write rates.

- The **Summary** section provides an overview of the infrastructure (the total number of hosts, datastores and VMs), shows the number of days left before specified thresholds will be reached, and the amount of resources required to sustain the current workloads without exceeding the specified thresholds.
    - The **Top 5 Utilized Clusters and Standalone Host** table displays objects that will run out of CPU or memory resources sooner than others. It shows the bottleneck parameter for each object and its average usage. This data is used to predict how many days are left before the object reaches the threshold.

      Some values in this section may be highlighted with red. If a value in the **Average Usage** column is highlighted with red, the resource usage value has reached the specified threshold. The **Days Remaining** value is highlighted with red if the number of days left until the parameter reaches the threshold is less than 183 (6 months).
- The **Details** section displays host hardware configuration and resource usage, analyzes historical performance data for the specified period in the past to calculate the performance utilization trend, and provides recommendations on how to keep the resource utilization below the specified thresholds.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines virtual infrastructure objects and sub-components you want to analyze in the report.
- **Datastores**: defines a list of datastores to analyze in the report.
- **Analyze performance data for**: defines a time period in the past the report will use to accumulate performance data and calculate the performance trend.
- **Perform planning for**: defines a time period in the future for which performance data will be used to forecast resource usage trend.
- **CPU utilization (%)**: defines the CPU usage threshold as a percentage of total CPU resources of virtual infrastructure objects.
- **Memory utilization (%)**: defines the used memory threshold as a percentage of total memory resources of virtual infrastructure objects.
- **Space utilization (%)**: defines the maximum amount of space in use on a datastore.
- **Free space (min)**: defines the minimum amount of free space left on a datastore in GB.
- **Read/write speed (max)**: defines the maximum read and write rates in MB per second for a datastore.
- **Business hours from - to**: defines time of a day for which historical performance data will be used to calculate the performance trend. All data beyond this interval will be excluded from the baseline used for data analysis.

- **Show graphs**: defines whether the report must include charts that illustrate historical performance data for the specified period.

Capacity Planning

Description

This report predicts when resource utilization for selected objects in the infrastructure will reach the configured threshold.

Report Parameters

Scope:	Virtual Infrastructure
Datastores:	All Datastores
Analyze performance data for:	Past 6 months
Perform planning for:	Next 6 months
CPU utilization threshold:	80.00 %
Memory utilization threshold:	80.00 %
Datastore space utilization threshold:	90.00 %
Datastore read/write speed (max) threshold:	50 MBps

Summary

Virtual Infrastructure		Days Remaining		Resources Required	
Number of standalone hosts:	1	CPU:	∞	CPU:	0.00 GHz
Number of hosts:	1	Memory:	∞	Memory:	0.00 GB
Number of datastores:	2	Datastore space utilization:	∞	Datastore capacity:	0.00 TB
Number of VMs:	16	Datastore read rate:	∞		
Number of powered on VMs:	10	Datastore write rate:	∞		

Top 5 Utilized Clusters and Standalone Hosts

Object Name	Bottleneck	Average Usage	Days Remaining
pdctwhv01.tech.local	CPU usage	15.60 %	∞

Details

Selected Object: pdctwhv01.tech.local

Physical Resources

CPU (GHz)	CPU Sockets	CPU Cores	Memory (GB)	Datastore Capacity (GB)
50.42	2	24	382.67	16764.94

Resource Usage

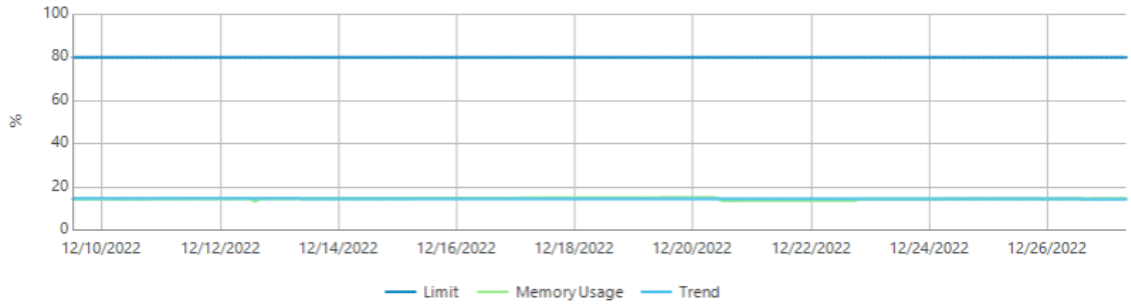
Resources	Memory Usage	CPU Usage	Datastore Used Space	Read Rate	Write Rate
Current usage	14.64 %	14.00 %	14.39 %	1.11 MBps	1.13 MBps
Average usage	14.54 %	15.60 %	14.39 %	5.94 MBps	1.52 MBps
Days remaining	∞	∞	∞	∞	∞

Recommendations

The selected object has enough capacity to maintain the current workload, no additional resources are required.

Performance Trends

Memory Usage



Memory Usage (%)

Object Name	Minimum	Maximum	Average	Std.Deviation	Days Left
pdctwhv01.tech.local	13.35	15.18	14.54	0.41	∞

Use Case

This report helps you plan workloads to avoid resource shortage. It analyzes historical performance to calculate typical resource utilization. The report extrapolates received data to the future to predict when you will run out of resources and provide recommendations on resources you need to add to maintain stable operation.

Capacity Planning (vSphere)

This report forecasts how many days remain before the level of resource utilization reaches the specified threshold values. The report allows you to analyze the following resource utilization parameters: CPU, memory, datastore free space, read and write rates.

- The **Summary** section provides an overview of the current state of the infrastructure (the total number of hosts, datastores and VMs), shows the number of days left before specified thresholds will be reached, and the amount of resources required to sustain the current workloads without exceeding the specified thresholds.
    - The **Top 5 Utilized Clusters and Standalone Hosts** table displays objects that will run out of CPU or memory resources sooner than others. It shows the bottleneck parameter for each object and its average usage. This data is used to predict how many days are left before the object reaches the threshold.

      If the **Average Usage** value is highlighted with red, it means that the resource usage value has reached the specified threshold. If the **Days Remaining** value is highlighted with red, it means that the number of days left until the parameter reaches the threshold is less than 183 (6 months).
- The **Details** section displays host hardware configuration and resource usage, analyzes historical performance data for the specified period in the past to calculate the performance utilization trend, and provides recommendations on how to keep the resource utilization below the specified thresholds.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **Datastores**: defines a list of datastores to analyze in the report.
- **Analyze performance data for**: defines a time period in the past for which historical performance data will be used to calculate the performance trend.
- **Perform planning for**: defines a time period in the future for which performance data will be used to forecast resource usage trend.
- **CPU utilization (%)**: defines the CPU usage threshold as a percentage of total cluster CPU resources.
- **Memory utilization (%)**: defines the used memory threshold as a percentage of total cluster memory resources.
- **Space utilization (%)**: defines the maximum amount of space in use on a datastore.
- **Free space (min)**: defines the minimum amount of free space in GB left on a datastore.
- **Read/write speed (max)**: defines the maximum read and write rates in MB per second for a datastore.
- **Business hours**: defines time of a day for which historical performance data will be used to calculate the performance trend. All data beyond this interval will be excluded from the baseline used for data analysis.
- **Show graphs**: defines whether the report must include charts that illustrate historical performance data for the specified period.

View Report Example

Use Case

This report helps you plan workloads to avoid resource shortage. It analyzes historical performance to calculate typical resource utilization. The report extrapolates received data to the future to predict when you will run out of resources and provide recommendations on resources you need to add to maintain stable operation.

Capacity Planning for Backup Repositories

This report estimates the amount of free space available on backup repositories and forecasts how many days remain before a repository will run out of available storage capacity.

Backup repositories tend to run out of free space when outdated restore points overload the datastore. This report helps you ensure there is enough space for your backup data at any point in time. The report also provides recommendations on how to adjust the allocated storage resources to meet the future demand for backup storage. Furthermore, it calculates the amount of additional space that needs to be provisioned to accommodate the necessary restore points.

To calculate future repository performance, the report analyzes historical performance data for the selected time period, calculates the performance utilization trend and applies this trend to the safety interval (that is, the selected number of days during which the specified threshold should not be breached). This helps you rationally plan your resources.

- The **Summary** display provides an overview of the backup infrastructure (the total number of repositories, jobs and stored computers, VMs and file shares), shows repositories capacity, the amount of free space, the utilization ratio, the number of days left before specified thresholds will be reached, and the amount of space required to sustain the current workloads without exceeding the specified thresholds.
    - The **Top 5 Utilized Repositories** and **Top 5 Repositories by Days Left** charts display 5 repositories that will run out of free space sooner than other repositories and the number of days left before space usage level on these repositories breaches the specified threshold. Additionally, each each repository configured for the report has its own accompanying virtual chart.
- The **Report Data** display provides the **Details** and **Backup Repository Free Space Usage** tables displaying information on the total repository capacity, number of VMs, computers, file shares, applications and object storage data in backups stored on the repository and the number of days left before the repository runs out free space.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a list of backup repositories to analyze in the report.
- **Space utilization threshold**: defines the maximum amount of used space measured as a percentage of total capacity on the available repositories.
- **Free space (min) threshold**: defines the minimum total amount of free space on the repositories.
- **Safety interval**: defines the safety interval (that is, the required minimum number of days during which the specified space threshold should not be breached).
- **Analyze performance data for**: defines the time period to analyze in the report.

View Report Example

Use Case

The report allows you to analyze configuration and space usage on backup repositories and to forecast how many days remain before the repository reaches its full capacity. You can use the report to assess the required amount of additional space that needs to be allocated to support the uninterrupted backup operations for a specified number of days into the future.

Catalogs Overview

This report displays an inventory of catalogs created for selected organizations.

- The **Catalogs** table provides information on catalogs for each organization, including catalog name, sharing status, publish status, catalog owner, date when catalog was created and number of vApp templates.
- The **vApp Templates** table provides information on vApp templates stored in the catalog, including template name, hardware version, OS and allocated vCPU, memory and storage resources.

Report Parameters

You can specify the following report parameters:

- **VMware Cloud Director objects**: defines a list of organizations to analyze in the report.

Catalogs Overview

Description

This report provides overview information on all catalogs in managed VMware Cloud Director organizations.

Report Parameters

VMware Cloud Director objects:	VMware Cloud Director

Catalogs

Organization	Catalog	Shared	Publish Status	Owner	Created on	vApp Templates
⊟organization01	1					
	catalog01	No	-	system	12/30/2022	1

vApp Templates

Catalog	vApp Template	Hardware Version	OS	vCPU	Memory (GB)	Storage (GB)
⊟catalog01	1					
	template01	vmx-07	Other Linux (64-bit)	1	1.00	

Use Case

Outdated catalog data consume valuable cloud resources. Use this report to review content of VMware Cloud Director catalogs and to track the amount of space consumed by catalog content across organizations.

CDP SLA Compliance

This report analyzes continuous data protection of VMs in your virtual infrastructure. The report examines whether VMs protected by CDP policy are compliant with SLA target.

- The **Summary** section includes the following elements:
  - The **Average SLA** chart shows the average SLA percentage for protected and unprotected VMs.
  - The **Workloads by Compliance State** chart shows the number of VMs that meet the target SLA, VMs that breach the target SLA and VMs that do not have a CDP replica.
  - The **Workloads by SLA** chart shows the SLA value for protected and unprotected VMs.
  - The **Sync Sessions Statistics** chart shows number of job sessions for protected and unprotected VMs finished with different statuses.
- The **Report Data** section displays three tables, *Workloads That Meet Target SLA, Workloads That Missed Target SLA*, and *CDP Sessions Issues and* provides information on all VMs protected by CDP policies, including VM name, CDP policy name, VM location, replica location, RPO, average SLA, maximum delay, number of crash-consistent and application-consistent restore points, status of the last replication session, amount of transferred data, primary bottleneck and date and time of the last successful replication session.

Report Parameters

You can specify the following report parameters:

- **Protected infrastructure**: defines the platform to analyze in the report.
- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **VM folders**: defines a list of VMware folders to include in the report (applies to VMware vSphere environments only). VM folders view is an alternate way to present the virtual infrastructure. If VMs in your infrastructure are grouped into folders according to their profile, you can limit the report scope by specifying the necessary folders only.
- **Business View objects**: defines Business View groups to analyze in the report. The parameter options are limited to objects of the Virtual Machine type.
- **VMware Cloud Director objects**: defines VMware Cloud Director components to analyze in the report.
- **Period**: defines the time period to analyze in the report.
- **VM exclusion rule**: defines a list of VMs that should be excluded from the report scope. You can enter VM names explicitly or create a wildcard mask by using the asterisk (*) to replace any number of characters. Multiple entries are separated by comma. Usage example: the following string will exclude machines with the _R&D suffix from appearing in the report: **_R&D*.
- **Target SLA**: defines the target SLA value (in percent).
- **Show non-compliant VMs**: defines whether VMs not compliant with the target SLA should be included in the report. You can choose to show all non-compliant VMs or only VMs added to CDP policies.
- **Include Business View groups**: defines whether to include business view groups in the report.

View Report Example

Use Case

This report helps you discover VMs that breach the target SLA or do not have a CDP replica. It provides details on the state of CDP policies so that you can reconfigure current policy settings or include mission critical VMs in CDP policies.

Cloud Connect Inventory

This report provides inventory information on the Veeam Backup & Replication and Veeam Cloud Connect infrastructures.

- The **License Information** section shows product license details, including the total number of instances consumed by physical computers (workstations and servers) backup, number of instances consumed by cloud backups and replicas, the breakdown of total and used instances for licensed objects, and license expiration date.
- The **Rental Licenses** section shows number of rental instances consumed by tenants' physical computers (workstations and servers) and VM cloud backup, as well as total and used instances.
- The **Veeam B&R Infrastructure** section provides information about backup servers, including the version of Veeam Backup & Replication installed, the number and type of backup proxies and backup repositories managed by backup servers.
- The **Backup Proxies** section provides information about backup proxy servers, including the server type (file proxy or VM proxy), the type of transport mode chosen for proxy servers, the number of maximum allowable concurrent tasks, connected datastores, and shows whether throttling is enabled for these servers.

  Veeam Cloud Connect service providers cannot see performance data for proxies used by tenant data protection jobs.
- The **Tape Servers** section provides information about tape servers and tape libraries connected to the servers, and shows whether throttling is enabled for these servers.
- The **Backup Repositories** section shows a list of backup repositories and provides additional details including the repository capacity and free space, the amount of space used by full and incremental backups, the number of backup jobs utilizing a repository and the number of VMs and computers residing in backups stored on a repository.
- The **Scale-Out Backup Repositories** section shows a list of scale-out backup repositories and provides additional details including the repository regular extents and capacity tiers, their capacities and free space, the amount of used space, the number of backup jobs utilizing a repository and the number of VMs and computers residing in backups stored on a repository.
- The **WAN Accelerators** section provides information about WAN accelerators and their configuration, including a port number, the number of allowed concurrent connections, cache size, the amount of free space in cache, and cache location.

  For WAN accelerators used in Veeam Cloud Connect jobs, performance data is available only if the target WAN accelerator is present in the Veeam ONE infrastructure.
- The **Cloud Repositories** section provides information about cloud repositories including underlying backup repositories, quotas, the amount of free space left, the number of VMs and computers residing in backups stored on the repositories, and quota expiration dates.
- The **Cloud Gateway Servers** section provides information about configuration of cloud gateways including guest OSes, IP addresses, ports numbers and related gateway pools.
- The **Cloud Gateway Pools** section provides information about number of gateways in each gateway pool.
- The **Hardware Plans** section shows the amount of virtual computing, memory and storage resources allocated to a hardware plan and the number of users subscribed to each plan.
- The **Clusters/Hosts** section provides information about hosts and clusters unitized in cloud hardware plans, their CPU and memory resources, and the number of VM replicas on a host/cluster.

- The **Storages** section shows total capacity of cloud storage, amount of free space and the number of VM replicas located on each storage.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a list of Veeam Backup & Replication servers to include in the report.

> **NOTE:**
> - Infrastructure topology view in Veeam ONE and Veeam Backup & Replication must match. Otherwise, Veeam ONE Web Client may show invalid data for Veeam Backup & Replication reports and dashboards.
> - To analyze data about replicated VMs in the report, you must connect the target virtualization servers to Veeam ONE. For details on, see Add Data Source.

View Report Example

Use Case

This report displays inventory information for the Veeam Backup & Replication and Veeam Cloud Connect infrastructure components including licensing details.

Cloud Connect Replication Provisioning

This report allows you to identify cloud hosts, clusters and datastores that are over-provisioned and under-provisioned with resources and make sure CPU, memory and storage resources are allocated efficiently.

- The **Summary** display includes the following elements:
  - The **Top 5 Over-provisioned Hosts/Clusters (by CPU), GHz** chart displays 5 most over-provisioned cloud hosts and clusters by CPU and displays their total CPU capacity and the amount of computing resources provisioned for them.
  - The **Top 5 Over-provisioned Hosts/Clusters (by Memory), GB** chart displays 5 most over-provisioned cloud hosts and clusters by memory and displays their total memory capacity and the amount of memory resources provisioned for them.
  - The **Top 5 Over-provisioned Datastores, GB** chart displays 5 most over-provisioned cloud datastores by memory and displays their total memory capacity and the amount of memory resources provisioned for them.
- The **Report Data** display provides the **Provisioned Hosts (by CPU)**, **Provisioned Hosts (by Memory)** and **Provisioned Datastores** tables that display information on cloud hosts and clusters that are over-provisioned and under-provisioned with CPU, memory and storage resources and provides information about resource allocation on these hosts.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a list of virtual infrastructure objects to include in the report.
- **CPU Utilization Thresholds**: defines minimum and maximum CPU utilization thresholds in percent.
- **Memory Utilization Thresholds**: defines minimum and maximum memory utilization thresholds in percent.
- **Datastore Utilization Thresholds**: defines minimum and maximum storage utilization thresholds in percent.

NOTE:

- Infrastructure topology view in Veeam ONE and Veeam Backup & Replication must match. Otherwise, Veeam ONE Web Client may show invalid data for Veeam Backup & Replication reports and dashboards.
- To analyze data about replicated VMs in the report, you must connect the target virtualization servers to Veeam ONE. For details on, see Add Data Source.
- When specifying threshold intervals, note the following:
  - If the amount of provisioned CPU, memory or storage resources is higher than the specified maximum threshold, an object (such as a host, cluster or datastore) is considered over-provisioned.
  - If the amount of provisioned CPU, memory or storage resources is less than the specified minimum threshold, an object (such as a host, cluster or datastore) is considered under-provisioned.
  - If the amount of provisioned CPU, memory or storage resources is between the minimum and maximum thresholds, an object (such as a host, cluster or datastore) will not be included in the report charts or tables as the provisioning value is considered normal.

View Report Example

Use Case

The report helps define whether existing hardware plans match hosts and datastores capabilities. Use this data to avoid potential issues that may be caused by excessive over-provisioning of cloud replication hosts.

Cloud Connect User Report (Backup)

This report gathers information on storage quota usage and activity of users that consume Veeam Cloud Connect repository resources. The report forecasts the date when cloud repositories will run out of available storage quota and helps you ensure there is enough space for backup data at any point in time.

- The **Summary** display includes the following elements:
  - The **Overview** subsections provide information on the total number of users, the number of users who were active/inactive during past 30 days, the number of users who will run out of quota in the next 30 days, the total number of cloud repositories, the total storage quota, total amount of space used and left on repositories, and number of VMs and computers.
  - The **Top Users By Days Left to Reach Quota** and **Top Users By Quota Utilization (%)** charts display 5 users that will run out of space sooner than other users and 5 users with the highest level of space utilization.
- The **Report Data** display provides the **Tenant Detail** and **Tenant Session Details** tables that show information on user activity on each day of the reporting period, the number of VMs and computers in backups stored on the repository, cloud repository quota assigned to the user, the amount of used and free space on the repository, amount of data transferred to the cloud, space usage trend, the date the user contract expires and the last time and date when the user was active. The report also forecasts the number of days left before the user runs out of quota.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a list of Veeam Backup & Replication servers and Veeam Cloud Connect tenants to include in the report.
- **Last <N> weeks/months**: defines the time period to analyze in the report.

> **NOTE:**
>
> The number of VMs and computers in backups on cloud repositories may differ from the number of VMs and computers specified in Veeam Backup & Replication. Veeam Backup & Replication shows the number of licensed VMs and computers only, while Veeam ONE shows the total for licensed and stored VMs and computers.

View Report Example

Use Case

This report allows Veeam Cloud Providers (VCPs) to analyze configuration and quota usage on cloud repositories. The report helps VCPs define which repositories are running out of free space, keep an eye on user activity and decide whether to increase quota for the users.

Cloud Connect User Report (Replication)

This report analyzes Veeam Cloud Connect users' replication activity, and provides information on cloud host and storage quota usage over the specified period. The report reveals Veeam Cloud Connect users with the greatest amount of provisioned CPU, memory and storage resources, as well as users with the greatest number of replicated VMs.

- The **Summary** section includes the following elements:
  - The **Overview** subsections provide information on the total number of Veeam Cloud Connect replication users, number of users with standalone and VMware Cloud Director accounts, configured hardware plans and total VMs replicated. It also includes information on standalone and VMware Cloud Director tenants' compute and storage resources, their capacity, amount of provisioned and used resources.
  - The **Top Users by VMs Replicated** chart displays 5 users with the greatest number of VMs replicated to cloud.
  - The **Top Users by CPU/Memory/Storage Quota** charts display 5 users with the greatest amount of provisioned CPU, memory and storage resources, and visualize the amount of used cloud resources.
- The **Report Data** display shows the **Details** and **VM Details** tables that provide information on Veeam Cloud Connect users, their virtualization platform, hardware plan, number of VMs replicated to cloud on each day of the reporting period, amount of provisioned and used CPU, memory and storage resources. If the resource usage value is approaching the quota limit, the value is highlighted with yellow in the table. If the quota is exceeded, the resource usage value is highlighted with red.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a list of Veeam Backup & Replication servers and Veeam Cloud Connect tenants to include in the report.
- **Last <N> weeks/months**: defines a time period to analyze in the report.

> **NOTE:**
> - Infrastructure topology view in Veeam ONE and Veeam Backup & Replication must match. Otherwise, Veeam ONE Web Client may show invalid data for Veeam Backup & Replication reports and dashboards.
> - To analyze data about replicated VMs in the report, you must connect the target virtualization servers to Veeam ONE. For details on, see Add Data Source.

View Report Example

Use Case

This report allows Veeam Cloud Providers (VCPs) to analyze cloud host and storage configuration and quota usage. The report helps VCPs reveal whether cloud compute and storage resources are approaching their limits, keep an eye on users replicating their workloads to cloud, and decide whether it is necessary to increase users' quotas.

Cluster Configuration (Hyper-V)

This report documents the current configuration of clusters in your infrastructure.

- The **Total CPU (GHz)**, **Total Memory (GB)** and **Total Storage (GB)** charts show the amount of resources allocated to clusters.
- The **Details** table provides information on each cluster, including total number of hosts and VMs in the cluster, total amount of available cluster resources and the name of the cluster host owner.

  Click a number in the **Total Hosts** column to drill down to host configuration details.

  Click a number in the **HA VMs** column to drill down to VM configuration details.
- The **Networking** table provides information on network configuration for each cluster, including subnets, networks, cluster use and the number of VMs.

Report Parameters

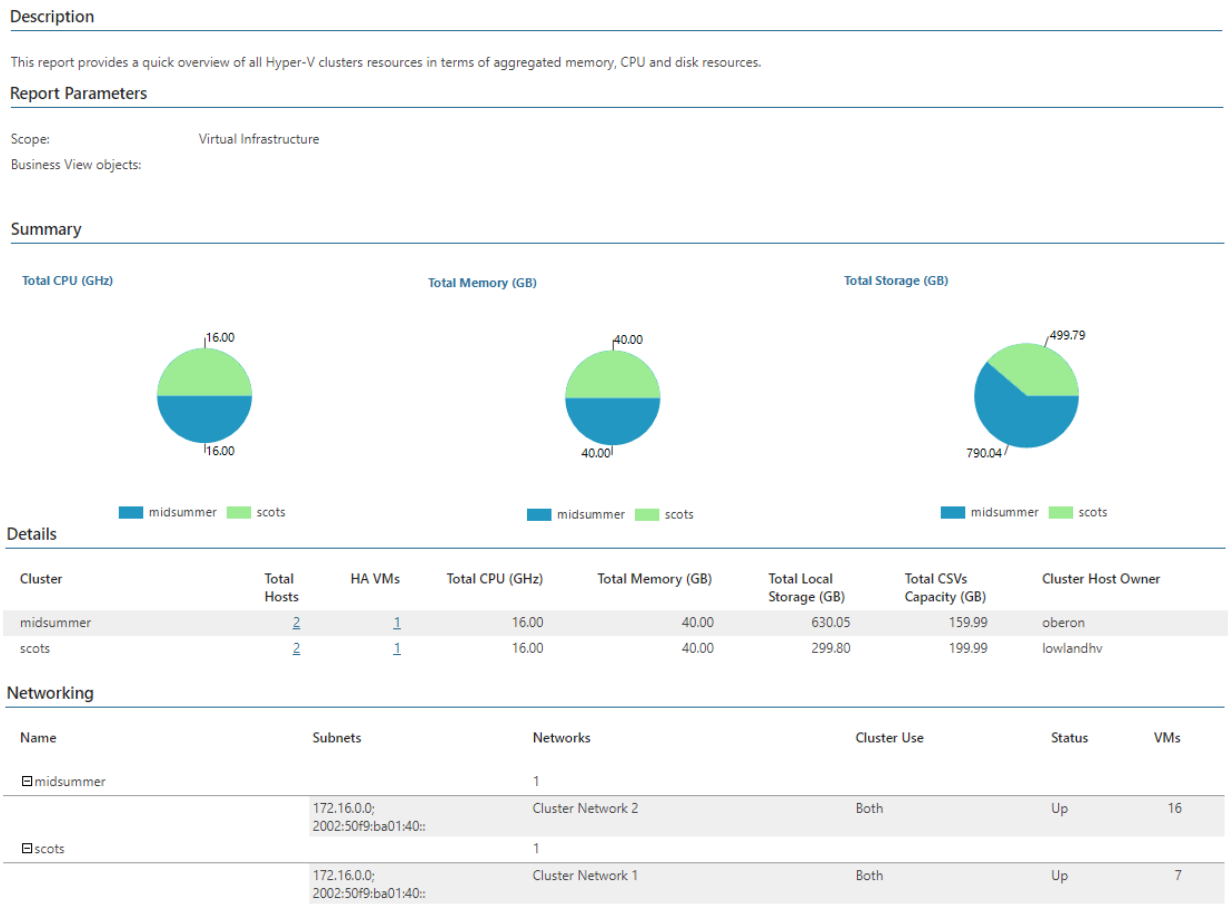
You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.

- **Business View objects**: defines Business View groups to analyze in the report. The parameter options are limited to objects of the Cluster type.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.

Cluster Configuration



Description

This report provides a quick overview of all Hyper-V clusters resources in terms of aggregated memory, CPU and disk resources.

Report Parameters

Scope: Virtual Infrastructure

Business View objects:

Summary

Total CPU (GHz)

Total Memory (GB)

Total Storage (GB)

Details

Cluster	Total Hosts	HA VMs	Total CPU (GHz)	Total Memory (GB)	Total Local Storage (GB)	Total CSVs Capacity (GB)	Cluster Host Owner
midsummer	2	1	16.00	40.00	630.05	159.99	oberon
scots	2	1	16.00	40.00	299.80	199.99	lowlandhv

Networking

Name	Subnets	Networks	Cluster Use	Status	VMs
⊟midsummer		1			
	172.16.0.0; 2002:50f9:ba01:40::	Cluster Network 2	Both	Up	16
⊟scots		1			
	172.16.0.0; 2002:50f9:ba01:40::	Cluster Network 1	Both	Up	7

Use Case

The report allows you to keep an eye on the state of hardware resources provisioned to your clusters, and to verify configuration settings applied to these clusters. This may help you balance workloads and right-size the environment to attain higher performance.

Cluster Configuration (vSphere)

This report documents the current configuration of clusters in your infrastructure.

- The **Summary** section charts provide an overview of cluster resources in terms of memory, CPU and storage utilization.
- The **Details** table provides information on each cluster, including total number of hosts in the cluster, the amount of allocated resources and statuses of HA (High Availability) and DRS (Distributed Resource Scheduler) features.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **Business View objects**: defines Business View groups to analyze in the report. The parameter options are limited to objects of the Cluster type.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.

View Report Example

Use Case

The report allows you to keep an eye on the state of hardware resources provisioned to your clusters, and to verify configuration settings applied to these clusters. This may help you balance workloads and right-size the environment to attain higher performance.

Cluster Hosts Performance

This report aggregates historical data and shows performance statistics for all hosts in selected clusters across a time range. The report features a predefined list of performance counters and allows you to report on memory, CPU, disk and network usage.

- For each host in the cluster, the **Summary** section includes the following elements:
  - The summary table describes configuration of each host in the cluster, including allocated memory and CPU resources and the number of CPU cores and sockets.
  - The resource usage subsections provide information on CPU, memory, disk and network usage and analyzes resource usage trends for each host.

    Click a host name in the summary table or in the resource usage table to drill down to performance charts with statistics on CPU, memory, disk and network usage for the host, and the list of top resource consuming VMs. You can click a VM name in the list to drill down to performance charts with statistics on CPU, memory, disk and network usage for the VM.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **Period**: defines the time period to analyze in the report. Note that the reporting period must include at least one successfully completed *Object properties data collection* task for the selected scope. Otherwise, the report will contain no data.
- **Business hours only**: defines time of a day for which historical performance data will be used to calculate the performance trend. All data beyond this interval will be excluded from the baseline used for data analysis.
- **Metrics**: defines a list of performance counters to analyze in the report.

View Report Example

Use Case

The report provides an overview of hardware resource consumption across your hosts. This information may help you identify hosts with performance issues, balance workloads, right-size resource provisioning, redefine DRS settings and optimize cluster overall performance.

Cluster Performance

This report aggregates historical data and shows performance statistics for a selected cluster across a time range.

- The **Summary** section describes configuration of each host in the cluster, including allocated memory and CPU resources and the number of CPU cores and sockets.
- The **Performance** subsections provide information on CPU, memory, disk and network usage, including usage trends and top resource consuming hosts and VMs in the cluster.

  Click a host name in the summary table or in the list of top resource consuming hosts to drill down to performance charts with statistics on CPU, memory, disk and network usage for the host.

  Click a VM name in the list of top resource consuming VMs to drill down to performance charts with statistics on CPU, memory, disk and network usage for the VM.

Report Parameters

You can specify the following report parameters:

- **Object**: defines the cluster to analyze in the report.
- **Period**: defines the time period to analyze in the report. Note that the reporting period must include at least one successfully completed *Object properties data collection* task for the selected cluster. Otherwise, the report will contain no data.
- **Business hours only**: defines time of a day for which historical performance data will be used to calculate the performance trend. All data beyond this interval will be excluded from the baseline used for data analysis.
- **Top N**: defines the maximum number of hosts and VMs to display in the report output.

View Report Example

Use Case

The report provides an overview of hardware resource consumption for the selected cluster. This information may help you identify clusters with performance issues, balance workloads, right-size resource provisioning, redefine DRS settings and optimize cluster overall performance.

Computer Backup Status

This report provides information on daily backup status for all protected and unprotected computers.

- The **Summary** display contains the **Agents Backup Status** chart that displays the number of jobs whose sessions completed successfully, the number of jobs whose sessions completed with warnings and the number of jobs whose sessions failed. If a job has been launched several times a day, the report shows the best job status. If a job includes multiple computers, each computer has its own status in the chart and the report shows the best result of the job for each agent.
- The **Report Data** display provides a list of protected agents and displays daily job completion results.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a list of Veeam Backup & Replication servers to include in the report.
- **Business View objects**: defines Business View groups to analyze in the report. The parameter options are limited to objects of the Computer type.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.
- **Backup jobs/policies**: defines a list of agent backup jobs to include in the report.
- **Agent types**: defines types of Veeam backup agents to include in the report.
- **Period**: defines a time period to analyze in the report (number of weeks from 1 to 10).
- **Computer inclusion rule**: defines names of computers to include in the report.

View Report Example

Use Case

The report helps you detect failed agent backup jobs, identify jobs that triggered warnings and ensure that protected computers can be easily recovered in case of a disaster.

Computers with no Archive Copy

The main purpose of backup is to protect your data against disasters and agents failures. Having only one copy of a backup file does not provide the necessary level of safety. To build a successful data protection and disaster recovery plan, you must have at least three copies of your data, for example, production data, backup and its copy, and two different types of media to store copies of your data, for example, disk storage and tape.

To learn more about the 3-2-1 backup strategy, see the Veeam Blog article How to follow the 3-2-1 backup rule with Veeam Backup & Replication.

This report highlights all agents that do not have backup copies archived to tapes.

> **NOTE:**
>
> This report does not consider backups stored on cloud backup repositories.

- The **Summary** display includes the following elements:
  - The **Computers Archive Status** chart displays the number of agents with and without archive copy.
  - The **Archive Copies by Location Type** chart displays the types of backup target locations.
  - The **Report Parameters** table provides information on the report's configured parameters.
- The **Report Data** display includes the following elements:
  - **Computers with Archive Copy** displays data about agent jobs for which a backup copy exists within the specified period.
  - **Computers without Archive Copy** displays data about agent jobs for which there is no backup copy within the specified period.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a list of Veeam Backup & Replication servers to include in the report.
- **Business View objects**: defines Business View groups to analyze in the report. The parameter options are limited to objects of the *Computer* type.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.
- **Backup jobs/policies**: defines a list of agent backup jobs to include in the report.
- **Agent types**: defines types of Veeam backup agents to include in the report.
- **Computer inclusion rule**: defines names of computers to include in the report.
- **Last <N> days/weeks/months**: defines the time period to analyze in the report.
- **Show computers with no primary backup within the reporting period**: defines whether to include in the report agents without primary backup that is valid within the defined time period.

View Report Example

Use Case

This report helps backup administrators check whether agents are protected with backup copies stored on secondary backup repositories and on tape.

Configuration Assessment

The report analyzes configuration of the Hyper-V infrastructure against a set of recommended settings and best practices, identifies clusters, hosts and\or VMs that are configured inefficiently and verifies problem areas to help mitigate issues and prepare VMs for backup with Veeam Backup & Replication.

- The **Summary** section includes the following elements:
  - The **Verification Results** chart displays the share of failed and passed verification tests, and tests that completed with warnings.
  - The **Assessment Criteria** table lists criteria used in the report to assess the Hyper-V infrastructure, and shows the assessment results.
- The **Optimization** tables show detailed assessment result for each criterion and provides recommendations on how to improve infrastructure configuration.

The report takes into account the following criteria when analyzing Hyper-V configuration:

Cluster Optimization

Criterion	Description
Hosts use same CPU vendors/models	The report analyzes cluster configuration to make sure clusters include hosts with CPUs of the same vendors. A cluster that includes hosts with CPUs from different vendors may not operate correctly when you perform some tasks in Veeam Backup & Replication. For example, migration or restore of VMs to a host with a different processor may fail as some applications only run on processors of a specific vendor.
Hosts are updated equally	The report verifies that hosts in a cluster have the same Hyper-V version installed. When hosts in a cluster have different Hyper-V versions installed, it may cause compatibility issues and unexpected errors.
Storage controllers are of the same vendors	The report analyzes cluster configuration to verify that storage controllers installed on hosts are of the same vendor. If you have storage controllers of different vendors on hosts in a cluster, you may experience unexpected errors and failures.
NICs compatibility	The report analyzes cluster configuration to verify whether NIC cards within a cluster are of the same vendor. Incompatible NIC cards may cause issues during backup and restore operations in a cluster.

Host Optimization

Criterion	Description
Host is not running on a balanced power plan	The report analyzes host configuration to verify whether hosts in the infrastructure are running on a balanced power plan. The **Balanced** power plan is the default power plan in Windows operating systems. However, to increase host efficiency, you are recommended using the **High Performance** power plan.
No RDP printers mapped	The report analyzes your infrastructure to verify that there are no RDP mapped printers on hosts. Printers mapped through RDP may not work efficiently and may cause unexpected errors and failures. You can disable RDP printer mapping through a group policy.
Virtual CPUs/Logical CPUs ratio	The report analyzes the infrastructure to verify that maximum vCPU per host CPU core ratio is below the specified value. The default ratio is 8. If CPU configuration is not balanced, VMs may not obtain enough processor resources. For information on how to measure processor performance, see this Microsoft article.

VM Optimization

Criterion	Description
Integration Services state	The report analyzes your infrastructure to verify that all Integration Services on VMs in the infrastructure are enabled. Integration Services participate in application-aware image processing during backup in Veeam Backup & Replication. To use application-aware image processing efficiently, enable Integration Services.
Hyper-V VSS Requestor state	The report analyzes the infrastructure to identify the state of VSS Requestor on VMs. If VSS Requestor is not started on a VM, this may cause issues during backup as VSS services will not be able to create a shadow copy and prepare data for backup. If the state of VSS Requestor on a VM is **Started/Automatic or Started/Automatic (Delayed Start)**, the report will show the **Success** verification result. In other cases, the verification result will be **Warning**.

Criterion	Description
No Checkpoints used	The report analyzes the virtual infrastructure to find VMs with existing checkpoints. To use Veeam Changed Block Tracking for incremental backup, you must remove snapshots.
No VMs on datastores with less than 10% of free space	The report analyzes the Hyper-V infrastructure to find datastores that have less than 10% of free space. During backup Veeam Backup & Replication triggers a checkpoint that is normally stored next to VM files on the source datastore. To eliminate the problem of datastores running low on free space during backup, it is required that the free space is more than 10%.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **Business View objects**: defines Business View groups to analyze in the report. The parameter options are limited to objects of the Cluster type.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.
- **Objects to assess**: defines types of objects to analyze in the report.

- **Max vCPUs per physical core**: defines the threshold for the maximum number of vCPU cores per a single instance of the physical CPU core.

Configuration Assessment

Description

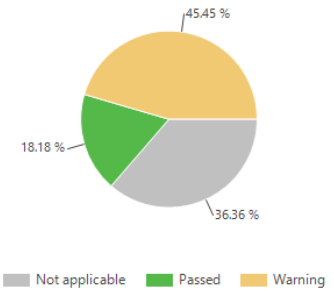
This report helps you to assess your Hyper-V configuration and identify potential configuration improvements.

Report Parameters

Scope:	Virtual Infrastructure
Business View objects:	
Objects to assess:	All items
Max vCPUs per physical core:	8

Summary

Verification Results



Assessment Criteria	Verification Results
Criteria Group: Cluster optimization	**Not applicable**
Hosts use same CPU vendors / models	Not applicable
Hosts are updated equally	Not applicable
Storage controllers are of the same vendor	Not applicable
NICs compatibility	Not applicable
Criteria Group: Host optimization	**Warning**
Host is not running on a balanced power plan	Warning
No RDP printers mapped	Warning
Virtual CPUs / Logical CPUs ratio	Passed
Criteria Group: VM optimization	**Warning**
Integration Services state	Warning
Hyper-V VSS Requestor state	Warning
No Checkpoints used	Warning
No VMs on datastores with less than 10% of free space	Passed

Host Optimization

Host Is Not Running on A Balanced Power Plan

Recommendation: For better host performance in POWERCFG.EXE/S SCHEME_MIN to change "min" to "max".

Host	Cluster	Balanced Power Plan Is Disabled	Verification Result
pdctwhv01.tech.local	-	False	Warning

No RDP Printers Mapped

Recommendation: Use Group Policy to disable remote desktop printer mapping on the Hyper-V hosts.

Host	Cluster	RDP Client Printer Mapping Is Disabled	Verification Result
pdctwhv01.tech.local	-	False	Warning

Virtual CPUs / Logical CPUs Ratio

Recommendation: Your Hyper-V infrastructure meets all known best practices.

Host	Cluster	VP/LP Ratio	Verification Result
pdctwhv01.tech.local	-	0.77	Success

Use Case

This report shows a list of clusters, hosts and VMs in your virtual environment that could experience potential issues during backup, gets guidance on how to resolve these issues.

Current Backup Alarms State Overview

This report shows all unresolved alarms that Veeam ONE Client triggered for the Veeam Backup & Replication infrastructure.

- The **Summary** display includes the following elements:
  - The **Total Issues Number** chart shows the total number of alarms specified in the **Alarm Status** parameter.
  - The **Top 10 Issues** table displays 10 most frequent unresolved alarms, their status, and how many times they were triggered.
- The **Report Data** display shows objects names, backup servers, object types, names of triggered alarms, their status, repeat count, triggering events and time, and affected backup infrastructure objects.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a list of Veeam Backup & Replication servers to include in the report.
- **Alarms statuses**: defines statuses of alarms to display in the report (*Acknowledged*; *Error*; *Error, Warning*; *Error, Warning, Acknowledged*).

View Report Example

Use Case

You can use this report to detect and resolve current and the most pressing issues with Veeam Backup & Replication.

Custom Infrastructure

This report features a collection of custom properties and filters to help you analyze virtual infrastructure aspects not covered by other reports.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **Business View objects**: defines Business View groups to analyze in the report.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.
- **Object type**: defines a list of infrastructure objects to analyze in the report.
- **Columns**: defines configuration properties to analyze in the report. The list of available properties will depend on the selected object type. Use the **Filter** field to search for the necessary properties by name. Note that the number of selected properties must not exceed 50.
- **Custom filters**: defines filters for the selected object properties.
- **Group by**: defines whether infrastructure objects in the report must be grouped based on the value of a specific property. To group infrastructure objects by property value, select that property from the **Group by** drop-down list.

  You can also use the Sum, Max or Count function to calculate aggregate values of other properties for each group in the report. To do that, select the necessary aggregate functions for required properties in the list.
- **Sort by**: defines how data will be sorted in the report.
- **Show all groups expanded**: defines whether the report should display results in the collapsed or expanded view.

View Report Example

Use Case

Use the advanced collection of properties to report on licensing information, host hardware configuration, CPU, RAM, storage and networking performance, and many other aspects to better manage the virtual infrastructure.

Data Change Rate History

This report allows you to track backup and replication jobs and workloads whose backup files and replicas grow too fast and may quickly consume storage space on the target repository or target datastore.

- The **Change Rate History** chart shows percentage of VMs and computers data changes that took place during the reporting period.
- The **Objects with Largest Change Rate (GB)** and **Objects with Least Change Rate (GB)** charts displays the most and least active VMs and computers in terms of the amount of data changes that occurred on their virtual disks.
- The **Details** table provides information on the list of workloads included in the backup and replication jobs, the average and aggregate amount of data changes that took place during the reporting period, the number of full backups and increments, and the size of the current full backup file*.

  Click a VM name to drill down to change rate statistics for each day of the reporting period.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **VM folders**: defines a list of VMware folders to include in the report (applies to VMware vSphere environments only). VM folders is an alternate way to present the virtual infrastructure. If VMs in your infrastructure are grouped into folders according to their profile, you can limit the report scope by specifying the necessary folders only.
- **VMware Cloud Director objects**: defines VMware Cloud Director components to analyze in the report.
- **Business View objects**: defines Business View groups to analyze in the report. The parameter options are limited to objects of the Virtual Machine type.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.
- **Backup Infrastructure objects**: defines Veeam Backup & Replication servers to analyze in the report.
- **Period**: defines the time period to analyze in the report.
- **Job types**: defines a job type to evaluate in the report (*VM Backup*, *Replication*, *Agent backup policy*, *Agent backup*, *All items*).
- **Exclude jobs**: defines a list of backup and replication jobs to exclude from the report.
- **Calculate change rate based on**: defines the way change rate will be calculated in the report (based on *Data transferred* or *Data read*).

> **NOTE:**
>
> Infrastructure topology view in Veeam ONE and Veeam Backup & Replication must match. Otherwise, Veeam ONE Web Client may show invalid data for Veeam Backup & Replication reports and dashboards.

View Report Example

Use Case

To perform incremental backup, Veeam Backup & Replication needs to know which data blocks have changed since the previous job run. For VMware VMs with hardware version 7 or later, Veeam Backup & Replication employs VMware vSphere Changed Block Tracking (CBT) — a native VMware feature that backs up only the list of VM blocks that have changed since the last run of this particular job. Use of CBT reduces backup session duration, and increases the speed and efficiency of block-level incremental backups.

The report analyzes changes occurred on VM disks and estimates the amount of changed data. This can help you decide whether to allocate more space on the target repository or datastore in case VM files grow too fast.

The report is also handy for people planning to do replication as a way to figure out if their bandwidth can handle the replication.

*Note that no data will be available for synthetic or reversed backup, as well as for replicas.

Data Sovereignty Overview

This report lists all protected objects, backups and replicas grouped by location.

- The **Summary** display contains charts that display locations of production data, their backups, backup copies and replicas.
- The **Report Data** display shows the following:
  - The **Backup Infrastructure Objects** table lists all objects of a backup infrastructure and their locations.
  - The **Data Location** table shows details on the location of backups, backup copies and replicas for data sources grouped by production data location.

Report Parameters

You can specify the following report parameters:

- **Infrastructure Objects**: defines a list of Veeam Backup & Replication servers to include in the report.
- **VM and computer locations**: defines a list of locations configured on monitored Veeam Backup & Replication servers.

> **NOTE:**
>
> Infrastructure topology view in Veeam ONE and Veeam Backup & Replication must match. Otherwise, Veeam ONE Web Client may show invalid data for Veeam Backup & Replication reports and dashboards.

View Report Example

Use Case

Veeam Backup & Replication supports a notion of location which you can assign to virtual infrastructure, backup infrastructure and agent management objects. Location settings helps to monitor where production data and their copies and replicas reside geographically.

The report analyzes the location of backups, backup copies and replicas for a data source and displays it as pie charts. This visual representation will help you monitor your data in a geographically disperse infrastructure.

Data Sovereignty Violations

This report shows potential data sovereignty violations by listing all protected objects with backups or replicas residing in a different location.

- The **Summary** display contains charts that display the sovereignty violations of production data, their backups, backup copies and replicas.
- The **Report Data** display contains the **Data Sovereignty Violations** tables that show details on the location mismatch of backups, backup copies, tapes and replicas for a data source grouped by Veeam Backup & Replication server name. The **Objects with no Location Tag** table displays all objects in the infrastructure that have no location tag grouped by the type of object.

Report Parameters

You can specify the following report parameters:

- **Scope**: defines a list of Veeam Backup & Replication servers to include in the report.
- **Protection types**: defines a list of Veeam Backup & Replication jobs to include in the report.
- **Workload types**: defines whether physical computers or virtual machines are included in the report.

> **NOTE:**
>
> Infrastructure topology view in Veeam ONE and Veeam Backup & Replication must match. Otherwise, Veeam ONE Web Client may show invalid data for Veeam Backup & Replication reports and dashboards.

View Report Example

Use Case

Veeam Backup & Replication supports a notion of location which you can assign to virtual infrastructure, backup infrastructure and agent management objects. Location settings helps to monitor where production data and their copies and replicas reside geographically.

The report analyzes whether any backups, backup copies and replicas reside in a location different from a data source and displays results as pie charts. This visual representation will help you identify which jobs and objects violate data protection regulations accepted in your organization.

Database Log Protection History

This report provides historical overview of all database log backup jobs. It also includes the list of protected and unprotected databases for each virtual and physical machine. The report helps you ensure that critical databases are properly protected and that transaction logs for these databases have been successfully backed up.

A database is considered to be *Protected* if it was backed up at least once during the last backup job session. A database is considered to be *Unprotected* if it was not backed up during the last backup job session.

- The **Summary** display includes the following elements:
  - The **Databases by Protection State** chart shows the number of protected and unprotected databases and databases excluded from processing.
  - The **SLA** chart shows how many log backup intervals within the specified RPO period completed with successful log shipment (in percentage).
  - The **Job Sessions by Status** chart shows results of job sessions.
  - The **Summary** panel shows the number of configured backup jobs, the total number of VMs and computers included in these jobs, the number of processed application servers and clusters, and the total number of hosted databases.
- The **Details** table provides additional information on the efficiency of executed jobs, number of protected, unprotected and excluded databases, number of missed intervals, actual difference between configured log backup interval and time actually required.
- The **Backup Copy Job Details** table provides information about each backup copy job. This table helps users monitor job progress and troubleshoot issues with backup copy operations.
- The **Database Protections Details** table provides protection details for monitored databases. This table enables users to verify database backup coverage and identify databases that may require attention.

> **NOTE**
>
> Values displayed in the SLA column on this report are for the average of the selected period, not the latest session.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a list of Veeam Backup & Replication servers to include in the report.
- **Database types**: defines a list of database types to include in the report (*Microsoft SQL*, *Oracle Database*, *PostgreSQL*, *SAP HANA*, *SAP on Oracle, SAP on MaxDB*).
- **Job types**: defines the types of jobs that can be selected to include in the report (*VM backup*, *Agent backup*, *Agent backup policy*, *Application backup policy*).
- **Backup jobs**: defines a list of backup jobs to include in the report. Note that the report will include information on Oracle backup jobs only for Veeam Backup & Replication servers version 11 or later.
- **Show backup copy (immediate copy) jobs**: defines whether to include information on immediate backup copy jobs in the report.
- **Interval**: defines the time period to analyze in the report.

View Report Example

Use Case

A database is a software component that is mission critical for a modern enterprise. The role of database management is constantly expanding, that is why you need to be sure that your databases are safely protected.

The report allows you to track historical statistics for SQL and Oracle backup jobs, ensure that the configured jobs allow you to meet the desired SLA requirements.

> **NOTE**
>
> This report supports SQL, PostgreSQL and Oracle database log backup jobs and Enterprise Application plugins.

Database Processing Verification

This report assesses application servers and application clusters added to the protection groups of Veeam Enterprise Application Plug-ins and lists databases with the information on whether these databases were processed or not.

- The **Summary** section includes information on the total number of processed and unprocessed databases and number of databases of each platform. Also the section includes the following elements:
  - The **Databases by Processing State** chart shows the number of processed and unprocessed databases.
  - The **Databases by Latest Data Backup Session Status** chart shows the number of databases with each status of the latest backup session.
  - The **Databases by Platform by Processing State** chart shows the number of processed and unprocessed databases of each platform.
- The **Details** table provides information on processed and unprocessed databases: servers or clusters on which the databases reside, database platforms, protection groups that include databases, backup policies that protect databases, backup repository that stores the database backups, number of backup sessions, date and time of the latest backup session, status of the latest backup session, date and time of the latest log backup session.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a list of Veeam Backup & Replication servers to include in the report.
- **Business View objects**: defines Business View groups to analyze in the report.
- **RPO**: defines the maximum amount of data that you may accept to lose, expressed in time. RPO defines the age of the latest backup or replica files required to resume normal operation if system failure occurs. For example, to compile a list of VMs protected on a daily basis, you need to set the RPO value to 1 day or 24 hours.
- **Platforms**: defines a list of database platforms to include in the report (*Oracle Database*, *SAP HANA*, *SAP on Oracle, Microsoft SQL Server*).
- **Backup policies**: defines a list of backup policies protecting the databases to include in the report.
- **Database exclusion rule**: defines a list of databases that should be excluded from the report scope. You can enter database names explicitly or create a wildcard mask by using the asterisk (*) to replace any number of characters. Multiple entries are separated by semicolon. For example, the following string will exclude databases with the _R&D suffix from appearing in the report: **_R&D*.

View Report Example

Use Case

A database is a software component that is mission critical for a modern enterprise. The role of database management is constantly expanding, that is why you need to be sure that your databases are safely protected.

The report helps to identify databases that were not added to or were not successfully processed by backup policies.

Datastore Capacity

This report helps administrators evaluate available datastore capacities across the infrastructure.

- The **Storage Overview (Top N)** chart shows top datastores with the greatest amount of used disk space.

  Click the **Details** link at the bottom of the chart to drill down to the list of datastores that includes details on total storage capacity, the amount of free and used space, and the number of VMs that reside on these datastores.

- The **Virtual Disks Capacity (Top N)** chart shows top VMs with the greatest virtual disk size.

  Click the **Details** link at the bottom of the chart to drill down to the full list of VMs that includes details on total virtual disk size, snapshot size, and the power state of these VMs.

- The **Logical Disks (Top N)** chart shows top VMs with greatest logical disk size.

  Click the **Details** link at the bottom of the chart to drill down to the full list of VMs that includes details on total logical disk capacity, the amount of free and used space, and the power state of these VMs.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **Business View objects**: defines Business View groups to analyze in the report. The parameter options are limited to objects of the Storage type.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.

- **Top N**: defines the number of top datastores, virtual and logical disks that will be displayed in the report charts.

View Report Example

Use Case

The report helps you monitor storage capacities to ensure your VMs have sufficient room to operate.

Datastore Configuration (Hyper-V)

This report documents the current configuration of CSVs, SMB shares and local disks in your infrastructure.

- The **Summary** section includes the following elements:
  - The **Utilization (%)** chart shows the percentage of used and free space on all datastores.
  - The **Provisioned Space (GB)** chart shows datastore capacity and the amount of provisioned space.
  - The summary table provides information on each volume, including owner name, total capacity, free and provisioned space, provisioning ratio and free space utilization trend.

    Click a link in the **Free Space Trend** column to drill down to daily information on total capacity, the amount of used and provisioned space, and the number of VMs that store data on the CSV/SMB share/local disk.
- The **Top N VMs** section provides information on top space consuming VMs, including VM name, number of disks and the amount of used space.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **Business View objects**: defines Business View groups to analyze in the report. The parameter options are limited to objects of the Storage type.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.

- **Top N VMs:** defines the number of top virtual machines that will be displayed in the report charts.

Datastore Configuration

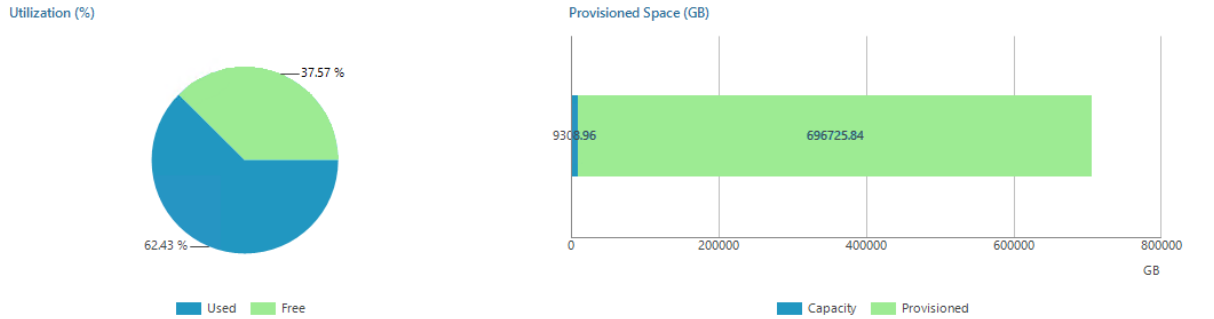
Description

This report provides information about Hyper-V datastore type and other general information including total capacity, free and provisioned space.

Report Parameters

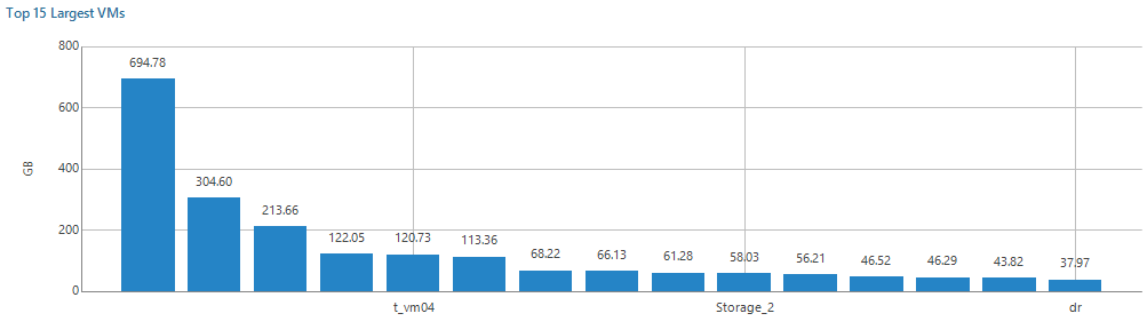
Scope: Virtual Infrastructure
Business View objects:
Top N VMs: 15

Summary



Name	Owner	Capacity (GB)	Free Space (GB)	Provisioned Space (GB)	Provisioning Ratio (%)	Free Space Trend
Disk 0 C: D: E:	hyperv02	4654.48	1070.44	563042.55	12096.78	Increasing
Disk 0 C: D: E:	hyperv01	4654.48	2427.09	133683.29	2872.14	Decreasing

Top 15 VMs



VM Name	Number of Disks	Space Used (GB)
fileserver04	1	694.78
Storage_3	1	304.60
repo30	1	213.66
Storage_1	1	122.05
t_vm04	1	120.73
MSSQLSERVER	1	113.36
prod	1	68.22
winsrv22	1	66.13
sampledb	1	61.28
Storage_2	1	58.03
BETA	1	56.21
veeamcol1	1	46.52
wan31	1	46.29
ORACLEDBLINUX	1	43.82
dr	1	37.97

Use Case

The report helps you monitor storage capacities to ensure your VMs have sufficient room to operate.

Datastore Configuration (vSphere)

This report documents the current configuration of datastores in your infrastructure.

- The **Summary** section includes the following elements:
  - The **Utilization (%)** chart shows the amount of free and used space on datastores.
  - The **Provisioned Space (GB)** chart shows datastores capacity and the amount of space provisioned to VMs.
  - The summary table provides configuration details for each datastore, including the datastore capacity, amount of free space, amount of provisioned space, provisioning ratio (datastore capacity against provisioned space) and free space usage trend.

    Click a hyperlink in the **Free Space Usage Trend** column table to drill down to daily information on total capacity, the amount of used and provisioned space, and the number of VMs residing on the datastore.
- The **Top 3 VMs** section shows VMs that consume more storage space than other VMs.
- The **General Information** table provides information about the datastore owner, datastore type, file system, block size, and the number of VMs residing on the datastore.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **Business View objects**: defines Business View groups to analyze in the report. The parameter options are limited to objects of the Storage type.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.

View Report Example

Use Case

The report helps you monitor storage capacities to ensure your VMs have sufficient room to operate.

Datastore Performance

This report aggregates historical data and shows performance statistics for a selected datastore across a time range.

- The **Summary** subsection provides information on type, capacity, free space, number of VMs and VM templates.
- The **Datastore IOPs**, **Datastore Usage**, **Datastore Latency** and **Datastore Errors** subsections provide information on IOPs, read/write rates, read/write latency and errors for the disk, including top 3 resource consuming VMs and resource usage trends.

  Click a VM name in the list of top 3 resource consuming VMs to drill down to performance charts with statistics on CPU, memory, disk and network usage for the VM.

Report Parameters

You can specify the following report parameters:

- **Object**: defines the datastore to analyze in the report.
- **Period**: defines the time period to analyze in the report. Note that the reporting period must include at least one successfully completed *Object properties data collection* task for the selected datastore. Otherwise, the report will contain no data.

- **Business hours only**: defines time of a day for which historical performance data will be used to calculate the performance trend. All data beyond this interval will be excluded from the baseline used for data analysis.

Datastore Performance

Description

This report shows datastore performance history that includes Usage, Latency and IOPS counters.

Report Parameters

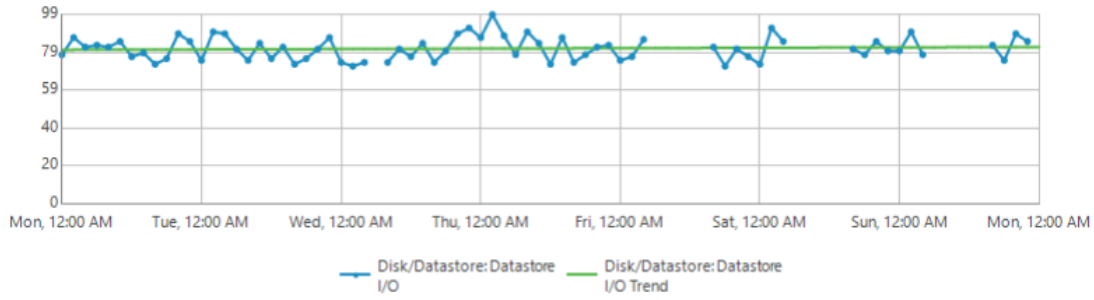
Selected object:	prgtwesx01-ds01
Object location:	\\Virtual Infrastructure\vcenter01.tech.local\Prague
Reporting period:	1/2/2023 - 1/8/2023

Summary

Name:	prgtwesx01-ds01
Type:	local storage
Capacity:	3.6TB
Free space:	701.4GB
Virtual machines:	26
VM templates:	0

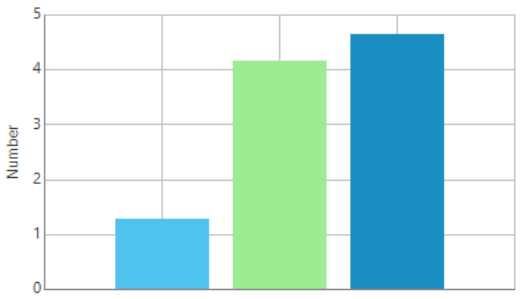
Datastore IOPs

Disk/Datastore: Datastore I/O (Number)

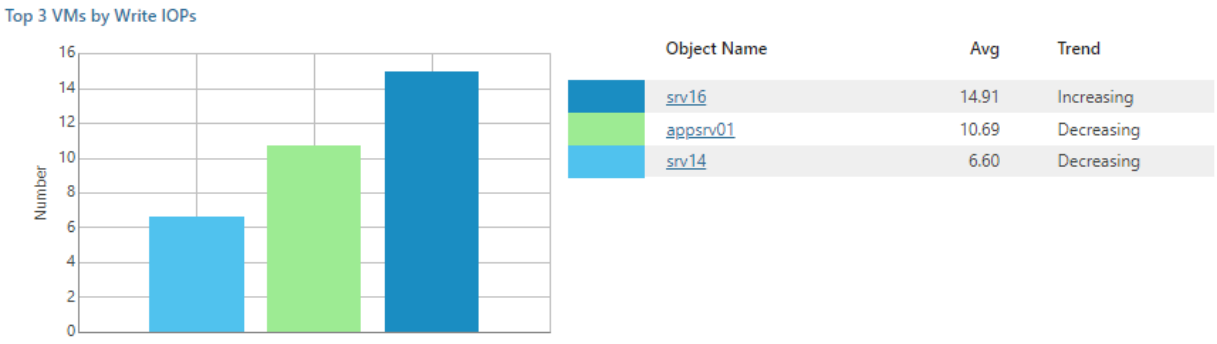


Object Name	Average	Minimum	Maximum	Std. Deviation	Trend
prgtwesx01-ds01	81.22	72.00	99.00	5.99	Increasing

Top 3 VMs by Read IOPs



Object Name	Avg	Trend
srv16	4.63	Increasing
srv14	4.15	Decreasing
serv04_release	1.28	Increasing



Use Case

The report helps you assess current load on your datastores and identify performance issues, such as excessive bus resets or high command aborts rates.

Datastore Performance Assessment

This report analyzes datastore performance and detects whether your datastores can sustain the current workload.

- The **Assessment Results** table shows the number of hosts connected to each datastore included in the report scope, the number of VMs that store data on the datastores, the number of virtual disks, and the average latency/IOPS values for each datastore. The report also provides recommendations on how to meet the defined parameters.
- The **Top Datastores by Latency**, **Top Datastores by IOPS**, **Bottom Datastores by Latency** and **Bottom Datastores by IOPS** charts show 5 most and least loaded datastores in terms of the highest and the lowest IOPS and latency values.
- The **Details** sections show performance charts with IOPS and latency statistics for each datastore, and details tables with latency and IOPS values for every host connected to the datastore.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **Datastores**: defines the datastore to analyze in the report.
- **Interval**: defines the time period to analyze in the report.
- **Read latency (max) threshold**: defines a threshold for the highest latency value for read operations. If the average read latency value for a datastore breaches the threshold, the datastore will be highlighted with red.
- **Write latency (max) threshold**: defines a threshold for the highest latency value for write operations. If the average write latency value for a datastore breaches the threshold, the datastore will be highlighted with red.
- **Read operations count (max) threshold**: defines a threshold for the maximum number of read operations. If the number of read operations for a datastore breaches the threshold, the datastore will be highlighted with red.
- **Write operations count (max) threshold**: defines a threshold for the maximum number of write operations. If the number of write operations for a datastore breaches the threshold, the datastore will be highlighted with red.

View Report Example

Use Case

Veeam Backup & Replication provides Backup I/O Control, a capability that allows you to define latency and IOPS thresholds for any datastore:

- The **Stop assigning new tasks to datastore at** option means that when the backup server is assigning a proxy for the virtual disk, it will take latency (IOPS) into consideration, and the backup job will wait for the datastore to become free before starting the backup.

- The **Throttle I/O existing tasks at** option is designed for situations when a backup job is already running and latency becomes an issue due to an external load. For example, if a SQL maintenance process were to start running in a VM using the same datastore as the backup job, then the backup job will automatically throttle its read I/O from the datastore so that latency drops below the specified threshold.

The report helps you assess current load on your datastores and make sure that by specifying the certain thresholds in Veeam Backup & Replication you maximize possible backup performance while minimizing the impact on production workloads.

Datastore Space Usage History

This report analyzes the amount of space consumed by files of VMs on datastores and helps evaluate available datastore resources in the infrastructure.

- The **Summary** section includes the following elements:
  - The **Datastores with Most Free Space** and **Datastores with Least Free Space** charts display top datastores with the smallest and the largest amount of used space.
  - The **Most Growing Datastores** and **Least Growing Datastores** charts display top datastores with smallest and largest decrease in free space during the specified time period.
- The **Details** table shows datastore space usage statistics and the total number of VMs residing on datastores.

  Click a datastore name to drill down to the **Datastore Usage History** chart that shows how the amount of free, used and provisioned space has been changing during the reporting period.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **Business View objects**: defines Business View groups to analyze in the report. The parameter options are limited to objects of the Storage type.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.
- **Period**: defines the time period to analyze in the report. Note that the reporting period must include at least one successfully completed *Object properties data collection* task for the selected scope. Otherwise, the report will contain no data.
- **Group by**: defines how data will be grouped in the report output (by *Virtual Server* or *Datacenter*).

View Report Example

Use Case

The report helps you monitor storage capacities to ensure your VMs have sufficient room to operate.

Delegated Restore Permissions Overview

This report analyzes restore permissions configured in Veeam Backup Enterprise Manager.

- The **Details** section displays the list of users who can restore entire VMs, guest OS files and application items with the Veeam Backup Enterprise Manager or Veeam Self Service File Restore portal, and shows what type of data these users can restore according to the effective policies.

Report Parameters

You can specify the following report parameters:

- **Enterprise Manager servers**: defines a list of Veeam Backup Enterprise Manager servers to include in the report.

View Report Example

Use Case

Auditing of restore permissions manually can be quite a challenge, especially for large environments with dozens of restore operators. This may cause inefficient resource usage and unwarranted or uncoordinated restores.

This report allows backup administrators and senior IT management staff to review and adjust restore policies to better address the demands of a dynamic multi-user backup environment.

Exported Tapes

The report provides inventory information on tapes exported from tape libraries connected to Veeam Backup & Replication servers.

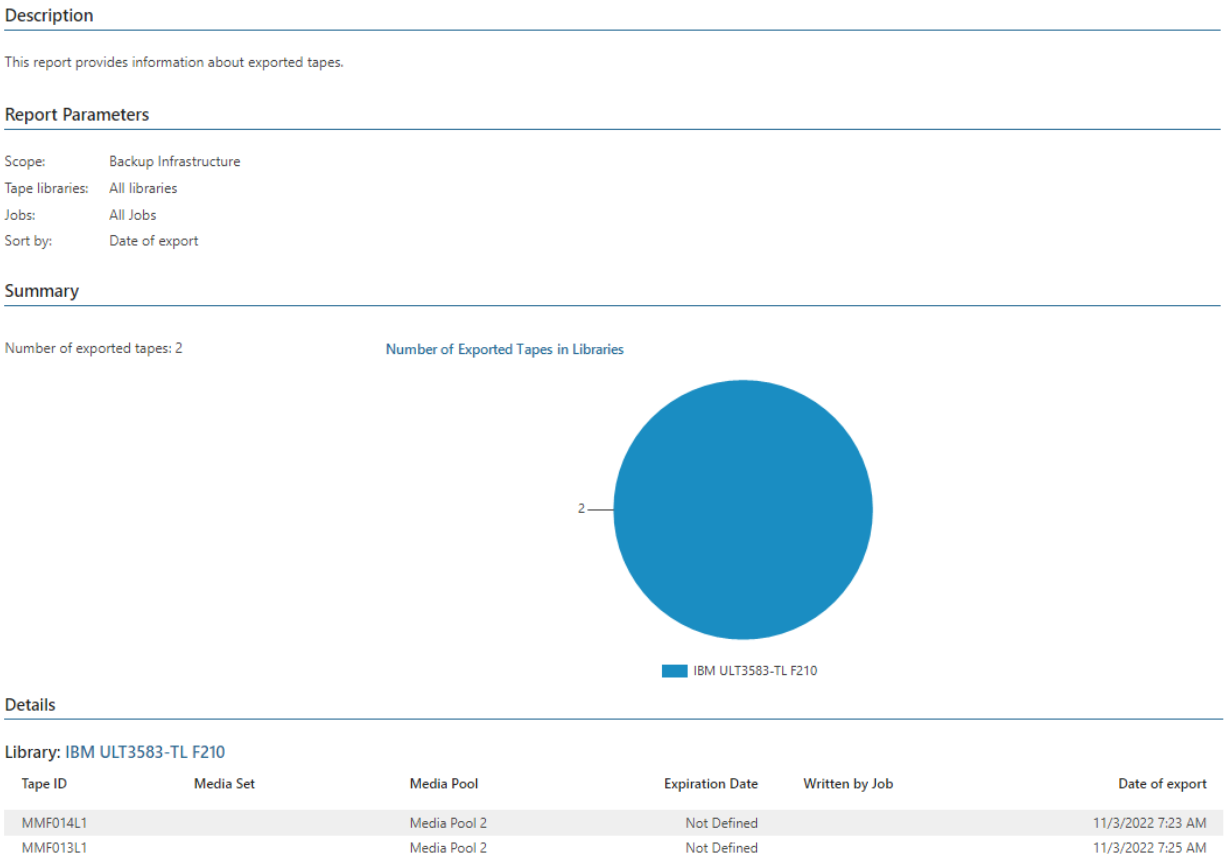
- The **Summary** section shows the total number of exported tapes.
- The **Number of Exported Tapes in Libraries** chart displays how many tapes were exported from connected libraries.
- The **Details** table provides information on each tape library, including a list of all exported tapes, their IDs, media sets and media pools, backup job and exportation date and time.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a list of Veeam Backup & Replication servers to include in the report.
- **Tape libraries**: defines tape libraries to include in the report.
- **Jobs**: defines a list of tape jobs to analyze in the report.

Exported Tapes



Description

This report provides information about exported tapes.

Report Parameters

Scope: Backup Infrastructure
Tape libraries: All libraries
Jobs: All Jobs
Sort by: Date of export

Summary

Number of exported tapes: 2

Number of Exported Tapes in Libraries

Details

Library: IBM ULT3583-TL F210

Tape ID	Media Set	Media Pool	Expiration Date	Written by Job	Date of export
MMF014L1		Media Pool 2	Not Defined		11/3/2022 7:23 AM
MMF013L1		Media Pool 2	Not Defined		11/3/2022 7:25 AM

Use Case

The report allows you to trace tapes exported from tape libraries. You can use this report to find the necessary backup files on tape.

Failover Cluster Performance

The report analyzes performance history of the failover cluster hosts and delivers statistics on CPU, memory disk and network usage over the specified reporting period.

- The **Summary** section describes configuration of each host in the cluster, including allocated memory and CPU resources and the number of CPU cores and sockets.
- The **Performance** subsections provide information on CPU, memory, disk and network usage, including usage trends and top resource consuming hosts and VMs in the cluster.

  Click a host name in the summary table or in the list of top resource consuming hosts to drill down to performance charts with statistics on CPU, memory, disk and network usage for the host.

  Click a VM name in the list of top resource consuming VMs to drill down to performance charts with statistics on CPU, memory, disk and network usage for the VM.

Report Parameters

You can specify the following report parameters:

- **Object**: defines a cluster to analyze in the report.
- **Period**: defines the time period to analyze in the report. Note that the reporting period must include at least one successfully completed *Object properties data collection* task for the selected cluster. Otherwise, the report will contain no data.
- **Business hours from - to**: defines time of a day for which historical performance data will be used to calculate the performance trend. All data beyond this interval will be excluded from the baseline used for data analysis.

- **Top N**: defines the maximum number of hosts and VMs to display in the report.

Failover Cluster Performance

Description

This report shows cluster host performance history that includes CPU, Memory, Disk and Network counters.

Report Parameters

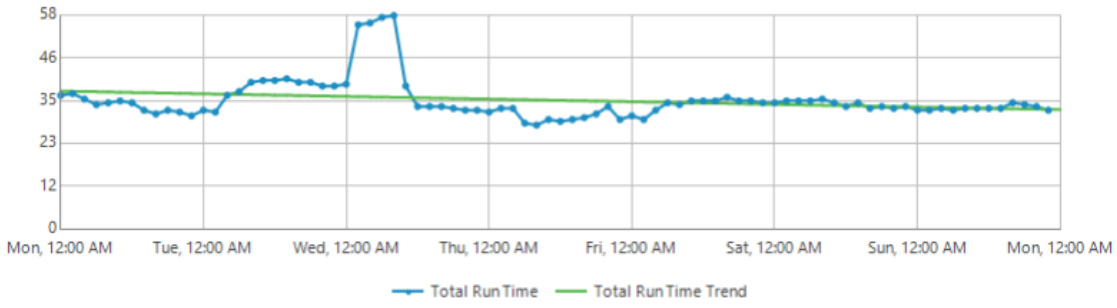
Selected object:	ms-cluster.tech.local
Object location:	\\Virtual Infrastructure
Reporting period:	12/19/2022 - 12/25/2022
Top N:	3

Summary

Host Name	Memory Size, GB	Total CPU, GHz	Cores	Sockets
ms-node-01	16	4.8	2	1
ms-node-02	16	4.8	2	1
Total:	**32**	**9.6**	**4**	**2**

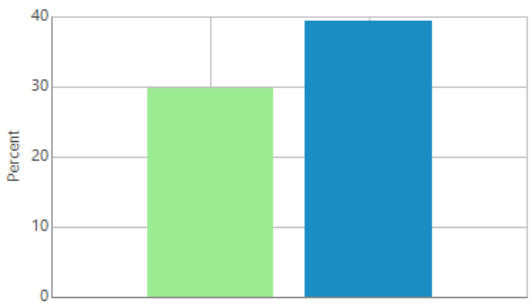
CPU Performance

Total Run Time (Percent)



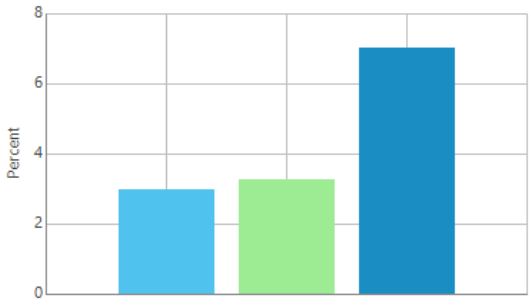
Object Name	Average	Minimum	Maximum	Std. Deviation	Trend
ms-cluster.tech.local	34.67	28.00	57.50	5.58	Decreasing

Top 3 Hosts by Total Run Time



Object Name	Avg	Trend
ms-node-02	39.46	Decreasing
ms-node-01	29.88	Decreasing

Top 3 VMs by Total Run Time



Object Name	Avg	Trend
win19-dyn	7.02	Decreasing
ms-19-1	3.25	Increasing
win19-static	2.96	Decreasing

Use Case

The report shows resource consumption data for the selected cluster within a specified reporting period. You can use this data to detect clusters with performance issues, review resource provisioning, adjust workloads and optimize cluster overall performance.

Garbage Files

This report shows an overview of storage consumed by files that do not belong to VMs comprised in the infrastructure inventory.

- The **Summary** chart displays total amount of free space, amount of space consumed by non-garbage files and amount of space consumed by garbage files on datastores from the selected scope (in percentage).
- The **Details** table shows the full list of datastores with folders that contain garbage files.

  Click a folder name in the details table to drill down to the list of garbage files in the folder.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **Business View objects**: defines Business View groups to analyze in the report. The parameter options are limited to objects of the Storage type.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.

> **NOTE:**
> - You can exclude specific datastores from this report. This can be useful when you are not interested in examining particular datastores for garbage files (for example, local datastores, datastores hosting ISO files or backups). In this case, you can exclude unnecessary datastores from the collection scope. For more information, see Choosing Datastores to Report On.
> - If you run the Garbage Files report with **Veeam backup data and large-scale virtual infrastructure performance monitoring** mode selected, no data will display in the report. For more information on data collection modes, see Scalability and Choose Data Collection Mode.

View Report Example

Use Case

If a VM was improperly deleted or relocated, or if a snapshot operation failed, some residual elements belonging to the VM may remain on the datastore.

This report allows you to check your infrastructure for garbage files that waste storage space and impact ROI.

GFS Backup Files

This report provides historical information about restore points for Veeam Backup & Replication jobs with the Grandfather-Father-Son (GFS) retention policy.

- The **Summary** section provides information about jobs configured with the GFS retention policy, the number of historical backup files, restore points in these files and the amount of space occupied by historical backup files.
    - The **Restore Points Age** chart shows the share of weekly, monthly and yearly restore points.
    - The **Top 5 Jobs by Number of Restore Points** chart displays 5 jobs with the greatest number of GFS restore points.
- The **Next Restore Points to Be Deleted by Retention** table shows restore points that will soon be deleted according to the retention policy, as well as their size, type and objects they contain.

  Click a job name to drill down to the job details section.
- The **Job** subsections display information about jobs with GFS retention policy: job retention configuration, a list of existing restore points and their details. You can also view distribution of GFS restore points of all types for the current calendar year.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a list of Veeam Backup & Replication servers to include in the report.
- **Job types**: defines a job type to evaluate in the report (*VM backup*, *Backup copy*, *Agent backup*, *Agent backup policy*, *All items*).
- **Jobs**: defines a list of jobs to analyze in the report.

View Report Example

Use Case

If you have a large backup infrastructure with a great number of restore points with GFS retention policy, you may find it difficult to track these points. The report allows you to inventory restore points created with the GFS retention policy, and check what restore points will soon be removed by retention.

Guest Disk Free Space (Hyper-V)

The report provides information on the amount of free disk space for VM guest OS.

NOTE:

- To view the report, you must specify guest OS credentials for the guest OS of Microsoft Hyper-V VMs. For details, see Specify VM Guest OS Credentials.
- The report includes information only for VMs running Windows guest OSes.

The report analyzes VM guest disks and displays their capacity, the amount of guest disk free space, shows disk space usage trends, and predicts how many days are left for a disk to reach the specified threshold.

- The **Summary** section provides an overview of analyzed VM guest disks, shows how many VMs will run out of disk resources sooner than other VMs, and shows average disk growth trends.
- The **Disks to reach threshold first** table displays a list of VMs that will run out of guest disk space sooner than other VMs. For each VM, the table shows guest disk capacity and the amount of free space left, daily disk growth trend and the number of days left before the occupied disk space will reach 90% and 100% of its capacity.

  If a value in the **Days to reach 90%** or **Days to reach 100%** column is highlighted with red, a disk will reach the specified threshold in less than 180 days.
- The **Top 10 Partitions by Relative Space Growth** chart shows 10 guest disks that used the greatest amount of space over the reporting period in relative terms (amount of occupied disk space against the disk capacity).
- The **Top 10 Partitions by Absolute Space Growth** chart shows 10 guest disks that used more space over the reporting period in absolute terms (amount of occupied disk space in GB).
- The **Guest Disk Free Space (GB)** section displays a list of all VMs included into the report and their guest disks. The table details disk capacity, the amount of free and used space, trends for disk space usage growth, daily disk growth, and shows how many days are left until a disk reaches its limit.

  Click a VM name in the **Virtual Machine** column to drill down to VM guest disk space usage details.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **Business View objects**: defines Business View groups to analyze in the report. The parameter options are limited to objects of the Virtual Machine type.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.
- **Period**: defines the time period to analyze in the report.
- **Disk capacity, more than**: defines the minimum capacity threshold for a disk to analyze in the report. If disk capacity is less than the specified value, the report will not analyze this disk.
- **Free space, less than**: defines the maximum amount of free space for a disk to analyze in the report. If the amount of free space on a disk is more than the specified value, the report will not analyze this disk.

- **Sort by**: defines how data will be sorted in the report (*Virtual Machines*, *Relative Growth*, *Absolute Growth*).
- **Ignore excluded disks**: defines whether guest disks excluded in Veeam One Monitor to analyze in the report.

You can exclude certain VM guest disks from monitoring in Veeam ONE Client. To learn more, see Virtual Machine Summary.

Guest Disk Free Space

Description

This report provides information about free space for all VMs guest disks.

Report Parameters

Scope:	\\Virtual Infrastructure
Business View objects:	
Interval:	1 week (2/9/2021 - 2/15/2021)
Disk capacity, more than:	5 GB
Free space, less than:	50.00 %
Sort by:	Virtual machines
Ignore excluded disks:	True

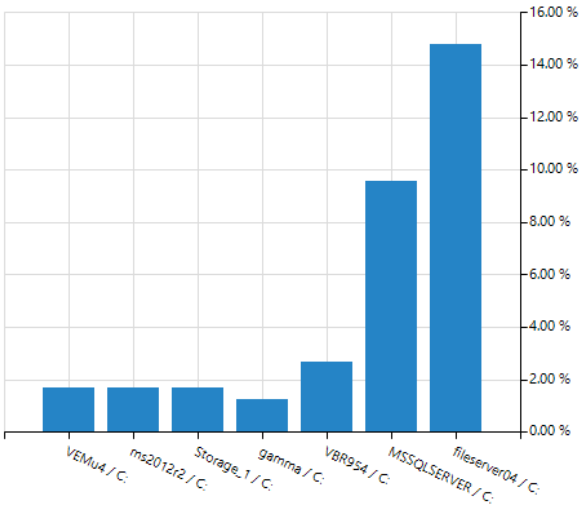
Summary

Overview		
VMs analyzed		7
Virtual disks in the infrastructure		20
Including	Fixed disks	0
	Dynamic disks	19
	Differencing disks	1
Disks to reach 100% in less than 30 days		0
Disks to reach 100% in less than 60 days		0
Disks with less than 1 GB of free space		0
Disks with less than 1% of free space		0
Average disks` daily growth [GB]		0.67
Average disks` daily growth [%]		0.15 %

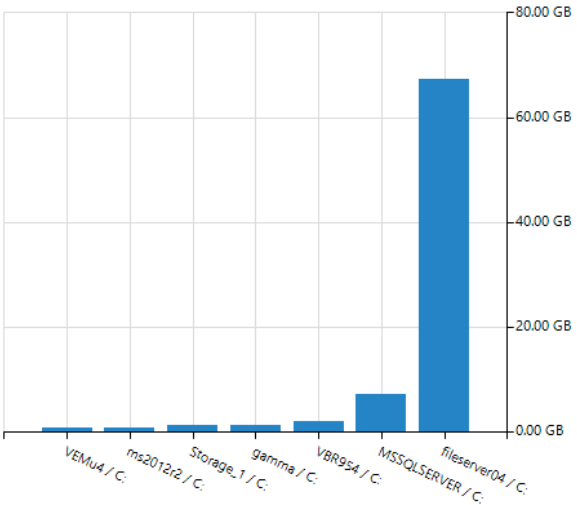
Disks to reach threshold first

Virtual Machine	Partition	Capacity (GB)	Free Space (GB)	Daily Growth (GB)	Days to Reach 90%	Days to Reach 100%
MSSQLSERVER	C:	126.66	45.63	0.42	63	88
fileserver04	C:	1023.66	501.87	3.96	76	97
gamma	C:	126.66	23.52	0.08	266	560
VBR954	C:	126.48	47.25	0.12	529	∞
Storage_1	C:	126.66	54.18	0.07	∞	∞
ms2012r2	C:	59.48	17.56	0.04	∞	∞
VEMu4	C:	59.48	17.56	0.04	∞	∞

Top 10 Partitions by Relative Space Growth



Top 10 Partitions by Absolute Space Growth



Guest Disk Free Space (GB)

Virtual Server: ms-node-02

Virtual Machine	Partition	Guest Disk Size (GB)	Guest Disk Used Space (%)	Guest Disk Used Space (GB)	Guest Disk Free Space (%)	Guest Disk Free Space (GB)	Disk`s Used Space Growth (GB)	Daily Growth (GB)	Days to Reach 100%
win19-static	C:	39.40	43.70	17.22	56.30	22.18	0.01	0.00	∞

Use Case

The report allows you to examine VM guest disk utilization and track disk usage growth. This helps you plan resource allocation and ensure your VMs have enough disk resources for stable operation.

Guest Disk Free Space (vSphere)

The report provides information on the amount of free disk space for VM guest OS. The report analyzes VM guest disks and displays their capacity, the amount of guest disk free space, shows disk space usage trends, and predicts how many days are left for a disk to reach the specified threshold.

- The **Summary** section includes the following elements:
  - The **Overview** table provides an overview of analyzed VM guest disks, shows how many VMs will run out of disk resources sooner than other VMs, and shows average disk growth trends.
  - The **Disks to Reach Threshold First** table displays a list of VMs that will run out of guest disk space sooner than other VMs. For each VM, the table shows guest disk capacity and the amount of free space left, daily disk growth trend and the number of days left before the occupied disk space will reach 90% and 100% of its capacity.

    If a value in the **Days to reach 90%** or **Days to reach 100%** column is highlighted with red, a disk will reach the specified threshold in less than 180 days.
  - The **Top 10 Partition by Relative Space Growth** chart shows 10 guest disks that used the greatest amount of space over the reporting period in relative terms (amount of occupied disk space against the disk capacity).
  - The **Top 10 Partition by Absolute Space Growth** chart shows 10 guest disks that used more space over the reporting period in absolute terms (amount of occupied disk space in GB).
- The **Guest Disk Free Space (GB)** section displays a list of all VMs included into the report and their guest disks. The table details disk capacity, the amount of free and used space, trends for disk space usage growth, daily disk growth, and shows how many days are left until a disk reaches its limit.

  Click a VM name in the **Virtual Machine** column to drill down to VM guest disk space usage details.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **Business View objects**: defines Business View groups to analyze in the report. The parameter options are limited to objects of the Virtual Machine type.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.
- **Last <N> days/weeks**: defines the time period to analyze in the report.
- **Disk capacity, more than (GB)**: defines the minimum capacity threshold for a disk to analyze in the report. If disk capacity is less than the specified value, the report will not analyze this disk.
- **Free space, less than (%)**: defines the maximum amount of free space for a disk to analyze in the report. If the amount of free space on a disk is more than the specified value, the report will not analyze this disk.
- **Sort by**: defines how data will be sorted in the report (*Virtual Machines*, *Relative Growth*, *Absolute Growth*).

- **Hide disks with "Suppress alarm" setting enabled in Veeam ONE Client**: defines whether guest disks excluded in Veeam ONE Client to analyze in the report.

  You can exclude certain VM guest disks from monitoring in Veeam ONE Client. To lean more, see Virtual Machine Summary.

View Report Example

Use Case

The report allows you to examine VM guest disk utilization and track disk usage growth. This helps you plan resource allocation and ensure your VMs have enough disk resources for stable operation.

Host Configuration (Hyper-V)

This report documents the current configuration of hosts in your infrastructure.

- The **Summary** section provides an overview of the infrastructure, including the total number of hosts, number of VMs per host and number of hosts per datastore.
- The **General Information** section provides information on each host, including host name, manufacturer, system model, OS type, update version and host status.
- The **Available Resources** section provides information on resources available for each host, including CPU frequency, number of cores, amount of physical and virtual memory, local and shared storage size and the number of VMs.
- The **Network Configuration** section provides information on network configuration for each host, including network name, type, number of VMs, adapter and IP address.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.

- **Business View objects**: defines Business View groups to analyze in the report. The parameter options are limited to objects of the Host type.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.

Host Configuration

Description

This report provides general Hyper-V hosts configuration information, including available resources and network configuration.

Report Parameters

Scope: Virtual Infrastructure

Business View objects:

Summary

Total number of hosts 2

VMs per host 32.00

Hosts per datastore 0.33

General Information

Name	Manufacturer	System Model	OS Type	Update Version	Status
hyperv01	Supermicro	X9DR3-F	Microsoft Windows Server 2012 R2 Datacenter	6.3.9600	Up
hyperv02	Supermicro	X9DR3-F	Microsoft Windows Server 2012 R2 Datacenter	6.3.9600	Up

Available Resources

Name	Physical CPU (GHz)	Total Cores	Physical Memory (GB)	Virtual Memory (GB)	Local Storage (GB)	Shared Storage (GB)	Number of VMs
hyperv01	25.20	12	128	160	4854	0	28
hyperv02	25.20	12	128	147	5638	0	36

Network Configuration

Network		Network Type	VMs	Adapter	IP Address
Host Name: hyperv01	5		29		
Intel(R) I350 Gigabit Network Connection - Virtual Switch		External	27	Intel(R) I350 Gigabit Network Connection	172.17.52.13
Lab Isolated Network (Exchange Virtual Lab)		Private	0	-	-
Lab Isolated Network (hyperv vlab)		Private	0	-	-
Lab Isolated Network (SQL vLab)		Private	0	-	-
Lab Isolated Network (Virtual Lab 2)		Private	2	-	-
Host Name: hyperv02	6		49		
Lab Isolated Network (Microsoft Exchange Lab)		Private	0	-	-
Intel(R) I350 Gigabit Network Connection - Virtual Switch		External	41	Intel(R) I350 Gigabit Network Connection #2	172.17.52.35 172.17.52.14
Lab Isolated Network (AppleDream)		Private	2	-	-
Lab Isolated Network (MadTeaPot)		Private	2	-	-
Lab Isolated Network (MadTea)		Private	2	-	-
Lab Isolated Network (test)		Private	2	-	-

Use Case

The report allows you to identify configuration issues, optimize resource provisioning and better handle current and future workloads.

Host Configuration (vSphere)

This report documents the current configuration of hosts in the virtual infrastructure.

- The **Summary** section provides an overview of the infrastructure, including the total number of hosts, number of VMs per host and number of hosts per datastore.
- The **General Information** section provides information on each host, including host name, manufacturer, system model, hypervisor version and host status.
- The **Available Resources** section provides information on resources available for each host, including CPU frequency, number of cores, amount of physical and virtual memory, local and shared storage size and the number of VMs.
- The **Network Configuration** section provides information on network configuration for each host, including network name, type, number of VMs, adapter and IP ranges.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **Business View objects**: defines Business View groups to analyze in the report. The parameter options are limited to objects of the Host type.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.
- **Show host network configuration**: defines whether host network configuration details must be included in the report.

View Report Example

Use Case

The report allows you to identify configuration issues, optimize resource provisioning and better handle current and future workloads.

Host Configuration Chargeback

This report helps to make infrastructure costs audit and identify the most and least expensive VMs based on the hardware price and VM configuration.

The report analyzes hardware CPU, memory, storage capacities and their cost to calculate the cost of resources allocated to VMs. The cost of resources allocated to a VM is calculated based on VM configuration: the amount of vCPU, vRAM and storage resources provisioned to a VM.

> **NOTE:**
> - For VMs with thin-provisioned or dynamic disks, the report takes into account the amount of provisioned disk space, not actually used disk space.
> - For VMs with dynamic memory, the report takes into account the amount of allocated memory.

- The **Summary** section includes the following elements:
  - Number of hosts, datastores and VMs, average costs of physical and virtual resources (processor core, virtual CPU, memory GB, storage TB), and total hardware cost.
  - The **Cost Distribution** chart shows the cost of hardware CPU, memory and storage resources.
  - The **VM Power Status** chart shows the number of running and powered-off VMs.
  - The **Top 10 Most Expensive VMs** subsection shows the most expensive VMs in terms of consumed resources, and provides cost of average CPU, memory and storage resources used by each VM. This chart is available if you choose to include VM details in the report.
- The **Details** tables provide information on physical CPU, memory and storage capacities, amount of provisioned vCPU, vRAM and storage resources, and the cost of these resources. If you choose to show VM cost details in the report parameters, the report also provides analysis of VM configuration cost in terms of vCPU, vRAM, storage and the total VM cost.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a list of virtual infrastructure level and its sub-components to analyze in the report.
- **Currency**: defines a payment currency.
- **Calculate host costs based on**: defines how host costs will be calculated in the report. You can select one of the following options:
  - **Total host cost** — defines the total cost of CPU and memory hardware resources for all hosts included in the report, in the selected currency.
  - **Individual host costs** — defines the hardware cost of each host separately.

    To edit host costs:
    - Click **Configure**.
    - In the **Configure Individual Host Costs** window, select the necessary host and click **Edit**.
    - In the **Set Individual Host Cost** window, specify the desired cost and click **Save**.
    - Repeat steps 2-3 for each host cost you want to edit.

- **CPU/RAM slider**: defines the percentage of cost, or cost share of CPU and memory hardware resources for all hosts included in the report. For example, if the cost of CPU hardware resources make a quarter of the total cost, set the *CPU* parameter value to *25%*. The *RAM* parameter value will adjust automatically.
- **Calculate datastore costs based on**: defines how datastore costs will be calculated in the report. You can select one of the following options:
    - **Exclude datastores from the calculation** – defines to exclude datastores cost details from the report.
    - **Total datastore cost** – defines the total cost of storage resources in the selected currency.
    - **Individual datastore costs** – defines the cost of each datastore separately.

      To edit datastore costs:

        1. Click **Configure**.
        2. In the **Configure Individual Datastore Costs** window, select the necessary datastore and click **Edit**.
        3. In the **Set Individual Datastore Cost** window, specify the desired cost and click **Save**.
        4. Repeat steps 2-3 for each datastore cost you want to edit.
- **Calculate VM storage hosts based on**: defines how VM storage host must be calculated in the report (*Provisioned space, Used space*).
- **Include powered-off VMs in the calculation**: defines whether powered-off VMs must be analyzed in the report.
- **Show VM details**: defines whether the report must include VM cost details.

  If this option is enabled, the report will include the **Top 10 Most Expensive VMs** section and a table that details VMs cost based on VM configuration.

> **NOTE:**
>
> Building the report may take some time if the chosen reporting period is significant, or if you choose to calculate VM cost for a large virtual infrastructure.

View Report Example

Use Case

IT departments can use the report as a showback instrument to raise awareness within organization and demonstrate costs associated with provisioning VMs. The report helps calculate a budget share of allocated virtual infrastructure resources for each application owner, department or business unit within an organization, justify IT budget and assess the amount of future funding requests.

In combination with Veeam ONE optimization reports, this report can be used to encourage application owners to right size their VMs, prevent VM proliferation and reclaim wasted resources.

Service providers that do not have flat fees on virtual infrastructure resources can use this report as a chargeback instrument to calculate the cost of virtual infrastructure resources allocated to their clients.

Host Failure Modelling (Hyper-V)

This report allows you to both simulate a failure of one or more hosts and forecast CPU and memory usage for Hyper-V clusters.

- The **Summary** section provides an overview of the current state of your infrastructure (the total number of clusters, hosts, datastores, and VMs) and shows recommendations on resource allocation.
- The **Modelling Results** charts display the amount of CPU and memory resources left and lost in case of a host failure.
- The **VMs Migration Count** chart shows the number of VMs that will need to be relocated to another host (*VMs to Migrate*) and the number of VMs that will operate as usual (*Unaffected VMs*) in case of a host failure.
- The **Details** table provides details on CPU and memory current and predicted utilization for all clusters included in the report.
- The **Recommendations** section provides recommendations for the resources whose utilization thresholds will be breached.

TIP:

- Click a cluster name in the **Details** table to drill down to details on current and predicted resource usage for the cluster.
- Click a number in the **Affected VMs** column of the **Details** table to drill down to details for the VM that needs to be migrated.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **Number of failed hosts**: defines the number of random hosts for which you want to simulate a failure.
- **Failed hosts**: defines a list of hosts for which you want to simulate a failure.
- **Business View migration scope**: filters report scope objects that belong to the selected Business View groups.
- **CPU utilization threshold (%)**: defines the CPU usage threshold as a percentage of total cluster CPU resources.

- **Memory utilization threshold (%)**: defines the used memory threshold as a percentage of total cluster memory resources.

Host Failure Modelling

Description

This report predicts resource utilization in case of a host failure.

Report Parameters

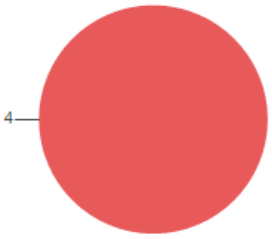
Scope:	Virtual Infrastructure
Number of failed hosts:	1
CPU utilization threshold:	90.00%
Memory utilization threshold:	80.00%
Business View migration scope:	

Summary

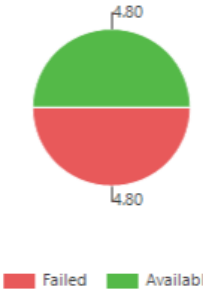
Virtual Infrastructure		Physical Resources		Resources Required	
Number of clusters:	1	CPU:	9.60 GHz	CPU:	0.00 GHz
Number of hosts:	2	Memory:	32.00 GB	Memory:	9.79 GB
Number of datastores:	4	**Physical Resources After 1 Hosts Failure**			
Number of VMs:	32	CPU:	4.80 GHz		
Number of powered on VMs:	4	Memory:	16.00 GB		

Modelling Results

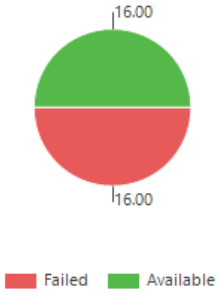
VMs Migration Count



Available CPU Resources (GHz)



Available Memory Resources (GB)



Details

Cluster	Average CPU Usage (%)	Average Memory Usage (%)	Predicted CPU Usage (%)	Predicted Memory Usage (%)	Failed Hosts	Affected VMs
ms-22-cluster.n.local	33.78	70.59	67.55	141.19	1	4
					ms-22-node-02	4

Recommendations

ms-22-cluster.n.local:

To ensure this Cluster remains functional after 1 hosts failure, add one host with (at least): Memory: 9.79 GB

Use Case

The report provides recommendations on appropriate resource allocation, which can help prevent possible CPU and memory resource shortfalls in future and maintain the optimal performance of your infrastructure.

Host Failure Modelling (vSphere)

This report allows you both to simulate a failure of one or more hosts, and forecast CPU and memory usage for clusters.

- The **Summary** section provides an overview of the current state of your infrastructure (the total number of clusters, hosts, datastores and VMs) and shows recommendations on resource allocation.
- The **Modelling Results** charts display the total amount of CPU and memory resources left and lost in clusters in case of a host failure. The **VMs Migration Count** chart shows the number of VMs that will need to be relocated to another host (VMs to Migrate) and the number of VMs that will operate as usual (Unaffected VMs) in case of a host failure.
- The **Details** table provides details on CPU and memory current and predicted utilization for all clusters included in the report.

  Click a cluster name to drill down to details on current and predicted resource usage for the cluster. Click a number in the **Affected VMs** column to drill down to details for the VMs that need to be migrated.
- The **Recommendations** section provides recommendations for the resources whose utilization thresholds will be breached.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **Number of failed hosts**: defines the number of random hosts for which you want to simulate a failure.
- **Failed hosts**: defines a list of hosts for which you want to simulate a failure.
- **Business View migration scope**: filters report scope objects that belong to the selected Business View groups.
- **CPU utilization threshold (%)**: defines the CPU usage threshold as a percentage of total cluster CPU resources.
- **Memory utilization threshold (%)**: defines the used memory threshold as a percentage of total cluster memory resources.

View Report Example

Use Case

The report provides recommendations on appropriate resource allocation, which can help prevent possible CPU and memory resource shortfalls in future and maintain the optimal performance of your infrastructure.

Host Performance (Hyper-V)

This report aggregates historical data and shows performance statistics for a selected host across a time range.

The report shows tables and performance charts with statistics on CPU, memory, disk and network usage for the host. The report also lists top resource consuming VMs and calculates resource usage trends for them.

- The **Navigation** section shows path to the selected object, including VMware vSphere VC, datacenter, cluster and host system.

  Click a cluster name to drill down to performance charts with statistics on CPU, memory, disk and network usage for the cluster.

- The **Performance** subsections provide information on CPU, memory, disk and network usage, including usage trends and top resource consuming VMs for the host.

  Click a VM name in the list of top resource consuming VMs to drill down to performance charts with statistics on CPU, memory, disk and network usage for the VM.

Report Parameters

You can specify the following report parameters:

- **Object**: defines the host to analyze in the report.
- **Period**: defines the time period to analyze in the report. Note that the reporting period must include at least one successfully completed *Object properties data collection* task for the selected host. Otherwise, the report will contain no data.
- **Business hours only**: defines time of a day for which historical performance data will be used to calculate the performance trend. All data beyond this interval will be excluded from the baseline used for data analysis.

- **Top N**: defines the maximum number of hosts and VMs to display in the report output.

Host Performance

Description

This report shows host performance history that includes CPU, Memory, Disk and Network counters.

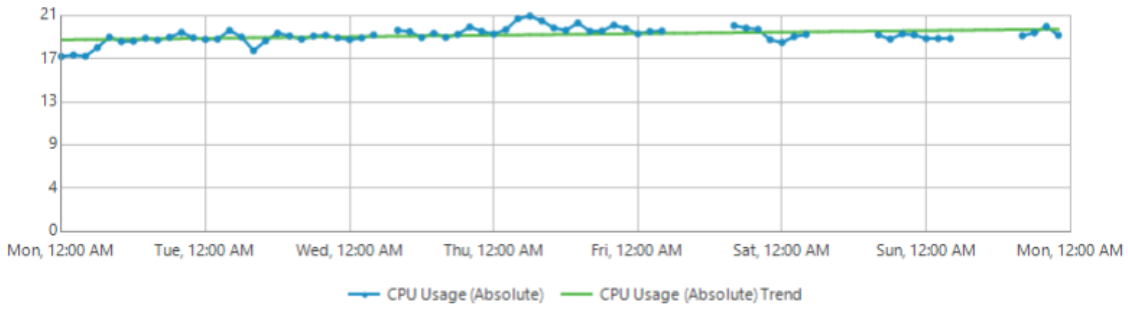
Report Parameters

Selected object:	prgtwesx01.tech.local
Object location:	\\Virtual Infrastructure\vcenter01.tech.local\Prague
Reporting period:	1/2/2023 - 1/8/2023
Top N:	3

⊞Navigation

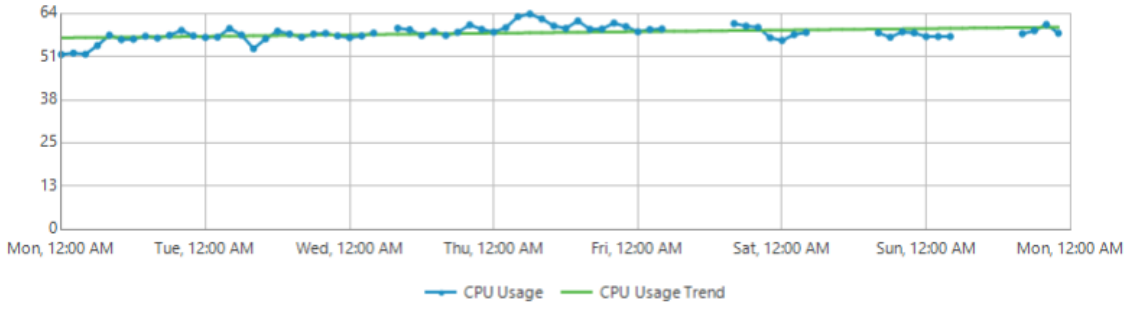
CPU Performance

CPU Usage (GHz)



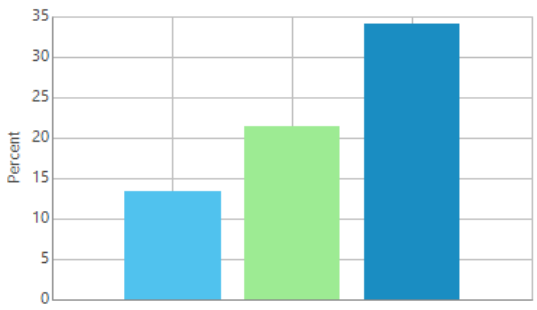
Object Name	Average	Minimum	Maximum	Std. Deviation	Trend
prgtwesx01.tech.local	19.47	17.35	21.37	0.75	Increasing

CPU Usage (Percent)



Object Name	Average	Minimum	Maximum	Std. Deviation	Trend
prgtwesx01.tech.local	57.95	51.65	63.61	2.22	Increasing

Top 3 VMs by CPU Usage



Object Name	Avg	Trend
serv02_vbo	34.04	Decreasing
enterprise05	21.37	Increasing
appsrv01	13.37	Decreasing

Use Case

The report provides an overview of hardware resource consumption for the selected host. This information may help you identify hosts with performance issues, balance workloads, right-size resource provisioning and assure high availability/failover protection for VMs across the growing virtual environment.

Host Performance (vSphere)

This report aggregates historical data and shows performance statistics for a selected host across a time range.

- The **Performance** subsections provide information on CPU, memory, disk and network usage, including usage trends and top resource consuming VMs for the host.

  Click a VM name in the list of top resource consuming VMs to drill down to performance charts with statistics on CPU, memory, disk and network usage for the VM.

Report Parameters

You can specify the following report parameters:

- **Object**: defines the host to analyze in the report.
- **Period**: defines the time period to analyze in the report. Note that the reporting period must include at least one successfully completed *Object properties data collection* task for the selected host. Otherwise, the report will contain no data.
- **Business hours only**: defines time of a day for which historical performance data will be used to calculate the performance trend. All data beyond this interval will be excluded from the baseline used for data analysis.
- **Top N**: defines the maximum number of VMs to display in the report output.

View Report Example

Use Case

The report provides an overview of hardware resource consumption for the selected host. This information may help you identify hosts with performance issues, balance workloads and right-size resource provisioning for VMs across the growing virtual environment.

Host Resource Usage Chargeback

This report helps to make infrastructure costs audit and identify the most and least expensive VMs based on the hardware price and VM performance.

The report analyzes hardware CPU, memory, storage capacities and total cost of these resources to calculate the cost of resources consumed by VMs. The cost of consumed resources is calculated based on average CPU, memory and storage usage for a specified period.

- The **Summary** section includes the following elements:
  - Details on the number of hosts, datastores and VMs, average cost of physical resources (processor GHz, memory GB, storage TB), average VM cost and total hardware cost.
  - The **Cost Distribution** chart shows the cost of hardware CPU, memory and storage resources.
  - The **Top 5 Hosts with Expensive CPU/Memory Resources** tables show 5 most expensive hosts in terms of consumed CPU and memory resources.
  - The **Top 5 Datastores with Expensive Resources** table shows 5 most expensive datastores in terms of consumed storage resources.
  - The **Top 10 Most Expensive VMs** subsection shows 10 most expensive VMs in terms of consumed resources, and provides cost of average CPU, memory and storage resources used by each VM. This chart is available if you choose to include VM details in the report.
- The **Details** tables provide information on physical CPU, memory and storage capacities, cost of physical and virtual resources. If you choose to calculate per-VM cost in the report parameters, the report also provides detailed analysis of VM cost based on the average usage of CPU, RAM and storage resources within the reporting period.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a list of virtual infrastructure level and its sub-components to analyze in the report.
- **Currency**: defines a payment currency.
- **Calculate host costs based on**: defines how host costs will be calculated in the report. You can select one of the following options:
  - **Total host cost** — defines the total cost of CPU and memory hardware resources for all hosts included in the report, in the selected currency.
  - **Individual host costs** — defines the hardware cost of each host separately.

    To edit host costs:
    1. Click **Configure**.
    2. In the **Configure Individual Host Costs** window, select the necessary host and click **Edit**.
    3. In the **Set Individual Host Cost** window, specify the desired cost and click **Save**.
    4. Repeat steps 2-3 for each host cost you want to edit.

- **CPU/RAM slider**: defines the percentage of cost, or cost share of CPU and memory hardware resources for all hosts included in the report. For example, if the cost of CPU hardware resources make a quarter of the total cost, set the *CPU* parameter value to *25%*. The *RAM* parameter value will adjust automatically.
- **Calculate datastore costs based on**: defines how datastore costs will be calculated in the report. You can select one of the following options:
    - **Exclude datastores from the calculation** — defines to exclude datastores cost details from the report.
    - **Total datastore cost** — defines the total cost of storage resources in the selected currency.
    - **Individual datastore costs** — defines the cost of each datastore separately.

      To edit datastore costs:

        1. Click **Configure**.
        2. In the **Configure Individual Datastore Costs** window, select the necessary datastore and click **Edit**.
        3. In the **Set Individual Datastore Cost** window, specify the desired cost and click **Save**.
        4. Repeat steps 2-3 for each datastore cost you want to edit.
- **Period**: defines a period in the past for which historical performance data must be analyzed in the report. For example, if you specify the previous week as the reporting period, the report will calculate the VM cost based on the average VM CPU, memory and storage utilization values for the previous week. Note that the reporting period must include at least one successfully completed *Object properties data collection* task for the selected scope. Otherwise, the report will contain no data.
- **Business hours only**: defines time of a day for which historical performance data must be used to calculate the VM cost. Data outside this interval will be excluded from the baseline used for data analysis.

- **Show VM details**: defines whether the report must include VM cost details.

  If this option is disabled, the report will not display the most expensive VMs, and will not provide VM cost in terms of utilized CPU, RAM and storage resources.

Host Resource Usage Chargeback

Description

This report helps you to perform an infrastructure costs audit and identify the most and least expensive VMs based on the hardware price and VM performance.

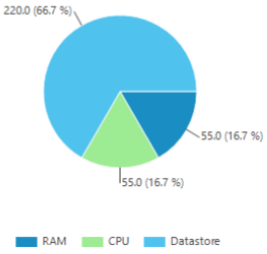
Report Parameters

Hosts:	Virtual Infrastructure
Hosts cost:	110.00 USD
Host expenses distribution:	CPU: 50% / RAM: 50%
Datastores cost:	220.00 USD
Reporting period:	1 month (12/3/2022 - 1/2/2023)
Business hours:	From 9:00 AM To 6:00 PM
Show VM details:	True

Summary

Hosts:	6	CPU, GHz average cost:	0.23 USD
VMs:	228	RAM, GB average cost:	0.09 USD
Datastores:	11	Datastore, TB average cost:	35.30 USD
Average VM price:	0.48 USD		
Total hardware cost:	330.00 USD		

Cost Distribution



Top 5 Hosts with Expensive CPU Resources

Host Name	CPU GHz Cost, USD	Average VM Price, USD
prgtwesx01-virt.tech.local	0.32	2.04
prgtwesx02-virt.tech.local	0.32	1.83
prgtwesx01.tech.local	0.27	0.21
pdctwhv01.tech.local	0.18	1.15
prgtwesx02.tech.local	0.16	0.35

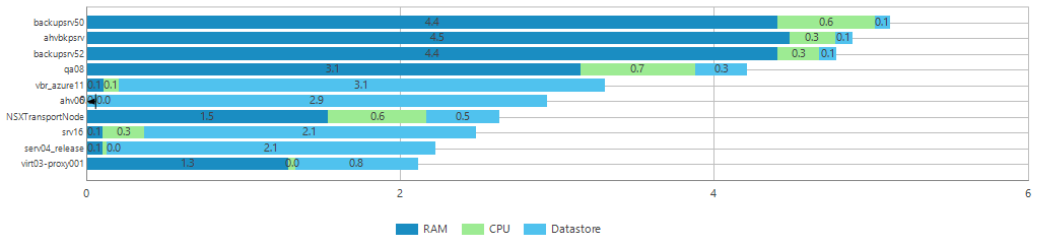
Top 5 Hosts with Expensive Memory Resources

Host Name	GB RAM Cost, USD	Average VM Price, USD
prgtwesx01-virt.tech.local	0.23	2.04
prgtwesx02-virt.tech.local	0.23	1.83
prgtwesx03.tech.local	0.02	0.30
prgtwesx02.tech.local	0.02	0.35
pdctwhv01.tech.local	0.02	1.15

Top 5 Datastores with Expensive Resources

Datastore Name	Store TB Cost, USD	Average VM Price, USD
Veeam_dr_v6_nfs41_5HNufyTQKzk1Xc3a0SzRJ3	225.28	0.10
docopsubuntunfs01	45.87	0.50
docopslinuxnfs	45.87	4.51
prgtwesx01-virt-ds1	28.43	1.08
prgtwesx02-virt-ds1	28.43	0.33

Top 10 Most Expensive VMs



Details (VMware)

CPU

vCenter Server: vcenter01.tech.local

Host	VMs	CPU Cost, USD	# of Cores	Clock Speed, GHz	CPU Capacity, GHz	Cost per GHz, USD
⊟Cluster: Standalone hosts	203	27.50	64	6.90	148.80	0.59
prgtwesx01.tech.local	88	9.17	16	2.10	33.60	0.27
prgtwesx02.tech.local	53	9.17	24	2.40	57.60	0.16
prgtwesx03.tech.local	62	9.17	24	2.40	57.60	0.16
⊟Cluster: CDP cluster	19	18.33	24	4.80	57.60	0.64
prgtwesx01-virt.tech.local	9	9.17	12	2.40	28.80	0.32
prgtwesx02-virt.tech.local	10	9.17	12	2.40	28.80	0.32

Memory

vCenter Server: vcenter01.tech.local

Host	VMs	Memory Cost, USD	RAM Capacity, GB	RAM GB Cost, USD
⊟Cluster: CDP cluster	19	18.33	79.99	0.46
prgtwesx01-virt.tech.local	9	9.17	40.00	0.23
prgtwesx02-virt.tech.local	10	9.17	40.00	0.23
⊟Cluster: Standalone hosts	203	27.50	1277.22	0.07
prgtwesx01.tech.local	88	9.17	511.89	0.02
prgtwesx02.tech.local	53	9.17	382.66	0.02
prgtwesx03.tech.local	62	9.17	382.66	0.02

Datastores

Datastore Name	Type	Owner	VMs	Cost, USD	Capacity, TB	TB Cost, USD
⊟vCenter Server: vcenter01.tech.local						
prgtwesx01-ds01	VMFS	prgtwesx01.tech.local	26	22.00	3.63	6.06
prgtwesx01-ds02	VMFS	prgtwesx01.tech.local	60	22.00	7.28	3.02
Veeam_dr_v6_nfs41_5HNufyTQKzk1Xc3a0SzRJ3	NFS	prgtwesx01.tech.local	2	22.00	0.10	225.28
prgtwesx01-virt-ds1	VMFS	prgtwesx01-virt.tech.local	5	22.00	0.77	28.43
prgtwesx02-ds01	VMFS	prgtwesx02.tech.local	53	22.00	16.25	1.35
docopsubuntunfs01	NFS	prgtwesx02-virt.tech.local	9	22.00	0.48	45.87
prgtwesx02-virt-ds1	VMFS	prgtwesx02-virt.tech.local	5	22.00	0.77	28.43
docopslinuxnfs	NFS	prgtwesx03.tech.local	1	22.00	0.48	45.87
prgtwesx03-ds01	VMFS	prgtwesx03.tech.local	62	22.00	16.25	1.35

VM Cost (VMware)

vCenter Server: vcenter01.tech.local

Host	Virtual Machine	VM Uptime	CPU		Memory		Datastore		Total VM Cost, USD
			Avg. Usage, GHz	Cost, USD	Avg. Usage, GB	Cost, USD	Avg. Usage, GB	Cost, USD	
Cluster: Standalone hosts	193			10.97		18.29		47.52	76.78
prgtwesx01.tech.local	88			5.70		5.91		31.86	43.47
	srv16	99.28 %	0.97	0.26	6.00	0.11	356.97	2.11	2.48
	serv04_release	99.25 %	0.09	0.02	6.00	0.11	354.12	2.10	2.23
	srv14	99.27 %	0.50	0.13	6.00	0.11	307.81	1.82	2.06
	backupserver004	99.28 %	1.89	0.51	8.00	0.14	323.89	0.96	1.61
	srv12	99.25 %	0.84	0.23	8.00	0.14	395.90	1.17	1.54
	serv45	99.28 %	0.08	0.02	7.97	0.14	227.83	1.35	1.51
	enterprise05	99.20 %	3.78	1.02	8.00	0.14	103.21	0.30	1.47
	serv21	99.28 %	0.64	0.17	5.85	0.10	324.87	0.96	1.23
	enterprise03	99.28 %	0.20	0.05	4.00	0.07	372.14	1.10	1.22
	filesrv01	99.28 %	0.16	0.04	5.81	0.10	163.74	0.97	1.12
	vcenter01	99.28 %	0.54	0.15	18.88	0.34	214.15	0.63	1.11
	srv13	99.19 %	0.82	0.22	6.00	0.11	253.43	0.75	1.08
	dlsql01	99.28 %	0.13	0.04	8.00	0.14	142.86	0.85	1.02
	appsrv01	99.28 %	0.56	0.15	6.00	0.11	105.26	0.62	0.88
	linuxsrv001	99.28 %	0.36	0.10	14.70	0.26	168.08	0.50	0.85
	serv02_vbo	99.28 %	2.13	0.58	4.00	0.07	69.05	0.20	0.85
	winsrv0022016	99.28 %	1.36	0.37	6.00	0.11	111.02	0.33	0.80
	backupserver001	0.00 %	0.00	0.00	0.00	0.00	253.98	0.75	0.75
	winorcl01	99.28 %	0.24	0.07	8.00	0.14	176.52	0.52	0.73
	vcenter-old	0.00 %	0.00	0.00	0.00	0.00	242.94	0.72	0.72
	enterprise07	99.28 %	0.17	0.05	8.00	0.14	172.16	0.51	0.70
	avspem1	0.00 %	0.00	0.00	0.00	0.00	116.08	0.69	0.69
	winsrv004	99.24 %	1.00	0.27	7.99	0.14	82.82	0.24	0.66
	winsrv001	99.22 %	0.25	0.07	6.00	0.11	163.53	0.48	0.66
	serv01_vbo	99.28 %	0.34	0.09	8.00	0.14	139.57	0.41	0.65
	winsrv88	99.28 %	0.11	0.03	6.00	0.11	78.25	0.46	0.60

Use Case

IT departments can use the report as a showback instrument to raise awareness within organization and demonstrate costs associated with the amount of compute and storage resources utilized by VMs. The report helps calculate a budget share of used virtual infrastructure resources for each application owner, department or business unit within an organization, justify IT budget, and assess the amount of future funding requests.

The report can also be used to prevent excessive resource consumption and ensure that virtual infrastructure resources are utilized in line with the business needs.

Service providers that do not have flat fees on virtual infrastructure resources, can use this report as a chargeback instrument to calculate the cost of resources their clients have utilized during the billing period, and charge for provided services based on the actual resource consumption.

Host Uptime (Hyper-V)

This report analyzes host uptime statistics to track host availability.

- The **Summary** section includes the following elements:
  - The **Top Uptime** and **Lowest Uptime** charts display top 5 hosts in terms of the highest and the lowest uptime values.
  - The **Uptime Distribution** chart shows uptime values of all available hosts.
- The **Host Uptime** table provides the list of hosts whose uptime values are not within the specified thresholds.

  Click a host name in the **Host** column to drill down to details on alarms triggered by Veeam ONE Client and host restarts.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **Business View objects**: defines Business View groups to analyze in the report. The parameter options are limited to objects of the Host type.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.
- **Period**: defines the time period to analyze in the report. Note that the reporting period must include at least one successfully completed *Object properties data collection* task for the selected scope. Otherwise, the report will contain no data.
- **Business hours only**: defines time of a day for which historical performance data will be used to calculate the performance trend. All data beyond this interval will be excluded from the baseline used for data analysis.
- **Uptime, greater than**: defines the desired minimum uptime value.
- **Uptime, less than**: defines the desired maximum uptime value.

- **Group by**: defines how data will be grouped in the report output (by *Uptime*, *Datacenter* or *Cluster*).

Host Uptime

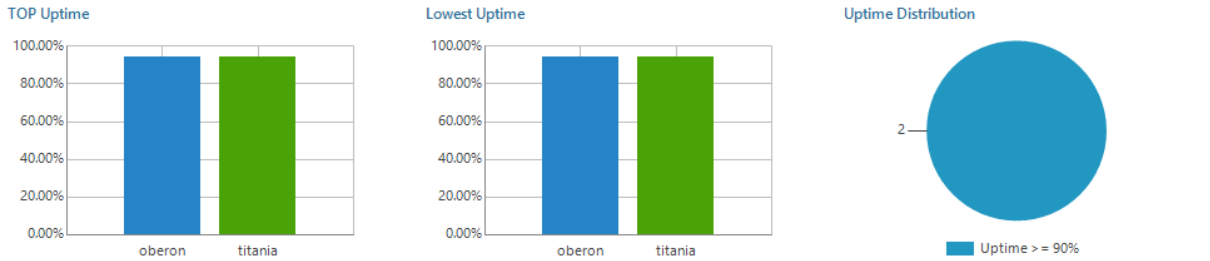
Description

This report provides an overview of hosts uptime including hosts with lowest and highest uptime values.

Report Parameters

Scope:	Virtual Infrastructure
Reporting period:	Current month (2/1/2021 - 2/28/2021)
Uptime:	greater than 80.00% and lower than 100.00%
Grouping:	Group by Uptime
Business View objects:	
Business hours:	From 12:00 AM to 12:00 AM

Summary



Host Uptime

Cluster	Host	Number of Restarts	Number of Alarms	Downtime	Sum of Uptime (%)
Uptime: Uptime >= 90%					
midsummer	oberon	0	2	00:35:00	94.17%
midsummer	titania	0	4	00:35:00	94.17%

Use Case

This report helps you discover the most and the least utilized hosts in the environment to restore their efficiency and improve target ROI.

Host Uptime (vSphere)

This report analyzes host uptime statistics to track host availability.

- The **Top Uptime** and **Lowest Uptime** charts display top 5 hosts in terms of the highest and the lowest uptime values.
- The **Host Uptime** table provides the list of hosts whose uptime values are lower and greater than the specified thresholds.

  Click a host in the **Host** column table to drill down to details on alarms triggered by Veeam ONE and host restarts.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **Business View objects**: defines Business View groups to analyze in the report. The parameter options are limited to objects of the Host type.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.
- **Period**: defines the time period to analyze in the report. Note that the reporting period must include at least one successfully completed *Object properties data collection* task for the selected scope. Otherwise, the report will contain no data.
- **Business hours only**: defines time of a day for which historical performance data will be used to calculate the performance trend. All data beyond this interval will be excluded from the baseline used for data analysis.
- **Uptime, greater than**: defines the desired minimum uptime value.
- **Uptime, less than**: defines the desired maximum uptime value.
- **Group by**: defines how data will be grouped in the report output (by *Uptime*, *Datacenter* or *Cluster*).

View Report Example

Use Case

This report helps you discover the most and the least utilized hosts in the environment to restore their efficiency and improve target ROI.

How Many More VMs Can be Provisioned

This report calculates the number of additional VMs that your existing infrastructure can support before the resource utilization reaches the specified threshold value.

The report evaluates total capacity of your infrastructure and provides estimation of how many sample VMs of a certain profile can be added without causing the specified resource utilization threshold to be breached. Calculation of additional VM sets is based on the predicted future performance of the sample VM and the predicted virtual infrastructure capacities.

- The **Summary** section provides information on total number of VMs in capacity, number of existing VMs and VMs that can be added, and VM configuration and average performance.
    - The **Constraining Resource Per Each Object** table displays resources for which the specified thresholds will be breached first for each host, cluster or datastore.
- The **Details** table provides information on average and predicted resource usage for each host, cluster or datastore.

  Click a host, cluster or datastore name in the details table to drill down to in-depth forecast information for the host, cluster or datastore.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **Business View objects**: defines Business View groups to analyze in the report. The parameter options are limited to objects of the Host type.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.
- **Datastores**: defines a list of datastores to analyze in the report.
- **VM sample**: defines a VM profile that will be used as a sample for calculating the number of VM sets:
    - If you choose a specific VM, the report will calculate how many similar VMs can be added.
    - If you choose *Average VM configuration*, the report will assess average configuration across all your VMs, and calculate how many VM of this configuration can be added.

  Note that VMs in the profile must be currently in the powered on state, and that performance data collection must be completed for the given VMs.
- **Count reserved CPU and memory**: defines whether CPU and memory reservations should be taken into account when calculating the number of VMs to be added.
- **CPU utilization (%)**: defines the CPU usage threshold as a percentage of total cluster CPU resources.
- **Memory utilization (%)**: defines the used memory threshold as a percentage of total cluster memory resources.
- **Space utilization (%)**: defines the threshold for the maximum amount of space in use on a datastore.

- **Free space (min)**: defines the threshold for the minimum amount of free space in GB left on a datastore.
- **Read speed (max)**: defines the threshold for read rate in MB per second for datastores.
- **Write speed (max)**: defines the threshold for write rate in MB per second for datastores.
- **Max vCPUs per physical core**: defines the threshold for the maximum number of vCPU cores per a single instance of the logical CPU core.
- **Put 1 host from each cluster into maintenance mode**: defines whether to simulate putting one host into maintenance mode when calculating the number of VMs to be added.

View Report Example

Use Case

This report helps administrators to discover how many additional VMs can be deployed without affecting infrastructure performance.

Hyper-V Custom Performance

This report allows you to define specific CPU, memory, network and disk metrics to analyze performance of Hyper-V hosts, VMs, Cluster Shared Volumes and SMB shares.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **Business View objects**: defines Business View groups to analyze in the report.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.
- **Period**: defines the time period to analyze in the report. Note that the reporting period must include at least one successfully completed *Object properties data collection* task for the selected scope. Otherwise, the report will contain no data.
- **Business hours only**: defines time of a day for which historical performance data will be used to calculate the performance trend. All data beyond this interval will be excluded from the baseline used for data analysis.
- **Object type**: defines the infrastructure object to analyze in the report (*Hosts*, *Virtual Machines*, *Local Datastore*, *CSV 2008*, *CSV*, *SMB Shares*).
- **Measured entities**: defines subsystems to analyze in the report (*CPU*, *Memory*, *Network*, *Disk* or *Virtual Switch*). The list of available subsystems will depend on the selected object type.
- **Metrics**: defines metrics to analyze in the report. The list of available metrics will depend on the selected monitor subsystem.
- **Inclusion rule/Exclusion rule**: defines a list of objects that should be included in/excluded from the report scope:
  - Use the **Inclusion rule** option to define names of virtual infrastructure objects that should be included in the report. All objects not specified in the **Inclusion rule** field will be excluded from the baseline used for data analysis.
  - Use the **Exclusion rule** option to define names of virtual infrastructure objects that should be excluded from the report. All objects not specified in the **Exclusion rule** field will be included in the baseline used for data analysis.

> **NOTE:**
>
> The **Inclusion rule/Exclusion rule** parameters support wildcards. Search is not case sensitive.
>
> To illustrate how to use wildcard queries, consider the following example. You have selected 4 hosts as a report scope: 2 NAS servers (*NASserv1*, *NASserv2*) and 2 Active Directory servers (*AD01* and *AD02*).
>
> If you want the report to show performance details only for the NAS servers, type *nasserv** in the **Inclusion rule** field. Alternatively, type *ad** in the **Exclusion rule** field.

- **Top N**: defines the maximum number of VMs to display in the report.
- **Show graphs**: defines whether to show charts in the report output.

Hyper-V Custom Performance

Description

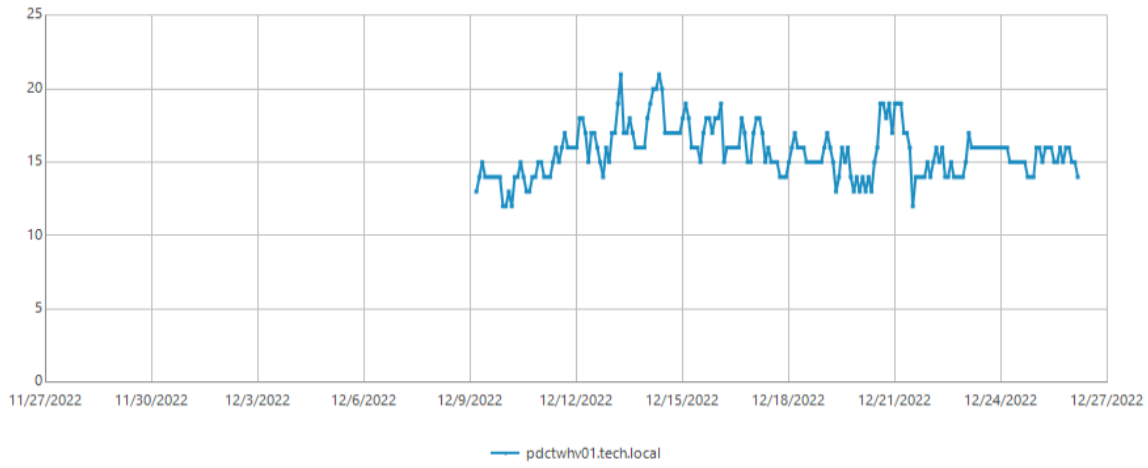
This report allows you to define specific metrics to analyze performance of Hyper-V infrastructure elements.

Report Parameters

Selected object:	Virtual Infrastructure
Report creation date:	12/26/2022 5:33 AM
Report period:	1 month (11/27/2022 - 12/26/2022)
Object type:	Hosts
Exclusion rule:	
Inclusion rule:	*
Business View objects:	
Top N:	All Items
CPU:	Total Run Time (Percent), Total Run Time (MHz)
Memory:	Memory Usage (Percent), Hyper-V Services Memory Consumed (B)

CPU

Total Run Time (Percent)



Virtual Server	Object Name	Average	Maximum	Minimum	Std. Deviation	Trend
pdctwhv01.tech.local						
	pdctwhv01.tech.local	15.71	21.00	12.00	1.71	Decreasing

Use Case

Use this report to investigate specific performance issues in the environment.

Hyper-V Raw Performance Data

This report allows you to get detailed raw data on specific CPU, memory, network and disk metrics to analyze performance of Hyper-V hosts, VMs, Cluster Shared Volumes and SMB shares.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **Business View objects**: defines Business View groups to analyze in the report.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.
- **Period**: defines the time period to analyze in the report. Note that the reporting period must include at least one successfully completed *Object properties data collection* task for the selected scope. Otherwise, the report will contain no data.
- **Sample size**: defines the resolution level, that is, granularity of raw data that should be displayed in the report output. Note that data with the Raw sample length (5-minute resolution) is available only for the custom interval of last week; if you select Year/Quarter/Month as a reporting interval, the report will show data with 2-hour resolution.
- **Object type**: defines the infrastructure object to analyze in the report (*Hosts*, *Virtual Machines*, *Local Datastore*, *CSV 2008*, *CSV*, *SMB Shares*).
- **Measured entities**: defines subsystems to analyze in the report (*CPU*, *Memory*, *Network*, *Disk* or *Virtual Switch*). The list of available subsystems will depend on the selected object type.
- **Metrics**: the performance metrics to analyze in the report. The choice of available metrics will depend on the selected monitored subsystems.
- **Inclusion rule/Exclusion rule**: defines a list of objects that should be included in/excluded from the report scope:
  - Use the **Inclusion rule** option to define names of virtual infrastructure objects that should be included in the report. All objects not specified in the **Inclusion rule** field will be excluded from the baseline used for data analysis.
  - Use the **Exclusion rule** option to define names of virtual infrastructure objects that should be excluded from the report. All objects not specified in the **Exclusion rule** field will be included in the baseline used for data analysis.

> **NOTE:**
>
> The **Inclusion rule/Exclusion rule** parameters support wildcards. Search is not case sensitive.
>
> To illustrate how to use wildcard queries, consider the following example. You have selected 4 hosts as a report scope: 2 NAS servers (*NASserv1*, *NASserv2*) and 2 Active Directory servers (*AD01* and *AD02*).
>
> If you want the report to show performance details only for the NAS servers, type *nasserv** in the **Inclusion rule** field. Alternatively, type *ad** in the **Exclusion rule** field.

Hyper-V Raw Performance Data

Description

This report allows you to get detailed raw data on specific metrics to analyze performance of Hyper-V infrastructure elements.

Report Parameters

Selected object:	Virtual Infrastructure
Report creation date:	12/26/2022 6:03 AM
Report period:	11/26/2022 - 12/26/2022
Object type:	Hosts
Exclusion rule:	
Inclusion rule:	*
Business View objects:	
Sample size:	Raw
CPU:	Total Run Time (Percent), Total Run Time (MHz)

Subsystem: CPU

Counter: Total Run Time

Object Name	Value (Percent)	Time
hyperv01	4410.00	1/7/2019 1:00 PM
hyperv01	21.00	1/7/2019 3:00 PM
hyperv01	5187.00	1/7/2019 3:00 PM
hyperv01	18.00	1/7/2019 5:00 PM
hyperv01	4475.00	1/7/2019 5:00 PM
hyperv01	17.00	1/7/2019 7:00 PM
hyperv01	4225.00	1/7/2019 7:00 PM
hyperv01	17.00	1/7/2019 9:00 PM
hyperv01	4259.00	1/7/2019 9:00 PM
Max Observed:	21.00	1/7/2019 3:00 PM
Min Observed:	17.00	1/1/2019 1:00 AM
Average:	17.44	1/1/2019 1:00 AM - 1/7/2019 9:00 PM

Object Name	Value (Percent)	Time
hyperv02	10.00	1/1/2019 1:00 AM
hyperv02	2510.00	1/1/2019 1:00 AM
hyperv02	10.00	1/1/2019 3:00 AM
hyperv02	2516.00	1/1/2019 3:00 AM
hyperv02	10.00	1/1/2019 5:00 AM
hyperv02	2497.00	1/1/2019 5:00 AM
hyperv02	10.00	1/1/2019 7:00 AM
hyperv02	2497.00	1/1/2019 7:00 AM
hyperv02	10.00	1/1/2019 9:00 AM
hyperv02	2512.00	1/1/2019 9:00 AM
Max Observed:	10.00	1/1/2019 3:00 AM
Min Observed:	10.00	1/1/2019 9:00 AM
Average:	10.00	1/1/2019 1:00 AM - 1/1/2019 9:00 AM

Use Case

This report provides advanced historical performance data that you can export to a spreadsheet application and use for analysis and reporting purposes.

Hypervisor Version

This report provides information on hypervisor versions used in your infrastructure.

- The **Summary** section includes the following charts:
  - The **VMware ESXi** chart shows the versions and build numbers of VMware ESXi servers and the percentage of hosts on which each hypervisor runs.
  - The **VMware vCenter** chart shows the versions and build numbers of VMware vCenter servers and the number of servers on which each VMware vCenter entity runs.
- The **Details** table provides information on the vCenter server and hypervisor version with the build number and the hosts on which each hypervisor version runs.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.

View Report Example

Use Case

To improve host performance, enhance compatibility and enable additional features across the environment, VMware recommends that you upgrade to the latest hypervisor version.

The report allows you to check hypervisor versions installed on your hosts, and make sure you run the latest available version.

Idle Templates

Templates are preconfigured images of your VMs that help you to easily deploy multiple copies of the model VMs across the infrastructure.

- The **Summary** section shows the total number of templates, the number of idle templates and the amount of wasted storage space.
- The **Details** table provides information on inactive templates, including template location, size and the last time the template was used.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **Allowed period of inactivity**: defines the amount of time that the template must be inactive to be included in the report.

> **NOTE:**
>
> You can exclude specific datastores from this report. This can be useful when you are not interested in examining particular datastores for garbage files (for example, local datastores, datastores hosting `ISO` files or backups). In this case, you can exclude unnecessary datastores from the collection scope. For more information, see Choosing Datastores to Report On.

View Report Example

Use Case

VM templates consume valuable storage resources. Use this report to review the list of your templates and identify templates that can be deleted or moved to less costly datastores to reclaim additional storage space.

Idle VMs (Hyper-V)

Idle VMs are virtual machines that continue to operate even though they are no longer in use. These Idle VMs keep consuming resources and provide no value.

- The **Summary** section includes the following elements:
  - The **Idle/Active VMs** chart shows the number of idle and active VMs.
  - The **Wasted Storage, GB** chart shows the amount of valuable and wasted storage resources.
  - The **Idle CPU, GHz** and **Idle Memory, GB** charts show the amount of active and idle CPU and memory resources.
- The **Details** table provides information on idle VMs, including cluster or host name, VM name, CPU, memory, disk and network usage, and the number of days during which VM was inactive.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **Business View objects**: defines Veeam Backup & Replication groups to analyze in the report. The parameter options are limited to objects of the Virtual Machine type.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.
- **Period**: defines the time period to analyze in the report. Note that the reporting period must include at least one successfully completed *Object properties data collection* task for the selected scope. Otherwise, the report will contain no data.
- **CPU usage, less than**: defines a CPU usage threshold. If the average CPU usage for a VM is below the threshold during a certain number of days (specified with the Time in the selected state parameter), the VM will be considered "Idle".
- **Memory pressure, less than**: defines memory usage threshold. If the average memory usage for a VM is below the threshold during a certain number of days (specified with the Time in the selected state parameter), the VM will be considered "Idle".
- **Disk usage, less than**: defines a disk usage threshold. If the average disk usage for a VM is below the threshold during a certain number of days (specified with the Time in the selected state parameter), the VM will be considered "Idle".
- **Network usage, less than**: defines a network usage threshold. If the average network usage for a VM is below the threshold during a certain number of days (defined by Time in the selected state), the VM will be considered "Idle".
- **Time spent in the defined conditions**: defines the percentage of days in the reporting period when the average resource usage (CPU, Memory, Disk and Network) of the VM was below the selected thresholds.

NOTE:

Veeam ONE Web Client checks whether the **CPU usage**, **Memory pressure**, **Disk usage** and **Network usage** conditions are all true (in other words, the conditions are joined by Boolean "AND").

Idle VMs

Description

This report shows a list of idle VMs in terms of CPU, memory, disk and network utilization parameters.

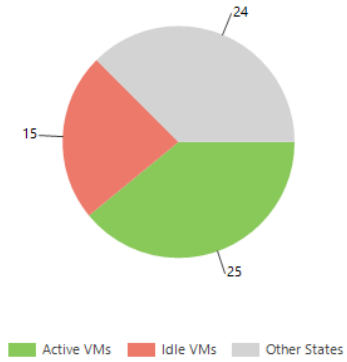
Report Parameters

Scope:	Virtual Infrastructure
Interval:	1 week (2/9/2021 - 2/15/2021)
CPU usage:	0.1 GHz
Memory pressure:	0.256 GB
Disk usage:	20 KBps
Network usage:	1 KBps
Time spent in the defined conditions:	for more than 90 % of the time
Business View objects:	

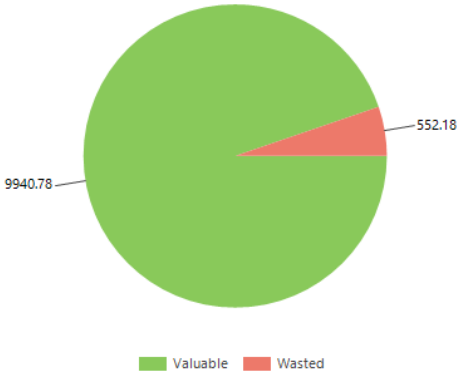
Summary

Total VMs:	64
Idle VMs:	15
Powered-off VMs:	24

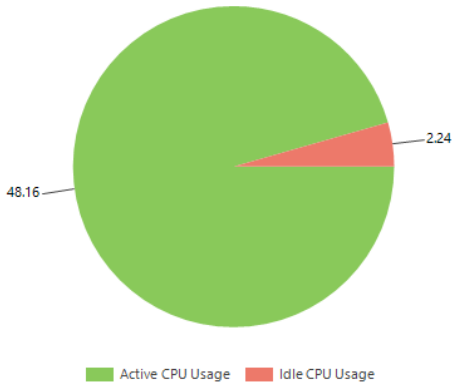
Idle/Active VMs



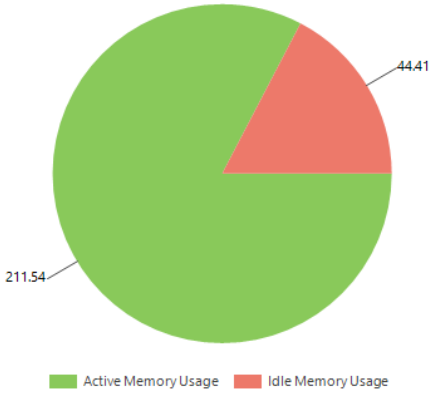
Wasted Storage, GB



Idle CPU, GHz



Idle Memory, GB



Details

SCVMM: N/A

Cluster/Host	Virtual Machine	CPU Usage (MHz)	Memory Usage (GB)	Disk Usage (KBps)	Network Usage (KBps)	Time in This State (days)
cluster01	15					
	Lin13	0.00	0.50	0.00	1.10	9
	oracle03	0.00	0.00	0.00	1.10	9
	ORACLEDBLINUX	0.00	4.00	0.00	1.10	9
	VBR_REPOSITORY	0.00	4.00	0.00	1.10	9
	veeamcol1	0.00	0.99	0.00	1.10	9
	VM2	0.00	3.91	0.00	1.10	9
	fileserv03	0.00	0.00	2.36	1.23	9
	wrk03	89.35	4.00	24.88	4.08	8
	zeta	0.00	4.00	3.11	1.19	7
	Storage_1	16.04	4.00	4.37	1.76	6
	db001	4.58	4.00	9.29	1.20	6
	VBR01Repository	586.47	6.00	55.12	1.79	6
	VBR01	756.00	4.00	9.15	1.32	4
	vsa	767.45	1.01	5.57	4.55	1
	Storage_3	18.33	4.00	5.42	2.07	1

Use Case

This report can help you track VMs that can be shut down or decommissioned to reclaim resources and improve performance of your virtual infrastructure.

Idle VMs (vSphere)

Idle VMs are virtual machines that remain running even though they are no longer used, for example the project or POC is complete — but the VMs were never decommissioned. These Idle VMs consume CPU, memory and storage resources that could be used by other active machines.

This report shows a list of idle VMs in terms of CPU, memory, disk and network utilization.

- The **Summary** section includes the following elements:
  - The **Idle/Active VMs** chart shows the number of idle and active VMs.
  - The **Wasted Storage, GB** chart shows the amount of valuable and wasted storage resources.
  - The **Idle CPU, GHz** and **Idle Memory, GB** charts show the amount of active and idle CPU and memory resources.
- The **Details** table provides information on idle VMs, including cluster or host name, VM name, CPU, memory, disk and network usage, and the number of days during which VM was inactive.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **VMware Cloud Director objects**: defines VMware Cloud Director components to analyze in the report.
- **Business View objects**: defines Business View groups to analyze in the report. The parameter options are limited to objects of the Virtual Machine type.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.
- **Last <N>**: defines the time period to analyze in the report. Note that the reporting period must include at least one successfully completed *Object properties data collection* task for the selected scope. Otherwise, the report will contain no data.
- **CPU usage, less than (GHz)**: defines CPU usage threshold. If the average CPU usage for a VM is below the threshold during certain number of days (defined by Time in the selected state), the VM will be considered to be "Idle".
- **Memory consumed, less than (GB)**: defines memory usage threshold. If the average memory usage for a VM is below the threshold during certain number of days (defined by Time in the selected state), the VM will be considered to be "Idle".
- **Disk usage, less than (KBps)**: defines disk usage threshold. If the average disk usage for a VM is below the threshold during certain number of days (defined by Time in the selected state), the VM will be considered to be "Idle".
- **Network usage, less than (KBps)**: defines network usage threshold. If the average network usage for a VM is below the threshold during certain number of days (defined by Time in the selected state), the VM will be considered to be "Idle".

- **Time spent in the defined conditions (%)**: defines the percentage of days in the reporting period when the average resource usage (CPU, Memory, Disk and Network) of the VM was below the selected thresholds.

> **NOTE:**
>
> Veeam ONE Web Client checks whether the **CPU usage**, **Memory consumed**, **Disk usage** and **Network usage** conditions are true at the same time (in other words, the conditions are joined by "AND").

View Report Example

Use Case

Idle VMs waste valuable storage resources. Use this report to review performance of your VMs and identify VMs that can be shut down or reconfigured to reclaim additional storage resources.

Immutable Workloads

This report lists workloads and their restore points providing information on whether immutability targets are met by these workloads and their backups.

- The **Summary** section provides the numbers of mutable and immutable workloads and restore points as well as their immutability ratio, and includes the following elements:
  - The **Workloads by Immutability** chart shows the number of mutable and immutable workloads.
  - The **Restore Points by Immutability** chart shows the number of mutable and immutable restore points.
  - The **Workload Types by Immutability** chart shows the number of mutable and immutable workloads of each workload type.
- The **Details** table provides information about every immutable and mutable workload including the workload platform, name and type of a backup job, target repository, number of available and immutable restore points, date and time of the latest and oldest immutable restore points creation.

  To get the detailed information on restore points of each workload, click the link in the workload name. The drill-down report page will open.

  To get the detailed information on restore points created by a specific backup job, click the link in restore point number. The drill-down report page will open.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a list of Veeam Backup & Replication servers to include in the report.
- **Business View objects**: defines Business View groups to analyze in the report.
- **Protected workload types**: defines types of protected workloads to analyze in the report (*Virtual machine*, *Computer*, *Unstructured data*, *Cloud instance*, *Enterprise application*).
- **Job types**: defines a job type to analyze in the report (*VM backup*, *Backup copy*, *Agent backup policy*, *Agent backup*, *File backup*, *Cloud backup policy*, *Application backup policy*, *Object Storage backup Cloud Director backup*).
- **Jobs**: defines a list of jobs to analyze in the report.
- **Workload exclusion rule**: defines a list of workloads that should be excluded from the report scope. You can enter workload names explicitly or create a wildcard mask by using the asterisk (*) to replace any number of characters. Multiple entries are separated by semicolon. Usage example: the following string will exclude workloads with the _R&D suffix from appearing in the report: **_R&D*.
- **Detailed immutability target**: defines whether specific immutability target values must be applied to the analyzed workloads. You can specify target immutability period and number of immutable restore points.

> **NOTE:**
>
> Infrastructure topology view in Veeam ONE and Veeam Backup & Replication must match. Otherwise, Veeam ONE may show invalid data for Veeam Backup & Replication reports and dashboards.

View Report Example

Use Case

This report helps to make sure workloads and their backups are safely protected from loss as a result of attacks, malware activity or any other injurious actions.

Inefficient Datastore Usage

This report provides an overview of storage devices that accommodate inactive virtual machines.

- The **Storage Consumed by Inactive VMs (GB)** chart displays the amount of storage space consumed by VMs that have been inactive for one month, six months and one week.
- The **Details** table shows the full list of inactive VMs and rates the VMs by the amount of consumed storage.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **VMware Cloud Director objects**: defines VMware Cloud Director components to analyze in the report.
- **Business View objects**: defines Business View groups to analyze in the report. The parameter options are limited to objects of the Virtual Machine type.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.

View Report Example

Use Case

Inactive VMs consume valuable storage space. Use this report to review performance of your VMs and identify VMs that can be deleted or relocated to less costly datastores to reclaim additional storage space.

Infrastructure Changes Audit

This report analyzes virtual infrastructure configuration changes and provides information on users who performed these changes.

- The **Summary** section includes the following elements:
  - The **Top 10 VMs/Hosts/Datastores with Changes** tables show VMs, hosts and datastores with the biggest number of changes.
  - The **Number of Changes Made** chart shows how many changes were made during the reporting period.
  - The **Modifications per User (Top 5)** chart shows users who made the most changes during the reporting period.
- The **Change Details** table provides information on changes made, including initiator, event description, changed object name, location and type, and date and time when event occurred.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **Business View objects**: defines Business View groups to analyze in the report.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.
- **Period**: defines the time period to analyze in the report. Note that the reporting period must include at least two successfully completed *Object properties data collection* tasks for the selected scope. Otherwise, the report will contain no data.
- **Object types**: defines types of virtual infrastructure objects to analyze in the report.
- **Users**: defines users whose activity should be analyzed in the report.

- **Sort by**: defines how data should be sorted in the report (by *Time of Occurrence*, *Initiator*, *Object Name*).

Infrastructure Changes Audit

Description

This report tracks configuration changes in your virtual environment, providing detailed information about every change for each user.

Report Parameters

Scope:	Virtual Infrastructure
Reporting period:	1 week (1/5/2023 - 1/11/2023)
Object types:	Any object types
Users:	All
Sort by:	Time of occurrence

Summary

Top 10 VMs with Changes

VM Name	Cluster/Host	# of Changes
winorcl01	prgtwesx01.tech.local	18674
dlsql01	prgtwesx01.tech.local	11974
as2016DC	prgtwesx01.tech.local	2357
enterprise05	prgtwesx01.tech.local	327
vbr12servicevm4	prgtwesx03.tech.local	297
vboservicevm	prgtwesx03.tech.local	184
vbr12servicevm3	prgtwesx03.tech.local	153
ts-vm01-xbds	prgtwesx01-virt.tech.local	67
ts-vm022-lVrN	prgtwesx01-virt.tech.local	67
winsrv002	prgtwesx01.tech.local	57

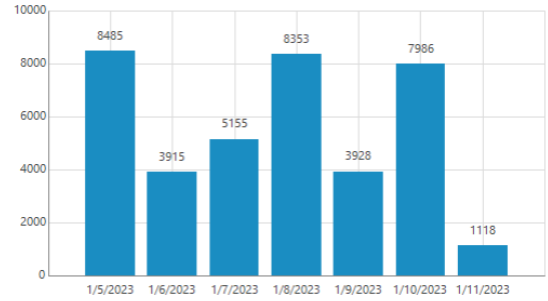
Top 10 Hosts with Changes

Host Name	# of Changes
prgtwesx01.tech.local	681
prgtwesx02-virt.tech.local	106
prgtwesx02.tech.local	61
prgtwesx03.tech.local	61
prgtwesx01-virt.tech.local	50

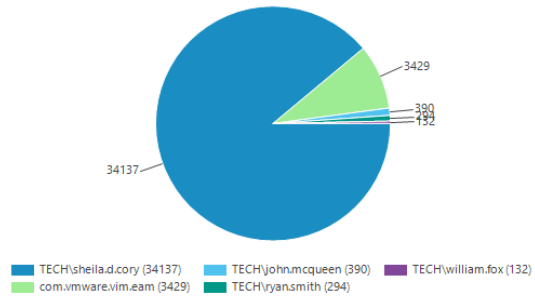
Top 10 Datastores with Changes

Datastore Name	# of Changes
prgtwesx01-ds01	1

Number of Changes Made



Modifications per User (Top 5)



Change Details

Initiator	Event Description	Time	Object	Location	Object Type
TECH\sheila.d.cory	Guest operation Validate Credentials performed on Virtual machine winorcl01.	1/5/2023 12:00:30 AM	winorcl01	>Virtual Infrastructure>vcenter01.tech.local>Prague>prgtwesx01.tech.local	vSphere Virtual Machine
TECH\sheila.d.cory	Guest operation Validate Credentials performed on Virtual machine winorcl01.	1/5/2023 12:00:31 AM	winorcl01	>Virtual Infrastructure>vcenter01.tech.local>Prague>prgtwesx01.tech.local	vSphere Virtual Machine
TECH\sheila.d.cory	Guest operation Validate Credentials performed on Virtual machine virt01-vm33.	1/5/2023 12:00:44 AM	virt01-vm33	>Virtual Infrastructure>vcenter01.tech.local>Prague>CDP cluster>prgtwesx01-virt.tech.local	vSphere Virtual Machine
TECH\sheila.d.cory	Guest operation Create Temporary File performed on Virtual machine virt01-vm33.	1/5/2023 12:00:44 AM	virt01-vm33	>Virtual Infrastructure>vcenter01.tech.local>Prague>CDP cluster>prgtwesx01-virt.tech.local	vSphere Virtual Machine
TECH\sheila.d.cory	Guest operation Delete File performed on Virtual machine virt01-vm33.	1/5/2023 12:00:44 AM	virt01-vm33	>Virtual Infrastructure>vcenter01.tech.local>Prague>CDP cluster>prgtwesx01-virt.tech.local	vSphere Virtual Machine
TECH\sheila.d.cory	Guest operation List Files performed on Virtual machine virt01-vm33.	1/5/2023 12:00:44 AM	virt01-vm33	>Virtual Infrastructure>vcenter01.tech.local>Prague>CDP cluster>prgtwesx01-virt.tech.local	vSphere Virtual Machine

Use Case

The report allows IT administrators to get details on recent infrastructure changes made by authorized users so that any unwanted action can be quickly rolled back.

Infrastructure Changes by Object

This report analyzes virtual infrastructure configuration changes and provides detailed information on changes performed for each object within the reporting period.

- The **Summary** section shows which object types were modified during the reporting period and provides information on update, deletion and creation counts for each object type.
- The **Details** table provides information on modified objects, including change type, object name, type and location, property changed and new and old values of the property.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **Business View objects**: defines Business View groups to analyze in the report.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.
- **Period**: defines the time period to analyze in the report. Note that the reporting period must include at least two successfully completed *Object properties data collection* tasks for the selected scope. Otherwise, the report will contain no data.
- **Object types**: defines a list of infrastructure objects to analyze in the report. To select multiple items, use the [Ctrl] or [Shift] key.
- **Object properties**: defines configuration properties for which the report will track changes. The list of available properties will depend on the selected object type. Use the **Filter** field to search for the necessary properties by name.

- **Show all historical changes of properties during the selected period**: defines whether to include in the report all historical changes for the specified time period.

Infrastructure Changes by Object

Description

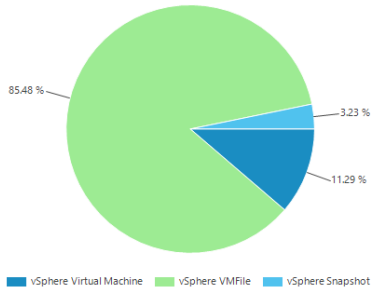
This report tracks configuration changes in your virtual environment, providing detailed information about every change for each object.

Report Parameters

Scope:	Virtual Infrastructure
Reporting period:	1 day (1/10/2023)
Object types:	Any object types
Object properties:	Power state
Show all historical changes of properties during the selected period:	True

Summary

Modified Objects Per Object Types



Object Type	Object Update Count	Object Deletion Count	Object Creation Count
vSphere Virtual Machine	7	0	0
vSphere VMFile	0	11	42
vSphere Snapshot	0	0	2

Details

Object Type: vSphere Virtual Machine

Object Name	Object Location	Property	New Value	Old Value
Change Type: Updated				
winsrv005	>Virtual Infrastructure>vcenter01.tech.local>Prague>prgtwesx01.tech.local	Power state	poweredOff	poweredOn
backupserver001	>Virtual Infrastructure>vcenter01.tech.local>Prague>prgtwesx01.tech.local	Power state	poweredOn	poweredOff
wrk004	>Virtual Infrastructure>vcenter01.tech.local>Prague>prgtwesx01.tech.local	Power state	poweredOn	poweredOff
SQLSRV002	>Virtual Infrastructure>vcenter01.tech.local>Prague>prgtwesx01.tech.local	Power state	poweredOn	poweredOff
SQLSRV001	>Virtual Infrastructure>vcenter01.tech.local>Prague>prgtwesx01.tech.local	Power state	poweredOn	poweredOff
ts-vm01-ZVIV	>Virtual Infrastructure>vcenter01.tech.local>Prague>CDP cluster>prgtwesx01-virt.tech.local	Power state	suspended	poweredOn
ts-vm022-1ZGE	>Virtual Infrastructure>vcenter01.tech.local>Prague>CDP cluster>prgtwesx02-virt.tech.local	Power state	suspended	poweredOn

Use Case

The report allows senior IT administrators to get details on recent infrastructure modifications made to target objects so that any unwanted action can be quickly rolled back.

Infrastructure Overview (Hyper-V)

This report reveals the necessary Hyper-V inventory configuration specifics and allows you to evaluate the current state of your virtual environment.

The subsections provide detailed information on SCVMM servers, clusters, CSVs, SMB shares, local disks, host systems and networks. The report also includes charts that display percentage distribution of VM power states, Integration Services statuses and Business View groups across the infrastructure.

TIP:

- Click a SCVMM server name in the **SCVMM Servers** table to drill down to details on hypervisor version installed on the server and the list of hosts that run on the server.
- Click the **Details** link below the **Power State** chart to drill down to the full list of VMs and their power states.
- Click the **Details** link below the **Integration Service Status** chart to drill down to the full list of VMs and statuses of Integration Services running in these VMs.
- Click the **Details** link below the **BV Chart** to drill down to the full list of Business View categories and VMs that belong to these categories.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.

- **Business View VM category**: defines a Business View group that includes VMs to analyze in the report.

Infrastructure Overview

Description

This report provides general Hyper-V inventory configuration information, including all SCVMMs, clusters, hosts, VMs, datastores, and networks in your virtual environment.

Report Parameters

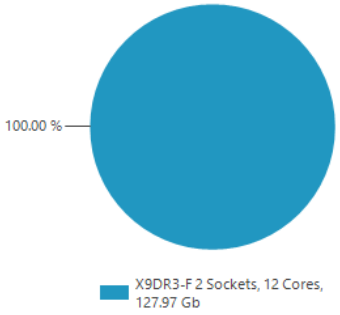
Scope:	Virtual Infrastructure
Business View VM category:	SLA

Summary

Hosts per Cluster:	2.0
VMs per Host:	13.0
Datastores per Host:	2.5
VMs per Datastore:	5.2

Hosts

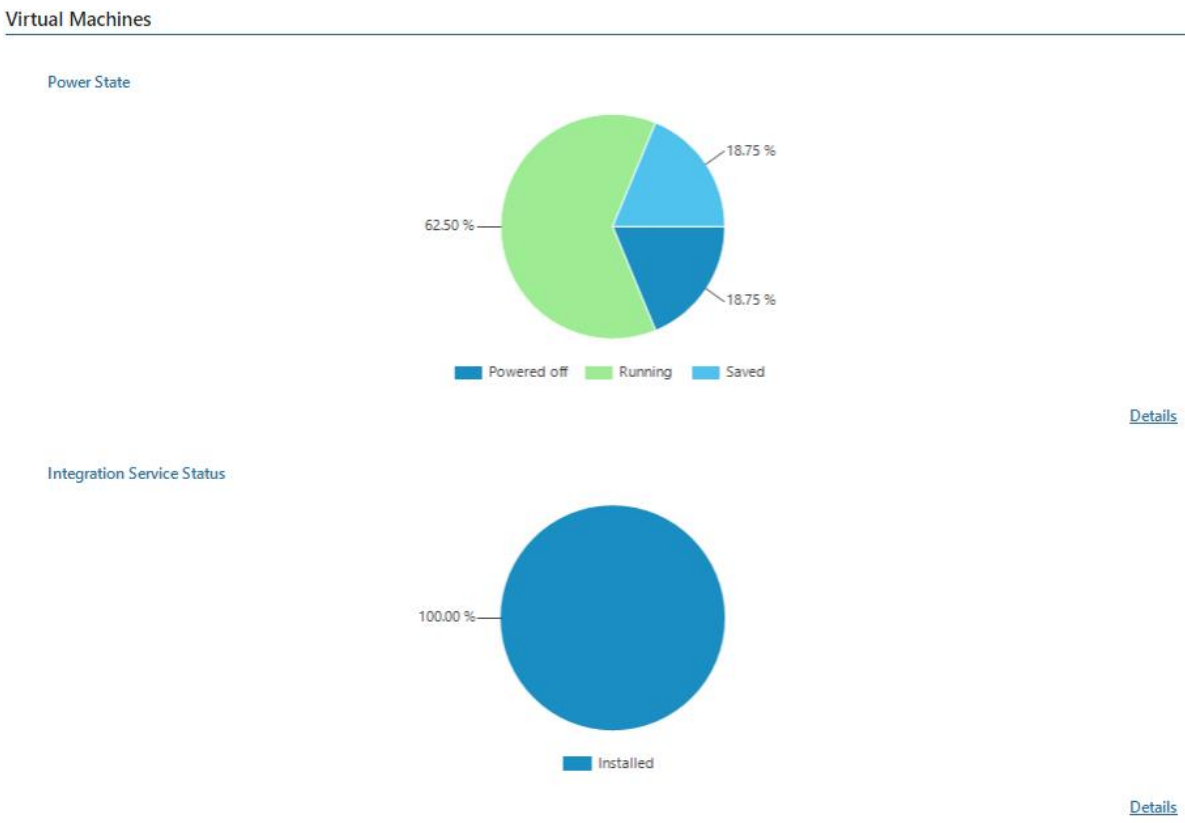
Top Hosts Configurations



Details

All Hosts Configurations

SCVMM	Cluster	Cores	Memory (GB)	Host
N\A	⊟ cluster01	24	255.95	2
		12	127.97	hyperv01
		12	127.97	hyperv02
Total:		24	255.95	2



Use Case

The report helps administrators track the state of monitored virtual infrastructure.

Infrastructure Overview (Visio)

This report shows a diagram of the VMware vSphere and Microsoft Hyper-V infrastructure. The infrastructure is presented with a set of diagrams that illustrate different views, or inventories:

- Configuration inventory
- Storage inventory
- Network inventory (available for VMware vSphere only)
- Datastore Utilization (available for VMware vSphere only)
- vMotion (available for VMware vSphere only)

> **NOTE:**
>
> To view the report, you must have Microsoft Visio installed.

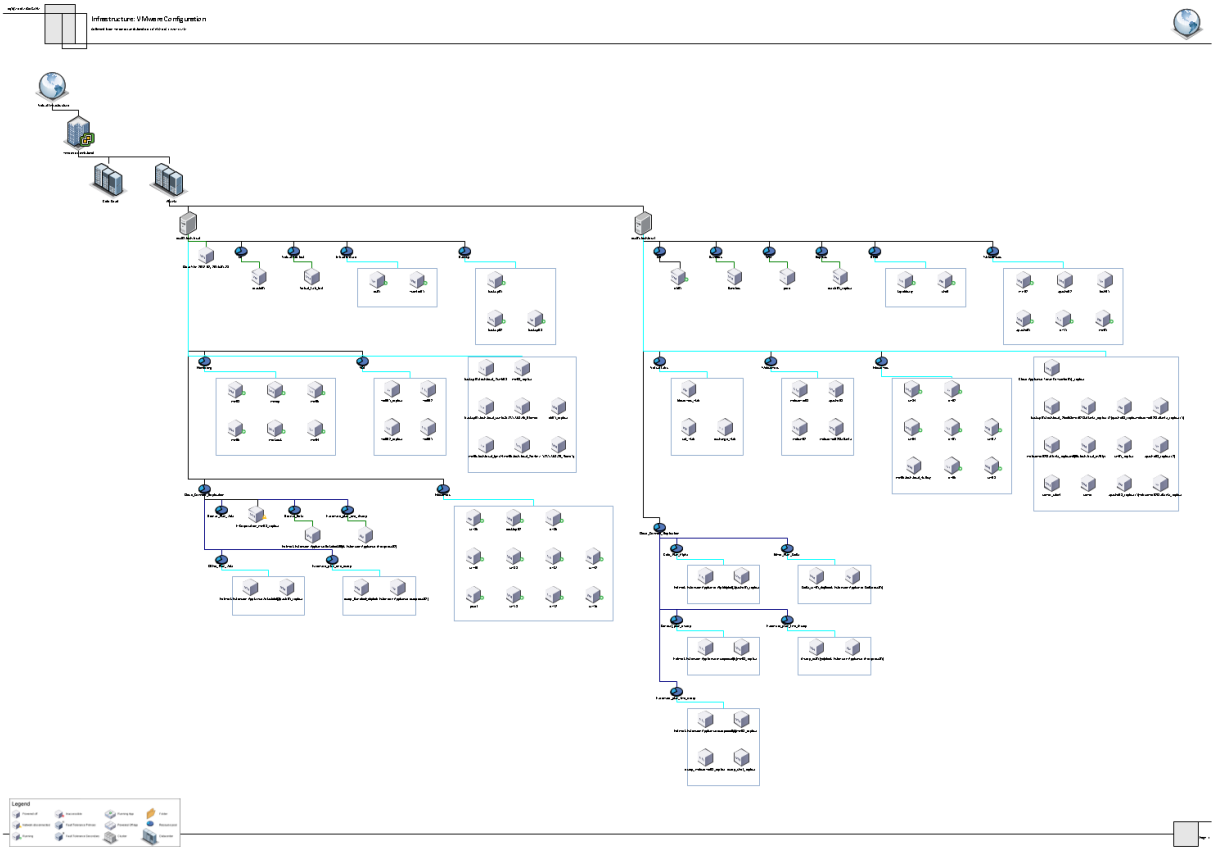
Report Parameters

You can specify the following report parameters:

- **Scope**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **Show VMs**: defines whether to show VMs in the report.

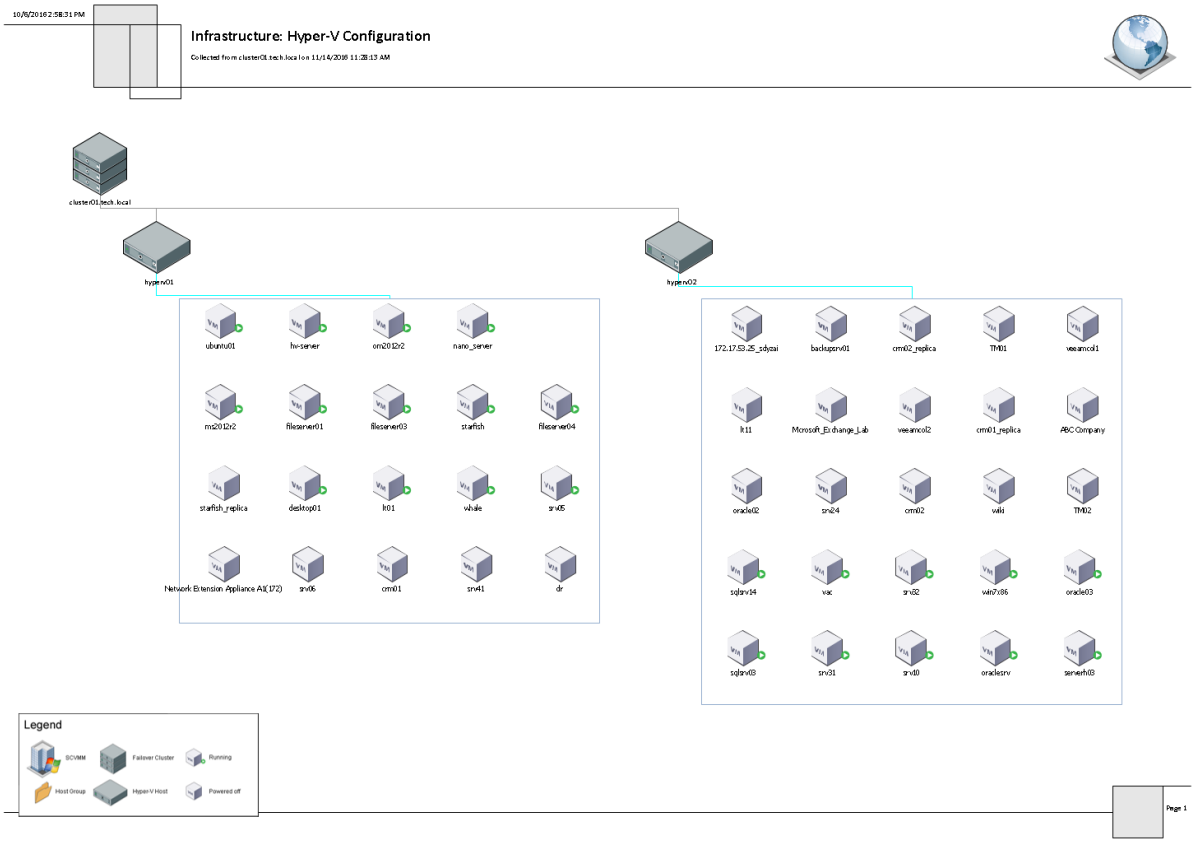
Infrastructure: VMware Configuration

The following diagram displays VMware vSphere configuration inventory.



Infrastructure: Hyper-V Configuration

The following diagram displays Microsoft Hyper-V configuration inventory.



Use Case

The report includes a set of Microsoft Visio diagrams that show infrastructure configuration from different viewpoints.

This offline report provide details on major health and configuration properties. Advanced topology maps that are not available with other competing products provide automatically generated representation of your virtual infrastructure layout in a Visio format. To view this report offline, you must first install Veeam Report Viewer and

Installing Veeam Report Viewer

To view Veeam ONE offline reports, Veeam Report Viewer software is required.

To download and install Veeam Report Viewer:

1. Open Veeam ONE Web Client.
2. Open the **Reports** section.
3. In the hierarchy on the left, select **Offline Reports**.
4. In the list of offline reports, click any report.
5. In the information section, click the **Veeam Report Viewer** link.

6. Download the `VmReportViewerSetup.msi` installer file.
7. On the machine where you want to install the Veeam Report Viewer, launch the installer file to start the **Veeam Report Viewer** setup wizard.
8. Follow the steps of the setup wizard to install Veeam Report Viewer.

Viewing Offline Reports

To access and view offline reports:

1. In the list of offline reports, click the report.
2. Specify the report parameters.
3. Click **Preview** to generate a report file.

   Veeam ONE Web Client will generate a file with the `VMR` extension and save it to the download location.
4. Open the downloaded file on the machine where Veeam Report Viewer is installed.

Veeam Report Viewer will process data in the VMR report and prepare the output. The output contains data viewable in Microsoft Visio. Make sure that you have Visio software to open report output files.

Infrastructure Overview (vSphere)

This report provides VMware vSphere inventory configuration information, including all vCenter servers, clusters, hosts, VMs, datastores, and networks in the virtual environment.

The subsections provide detailed information on vCenter servers, clusters, datastores, host systems and networks. The report also includes charts that display percentage distribution of VM power states, VMware Tools statuses and Business View groups across the infrastructure.

TIP:

- Click a vCenter Server name in the **vCenter Servers** table to drill down to the list of hosts managed by the vCenter Server and details on hypervisor version installed on the hosts.
- Click the **Details** link below the **Power State** chart to drill down to the table that shows the list of VMs and their power state.
- Click the **Details** link below the **Tools Status** chart to drill down to the table that shows the list of VMs and status of VMware Tools running on these VMs.
- Click the **Details** link below the **BV Chart** to drill down to the table that shows the list of Business View categories and groups, as well as VMs in these groups.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **Business View VM category**: defines a Business View group that includes VMs to analyze in the report.

View Report Example

Use Case

The report helps administrators track the state of the managed virtual infrastructure.

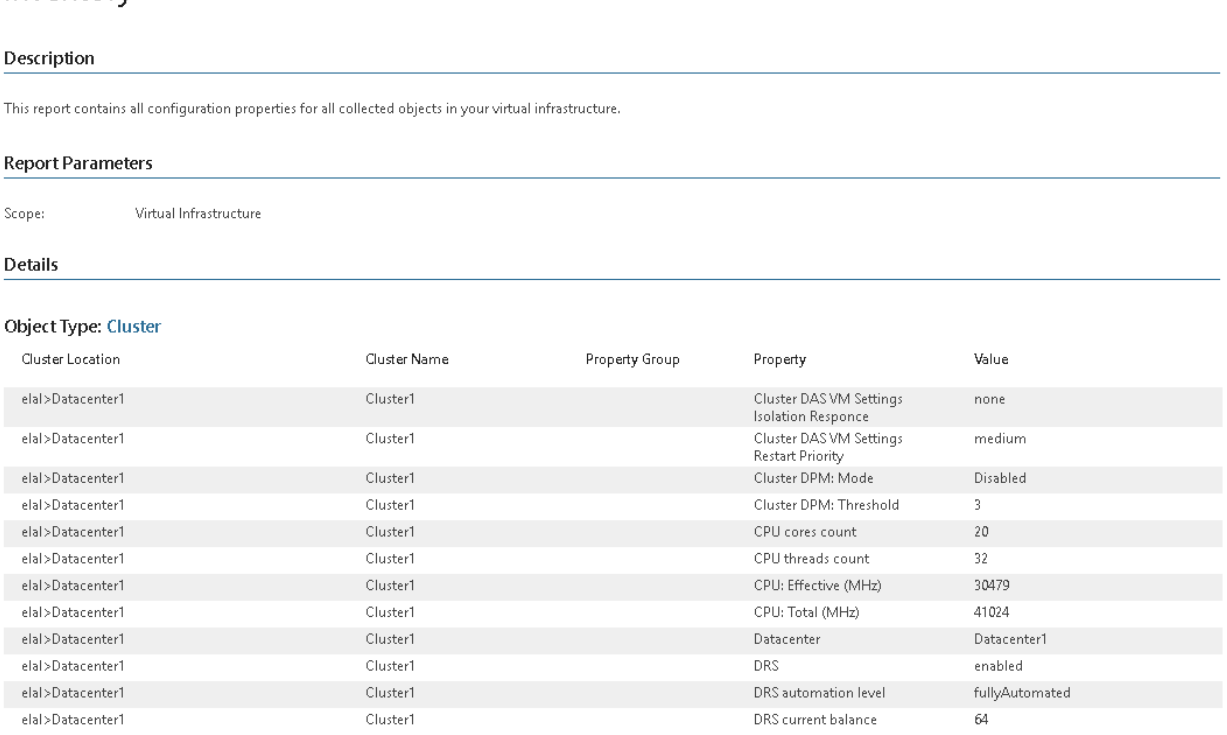
Inventory

This report provides the most complete and up-to-date configuration information on all objects in your virtual environment.

Report Parameters

You can specify the following report parameter:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.



Inventory

Description

This report contains all configuration properties for all collected objects in your virtual infrastructure.

Report Parameters

Scope: Virtual Infrastructure

Details

Object Type: Cluster

Cluster Location	Cluster Name	Property Group	Property	Value
elal>Datacenter1	Cluster1		Cluster DAS VM Settings Isolation Responce	none
elal>Datacenter1	Cluster1		Cluster DAS VM Settings Restart Priority	medium
elal>Datacenter1	Cluster1		Cluster DPM: Mode	Disabled
elal>Datacenter1	Cluster1		Cluster DPM: Threshold	3
elal>Datacenter1	Cluster1		CPU cores count	20
elal>Datacenter1	Cluster1		CPU threads count	32
elal>Datacenter1	Cluster1		CPU: Effective (MHz)	30479
elal>Datacenter1	Cluster1		CPU: Total (MHz)	41024
elal>Datacenter1	Cluster1		Datacenter	Datacenter1
elal>Datacenter1	Cluster1		DRS	enabled
elal>Datacenter1	Cluster1		DRS automation level	fullyAutomated
elal>Datacenter1	Cluster1		DRS current balance	64

Use Case

This report allows you to document the current configuration of your virtual infrastructure for audit purposes.

Job Configuration Change Tracking

This report allows you to keep an eye on backup job configuration changes that occurred during a specified period.

- The **Summary** section includes the following elements:
  - The **Job Modifications by User** chart shows the number of job configuration changes performed by each authorized user.
  - The **Modifications by Day** chart shows the daily number of changes.
- The **Details** table provides information about every change performed within the reporting period, including the backup server where the change was made, the changed job, wizard page, property changed, previous and new setting values, modification date and time, and name of the user who made the change.

Report Parameters

You can specify the following report parameters:

- **Scope**: defines a list of Veeam Backup & Replication servers to include in the report.
- **Period**: defines the time period to analyze in the report.
- **Users**: defines users whose activity must be analyzed.
- **Protection types**: defines a protection type to evaluate in the report (*SureBackup, VM Backup*, *Replication*, *File to tape, Backup copy*, *Agent backup policy, Agent backup, File backup, Nutanix AHV Backup and Snapshot, CDP policy, Application backup policy, Object storage backup, Object to tape backup*).

View Report Example

Use Case

Backup jobs can be configured from the Veeam Backup & Replication console, Veeam Backup Enterprise Manager console, using PowerShell scripts or through REST API. In large environments with multiple backup administrators it is often hard to tell who, when and what changed.

The report helps you review user activity, track job modifications and simplifying troubleshooting.

Job Configuration Dump

The report provides configuration details for Veeam Backup & Replication jobs.

- The **Details** section provides information on Veeam Backup & Replication jobs configuration properties and settings configured for these properties, including schedule, notifications, and backup file encryption settings amongst other additional properties.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a list of Veeam Backup & Replication servers to include in the report.
- **Protection type**: defines types of Veeam Backup & Replication jobs to include in the report (*All items*, *VM backup*, *Replication*, *Backup copy*, *Surebackup*, *File to tape backup*, *Backup to tape*, *File backup*, *Agent backup job*, *Agent backup policy*, *CDP policy*, *Application backup policy, Object storage backup, Object to tape*).
- **Jobs**: defines Veeam Backup & Replication jobs to analyze in the report.
- **Configuration setting areas**: defines job configuration properties to include in the report.

View Report Example

Use Case

The report helps you review settings of Veeam Backup & Replication jobs to ensure that the jobs are properly configured.

Job Data Exclusions

The report provides information about objects, such as VMs, disks, folders and templates, excluded from backup, backup copy and replication jobs in Veeam Backup & Replication.

- The **Summary** section includes **Jobs with Object-level Exclusions**, **Jobs with Disk Exclusions** and **File System Exclusions** charts that display the share of jobs with excluded objects, disks and file system objects and jobs without exclusions.
- The **Exclusions** tables show exclusion settings and objects excluded from processing in Veeam Backup & Replication.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a list of Veeam Backup & Replication servers to include in the report.
- **Job type**: defines types of Veeam Backup & Replication jobs to analyze in the report (*Backup*, *Replication*, *Backup Copy*, *All types*).
- **Jobs**: defines Veeam Backup & Replication jobs to analyze in the report.

View Report Example

Use Case

The report allows you to review exclusion settings configured in jobs and check objects excluded from backups and replicas. For more information in exclude types available in Veeam Backup & Replication, see section Data Exclusion of the Veeam Backup & Replication User Guide.

Job History

This report provides advanced information on completed backup and replication job sessions, and helps you identify possible performance bottlenecks.

- The **Summary** display includes the following elements:
  - The **Top 5 Jobs by Average Duration** and **Top 5 Jobs by Transferred Data** charts display top 5 jobs in terms of the longest backup duration and the largest amount of transferred data.
  - The **Successful Backup Ratio by Day (%)** chart displays the percentage of backup and replication job sessions that completed successfully during the reporting period. If a job session finished with warning but a restore point was created successfully, the job will be displayed as successful.
- The **Report Data** display includes the following elements:
  - The **Job Details** table displays a log of all backup and replication job sessions, including key metrics such as job duration, data size, and transfer rate. Use this table to review historical job performance.
  - The **Job Details (Unstructured Data)** table displays job history details for file share and object storage backups, focusing on jobs that protect unstructured data sources.
  - The **VM Details** table displays per-object details for a specific backup job run, listing each processed virtual machine and showing individual performance metrics such as processing speed and resource usage.
  - The **Unstructured Data Details** table displays a per-source breakdown for an unstructured data backup job, listing each file share or object storage source with associated metrics.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a list of Veeam Backup & Replication servers to include in the report.
- **Job type**: defines a job type to evaluate in the report (*Backup to tape*, *Cloud Director backup*, *Cloud Director replication*, *File backup*, *File copy*, *File to tape*, *Nutanix backup*, *Replication*, *VM backup*, *VM copy*, *All and Add Object Storage*).
- **Jobs**: defines a list of backup and replication jobs to include in the report.
- **Job status**: defines a job status to include in the report (*Success, Success and warnings, Failures and warnings, Failures only, All*).
- **Period**: defines the time period to analyze in the report.

View Report Example

Use Case

This report shows exhaustive information on the state of recent job sessions and reveals key statistics demanded by backup operators.

You can change the default report parameters to focus on particular jobs that include critical VMs; this will allow you to regularly receive information on vital job sessions by email or through a shared portal.

Job History (Veeam Backup for Microsoft 365)

This report provides advanced information on completed Veeam Backup for Microsoft 365 job sessions, and helps you identify possible performance bottlenecks.

- The **Summary** section includes the following elements:
  - The **Top 5 Jobs by Average Duration** and **Top 5 Jobs by Transferred Data** charts display jobs in terms of the backup duration and amount of transferred data.
  - The **Successful Backup Ratio by Day (%)** chart displays the percentage of job sessions that completed successfully during the reporting period. If a job session finished with warning but a restore point was created successfully, the job will be displayed as successful.
- The **Details** table provides information on each performed job, including completion status, number of processed objects, session start time, job duration, processing rate and the amount of transferred data.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a list of Veeam Backup for Microsoft 365 servers to include in the report.
- **Organizations**: defines Microsoft organizations to analyze in the report.
- **Job types**: defines a job type to evaluate in the report (*Backup*, *Backup Copy*).
- **Jobs**: defines a list of jobs to include in the report.
- **Job status**: defines a job status to include in the report (*Success*, *Failed*, *Warning*).
- **Period**: defines the time period to analyze in the report.

View Report Example

Use Case

This report shows exhaustive information on the state of recent job sessions and reveals key statistics demanded by backup operators.

You can change the default report parameters to focus on particular jobs; this will allow you to regularly receive information on vital job sessions by email or through a shared portal.

Latest Job Status

This report evaluates the success status of recently performed backup, replication and backup copy jobs. The report shows whether they triggered any errors, warnings or completed successfully on the latest session.

- The **Summary** display includes the following elements:
  - The **Job Status** chart represents overall efficiency of workload protection operations by displaying the total number of idle jobs and jobs whose last session completed successfully/with warnings.
  - The **Top 10 Jobs by Duration** table provides a summary of the top 10 jobs with the longest backup duration.
- The **Report Data** display shows two tables.
  - The **Details** table shows information on backup servers, all jobs performed during the reporting period: job duration, last run and status, objects in job, backed up objects in job, objects with anomalies, the number of processed workloads, the amount of transferred data, retry count, average duration and duration trends. For failed jobs, the report also shows error text.
  - The **Additional Details** table shows information additionally to the details table including object names, backup types, transferred data (in GB), job details, vApp names and object types.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a list of Veeam Backup & Replication servers to include in the report.
- **Period**: defines the time period to analyze in the report.
- **Job types**: defines a list of job types to evaluate in the report (*VM backup*, *Replication*, *File to tape*, *Backup to tape*, *Backup copy*, *Agent backup policy*, *Agent backup*, *Cloud Director Backup*, *Cloud Director Replication* and *Object Storage job types*).
- **Latest statuses**: defines a job run status to include in the report (*Success*, *Warning*, *Failed*).

View Report Example

Use Case

This report helps backup administrators track the recent VM protection operations and identify root causes of failed jobs.

Latest Job Status (Veeam Backup for Microsoft 365)

This report evaluates the success status of recently performed backup and backup copy jobs. The report shows whether they triggered any errors, warnings or completed successfully on the latest session.

- The **Summary** section includes the following elements:
  - The **Job Statuses** chart represents overall efficiency of protection operations by displaying the total number of idle jobs and jobs whose last session completed successfully/with warnings.
  - The table containing a summary of the jobs with the longest backup duration.
- The **Details** section displays information on all jobs performed during the reporting period: job duration and status, the number of processed objects, the amount of transferred data.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a list of Veeam Backup for Microsoft 365 servers to include in the report.
- **Organizations**: defines Microsoft organizations to analyze in the report.
- **Period**: defines the time period to analyze in the report.
- **Job types**: defines a list of job types to evaluate in the report (*Backup*, *Backup Copy*).
- **Latest job statuses**: defines job session statuses to include in the report (*Success*, *Warning*, *Failed*).

View Report Example

Use Case

This report helps backup administrators track the recent Microsoft 365 object protection operations and identify root causes of failed jobs.

Local Datastore Performance

This report aggregates historical data and shows performance statistics for a selected local disk across a time range.

- The **Datastore** subsections provide information on read/write rates, read/write latency and IOPS for the disk, including top 3 resource consuming VMs and resource usage trends.

  Click a VM name in the list of top 3 resource consuming VMs to drill down to performance charts with statistics on CPU, memory, disk and network usage for the VM.

Report Parameters

You can specify the following report parameters:

- **Object**: defines the local disk to analyze in the report.
- **Period**: defines the time period to analyze in the report. Note that the reporting period must include at least one successfully completed *Object properties data collection* task for the selected disk. Otherwise, the report will contain no data.

- **Business hours only**: defines time of a day for which historical performance data will be used to calculate the performance trend. All data beyond this interval will be excluded from the baseline used for data analysis.

Local Datastore Performance

Description

This report shows datastore performance history that includes Usage, Latency and IOPS counters.

Report Parameters

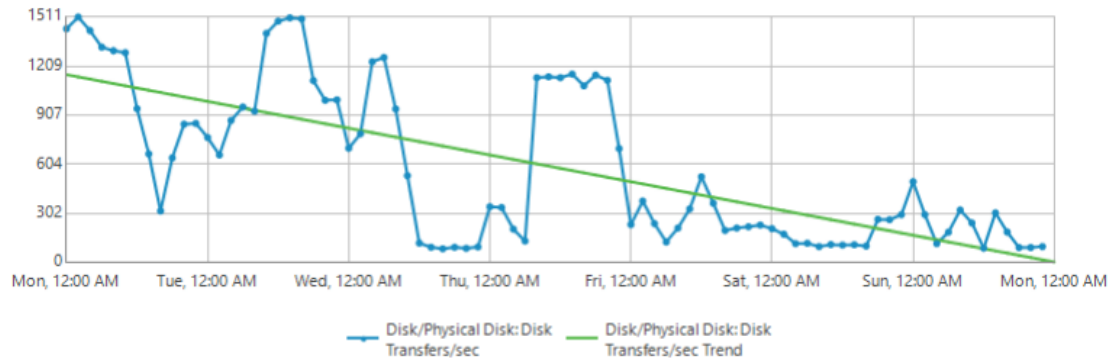
Selected object:	Disk 0 C: D:
Object location:	Virtual Infrastructure\pdctwhv01.tech.local
Reporting period:	12/19/2022 - 12/25/2022

Summary

Name:	Disk 0 C: D:
Type:	local storage
Capacity:	16.4TB
Free Space:	14.0TB
Virtual Machines:	16

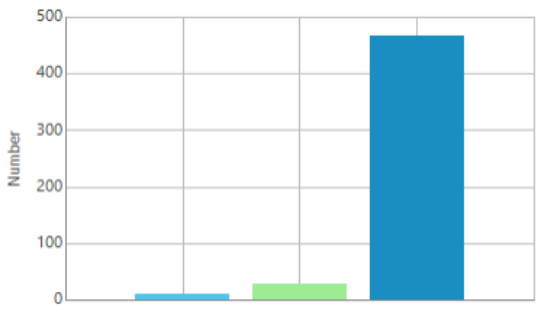
Datastore IOPs

Disk/Physical Disk: Disk Transfers/sec (Number)



Object Name	Average	Minimum	Maximum	Std. Deviation	Trend
Disk 0 C: D:	587.17	85.00	1511.00	476.60	Decreasing

Top 3 VMs by Virtual Storage Reads/Sec



Object Name	Avg	Trend
srv08	467.99	Decreasing
backupsrv50	26.80	Increasing
repo30	11.14	Decreasing

Report created: 12/29/2022 11:52:07 PM ((UTC-08:00) Pacific Time (US & Canada))

Page: 1 of 4

Use Case

The report helps you identify local disks with performance issues.

Malware Detection

This report provides detailed security information about malware anomalies detected across workloads and restore points.

- The **Summary** section includes information for *infected*, *suspicious* and *no anomalies* malware detections:
  - The **Malware-analyzed workloads** chart and table show the total workloads operating on your backup servers by volume that show no suspicious malware activity alongside those displaying suspicious activity.
  - The **Malware-analyzed restore points** chart and table show restore points on your backup servers by volume that show no suspicious activity alongside those displaying suspicious activity.
  - The **Top 5 Backup Servers with workloads anomalies** chart and table display the backup servers that show the most suspicious malware activity.
- The **Details** table displays malware detection information on all backup servers and associated workloads including infected, suspicious, clean and OK statuses. Expand a workload entry to see detection details with a list of individual detection statuses and malware names.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a list of Veeam Backup & Replication servers to include in the report.
- **Workload Status** : defines the status of workloads monitored on your Veeam Backup & Replication servers (*Infected*, *Suspicious*, *Clean*, *OK*).
- **Events to display** : defines the number of events on each of your affected workloads.

View Report Example

Use Case

This report is used to display all potential suspicious and detected malware on your Veeam Backup & Replication servers.

Multiple Clusters Performance

This report aggregates historical data and shows performance statistics for selected clusters across a time range. The report features a predefined list of performance counters and allows you to report on memory, CPU, disk and network usage.

- The **Summary** section describes configuration of each selected cluster, including allocated memory and CPU resources, the number of CPU cores and sockets and CPU and memory usage rates.

  Click a cluster name to drill down to performance charts with statistics on CPU, memory, disk and network usage for the cluster.

- The **Performance** subsections provide information on CPU, memory, disk and network usage, including usage trends and top resource consuming hosts and VMs in the cluster.

  Click a host name in the list of top resource consuming hosts to drill down to performance charts with statistics on CPU, memory, disk and network usage for the host.

  Click a VM name in the list of top resource consuming VMs to drill down to performance charts with statistics on CPU, memory, disk and network usage for the VM.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **Period**: defines the time period to analyze in the report. Note that the reporting period must include at least one successfully completed *Object properties data collection* task for the selected scope. Otherwise, the report will contain no data.
- **Business hours only**: defines time of a day for which historical performance data will be used to calculate the performance trend. All data beyond this interval will be excluded from the baseline used for data analysis.
- **Top N**: defines the maximum number of hosts and VMs to display in the report output.
- **Metrics**: defines a list of performance counters to analyze in the report.

View Report Example

Use Case

The report provides an overview of hardware resource consumption across your clusters. This information may help you identify clusters with performance issues, balance workloads, right-size resource provisioning, redefine DRS settings and optimize cluster overall performance.

Multiple Organizations vDC Performance

This report aggregates historical data and shows performance statistics for selected organization virtual datacenters across a time range. The report features a predefined list of performance counters and allows you to report on memory, CPU, disk and network usage.

- The **Summary** table provides an overview on organization datacenters, including allocation model, used CPU, memory and storage allocation and used network count.

  Click an organization virtual datacenter name in the summary table or in the resource usage table to drill down to performance charts with statistics on CPU, memory, disk and network usage for the virtual datacenter.

- The **Performance** subsections show performance charts with resource usage statistics, list top resource consuming vApps and VMs and resource usage trends for them.

  Click a vApp name in the list of top resource consuming vApps to drill down to performance charts with statistics on CPU, memory, disk and network usage for the vApp.

  Click a VM name in the list of top resource consuming VMs to drill down to performance charts with statistics on CPU, memory, disk and network usage for the VM.

Report Parameters

You can specify the following report parameters:

- **VMware Cloud Director objects**: defines a list of organization virtual datacenters to analyze in the report.
- **Period**: defines the time period to analyze in the report.
- **Business hours only**: defines time of a day for which historical performance data will be used to calculate the performance trend. All data beyond this interval will be excluded from the baseline used for data analysis.
- **Metrics**: defines a list of performance counters to analyze in the report.

- **Top N**: defines the maximum number of vApps and VMs to display in the report output.

Multiple Organizations VDC Performance

Description

This report shows organizations VDC performance history, including CPU, memory, disk and network performance history.

Report Parameters

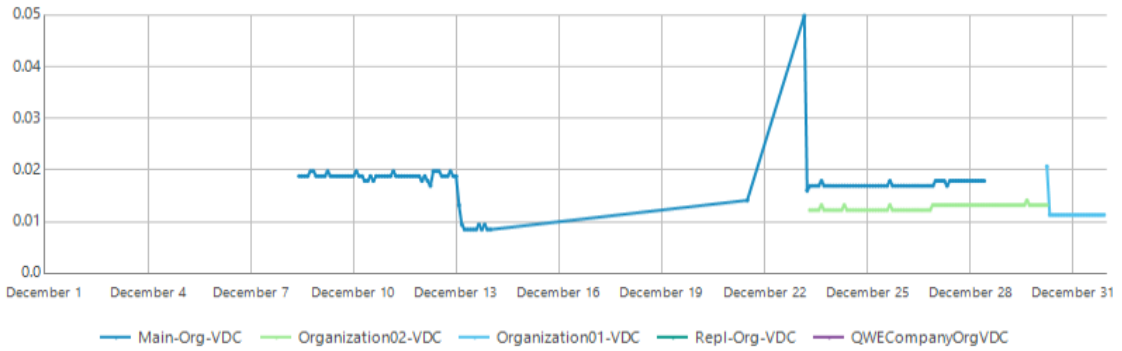
VMware Cloud Director objects:	VMware Cloud Director
Reporting period:	12/1/2022 - 12/31/2022
Metrics:	CPU usage (GHz), Memory usage (GB)
Top N:	3

Summary

Org Virtual Datacenter	Allocation Model	CPU Allocation Used	Memory Allocation Used	Storage Allocation Used	Used Network Count
Main-Org-VDC	Pay As You Go	4.00 GHz	2.00 GB	76.00 GB	0
Repl-Org-VDC	Allocation Pool	0.00 GHz (0.00 %)	0.00 GB (0.00 %)	34.00 GB	0
Organization02-VDC	Pay As You Go	0.00 GHz	0.00 GB	3.00 GB	0
Organization01-VDC	Pay As You Go	0.00 GHz	0.00 GB	2.00 GB	0
QWECompanyOrgVDC	Allocation Pool	0.00 GHz (0.00 %)	0.00 GB (0.00 %)	0.00 GB (0.00 %)	0

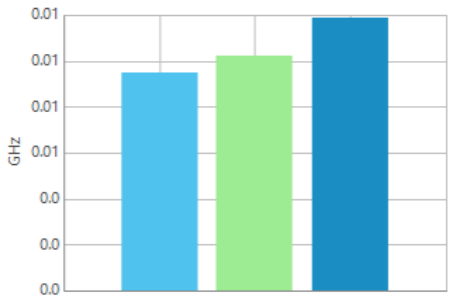
CPU Performance

CPU Usage (Absolute) (GHz)



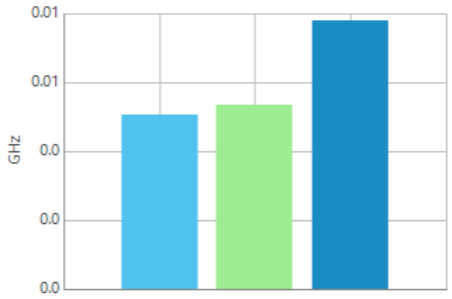
Object Name	Average	Minimum	Maximum	Std. Deviation	Trend
Main-Org-VDC	0.02	0.01	0.05	0.00	Decreasing
Organization02-VDC	0.01	0.01	0.02	0.00	Increasing
Organization01-VDC	0.01	0.01	0.02	0.00	Decreasing
Repl-Org-VDC	0.00	0.00	0.00	0.00	No changes
QWECompanyOrgVDC	0.00	0.00	0.00	0.00	No changes

Top 3 vApps by CPU Usage (Absolute)



Org vDC	vApp	Avg	Trend
Organization01-VDC	vApp01	0.01	Increasing
Main-Org-VDC	vApp-TS	0.01	Decreasing
Organization02-VDC	vApp02	0.01	Increasing

Top 3 VMs by CPU Usage (Absolute)



Org vDC	Virtual Machine Name	Avg	Trend
Organization01-VDC	vm02	0.01	Decreasing
Main-Org-VDC	ts-vm01	0.01	Decreasing
Organization02-VDC	linux02	0.01	Increasing

Use Case

The report helps you identify organization virtual datacenters with performance issues, right-size resource provisioning and eliminate potential performance bottlenecks.

Multiple vApps Performance

This report collects historical information and shows performance statistics on vApps over a specific time period. The report features a list of predefined performance counters and allows you to analyze memory, CPU, memory, disk and network usage.

- The **Performance** subsections show performance charts with resource usage statistics, rate the VMs by the resource usage level, and analyze the resource usage trend.

Report Parameters

You can specify the following report parameters:

- **VMware Cloud Director objects**: defines the organization whose vApps must be analyzed in the report.
- **Period**: defines the time period to analyze in the report.
- **Business hours only**: defines time of a day for which historical performance data will be used to calculate the performance trend. All data beyond this interval will be excluded from the baseline used for data analysis.
- **Metrics**: defines a list of performance counters to analyze in the report.
- **Top N**: defines the maximum number of VMs to display in the report output.

- **Show graphs**: defines whether to include charts in the report output.

Multiple vApps Performance

Description

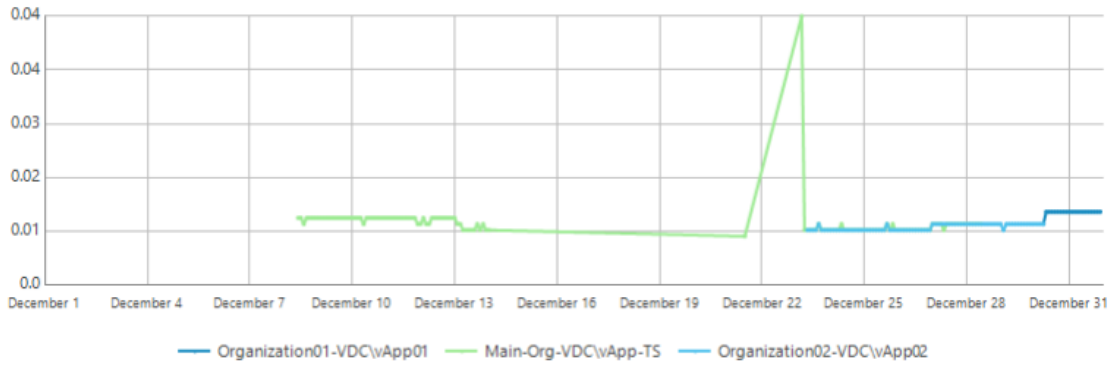
This report shows multiple vApps performance history, including CPU, memory, disk and network performance history.

Report Parameters

VMware Cloud Director objects:	VMware Cloud Director
Reporting period:	12/1/2022 - 12/31/2022
Metrics:	CPU usage (GHz), Memory usage (GB)
Top N:	3

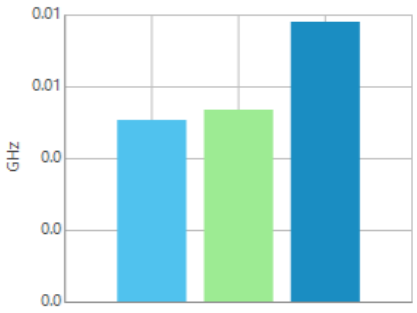
CPU Performance

CPU Usage (Absolute) (GHz)



Object Name	Average	Minimum	Maximum	Std. Deviation	Trend
Organization01-VDC\vApp01	0.01	0.01	0.01	0.00	Increasing
Main-Org-VDC\vApp-TS	0.01	0.01	0.04	0.00	Decreasing
Organization02-VDC\vApp02	0.01	0.01	0.01	0.00	Increasing
Main-Org-VDC\vApp02-TS	0.01	0.01	0.01	0.00	Decreasing
Organization02-VDC\vApp01	0.00	0.00	0.00	0.00	No changes
Repl-Org-VDC\vApp-TS_vcd_cdp_replica					No changes

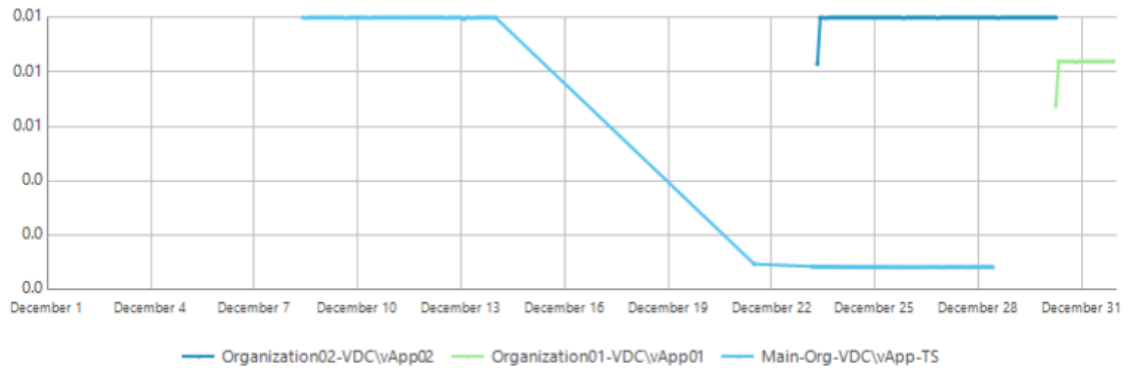
Top 3 VMs by CPU Usage (Absolute)



vApp Name	Virtual Machine Name	Avg	Trend
vApp01	vm02	0.01	Decreasing
vApp-TS	ts-vm01	0.01	Decreasing
vApp02	linux02	0.01	Increasing

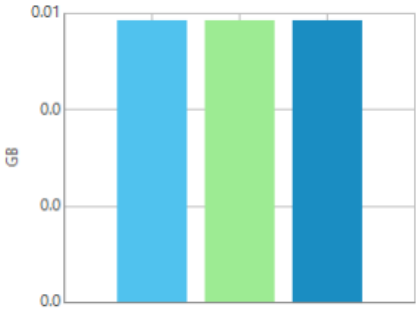
Memory Performance

Memory Consumed (GB)



Object Name	Average	Minimum	Maximum	Std. Deviation	Trend
Organization02-VDC\vApp02	0.01	0.01	0.01	0.00	Increasing
Organization01-VDC\vApp01	0.01	0.01	0.01	0.00	Increasing
Main-Org-VDC\vApp-TS	0.01	0.00	0.01	0.01	Decreasing
Organization02-VDC\vApp01	0.01	0.01	0.01	0.00	No changes
Main-Org-VDC\vApp02-TS	0.00	0.00	0.00	0.00	No changes
Repl-Org-VDC\vApp-TS_vcd_cdp_replica					No changes

Top 3 VMs by Memory Consumed



vApp Name	Virtual Machine Name	Avg	Trend
vApp01	linux01	0.01	No changes
vApp02	linux02	0.01	No changes
vApp02	linux03	0.01	No changes

Use Case

The report provides an overview resource consumption of multiple vApps. This information may help you identify VMs with performance issues, balance workloads, right-size resource provisioning and optimize overall performance.

Organization Configuration

This report documents the current configuration of organizations in your VMware Cloud Director infrastructure.

- The **Summary** table displays general information on statuses of organizations included in the report scope, the total number of virtual datacenters to which these organizations have access, the total number of catalogs created for the organizations and the total number of vApps in the catalogs.
- The **Virtual Datacenters** table provides details on resource utilization for each virtual datacenter and shows the total number of deployed vApps.

  Click a number in the vApps column to drill down to configuration details for the vApp.
- The **vApps** table shows vApp properties, such as vApp power status, vApp owner and the number of resident VMs.
- The **vApp Policies** table displays information on lease policies for compute and storage resources applied to organizations included in the report scope.
- The **Org Network Pools** table shows network pool properties, such as pool type and the current resource utilization level.

Report Parameters

You can specify the following report parameters:

- **VMware Cloud Director objects**: defines a list of organizations to analyze in the report.

Organization Configuration

Description

This report provides general information on VMware Cloud Director organizations configuration.

Report Parameters

VMware Cloud Director objects: VMware Cloud Director

Summary

Organization	Status	Virtual Datacenters	Catalogs	vApps	Total VMs	Running VMs	Users
Main-Org	Enabled	1	0	2	4	2	0
organization01	Enabled	1	1	1	2	0	3
organization02	Enabled	1	0	2	3	0	1
QWECompanyOrg	Enabled	1	0	0	0	0	2
Replica-Org	Enabled	1	0	1	2	0	0

Virtual Datacenters

Organization	Org Virtual Datacenter	Status	Allocation Model	Processor Usage	Memory Usage	Storage Usage	Used Network Count	vApps
⊟Main-Org								
	Main-Org-VDC	Enabled	Pay-As-You-Go	4.00 GHz	2.00 Gb	76.00 Gb	0	2
⊟organization01								
	Organization01-VDC	Enabled	Pay-As-You-Go	0.00 GHz	0.00 Gb	2.00 Gb	0	1
⊟organization02								
	Organization02-VDC	Enabled	Pay-As-You-Go	0.00 GHz	0.00 Gb	3.00 Gb	0	2
⊟QWECompanyOrg								
	QWECompanyOrgVDC	Enabled	Allocation Pool	0.00 GHz	0.00 Gb	0.00 Gb	0	0
⊟Replica-Org								
	Repl-Org-VDC	Enabled	Allocation Pool	0.00 GHz	0.00 Gb	34.00 Gb	0	1

vApps

Organization	Org Virtual Datacenter	vApp	Status	VMs	Created on	Owner
⊟Main-Org	1	2				
	⊟Main-Org-VDC	2				
		vApp02-TS	POWERED_OFF	2	11/17/2022	system
		vApp-TS	POWERED_ON	2	11/11/2022	system
⊟organization01	1	1				
	⊟Organization01-VDC	1				
		vApp01	MIXED	2	12/23/2022	system
⊟organization02	1	2				
	⊟Organization02-VDC	2				
		vApp02	POWERED_OFF	2	12/23/2022	system
		vApp01	POWERED_OFF	1	12/23/2022	system
⊟Replica-Org	1	1				
	⊟Repl-Org-VDC	1				
		vApp-TS_vcd_cdp_replica	POWERED_OFF	2	1/3/2023	system

vApp Policies

Organization	Max. Runtime vApp Lease (Days)	Max vApp Storage Lease (Days)	Storage Cleanup Action	Max N. of VMs	Max N. of Running VMs
Main-Org	7.0	30.0	Move to Expired Items	Unlimited	Unlimited
organization01	7.0	30.0	Move to Expired Items	Unlimited	Unlimited
organization02	7.0	30.0	Move to Expired Items	Unlimited	Unlimited
QWECompanyOrg	7.0	30.0	Move to Expired Items	Unlimited	Unlimited
Replica-Org	7.0	30.0	Move to Expired Items	Unlimited	Unlimited

Org Network Pools

Organization	Org Virtual Datacenter	Name	Status	Type	Pool Used	VDS
⊟Main-Org	1	1				
	⊟Main-Org-VDC	1				
		Main Network Pool	success	VMWNetworkPoolTy	0 of 100000 (0%)	--
⊟organization01	1	1				
	⊟Organization01-VDC	1				
		Main Network Pool	success	VMWNetworkPoolTy	0 of 100000 (0%)	--
⊟organization02	1	1				
	⊟Organization02-VDC	1				
		Main Network Pool	success	VMWNetworkPoolTy	0 of 100000 (0%)	--
⊟QWECompanyOrg	1	1				
	⊟QWECompanyOrgVDC	1				
		Main Network Pool	success	VMWNetworkPoolTy	0 of 100000 (0%)	--
⊟Replica-Org	1	1				

Use Case

The report helps administrators assess configuration properties of organizations in the monitored VMware Cloud Director infrastructure.

Organization VDC Performance

This report aggregates historical data and shows performance statistics for a selected organization virtual datacenter across a time range.

- The **Summary** table provides an overview on organization datacenters, including allocation model, used CPU, memory and storage allocation and used network count.
- The **Performance** subsections show performance charts with resource usage statistics, list top resource consuming vApps and VMs and resource usage trends for them.

  Click a vApp name in the list of top resource consuming vApps to drill down to performance charts with statistics on CPU, memory, disk and network usage for the vApp.

  Click a VM name in the list of top resource consuming VMs to drill down to performance charts with statistics on CPU, memory, disk and network usage for the VM.

Report Parameters

You can specify the following report parameters:

- **Organization virtual datacenter**: defines the organization virtual datacenter to analyze in the report.
- **Period**: defines the time period to analyze in the report.
- **Business hours only**: defines time of a day for which historical performance data will be used to calculate the performance trend. All data beyond this interval will be excluded from the baseline used for data analysis.

- **Top N**: defines the maximum number of vApps and VMs to display in the report output.

Organization VDC Performance

Description

This report shows organization VDC performance history, including CPU, memory, disk and network performance history.

Report Parameters

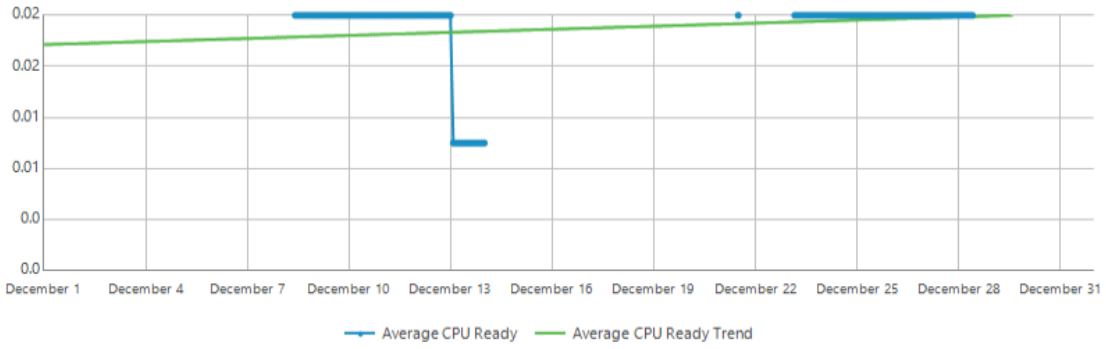
Organization virtual datacenter: Main-Org-VDC
Virtual datacenter location: \\prgclouddirector01.tech.local\Main-Org\Main-Org-VDC
Reporting period: 12/1/2022 - 12/31/2022

Summary

Org Virtual Datacenter	Allocation Model	CPU Allocation Used	Memory Allocation Used	Storage Allocation Used	Used Network Count
Main-Org-VDC	Pay As You Go	0.00 GHz	0.00 GB	76.00 GB	0

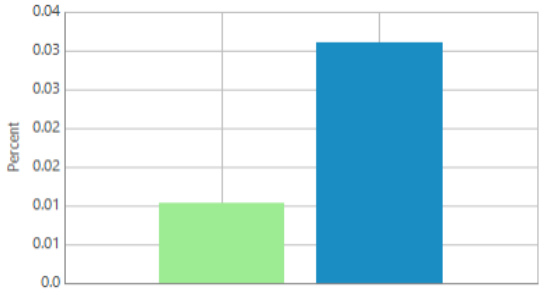
CPU Performance

Average CPU Ready (Percent)



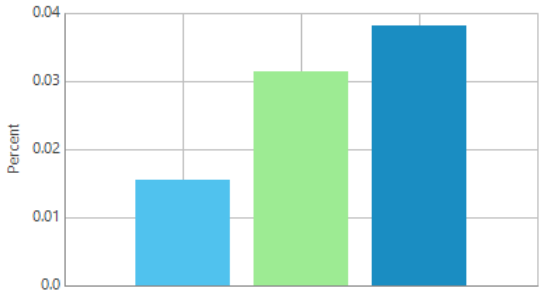
Object Name	Average	Minimum	Maximum	Std. Deviation	Trend
Main-Org-VDC	0.02	0.01	0.02	0.00	Increasing

Top 3 vApps by Average CPU Ready



vApp	Avg	Trend
vApp02-TS	0.03	Increasing
vApp-TS	0.01	Increasing

Top 3 VMs by Average CPU Ready



Virtual Machine Name	Avg	Trend
win-vm04-ts	0.04	Increasing
ubuntu-vm03-ts	0.03	Increasing
ts-vm022	0.02	Increasing

Use Case

The report helps you identify organization virtual datacenters with performance issues, right-size resource provisioning and eliminate potential performance bottlenecks.

Orphaned VM Snapshots

This report detects VM snapshots that reside on datastores but do not show up in the VMware Snapshot Manager.

- The **Datastore Space Usage (GB)** chart displays the total amount of free space, amount of space consumed by files other than orphaned snapshots and amount of space consumed by orphaned snapshots on datastores from the selected scope.
- The **Details** table provides the full list of datastores with folders that contain orphaned snapshots.

  The red color bar in the **Snapshot: File name** column shows how much datastore space is used by each folder with orphaned snapshots.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **Datastores**: defines datastores to analyze for the presence of orphaned snapshots.

> **NOTE:**
>
> If you run the Orphaned VM Snapshots report with **Veeam backup data and large-scale virtual infrastructure performance monitoring** mode selected, no data will display in the report. For more information on data collection modes, see Scalability and Choose Data Collection Mode.

View Report Example

Use Case

Orphaned snapshots consume valuable storage resources. Use this report to discover locations of useless snapshots that can be deleted to reclaim additional storage space.

Orphaned VMs

This report discovers VMs that are present in existing backup files, but are missing in backup, replication or backup to tape jobs. The report examines the content of backups on disk and tape and compares this data to the configuration properties of scheduled jobs, listing VMs that are not included in the jobs.

- The **Summary** section includes the **VMs without Backup Jobs** chart that shows the number of VMs that are not included in jobs.
- The **Details** table provides information on orphaned VMs, including protection type, the number of restore points, backup location, the date of the last backup session and the date when the backup will be deleted according to the current file retention policy.

Report Parameters

You can specify the following report parameters:

- **Scope**: defines a list of Veeam Backup & Replication servers to include in the report.
- **Protection type**: defines a job type to include in the report (*Backup*, *Replication*, *Archive*, *All*).

View Report Example

Use Case

A VM may become orphaned due to an error or oversight, job misconfiguration or a lack of coordination between several backup administrators, for example, when someone changed the configuration of the job and by mistake forgot to include the VM in that job. A VM may also become orphaned due to some automatic procedures, for example, when the VM migrated to an unprotected host through vMotion or as a result of DRS activating.

This report helps decide whether to modify the backup job settings for the VM if it is a mission critical one, or to delete the VM from the backup if it is no longer necessary.

Over-Provisioned Backup Repositories

When configuring cloud repositories, cloud administrators can allocate more storage space than there is available on the underlying backup repository. This report helps you assess the potential impact of excessive over-provisioning for cloud repositories.

- The **Summary** display includes the following elements in addition to individual charts for each connected repository:
  - The **Top 5 Over-provisioned Repositories** chart shows 5 repositories whose amount of provisioned storage space exceeds the total capacity.
  - The **Top 5 Under-provisioned Repositories** chart shows 5 repositories whose amount of provisioned storage space is way below the total capacity.
  - The **Top Repositories with Least Amount of Free Space** table displays top 5 repositories that will run out of free space sooner than other repositories.
- The **Report Data** display includes **Details** table that provides information on the repository capacity, amount of free space, amount of space provisioned to Veeam Cloud Connect tenants, provisioning ratio and the number of VMs and computers stored on the repository.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a list of Veeam Backup & Replication servers and repositories to include in the report.
- **Space utilization**: defines the threshold for the amount of space in use on repositories.
- **Free space (min)**: defines the threshold for the amount of free space left on repositories.
- **Show graphs**: defines whether to include charts in the report output.

View Report Example

Use Case

The report analyzes repository space utilization trend and calculates the number of days left before storage utilization will breach the specified threshold.

Over-Provisioned Datastores (Hyper-V)

Dynamic disk technology allows administrators to dedicate more storage space to VMs than there is real physical capacity. This report helps you assess the potential impact of excessive over-provisioning of disks on your virtual environment.

- The **Summary** section includes the following elements:
  - The **Top 5 Over-provisioned Datastores** chart shows 5 disks whose amount of provisioned storage space exceeds the total capacity.
  - The **Top 5 Under-provisioned Datastores** chart shows 5 disks whose amount of provisioned storage space is way below the total capacity.
  - The **Top 5 Datastores with Least Amount of Free Space** table displays top 5 disks that will run out of free space sooner than other disks.
- The **Details** tables provide information on storage space utilization and the number of days left before the specified space utilization/free space threshold will be breached. Arrows in the **Out of Free Space in ... (Days)** column show whether the amount of free space on the disk has increased (green arrow), decreased (red arrow) or stayed the same (grey arrow) over the previous week.

  Click a number in the **VM Count** column of the **Top 5 Datastores with Least Amount of Free Space** table or of the details table to get the list of VMs that store data on the disk and to discover how much space is provisioned for these VMs.

  Click a number in the **Out of Free Space in ... (Days)** column of the details table to drill down to details and recommendations for the disk.

> **NOTE:**
>
> The **Provisioned Space (GB)** column shows the size of all datastore files, including files that are not associated with any VM.
>
> If you want to see the size of files associated with VMs that store data on disk, click a number in the **VM Count** column.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **Business View objects**: defines Business View groups to analyze in the report. The parameter options are limited to objects of the Storage type.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.
- **Space utilization threshold**: defines the threshold for the amount of space in use on the disks.

- **Minimum free space threshold**: defines the threshold for the amount of free space left on the disks.

Over-Provisioned Datastores

Description

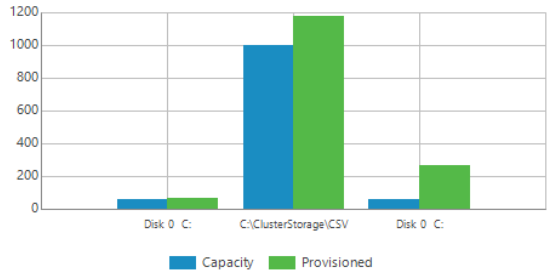
This report helps to identify potential impact of excessive over-provisioning of datastores on your virtual environment.

Report Parameters

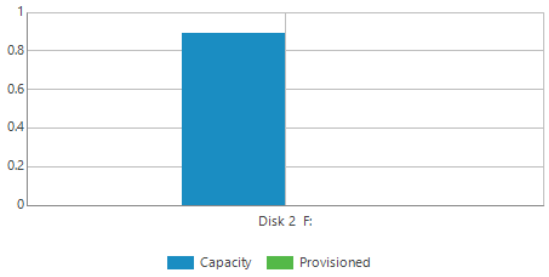
Scope: Virtual Infrastructure
Space utilization threshold: 80.00%
Business View objects:

Summary

Top 5 Over-provisioned Datastores (GB)



Top 5 Under-provisioned Datastores (GB)



Top 5 Datastores with Least Amount of Free Space

Datastore Name	Parent Node	SCVMM	Free Space (GB)	Capacity (GB)	Provisioned Space (GB)	Provisioning Ratio (%)	VM Count
Disk 2 F:	ms-22-node-01		0.8	0.9	0.0	0.00	0
Disk 0 C:	ms-22-node-02		4.8	59.4	62.0	104.42	2
Disk 0 C:	ms-22-node-01		11.7	59.4	263.0	442.96	6
C:\ClusterStorage\CSV	ms-22-cluster.tech.local		677.8	999.6	1173.0	117.35	20

Details

Over-provisioned Datastores

Parent Node	Datastore Name	Free Space (GB)	Capacity (GB)	Provisioned Space (GB)	Provisioning Ratio (%)	VM Count	Out of Free Space in... (Days)
ms-22-node-02							
	Disk 0 C:	4.8	59.4	62.0	104.42	2	0
ms-22-node-01							
	Disk 0 C:	11.7	59.4	263.0	442.96	6	0
ms-22-cluster.tech.local							
	C:\ClusterStorage\CSV	677.8	999.6	1173.0	117.35	20	...

Under-provisioned Datastores

Parent Node	Datastore Name	Free Space (GB)	Capacity (GB)	Provisioned Space (GB)	Provisioning Ratio (%)	VM Count	Out of Free Space in... (Days)
ms-22-node-01							
	Disk 2 F:	0.8	0.9	0.0	0.00	0	...

Use Case

The report analyzes disk space utilization trend and calculates the number of days left before storage utilization will breach the specified threshold.

Over-Provisioned Datastores (vSphere)

Thin provisioning allows administrators to dedicate more datastore space to VMs than there is real physical capacity. This report helps you assess the potential impact of excessive over-provisioning of datastores on performance of your virtual environment.

- The **Summary** section includes the following elements:
  - The **TOP 5 Over-provisioned Datastores** chart shows 5 datastores whose amount of provisioned storage space exceeds the total capacity.
  - The **TOP 5 Under-provisioned Datastores** chart shows 5 datastores whose amount of provisioned storage space is way below the total capacity.
  - The **TOP 5 Datastores with Least Amount of Free Space** table displays top 5 datastores that will run out of free space sooner than other datastores.

    Click a number in the **VM Count** column to get the list of VMs that store data on the datastore and to discover how much space is provisioned for these VMs.
- The **Details** section provides information on storage space utilization and the number of days left before the specified space utilization/free space threshold will be breached. Arrows in the **Out of Free Space in ... (Days)** column show whether the amount of free space on the datastore has increased (green arrow), decreased (red arrow) or stayed the same (grey arrow) over the previous week.

  Click a number in the **VM Count** column to get the list of VMs that store data on the datastore and to discover how much space is provisioned for these VMs.

  Click a number in the **Out of Free Space in ... (Days)** column to drill down to performance details for the datastore.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **Business View objects**: defines Business View groups to analyze in the report. The parameter options are limited to objects of the Storage type.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.
- **Space utilization threshold**: defines the threshold for the amount of space in use on datastores.
- **Minimum free space threshold**: defines the threshold for the amount of free space left on datastores.
- **Show graphs**: defines whether to include charts in the report output.

View Report Example

Use Case

The report analyzes datastore space utilization trend and calculates the number of days left before storage utilization will breach the specified threshold.

Oversized VMs (Hyper-V)

This report allows you to identify VMs that have more allocated resources such as vRAM or vCPU than they require.

- The **Summary** section provides an overview of the current state of your infrastructure, including the total number of VMs and the number of CPU and memory oversized VMs, and shows recommendations on resource allocation.
- The **Oversized Virtual Machines by CPU** and **Oversized Virtual Machines by Memory** tables display VMs with excessive CPU and memory resources and deliver recommendations for their reconfiguration.

  Click a VM name in the **Virtual Machine** column to drill down to VM performance charts that show how CPU and memory usage has been changing within the reporting period.
- The **Virtual Machines with Static Memory** table lists all discovered VMs with static memory, their location and the amount of provisioned memory resources. You can use this information to consider enabling dynamic memory for these VMs.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **Business View objects**: defines Business View groups to analyze in the report. The parameter options are limited to objects of the Virtual Machine type.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.
- **Period**: defines the time period to analyze in the report. Note that the reporting period must include at least one successfully completed *Object properties data collection* task for the selected scope. Otherwise, the report will contain no data.
- **Business hours only**: defines time of a day for which historical performance data will be used to calculate the performance trend. All data beyond this interval will be excluded from the baseline used for data analysis.

- **Top N**: defines the maximum number of VMs the report will analyze.

Oversized VMs

Description

This report helps you to discover VMs with under-utilized CPU and memory resources. It analyzes VMs historical performance and configuration data to provide recommendations on appropriate vCPU and vRAM allocation for VMs.

Report Parameters

Scope:	Virtual Infrastructure
Reporting period:	1 week (12/24/2022 - 12/30/2022)
Business View objects:	
Top N:	5
Working hours:	

Summary

Total oversized VMs:	6
Total VMs:	16
CPU oversized VMs:	6
Memory oversized VMs:	2
CPU resources that can be reclaimed:	8 vCPUs
vRAM amount that can be reclaimed:	3.40 GB

Oversized Virtual Machines by CPU

⊟SCVMM:

Cluster/Host	Virtual Machine	CPU vCPUs	CPU Average Usage (%)	CPU Peak Usage (%)	Reclaimed CPU Resource	Recommended Number of vCPUs
⊟pdctwhv01.tech.local					7	
	ahvbkpsrv	4	12.00	25.00	2	2
	backupsrv52	4	17.37	22.00	2	2
	repo31	2	2.00	2.00	1	1
	qa04	2	1.98	2.00	1	1
	qa05	2	0.19	1.00	1	1

Virtual Machines With Static Memory

Recommendation: Enable Dynamic Memory for these VMs.

⊟SCVMM:

Host	Virtual Machine	Assigned Memory (MB)
Cluster:		
⊟pdctwhv01.tech.local	5	
	ahvbkpsrv	6,144.00
	qa04	4,096.00
	qa05	4,096.00
	qa08	5,120.00
	repo30	2,048.00

Use Case

By analyzing historical performance, this report helps you identify VMs with excessive resource provisioning. You can use data in this report to change the current VM configuration and relocate VMs to other hosts.

Oversized VMs (vSphere)

This report helps you to detect VMs that have more allocated vRAM or vCPU resources than they require. The report analyzes historical performance and configured resource allocation to provide recommendations for an optimized VM configuration and allocation of resources.

- The **Summary** section provides details on the total number of VMs, number of oversized VMs by vCPU and vRAM, and amount of vCPU and vRAM resources that can be reclaimed.
- The **Oversized Virtual Machines by CPU** table provides a list of VMs from which you can reclaim vCPU resources. For each VM, the table details the number of configured vCPUs, average and peak CPU usage, and provides recommendations on vCPU configuration.

  Click a VM name to drill down to VM performance charts that show how CPU usage was changing during the reporting period.
- The **Oversized Virtual Machines by Memory** table provides a list of VMs from which you can reclaim vRAM resources. For each VM, the table details the amount of allocated memory, average and peak memory usage, and provides recommendations on memory configuration.

  Click a VM name to drill down to VM performance charts that show how memory usage was changing during the reporting period.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **VMware Cloud Director objects**: defines VMware Cloud Director components to analyze in the report.
- **Business View objects**: defines Business View groups to analyze in the report. The parameter options are limited to objects of the Virtual Machine type.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.
- **Last <N>**: defines the time period to analyze in the report. Note that the reporting period must include at least one successfully completed *Object properties data collection* task for the selected scope. Otherwise, the report will contain no data.
- **Business hours only**: defines time of a day for which historical performance data will be used to calculate the performance trend. All data beyond this interval will be excluded from the baseline used for data analysis.
- **Memory counter type**: defines whether the *Memory Active* or *Memory Consumed* performance metric should be analyzed in the report.
- **Top N**: defines the maximum number of VMs to display in the report output.

View Report Example

Use Case

This report helps you discover VMs with excessive hardware provisioning. You may consider decreasing hardware provisioning for the VM in vSphere configuration options, relocating the VM to less powerful hosts, or adding more VMs to a shared resource pool to optimize resource allocation and reclaim wasted resources.

Performance Assessment

This report evaluates whether the Microsoft Hyper-V infrastructure is configured optimally, helps find potential issues and suggests actions aimed at boosting its efficiency. The report analyzes data over the past 2 weeks and checks whether performance thresholds are exceeded or the number of times Veeam ONE Client triggered *Error* and *Warning* alarms. Performance thresholds are defined in alarm counters in Veeam ONE Client. If a threshold is exceeded, the report will deliver *Warning* or *Error* verification result depending on counter settings.

- The **Summary** section includes the following elements:
  - The **Verification Result** chart displays the share of failed and passed verification tests, test that are not applicable, and tests that completed with warnings.
  - The **Assessment Criteria** table lists criteria used in the report to evaluate Hyper-V infrastructure performance, and shows the assessment results.
- The **Performance** tables show detailed assessment result for each criterion and provides recommendations on how to improve infrastructure performance.

The report takes into account the following criteria when analyzing performance parameters:

CPU Performance

Criterion	Description
CPU Runtime	The criterion thresholds are specified in the **Total run time** counter settings of the **Host CPU Usage** alarm.

Memory Performance

Criterion	Description
Available Memory	The criterion thresholds are specified in the **Hyper-V Services Memory Usage** counter settings of the **Host Available Memory** alarm.
Memory Pages Rate	The criterion thresholds are specified in the **Pages/sec** counter settings of the **Host Memory Pages Usage** alarm. For more information about memory page rate counters, see Microsoft TechNet article.
Host Memory Pressure	The criterion thresholds are specified in the **Average Pressure** counter settings of the **Host Average Memory Pressure** alarm.

Disk Performance

Criterion	Description
Disk read Latency	The criterion thresholds are specified in the **Disk/Physical Disk: Avg Disk sec/Read** counter settings of the **Datastore read latency** alarm.
Disk write Latency	The criterion thresholds are specified in the **Disk/Physical Disk: Avg Disk sec/Write** counter settings of the **Datastore write latency** alarm.
Cluster Shared Volume read latency	The criterion thresholds are specified in the **Disk/CSV: Read Latency** counter settings of the **Cluster shared volume read latency** alarm.
Cluster Shared Volume write latency	The criterion thresholds are specified in the **Disk/CSV: Write Latency** counter settings of the **Cluster shared volume write latency** alarm

Network Performance

Criterion	Description
Network Output Queue Length	The criterion thresholds are specified in the **Network Output Queue Length** counter of the **Host network average output queue length** alarm.
Network Interface Transmission Rate	The criterion threshold is calculated the following way: **Network Bytes Total/sec** counter value divided by the **Network Bandwidth** value specified in the report parameters.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **Business View objects**: defines Business View groups to analyze in the report. The parameter options are limited to objects of the Host type.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.
- **Network bandwidth**: defines network bandwidth to analyze in the report.

- **Areas to assess**: defines a type of resources to analyze in the report (*All*, *CPU*, *Memory*, *Disk*, *Network*).

Performance Assessment

Description

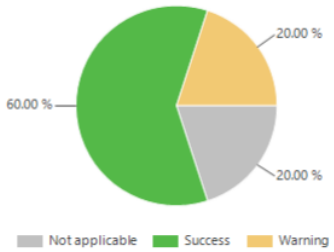
This report helps you to assess your Hyper-V performance and identify potential improvements. The report uses two-hour intervals.

Report Parameters

Scope:	Virtual Infrastructure
Business View objects:	
Areas to assess:	All
Network bandwidth:	1 Gbps

Summary

Verification Results



Assessment Criteria	Verification Results
Criteria Group: CPU Performance	Success
Hyper-V Hypervisor Logical Processor Total Run Time	Success
Criteria Group: Memory Performance	Warning
Available Memory	Success
Memory Pages Rate	Success
Memory Pressure	Warning
Criteria Group: Disk Performance	Success
Disk read latency	Success
Disk write latency	Success
Cluster Shared Volume read latency	Not applicable
Cluster Shared Volume write latency	Not applicable
Criteria Group: Network Performance	Warning
Network Output Queue Length	Success
Network Interface Transmission Rate	Warning

Memory Performance

Available Memory

Recommendation: -

Host	Host Memory (GB)	Cluster	Memory Usage, %			Alarms Triggered		Verification Result
			Avg.	Max.	Recommended	Warning	Error	
pdctwhv01.tech.local	382.67	-	16.59	17.20	<80 (306.13 GB)	0	0	Success

Memory Pages Rate

Recommendation: -

Host	Cluster	Memory, Pages/Sec			Alarms Triggered		Verification Result
		Avg.	Max.	Recommended	Warning	Error	
pdctwhv01.tech.local	-	3.15	11.00	<500	0	0	Success

Host Memory Pressure

Recommendation: Check historical memory pressure usage, number of VMs running, alerts for VMs with high memory pressure.

Host	Cluster	Host Memory Pressure, %			Alarms Triggered		Verification Result
		Avg.	Max.	Recommended	Warning	Error	
pdctwhv01.tech.local	-	83.57	91.00	<90	73	0	Warning

Use Case

The report analyzes performance of the Microsoft Hyper-V infrastructure and provides recommendations to improve its configuration. You can use report results to implement the necessary hardware and software optimizations.

Permissions by Object

This report provides information about permissions assigned in your virtual environment, including individual permissions for every object. The report lists virtual infrastructure objects and shows permissions that each registered user has for these items.

- The **Permissions** subsections provide information on permissions for each object, including object name, location, user or group, permissions assigned to this user or group and whether permissions can be propagated.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **Object name**: defines a name of the virtual infrastructure object for which permissions should be shown. You can specify either an exact object name or a part of the name.
- **Object type**: defines a type of virtual infrastructure objects for which permissions should be shown.
- **User/User group**: defines a user or a user group for which permissions should be shown.
- **User role**: defines a user role that should be included in the report.
- **Propagated permissions**: defines whether permissions that can be propagated to child/dependent objects should be included in the report.

View Report Example

Use Case

This report helps senior IT administrators review permissions for any given object (vCenter Server, cluster, storage, datacenter, resource pool, vApp, host system or VM).

Permissions by User

This report provides information about permissions assigned in your virtual environment, including individual permissions for every user. The report lists registered users and shows permissions that each user has for different virtual infrastructure objects.

- The **Permissions** subsections provide information on permissions of each user, including object name, location, user role and whether permissions can be propagated.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **Object name**: defines a name of the virtual infrastructure object for which permissions should be shown. You can specify either an exact object name or a part of the name.
- **Object type**: defines a type of virtual infrastructure objects for which permissions should be shown.
- **User/User group**: defines a user or a user group for which permissions should be shown.
- **User role**: defines a user role that should be included in the report.
- **Propagated permissions**: defines whether permissions that can be propagated to child/dependent objects should be included in the report.

View Report Example

Use Case

This report helps senior IT administrators review permissions assigned to any registered user.

Powered Off VMs (Hyper-V)

The report provides information on VMs powered off throughout a specified time period.

- The **Summary** section shows the total number of VMs in the selected scope, the number of powered off VMs and their total size on disk.
- The **Powered Off Virtual Machines** table lists powered off VMs, their location and disk size.

  The **Powered Off status (%)** column displays the amount of time during which a VM was powered off against the time of the reporting period in percent.

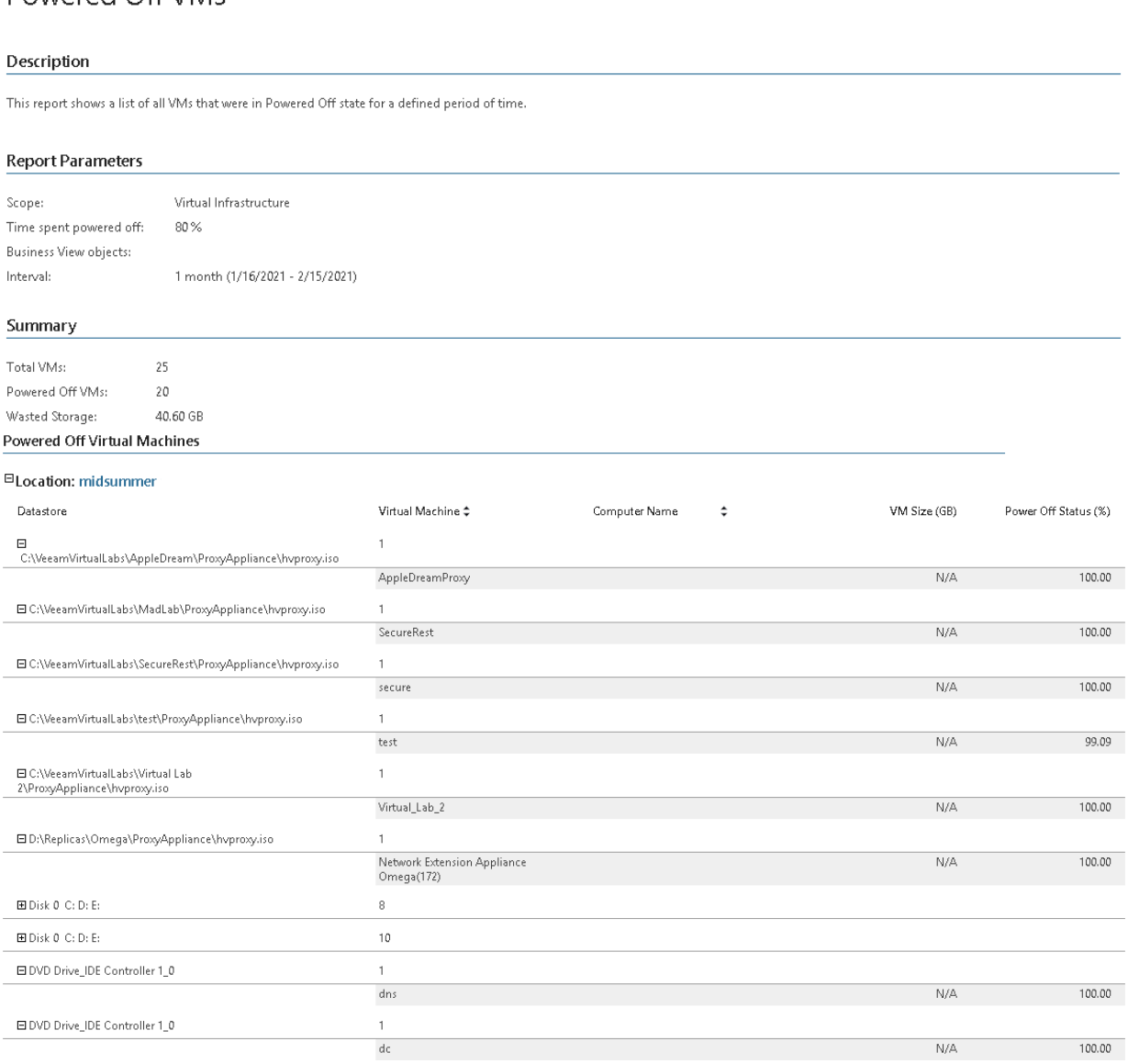
Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **Business View objects**: defines Business View groups to analyze in the report. The parameter options are limited to objects of the Virtual Machine type.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.
- **Period**: defines the time period to analyze in the report. Note that the reporting period must include at least one successfully completed *Object properties data collection* task for the selected scope. Otherwise, the report will contain no data.

- **Time spent powered off**: defines the threshold for the amount of time when a VM was powered off against the amount of time in the reporting period (in percentage). If the time during which a VM was powered off is less than the specified value in percent, the report will not analyze this VM.



Powered Off VMs

Description

This report shows a list of all VMs that were in Powered Off state for a defined period of time.

Report Parameters

Scope: Virtual Infrastructure
Time spent powered off: 80 %
Business View objects:
Interval: 1 month (1/16/2021 - 2/15/2021)

Summary

Total VMs: 25
Powered Off VMs: 20
Wasted Storage: 40.60 GB

Powered Off Virtual Machines

Location: midsummer

Datastore	Virtual Machine	Computer Name	VM Size (GB)	Power Off Status (%)
C:\VeeamVirtualLabs\AppleDream\ProxyAppliance\hvproxy.iso	1			
	AppleDreamProxy		N/A	100.00
C:\VeeamVirtualLabs\MadLab\ProxyAppliance\hvproxy.iso	1			
	SecureRest		N/A	100.00
C:\VeeamVirtualLabs\SecureRest\ProxyAppliance\hvproxy.iso	1			
	secure		N/A	100.00
C:\VeeamVirtualLabs\test\ProxyAppliance\hvproxy.iso	1			
	test		N/A	99.09
C:\VeeamVirtualLabs\Virtual Lab 2\ProxyAppliance\hvproxy.iso	1			
	Virtual_Lab_2		N/A	100.00
D:\Replicas\Omega\ProxyAppliance\hvproxy.iso	1			
	Network Extension Appliance Omega(172)		N/A	100.00
Disk 0 C: D: E:	8			
Disk 0 C: D: E:	10			
DVD Drive_IDE Controller 1_0	1			
	dns		N/A	100.00
DVD Drive_IDE Controller 1_0	1			
	dc		N/A	100.00

Use Case

The report allows you to track VMs that have been in the powered off state for a specified time period. Since powered off VMs consume space required to store their disks and configuration data, you can review storage usage and relocate these machines, or decommission machines that you no longer need.

Powered Off VMs (vSphere)

This report shows a list of VMs that were remaining in the powered off state during the specified period.

For each powered off VM, the report shows its location, size and the datastore where the VM files are stored.

- The **Summary** section shows the total number of VMs in the selected scope, the number of powered off VMs and their total size on disk.
- The **Powered Off Virtual Machines** table lists powered off VMs, their location and disk size.

  The **Powered Off status (%)** column displays the amount of time during which a VM was powered off against the time of the reporting period in percent.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **VMware Cloud Director objects**: defines VMware Cloud Director components to analyze in the report.
- **Business View objects**: defines Business View groups to analyze in the report. The parameter options are limited to objects of the Virtual Machine type.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.
- **Last <N>**: defines the time period to analyze in the report. Note that the reporting period must include at least one successfully completed *Object properties data collection* task for the selected scope. Otherwise, the report will contain no data.

- **Time spent powered off**: defines the amount of time when the VM was powered off against the amount of time in the reporting period (in percentage).

Powered Off VMs

Description

This report shows a list of all VMs that were in Powered Off state for a defined period of time.

Report Parameters

Scope: Virtual Infrastructure
Time spent powered off: 80 %
Interval: 1 week (1/10/2023 - 1/16/2023)

Summary

Total VMs: 212
Powered Off VMs: 67
Wasted Storage: 4,078.51 GB

Powered Off Virtual Machines

Location: vcenter01.tech.local

Datastore	Virtual Machine	Computer Name	VM Size (GB)	Power Off Status (%)
ubuntunfs01	10			
	vApp01-7nFN	Not set	0.00	100.00
	linux03-zRea	Not set	0.00	100.00
	linux02-OeX8	Not set	0.00	100.00
	linux01-7IN9	Not set	0.00	100.00
	vm02-RqUH	Not set	0.00	100.00
	template01-eoCy	Not set	0.00	100.00
	ts-vm01-xbds	Not set	0.00	100.00
	ts-vm022-IVrN	Not set	0.00	100.00
	win-vm04-ts-U1bl	Not set	0.00	100.00
	ts-vm01-ZVIV	Not set	0.88	95.89
prgtwesx01-ds01	8			
	avspem1	avspem1	116.09	100.00
	172.35.42.67_pskehq	pskehq	0.11	100.00
	unixsrv01	Not set	41.15	100.00
	172.24.31.67_xxjx2s	xxjx2s	0.11	100.00
	ABC Company_filesrv04_replica	Not set	27.78	100.00
	ABC Company_filesrv03_replica	Not set	41.22	100.00
	ABC Company	Not set	0.00	100.00
	172.35.42.67_sjnmu7	Not set	0.11	100.00

Use Case

Powered off VMs do not consume CPU, memory or network resources, but they take up storage space required to accommodate their disk files, snapshots and configuration data.

The report helps you detect VMs that can be relocated to less costly datastores and identify neglected VMs that can be decommissioned.

Protected Cloud Instances

This report analyzes backup, snapshot, replication, backup copy and archive protection of cloud instances in your Veeam Backup for Microsoft Azure, Amazon Web Services and Google Cloud Platform cloud infrastructures. Note that report scope includes only target repositories connected to Veeam Backup & Replication server.

A cloud instance is considered *Protected* if there is at least one valid backup, snapshot, replication, backup copy or archive protection restore point that meets the designated RPO for it. A cloud instance is considered *Unprotected* if it has outdated or missing restore points.

- The **Summary** section includes the following elements:
  - The **Instances by Protection State** chart shows the number of protected and unprotected cloud instances.
  - The **Instances by Last Session Status** chart shows status of the latest job session for discovered cloud instances.
  - The **Unprotection Reason** chart shows reasons for non-compliance with the specified RPO requirements.
- The **Details** section provides information on all protected and unprotected cloud instances including instance ID, protection type, policy name, backup, snapshot, replication, backup copy or archive protection target, number of available restore points and date and time of the latest backup, snapshot, replication, backup copy or archive protection.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a list of Veeam Backup & Replication servers to include in the report.
- **RPO (Recovery Point Objective)**: defines the maximum amount of data that you may accept to lose, expressed in time. RPO defines the age of the latest backup, snapshot, replication, backup copy or archive protection files required to resume normal operation if system failure occurs. For example, to compile a list of cloud instances protected on a daily basis, you need to set the RPO value to 1 day.
- **Instance types**: defines a type of cloud instances to include in the report (*Amazon Web Services*: *EC2*, *RDS*, *EFS*, *VPC, DynamoDB, FSx, Redshift, Redshift Serverless*; *Microsoft Azure*: *Virtual Machines*, *SQL Database*, *Files, Virtual Network, Cosmos DB*; *Google Cloud*: *VMs*, *SQL, Spanner)*.
- **Protection types**: defines a type of protection to include in the report (*Backup*, *Snapshot*, *Replication*, *Archive*).
- **Instance filter type**: defines the filter type to apply to cloud instances defined in the *Rule* section (*Inclusion, Exclusion*)
- **Rule**: defines a list of cloud instances that should be included or excluded from the report scope depending on the *Instance filter type* selection. You can enter cloud instance names explicitly or create a wildcard mask by using the asterisk (*) to replace any number of characters. Multiple entries are separated by semicolon. For example, the following string will exclude cloud instances with the _R&D suffix from appearing in the report: **_R&D*.

NOTE

The *Region* and *Instance ID* columns may display an entry as *Undefined*. This can occur either when a Veeam Backup server or platform service is unavailable, or if an instance has been deleted but restore points remain. Veeam Backup & Replication does not store instance ID or region information, leading to these fields displaying *Undefined* in the report.

View Report Example

Use Case

When you set up your backup jobs based on resource groups or employ complex exclusion parameters in job properties, some cloud instances may turn out to be excluded from the backup policies and therefore will lack proper protection.

This report displays a list of cloud instances protected by up-to-date backups and snapshots, as well as a list of unprotected cloud instances which have outdated or missing restore points. This information helps you validate the state of data protection in your organization.

Protected Computers

This report provides information on all protected and unprotected computers including their last backup state.

A computer is considered to be *Protected* if there is at least one valid backup restore point that meets the designated RPO for it. A computer is considered to be *Unprotected* if it has an outdated or missing backup restore point.

The report examines whether computers have valid backup restore points created within the specified time range (RPO period), shows the total number of restore points available for each protected computer, and provides information on the completion status of recent backup job sessions.

- The **Summary** display contains the following charts:
  - The **Protected Computers** chart shows the number of protected and unprotected computers.
  - The **Computer Type** chart shows types of protected computers.
  - The **Computer Last Backup State** chart shows status of the latest job session for a discovered/protected computer.
  - The **Unprotection Reason** chart shows reasons for non-compliance with the specified RPO requirements.
  - The **Report Parameters** and **Summary** panels show the specific configured parameters for the report and provide information on the number of discovered, backed up and protected computers.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a list of Veeam Backup & Replication servers and protection groups to include in the report.
- **Business View objects**: defines a list of business groups to include in the report. The parameter options are limited to objects of the Computer type.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.
- **Backup jobs/policies**: defines a list of backup jobs and policies to include in the report.
- **Agent types**: defines types of Veeam backup agents to include in the report.
- **Computer inclusion rule**: defines names of computers that must be included in the report.

  In the **Computer inclusion rule** field, you can specify a mask for names of computers that must be included in the report scope. The mask can contain the asterisk (*) that stands for zero or more characters. You can specify multiple masks or computer names separated with commas.
- **RPO (Recovery Point Objective)**: defines the maximum amount of data that you may accept to lose, expressed in time. RPO defines the age of the latest backup files required to resume normal operation if system failure occurs. For example, to compile a list of computers protected on a daily basis, you need to set the RPO value to 1 day.

View Report Example

Use Case

When you set up your agent backup jobs based on protection groups or employ complex exclusion parameters in job properties, some computers may turn out to be excluded from protection groups and therefore will lack proper protection.

This report displays a list of computers protected by up-to-date backups as well as a list of unprotected computers which have outdated or missing backups. This information helps you identify which computers in your environment function without proper protection and make sure the existing backups meet established RPO requirements.

Protected Files and Object Storage

This report analyzes backup protection of unstructured data stored in file shares and object storage. The report examines the status of Veeam Backup & Replication protected files and provides details on your infrastructure SLAs.

File shares, buckets and storage accounts that have not been added to any Veeam Backup & Replication inventory are not included in this report.

- The **Summary** display includes the following elements:
  - The **Report Parameters** and **Summary** sections shows the volume of backup objects by their data structure status on your backup servers (*Total Unstructured Data, Protected Unstructured Data, Unprotected Unstructured Data*).
  - The **Unstructured Data Protection Status** chart shows the division of your backup data into structured and unstructured instances.
  - The **Unstructured Data Last Backup State** chart shows the status of your data backups on their success or failure state.
  - The **Unstructured Data Last Backup Age** chart shows the status of your backup data based on its Recovery Point Objective status.
- The **Report Data** display includes the following tables:
  - The **Details - Protected Unstructured Data** table shows the status of all file and object storage sources that are successfully protected by a backup job including server and job names, protection types, processing and restore type data.
  - The **Details - Unprotected Unstructured Data** table shows the status of all file and object storage sources that are not currently protected by a backup job including server and job names, unprotected reason, processing and restore type data.
  - The **Job Details - Protected Unstructured Data** table shows the status of all discovered file and object storage sources that are currently protected including groups, backup servers, results, processing data and skipped locations.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a list of Veeam Backup & Replication servers to include in the report.
- **RPO**: defines the Recovery Point Objective time period which is the maximum period for acceptable loss of data (*value, time period definition* including *minutes, hours, days and so on*).
- **Processed Percentage**: defines the percentage of the acceptable volume of data retention for restore operations.
- **Unstructured Data exclusion rule**: defines a list of file/object that should be excluded from the report scope. You can enter names explicitly or create a wildcard mask by using the asterisk (*) to replace any number of characters. Multiple entries are separated by semicolon. For example, the following string will exclude machines with the _R&D suffix from appearing in the report:*_R&D.
- **Job types**: defines a job type to evaluate in the report (*File backup*, *Object storage backup*).

View Report Example

Use Case

This report helps you discover protected objects that breach the target SLA, and jobs that do not operate properly.

Protected Objects (Veeam Backup for Microsoft 365)

This report analyzes backup protection of Microsoft 365 objects in your virtual environment.

An object is considered *Protected* if there is at least one valid backup restore point that meets the designated RPO for it.

The report examines whether objects have valid backup restore points created within the specified time range (RPO period), shows the total number of restore points available for each protected object, and provides information on the completion status of recent backup job sessions.

The report helps you identify which objects in your environment function without proper protection and make sure the existing backups and replicas meet established RPO requirements.

- The **Summary** display includes the following elements:
  - The **Objects by Protection State** chart shows the number of protected and unprotected objects.
  - The **Objects by Type by Protection State** chart shows the number of protected and unprotected objects for each object type.
- The **Report Data** display provides the **User Details**, **Group Details**, **Site Details** and **Teams Details** tables that provide information on all protected and unprotected users, groups, sites and teams.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a list of Veeam Backup for Microsoft 365 servers to include in the report.
- **Organizations**: defines Microsoft organizations to analyze in the report.
- **RPO (Recovery Point Objective)**: defines the maximum amount of data that you may accept to lose, expressed in time. RPO defines the age of the latest backup files required to resume normal operation if system failure occurs. For example, to compile a list of objects protected on a daily basis, you need to set the RPO value to 1 day.
- **Object types**: defines Microsoft 365 object types to analyze in the report (*Users*, *Groups*, *Sites*, *Teams*).
- **User backup should contain**: defines user backup types to analyze in the report (*Mailbox*, *Archive*, *OneDrive*, *Site*).
- **Group backup should contain**: defines group backup types to analyze in the report (*Group mailbox*, *Group site*).
- **Hide objects with no restore point**: select the check-box to hide objects with no restore point.

View Report Example

Use Case

This report displays a list of Microsoft 365 objects protected by up-to-date backups, as well as a list of unprotected objects which have outdated or missing backups. This information helps you validate the state of backup protection in your organization.

Protected VMs

This report analyzes backup protection of VMware vSphere and Microsoft Hyper-V VMs in your virtual environment.

A VM is considered to be *Protected* if there is at least one valid backup or replica restore point that meets the designated RPO for it. A VM is considered to be *Unprotected* if it has an outdated or missing backup or replica restore points.

The report examines whether VMs have valid backup and replica restore points created within the specified time range (RPO period), shows the total number of restore points available for each protected VM, and provides information on the completion status of recent backup and replication job sessions.

The report helps you identify which VMs in your environment function without proper protection and make sure the existing backups and replicas meet established RPO requirements.

- The **Summary** section includes the following elements:
  - The **Protected VMs** chart shows the number of protected, unprotected VMs as well as VMs in multiple jobs (VMs in multiple jobs displays VMs that are protected by different jobs. For example, one VM with three jobs is counted as three protected VMs).
  - The **VM Last Backup State** chart shows status of the latest job session for discovered/protected VMs.
  - The **VM Last Backup Age** chart shows compliance of latest VM backups with the specified RPO requirements.
- The **Details** section provides information on all protected and unprotected VMs including VM location, protection type, job name, number of available restore points, date of the oldest restore point and date and time of the latest backup or replica.

NOTE:

- VM replicas not protected by any Veeam Backup & Replication job are not accounted in this report.

Report Parameters

You can specify the following report parameters:

- **Protected infrastructure**: defines the Veeam Backup & Replication infrastructure to analyze in the report.
- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **VM folders**: defines a list of VMware folders to include in the report (applies to VMware vSphere environments only). VM folders view is an alternate way to present the virtual infrastructure. If VMs in your infrastructure are grouped into folders according to their profile, you can limit the report scope by specifying the necessary folders only.
- **VMware Cloud Director objects**: defines VMware Cloud Director components to analyze in the report.
- **Business View objects**: defines Business View groups to analyze in the report. The parameter options are limited to objects of the Virtual Machine type.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.

- **RPO (Recovery Point Objective)**: defines the maximum amount of data that you may accept to lose, expressed in time. RPO defines the age of the latest backup or replica files required to resume normal operation if system failure occurs. For example, to compile a list of VMs protected on a daily basis, you need to set the RPO value to 1 day.
- **VM exclusion rule**: defines a list of VMs that should be excluded from the report scope. You can enter VM names explicitly or create a wildcard mask by using the asterisk (*) to replace any number of characters. Multiple entries are separated by semicolon. For example, the following string will exclude machines with the _R&D suffix from appearing in the report: *_R&D.
- **Job types**: defines a job type to evaluate in the report (*Backup*, *Replication*, *Backup Copy, Cloud Director Backup, Cloud Director Replication, All items*).
- **Exclude jobs**: defines a list of backup and replication jobs to exclude from the report.
- **Analyze VM templates**: defines whether VM templates should be included in the report.

View Report Example

Use Case

When you set up your backup, replication and backup copy jobs based on VI containers (such as folders, hosts or datastores) or employ complex exclusion parameters in job properties, some VMs may turn out to be excluded from the containers and therefore will lack proper protection.

This report displays a list of VMs protected by up-to-date backups and replicas, as well as a list of unprotected VMs which have outdated or missing backup or replicas. This information helps you validate the state of backup protection in your organization.

Protected VMs (KVM Environments)

This report analyzes backup protection of KVM VMs in your backup environment.

A VM is considered to be *Protected* if there is at least one valid backup restore point that meets the designated RPO for it. A VM is considered to be *Unprotected* if it has an outdated or missing backup restore points.

- The **Summary** section includes the following elements:
  - The **Protected VMs** chart shows the number of protected and unprotected VMs.
  - The **Last Backup State** chart shows status of the latest job session for discovered/protected VMs.
  - The **Unprotection Reason** chart shows reasons for non-compliance with the specified RPO requirements.
- The **Details** section provides information on all protected and unprotected VMs including name of a KVM cluster, job name, backup target, number of available restore points and date and time of the latest backup.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a list of Veeam Backup & Replication servers to include in the report.
- **RPO (Recovery Point Objective)**: defines the maximum amount of data that you may accept to lose, expressed in time. RPO defines the age of the latest backup files required to resume normal operation if system failure occurs. For example, to compile a list of VMs protected on a daily basis, you need to set the RPO value to 1 day.
- **VM Exclusion rule**: defines a list of VMs that should be excluded from the report scope. You can enter VM names explicitly or create a wildcard mask by using the asterisk (*) to replace any number of characters. Multiple entries are separated by semicolon. Usage example: the following string will exclude machines with the _R&D suffix from appearing in the report: **_R&D*.
- **Backup jobs**: defines a list of backup jobs to evaluate in the report.

View Report Example

Use Case

When you set up your backup jobs and employ complex exclusion parameters in job properties, some VMs may turn out to be excluded from the protection domains and therefore will lack proper protection.

This report displays a list of VMs protected by up-to-date backups, as well as a list of unprotected VMs which have outdated or missing backup. Data for VMs that are not added to a job and backed up are not displayed and unprotected VMs display only if the previously made backup was deleted. This information helps you validate the state of backup protection in your organization.

Protected VMs (Nutanix AHV)

This report analyzes backup protection of Nutanix AHV VMs in your backup environment.

A VM is considered to be *Protected* if there is at least one valid backup restore point that meets the designated RPO for it. A VM is considered to be *Unprotected* if it has an outdated or missing backup restore points.

- The **Summary** section includes the following elements:
  - The **Protected VMs** chart shows the number of protected and unprotected VMs.
  - The **Last Backup State** chart shows status of the latest job session for discovered/protected VMs.
  - The **Unprotection Reason** chart shows reasons for non-compliance with the specified RPO requirements.
- The **Details** section provides information on all protected and unprotected VMs including name of a Nutanix AHV cluster, protection domain to which the VM is added, job name, backup target, number of available restore points and date and time of the latest backup.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a list of Veeam Backup & Replication servers to include in the report.
- **RPO (Recovery Point Objective)**: defines the maximum amount of data that you may accept to lose, expressed in time. RPO defines the age of the latest backup files required to resume normal operation if system failure occurs. For example, to compile a list of VMs protected on a daily basis, you need to set the RPO value to 1 day.
- **VM exclusion rule**: defines a list of VMs that should be excluded from the report scope. You can enter VM names explicitly or create a wildcard mask by using the asterisk (*) to replace any number of characters. Multiple entries are separated by semicolon. Usage example: the following string will exclude machines with the _R&D suffix from appearing in the report: **_R&D*.
- **Backup jobs**: defines a list of backup jobs to evaluate in the report.

View Report Example

Use Case

When you set up your backup jobs based on protection domains or employ complex exclusion parameters in job properties, some VMs may turn out to be excluded from the protection domains and therefore will lack proper protection.

This report displays a list of VMs protected by up-to-date backups, as well as a list of unprotected VMs which have outdated or missing backup. This information helps you validate the state of backup protection in your organization.

Protected VMs Job Schedule

This report publishes the timetable for all scheduled backup, replication and backup copy jobs. The report analyzes all recurrent jobs in the selected scope and reveals advanced details:

- The **Summary** section includes the following elements:
  - The **Jobs Schedule** chart displays the total number of jobs running according to the specified schedules.
  - The **Protected VMs** chart displays the total number of VMs protected by scheduled backup, replication and backup copy jobs.
- The **Details** table shows VMs included in the jobs, scheduled run time and date, recurrence intervals, weekly full backup schedule for backup jobs and the effective backup file retention policy.

Report Parameters

You can specify the following report parameters:

- **Protected infrastructure**: defines the platform to analyze in the report.
- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **VMware Cloud Director objects**: defines VMware Cloud Director components to analyze in the report.
- **Business View objects**: defines Business View groups to analyze in the report. The parameter options are limited to objects of the Virtual Machine type.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.
- **Job types**: defines a job type to evaluate in the report (*VM backup*, *Replication*, *Backup copy*).
- **VM exclusion rule**: defines a list of VMs that should be excluded from the report scope. You can enter VM names explicitly or create a wildcard mask by using the asterisk (*) to replace any number of characters. Multiple entries are separated by semicolon. Usage example: the following string will exclude machines with the _R&D suffix from appearing in the report: **_R&D*.
- **Analyze VM templates**: defines whether VM templates should be included in the report.

View Report Example

Use Case

This report helps you ensure that applied data protection job schedules are configured in accordance to the backup policies and allow you to meet the desired RPO requirements.

Provider VDCs Performance

This report aggregates historical data and shows performance statistics for selected provider virtual datacenters across a time range.

- The **Summary** section includes **Top N** charts that display provider virtual datacenters with the largest amount of allocated resources and the highest level of CPU, memory and storage utilization.
- The **Current Usage Details** section shows general configuration data for the selected provider virtual datacenters.
- The **Performance Charts** section displays tables and performance charts with resource usage statistics for each provider virtual datacenter included in the report scope.

Report Parameters

You can specify the following report parameters:

- **Provider virtual datacenters**: defines a list of provider virtual datacenters to analyze in the report.
- **Period**: defines the time period to analyze in the report.
- **Business hours only**: defines time of a day for which historical performance data will be used to calculate the performance trend. All data beyond this interval will be excluded from the baseline used for data analysis.

- **Top N**: defines the maximum number of provider virtual datacenters to display in the report output.

Provider VDCs Performance

Description

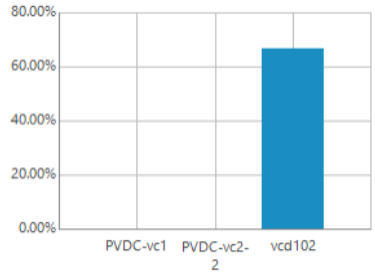
This report provides information on provider VDCs resource usage, including CPU and memory usage history.

Report Parameters

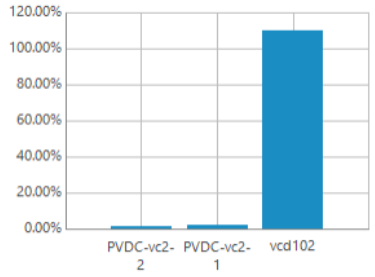
Provider virtual datacenters:	All Providers
Top N:	3
Reporting period:	12/1/2022 - 12/31/2022

Summary

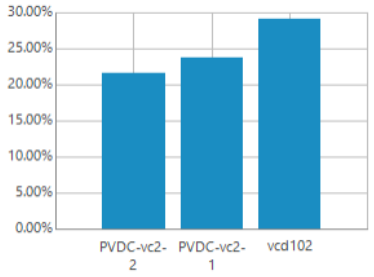
Top 3 Providers by CPU Usage



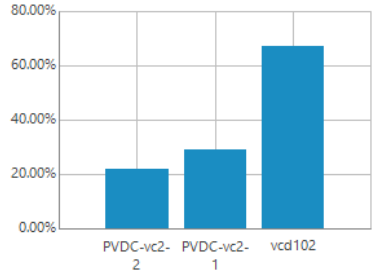
Top 3 Providers by Memory Usage



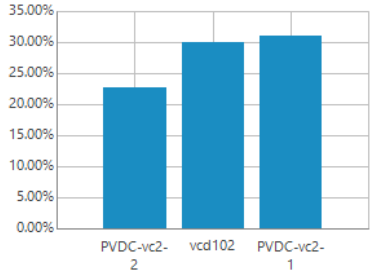
Top 3 Providers by Storage Usage



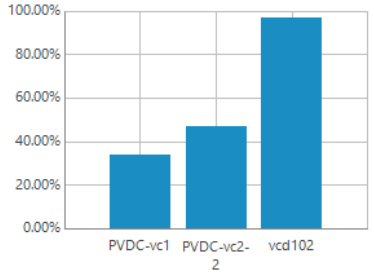
Top 3 Providers by CPU Allocation



Top 3 Providers by Memory Allocation



Top 3 Providers by Storage Allocation

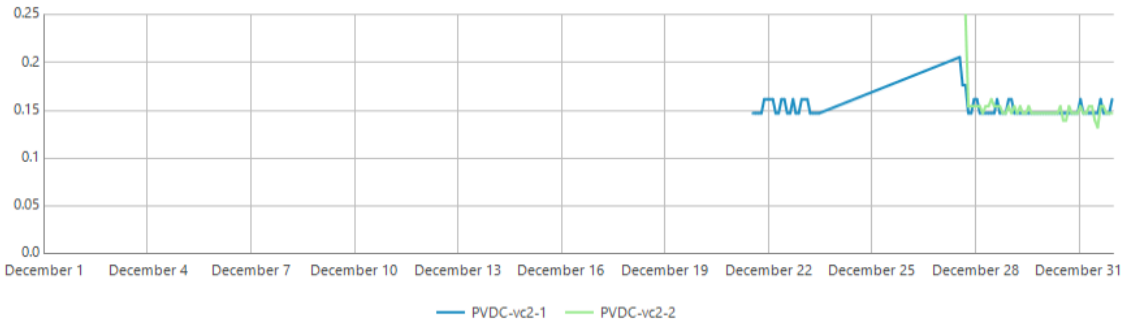


Current Usage Details

Name	Status	Org Virtual Datacenters	CPU Used (GHz)	Memory Used (GB)	Storage Used (GB)	CPU Allocation (GHz)	Memory Allocation (GB)	Storage Allocation (GB)
PVDC-vc1	READY	1	0.00 GHz (0.00%)	0.00 GB (0.00%)	18.30 GB (9.16%)	0.00 GHz (0.00%)	0.00 GB (0.00%)	68.00 GB (34.04%)
		VDC1(vvg130-1)	0.00 GHz	0.00 GB	68.00 GB	0.00 GHz	0.00 GB	0.00 GB (0.00%)
PVDC-vc2-2	READY	2	0.00 GHz (0.00%)	0.16 GB (1.19%)	85.79 GB (21.48%)	3.00 GHz (21.87%)	3.00 GB (22.60%)	187.00 GB (46.81%)
		VDC4(vvg130-3) PVDC-vc2-2	3.00 GHz	3.00 GB	85.00 GB	0.00 GHz (0.00%)	0.00 GB (0.00%)	0.00 GB (0.00%)
		VDC3(vvg130-2) PVDC-vc2-2	0.00 GHz	0.00 GB	102.00 GB	0.00 GHz (0.00%)	0.00 GB (0.00%)	0.00 GB (0.00%)
PVDC-vc2-1	READY	1	0.00 GHz (0.00%)	0.11 GB (1.75%)	47.28 GB (23.67%)	2.00 GHz (29.15%)	2.00 GB (30.89%)	34.00 GB (17.02%)
		VDC2(vvg130-2) PVDC-vc2-1	2.00 GHz	2.00 GB	34.00 GB	0.00 GHz (0.00%)	0.00 GB (0.00%)	0.00 GB (0.00%)
vcd102	READY	15	33.86 GHz (66.61%)	333.04 GB (109.77%)	14035.88 GB (29.07%)	34.10 GHz (67.09%)	91.04 GB (30.01%)	46870.39 GB (97.07%)

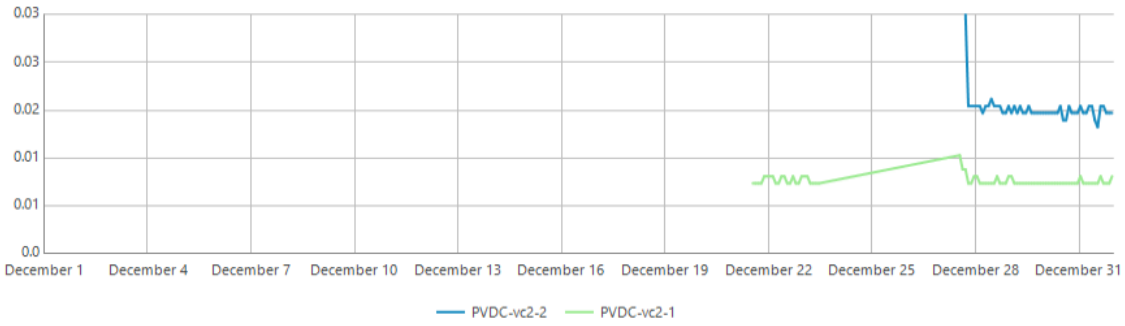
CPU Usage (Absolute)

CPU Usage (Absolute) (Percent)



Object Name	Average	Minimum	Maximum	Std. Deviation	Trend
PVDC-vc2-1	0.15	0.15	0.20	0.01	Decreasing
PVDC-vc2-2	0.15	0.13	0.25	0.01	Decreasing

CPU Usage (Absolute) (GHz)



Object Name	Average	Minimum	Maximum	Std. Deviation	Trend
PVDC-vc2-2	0.02	0.02	0.03	0.00	Decreasing
PVDC-vc2-1	0.01	0.01	0.01	0.00	Decreasing

Use Case

The report helps you identify provider virtual datacenters with performance issues, balance workloads and optimize resource allocation.

Recovery Verification Overview

This report validates the completion status of SureBackup jobs and displays the results of recovery verification tests. The report helps you reveal the list of operational VMs that can be restored from the produced backup or replicas.

- The **Summary** section includes the following elements:
  - The **SureBackup Job Status** chart chows the latest state of SureBackup job sessions.
  - The **Verified VMs Status** chart shows the percentage of VMs for which the latest SureBackup job session completed successfully, completed with warnings or failed, and percentage of VMs for which SureBackup jobs have not been run at all.
  - The **Antivirus Check** chart shows the results of the last antivirus check run.
- The **Details** table shows the results of completed SureBackup job sessions, including the name and status of the evaluated SureBackup job, the list of VMs included in the job, the application type of the verification model used to test each VM, the verification date and the date when backup or replica was created, the results of *ping*, *heartbeat* and *script execution* commands executed to verify recoverability of created copies, the version of the antivirus installed on a VM and the last antivirus check result.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a list of Veeam Backup & Replication servers to include in the report.
- **Business View objects**: defines Business View groups to analyze in the report. The parameter options are limited to objects of the Virtual Machine type.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.
- **Job type**: defines a SureBackup job type to evaluate in the report (*Backup*, *Replica*, *All*).

> **NOTE:**
>
> Infrastructure topology view in Veeam ONE and Veeam Backup & Replication must match. Otherwise, you will not be able to generate the report based on **Business View objects**.

View Report Example

Use Case

SureBackup is a unique Veeam technology that ensures that the VM being backed up or replicated is safely recoverable from the media. SureBackup allows you to validate backups and replicas of your VMs without impacting the production infrastructure. You can automatically verify every created restore point of every VM and ensure that they will function as expected in case a disaster strikes.

The report helps you discover issues that occur in operation of your backup infrastructure. It provides details on the state of SureBackup jobs so that you can reconfigure current job settings or include mission critical VMs in SureBackup jobs.

Replica Billing

This report helps you assess storage management costs for the backup infrastructure and tracks the consumption of storage by VM replicas.

The report estimates storage resources required to store replicas. The cost can be calculated based on the price of 1 GB or TB of consumed storage space or on the price of a single VM replica. If there is a datastore or volume that is more expensive than other ones, an administrator can also specify the price adjustment factor (or the multiplier) that characterizes the premium charged for access to the datastore/volume.

- The **Details** section provides information on each replication job, including the number of replicated up VMs, total amount of gigabytes transferred to the storage and total cost.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a backup infrastructure subset to analyze in the report.
- **Replication jobs**: defines a list of replication jobs to include in the report.
- **Period**: defines the interval for which the billing statement is required.
- **Price**: defines a storage price for accommodating 1 GB/TB of replica files or a price for a VM replica.
- **Individual datastore price multipliers**: defines the price adjustment factor that characterizes the benefit (and the expense) of using the preferred datastore/volume storage capabilities. The resulting cost is calculated by multiplying the basic rate by the datastore multiplier.

  To edit price multipliers:

  a. Click **Configure**.

  b. In the **Configure Individual Datastore Price Multipliers** window, select the target datastore and click **Edit**.

  c. In the **Set Individual Datastore Price Multiplier** window, specify the desired price adjustment multiplier and click **Save**.

  d. Repeat steps **b–c** for each datastore price multiplier you want to edit.
- **Datastores**: defines a list of datastores and volumes that will be analyzed in the report.
- **Customer**: defines a customer name to be displayed in the report output.

> **NOTE:**
>
> Infrastructure topology view in Veeam ONE and Veeam Backup & Replication must match. Otherwise, Veeam ONE Web Client may show invalid data for Veeam Backup & Replication reports and dashboards.

Replica Billing

Description

This report provides chargeback capabilities for the backup infrastructure.

Report Parameters

Scope:	Backup Infrastructure
Replication Job:	All Jobs
Customer:	
Price per VM:	1
Interval:	12/1/2022 - 12/31/2022
Datastores:	All

Details

Datastore Name: Datacenter\pdc99

Backup Server: ms-vbr11a.tech.local

Price Multiplier: x1.00

Job	Job Runs	N. of VMs	Stored Size (GB)	Transferred Size (GB)
⊟ Replication Job 2		1	40.65	4.95
	12/10/2022 2:19 PM	1	40.65	4.95
			Total Size (GB):	40.65
			Total VMs:	2
			Total Cost:	2.00

Use Case

This report allows managed storage providers (MSP) to generate billing statements for customers and charge them for the used storage.

The report can help administrators to evaluate efficiency of the storage resources utilization.

Report Builder

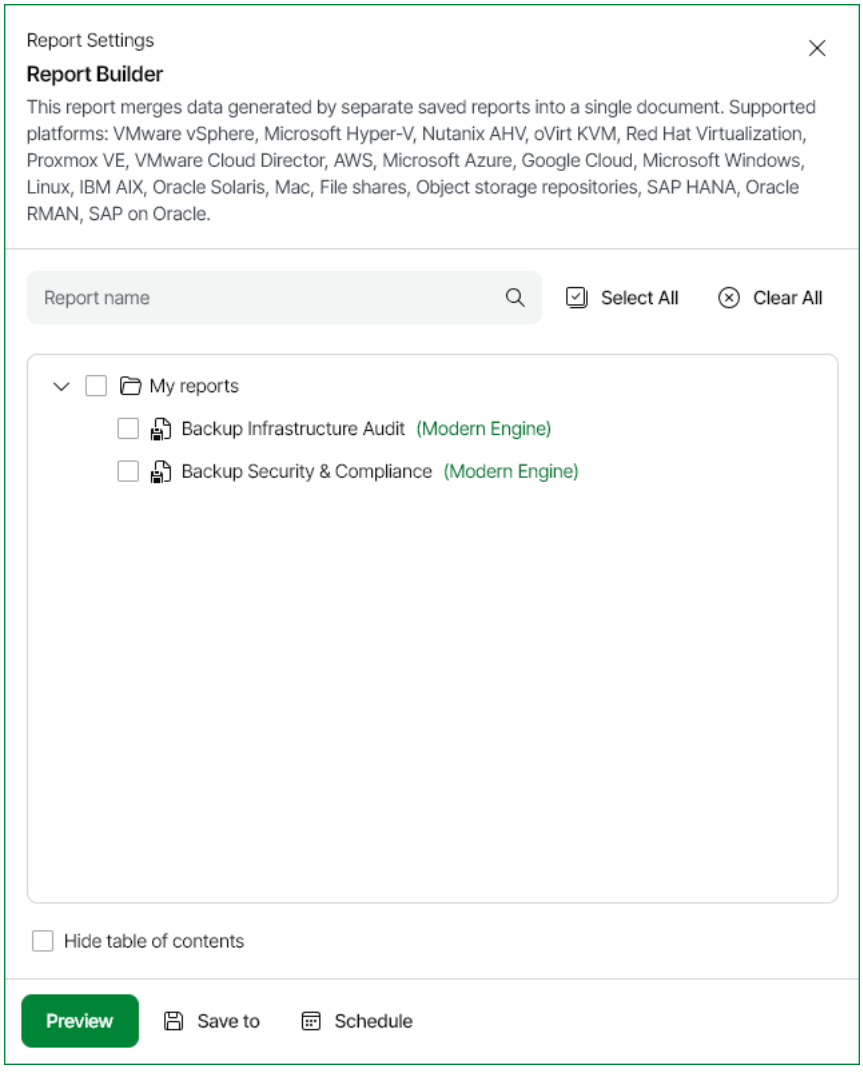
This report merges data generated by separate custom reports into a single document.

To use the Report Builder, you first need to configure and save custom reports in the **My reports** folder. The Report Builder will then offer you to include different sections from the saved reports into the resulting report providing you a consolidated view of core virtual environment properties.

Report Parameters

You can specify the following report parameters:

- **My Reports**: select the saved reports that should be included in the resulting custom report.
- **Hide table of contents**: defines whether the report output will include table of contents or display results in the expanded view.



Use Case

This report eliminates data redundancy and helps you focus on the most relevant and important information about your infrastructure.

Resource Pool and vApp Performance

This report aggregates historical data and shows performance statistics for a selected resource pool/vApp across a time range.

The report shows tables and performance charts with statistics on CPU, memory, disk and network usage for the resource pool/vApp. The report also lists top resource consuming VMs and calculates resource usage trends for them.

- The **Navigation** section shows path to the selected object, including VMware vSphere VC, datacenter, cluster and resource pool.

  Click a cluster name to drill down to performance charts with statistics on CPU, memory, disk and network usage for the cluster.

- The **Performance** subsections provide information on CPU, memory, disk and network usage, including usage trends and top resource consuming VMs.

  Click a VM name in the list of top resource consuming VMs to drill down to performance charts with statistics on CPU, memory, disk and network usage for the VM.

Report Parameters

You can specify the following report parameters:

- **Object**: defines the resource pool or vApp to analyze in the report.
- **Period**: defines the time period to analyze in the report. Note that the reporting period must include at least one successfully completed *Object properties data collection* task for the selected resource pool/vApp. Otherwise, the report will contain no data.
- **Business hours only**: defines time of a day for which historical performance data will be used to calculate the performance trend. All data beyond this interval will be excluded from the baseline used for data analysis.
- **Top N**: defines the maximum number of VMs to display in the report output.

View Report Example

Use Case

The report helps you identify resource pools and vApps with performance issues, evaluate how efficiently your resource pools and vApps are performing, and decide whether additional right-sizing or reconfiguration actions are necessary.

Restore Operator Activity

This report allows you to keep an eye on all types of restore actions performed across the selected Veeam Backup & Replication servers. The report analyzes all guest file, application-level and full VM restore activities performed by any authorized user and arranges this information by restore date (from newest to oldest).

- The **Summary** section includes the following elements:
  - The **Restores by User** chart shows the number of restore actions performed by each authorized user.
  - The **Restore Session Statistics** chart shows the number of restore actions performed during the reporting period.
- The **Details** table provides information on restore actions, including restore type, initiating user, name of the recovered item or VM, restore point age, the intended restore destination and the success status of the completed job.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a list of Veeam Backup & Replication servers to include in the report.
- **Users**: defines backup administrators and restore operators whose restore activity must be analyzed.
- **Restore type**: defines a restore type to evaluate in the report (*Full VM restore**, *Guest files (OS and NAS files)*, *Application item restores*, *Restore from tape*, *All*).
- **Period**: defines the time period to analyze in the report.

*This entry includes the following components: full VM restores, Instant VM Recovery, restore of virtual disks, VM files, Replica Failover.

View Report Example

Use Case

Since data can be restored from the Veeam Backup & Replication console, Veeam Backup Enterprise Manager and Veeam self-service restore portals, using PowerShell scripts or through REST API, in large environments with multiple backup administrators it is often hard to track all performed restore actions.

The report helps you track the initiator of each restore attempt, find out the most popular recovery items and establish historical trends.

Restore Operator Activity (Veeam Backup for Microsoft 365)

This report allows you to monitor all types of restore actions performed across your selected Veeam Backup for Microsoft 365 servers. The report analyzes restored applications including mail, OneDrive, sites and Teams performed by any authorized user that can additionally be grouped by customized settings.

- The **Summary** section includes the following elements:
  - The **Top 10 Operators by Restores** list shows the top 10 users who have initiated the largest number of restore sessions.
  - The **Top 10 Restored Objects** list shows the top 10 objects with the largest number of restore sessions.
  - The **Restores by Type** chart shows restore operations by type (*Restore, View, Save, Export, Send*).
  - The **Restores by Application** chart shows the number of restores by type of application (*Mail, OneDrive, Site, Teams*).
  - The **Restore Sessions by Application Type** chart and table shows the number of restore sessions per day by application type (Mail, OneDrive, Site, Teams).
  - The **Restore Sessions Details** table provides information on each restore action, including restore type, initiating user, name of recovered item, restore start time and item size, intended restore destination and status of intended job.
- The **Report Data** display provides information on each restore action, including restore type, initiating user, name of recovered item, restore start time and item size, intended restore destination and status of intended job.

> **NOTE:**
>
> Veeam ONE only collects information about restores from Veeam Backup for Microsoft 365 versions 8 and above. Restore data from versions below 8 is not presented in this report.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a list of Veeam Backup for Microsoft 365 servers to include in the report.
- **Organizations**: defines the Microsoft organizations to analyze in the report.
- **Restore types**: defines the list of restore types to analyze in the report (*Restore, View, Save, Export* and *Send*).
- **Application types**: defines the list of application types to analyze in the report.
- **Period**: defines the time period to analyze in the report.

View Report Example

Use Case

As data can be restored from the Veeam Backup for Microsoft 365 console, using PowerShell scripts or through REST API, in large environments with multiple backup administrators it is often hard to track all performed restore actions.

This report helps you track the initiator of each restore attempt, asses the most regularly restored objects and establish historical trends.

Scale-Out Backup Repository Configuration

The report provides configuration and resource utilization details for scale-out backup repositories in Veeam Backup & Replication.

- The **Summary** section provides an overview of configured scale-out repositories, such as the total number of the connected repositories, their capacity and utilization ratio, number of extents, their types, and a policy used for each repository.
    - The **Top N Utilized Scale-Out Repositories (GB)** and **Top N Utilized Extents (GB)** charts show most utilized scale-out repositories and their extents, total capacity, used space.
- The **Details** section provides information on each connected scale-out repository included in the report:
    - The **Overview** table shows the list of extents in the repository, their type, type of stored backup files, maximum number of concurrent tasks, region, container, operational restore windows settings, immutability, encryption settings, infrequent access storage, storage consumption limit, archive policy settings and deep archive settings.
    - The **Dynamics of SOBR free space usage** chart shows scale-out repository space usage dynamics over the past month.
    - The **Details** table provides information about extent capacity and free space in GB, size of full and incremental backups, and the number of VMs and computers stored on each extent.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a list of Veeam Backup & Replication servers to include in the report.
- **Top N**: defines the maximum number of scale-out repositories to display in the report.

View Report Example

Use Case

The report shows configuration and utilization data for scale-out backup repositories and their extents.

Tape Backup Jobs

The main backup purpose is to protect your data against disasters and failures. Having only one copy of a backup file does not provide the necessary level of safety. To build a successful data protection and disaster recovery plan, you must have two different types of media to store copies of your data, for example, disk storage and tape.

To learn more about the 3-2-1 backup strategy, see the Veeam Blog article How to follow the 3-2-1 backup rule with Veeam Backup & Replication.

This report maintains a record of VMs and computers archived to tapes.

- The **Summary** section provides information on the number of VMs and computers in backups stored on disk and archived to tapes, consumed tape capacity, and the total number of used tapes.
- The **Details** and **Tape Details** tables show properties of each backup to tape job: the total number of available restore points, restore point creation date, number of VMs and computers in the backup file and backup type (full or incremental).

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a list of Veeam Backup & Replication servers to include in the report.

View Report Example

Use Case

The report provides a summary of all backup to tape operations that took place on the managed backup server. The report displays an inventory list of items archived to the tape media. This allows you to make sure that mission critical VMs and computers have backups on tapes and are safely protected.

Tape GFS Backup Files

This report provides historical information about backups for Veeam Backup & Replication backup to tape with GFS retention policy.

- The **Summary** section provides information on the number of GFS media pools, number of historical backup files, number of restore points in these files, and the amount of space consumed by historical backup files on tape.
    - The **Historical Restore Points Count** chart shows the number of daily, weekly, monthly, quarterly and yearly restore points in historical backup files.
- The **Details** table provides information about historical restore points in GFS media pools, including the media set, number of VMs and computers, date when restore point was created, name of a tape job that created the restore point, and ID of tapes on which the restore point resides.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a list of Veeam Backup & Replication servers to include in the report.
- **Media pools**: defines a list of Veeam Backup & Replication GFS media pools to analyze in the report.

View Report Example

Use Case

The report allows you to inventory historical backups on tape created in accordance with the GFS retention scheme. You can track historical restore points on tape and make sure that you have backups archived for long-term retention.

Tape GFS Configuration

The report provides information about GFS Media Pools configuration and backup to tape jobs that write restore points to the Media Pools.

- The **Details** section displays media pool configuration — how many tapes and tape libraries are assigned to the pool, and the number of free tapes.
- The **Media Pool Configuration** table provides details on media sets, such as GFS retention period for every backup restore point, how many tapes are assigned to each media set, and where tapes must be exported when a job is finished.
- The **List of Tapes Assigned** table shows additional information about jobs assigned to specific media sets.
- The **Jobs Writings to The Media Pool** section shows information about backup to tape jobs that write restore points to media pools and their backup schedule.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a list of Veeam Backup & Replication servers to include in the report.
- **Media pools**: defines a list of Veeam Backup & Replication GFS media pools to analyze in the report.

View Report Example

Use Case

The report allows you to review configuration of media pools and GFS backup to tape jobs. You can trace tapes assigned to each media set, when media sets must be exported and where the exported tapes are stored.

Tape Media Retention Period

This report provides information on retention policy settings configured for tape media pools in Veeam Backup & Replication.

- The **Summary** section includes the following elements:
  - The **Tapes By Expiration Status** chart shows the number of protected tapes, the number of tapes with no expiration date, the number of tapes without defined expiration date and the number of tapes which can expire any time.
  - The **Expired Tapes Status** chart shows the share of online and offline expired tapes.
- The **Report Data** section information on tape media, including media pool to which the tape medium belongs, backup server, tape status, library, protection period, media set, tape, tape state, tape location, last write time, capacity (GB), free space (GB) and expiration date.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a list of Veeam Backup & Replication servers to include in the report.
- **Tape status**: defines whether the status of tapes to include in the report (*Expired*, *Protected*, *No expiration, Other*, *All*).

View Report Example

Use Case

This report allows you to review retention policies applied to tapes and estimate available tape resources.

Tape Vaults Overview

This report provides information on tape vaults created in Veeam Backup & Replication, lists all tapes archived in these vaults and previous tape location.

- The **Summary** section includes the **Tapes By Expiration Date** chart that shows how soon data in tape vaults will expire and how many tapes will expire within the specified period.
- The **Report Data** section provides the **Details** and **Tape Vaults Overview** tables detailing information on the Veeam Backup & Replication server where the vault was created, stored offline tapes, previous location of each tape and how soon media sets will expire.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a list of Veeam Backup & Replication servers to include in the report.

- **Vaults**: defines a list of vaults to include in the report.

Tape Vaults Overview

Description

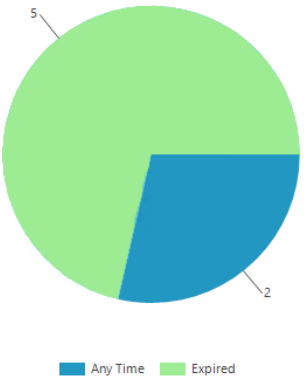
This report shows all tape vaults created and lists all tapes stored in these vaults.

Report Parameters

Scope: Backup Infrastructure
Vaults: All

Summary

Tapes by Expiration Date



Details

Backup Server: etna

Vault Name	Tape	Tape Library	Media Pool	Media Set	Retention	Expires in...
Atlanta Veeam Media Vault	1	1	1	1		
	0014003F	HP MSL G3 Series 3.00	GFS Media Pool 1	Daily media set #1 1/14/2019 11:59 PM	Not defined	Expired
Delta Veeam Media Vault	3	1	1	1		
	0014003E	HP MSL G3 Series 3.00	GFS Media Pool 1	Daily media set #1 1/14/2019 11:59 PM	Not defined	Expired
	0014003D	HP MSL G3 Series 3.00	GFS Media Pool 1	Daily media set #1 1/14/2019 11:59 PM	Not defined	Expired
	0014003A	HP MSL G3 Series 3.00	GFS Media Pool 1	Daily media set #1 1/14/2019 11:59 PM	Not defined	Expired

Use Case

This report allows you to track offline tapes stored in vaults that were created by Veeam Backup & Replication servers. Since vaults keep information about original location of tapes, such as library and media pool, data written to tapes and retention policy, you can also use the information provided in the report to facilitate offline tape management and track VMs and computers stored on these tapes.

Tenants Backup Compatibility

This report shows what versions of Veeam Backup & Replication run on backup servers of Veeam Cloud Connect tenants.

- The **Details** section shows a list of tenants and version and build number of Veeam Backup & Replication running on tenants backup servers.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a list of Veeam Backup & Replication servers to include in the report.
- **Tenants**: defines a list of Veeam Cloud Connect tenants to include in the report.

View Report Example

Use Case

If the service provider runs the latest version of Veeam Backup & Replication, it is recommended that tenants connected to this service provider also upgrade to the latest version of Veeam Backup & Replication. Tenants who run an earlier version of Veeam Backup & Replication cannot leverage the full cloud connect functionality, as features introduced in the latest version will not work for them and may result in failed jobs.

For details, see section Console Versions in Veeam Cloud Connect Infrastructure of the Veeam Cloud Connect Guide.

Undersized VMs (Hyper-V)

This report allows you to identify VMs that have less allocated resources such as vRAM or vCPU than they require.

- The **Summary** section provides an overview of the current state of your infrastructure, including the total number of VMs and the number of CPU and memory undersized VMs, and shows recommendations on resource allocation.
- The **Undersized Virtual Machines by CPU** and **Undersized Virtual Machines by Memory** tables display VMs with insufficient CPU and memory resources and deliver recommendations for their reconfiguration.

  Click a VM name in the **Virtual Machine** column to drill down to VM performance charts that show how CPU and memory usage has been changing within the reporting period.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **Business View objects**: defines Business View groups to analyze in the report. The parameter options are limited to objects of the Virtual Machine type.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.
- **Period**: defines the time period to analyze in the report. Note that the reporting period must include at least one successfully completed *Object properties data collection* task for the selected scope. Otherwise, the report will contain no data.
- **Business hours from - to**: defines time of a day for which historical performance data will be used to calculate the performance trend. All data beyond this interval will be excluded from the baseline used for data analysis.
- **CPU usage, more than**: defines the CPU utilization threshold in percent. If the CPU usage value for a VM exceeds the specified threshold, the VM will be included in the report.
- **Memory pressure, more than**: defines the dynamic memory pressure threshold in percent. If the memory pressure value for a VM exceeds the specified threshold, the VM will be included in the report.
- **Physical memory, more than**: defines the threshold for the amount of physical memory assigned to a VM. If the physical memory amount exceeds the specified threshold, this VM will be analyzed in the report.

> **NOTE:**
>
> Veeam ONE Web Client checks whether the **CPU ready** and **CPU Usage** conditions are true at the same, and then whether **Swap out rate** and **Memory Usage** conditions are true at the same time (in other words, the conditions in each pair are joined by Boolean "AND").
>
> Veeam ONE Web Client checks whether a pair of these conditions is true, in other words, pairs of these conditions are joined by Boolean "OR".

Undersized VMs

Description

This report helps you to discover VMs with over-utilized CPU and memory resources. It analyzes VMs historical performance and configuration data to provide recommendations on appropriate vCPU and vRAM allocation for VMs.

Report Parameters

Scope:	Virtual Infrastructure
Reporting period:	1 week (12/24/2022 - 12/30/2022)
Business View objects:	
CPU usage, more than:	80 %
Physical memory, more than:	1 GB
Memory pressure, more than:	80 %
Working hours:	

Summary

Total undersized VMs:	2
Total VMs:	16
CPU undersized VMs:	0
Memory undersized VMs:	2
CPU resources to be assigned:	0 vCPUs

Undersized Virtual Machines by Memory

⊟SCVMM:

Cluster/Host	Virtual Machine	Memory				Recommended Amount of RAM
		Capacity (GB)	Average Demand (GB)	Peak Demand (GB)	Peak Pressure (%)	
⊟pdctwhv01.tech.local	2					
	ahvbkpsrv	6.00	5.58	6.47	108.00	6.5 GB
	srv08	5.00	7.29	7.81	156.00	8 GB

Note: Consider relocating VM to a different host, if present does not have enough memory resources.

Use Case

This report uses the specified parameters to identify VMs with insufficient CPU and memory resources. The report delivers detailed information on detected VMs and suggests recommendations for better resource allocation. You may consider adding the specified amount of resources for the VM, relocating the VM to a more powerful host, or adding more resources for undersized VM.

Undersized VMs (vSphere)

This report helps you detect virtual machines that have less allocated vRAM or vCPU resources than they require. The report analyzes historical performance and configured resource allocation to provide recommendations for an optimized VM configuration and allocation of resources.

- The **Summary** section provides an overview of the current state of your infrastructure, including the total number of VMs and the number of CPU and memory undersized VMs, and shows recommendations on resource allocation.
- The **Undersized Virtual Machines by CPU** and **Undersized Virtual Machines by Memory** tables display VMs with insufficient CPU and memory resources and deliver recommendations for their reconfiguration.

  Click a VM name in the **Virtual Machine** column to drill down to VM performance charts that show how CPU and memory usage has been changing within the reporting period.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **VMware Cloud Director objects**: defines VMware Cloud Director components to analyze in the report.
- **Business View objects**: defines Business View groups to analyze in the report. The parameter options are limited to objects of the Virtual Machine type.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.
- **Last <N>**: defines the time period to analyze in the report. Note that the reporting period must include at least one successfully completed *Object properties data collection* task for the selected scope. Otherwise, the report will contain no data.
- **Business hours only**: defines time of a day for which historical performance data will be used to calculate the performance trend. All data beyond this interval will be excluded from the baseline used for data analysis.
- **CPU ready, more than (%)**: defines the threshold for the percentage of time during which CPU resources were in the ready state. If the CPU Ready Time value for a VM exceeds the specified threshold, the VM will be included in the report.
- **Swap out rate, more than (KBps)**: defines the threshold for the percentage of the time which a VM spent waiting for memory to be swapped back in from disk. If the Swap Wait Time value for a VM exceeds the specified threshold, the VM will be included in the report.
- **CPU utilization (%)**: defines the CPU utilization threshold. If the CPU usage value for a VM exceeds the specified threshold, the VM will be included in the report.
- **Memory utilization (%)**: defines the memory utilization threshold. If the memory usage value for a VM exceeds the specified threshold, the VM will be included in the report.
- **Memory counter type**: defines whether the *Memory Active* or *Memory Consumed* performance metric should be analyzed in the report.

NOTE:

Veeam ONE Web Client checks whether the **CPU ready** and **CPU Usage** conditions are true at the same time, and then whether **Swap out rate** and **Memory Usage** conditions are true at the same time (in other words, the conditions in each pair are joined by Boolean "AND").

Then Veeam ONE Web Client checks whether a pair of these conditions is true, in other words, pairs of these conditions are joined by Boolean "OR".

Undersized VMs

Description

This report helps you to discover VMs with over-utilized CPU and memory resources. It analyzes VMs historical performance and configuration data to provide recommendations on appropriate vCPU and vRAM allocation for VMs.

Report Parameters

Scope:	Virtual Infrastructure
Interval:	1 month (12/16/2018 - 1/15/2019)
Business View objects:	
CPU ready, more than:	10 %
CPU utilization:	90 %
Swap out rate, more than:	0 Kbps
Memory utilization:	90 %
Memory counter type:	Active

Summary

Total undersized VMs:	5
Total VMs:	544
CPU undersized VMs:	1
Memory undersized VMs:	4
CPU resources to be assigned:	1 vCPUs

Undersized Virtual Machines by CPU

⊟Virtual Server: elal.dev

Cluster/Host	Virtual Machine	vCPUs	CPU Utilization (%)	CPU Ready (%)	Recommended Number of vCPUs
⊟ Cluster1	1				
	SA5_VM6_Win10x64_EM_sql (f5a52a2a-a188-4b1c-b320-ed2deccb9b13)	6	92.00	32.00	7

Note: Consider relocating VM to a different host, if present does not have enough CPU resources.

Undersized Virtual Machines by Memory

⊟Virtual Server: elal.dev

Cluster/Host	Virtual Machine	Allocated (GB)	Memory Average Usage (%)	Swap out Rate (Kbps)	Recommended Amount of RAM
⊟ Cluster1	2				
	2 SA VBR 10	4.00	95.12	0.00	5.1 GB
	vCenter Appliance	8.00	91.05	0.00	10.1 GB
⊟ Cluster2	1				
	SA_L2_VM1_Win10_1809	4.00	38.81	0.00	5.1 GB

⊟Virtual Server: vcenter01

Cluster/Host	Virtual Machine	Allocated (GB)	Memory Average Usage (%)	Swap out Rate (Kbps)	Recommended Amount of RAM
⊟ esx01	1				
	srv11	4.00	93.94	0.00	5.1 GB

Note: Consider relocating VM to a different host, if present does not have enough memory resources.

Use Case

This report provides practical recommendations for restoring performance of VMs that have less resources than they need. You may consider adding the specified amount of resources for the VM, relocating the VM to a more powerful host, or committing increased resources to a resource pool shared by the undersized VM.

Unmapped Datastore LUNs

This report provides information about all detected shared datastores that are not mapped to any existing backup proxy. If you are going to use the Direct SAN Access mode, datastore LUNs must be mapped to a proxy server.

- The **Summary** section provides an overview on the total number of datastores, the number of unmapped datastores, their capacity and the number of VMs on unmapped datastores.
- The **Details** section displays detailed mapped and unmapped datastore information, such as capacity the amount of free and used space, and the number of stored VMs.

Report Parameters

You can specify the following report parameters:

- **Scope**: defines a virtual infrastructure level and its sub-components to analyze in the report.

> **NOTE:**
>
> Infrastructure topology view in Veeam ONE and Veeam Backup & Replication must match. Otherwise, Veeam ONE Web Client may show invalid data for Veeam Backup & Replication reports and dashboards.

View Report Example

Use Case

The Direct SAN Access mode is recommended if the ESXi host uses shared storage. In the Direct SAN mode, proxy servers will not be able to read data from LUNs if they are not mapped. This report allows you to detect datastore LUNs that are not mapped to any proxy server in your backup infrastructure.

vApp Configuration

This report provides an overview of vApp configuration for a selected organization.

- The **Summary** section includes the following elements:
  - The **vApps by Status** chart shows the number of powered off, powered on, resolved and suspended vApps.
  - The **VMs by VMware Tools Status** chart shows statuses of VMware Tools installed in VMs that belong to the organization.
  - The **Top 5 vApp** charts that display vApps with the highest level of CPU, memory and storage utilization.
- The **Details** table displays detailed information on configuration properties for each vApp created by organization users.

Report Parameters

You can specify the following report parameters:

- **Organization:** defines the organization whose vApps should be analyzed in the report.

vApp Configuration

Description

This report provides general information on vApp configuration for selected organization.

Report Parameters

Organization: Main-Org

Summary

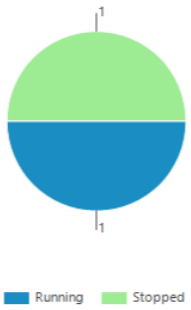
General Overview

N. of Virtual Datacenters:	1
N. of vApps:	2
N. of VMs:	4

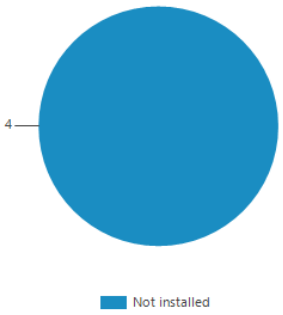
Resource Allocation

Allocated CPU (GHz):	6.00
Allocated Memory (GB):	4.00
Allocated Storage (GB):	72.00

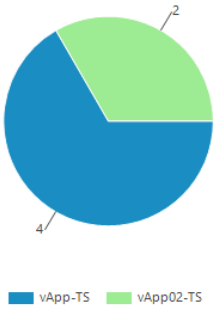
vApps by Status



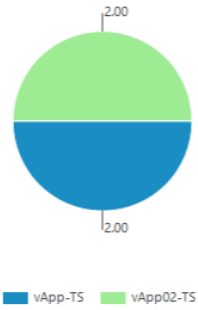
VMs by VMware Tools Status



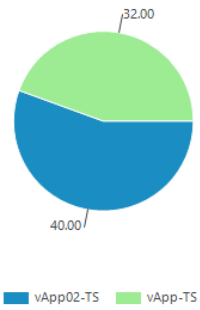
Top 5 vApp by CPU Quota



Top 5 vApp by Memory Quota



Top 5 vApp by Storage Quota



Details

Organization: Main-Org

vApp Configuration

vApp	Virtual Datacenter	Virtual Machine	Runtime Lease Expires on	Storage Lease Expires on
vApp02-TS	Main-Org-VDC	2	-	1/27/2023 11:56 AM
vApp-TS	Main-Org-VDC	2	1/10/2023 9:37 AM	-

vApp Virtual Machines

vApp	Virtual Machine	Status	VMware Tools Status	Processor	Memory (GB)	Storage (GB)
⊟vApp02-TS	2	Stopped		2	2.00	40.00
	ubuntu-vm03-ts	Powered Off	Not installed	1	1.00	16.00
	win-vm04-ts	Powered Off	Not installed	1	1.00	24.00
⊟vApp-TS	2	Running		4	2.00	32.00
	ts-vm01	Powered On	Not installed	2	1.00	16.00
	ts-vm022	Powered On	Not installed	2	1.00	16.00

Use Case

This report helps VMware Cloud Director administrator right-size resource provisioning to prevent resource waste and to eliminate potential performance bottlenecks.

vApp Performance

This report aggregates historical data and shows performance statistics for a selected vApp and resource pools across a time range.

- The **Performance** subsections show tables and performance charts with CPU, memory, disk and network usage statistics, list top resource consuming VMs and displays resource usage trends for them.

Report Parameters

You can specify the following report parameters:

- **vApp**: defines the vApp to analyze in the report.
- **Period**: defines the time period to analyze in the report.
- **Business hours only**: defines time of a day for which historical performance data will be used to calculate the performance trend. All data beyond this interval will be excluded from the baseline used for data analysis.

- **Top N**: defines the maximum number of VMs to display in the report output.

vApp Performance

Description

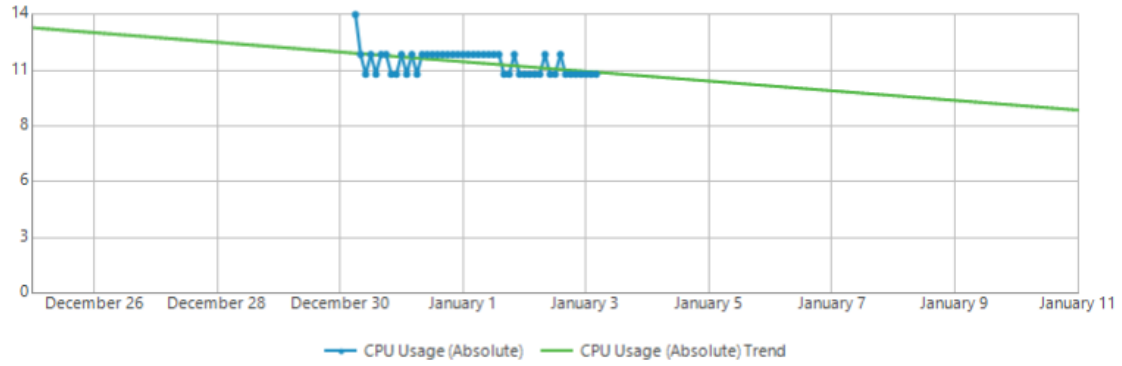
This report shows vApp performance history, including CPU, memory, disk and network performance history.

Report Parameters

vApp:	vApp01
vApp location:	\\prgclouddirector01.tech.local\organization01\Organization01-VDC\vApp01
Reporting period:	12/25/2022 - 1/10/2023

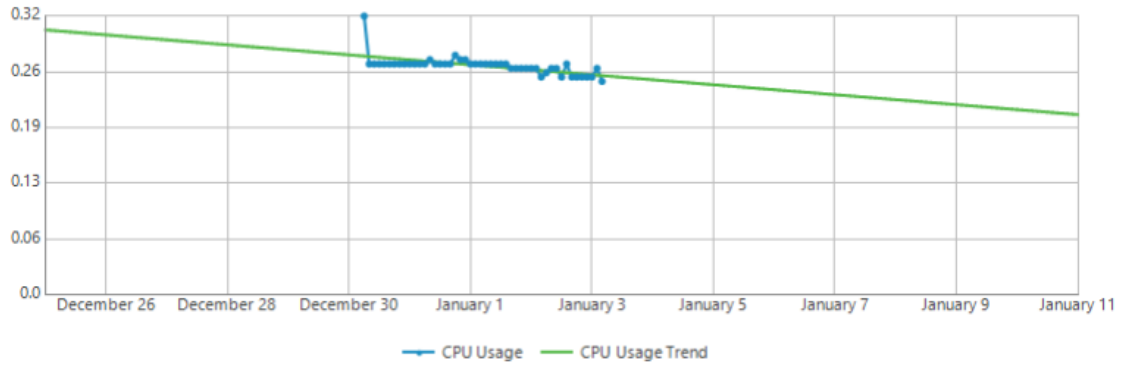
CPU Performance

CPU Usage (Absolute) (MHz)



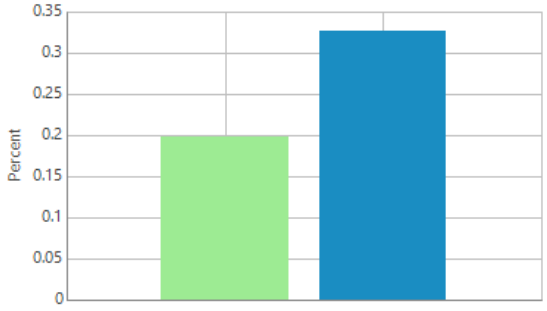
Object Name	Average	Minimum	Maximum	Std. Deviation	Trend
vApp01	11.58	11.00	14.00	0.61	Decreasing

CPU Usage (Percent)



Object Name	Average	Minimum	Maximum	Std. Deviation	Trend
vApp01	0.26	0.25	0.32	0.01	Decreasing

Top 3 VMs by CPU Usage



Object Name	Avg	Trend
vm02-RqUH	0.33	Decreasing
vApp01-7nFN	0.20	Decreasing

Use Case

The report helps you identify vApps with performance issues and decide whether additional right-sizing or reconfiguration actions are necessary.

Veeam Backup Files Growth

This report allows you to track how the size of backup files was changing during the specified time period, and identify jobs that consume the greatest amount of space on repositories.

- The **Summary** section provides a general overview of repository capacity, free space, backup size and restore points as well an overview of backup jobs, job runs and stored VMs and computers. It also displays the **Top 10 Jobs by Largest Backup File Size** table that shows 10 jobs that produced the greatest amount of backup data during the reporting period as well as a virtual chart for each connected repository.
- The **Report Data** section displays **Details** and **Extended Details** tables with information on repository space usage. For each repository, the report provides a chart that illustrates the repository capacity and the amount of free space left, as well as information about restore points that were created during the reporting period, including VMs and computers in the backup, backup file type, date and time when the file was created, restore point size and total space used.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a list of backup repositories to analyze in the report.
- **Jobs**: defines a list of backup jobs to include in the report.
- **Period**: defines the time period to analyze in the report.

View Report Example

Use Case

This report is useful for capacity planning purposes. The report allows you to assess historical growth of backup files and — in case backup files grow too fast — to decide whether to change job configuration to point it to another repository with larger capacity.

Verified VMs

This report provides information on SureBackup jobs performed by Veeam Backup & Replication and displays the summary of verified VMs.

SureBackup and SureReplica technologies allow virtualization administrators to validate the recoverability of created backups and replicas in an isolated test environment by examining their key viability indicators. This ensures that your backups and replicas are fully reliable and minimizes the risk of data loss in case a VM fails.

- The **Summary** section provides an overview on the number of protected and verified VMs, displays the status history of verified VMs and verification rate during the reporting period.
- The **Details** table provides information on VMs tested and verified with SureBackup and SureReplica, including the number of failed verifications, last verified restore point, status of the last verification and the results of VM verification tests (ping commands, scripts execution and heartbeat messages).

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a list of Veeam Backup & Replication servers to include in the report.
- **Business View objects**: defines Business View groups to analyze in the report. The parameter options are limited to objects of the Virtual Machine type.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.
- **Last <N> weeks/months**: defines the time period to analyze in the report.
- **Platform**: defines whether to analyze VMware vSphere or Microsoft Hyper-V infrastructure.
- **Job type**: defines a job type to evaluate in the report (*Backup and replication jobs*, *Backup jobs only*, *Replication jobs only*).

> **NOTE:**
>
> Infrastructure topology view in Veeam ONE and Veeam Backup & Replication must match. Otherwise, Veeam ONE Web Client may show invalid data for Veeam Backup & Replication reports and dashboards.

View Report Example

Use Case

This report helps administrators to quickly review the results of completed SureBackup jobs and confirm that the created backups and replicas are recoverable and error-free. This ensures that production VMs are reliably protected against failures and data corruption.

VM Backup Compliance Overview

This report returns a list of VMs that do not meet the requirement to have a minimal number of available backup copies.

To learn more about the 3-2-1 backup strategy, see the Veeam Blog article How to follow the 3-2-1 backup rule with Veeam Backup & Replication.

- The **Summary** section includes the **VM Compliance Status** chart that shows the proportion of backup-compliant VMs to the rest of VMs across the selected virtual infrastructure scope.
- The **Details** table provides information on non-compliant VMs properties, including VM location, number of backup copies/replicas, backup type and the date of the latest backup.

Report Parameters

You can specify the following report parameters:

- **Protected infrastructure**: defines the platform to analyze in the report.
- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **VM folders**: defines a list of VMware folders to include in the report (applies to VMware vSphere environments only). VM folders is an alternate way to present the virtual infrastructure. If VMs in your infrastructure are grouped into folders according to their profile, you can limit the report scope by specifying the necessary folders only.
- **Business View objects**: defines Business View groups to analyze in the report. The parameter options are limited to objects of the Virtual Machine type.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.
- **VMware Cloud Director objects**: defines VMware Cloud Director components to analyze in the report.
- **Required number of VM copies**: defines the minimum number of backup copies/replicas a virtual machine must have to meet the compliance requirements.
- **VM exclusion rule**: defines a list of VMs that should be excluded from the report scope. You can enter VM names explicitly or create a wildcard mask by using the asterisk (*) to replace any number of characters. Multiple entries are separated by semicolon. Usage example: the following string will exclude machines with the _R&D suffix from appearing in the report: *_R&D.

View Report Example

Use Case

This report allows you to make sure that all mission critical VMs have sufficient amount of backup copies in distinct locations within the organization, as requested by the 3-2-1 backup strategy. This information may help you modify job settings or dynamically adjust your backup file retention policies.

VM Change Rate Estimation (Hyper-V)

This report predicts the number of changed blocks (measured in GB) for virtual disks based on virtual machines write rate. The report analyzes rates at which data was written to virtual disks during the selected reporting interval, and displays VMs that grew faster and slower than other VMs.

- The **Summary** section contains the following charts:
  - The **Top 5 VMs with Largest Change Rate (GB)** chart shows 5 VMs with the greatest amount of changed blocks within the reporting period.
  - The **Top 5 VMs with Least Change Rate (GB)** chart shows 5 VMs with the least amount of changed blocks within the reporting period.
- The **Details** table provides information on the total change rate and the hourly, daily or weekly change rate (depending on the reporting interval).

  Click a VM name to drill down to change rate statistics for each VM disk.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **Business View objects**: defines Business View groups to analyze in the report. The parameter options are limited to objects of the Virtual Machine type.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.
- **Period**: defines the time period to analyze in the report.
- **Top N**: defines the number of top VMs that will be included in the report.

- **Show VMs with no changes**: defines whether VMs with no detected changes must be included in the report.

VM Change Rate Estimation

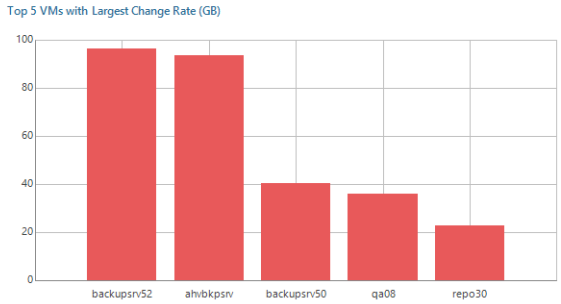
Description

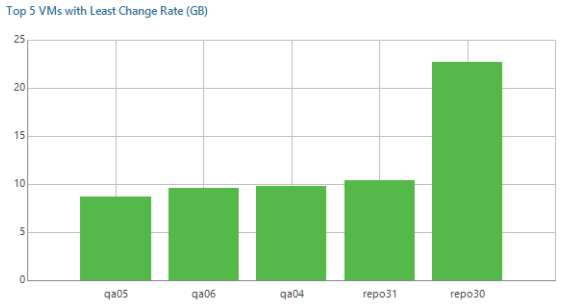
This report predicts the number of changed blocks (measured in GB) for virtual disks based on virtual machines write rate.

Report Parameters

Scope:	Virtual Infrastructure
Interval:	Current week (12/26/2022 - 1/1/2023)
Top N:	5
Show VMs with no changes:	False
Business View objects:	

Summary





Details

Scope	VM	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday	Total
⊟pdctwhv01.tech.local	9	114.34 GB	95.17 GB	102.93 GB	14.79 GB	-	-	-	327.23 GB
	backupsrv52	26.35 GB	26.87 GB	38.82 GB	4.35 GB	-	-	-	96.39 GB
	ahvbkpsrv	49.10 GB	23.08 GB	18.96 GB	2.34 GB	-	-	-	93.47 GB
	backupsrv50	12.33 GB	11.17 GB	12.94 GB	4.03 GB	-	-	-	40.48 GB
	qa08	10.64 GB	13.29 GB	10.31 GB	1.55 GB	-	-	-	35.80 GB
	repo30	4.64 GB	7.74 GB	9.04 GB	1.24 GB	-	-	-	22.67 GB
	repo31	3.00 GB	3.47 GB	3.38 GB	< 1 GB	-	-	-	10.34 GB
	qa04	2.91 GB	3.39 GB	3.32 GB	< 1 GB	-	-	-	9.79 GB
	qa06	2.79 GB	3.17 GB	3.16 GB	< 1 GB	-	-	-	9.61 GB
	qa05	2.57 GB	2.99 GB	2.99 GB	< 1 GB	-	-	-	8.69 GB
Total:		114.34 GB	95.17 GB	102.93 GB	14.79 GB	-	-	-	327.23 GB

Use Case

To perform incremental backup, Veeam Backup & Replication needs to know which data blocks have changed since the previous job run. The number of changed blocks reflects the amount of data written to the virtual disk.

Veeam Backup & Replication gathers this information to calculate the amount of new data that needs to be backed up. The more changes occur on the virtual disk, the larger amount of space is required to store data in backup. By estimating the change rate, the report helps you assess future needs for repository space.

VM Change Rate Estimation (vSphere)

This report predicts the number of changed blocks (measured in GB) for virtual disks based on virtual machines write rate. The report analyzes rates at which data was written to virtual disks during the selected reporting interval, and displays top N VMs that grew faster and slower than other VMs.

- The **Summary** section contains the following charts:
  - The **Top VMs with Largest Change Rate (GB)** chart shows VMs with the greatest amount of changed blocks within the reporting period.
  - The **Top VMs with Least Change Rate (GB)** chart shows VMs with the least amount of changed blocks within the reporting period.
- The **Details** table provides information on the total change rate and the hourly, daily or weekly change rate (depending on the reporting interval).

  Click a VM name to drill down to change rate statistics for each VM disk.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **VM folders**: defines a list of VMware vSphere folders to include in the report (applies to VMware vSphere environments only). VM folders view is an alternate way to present the virtual infrastructure. If VMs in your infrastructure are grouped into folders according to their profile, you can limit the report scope by specifying the necessary folders only.
- **VMware Cloud Director objects**: defines VMware Cloud Director components to analyze in the report.
- **Business View objects**: defines Business View groups to analyze in the report. The parameter options are limited to objects of the Virtual Machine type.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.
- **Period**: defines the time period to analyze in the report.
- **Top N**: defines the number of top VMs that will be included in the report.
- **Show VMs with no changes**: defines whether VMs with no detected changes must be included in the report.

View Report Example

Use Case

To perform incremental backup, Veeam Backup & Replication needs to know which data blocks have changed since the previous job run. The number of changed blocks reflects the amount of data written to the virtual disk.

Veeam Backup & Replication gathers this information to calculate the amount of new data that needs to be backed up. The more changes occur on the virtual disk, the larger amount of space is required to store data in backup. By estimating the change rate, the report helps you assess future needs for repository space.

VM Configuration Assessment

This report helps you to assess VMs readiness for performing backup with Veeam Backup & Replication. The report analyzes configuration of VMs in your virtual environment, and shows potential issues and possible limitations that could cause backup process to fail or prevent VMs from being properly backed up.

- The **Summary** section contains the following charts:
  - The **Virtual Machines Overview** chart shows VMs with potential issues and ready to backup VMs.
  - The **Potential Issues** chart shows number of VMs with potential issues.
- The **Details** section provides information on VMs with potential issues and recommendations on resolving the issues.

The report takes into account the following criteria when analyzing VM configuration:

VMware CBT

Criterion	Description
Existing Snapshots	The report analyzes your virtual infrastructure to find VMs with existing snapshots. To use VMware Changed Block Tracking for incremental backup, all existing snapshots must be removed.
Hardware Version 4 or earlier	The report analyzes your virtual infrastructure to find VMs with hardware version 4 or earlier. To use VMware Changed Block Tracking for incremental backup, hardware version of VMs must be 7 or later.

Virtual Disks

Criterion	Description
VMs with Independent Disks	The report analyzes your virtual infrastructure to find VMs with independent virtual disks. Veeam Backup & Replication does not support independent disks; these disks are skipped from processing automatically.
VMs with 2 TB virtual disks running in vSphere 5.1 or older	The report analyzes your virtual infrastructure to find VMs with 2 TB virtual disk size. For ESXi 5.1 and older, the maximum virtual disk (VMDK) size for snapshot operations is limited to 1.9844923662017202 TB. For details on, see this VMware KB article.

Criterion	Description
VMs with disks engaged in SCSI bus sharing	The report analyzes your virtual infrastructure to find VMs that use SCSI bus-sharing. VMware does not support taking snapshots of Microsoft Clustering Services (MSCS) VMs. For details on, see this VMware KB article.
Virtual disk size is not a multiple of 1 KB	The report analyzes your virtual infrastructure to find VMs with unaligned virtual disks. Veeam Backup & Replication does not support backup copy jobs and restore jobs for VMs with unaligned disks. For details on, see this Veeam KB article.
VMs with pRDMs	The report analyzes your virtual infrastructure to find VMs with RDMs used in physical compatibility mode. Veeam Backup & Replication will automatically exclude RDMs used in physical compatibility mode from the backup job. For details on, see this VMware KB article.

Application-Aware Image Processing

Criterion	Description
VMs with Windows Server 2000 Guest OS	The report analyzes your virtual infrastructure to find Windows Server 2000 VMs. To enable backup with application-aware image processing, upgrade guest OS to Windows Server 2003 or later.
VMware Tools Not Running	The report analyzes your virtual infrastructure to find VMs that do not have with VMware Tools installed or running. To enable backup with application-aware image processing, it is required that guest OS running inside your VMs has VMware Tools installed and running.

Datastore Free Space

Criterion	Description
VMs on datastores with 10% of free space	The report analyzes your virtual infrastructure to find datastores that have less than 10% of free space. When Veeam Backup & Replication backs up a VM, it triggers a VMware snapshot that is normally stored next to VM files on the source datastore. To eliminate the problem of datastores running low on free space during backup, it is required that the free space is more than 10%.

Other

Criterion	Description
Unsupported VM names	The report analyzes your virtual infrastructure to find VMs with names that contain the following symbols: @ / \ < >. Veeam Backup & Replication does not process VMs with names that contain mentioned symbols. If you want to back up these virtual machines, you must rename them.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **VMware Cloud Director objects**: defines VMware Cloud Director components to analyze in the report.
- **Business View objects**: defines Business View groups to analyze in the report. The parameter options are limited to objects of the Virtual Machine type.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.
- **Issues**: defines VM assessment criteria to include in the report.
- **Ignore replica VMs created by Veeam products**: defines whether to include in the report VM replicas created with Veeam Backup & Replication.

View Report Example

Use Case

This report allows you to obtain a list of VMs in your virtual environment that could experience potential issues with backups, and to get guidance on how to resolve these issues.

VM Configuration Chargeback

This report helps to make VM cost audit and identify the most and least expensive VMs based on the VM configuration.

The report analyzes VM cost based on flat fees for vCPU, vRAM and storage resources provisioned for a VM.

- The **Summary** section includes the following elements:
  - Details on the number of VMs, average VM cost and total cost of VMs.
  - The **Top 10 Most Expensive VMs** subsection shows 10 most expensive VMs in terms of allocated resources, and provides cost of vCPU, vRAM and storage resources configured for each VM.
  - The **Cost Distribution** chart shows the cost of hardware CPU, memory and storage resources.
  - The **VM Power Status** chart shows the number of running and powered-off VMs. This chart is available if you choose to include powered-off VMs in the report.
  - The **Business View Groups Cost** chart shows the cost of VMs included in Business View groups. This chart is available if you include Business View groups in the report scope.
- The **Details** table provides information on VM configuration cost in terms of vCPU, vRAM, storage and total cost.

NOTE:

- For VMs with thin-provisioned or dynamic disks, the report takes into account the amount of provisioned disk space, not actually used disk space.
- For VMs with dynamic memory, the report takes into account the amount of allocated memory.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components (hosts) to analyze in the report.
- **VMware Cloud Director objects**: defines VMware Cloud Director components to analyze in the report.
- **Business View objects**: defines Business View groups to analyze in the report. The parameter options are limited to objects of the Virtual Machine type.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.
- **Currency**: defines a payment currency.
- **Single vCPU cost**: defines the cost of one vCPU configured for a VM, in the selected currency.
- **Memory cost, per GB**: defines the cost of a memory GB allocated for a VM, in the selected currency.
- **Storage cost, per GB**: defines the cost of a storage GB allocated for a VM, in the selected currency.
- **Calculate storage hosts based on**: defines how VM storage host must be calculated in the report (*Provisioned space, Used space*).

- **Include powered-off VMs in the calculation**: defines whether powered-off VMs must be analyzed in the report.

VM Configuration Chargeback

Description

This report helps you to perform a VM costs audit and identify the most and least expensive VMs based on the current VM configuration.

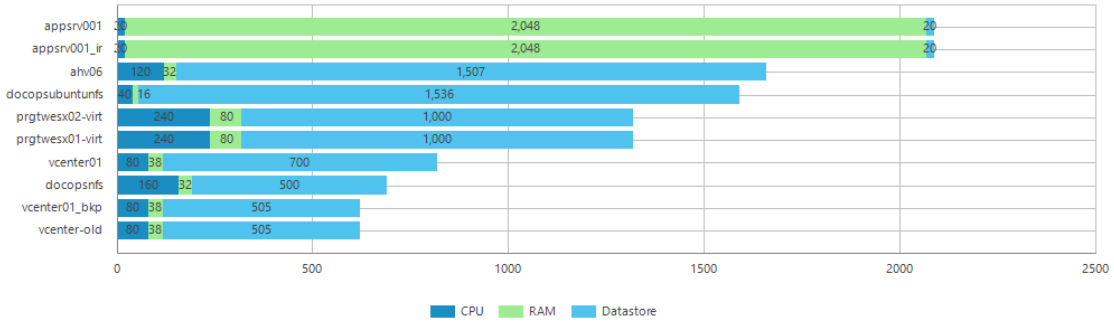
Report Parameters

Scope:	Virtual Infrastructure
Single vCPU cost:	20 USD
Memory cost, per GB:	2 USD
Storage cost, per GB:	1 USD
Include powered-off VMs in the calculation:	Yes
Calculate storage costs based on:	Provisioned space

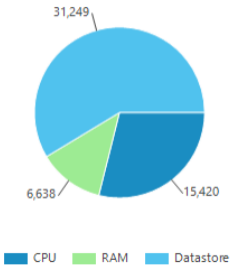
Summary

Number of VMs:	228
Average VM price, USD:	233.80
Total cost of VMs, USD:	53,307

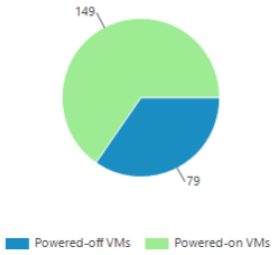
Top 10 Most Expensive VMs



Cost Distribution



VM Power Status



Details

VMware

vCenter Server: vcenter01.tech.local

Host	Virtual Machine	Power Status	vCPUs		RAM		Datastore		Total Price, USD
			Count	Cost, USD	Quantity, GB	Cost, USD	Quantity, GB	Cost, USD	
Cluster:	193								
⊟prgtwesx01.tech.local	88		291	5,820.00	520.88	1,041.75	12,060.39	12,060.39	18,922.14
	vcenter01	On	4	80.00	19.00	38.00	700.17	700.17	818.17
	vcenter01_bkp	Off	4	80.00	19.00	38.00	504.71	504.71	622.71
	vcenter-old	Off	4	80.00	19.00	38.00	504.71	504.71	622.71
	enterprise03	On	3	60.00	4.00	8.00	500.00	500.00	568.00
	srv12	On	4	80.00	8.00	16.00	400.00	400.00	496.00
	serv21	On	8	160.00	32.00	64.00	260.00	260.00	484.00
	srv13	On	4	80.00	6.00	12.00	350.00	350.00	442.00
	backupserver004	On	8	160.00	8.00	16.00	260.00	260.00	436.00
	backupserver001	Off	4	80.00	12.00	24.00	300.00	300.00	404.00
	serv02_vbo	On	3	60.00	4.00	8.00	300.00	300.00	368.00
	winsrv001	On	4	80.00	6.00	12.00	270.00	270.00	362.00
	enterprise05	On	6	120.00	8.00	16.00	220.00	220.00	356.00
	linuxsrv001	On	8	160.00	16.00	32.00	152.00	152.00	344.00
	srv16	On	4	80.00	6.00	12.00	250.00	250.00	342.00
	avspem1	Off	4	80.00	4.00	8.00	250.00	250.00	338.00
	enterprise07	On	6	120.00	8.00	16.00	200.00	200.00	336.00
	winsrv002	On	4	80.00	6.00	12.00	220.00	220.00	312.00
	enterprise01	On	4	80.00	8.00	16.00	200.00	200.00	296.00
	winorcl01	On	4	80.00	8.00	16.00	200.00	200.00	296.00
	linorcl01	On	4	80.00	8.00	16.00	200.00	200.00	296.00

Use Case

The report is intended for service providers that have flat fees on allocated virtual infrastructure resources. The report helps calculate the cost of resources that were allocated to each client or application owner, and bill tenants, clients and application owners according to the allocated resources.

IT departments can use this report to calculate the cost of provisioned VMs for application owners and business units, provided that the VM cost model in the organization is based on VM configuration.

VM Daily Protection Status

This report provides information on the daily backup status for all protected VMs.

The report complements the Protected VMs report and shows job completion results for backup, backup copy and replication tasks for protected VMs.

- The **VM Backup Status** chart represents overall efficiency of daily protection operations by displaying the number of VM tasks completed successfully, the number of VM tasks completed with warnings and the number of VM tasks failed. If you have launched a VM job several times a day, the report will show the best VM task status.
- The **Details** table provides a list of protected VMs and displays daily job completion results.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a list of Veeam Backup & Replication servers and protected VI servers to include in the report.
- **VM folders**: defines a list of VMware folders to include in the report (applies to VMware vSphere environments only). VM folders is an alternate way to present the virtual infrastructure. If VMs in your infrastructure are grouped into folders according to their profile, you can limit the report scope by choosing the necessary folders only.
- **Business View objects**: defines Business View groups to analyze in the report. The parameter options are limited to objects of the Virtual Machine type.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.
- **Interval**: defines a time period to analyze in the report (*Current week*, *Past week*, *Past 7 days*).
- **1 week starting at**: defines a time period (a week) to analyze in the report.
- **7 days starting at**: defines a start date of the reporting period. The report will analyze a 7-day period starting from the selected date.
- **Last <N> weeks**: defines the number of weeks in the past (starting from today) to analyze in the report.
- **Job types**: defines a job type to evaluate in the report (*Backup*, *Replication*, *Backup Copy*, *All*).
- **Analyze VM templates**: defines whether VM templates should be included in the report.

> **NOTE:**
>
> Infrastructure topology view in Veeam ONE and Veeam Backup & Replication must match. Otherwise, you will not be able to generate the report based on **VM folders** or **Business View objects**.

View Report Example

Use Case

The report helps you discover issues with created backups and replicas: detect failed jobs, identify jobs that triggered warnings and ensure that critical machines can be easily recovered in case of a disaster.

VM Failover Plan Overview

This report analyzes configuration of regular and cloud failover plans, provides information on the number of VMs included in a failover plan and estimates the amount of data consumed by replica VMs on the target datastore.

- The **Summary** section includes the following elements:
  - The **Failover Plan by State** chart shows statuses of existing failover plans.
  - The **VMs per Failover Plan** chart shows the number of VMs comprised in each failover plan.
- The **Details** table shows VMs included in the failover plans, consumed storage capacity, the specified delay in a VM failover queue and the current plan state.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a list of Veeam Backup & Replication servers to include in the report.

- **Failover plans:** defines a list of failover plans to include in the report.

VM Failover Plan Overview

Description

This report lists all created failover plans with their configuration and added VMs.

Report Parameters

Scope: Backup Infrastructure
Failover plans: All Jobs

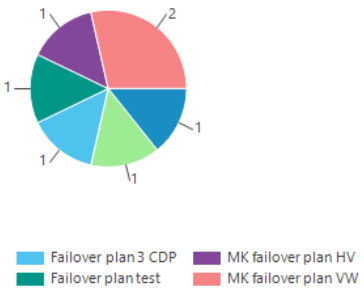
Summary

N. of Failover Plans: 6
Total VMs: 7
Total Data Size: 16.23 GB

Failover Plan by State



VMs per Failover Plan



Details

Backup Server: ms-vbr11a.tech.local

Platform: VMware

Failover Plan	VMs	Size (GB)	Delay (sec)	Created by	Status
⊟MK failover plan HV				TECH\administrator	Ready
	km-ub20 (Replica VM not found)	0.00	60		
Failover Plan	**VMs**	**Size (GB)**	**Delay (sec)**	**Created by**	**Status**
⊟MK failover plan VW				TECH\administrator	Ready
	KM-2012R2-WG (Replica VM not found)	1.68	60		
	mk-1 (Replica VM not found)	0.01	60		
⊟Failover plan test				TECH\administrator	Ready
	iiaut	4.48	60		
⊟Failover plan 3 CDP				TECH\administrator	Ready
	vvg7-centos (Replica VM not found)	0.00	60		

Use Case

The report allows you to keep records of your failover plans for auditing purposes and compliance tests.

VM Performance (Hyper-V)

This report aggregates historical data and shows performance statistics for a selected VM across a time range.

- The **Performance** subsections provide information on CPU, memory, disk and network usage and usage trends for the VM.

Report Parameters

You can specify the following report parameters:

- **Object**: defines the VM to analyze in the report.
- **Period**: defines the time period to analyze in the report. Note that the reporting period must include at least one successfully completed *Object properties data collection* task for the selected VM. Otherwise, the report will contain no data.
- **Business hours only**: defines time of a day for which historical performance data will be used to calculate the performance trend. All data beyond this interval will be excluded from the baseline used for data analysis.

VM Performance

Description

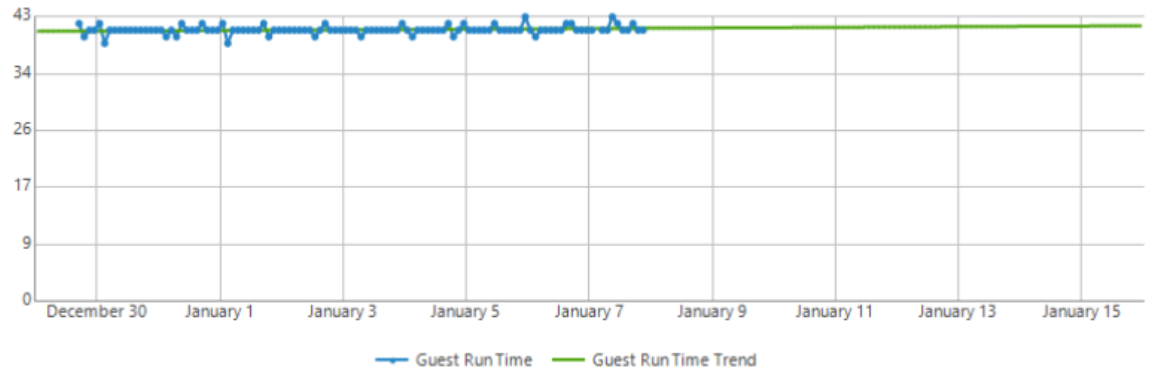
This report shows VMs performance history that includes CPU, Memory, Disk and Network counters.

Report Parameters

Selected object:	dr
Object location:	Virtual Infrastructure\cluster01\hyperv01
Reporting period:	12/29/2018 - 1/15/2019
Business hours:	From 12:00 AM to 11:00 PM

CPU Performance

Guest Run Time (Percent)



Object Name	Average	Minimum	Maximum	Std. Deviation	Trend
dr	41.05	39.00	43.00	0.60	Increasing

Use Case

The report allows you to verify that you have provided enough resources to the virtual machine.

VM Performance (VMware Cloud Director)

This report aggregates historical data and shows performance statistics for a selected VM across a time range.

- The **Performance** subsections show tables and performance charts with CPU, memory, disk and network usage statistics and displays resource usage trends.

Report Parameters

You can specify the following report parameters:

- **Virtual machine**: defines the VM that belongs to your organization and should be analyzed in the report.
- **Period**: defines the time period to analyze in the report.
- **Business hours only**: defines time of a day for which historical performance data will be used to calculate the performance trend. All data beyond this interval will be excluded from the baseline used for data analysis.

VM Performance

Description

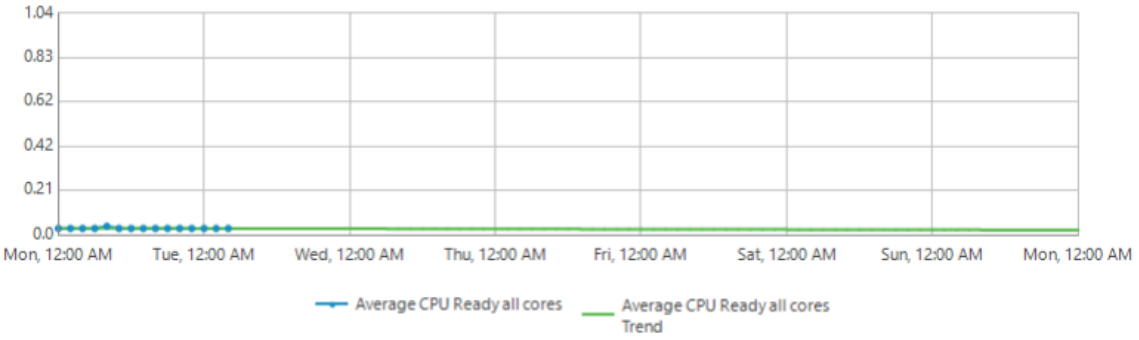
This report shows VM performance history, including CPU, memory, disk and network performance history.

Report Parameters

Virtual machine:	vm02
Virtual machine location:	\\prgclouddirector01.tech.local\organization01\Organization01-VDC\vApp01\vm02
Reporting period:	1/2/2023 - 1/8/2023

CPU Performance

Average CPU Ready All Cores (Percent)



Object Name	Average	Minimum	Maximum	Std. Deviation	Trend
vm02-RqUH	0.03	0.03	0.04	0.00	Decreasing

Use Case

The report allows you to verify that you have provided enough resources to the virtual machine.

VM Performance (vSphere)

This report aggregates historical data and shows performance statistics for a selected VM across a time range.

- The **Navigation** section shows path to the selected object, including VMware vSphere VC, datacenter, cluster and resource pool.

  Click a cluster, host or resource pool name to drill down to performance charts with statistics on CPU, memory, disk and network usage.

- The **Performance** subsections provide information on CPU, memory, disk and network usage and analyzes resource usage trends.

Report Parameters

You can specify the following report parameters:

- **Object**: defines the VM to analyze in the report.
- **Period**: defines the time period to analyze in the report. Note that the reporting period must include at least one successfully completed *Object properties data collection* task for the selected VM. Otherwise, the report will contain no data.
- **Business hours only**: defines time of a day for which historical performance data will be used to calculate the performance trend. All data beyond this interval will be excluded from the baseline used for data analysis.

View Report Example

Use Case

The report allows you to verify that you have provided enough resources to the virtual machine.

VM Performance Chargeback

This report helps to make VM cost audit and identify the most and least expensive VMs based on the VM performance.

The report analyzes VM cost based on hourly, daily or weekly fees for consumed vCPU, vRAM and storage resources. The cost of VM resources is calculated based on VM uptime multipled by the cost of average CPU, memory and storage usage observed during a specified period.

- The **Summary** section includes the following elements:
  - Details on the number of VMs and Business View groups, average VM cost and total cost of VMs.
  - The **Top 10 Most Expensive VMs** subsection shows 10 most expensive VMs in terms of consumed resources, and provides cost of vCPU, vRAM and storage resources utilized by each VM.
  - The **Cost Distribution** chart shows the cost of vCPU, vRAM and storage resources for all VMs included in the report.
  - The **Business View Groups Cost** chart shows the cost of VMs for Business View groups included in the report. This chart is available if you include Business View groups in the report scope.
- The **Details** table provides information on the VM uptime during the reporting period, average vCPU, vRAM and storage usage values, cost of consumed resources, and cost of VMs for the reporting period. Click a VM name to drill down to detailed VM uptime, resource usage and cost statistics for the reporting period.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components (hosts) to analyze in the report.
- **VMware Cloud Director objects**: defines VMware Cloud Director components to analyze in the report.
- **Business View objects**: defines Business View groups to analyze in the report. The parameter options are limited to objects of the Virtual Machine type.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.
- **Currency**: defines a payment currency.
- **Calculate costs for each**: defines a time measurement unit for which prices are set.
- **vCPU cost, per GHz**: defines a cost for each consumed CPU GHz.
- **Memory cost, per GB**: defines a cost for each consumed memory GB.
- **Storage cost, per GB**: defines a cost of each consumed storage GB.
- **Period**: defines a billing period that must be analyzed in the report. This is a period in the past for which historical performance data (CPU, memory and storage utilization metrics) must be analyzed in the report. Note that the reporting period must include at least one successfully completed *Object properties data collection* task for the selected scope. Otherwise, the report will contain no data.

- **Business hours only:** defines time of a day for which historical performance data must be used to calculate the VM cost. Data outside this interval will be excluded from the baseline used for data analysis.

VM Performance Chargeback

Description

This report helps you to perform a VM costs audit and identify the most and least expensive VMs based on the VM performance.

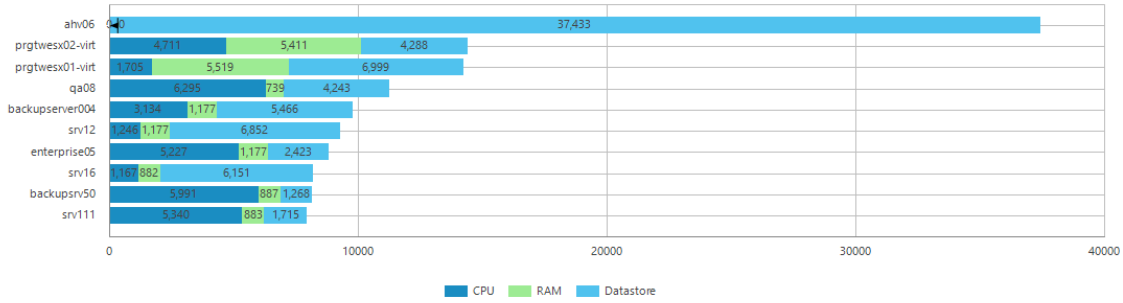
Report Parameters

Scope:	Virtual Infrastructure
vCPU cost, per GHz:	10 USD per hour
Memory cost, per GB:	1 USD per hour
Storage cost, per GB:	0.1 USD per hour
Reporting period:	1 week (12/27/2022 - 1/2/2023)

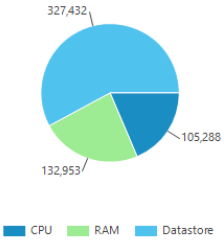
Summary

Number of VMs	230
Average VM price, USD	2,499.66
Total cost of VMs, USD	559,924.11

Top 10 Most Expensive VMs



Cost Distribution



Details

VMware

vCenter Server: vcenter01.tech.local

Host	Virtual Machine	VM Uptime Time	VM Uptime %	CPU Avg. Usage, GHz	CPU Cost, USD	Memory Avg. Usage, GB	Memory Cost, USD	Datastore Avg. Usage, GB	Datastore Cost, USD	VM Cost, USD
Cluster:	**193**			**57.15**	**82,719.43**	**856.59**	**125,174.77**	**18,099.22**	**304,061.83**	**511,956.03**
⊟	1			0.01	0.00	0.01	0.00	0.45	2.41	**2.41**
	apache04_restored		0.00%	0.01	0.00	0.01	0.00	0.45	2.41	**2.41**
⊟ prgtwesx01.tech.local	87			20.44	30,062.94	334.24	49,171.85	8,421.41	141,479.61	**220,714.40**
	backupserver004	6d 3h 7m	99.97%	2.13	3,133.59	8.00	1,176.74	325.35	5,465.88	**9,776.21**
	srv12	6d 3h 7m	99.97%	0.85	1,246.08	8.00	1,176.73	407.86	6,852.06	**9,274.87**
	enterprise05	6d 3h 7m	99.97%	3.55	5,227.06	8.00	1,176.79	144.22	2,422.97	**8,826.81**
	srv16	6d 3h 6m	99.95%	0.79	1,166.50	6.00	882.13	366.14	6,151.18	**8,199.81**
	vcenter01	6d 3h 7m	99.97%	0.53	773.83	18.89	2,778.56	223.70	3,758.21	**7,310.61**
	serv21	6d 3h 7m	99.97%	0.64	938.60	5.85	860.24	324.87	5,457.82	**7,256.67**
	srv14	6d 3h 6m	99.95%	0.50	738.44	6.00	882.51	320.62	5,386.38	**7,007.33**
	serv04_release	6d 3h 7m	99.97%	0.08	110.34	6.00	882.67	354.14	5,949.51	**6,942.51**
	srv13	6d 3h 7m	99.97%	0.85	1,243.14	6.00	882.59	284.45	4,778.80	**6,904.52**
	enterprise03	6d 3h 7m	99.97%	0.18	257.45	4.00	588.28	313.62	5,268.79	**6,114.53**

Hyper-V

SCVMM: N/A

Host	Virtual Machine	VM Uptime		CPU		Memory		Datastore		VM Cost, USD
		Time	%	Avg. Usage, GHz	Cost, USD	Avg. Usage, GB	Cost, USD	Avg. Usage, GB	Cost, USD	
Cluster:	**16**			**12.86**	**18,999.86**	**38.00**	**5,320.60**	**1,276.70**	**21,448.63**	**45,769.08**
⊟ pdctwhv01.tech.local	16			12.86	18,999.86	38.00	5,320.60	1,276.70	21,448.63	**45,769.08**
	qa08	6d 3h 46m	99.85%	4.26	6,295.36	5.00	738.89	252.56	4,243.08	**11,277.33**
	backupsrv50	6d 3h 46m	99.85%	4.05	5,990.93	6.00	886.67	75.50	1,268.47	**8,146.07**
	repo30	6d 3h 46m	99.85%	2.19	3,237.82	2.00	295.56	213.66	3,589.49	**7,122.87**
	backupsrv52	6d 3h 46m	99.85%	1.71	2,522.58	6.00	886.67	84.99	1,427.84	**4,837.08**
	srv24		0.00%	0.00		0.00		198.89	3,341.43	**3,341.43**
	ahvbkpsrv	6d 3h 46m	99.85%	0.41	610.32	6.00	886.67	81.54	1,369.92	**2,866.91**
	qa06	6d 3h 46m	99.85%	0.04	63.54	1.00	148.36	129.66	2,178.29	**2,390.19**
	qa04	6d 3h 46m	99.85%	0.08	112.31	4.00	591.11	42.00	705.67	**1,409.09**
	repo31	6d 3h 46m	99.85%	0.08	121.18	2.00	295.56	35.47	595.94	**1,012.68**
	qa05	6d 3h 46m	99.85%	0.03	45.81	4.00	591.11	19.13	321.37	**958.29**
	ext0230		0.00%	0.00		0.00		45.44	763.42	**763.42**
	qa09		0.00%	0.00		0.00		41.48	696.89	**696.89**
	ext0130		0.00%	0.00		0.00		36.29	609.59	**609.59**
	appsrv02		0.00%	0.00		0.00		20.07	337.12	**337.12**
	appsrv001		0.00%	0.00	0.00	2.00	0.00	0.00	0.07	**0.07**
	appsrv001_ir		0.00%	0.00		0.00		0.00	0.07	**0.07**

Use Case

The report is intended for service providers that have flat fees on consumed virtual infrastructure resources. The report helps calculate the cost of resources that were utilized by each client or application owner for each hour, day or week, and bill the client or application owner according to allocated resources.

IT departments can use this report to calculate the cost of provisioned VMs for application owners and business units, provided that the VM cost model in the organization is based on the amount of resources that a VM consumes.

> **NOTE:**
>
> The cost of storage resources is calculated based on the amount of space occupied by VM files. Business hours do not affect the cost of storage resources. For example, if a VM consumes 100 GB space, and storage price is 0.1 USD per week, the total cost of storage resources for the VM will be 10 USD.
>
> Note that the VM files growth factor can influence the cost of storage resources. The report calculates an average value of consumed storage space on each day of the specified interval. For example, if a VM occupied 50 GB at the beginning of the week, and grew up to 100 GB in the middle of the week, the average amount of occupied space will be 75 GB, and the total cost for the week will be 7.5 USD.

VM Uptime (Hyper-V)

This report analyzes VM uptime statistics to track VM availability.

- The **Top Uptime** and **Lowest Uptime** charts display top 5 VMs in terms of the highest and the lowest uptime values.
- The **vApp Virtual Machine Uptime** table provides the full list of VMs whose uptime values are lower and greater than the specified thresholds.

Report Parameters

You can specify the following report parameters:

- **VMware Cloud Director objects**: defines a list of organizations to analyze in the report.
- **Period**: defines the time period to analyze in the report.
- **Uptime, greater than**: defines the desired minimum uptime value.
- **Uptime, less than**: defines the desired maximum uptime value.
- **Group by**: defines how data will be grouped in the report output (by *Organization*, *Organization VDC*, *Uptime*, *vApp*).

VM Uptime

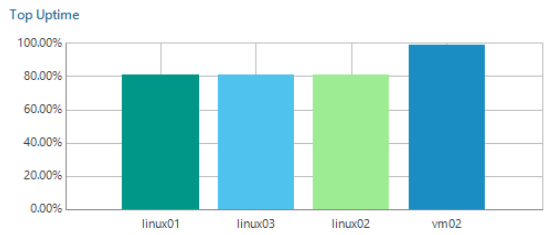
Description

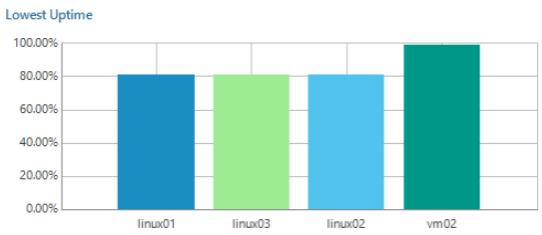
This report provides overview information on VMs uptime, including VMs with lowest and highest uptime values.

Report Parameters

VMware Cloud Director objects:	VMware Cloud Director
Reporting period:	Past month (12/1/2022 - 12/31/2022)
Uptime:	greater than 80.00% and lower than 100.00%
Group by:	vApp

Summary





vApp Virtual Machine Uptime

Organization	Virtual Datacenter	vApp	VM Name	Number of Restarts	Number of Alarms	Downtime	Sum of Uptime (%)
vApp: vApp02							**80.87%**
organization02	Organization02-VDC	vApp02	linux03	1	1	1 day(s) 16:05:00	80.73%
organization02	Organization02-VDC	vApp02	linux02	1	2	1 day(s) 15:29:00	81.02%
vApp: vApp01							**99.05%**
organization01	Organization01-VDC	vApp01	vm02	0	2	00:24:00	99.05%
vApp: vApp01							**80.69%**
organization02	Organization02-VDC	vApp01	linux01	1	1	1 day(s) 16:10:00	80.69%

Use Case

Uptime is a measure of time a VM has been up and actively running on a host. When a VM is not operating, cloud space allocated to it is not being used productively. Use this report to track uptime of virtualized workloads.

VM Uptime (VMware Cloud Director)

This report analyzes VM uptime statistics to track VM uptime.

- The **Summary** section includes the following elements:
  - The **Top Uptime** and **Lowest Uptime** charts display top 5 VMs in terms of the highest and the lowest uptime values.
  - The **Uptime Distribution** chart displays the number of VMs with different uptime values.
- The **Virtual Machine Uptime** table provides the full list of VMs whose uptime values are lower and greater than the specified thresholds.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **Business View objects**: defines Business View groups to analyze in the report. The parameter options are limited to objects of the Virtual Machine type.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.
- **Period**: defines the time period to analyze in the report. Note that the reporting period must include at least one successfully completed *Object properties data collection* task for the selected scope. Otherwise, the report will contain no data.
- **Uptime, greater than**: defines the desired minimum uptime value.

- **Uptime, less than**: defines the desired maximum uptime value.

VM Uptime

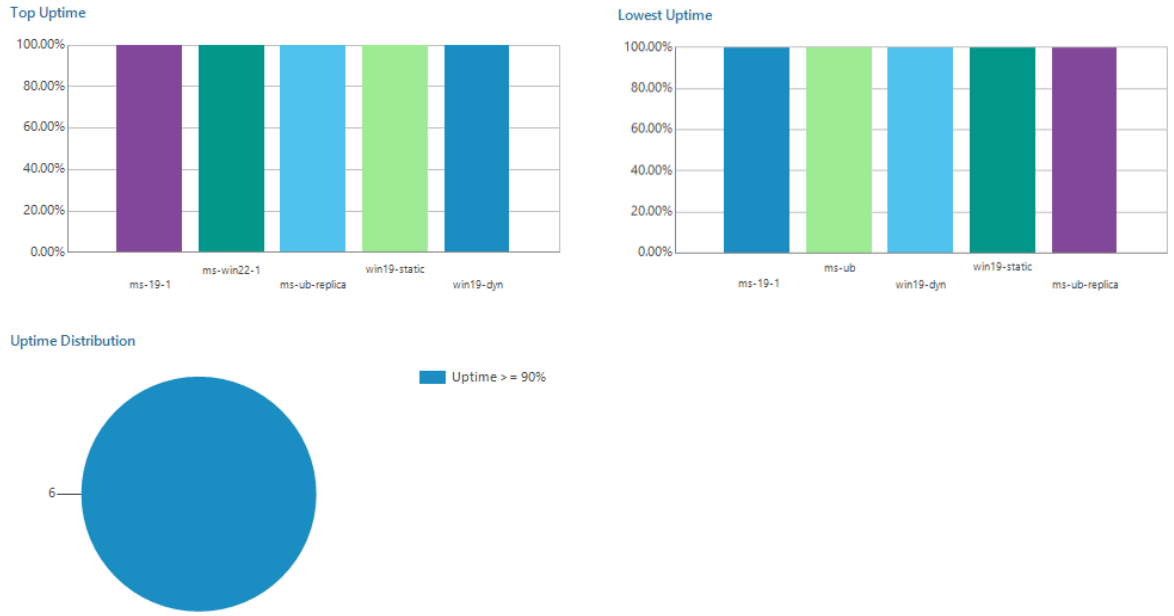
Description

This report provides an overview of VM uptime including VMs with lowest and highest uptime values.

Report Parameters

Scope:	Virtual Infrastructure
Reporting period:	Past month (11/1/2022 - 11/30/2022)
Uptime:	Greater than or equal to 80.00% and lower than or equal to 100.00%
Business View objects:	

Summary



Virtual Machine Uptime

Cluster	Host	VM Name	Number of Restarts	Number of Alarms	Downtime	Uptime (%)
Uptime: Uptime >= 90%						
ms-22-cluster.tech.local	ms-node-01	ms-19-1	0	3	01:25:45	99.56%
ms-22-cluster.tech.local	ms-node-01	ms-ub	0	2	01:25:45	99.56%
ms-22-cluster.tech.local	ms-node-02	ms-ub-replica	0	1	01:25:43	99.56%
ms-22-cluster.tech.local	ms-node-02	ms-win22-1	0	3	01:25:43	99.56%
ms-22-cluster.tech.local	ms-node-02	win19-dyn	0	3	01:25:43	99.56%
ms-22-cluster.tech.local	ms-node-02	win19-static	0	1	01:25:43	99.56%

Use Case

Uptime is a measure of time a VM has been up and actively running on a host. When a VM is not operating, storage space allocated to it is not being used productively. Use this report to track uptime of virtualized workloads.

VM Uptime (vSphere)

This report analyzes VM uptime statistics to track VM availability.

- The **Summary** section includes the following elements:
  - The **Top Uptime** and **Lowest Uptime** charts display top 5 VMs in terms of the highest and the lowest uptime values.
  - The **Uptime Distribution** chart displays the number of VMs with different uptime values.
- The **Virtual Machine Uptime** table provides the full list of VMs whose uptime values are lower and greater than the specified thresholds.

  Click a VM name to drill down to detailed information on triggered alarms and virtual machine restart events over a specified reporting period.

> **NOTE:**
>
> The **Number of Restarts** column shows the number of VM restarts from the VMware vSphere Client only.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **Business View objects**: defines Business View groups to analyze in the report. The parameter options are limited to objects of the Virtual Machine type.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.
- **Period**: defines the time period to analyze in the report. Note that the reporting period must include at least one successfully completed *Object properties data collection* task for the selected scope. Otherwise, the report will contain no data.
- **Business hours only**: defines time of a day for which historical performance data will be used to calculate the performance trend. All data beyond this interval will be excluded from the baseline used for data analysis.
- **Uptime, greater than**: defines the desired minimum uptime value.
- **Uptime, less than**: defines the desired maximum uptime value.
- **Group by**: defines how data will be grouped in the report output (by *Uptime*, *Datacenter*, *Cluster* or *Host*).

View Report Example

Use Case

Uptime is a measure of time a VM has been up and actively running on a host. When a VM is not operating, storage space allocated to it is not being used productively. Used this report to track uptime of virtualized workloads.

VMs Backed Up by Multiple Jobs

This report analyzes configuration of backup jobs to find VMs that are simultaneously included in several jobs. This helps you reduce backup windows and optimize backup infrastructure operation.

- The **Summary** display includes the following elements:
  - The **VMs with Largest Avg. Transferred Data (GB)** chart shows top 5 VMs with the largest amount of transferred backup data.
  - The **VMs with Largest Processing Time (Minutes)** chart shows top 5 VMs with the longest time interval required to produce a VM backup.
- The **Report Data** table provides information on the list of backup servers, backup jobs in which the VM is included, job schedules, target repository names, the average processing time, average VM transferred data (in GB), the number of restore points created for the VM, full backups and the last time the jobs ran.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a list of Veeam Backup & Replication servers to include in the report.
- **Business View objects**: defines Business View groups to analyze in the report. The parameter options are limited to objects of the Virtual Machine type.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.
- **Exclude jobs**: defines a list of backup and replication jobs to exclude from the report.

View Report Example

Use Case

The reason why some VMs may appear to be backed up by several jobs at a time can be a lack of coordination between several backup operators or the capability to include logical containers (vApps, resource pools, folders) in backup jobs. Both issues can cause repositories to run out of free space due to excessive duplicated backup files.

The report allows you to assess efficiency of the backup process and decide whether to reconfigure existing backup jobs so that they utilize fewer resources and complete in narrower intervals. This report ensures that all critical VMs are reliably protected while no redundant jobs exist across the backup environment.

VMs Configuration (Hyper-V)

This report documents the current configuration of VMs in the virtual infrastructure.

- The **Summary** section includes the following elements:
  - The **Integration Services Status** chart illustrates the status of Integration Services running on VMs.

    Click the **Details** link at the bottom of the chart to drill down to the list of VMs and statuses of Integration Services running on these VMs.
  - The **VM State Summary** chart illustrates the VM power state.

    Click the **Details** link at the bottom of the chart to drill down to the list of VMs and their power states.
  - The **Guest OS Distribution** chart illustrates what guest OSes are installed on VMs, and shows the share of a particular guest OS.

    Click the **Details** link at the bottom of the chart to drill down to the list of guest OSes present in the infrastructure and the list of VMs on which these guest OSes are installed.
- The **Details** table provides detailed information for every VM, including data on VM location, computer name, guest OS type, number of vCPUs, memory type, amount of allocated memory resources, amount of allocated and used storage resources.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.

- **Business View objects**: defines Business View groups to analyze in the report. The parameter options are limited to objects of the Virtual Machine type.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.

VMs Configuration

Description

This report provides a quick overview of all configured resources for virtual machines in terms of memory, CPU and virtual disk resources as well as VM state and Guest OS distribution summary.

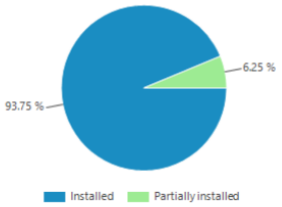
Report Parameters

Scope: Virtual Infrastructure

Business View objects:

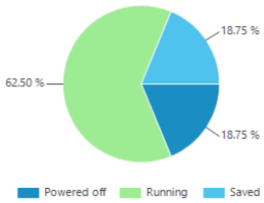
Summary

Integration Services Status



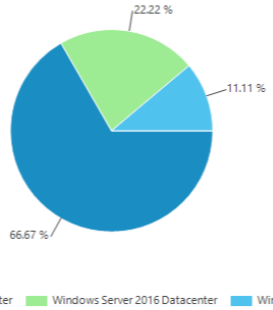
Details

VM State Summary



Details

Guest OS Distribution



Details

Details

SCVMM: N/A

Host	VM Name	Computer Name	Guest OS	vCPU	Memory Type	Startup Memory (MB)	Minimum Memory (MB)	Maximum Memory (MB)	Storage Allocated (GB)	Storage Used (GB)
⊟Cluster: N/A				**37**		**58,368**	**3,076**	**2,103,296**	**1,900.00**	**1,278.63**
⊟pdctwhv01.tech.local				37		58,368	3,076	2,103,296	1,900.00	1,278.63
	ahvbkpsrv	ahvbkpsrv.tech.local	Windows Server 2016 Standard	4	Static	6,144			130.00	81.79
	appsrv001			1	Dynamic	2,048	512	1,048,576	20.00	0.00
	appsrv001_ir			1	Dynamic	2,048	512	1,048,576	20.00	0.00
	appsrv02			1	Static	4,096			50.00	20.07
	backupsrv50	backupsrv50.tech.local	Windows Server 2016 Datacenter	4	Static	6,144			130.00	75.50
	backupsrv52	backupsrv52.tech.local	Windows Server 2016 Datacenter	4	Static	6,144			130.00	85.66
	ext0130			2	Static	2,048			60.00	36.29
	ext0230			2	Static	2,048			60.00	45.44
	qa04	qa04.tech.local	Windows Server 2012 R2 Datacenter	2	Static	4,096			130.00	42.00
	qa05	qa05.tech.local	Windows Server 2012 R2 Datacenter	2	Static	4,096			130.00	19.13
	qa06	qa06.tech.local	Windows Server 2012 R2 Datacenter	2	Dynamic	3,072	1,028	3,072	130.00	129.66
	qa08	qa08.tech.local	Windows Server 2012 R2 Datacenter	4	Static	5,120			130.00	253.59
	qa09			2	Dynamic	1,024	1,024	3,072	130.00	41.48
	repo30	repo30.tech.local	Windows Server 2012 R2 Datacenter	2	Static	2,048			250.00	213.66
	repo31	repo31.tech.local	Windows Server 2012 R2 Datacenter	2	Static	2,048			250.00	35.47
	srv24			2	Static	6,144			150.00	198.89

Use Case

The report helps administrators assess configuration properties of VMs in the monitored virtual infrastructure.

VMs Configuration (vSphere)

This report documents the current configuration of VMs in the virtual infrastructure.

- The **Summary** section includes the following elements:
  - The **Guest OS Distribution** chart illustrates what guest OSes are installed on VMs, and shows the share of a particular guest OS.

    Click the **Details** link at the bottom of the chart to drill down to the list of guest OSes present in the infrastructure and the list of VMs on which these guest OSes are installed.
  - The **Tools Status** chart illustrates the status of VMware Tools on VMs.

    Click the **Details** link at the bottom of the chart to drill down to the list of VMs and statuses of VMware Tools running on these VMs.
  - The **VM State Summary** chart illustrates the VM power state.

    Click the **Details** link at the bottom of the chart to drill down to the list of VMs and their power states.
- The **Details** table provides information for every VM, including data on VM location, computer name, guest OS type, number of vCPUs, amount of allocated memory resources, amount of allocated and used storage resources.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **Business View objects**: defines Business View groups to analyze in the report. The parameter options are limited to objects of the Virtual Machine type.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.

View Report Example

Use Case

The report helps administrators assess configuration properties of VMs in the monitored virtual infrastructure.

VMs Growth (Hyper-V)

This report tracks how the number of VMs in your virtual environment has been changing during the reporting period. The report analyzes the amount of allocated resources, displays changes in the number of VMs, and shows how these changes influenced resource provisioning in the infrastructure.

- The **Summary** section provides information on the total number of VMs, number of added and removed VMs, allocated vCPU, memory and storage resources, allocation ratios and VMs growth during the reporting period.
- The **Added VMs Details** table provides information on each added VM, including VM location, name, number of vCPUs, allocated memory and storage resources, initiator and the date and time when the VM was added.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **Business View objects**: defines Business View groups to analyze in the report. The parameter options are limited to objects of the Virtual Machine type.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.

- **Period**: defines the time period to analyze in the report. Note that the reporting period must include at least one successfully completed *Object properties data collection* task for the selected scope. Otherwise, the report will contain no data.

VMs Growth

Description

This report shows how many VMs have been added to the virtual environment during the selected period of time.

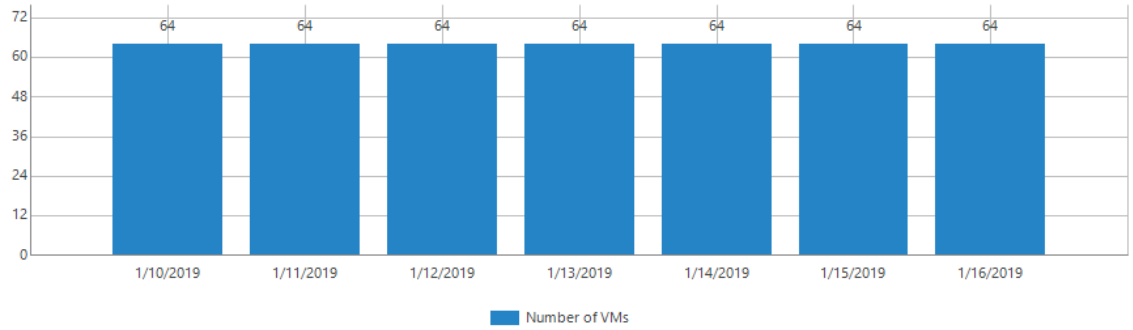
Report Parameters

Scope:	Virtual Infrastructure
Interval:	1 week (1/10/2019 - 1/16/2019)
Business View objects:	

Summary

Number of VMs		Allocated Resources		Ratios	
Total number of VMs:	64	vCPU:	89	vCPU/Core:	3.71
VMs added:	2	Memory:	26,654.00 GB	VMs per host:	32.00
VMs removed:	0	Storage:	11,482.00 GB	VMs per datastore:	10.67

VMs Growth



Added VMs Details

SCVMM: N/A

Cluster/Host: cluster01

Number of VMs: 64

Added VMs	vCPU	Memory (GB)	Storage (GB)	Initiator	Event Date
2	3	5.00	35.72		
TM02	2	4.00	35.72	tech\john.smith	1/14/2019 5:02 PM
TM01	1	1.00	0.00	tech\john.smith	1/15/2019 12:06 AM

Use Case

This report allows you to control virtual machine sprawl and to optimize resource utilization in your infrastructure.

VMs Growth (vSphere)

This report tracks how the number of VMs in your virtual environment has been changing during the reporting period. The report analyzes the amount of allocated resources, displays changes in the number of VMs, and shows how these changes influenced resource provisioning in the infrastructure.

- The **Summary** section provides information on the total number of VMs, number of added and removed VMs, allocated vCPU, memory and storage resources, allocation ratios and VMs growth during the reporting period.
- The **Added VMs Details** table provides information on each added VM, including VM location, name, number of vCPUs, allocated memory and storage resources, initiator and the date and time when the VM was added.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **Business View objects**: defines Business View groups to analyze in the report. The parameter options are limited to objects of the Virtual Machine type.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.
- **Period**: defines the time period to analyze in the report. Note that the reporting period must include at least one successfully completed *Object properties data collection* task for the selected scope. Otherwise, the report will contain no data.

View Report Example

Use Case

This report allows you to control virtual machine sprawl and to optimize resource utilization in your infrastructure.

VMs with no Archive Copy

The main backup purpose is to protect your data against disasters and VM failures. Having only one copy of a backup file does not provide the necessary level of safety. To build a successful data protection and disaster recovery plan, you must have at least three copies of your data, for example, production data, backup and its copy, and two different types of media to store copies of your data, for example, disk storage and tape.

To learn more about the 3-2-1 backup strategy, see the Veeam Blog article How to follow the 3-2-1 backup rule with Veeam Backup & Replication.

This report analyzes your backup infrastructure to find VMs that do not have backup copies stored on secondary backup repositories or on tapes.

- The **Summary** section includes the following elements:
  - The **VMs by Archive Status** chart shows the number of VMs with 1 or 2 archived copies.
  - The **VMs per Backup Location** chart shows the repositories where backups are stored.
- The **Details** table shows properties of each protected VMs and provides details on the location of a primary and secondary VM copy, availability of tape backups for the listed VMs and the date of the most recent VM backup.

Report Parameters

You can specify the following report parameters:

- **Protected infrastructure**: defines the platform to analyze in the report.
- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **VM folders**: defines a list of VMware folders to include in the report (applies to VMware vSphere environments only). VM folders is an alternate way to present the virtual infrastructure. If VMs in your infrastructure are grouped into folders according to their profile, you can limit the report scope by specifying the necessary folders only.
- **Business View objects**: defines Business View groups to analyze in the report. The parameter options are limited to objects of the Virtual Machine type.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.
- **VMware Cloud Director objects**: defines VMware Cloud Director components to analyze in the report.
- **Interval**: defines the time period to analyze in the report based on the last backup date of the virtual machine.
- **VM exclusion rule**: defines a list of VMs that should be excluded from the report scope. You can enter VM names explicitly or create a wildcard mask by using the asterisk (*) to replace any number of characters. Multiple entries are separated by semicolon. Usage example: the following string will exclude machines with the _R&D suffix from appearing in the report: *_R&D.

View Report Example

Use Case

This report helps backup administrators check whether mission critical VMs are protected with backup copies stored on secondary backup repositories and on tape.

vSphere Custom Performance

This report allows you to define specific CPU, memory, network and disk metrics to analyze performance of vSphere hosts, datastores and VMs.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **VMware Cloud Director objects**: defines VMware Cloud Director Infrastructure levels to analyze in the report.
- **Business View objects**: defines Business View groups to analyze in the report.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.
- **Period**: defines the time period to analyze in the report. Note that the reporting period must include at least one successfully completed *Object properties data collection* task for the selected scope. Otherwise, the report will contain no data.
- **Business hours from - to**: defines time of a day for which historical performance data will be used to calculate the performance trend. All data beyond this interval will be excluded from the baseline used for data analysis.
- **Object type**: defines the infrastructure object to analyze in the report.
- **Measured entities**: defines subsystems to analyze in the report (*CPU*, *Memory*, *Network*, *Disk*, *Storage Adapter*, *Storage Path*, *Datastore*, *Power* or *Guest Disk*). The list of available subsystems will depend on the selected object type.
- **Metrics**: defines metrics to analyze in the report. The list of available metrics will depend on the selected monitor subsystem.
- **Inclusion rule/Exclusion rule**: defines a list of objects that should be included in/excluded from the report scope:
  - Use the **Inclusion rule** option to define names of virtual infrastructure objects that should be included in the report. All objects not specified in the **Inclusion rule** field will be excluded from the baseline used for data analysis.
  - Use the **Exclusion rule** option to define names of virtual infrastructure objects that should be excluded from the report. All objects not specified in the **Exclusion rule** field will be included in the baseline used for data analysis.

NOTE:

The **Inclusion rule/Exclusion rule** parameters support wildcards. Search is not case sensitive.

To illustrate how to use wildcard queries, consider the following example. You have selected 4 hosts as a report scope: 2 NAS servers (*NASserv1*, *NASserv2*) and 2 Active Directory servers (*AD01* and *AD02*).

If you want the report to show performance details only for the NAS servers, type *nasserv** in the **Inclusion rule** field. Alternatively, type *ad** in the **Exclusion rule** field.

- **Top N**: defines the maximum number of VMs to display in the report.

- **Show graphs:** defines whether to show charts in the report output.

vSphere Custom Performance

Description

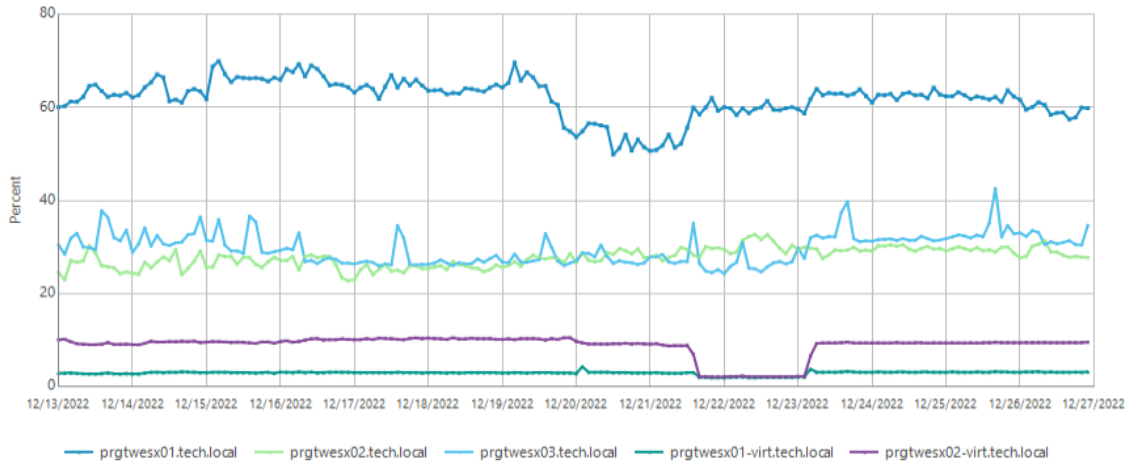
This report allows you to define specific metrics to analyze performance of vSphere infrastructure elements.

Report Parameters

Selected object:	Virtual Infrastructure
Report creation date:	12/26/2022 11:35 PM
Report period:	2 weeks (12/13/2022 - 12/26/2022)
Object type:	Hosts
Exclusion rule	
Inclusion rule:	*
Business View objects:	
Top N:	All Items
CPU:	CPU Usage (Percent), CPU Usage (Absolute) (MHz)
Memory:	Memory Usage (Percent)

CPU

CPU Usage (Percent)



Virtual Server	Object Name	Average	Maximum	Minimum	Std. Deviation	Trend
vcenter01.tech.local						
	prgtwesx01.tech.local	61.92	70.00	49.92	4.14	Decreasing
	prgtwesx03.tech.local	29.71	42.57	24.28	3.28	Increasing
	prgtwesx02.tech.local	27.80	32.72	22.75	2.04	Increasing
	prgtwesx02-virt.tech.local	8.81	10.50	2.07	2.38	Decreasing
	prgtwesx01-virt.tech.local	2.95	4.29	1.99	0.35	Decreasing

Use Case

Use this report to investigate specific performance issues in the environment.

vSphere Raw Performance Data

This report allows you to get detailed raw data on specific CPU, memory, network, storage and disk metrics to analyze performance of VMware hosts, VMs and datastores.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a virtual infrastructure level and its sub-components to analyze in the report.
- **Business View objects**: defines Business View groups to analyze in the report.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.
- **Period**: defines the time period to analyze in the report. Note that the reporting period must include at least one successfully completed *Object properties data collection* task for the selected scope. Otherwise, the report will contain no data.
- **Sample size**: defines the resolution level, that is, granularity of raw data that should be displayed in the report output. Note that data with the Raw sample length (5-minute resolution) is available only for the custom interval of last week; if you select Year/Quarter/Month as a reporting interval, the report will show data with 2-hour resolution.
- **Object type**: defines the infrastructure object to analyze in the report.
- **Measured Entities**: defines subsystems to analyze in the report (*CPU*, *Memory*, *Network*, *Storage Adapter*, *Storage Path*, *Datastore* or *Power*). The list of available subsystems will depend on the selected object type.
- **Metrics**: the performance metrics to analyze in the report. The choice of available metrics will depend on the selected monitored subsystems.
- **Inclusion rule/Exclusion rule**: defines a list of objects that should be included in/excluded from the report scope:
  - Use the **Inclusion rule** option to define names of virtual infrastructure objects that should be included in the report. All objects not specified in the **Inclusion rule** field will be excluded from the baseline used for data analysis.
  - Use the **Exclusion rule** option to define names of virtual infrastructure objects that should be excluded from the report. All objects not specified in the **Exclusion rule** field will be included in the baseline used for data analysis.

> **NOTE:**
>
> The **Inclusion rule/Exclusion rule** parameters support wildcards. Search is not case sensitive.
>
> To illustrate how to use wildcard queries, consider the following example. You have selected 4 hosts as a report scope: 2 NAS servers (*NASserv1*, *NASserv2*) and 2 Active Directory servers (*AD01* and *AD02*).
>
> If you want the report to show performance details only for the NAS servers, type *nasserv** in the **Inclusion rule** field. Alternatively, type *ad** in the **Exclusion rule** field.

vSphere Raw Performance Data

Description

This report allows you to get detailed raw data on specific metrics to analyze performance of vSphere infrastructure elements.

Report Parameters

Selected object:	Virtual Infrastructure
Report creation date:	12/26/2022 11:41 PM
Report period:	12/19/2022 - 12/25/2022
Object type:	Hosts
Exclusion rule:	
Inclusion rule:	*
Business View objects:	
Sample size:	Raw
CPU:	CPU Usage (Percent), CPU Usage (Absolute) (MHz)

Subsystem: CPU

Counter: CPU Usage

Object Name	Value (Percent)	Time
prgtwesx01.tech.local	59.63	12/26/2022 2:00 AM
prgtwesx01.tech.local	60.34	12/26/2022 4:00 AM
prgtwesx01.tech.local	60.86	12/26/2022 6:00 AM
prgtwesx01.tech.local	60.63	12/26/2022 8:00 AM
prgtwesx01.tech.local	58.63	12/26/2022 10:00 AM
prgtwesx01.tech.local	58.96	12/26/2022 12:00 PM
prgtwesx01.tech.local	58.79	12/26/2022 2:00 PM
prgtwesx01.tech.local	57.50	12/26/2022 4:00 PM
prgtwesx01.tech.local	57.83	12/26/2022 6:00 PM
prgtwesx01.tech.local	59.83	12/26/2022 8:00 PM
prgtwesx01.tech.local	59.94	12/26/2022 10:00 PM
prgtwesx01.tech.local	58.79	12/27/2022 12:00 AM
Max Observed:	**60.86**	**12/26/2022 6:00 AM**
Min Observed:	**57.50**	**12/26/2022 4:00 PM**
Average:	**59.31**	**12/26/2022 2:00 AM - 12/27/2022 12:00 AM**

Object Name	Value (Percent)	Time
prgtwesx02.tech.local	28.27	12/26/2022 2:00 AM
prgtwesx02.tech.local	30.11	12/26/2022 4:00 AM
prgtwesx02.tech.local	30.51	12/26/2022 6:00 AM
prgtwesx02.tech.local	31.22	12/26/2022 8:00 AM
prgtwesx02.tech.local	29.23	12/26/2022 10:00 AM
prgtwesx02.tech.local	28.93	12/26/2022 12:00 PM
prgtwesx02.tech.local	28.11	12/26/2022 2:00 PM
prgtwesx02.tech.local	27.77	12/26/2022 4:00 PM
prgtwesx02.tech.local	28.10	12/26/2022 6:00 PM
prgtwesx02.tech.local	27.92	12/26/2022 8:00 PM
prgtwesx02.tech.local	27.63	12/26/2022 10:00 PM
prgtwesx02.tech.local	28.50	12/27/2022 12:00 AM
Max Observed:	**31.22**	**12/26/2022 8:00 AM**
Min Observed:	**27.63**	**12/26/2022 10:00 PM**
Average:	**28.86**	**12/26/2022 2:00 AM - 12/27/2022 12:00 AM**

Use Case

This report provides advanced historical performance data that you can export to a spreadsheet application and use for analysis and reporting purposes.

Windows Cluster Shared Volume Performance

This report aggregates historical data and shows performance statistics for a selected Windows 2012+ Server Cluster Shared Volume across a time range.

- The **Performance** subsections provide information on read/write rates, read/write operations completed in the direct/redirected access mode, read/write latency, IOPS, top 3 resource consuming VMs and usage trends for the CSV.

  Click a VM name in the list of top 3 resource consuming VMs to drill down to performance charts with statistics on CPU, memory, disk and network usage for the VM.

Report Parameters

You can specify the following report parameters:

- **Object**: defines the Windows 2012+ Server CSV to analyze in the report.
- **Period**: defines the time period to analyze in the report. Note that the reporting period must include at least one successfully completed *Object properties data collection* task for the selected CSV. Otherwise, the report will contain no data.

- **Business hours only**: defines time of a day for which historical performance data will be used to calculate the performance trend. All data beyond this interval will be excluded from the baseline used for data analysis.

Windows Cluster Shared Volume Performance

Description

This report shows datastore performance history that includes Usage, Latency and IOPS counters.

Report Parameters

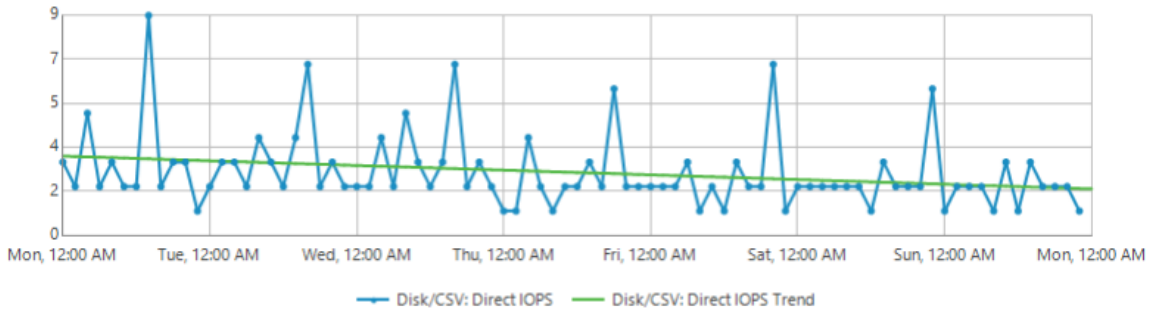
Selected object:	C:\ClusterStorage\CSV
Object location:	Virtual Infrastructure\ms-22-cluster.tech.local
Reporting period:	12/19/2022 - 12/25/2022

Summary

Name:	C:\ClusterStorage\CSV
Type:	CSV
Capacity:	999.6GB
Free Space:	678.1GB
Virtual Machines:	20

Datastore IOPs

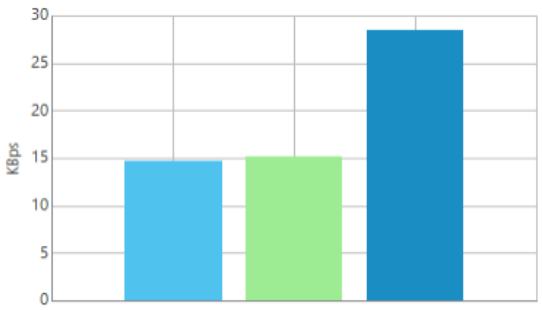
Disk/CSV: Direct IOPS (Number)



Object Name	Average	Minimum	Maximum	Std. Deviation	Trend
C:\ClusterStorage\CSV	2.58	1.00	9.00	1.51	Decreasing

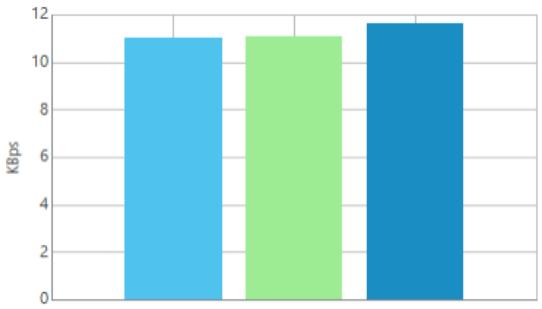
Datastore Usage

Top 3 VMs by Virtual Storage Read KBytes/Sec



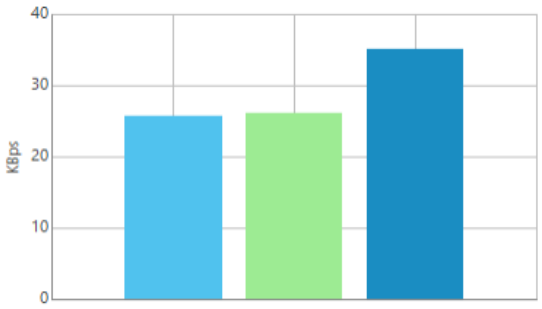
Object Name	Avg	Trend
win19-static-mem	28.56	Decreasing
win19-dyn-mem	15.09	Decreasing
ms-19-test-1	14.64	Decreasing

Top 3 VMs by Virtual Storage Write KBytes/Sec



Object Name	Avg	Trend
ms-win22-test-1	11.64	Increasing
ms-19-test-1	11.08	Decreasing
win19-dyn-mem	11.03	Increasing

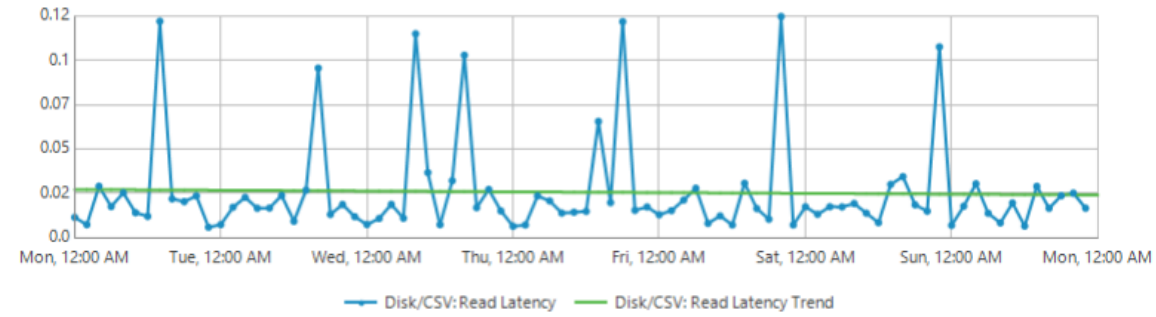
Top 3 VMs by Virtual Storage Total KBytes/Sec



Object Name	Avg	Trend
win19-static-mem	35.18	Decreasing
win19-dyn-mem	26.13	Increasing
ms-19-test-1	25.72	Decreasing

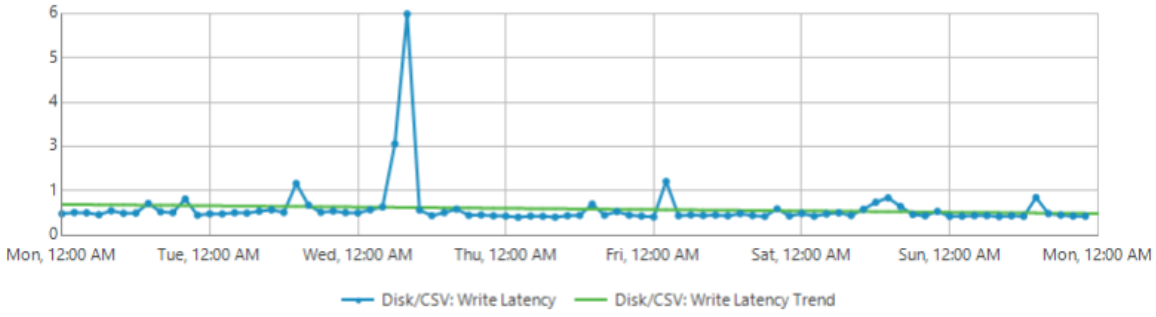
Latency

Disk/CSV: Read Latency (Millisecond)



Object Name	Average	Minimum	Maximum	Std. Deviation	Trend
C:\ClusterStorage\CSV	0.03	0.01	0.12	0.03	Decreasing

Disk/CSV: Write Latency (Millisecond)



Object Name	Average	Minimum	Maximum	Std. Deviation	Trend
C:\ClusterStorage\CSV	0.75	0.51	6.29	0.67	Decreasing

Use Case

The report assesses latency and IOPS values to identify Windows 2012+ Server Cluster Shared Volumes with performance issues.

Workload Protection History

This report provides historical information on workloads data protection.

- The **Summary** display includes the following elements:
  - The **Success and Failure Rates History** chart displays the amount of successful and failed resulting job sessions during the reporting period. A resulting job session is the last session started for a job on each day of the reporting period.
  - The **Success and Failure Rates History** table provides information on each day of the reporting period, including number of processed unique workloads, total number of sessions, number of resulting sessions finished successfully, finished with warning and finished with errors, number of running sessions and the percentage of resulting sessions finished successfully and finished with errors.
- The **Report Data** display provides information on each backup job based on the selected properties.

  Veeam Cloud Connect service providers cannot see performance data for proxies used by tenant data protection jobs.

Report Parameters

You can specify the following report parameters:

- **Infrastructure objects**: defines a list of Veeam Backup & Replication servers to include in the report.
- **Business View objects**: defines a list of Business View objects to include in the report.

  Business View groups from the same category are joined using Boolean OR operator, Business View groups from different categories are joined using Boolean AND operator. That is, if you select groups from the same category, the report will contain all objects that are included in groups. However, if you select groups from different categories, the report will contain only objects that are included in all selected groups.
- **Workload types**: defines a list of backup infrastructure objects to include in the report (*VM*, *Computer*, *Unstructured Data, Enterprise Application*).
- **Job types**: defines a list of job types to evaluate in the report (*VM backup*, *Replication*, *File to tape*, *Backup to tape*, *Backup copy*, *SQL log backup*, *Oracle log backup*, *Agent backup policy*, *Agent backup*, *File backup*, *Nutanix AHV backup*, *Application backup policy*, *PostgreSQL log backup*, *Cloud Director backup*, *Cloud Director replication*, *SOBR sessions*: *Offload (copy policy)*, *Offload (move policy)*, *Download*, *Archiving*, *Retrieval, Object to tape backup, Object storage backup*).
- **Jobs**: defines a list of jobs to include in the report.
- **Job statuses**: defines a backup job status to analyze in the report (*Success*, *Failed*, *Warning*, *Running*).
- **Job inclusion rule**: defines a job to include in the report. You can enter job name explicitly or create a wildcard mask by using the asterisk (*) to replace any number of characters. Multiple entries are separated by comma.
- **Period**: defines the time period to analyze in the report.

NOTE:
- Infrastructure topology view in Veeam ONE and Veeam Backup & Replication must match. Otherwise, you will not be able to generate the report based on **Business View objects**.
- Veeam ONE Web Client displays file backup copy jobs together with other backup copy jobs.

View Report Example

Use Case

This report provides historical information on backup sessions for workloads in your backup infrastructure.

Deployment Projects

Veeam ONE Web Client deployment projects allow you to predict future resource utilization and plan resource reservations in your virtual environment.

With deployment projects, you can run complex simulation tasks to predict the effects of:

- Adding or evicting hosts in a cluster
- Adding new VMs or decommissioning existing VMs

Deployment projects compare the projected resource capacities against the future resource demand, help identify potential resource shortages and provide practical recommendations that an administrator should undertake to succeed with the actual deployment.

For example, you can simulate how many VMs similar to an existing Microsoft SQL Server can be added in a cluster without the risk of causing resource contention or degraded cluster performance. Deployment projects can be helpful in assessing various hardware replacement scenarios or forecasting the amount of compute and storage resources that need to be provisioned.

> **NOTE:**
>
> Deployment projects are not available in Veeam ONE Community edition.

Deployment Projects and Scenarios

Every deployment project includes a specific simulation scenario. A simulation scenario describes what amount of resources must be added to or evicted from the managed environment.

In simulation scenarios, you can:

- Select an existing host or a VM and use it as a baseline model to calculate the effects of adding or evicting resources
- Explicitly specify host or VM configuration

Simulation scenarios can be targeted at a host or cluster, termed *container* — a recipient node that will undergo the capacity changes and whose future performance and resource utilization will be assessed.

Condition for Acceptance

The deployment project is considered successful if future resource utilization and performance metrics do not breach the designated thresholds that define the maximum tolerable resource load. The thresholds are preset and can be customized if necessary.

Tentatively successful projects (projects completed with warnings) will cause the metrics to breach the thresholds but stay beyond 100 percent of resource utilization (for example, memory usage exceeding a 90 percent threshold but being less than 100 percent).

Calculation Background

Resource availability and performance modelling is based on comparing future demand for resources against the projected resource capacity. The following factors are used in the analysis:

- Current compute capacities

- Additional capacities introduced through adding new hosts or evicting VMs
- Withdrawn compute capacities through evicting hosts
- Extra capacities required to run new VMs

The following algorithms are employed to forecast workloads:

- When a new VM is added, it is assumed that the VM will use all its provisioned resources.
- When an existing VM is selected as a baseline model, Veeam ONE will use the average value of the VM resource consumption during the current week.
- When calculating the amount of free space, Veeam ONE verifies that there is sufficient storage capacity for all virtual disks of the VM.

Deployment Project Interdependencies

You can create several simulation scenarios that describe complex conditions, such as introducing new and decommissioning existing hosts or VMs in the same container, at the same time. You can also create deployment scenarios with overlapping due dates.

When you create a new deployment project or make changes in the existing deployment project, Veeam ONE checks if there is any overlapping project. If there are changes that may affect the concurrent project, Veeam ONE Web Client will prompt you to recalculate the overlapping projects.

Getting Started with Deployment Projects

A typical workflow for creating a deployment project includes the following steps:

1. Check the effective thresholds and modify their values if necessary.
2. Create a new deployment project, specify its settings and add simulation scenarios.
3. Calculate the deployment project to run a simulation.
4. Create a report to examine results.
5. Complete the project after the actual resources have been added or evicted.

Creating Deployment Projects

To create a new deployment project, perform the following steps:

1. Launch Add Deployment Project Wizard
2. Specify Deployment Project Name and Description
3. Specify Deployment Infrastructure
4. Define Project Scenarios

Step 1. Launch Add Deployment Project Wizard

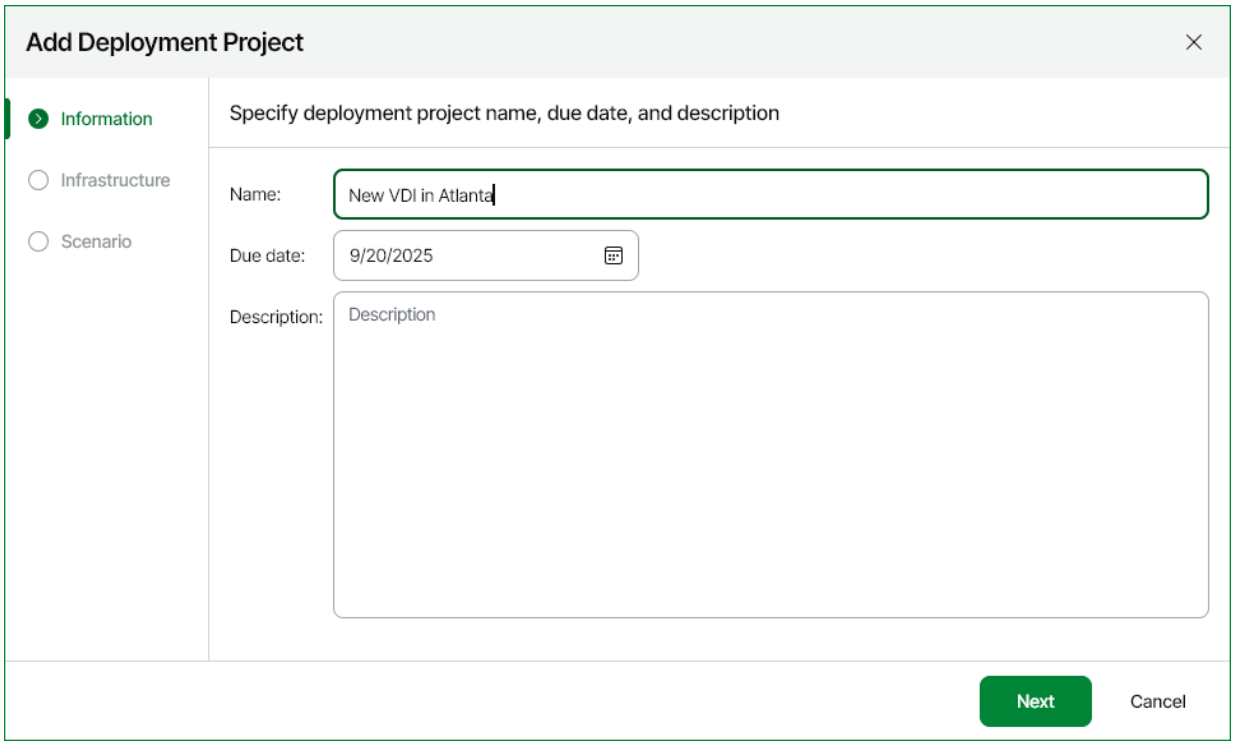
To launch the **Add Deployment Project** wizard:

1. Open Veeam ONE Web Client.
2. Click on the **Deployment Projects** section on the left.
3. At the top of the list, click **Add**.

   Veeam ONE Web Client will launch the **Add Deployment Project** wizard.

Step 2. Specify Deployment Project Name and Description

At the **Information** step of the wizard, specify deployment project name, description and the date when the deployment project must be completed.

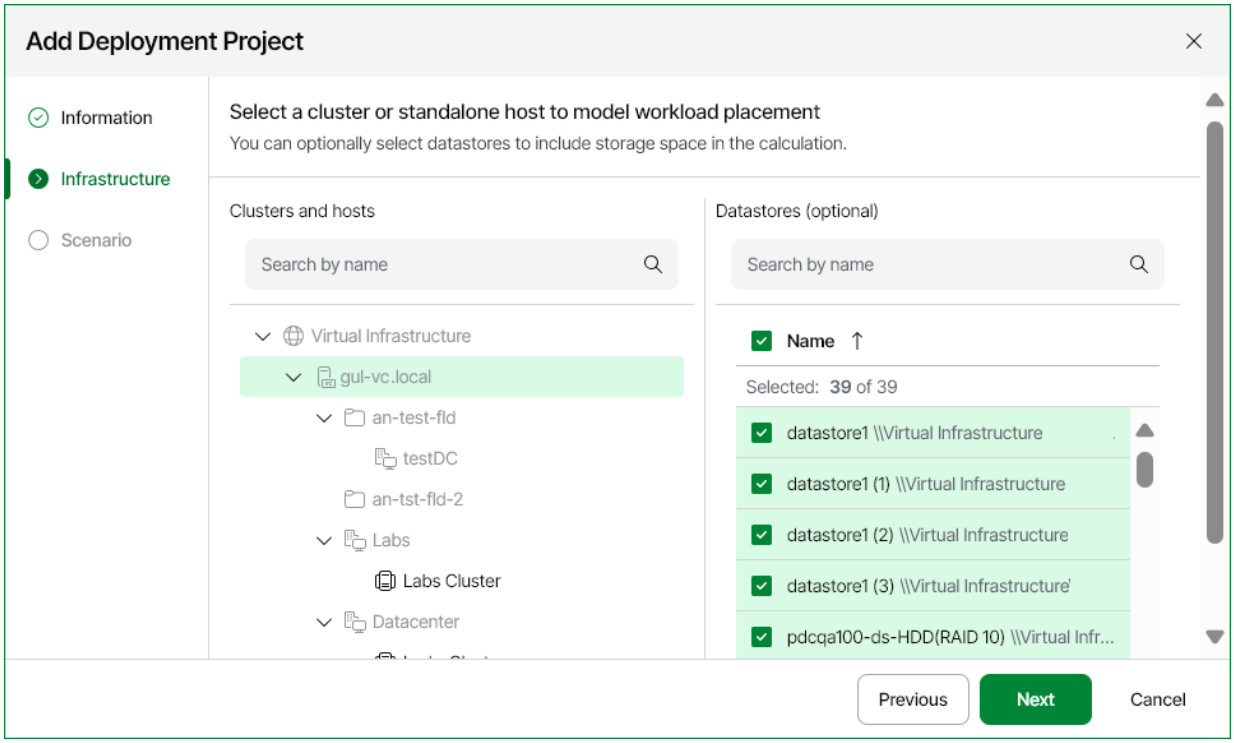


Step 3. Specify Deployment Infrastructure

At the **Infrastructure** step of the wizard, select cluster or host on which you want to build deployment project:

1. In the **Clusters and hosts** hierarchy, select a host or cluster to which you want to add hosts or VMs, or from which you want to remove hosts or VMs.
2. [Optional] In the **Datastores** list, select one or more datastores to which VMs will be deployed. Select datastores if you need to calculate storage resource requirements for new VMs.

   The datastore selection scope includes all datastores accessible by the selected container.



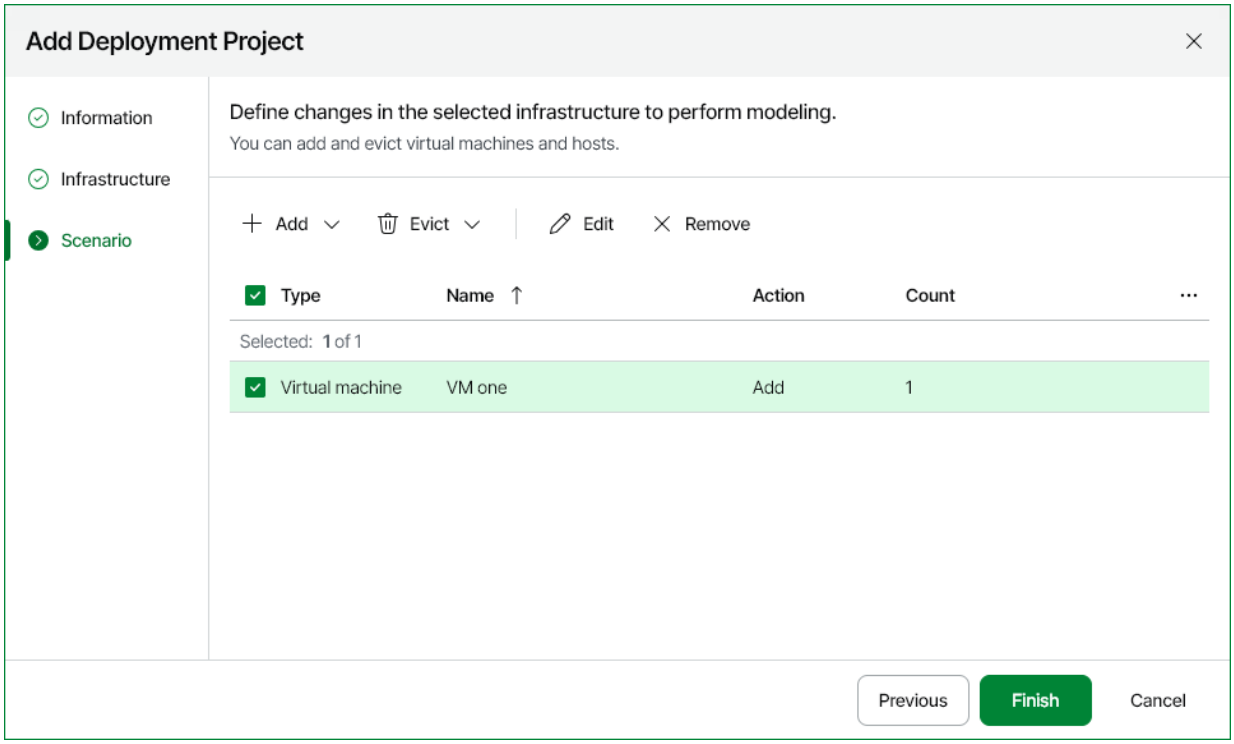
Step 4. Define Project Scenarios

At the **Scenario** step of the wizard, change parameters of the deployment project scenario. A deployment project scenario describes configuration of the hosts or VMs that must be added or evicted from the target container. One scenario can combine conditions for adding and evicting both hosts and VMs.

To change parameters of the deployment project scenario:

- Click **Add** and choose which object you want to add to the selected container:
  - New VM
  - New Host
  - Existing VM
  - Existing Host
- Click **Evict** and choose which object you want to evict from the selected container:
  - Existing VM
  - Existing Host
- Click **Edit** to modify the selected scenario entry.
- Click **Delete** to delete the selected scenario entry.

After you configure deployment scenario parameters, click **Finish** to save the deployment project.

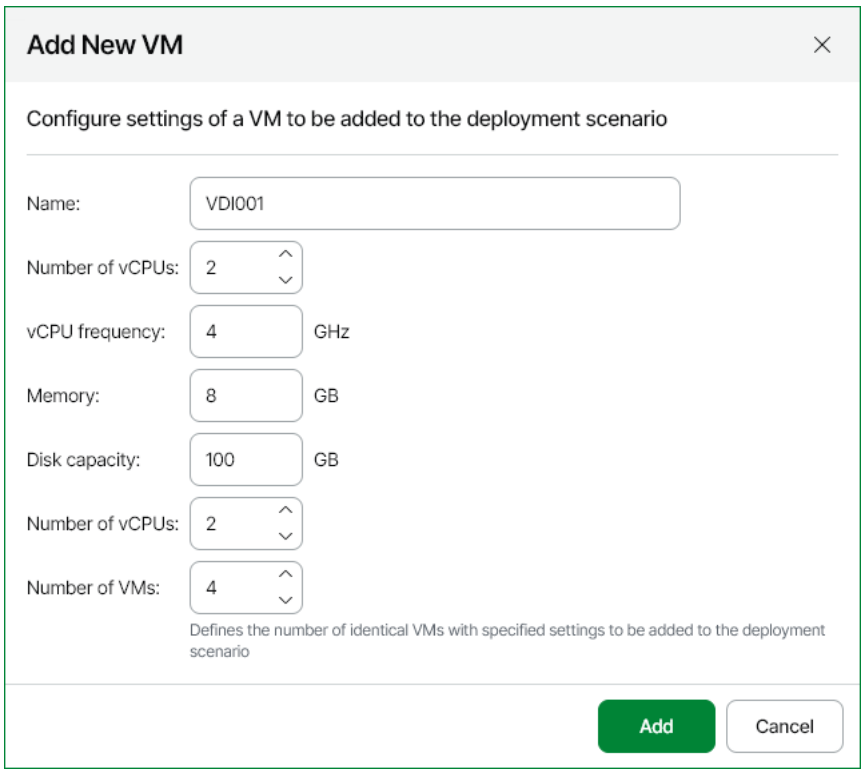


Adding New VM

To simulate a situation of adding new VMs to a host or cluster:

- At the **Scenario** step of the wizard, click **Add** and select **New VM**.

- In the **Add New VM** window, specify VM properties:
  - **Name** – VM name.
  - **Number of vCPUs** – the number of virtual CPU cores allocated to the VM.
  - **vCPU frequency** – each virtual CPU clock speed.
  - **Memory** – the amount of memory resources allocated to the VM.
  - **Disk capacity** – capacity of each virtual disk allocated to the VM.
  - **Number of disks** – the number of virtual disks allocated to the VM.
  - **Number of VMs** – the number of identical VMs to be added to the deployment project.
- Click **Add**.

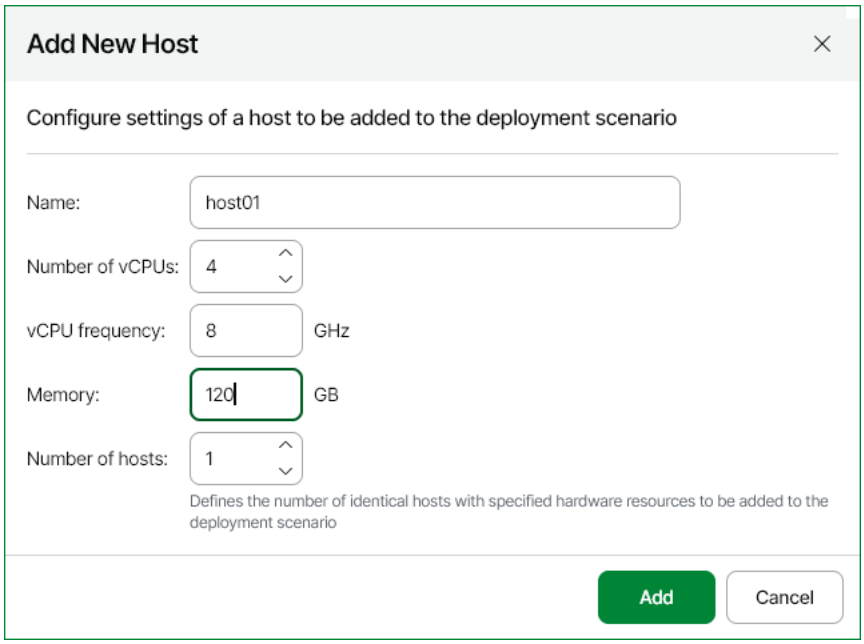


Adding New Host

To simulate a situation of adding new hosts to a cluster:

1. At the **Scenario** step of the wizard, click **Add** and select **New Host**.
2. In the **Add New Host** window, specify host properties:
   - **Name** – the host name.
   - **Number of vCPUs** – the number of virtual CPU cores allocated to the host.
   - **vCPU frequency** – each virtual CPU clock speed.
   - **Memory** – the amount of memory resources allocated to the host.
   - **Number of hosts** – the number of identical hosts to be added to the deployment project.

- Click **Add**.

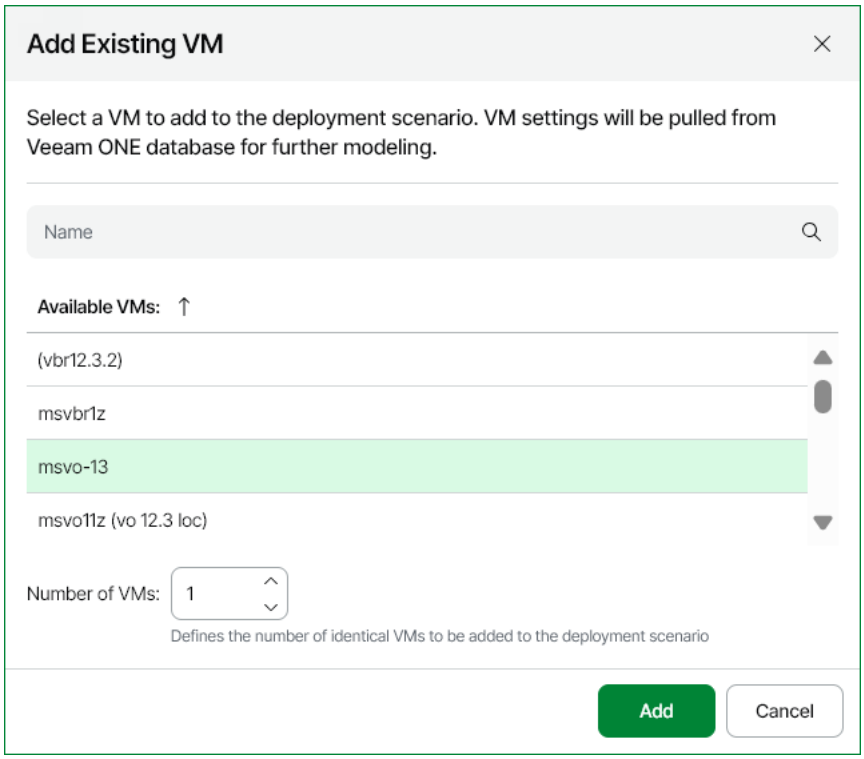


Adding Existing VM

To simulate a situation of adding copies of an existing VM to a host or cluster:

1. At the **Scenario** step of the wizard, click **Add** and select **Existing VM**.
2. In the **Add Existing VM** window, select a VM from the list and specify the number of VMs to be added.

   The VM selection scope includes all VMs in the selected container.
3. Click **Add**.

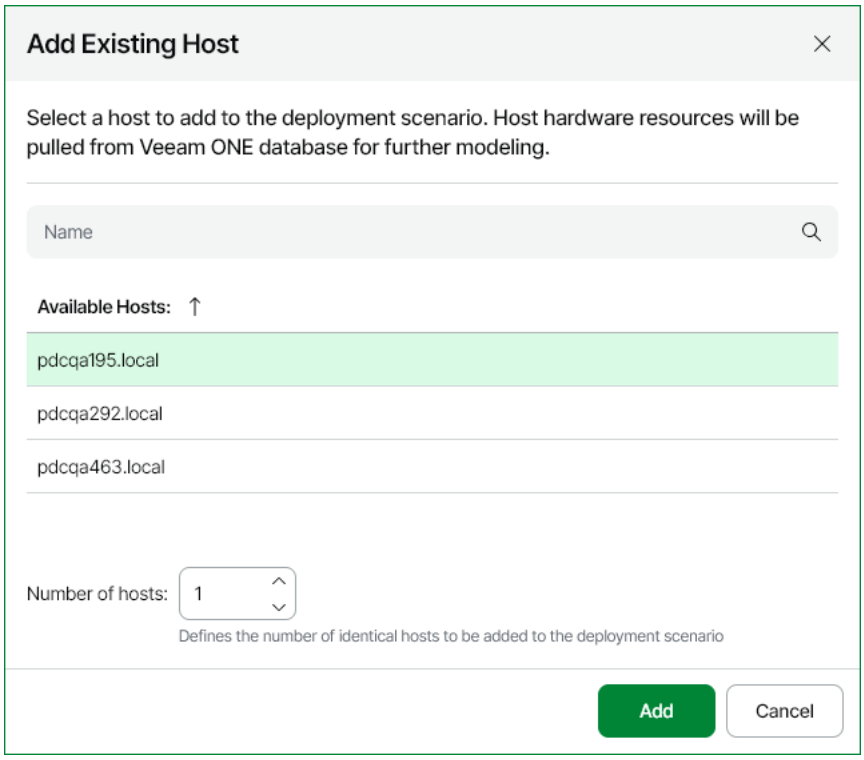


Adding Existing Host

To simulate a situation of adding copies of existing host to a cluster:

1. At the **Scenario** step of the wizard, click **Add** and select **Existing Host**.
2. In the **Add Existing Host** window, select a host from the list and specify the number of hosts to be added.

   The host selection scope includes all hosts in the selected container.
3. Click **Add**.



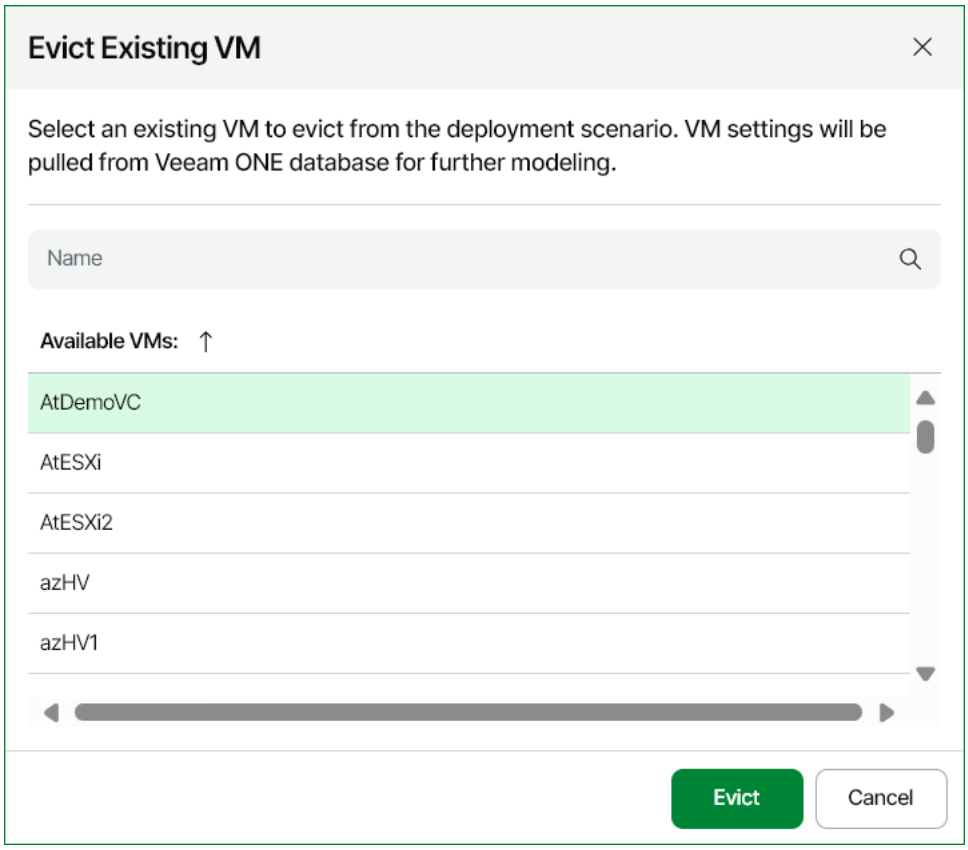
Evicting Existing VM

To simulate a situation of evicting a VM from a host or cluster:

1. At the **Scenario** step of the wizard, click **Evict** and select **Existing VM**.
2. In the **Evict Existing VM** window, select a VM from the list.

   The VM selection scope includes all VMs in the selected container.

3. Click **Evict**.



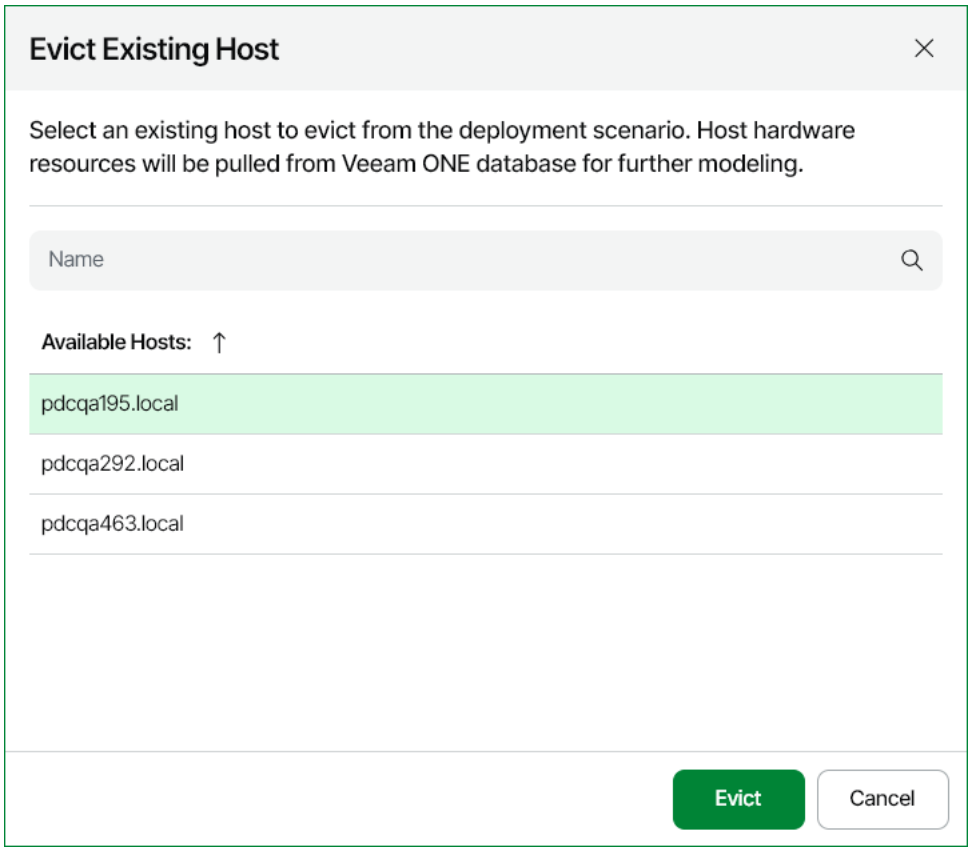
Evicting Existing Host

To simulate a situation of evicting a host from a cluster:

1. At the **Scenario** step of the wizard, click **Evict** and select **Existing Host**.
2. In the **Evict Existing Host** window, select a host from the list.

   The host selection scope includes all hosts in the selected container.

3. Click **Evict**.



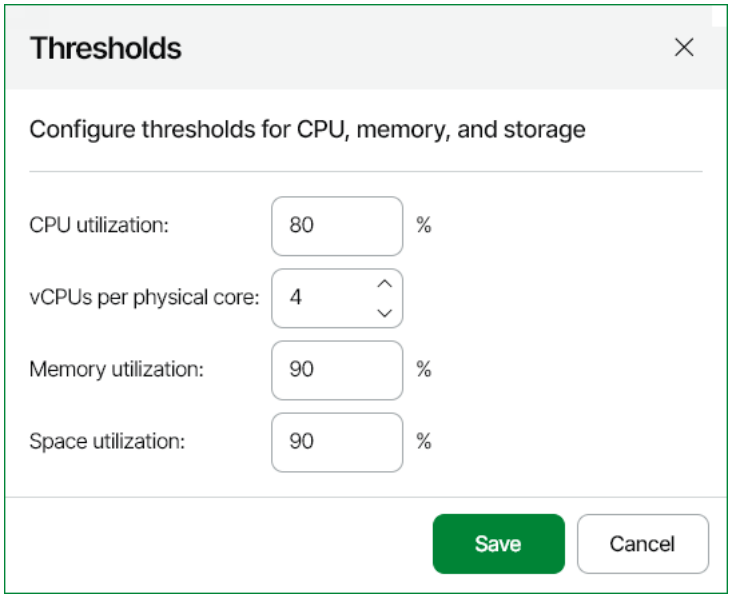
Adjusting Performance Thresholds

Before you run a scenario simulation, you may need to examine the effective performance thresholds and change them if necessary. The thresholds describe the maximum allowable resource utilization level that must not be exceeded after the deployment project changes come into effect.

The default performance thresholds are designed to ensure conservative resource utilization and are therefore appropriate for the majority of typical capacity planning projects.

To view and change performance thresholds:

1. Open Veeam ONE Web Client.
2. Open the **Deployment Projects** section.
3. At the top of the list, click **Thresholds**.
4. Change threshold values if required:
   - **CPU utilization** — maximum allowable processor utilization level on a physical host.
   - **vCPUs per physical core** — maximum allowable CPU allocation ratio (the ratio of vCPU to pCPU). It is calculated as the total number of allocated virtual cores divided by the number of physical cores in the target container.
   - **Memory utilization** — maximum allowable memory utilization level on the physical host.
   - **Space utilization** — maximum allowable amount of used space on the target datastores.
5. Click **Save**.



Calculating Deployment Projects

After you create a deployment project, you need to calculate it to run the scenario modeling and make sure that your capacities meet the deployment conditions.

You must recalculate a deployment project each time its settings change, or when the project is affected by changes in concurrent projects.

To calculate a deployment project:

1. Open Veeam ONE Web Client.
2. Open the **Deployment Projects** section.
3. Select the necessary deployment project in the list and click **Calculate**.

Veeam ONE Web Client will calculate the project and display the project result in the **Status** field. For details on deployment project statuses, see Deployment Project Statuses.

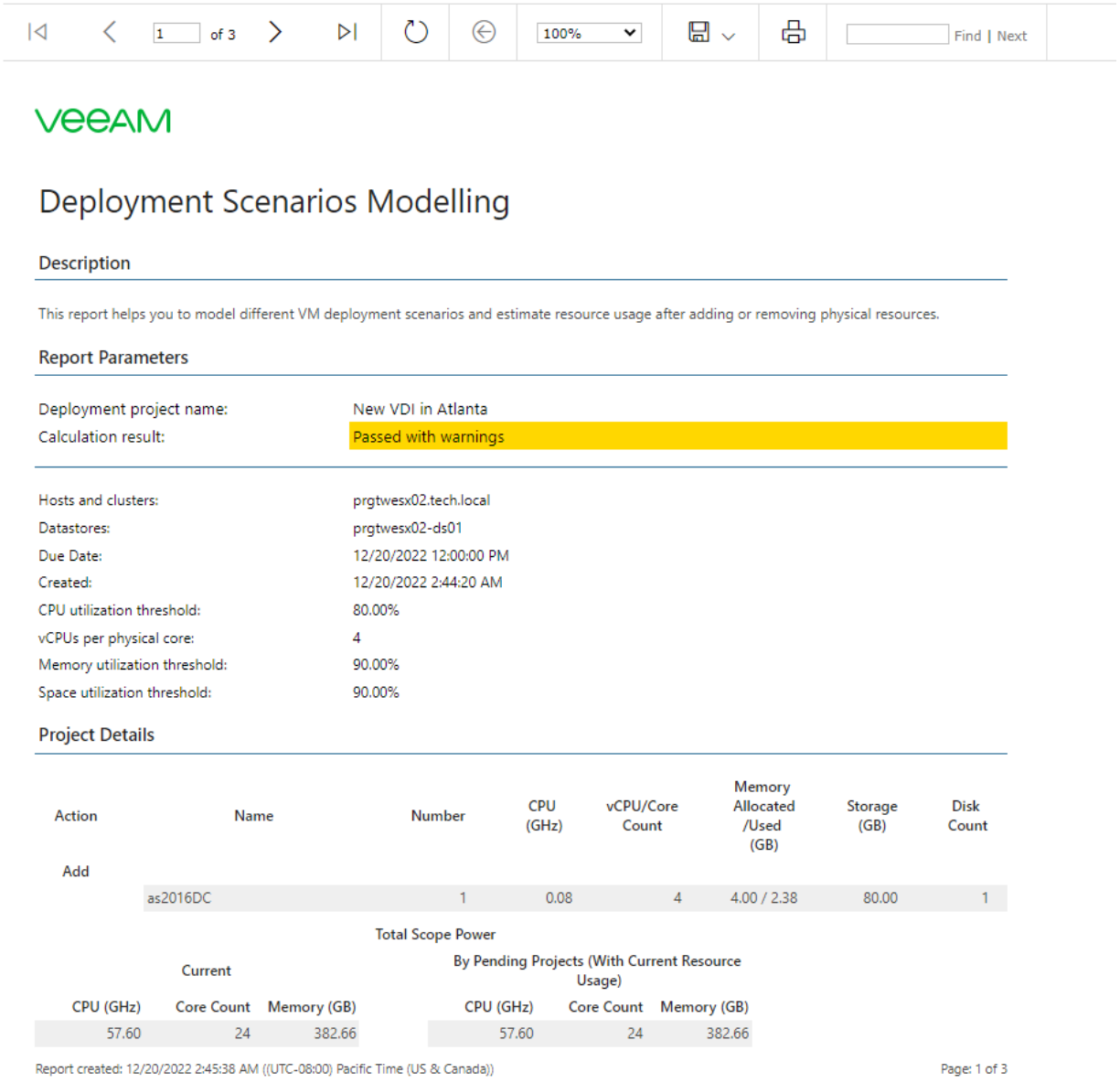
Viewing Deployment Project Report

After you calculate a project, you can view a report detailing the outcome of the simulated deployment:

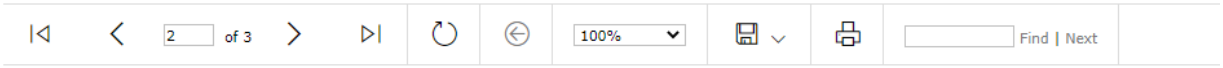
1. Open Veeam ONE Web Client.
2. Open the **Deployment Projects** section.
3. Select the necessary deployment project in the list and click **View Report**.

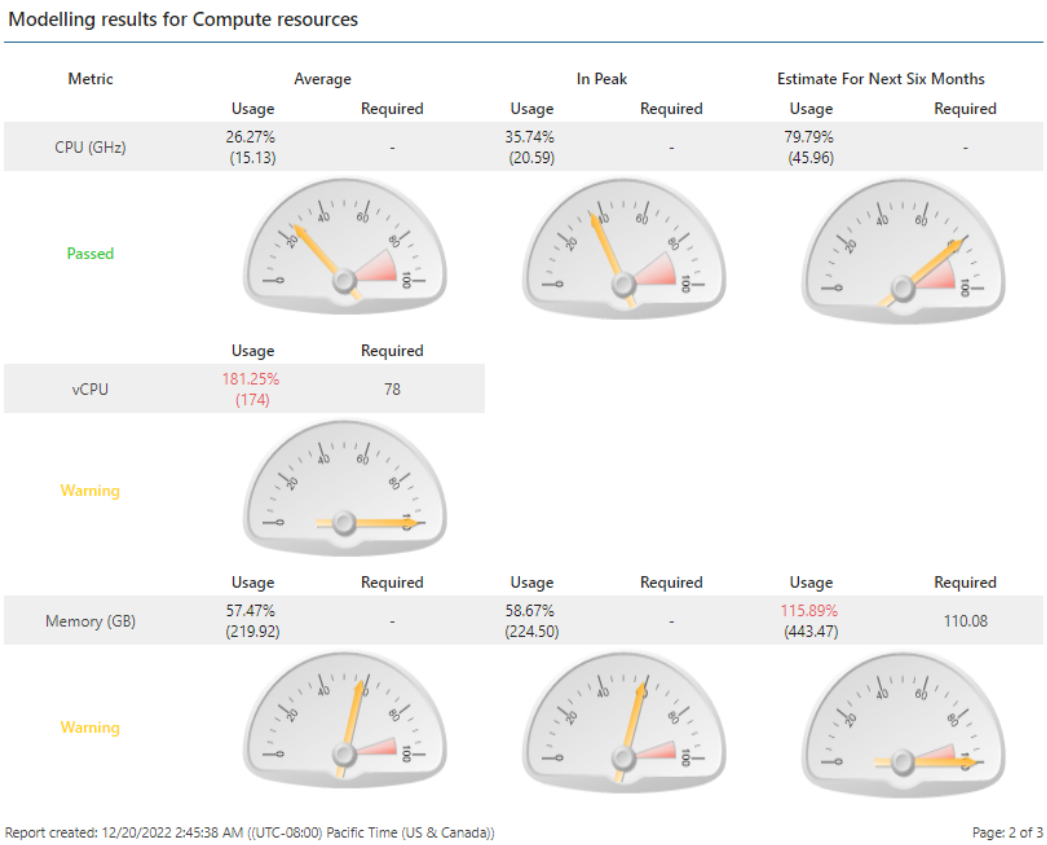
The report is designed to assist an administrator in implementing the deployment. The report details a projected resource usage, identifies a list of constraints and provides mitigation guidance.

The first report page outlines the projected changes and gives a summary of the constraining resources.



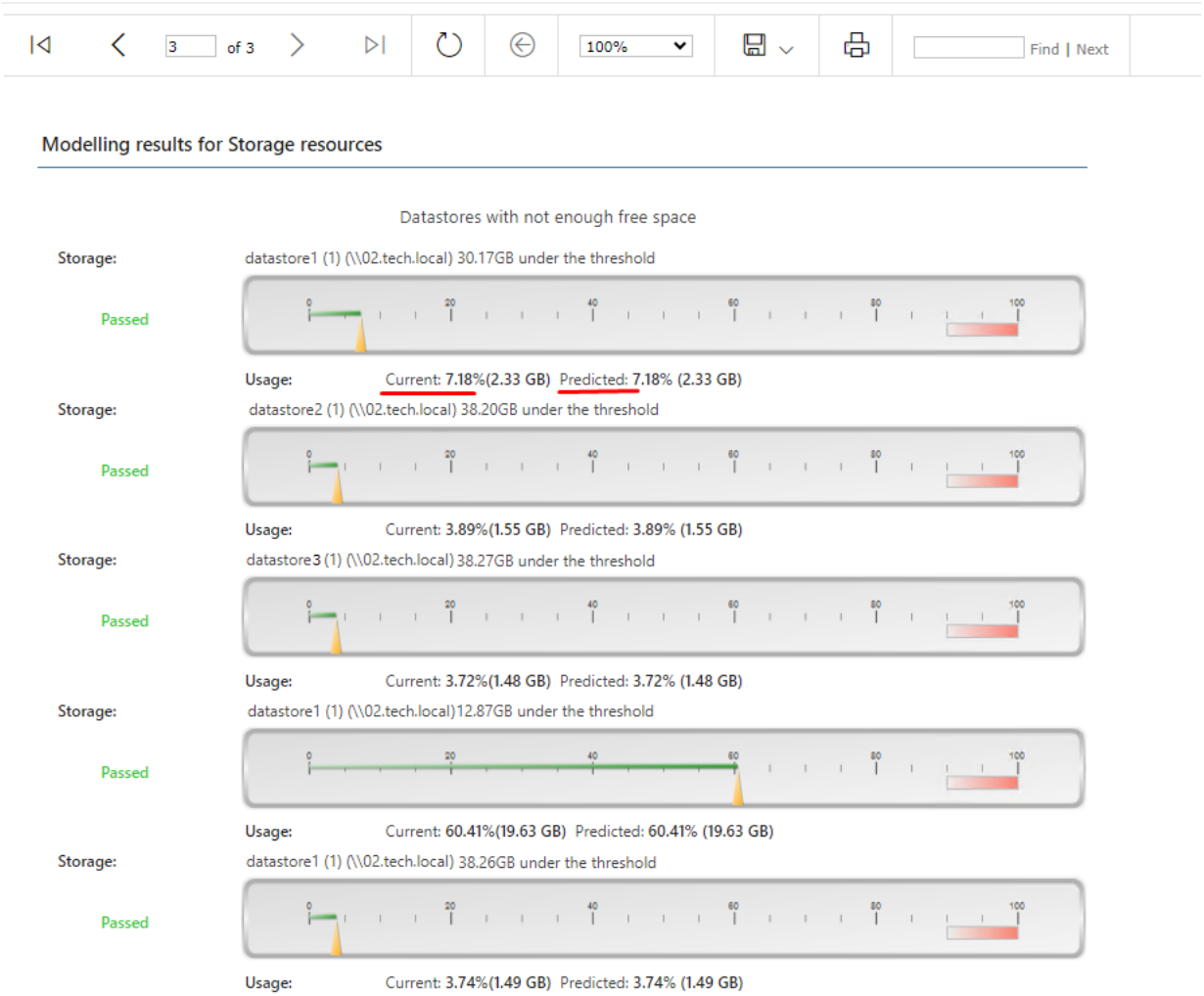
The subsequent pages show anticipated CPU, memory and storage usage levels and provide recommendations on capacity planning measures for maintaining robust and consistent performance in future.





The third report page displays storage modeling results including current and predicted storage usage.

Predicted storage usage shows expected user storage calculated in the following way: existing data on a storage plus space, reserved by previous linked projects plus space, reserved for new VMs minus space that can be released by deleted VMs.



Completing Deployment Projects

After you run a simulation based on a deployment project, you can flag the project as *Completed*.

By completing a deployment project, you instruct Veeam ONE Web Client to assume that all resources tied up to the project can be released and made available for calculation of the concurrent projects.

To complete a deployment project:

1. Open Veeam ONE Web Client.
2. Open the **Deployment Projects** section.
3. Select the necessary deployment project in the list and click **Complete**.
4. In the displayed dialog box, click **Complete** to confirm project completion.

After you complete a project, the date in the **Completed** column will be set to the current date.

Modifying Deployment Projects

You can modify settings of a deployment project that you have not completed yet. For example, you may need to update deployment project settings if the project was calculated with the *Failed* state.

To modify deployment project settings:

1. Open Veeam ONE Web Client.
2. Open the **Deployment Projects** section.
3. Select the necessary deployment project in the list and click **Edit**.
4. Change the deployment project settings as described in Creating Deployment Projects.
5. Save changes.

After you change project settings, you need to calculate the project anew. You may also need to recalculate overlapping or dependent projects. For example, if you change the project due date to an earlier date, Veeam ONE Web Client will offer you to recalculate all projects whose dates overlap with the changed project.

Deleting Deployment Projects

If you no longer need a deployment project, you can delete it:

1. Open Veeam ONE Web Client.
2. Open the **Deployment Projects** section.
3. Select the necessary deployment project in the list and click **Delete**.
4. In the displayed dialog box, click **Delete** to confirm project deletion.

After you delete a deployment project, you may need to rebuild overlapping or dependent projects. For details, see Calculating Deployment Projects.

Deployment Project Statuses

Veeam ONE deployment projects may have one of the following statuses.

- **To be calculated**

  The status indicates that project calculation is pending. Remediation action is to calculate the project. For details, see Calculating Deployment Projects.

- **To be recalculated**

  The status is assigned if the project settings have changed, or changes in a concurrent project affect the project. Remediation action is to calculate the project. For details, see Calculating Deployment Projects.

- **Not passed**

  The status indicates that the project simulation has completed but the deployment cannot be executed successfully due to anticipated resource constraints.

  The deployment simulation analysis has concluded that it is impossible to place the desired number of hosts or VMs without causing the future resource utilization to exceed 100 percent on any of the performance metrics.

  Remediation action is to view the project report and change the project settings in accordance with the report recommendations. For details, see Viewing Deployment Project Report and Modifying Deployment Projects.

- **Passed with warnings**

  This status indicates that the deployment is feasible but will cause the resource utilization to breach the threshold values. However, the resource utilization will not reach 100 percent.

  Remediation action is to view the project report and change the project settings in accordance with the report recommendations. For details, see Viewing Deployment Project Report and Modifying Deployment Projects.

- **Passed successfully**

  The status indicates that the project has completed successfully and its requirements are fully met. There are enough resources to accomplish the planned deployment and maintain an acceptable level of resource utilization.

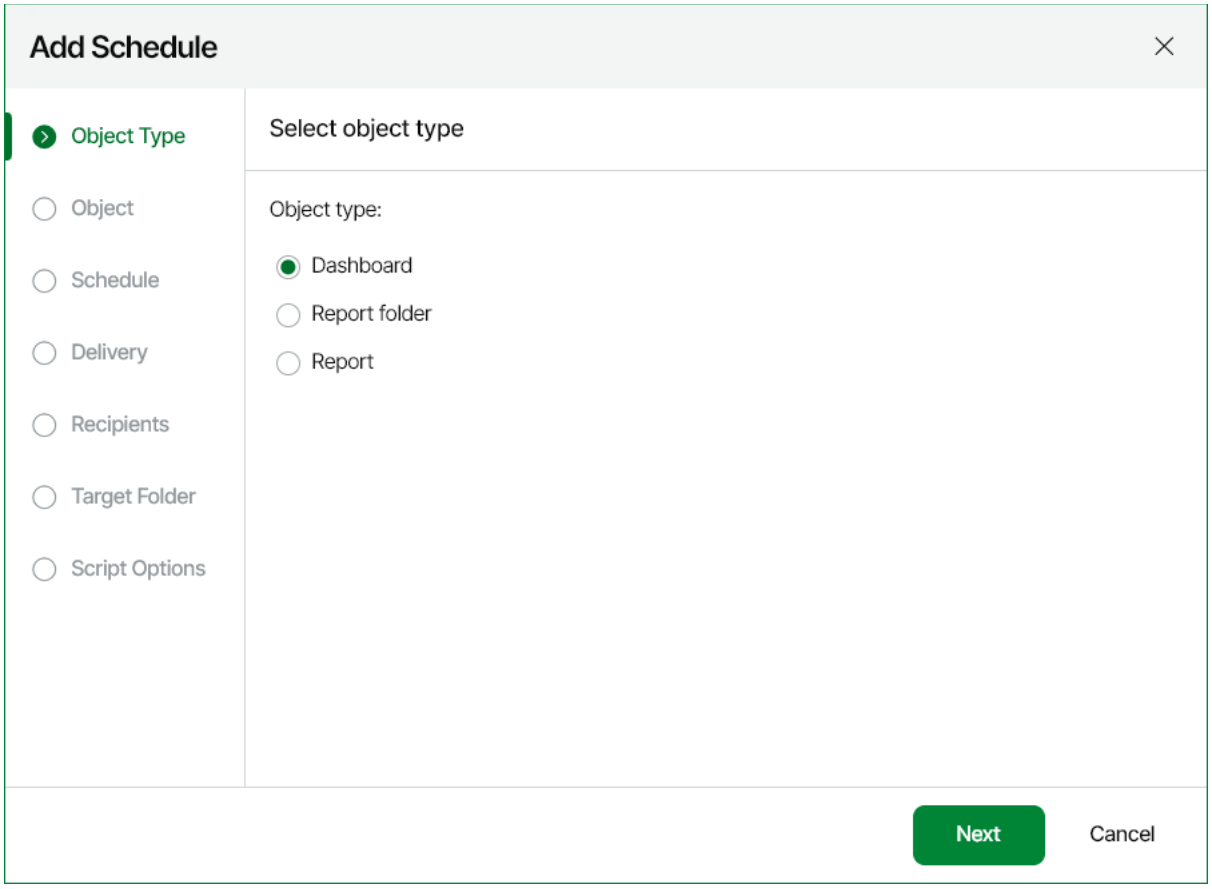
Scheduling

In Veeam ONE Web Client, you can schedule automatic delivery for dashboards, reports and report folders. You can choose to receive dashboards and reports by email, save dashboards and reports to a local folder or network share. Note that you can only schedule delivery for saved reports (that is, reports in the *My Reports* folder and its subfolders).

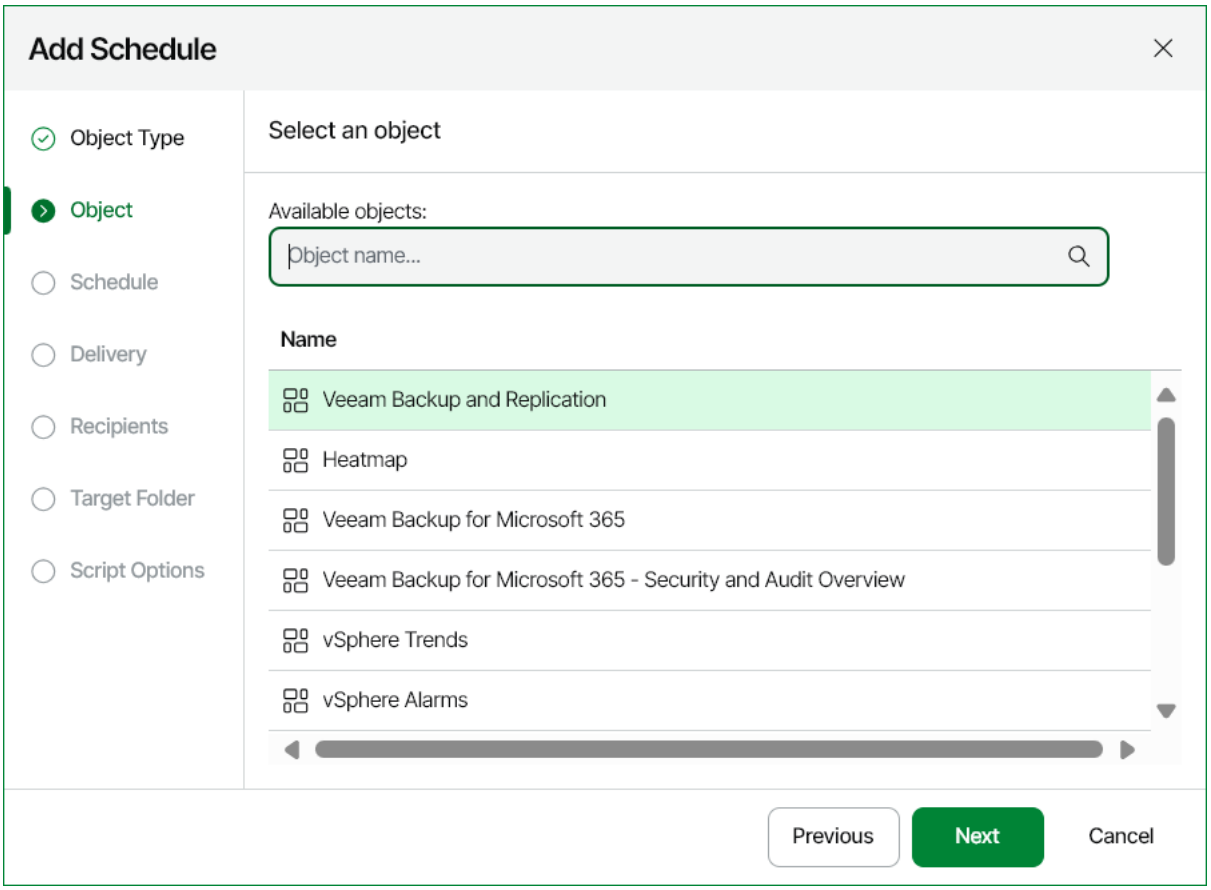
To schedule delivery for dashboards, reports and report folders:

1. Open Veeam ONE Web Client.
2. Open the **Scheduling** section.
3. At the top of the list, click **Add**.

   Veeam ONE Web Client will launch the **Add Schedule** wizard.
4. At the **Object Type** step of the wizard, specify the type of object for which you want to enable scheduled delivery.



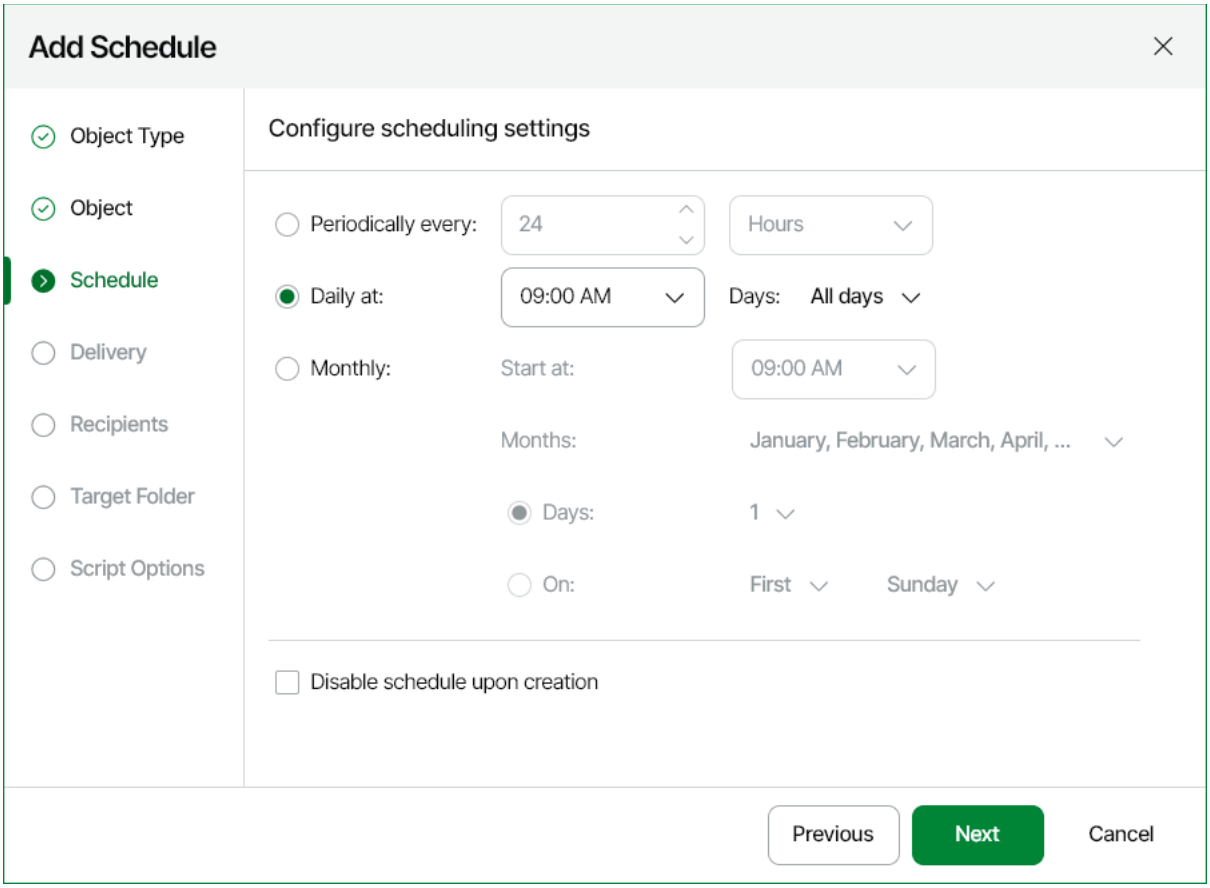
5. At the **Object** step of the wizard, select the dashboard, report or report folder for which you want to enable scheduled delivery.



6. At the **Schedule** step of the wizard, define a schedule according to which the object must be generated and delivered.
   - To generate and deliver the object repeatedly, with a specific time interval, select the **Periodically every** option and define the necessary interval.
   - To generate and deliver the object at specific time of day, select the **Daily at** option and specify the time and days of week on which the object must be delivered.
   - To generate and deliver the object on a monthly basis, select the **Monthly** option and choose the necessary months, dates or weekdays.

- To configure a schedule without enabling it, select the **Disable schedule upon creation** check box.

  You can enable the schedule later. For details on, see Managing Delivery Schedules.



7. At the **Delivery** step of the wizard, define object delivery options:

   - Select the **Send by email** check box to send objects by email.

     If this option is selected, the **Recipients** step will become available in the wizard.

     If you want to send objects by email, make sure you specified SMTP settings in Veeam ONE Client. For details on, see Configure SMTP Server Settings.

     [For the *Dashboard* object type] Additionally, you can select whether you want to attach a dashboard file to an email message or embed it into an email body.

     [For the *Report folder* object type] If you want to send several reports from the folder in a single email, select the **Send multiple reports in a single email** check box and specify the maximum number of reports to include in a single email. If the number of reports in the folder exceeds the specified maximum, Veeam ONE Web Client will send several emails.

   - Select the **Save to a folder** check box to save objects to a network share or a local folder on a machine where Veeam ONE Server component runs.

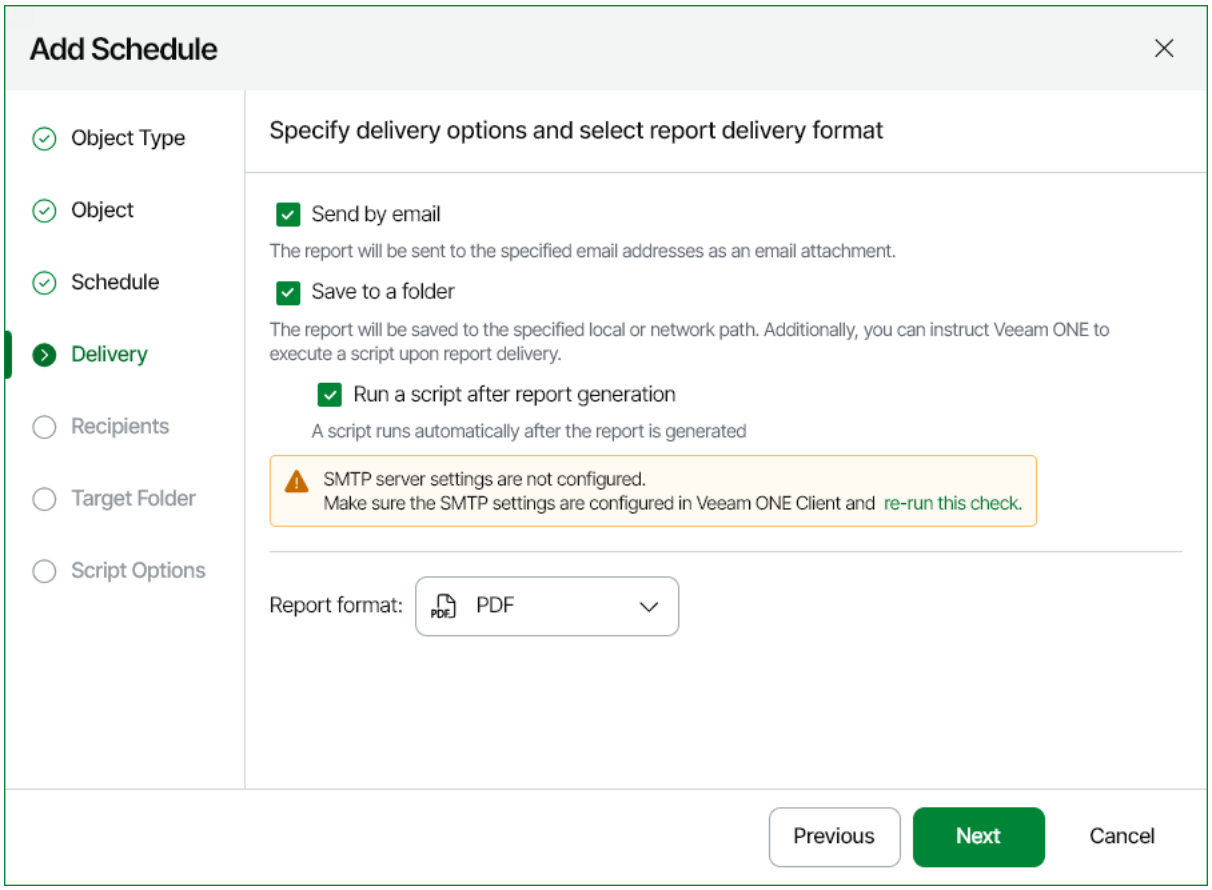
     With this option selected, the **Add Schedule** wizard will include an additional **Target Folder** step.

   - Select the **Run a script after report generation** check box to run a script file after generation is complete.

   - [For the *Report folder* and *Report* object types] From the **Report format** drop-down list, select the format in which the report must be saved. You can choose one of the following formats: *PDF*, *MS Word*, *MS Excel*, *CSV*, *XML*.

     Reports generated in Veeam ONE version 13's new report engine are only generated in PDF and CSV.

To save reports in CSV or XML format, you must configure an SRSS server. For details on, see Configuring SSRS Server Settings.



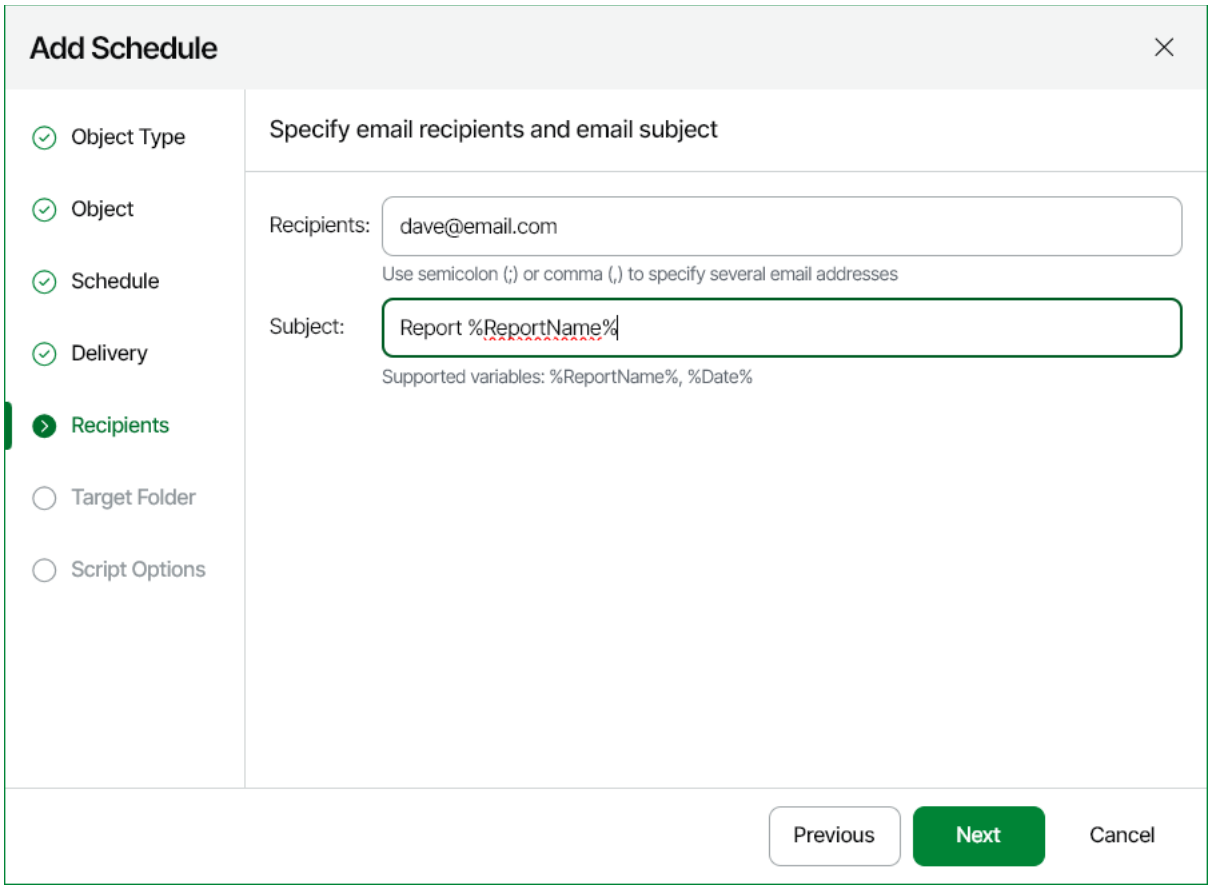
8. At the **Recipients** step of the wizard, configure object delivery by email:

   a. In the **Recipients** field, specify the recipient email address.

      If you want to send generated objects to multiple recipients, separate email addresses with a semicolon (;) or comma (,).

b. In the **Subject** field, specify an email subject title.

You can use the `%ReportName%` `%DashboardName%` and `%Date%` variables in the subject line — Veeam ONE will substitute these variables with the name of a delivered report, dashboard and the current date.



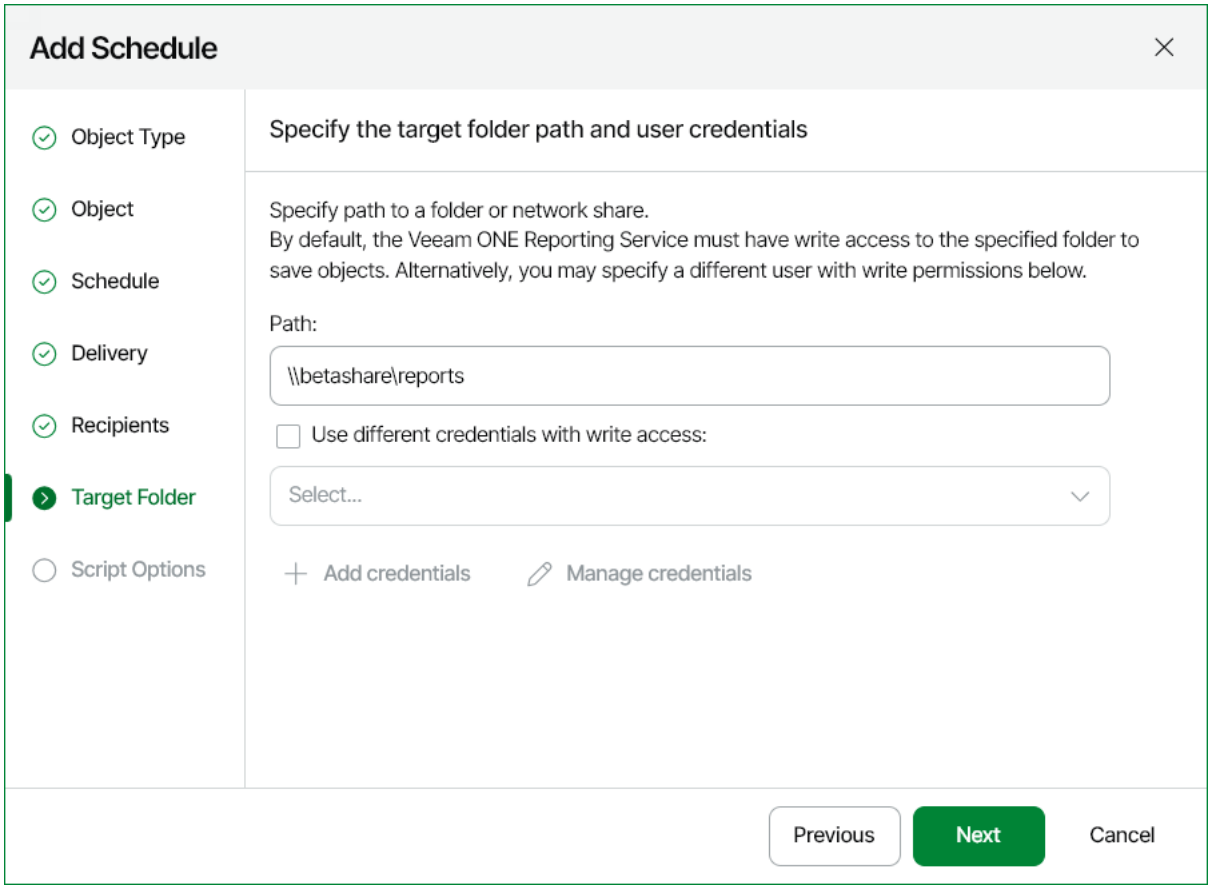
9. At the **Target Folder** step of the wizard, configure automated delivery to a local folder or a network share:

   a. In the **Path** field, specify a path to a local folder or network share.

   The path must refer to an existing folder. Veeam ONE will check if the specified folder exists and if the account under which Veeam ONE Reporting service runs has write permissions on the folder.

   b. Select the **Use different credentials with write access** check-box to select an alternative credentials account with access to the file path if required.

> **NOTE**
>
> The *Use different credentials with write access* option is only available for Veeam ONE Administrator accounts. For details, see Permissions and Security Groups.

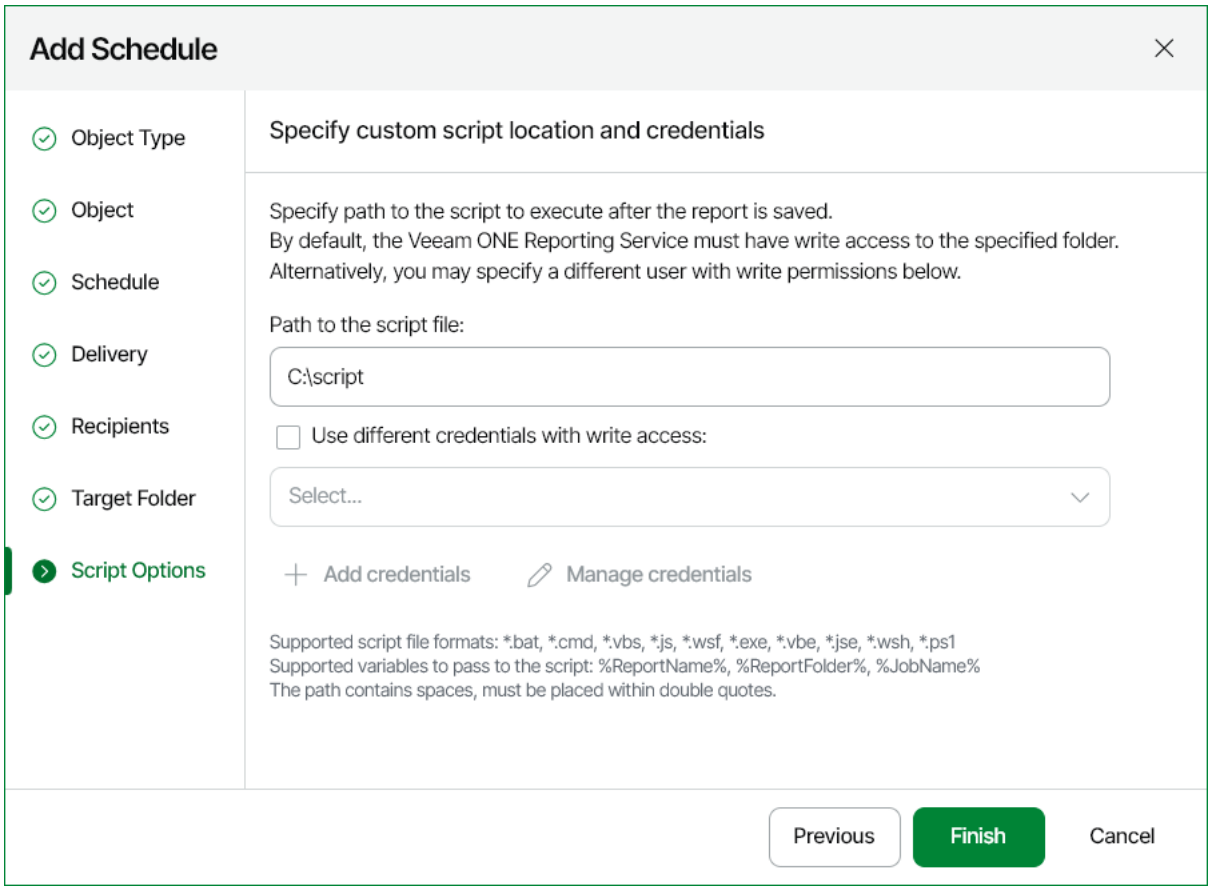


10. At the **Script Options** step of the wizard, configure the script file save path:

    a. In the **Path to the script file** field, specify a path to the script file location.

    The path must refer to an existing folder. Veeam ONE will check if the specified folder exists and if the account under which Veeam ONE Reporting service runs has write permissions on the folder.

b. Select the **Use different credentials with write access** check-box to select an alternative credentials account with access to the file path if required.



11. Click **Finish**.

If you want to configure multiple schedules, repeat steps **4-10** for each new schedule.

Managing Delivery Schedules

You can create multiple schedules for a single dashboard, report of report folder. Configuring multiple schedules allows you to set up complex scheduling and delivery method settings for the same object.

To manage delivery schedules:

1. Open Veeam ONE Web Client.
2. Open the **Scheduling** section.
3. Use controls at the top of the list to manage the delivery schedules:
   - To create a new delivery schedule, click **Add**.
   - To edit scheduling settings, select a schedule in the list and click **Edit**.
   - To enable previously disabled schedules, select one or more schedules in the list and click **Enable**.
   - To temporarily disable schedules, select one or more schedules in the list and click **Disable**.
   - To delete schedules, select one or more schedules in the list and click **Delete**.

Multi-Tenant Monitoring and Reporting

Veeam ONE supports multi-user access to its monitoring and reporting capabilities. Authorized users can concurrently access the same instance of Veeam ONE to monitor the health state of the virtual infrastructure, view dashboards and run reports.

To restrict access to sensitive infrastructure data, you can limit the scope of virtual infrastructure objects and associated data that must be available to a Veeam ONE user. Thus you can control what subset of the managed virtual infrastructure the user can see and work with.

User permissions can be restricted for two types of inventories only:

- VMware vSphere inventory
- VMware Cloud Director inventory

In a multi-tenant environment, you can configure restricted access to Veeam ONE data for owners of virtualized systems or responsible personnel and delegate monitoring and reporting tasks.

For example, if you manage VMware vSphere systems that belong to different business units, you can restrict permissions so that users can monitor and report on systems owned by their business unit. Or, if you manage resources for multiple organizations in a VMware Cloud Director environment, you can restrict permissions on a per-organization basis, so that users can monitor and report on vApps and VMs that belong to their organization.

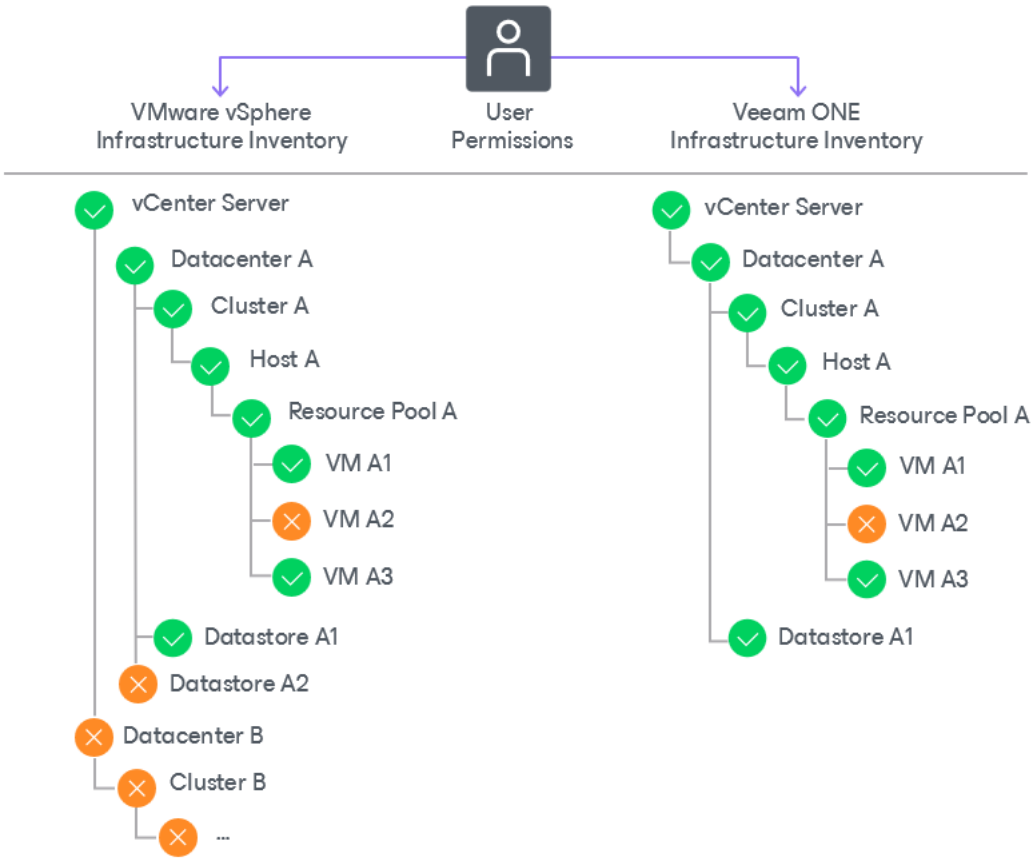
This document describes how to configure permissions for multi-tenant monitoring and reporting in Veeam ONE, and provides a basic configuration example.

How Access to Virtual Infrastructure Objects is Restricted

Veeam ONE collects inventory details about virtual infrastructure objects from connected VMware vSphere and VMware Cloud Director servers. In addition to objects and object properties, Veeam ONE gathers information about user permissions assigned to objects in VMware vSphere and VMware Cloud Director inventories. Permission details are gathered in real time, as part of the regular data collection procedure.

Collected permissions determine what users must (and must not) have access to objects in the Veeam ONE virtual infrastructure inventory. When a user authenticates to Veeam ONE, Veeam ONE checks what permissions are assigned to objects in the VMware vSphere and VMware Cloud Director inventories.

- If the user has appropriate permissions on an object, the user can access this object and associated data in the Veeam ONE infrastructure inventory.
- If the user does not have permissions on an object, the object is hidden. Data associated with this object is unavailable to the user.



Permissions and Security Groups

Do not mix permissions on virtual infrastructure inventory objects with the Veeam ONE security model that is based on security groups.

Users in Security Groups

Security groups define what actions users can perform in Veeam ONE. That is, what part of Veeam ONE functionality is available to users.

- *Veeam ONE Administrators* have access to all functions in Veeam ONE. They can perform all types of actions that Veeam ONE supports, including configuration actions.
- *Veeam ONE Power Users* have read access to monitoring data and can fully manage reports and dashboards but do not have access to Veeam ONE configuration settings.

  > **NOTE:**
  >
  > Members of the *Power Users* security group can run report and dashboard scheduling scripts on the machine on which the Veeam ONE Web Services component is installed. Include users into this group with caution.

- *Veeam ONE Read-Only Users* have limited access to Veeam ONE functions: they can access data in the read-only mode but cannot perform configuration tasks.

Users included in either Veeam ONE security group (*Administrators, Power Users* or *Read-Only Users*) have access to:

- All Veeam ONE consoles (Veeam ONE Client, Veeam ONE Web Client)
- All objects of the infrastructure inventory (including VMware vSphere, VMware Cloud Director, Microsoft Hyper-V, Veeam Backup & Replication and Veeam Backup for Microsoft 365)

Users with Restricted Permissions on Virtual Infrastructure Inventory

Permissions define what part of the virtual infrastructure is visible to a Veeam ONE user. To monitor and report on a restricted subset of the virtual infrastructure in Veeam ONE, a user must have permissions assigned on objects of the VMware vSphere or VMware Cloud Director inventory hierarchy. In this case, the user can utilize Veeam ONE monitoring and reporting capabilities for available objects of the VMware vSphere or VMware Cloud Director infrastructure. Microsoft Hyper-V, Veeam Backup & Replication and Veeam Backup for Microsoft 365 inventory objects are unavailable for the user. For details on limitations of functionality for users with restricted permissions, see Functional Restrictions.

> **IMPORTANT!**
>
> Do not include a user with restricted permissions into Veeam ONE security groups. Members of security groups always have access to the whole infrastructure inventory in Veeam ONE, regardless of their permissions on the VMware vSphere or VMware Cloud Director inventory hierarchy.

User Permissions

The following table describes what functionality is available to users in accordance with their user role.

Veeam ONE Web Client

Functionality	Veeam ONE Administrator	Veeam ONE Power User	Veeam ONE Read Only User
Threat Center	Full	Full	Read
Dashboards	Full	Full	Read
Jobs Calendar	Full	Full	N/A
Reports	Full	Full	Read
Alarms Overview	Full	Read	Read
Scheduling	Full	Limited (Choosing credentials for scheduling is unavailable)	N/A
Deployment Projects	Full	Full	Read
Veeam Intelligence	Full	N/A	N/A
Notification Bell	Full	Full	Full
Configuration	Full	N/A	N/A

Veeam ONE Client

Functionality	Veeam ONE Administrator	Veeam ONE Power User	Veeam ONE Read Only User
Alarms	Full	Read	Read
Infrastructure Changes	Full	N/A	N/A

Functionality	Veeam ONE Administrator	Veeam ONE Power User	Veeam ONE Read Only User
Monitoring	Full	Read	Read
Server Settings	Full	N/A	N/A
Client Settings	Full	Full	Full
Licensing	Full	N/A	N/A
Business View	Full	Read	Read
Notification Settings	Full	N/A	N/A
Credentials Manager	Full	N/A	N/A

Functional Restrictions

Users with restricted permissions on the virtual infrastructure inventory have limited access to Veeam ONE functionality. Functional restrictions prevent these users from changing settings that may affect other users in Veeam ONE.

Veeam ONE Web Client

In Veeam ONE Web Client, users with restricted permissions cannot perform the following tasks:

- Access and modify all configuration settings.
- Modify, delete and schedule predefined and custom dashboards.
- View custom reports that were saved by other users.
- Work with deployment projects.
- Work with specific reports.

  For the list of reports available to these users, see Reports for Users with Restricted Permissions.

Users with restricted permissions can access custom dashboards and saved reports that have been shared by *Veeam ONE Administrator* and *Veeam ONE Power User*. The virtual infrastructure scope on dashboards and in reports will be restricted in accordance with effective user permissions.

For details on sharing dashboards and reports, see sections Sharing Dashboards and Sharing Reports.

Veeam ONE Client

In Veeam ONE Client, users with restricted permissions cannot perform the following tasks:

- Access and modify configuration settings (connections to virtual servers, notification settings, Veeam ONE server settings and license).
- Create, modify, delete, acknowledge or resolve alarms.

Configuring Access for Users with Restricted Permissions

To provide access to Veeam ONE reporting and monitoring features for a user with restricted permissions, perform these steps:

1. Check Veeam ONE security group membership.
2. Check requirements to the user account.
3. Assign permissions on the VMware vSphere or VMware Cloud Director inventory objects.
4. Log in to Veeam ONE as the user with restricted permissions.

Step 1. Check Veeam ONE Security Group Membership

Check that the user is **not included** in Veeam ONE security groups (*Veeam ONE Administrators*, *Veeam ONE Power Users* or *Veeam ONE Read-Only Users*). Otherwise, the user will be granted access to the whole infrastructure inventory in Veeam ONE, including VMware vSphere, VMware Cloud Director, Microsoft Hyper-V, Veeam Backup & Replication and Veeam Backup for Microsoft 365.

For details, see Permissions and Security Groups.

Step 2. Check Requirements to User Account

You can provide access to Veeam ONE for single users and user groups.

The following table describes types of accounts for which you can configure restricted permissions.

Platform	Account Type	Description and Notes
vCenter Server	Domain users and groups	Members of the Active Directory domain. vCenter Server must be configured to use Active Directory for authentication. For details on user authentication in VMware vSphere, see Active Directory Identity Source Settings. To log in to Veeam ONE, you must provide user name in the following format: `domain\username`.
	Local users and groups	Local users and groups on the machine where vCenter Server is installed. To log in to Veeam ONE, you must provide user name in the following format: `hostname\username`.
	Single Sign-On users and groups	Single Sign-On users and groups on vCenter Server. For details, see vSphere Authentication with vCenter Single Sign-On. **Note**: Single Sign-On must be installed on the machine where vCenter Server runs, with the default installation path and port settings. Otherwise, Veeam ONE will not be able to detect its database with user groups and users. To log in to Veeam ONE, you must provide user name in the following format: `ssodomain\username`.
ESXi host	Domain users and groups	Members of the Active Directory domain. Standalone hosts must be configured to use Active Directory for authentication. For details, see Using Active Directory to Manage ESXi Users. To log in to Veeam ONE, you must provide user name in the following format: `domain\username`.

Platform	Account Type	Description and Notes
VMware Cloud Director	Domain users and groups	Members of the Active Directory domain. Users must be able to authenticate to an LDAP server. For details, see VMware Cloud Director documentation. To log in to Veeam ONE, you must provide user name in the following format: `domain\username`.
	Local users and groups	Local users and groups in VMware Cloud Director. To log in to Veeam ONE, you must provide user name in the following format: • For organization user: `organization\username` • For VMware Cloud Director administrator: `system\username`

NOTE:

For each local or Single Sign-On user that authenticates to Veeam ONE, Veeam ONE creates a temporary Windows account on the machine that runs the Veeam ONE Server component. This temporary account is deleted after 30 days of inactivity.

Authorizing with Veeam ONE

To authorize with Veeam ONE components (Veeam ONE Client and Veeam ONE Web Client), a user must have the *Allow log on locally* privilege assigned.

By default, this privilege is assigned to users included in the local Administrators group. For users not included in the local Administrators group, you must assign this privilege manually.

NOTE:

If you use the advanced deployment scenario, you must assign the *Allow log on locally* privilege on the machines that host the Veeam ONE Server and Veeam ONE Web UI components.

Step 3. Assign Permissions on Infrastructure Inventory Objects

To view and work with virtual infrastructure objects in Veeam ONE, the user must have appropriate permissions on these objects set in the VMware vSphere or VMware Cloud Director inventory.

VMware vSphere Permissions

Connect to vCenter Server or standalone host with vSphere Client and assign permissions on objects to which the user must have access.

The following table shows minimal required privileges on VMware vSphere inventory objects.

VI Inventory Object	VMware vSphere Privilege
vCenter Server (root) **Data Center** **Cluster** **Host** **Resource Pool/vApp** **Datastore Cluster** **Datastore**	Read-only
Virtual Machine	• Read-only • Virtual machine.Interaction.Answer question[1] • Virtual machine.Interaction.Console interaction[1]

[1] Required to access VM console in Veeam ONE Client

> **NOTE:**
>
> If you assign permissions to container objects (such as hosts, resource pools or vApps), consider enabling propagation. In this case, all new child objects that may be added to the container in future will become available to the user.

VMware Cloud Director Permissions

Connect to VMware Cloud Director and assign permissions on objects to which the user must have access.

The following table shows minimal required roles for VMware Cloud Director inventory objects.

VI Inventory Object	VMware Cloud Director Role
vCloud Director (root)	System Administrator
Organization	Console access only

Step 4. Log in to Veeam ONE as User with Restricted Permissions

Log in to Veeam ONE Client and Veeam ONE Web Client as the user to make sure the user has access to Veeam ONE.

For details on how to log in to Veeam ONE Client, see Access Veeam ONE Client. Veeam ONE Client will display the *[Restricted permissions mode]* label next to the user name under which you are logged in.

For details on how to log in to Veeam ONE Web Client, see Access Veeam ONE Web Client. Veeam ONE Web Client will display the *Restricted permissions user* label next to the user name under which you are logged in.

Reports for Users with Restricted Permissions

The following reports are available to users with restricted permissions:

Report Pack	Report	Available for VMware vSphere users	Available for VMware Cloud Director users
Infrastructure Chargeback	VM Configuration Chargeback	Yes	Yes
	VM Performance Chargeback	Yes	Yes
vSphere Infrastructure Assessment	Datastore Performance Assessment	Yes	No
	VM Change Rate Estimation	Yes	Yes
	VM Configuration Assessment	Yes	Yes
Veeam Backup Assessment	VM Backup Compliance Overview	Yes	Yes
	VMs with no Archive Copy	Yes	Yes
Veeam Backup Monitoring	Protected VMs	Yes	Yes
	VM Daily Protection Status	Yes	No
	Data Change Rate History	Yes	Yes
	CDP SLA Compliance	Yes	Yes
Veeam Backup Overview	Protected VMs Job Schedule	Yes	Yes
vSphere Overview	Cluster Configuration	Yes	No
	Datastore Capacity	Yes	No

Report Pack	Report	Available for VMware vSphere users	Available for VMware Cloud Director users
	Datastore Configuration	Yes	No
	Datastore Space Usage History	Yes	No
	Guest Disk Free Space	Yes	No
	Host Configuration	Yes	No
	Hypervisor Version	Yes	No
	Infrastructure Overview	Yes	No
	VMs Configuration	Yes	No
	VMs Growth	Yes	No
vSphere Monitoring	Alarms Current State Overview	Yes	No
	Alarms Overview	Yes	No
	Cluster Hosts Performance	Yes	No
	Cluster Performance	Yes	No
	Datastore Performance	Yes	No
	Host Performance	Yes	No
	Host Uptime	Yes	No
	Multiple Clusters Performance	Yes	No
	Resource Pool and vApp Performance	Yes	No
	VM Performance	Yes	No

Report Pack	Report	Available for VMware vSphere users	Available for VMware Cloud Director users
	VM Uptime	Yes	No
vSphere Optimization	Active Snapshots	Yes	Yes
	Garbage Files	Yes	No
	Idle VMs	Yes	Yes
	Inefficient Datastore Usage	Yes	Yes
	Orphaned VM Snapshots	Yes	No
	Oversized VMs	Yes	Yes
	Powered Off VMs	Yes	Yes
	Undersized VMs	Yes	Yes
vSphere Configuration Tracking	Infrastructure Changes Audit	Yes	No
	Infrastructure Changes by Object	Yes	No
Custom reports	vSphere Custom Performance	Yes	Yes
	vSphere Raw Performance Data	Yes	No
VMware Cloud Director	Catalogs Overview	No	Yes
	Organization Configuration	No	Yes
	Organization VDC Performance	No	Yes
	Provider VDCs Performance	No	Yes

Report Pack	Report	Available for VMware vSphere users	Available for VMware Cloud Director users
	vApp Configuration	No	Yes
	vApp Performance	No	Yes
	VM Uptime	No	Yes

Veeam Backup & Replication Monitoring

Veeam ONE Client offers advanced functionality for monitoring Veeam Backup & Replication infrastructure and data protection operations in the managed virtual environment.

With Veeam ONE Client, you can:

1. **Analyze Veeam Backup & Replication logs to find potential issues.**

   Configure Veeam ONE to perform automatic diagnostics of backup infrastructure to facilitate troubleshooting and avoid data protection problems.

   Veeam Intelligent Diagnostics feature allows you to receive alarms with recommendations and knowledge base articles on configuration of backup infrastructure and jobs.

2. **Monitor the overall state of the backup infrastructure**.

   Check the **Summary** dashboards to reveal hotspots in the Veeam Backup & Replication infrastructure.

   Quickly review the latest status of backup, replication and SureBackup jobs, examine configuration and performance of your backup infrastructure components, detect the most loaded proxies, repositories, WAN accelerators, tape servers, cloud gateways and cloud repositories, and check whether your jobs complete within the backup window.

   Summary dashboards help you quickly reveal issues that can lead to job failure, and cause loss of valuable data.

3. **View triggered alarms**.

   Go to the **Alarms** dashboard to see details on issues and problems in your backup infrastructure.

   Data protection alarms allow you to instantaneously react to potentially dangerous situations with ongoing data protection and take immediate actions to eliminate the risk of data loss.

4. **Check the latest job status**.

   Track the status of your backup, replication, SureBackup, backup copy, SQL database transaction log backup, Oracle database backup jobs, backup to tape, file to tape, VM copy and file copy jobs.

   Get up-to-date information on the efficiency of data protection in your virtual environment and address problems with jobs as soon as they appear.

5. **Work with performance charts**.

   Drill down to performance charts to diagnose performance problems with backup infrastructure components and identify bottlenecks.

   Track CPU, memory, disk and network performance for backup servers, proxies, repositories and WAN accelerators to make sure the backup data flow is efficient, and all resources engaged in the backup process are optimally used.

6. **View the list of events**.

   View the full list of events that triggered Veeam Backup & Replication alarms, and events notifying about connection problems with Veeam Backup & Replication servers or Veeam Backup Enterprise Manager.

Prerequisites

Before you start monitoring the Veeam Backup & Replication infrastructure, make sure you have configured connections to Veeam Backup & Replication servers from which Veeam ONE will collect data. For details on configuring server connections, see Connecting Veeam Backup & Replication Servers.

Veeam Intelligent Diagnostics

Veeam Intelligent Diagnostics is a feature that allows you to automatically detect known issues in configuration and performance of backup infrastructure. It enables Veeam ONE to parse logs from Veeam Backup & Replication servers and trigger alarms with recommendations based on the results of log analysis. This allows you to eliminate configuration issues without the necessity to address Veeam Technical Support.

Veeam Intelligent Diagnostics process involves the following components:

- **Signatures** — problem definitions that are based on common issues investigated by Veeam Technical Support.

  Signatures are stored in Veeam ONE database and displayed as Intelligent Diagnostics alarms in the **Alarm Management** view.

  Signatures can be updated manually or automatically. For details on updating and importing signatures, see Managing Signatures.

- **Veeam Analytics service** — collects monitoring and reporting data and enables communication with Veeam Backup & Replication servers, performs collection of logs, and sends remediation commands.

> **NOTE:**
>
> It is recommended to install Veeam Analytics service to improve data collection performance in large-scale Veeam Backup & Replication infrastructures.

  Veeam Analytics service can work in the following modes:

  - **Server**

    In this mode, Veeam Analytics service is responsible for analyzing log data and signature updates.

    Veeam Analytics service server is included into Veeam ONE installation package and deployed on the machine running Veeam ONE Server during product installation.

  - **Client**

    In this mode, Veeam Analytics service is responsible for collecting logs and executing remediation actions on Veeam Backup & Replication servers.

    Veeam Analytics service client is deployed on Veeam Backup & Replication servers when you connect these servers to Veeam ONE. For details on managing client Veeam Analytics service, see Managing Veeam Analytics Service.

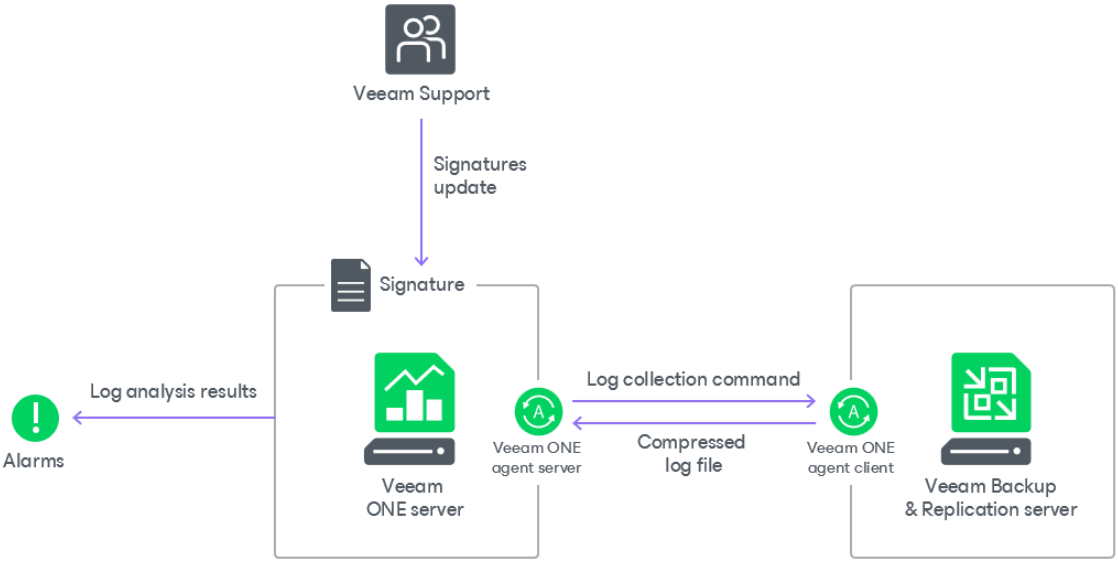
> **NOTE:**
>
> For proper operation of Veeam Intelligent Diagnostics feature, Veeam Backup & Replication servers on which you deploy Veeam Analytics service must have a PowerShell module deployed. For details on Veeam Backup PowerShell module, see Veeam PowerShell Reference.

How Veeam Intelligent Diagnostics Works

Veeam Intelligent Diagnostics works in the following way:

1. When Veeam Intelligent Diagnostics session starts, Veeam ONE Client sends a command to Veeam Analytics service client to collect logs from Veeam Backup & Replication.
2. Veeam Analytics service client creates a compressed log file and sends it to Veeam Analytics service server.

3. Veeam Analytics service server parses Veeam Backup & Replication logs for known exceptions and error messages by comparing logs with signatures.
4. If any known issues found, Veeam ONE Client triggers an alarm with recommendations and knowledge base articles from Veeam Technical Support.



How to Configure Veeam Intelligent Diagnostics

To configure Veeam Intelligent Diagnostics, perform the following steps:

1. Install Veeam Analytics service on Veeam Backup & Replication servers connected to Veeam ONE and configure agent settings.

   For details, see Managing Veeam ONE Agents.
2. Obtain an up-to-date version of signatures.

   For details, see Managing Signatures.
3. Configure log analysis schedule or start log analysis session manually.

   For details, see Performing Log Analysis.

Managing Veeam Analytics Service

In Veeam ONE Web Client you can install, remove, repair and configure Veeam Analytics service. For details, see Veeam Analytics Service.

Managing Signatures

If automatic signature update is enabled, and Veeam ONE server is connected to the Internet, it will connect to the Veeam Technical Support web server and update signatures automatically on a daily basis.

For details on enabling automatic signature update, see Other Settings.

Alternatively, you can manually check for an available update of signatures or import signatures from file provided by Veeam Technical Support.

Updating Signatures

To update diagnostic signatures:

1. Open Veeam ONE Web Client.

   For details, see Accessing Veeam ONE Components.

2. At the top right corner of the Veeam ONE Web Client window, click **Configuration**.
3. In the configuration menu on the left, click **Data Collection**.
4. Click **Update Signatures** in the **Veeam Intelligent Diagnostics** drop-down list.

Veeam ONE Web Client will connect to Veeam Technical Support server over the Internet, check if an update is available, and download the latest version of signatures.

Importing Signatures

If Veeam ONE Client server has no Internet connection, you can manually import the file with the latest version of signatures:

1. Obtain the `.package` file from Veeam website.
2. Open Veeam ONE Web Client.

   For details, see Accessing Veeam ONE Components.

3. At the top right corner of the Veeam ONE Web Client window, click **Configuration**.
4. In the configuration menu on the left, click **Data Collection**.
5. Click **Import Signatures** in the **Veeam Intelligent Diagnostics** drop-down list.
6. Specify a path to the `.package` file downloaded from Veeam website and click **Import**.

Performing Log Analysis

Veeam Intelligent Diagnostics is a feature that allows you to automatically detect known issues in configuration and performance of backup infrastructure.

To use **Veeam Intelligent Diagnostics**:

1. Open Veeam ONE Web Client.
2. At the top right corner of the Veeam ONE Web Client window, click **Configuration**.
3. In the configuration menu on the left, click **Data Collection**.
4. In the inventory pane, select the desired object in the **Object Name** column.
5. In the **Veeam Intelligent Diagnostics** drop-down list specify the diagnostic actions:
   - Click **Start log analysis** to start analysis.
   - Click **Stop log analysis** to stop analysis.
   - Click **Schedule** to schedule a start time for log analysis.

For details on Veeam Intelligent Diagnostics, see Veeam Intelligent Diagnostics.

Veeam Analytics service allows you to perform log analysis according to the defined schedule or manually:

- When a scheduled log analysis session starts, Veeam Analytics service analyzes Veeam Backup & Replication logs for the last 48 hours or since the last successful log analysis session (whichever is later).

  By default, Veeam Analytics service is set to perform log analysis daily at 7:00 AM. To change the default log analysis schedule, see Scheduling Automated Log Analysis.
- When you start a log analysis session manually, Veeam Analytics service analyzes Veeam Backup & Replication logs for the last 24 hours or since the last successful log analysis session (whichever is later).

  For details on starting log analysis manually, see Starting Log Analysis Manually.

> **NOTE:**
>
> If silence mode is active for the target Veeam Backup & Replication server, log analysis cannot be run manually or by schedule.

Scheduling Automated Log Analysis

To set up daily schedule for automated log analysis:

1. Open Veeam ONE Web Client.
2. At the top right corner of the Veeam ONE Web Client window, click **Configuration**.
3. In the configuration menu on the left, click **Data Collection**.
4. In the inventory pane, select the desired object from the list of Veeam Backup & Replication servers with installed Veeam Analytics service in the **Object Name** column.
5. In the **Veeam Intelligent Diagnostics** drop-down list click **Schedule**.
6. In the **Log Analysis Schedule** window, specify the time at which log analysis must start daily.

7. Click **Save**.

Starting Log Analysis Manually

1. Open Veeam ONE Web Client.
2. At the top right corner of the Veeam ONE Web Client window, click **Configuration**.
3. In the configuration menu on the left, click **Data Collection**.
4. In the inventory pane, select the desired object from the list of Veeam Backup & Replication servers with installed Veeam Analytics service in the **Object Name** column.
5. In the **Veeam Intelligent Diagnostics** drop-down list click **Start log analysis**.

Stopping Log Analysis

You can stop a session, for example, if log analysis is about to take long, and you do not want to produce workload on the production environment during business hours.

To stop log analysis:

1. Open Veeam ONE Web Client.
2. At the top right corner of the Veeam ONE Web Client window, click **Configuration**.
3. In the configuration menu on the left, click **Data Collection**.
4. In the inventory pane, select the desired object from the list of Veeam Backup & Replication servers with installed Veeam Analytics service in the **Object Name** column.
5. In the **Veeam Intelligent Diagnostics** drop-down list click **Stop log analysis**.

Veeam Backup & Replication Summary Dashboards

Veeam Backup & Replication summary dashboards serve as the 'launch point' for monitoring the backup infrastructure and data protection operations in the virtual environment. The dashboards reflect the latest state of backup, replication and SureBackup jobs, and help you analyze the performance and configuration of backup infrastructure components.

Veeam ONE Client offers the following types of summary dashboards for Veeam Backup & Replication infrastructure components:

- Backup Infrastructure Summary
- Backup Repositories Overview
- Backup Repository Summary
- Backup Proxies Overview
- Backup Proxy Summary
- WAN Accelerators Overview
- WAN Accelerator Summary
- Tape Servers Overview
- Tape Server Summary
- Cloud Repositories Overview
- Cloud Repository Summary
- Cloud Gateways Overview
- Cloud Gateway Pool Summary
- Cloud Gateway Summary

To view summary details for a specific backup infrastructure object or segment:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.
2. In the inventory pane, click **Veeam Backup & Replication**.
3. In the inventory pane, select the necessary infrastructure level.
4. Open the **Summary** tab.

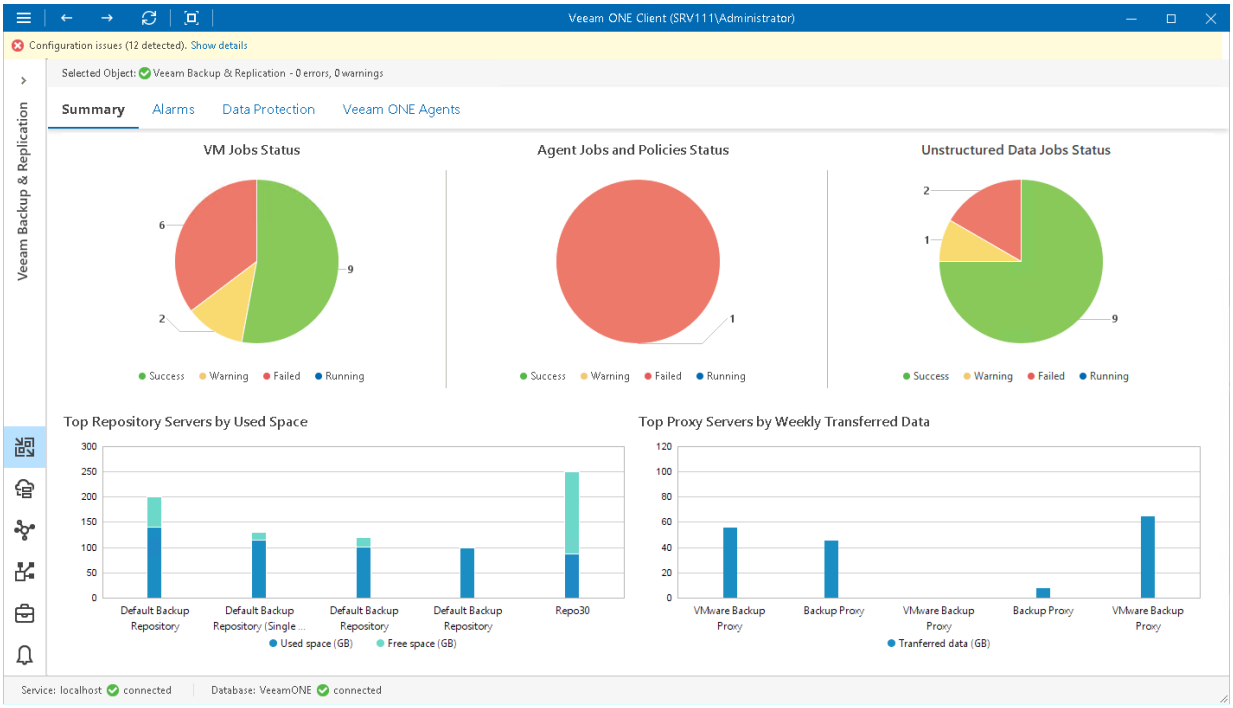
> **NOTE:**
>
> For proxy servers, repositories, WAN accelerators and tape servers, there are two summary dashboards:
>
> - **Summary** dashboards aggregate performance details for the previous week.
> - **Monthly Summary** dashboards aggregate performance details for the previous month.

Backup Infrastructure Summary

The backup infrastructure summary dashboard shows the latest state of data protection operations in the virtual environment and indicates the most intensively used resources in the backup infrastructure.

The dashboard is available for the following nodes:

- Backup Infrastructure
- Veeam Backup Enterprise Manager
- Veeam Backup & Replication server



VM Jobs Status, Agent Jobs and Policies Status, Unstructured Data Jobs Status

The charts reflect the latest status of VM protection jobs, agent protection jobs and policies, and file and object storage protection jobs for the selected level of the backup infrastructure hierarchy.

Every chart segment shows how many jobs ended with a specific status — failed jobs (red), jobs that ended with warnings (yellow), successfully performed jobs (green), and jobs that are currently running (blue). Click the necessary chart segment or a legend label to drill down to the list of jobs that ended up with the corresponding status.

For details on Veeam Backup & Replication VM job details, see Virtual Machines.

For details on Veeam Backup & Replication file and object storage job details, see Unstructured Data.

For details on Veeam Agent for Microsoft Windows, Veeam Agent for Linux, Veeam Agent for Mac and Veeam Agent for Unix jobs and policies managed by Veeam Backup & Replication servers, see Computers.

Top Repository Servers by Used Space

The chart shows 5 backup repositories with the greatest amount of used storage space.

For every repository in the chart, you can track the amount of used storage space against the amount of available space. If free space on the repository is running low, you may need to free up storage space, revise your backup retention policy or even move your backups from the repository and point backup jobs to a new location.

Top Proxy Servers by Weekly Transferred Data

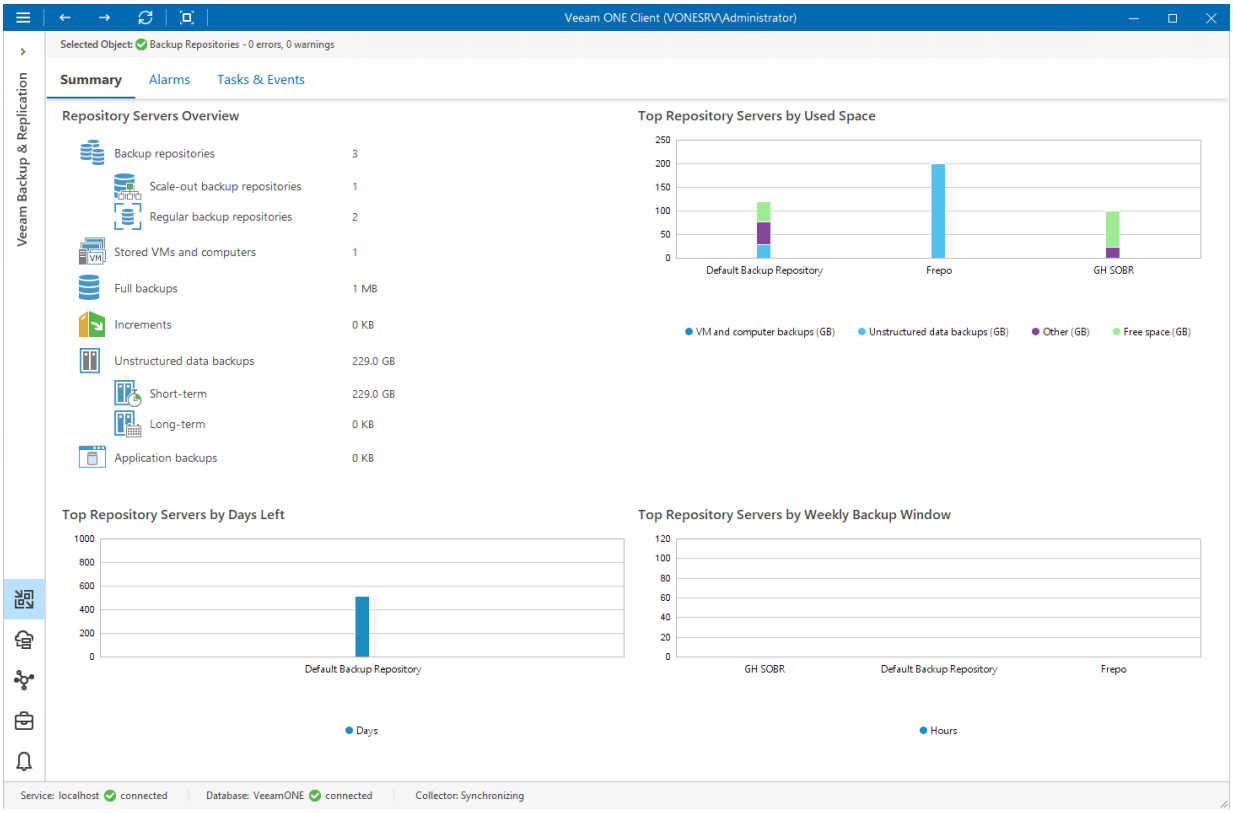
The chart shows 5 backup proxies that processed the greatest amount of data over the past 7 days.

To draw the chart, Veeam ONE analyzes how many VM disk, file share and object storage processing tasks were successfully performed by every proxy; failed tasks are not taken into account.

The chart helps you detect the most heavily loaded VM and file proxies and optimize the performance of your backup infrastructure. If specific proxies are overloaded with processing tasks, and the jobs often need to wait for proxy resources, you may need to deploy additional proxies or balance the processing load by assigning jobs to other proxies.

Backup Repositories Overview

The summary dashboard for the **Repositories** node provides a configuration overview and performance analysis for backup repositories managed by a backup server.



Repository Servers Overview

The section provides the following details:

- Number of repositories managed by the backup server
- Number of scale-out backup repositories
- Number of external repositories
- Number of object storage repositories
- Number of regular backup repositories
- Number of VMs and computers whose data is stored in backups on repositories
- Cumulative amount of storage space occupied by full VM and computer backups
- Cumulative amount of storage space occupied by incremental VM and computer backups
- Amount of space occupied by short-term and long-term unstructured data backups
- Amount of space occupied by application backups

Top Repository Servers by Used Space

The chart shows 5 backup repositories with the greatest amount of used storage space.

For every repository in the chart, you can see the amount of storage space used by VM, agent, unstructured data and application backups against the amount of available space. If free space on the repository is running low, you may need to free up storage space on the repository or revise your backup retention policy.

Top Repository Servers by Days Left

The chart shows 5 backup repositories that can run low on storage space sooner than others.

To draw the chart, Veeam ONE analyzes historical data and checks how fast free space on repositories has been decreasing in the past. Veeam ONE uses historical statistics to forecast how soon the repository will run out of space.

Top Repository Servers by Weekly Backup Window

The chart allows you to detect the most 'busy' repositories over the past 7 days.

For every repository, the chart shows the cumulative amount of time that the repository was busy with backup, backup copy and unstructured data backup job tasks.

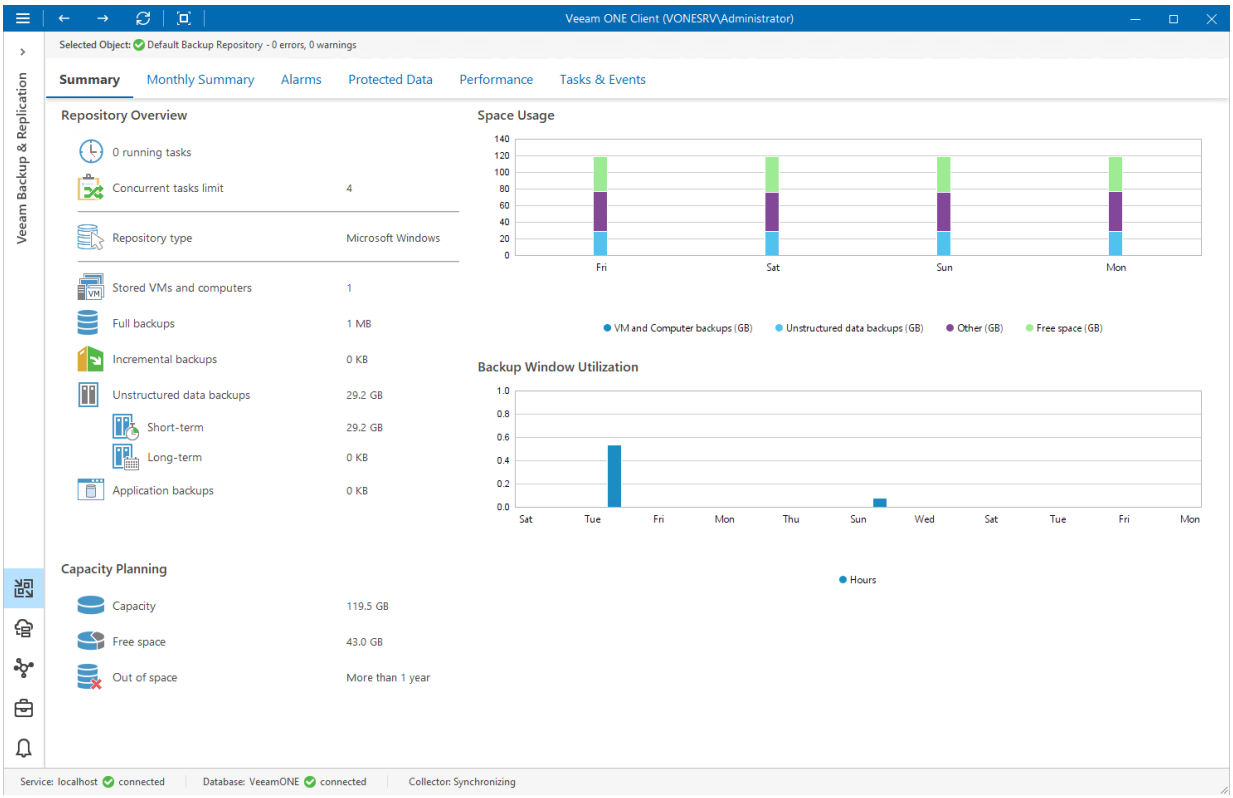
Backup Repository Summary

Veeam ONE Client offers the following types of summary dashboards for backup repositories:

- Regular backup repository summary
- Scale-out backup repository summary
- Object storage repository summary
- External repository summary

Regular Backup Repository Summary

The regular repository summary dashboard provides overview details, capacity planning information and performance analysis for a chosen backup repository for the last week or month.



Repository Overview

The section provides the following details:

- Number of tasks that are currently running on the repository
- Maximum number of concurrent tasks allowed for the repository
- Repository type
- [For Linux repositories] Immutability feature state (Enabled, Disabled, N/A)
- Number of VMs and computers whose data is stored in backups on the repository
- Cumulative amount of storage space occupied by full VM and computer backups

- Cumulative amount of storage space occupied by incremental VM and computer backups
- Cumulative amount of storage space occupied by short- and long-term unstructured data backups
- Cumulative amount of storage space occupied by enterprise application backups

Capacity Planning

The section provides the following details:

- Storage capacity of the repository
- Amount of free space on the repository
- Number of days before the repository runs out of free space

To forecast the value, Veeam ONE uses a trend that is calculated based on historical statistics — it analyzes how fast the amount of free space on the repository was decreasing in the past and uses historical statistics to forecast how soon the repository will run out of space.

Space Usage

The chart shows the amount of used storage space against the amount of available space on the repository.

If free space on the repository is running low, you may need to free up storage space on the repository, revise your backup retention policy, or consider pointing jobs to a scale-out backup repository.

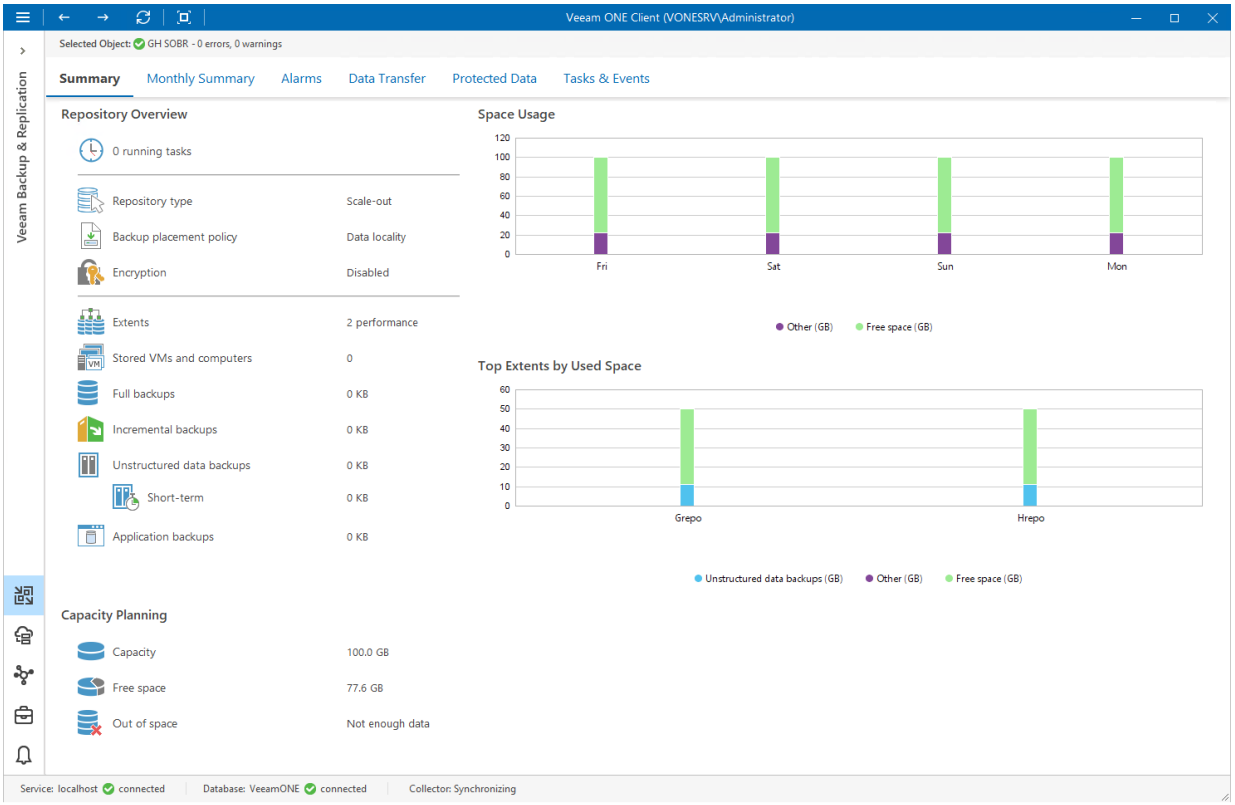
Backup Window Utilization

The chart shows the cumulative amount of time that the repository was busy with backup job tasks and backup copy job tasks during the past week or month.

The chart can help you reveal possible resource bottlenecks on the repository side. If the backup window on the chart is abnormally large, this may evidence that the required I/O operations cannot complete fast enough, and your target is presenting a bottleneck for the whole backup data processing conveyor. To identify performance bottlenecks, you can switch to repository Veeam Backup & Replication Performance Charts.

Scale-Out Backup Repository Summary

The scale-out repository summary dashboard provides overview details, capacity planning information and performance analysis for a chosen scale-out backup repository for the last week or month. You can select underlying scale-out repository extents to see details of performance, capacity and archive tiers. For details on scale-out repository configuration, see section Scale-Out Backup Repository of the Veeam Backup & Replication User Guide.



Repository Overview

The section provides the following details:

- Number of tasks that are currently running on the repository
- Repository type (Scale-out backup repository)
- Backup placement policy (as configured in the scale-out repository settings)
- Copy policy (as configured in the capacity tier settings)
- Move policy (as configured in the capacity tier settings)
- Archiving policy (as configured in the archive tier settings)
- Number of performance, capacity and archive tier extents that make up the scale-out backup repository
- Number of VMs and computers whose data is stored in backups on the repository
- Cumulative amount of storage space occupied by full VM and computer backups
- Cumulative amount of storage space occupied by incremental VM and computer backups
- Cumulative amount of storage space occupied by short- and long-term unstructured data backups

- Cumulative amount of storage space occupied by enterprise application backups

Capacity Planning

The section provides the following details:

- Storage capacity of the repository
- Amount of free storage space on the repository
- Number of days before the repository runs out of free space.

To forecast the value, Veeam ONE uses a trend that is calculated based on historical statistics — it analyzes how fast the amount of free space on the repository was decreasing in the past and uses historical statistics to forecast how soon the repository will run out of space.

Space Usage

The chart shows the amount of used storage space against the amount of available space on the repository.

If free space on the repository is running low, you may need to free up storage space on the repository, revise your backup retention policy, or consider pointing jobs to another repository.

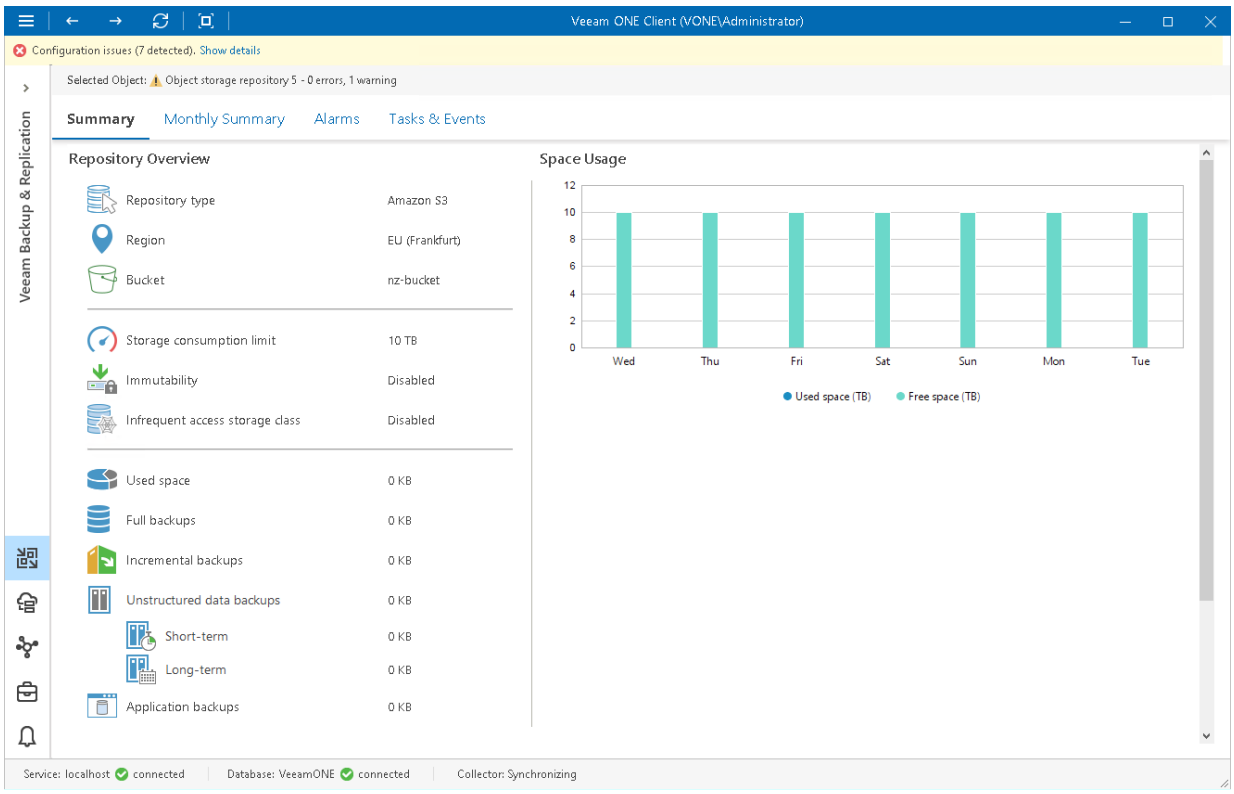
Top Extents by Used Space

The chart shows extents with the greatest amount of used storage space.

For every extent in the chart, you can see the amount of used storage space against the amount of available space.

Object Storage Repository Summary

The object storage repository summary dashboard provides overview details and performance analysis for a chosen object storage repository added as a Capacity Tier for the last week or month.



Repository Overview

The section provides the following details:

- Repository type
- Region at which the repository is located
- Name of bucket or container
- Limit of storage consumption
- Immutability feature state (Enabled, Disabled, N/A)
- Class of the infrequent access storage
- Cumulative amount of storage space occupied by full and incremental VM and computer backups
- Cumulative amount of storage space occupied by short- and long-term unstructured data backups

Capacity Planning

The section provides the following details:

- Storage capacity of the repository
- Amount of free storage space on the repository
- Number of days before the repository runs out of free space.

To forecast the value, Veeam ONE uses a trend that is calculated based on historical statistics — it analyzes how fast the amount of free space on the repository was decreasing in the past and uses historical statistics to forecast how soon the repository will run out of space.

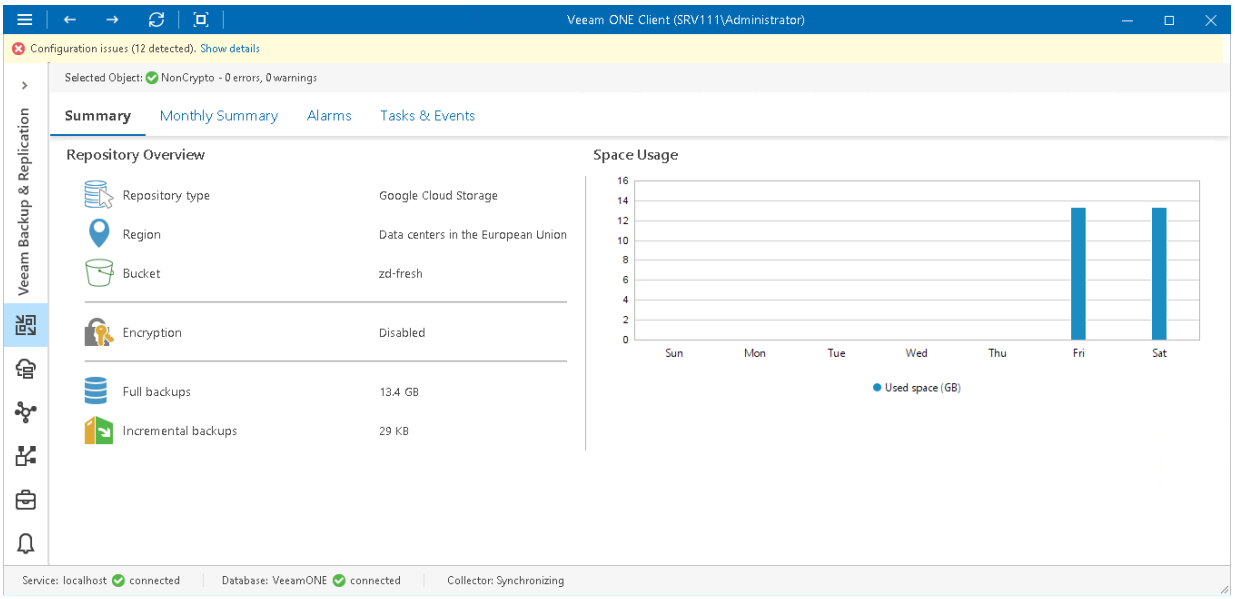
Space Usage

The chart shows the amount of used storage space against the amount of available space on the repository.

If free space on the repository is running low, you may need to free up storage space on the repository, revise your backup retention policy, or consider pointing jobs to another repository.

External Repository Summary

The external repository summary dashboard provides overview details and performance analysis for a chosen external repository for the last week or month.



Repository Overview

The section provides the following details:

- Repository type
- Region at which the repository is located
- Name of a bucket or container
- Number of cloud VMs whose data is stored in backups on the repository
- Cumulative amount of storage space occupied by full cloud VM backups
- Cumulative amount of storage space occupied by incremental cloud VM backups
- Encryption settings (as configured in the external repository settings)

Space Usage

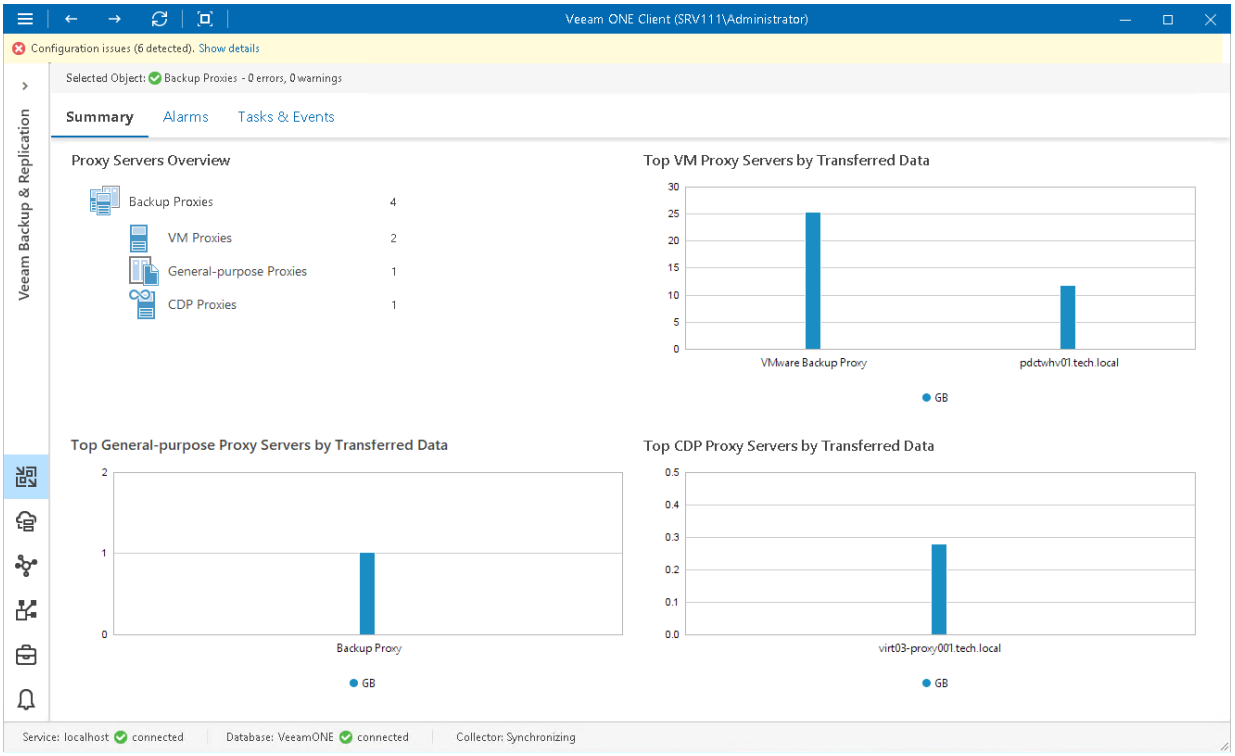
The chart shows the amount of storage space used by the files on the repository.

If the space consumed on the repository is running high, you may need to free up storage space on the repository, revise your backup retention policy, or consider using another repository.

Backup Proxies Overview

The summary dashboard for the **Proxies** node provides a configuration overview and performance analysis for VM, general-purpose and CDP proxies managed by a backup server.

This dashboard can help you detect configuration inefficiencies in your data protection infrastructure. If the same proxy server appears to process a great number of disks, transfer the greatest amount of backup data and use the largest backup window, you may need to re-balance the processing load across your backup proxies. The charts may also help you reveal 'lazy' proxies that you may decide to decommission.



Proxy Servers Overview

The section shows the breakdown of backup proxies by the proxy type (*VM Proxies*, *General-purpose Proxies*, *CDP Proxies*).

Top VM Proxy Servers by Transferred Data

The chart shows 5 backup proxies that transferred the greatest amount of backup data to the target destination (backup repository or replica datastore/volume) over the past 7 days.

For every backup proxy, the chart shows the total amount of data that the proxy transferred over the network after the source-side deduplication and compression. The chart can help you detect backup proxies that transfer the greatest amount of backup data and estimate the load that backup and replication jobs impose on the network.

Top General-purpose Proxy Servers by Transferred Data

The chart shows 5 file proxies that transferred the greatest amount of backup data to the target destination (backup repository) over the last 7 days.

For every backup proxy, the chart shows the total amount of data that the proxy transferred over the network after the source-side deduplication and compression. The chart can help you detect backup proxies that transfer the greatest amount of backup data and estimate the load that unstructured data backup jobs impose on the network.

Top CDP Proxy Servers by Transferred Data

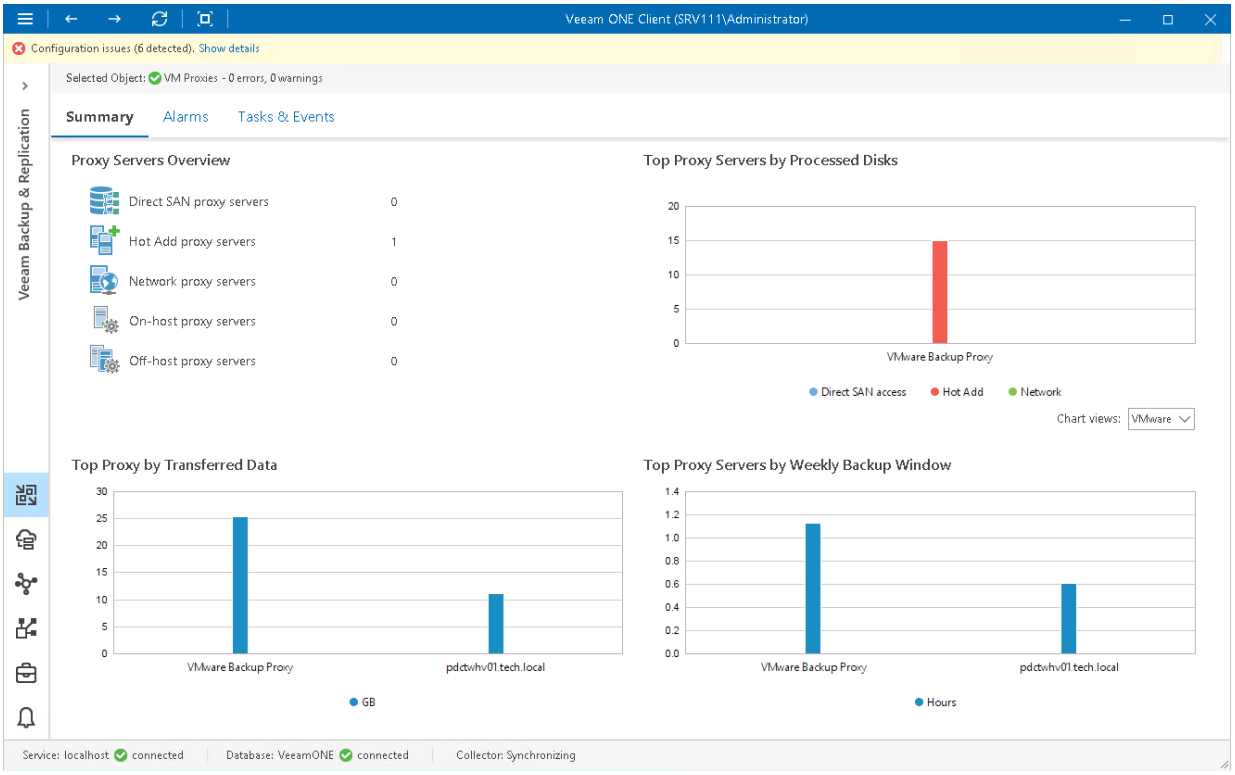
The chart shows 5 CDP proxies that transferred the greatest amount of VM data to the target host over the last 7 days.

For every proxy, the chart shows the total amount of data that the proxy transferred over the network after the source-side deduplication and compression. The chart can help you detect proxies that transfer the greatest amount of data and estimate the load that CDP sessions impose on the network.

VM Proxy Servers Overview

The summary dashboard for the **VM Proxies** node provides a configuration overview and performance analysis for VM proxies and file proxies managed by a backup server.

> **NOTE:**
>
> Veeam Cloud Connect service providers cannot see performance data for proxies used by tenant data protection jobs.



Proxy Servers Overview

The section shows the breakdown of backup proxies by the transport or backup mode:

- [VMware vSphere] You can see how many VMware backup proxies retrieve VM data from source datastores using the Direct SAN Access, Hot Add or Network transport mode.

  If a backup proxy uses different modes to retrieve VM data from various source datastores, Veeam ONE will detect its primary transport mode quantitatively, based on the number of processed VM disks. For example, if a backup proxy processed 10 VM disks using the Hot Add mode and 20 VM disks using the Network mode, the proxy would be reported as a 'Network proxy server'.

- [Microsoft Hyper-V] You can see how many Hyper-V proxies retrieve and process VM data in the on-host and off-host backup modes.

Top Proxy Servers by Processed Disks

The chart shows 5 backup proxies that processed the greatest number of VMs over the past 7 days.

To draw the chart, Veeam ONE analyzes how many VM processing tasks were successfully performed by every proxy; failed tasks are not taken into account.

The chart helps you detect the most heavily loaded backup proxies and optimize the performance of your backup infrastructure. If specific proxies are overloaded with VM processing tasks, and the tasks often need to wait for proxy resources, you may need to deploy additional proxies or balance the processing load by assigning jobs to other proxies.

You can use the **Chart views** list to view the number of VMs processed by VMware and Hyper-V backup proxies.

Top Proxy by Transferred Data

The chart shows 5 backup proxies that transferred the greatest amount of backup data to the target destination (backup repository or replica datastore/volume) over the past 7 days.

For every backup proxy, the chart shows the total amount of data that the proxy transferred over the network after the source-side deduplication and compression. The chart can help you detect backup proxies that transfer the greatest amount of backup data and estimate the load that backup and replication jobs impose on the network.

Top Proxy Servers by Weekly Backup Window

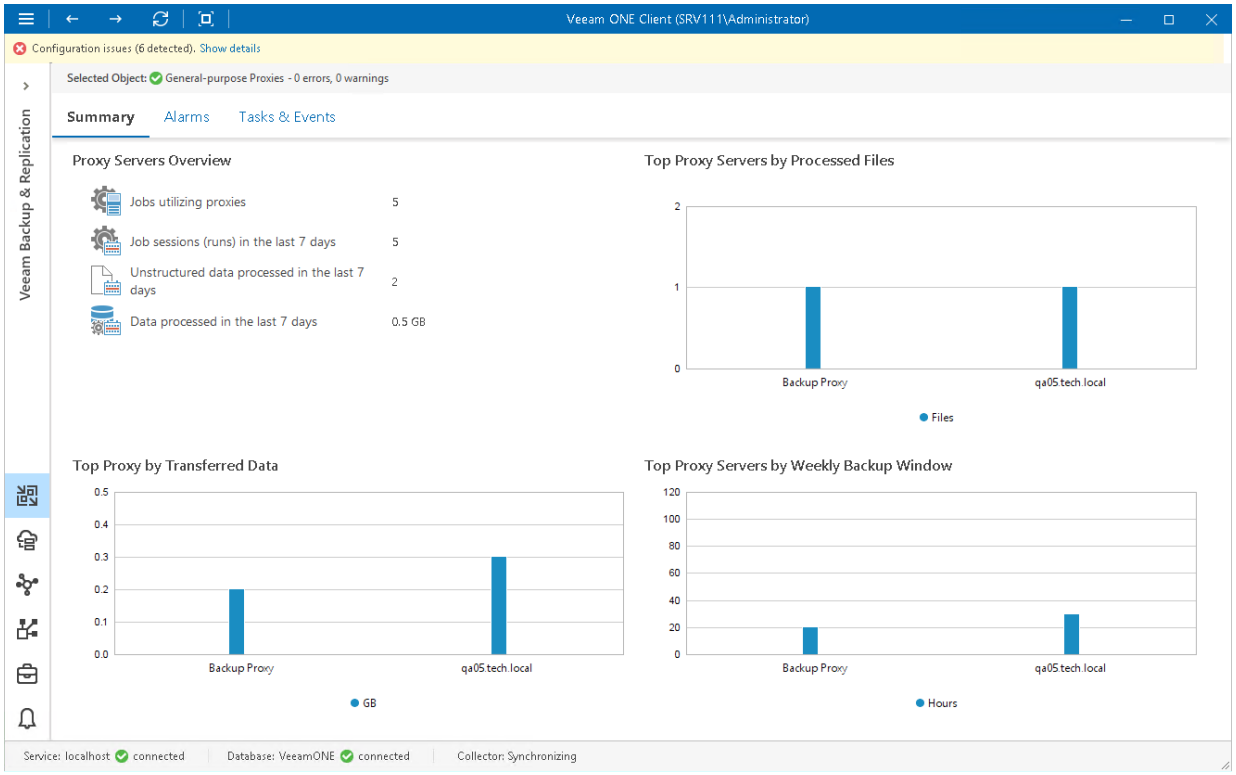
The chart allows you to detect the most 'busy' proxy servers over the past 7 days.

For every proxy, the chart shows the cumulative amount of time that the proxy was retrieving, processing and transferring VM data.

The chart can help you reveal possible resource bottlenecks. If the backup window on the chart is abnormally large, this can evidence of low source data retrieval speed, high proxy CPU load or insufficient network throughput.

General-Purpose Proxy Servers Overview

The summary dashboard for the **General-purpose Proxies** node provides a configuration overview and performance analysis for general-purpose proxies managed by a backup server.



Proxy Servers Overview

The section provides the following details:

- Number of file backup jobs configured to use proxies
- Number of job sessions that the proxies have processed during the last 7 days
- Number of unstructured data items that the proxies have processed during the last 7 days
- Total amount of data that the proxy has processed during the last 7 days

Top Proxy Servers by Processed Items

The chart shows 5 file proxies that processed the greatest number of unstructured data items over the last 7 days.

To draw the chart, Veeam ONE analyzes how many items were successfully processed by every proxy.

The chart helps you detect the most heavily loaded general-purpose proxies and optimize the performance of your backup infrastructure. If specific proxies are overloaded with unstructured data processing tasks, and the tasks often need to wait for proxy resources, you may need to deploy additional proxies or balance the processing load by assigning jobs to other proxies.

Top Proxy by Transferred Data

The chart shows 5 proxies that transferred the greatest amount of backup data to the target destination (backup repository) over the last 7 days.

For every proxy, the chart shows the total amount of data that the proxy transferred over the network after the source-side deduplication and compression. The chart can help you detect backup proxies that transfer the greatest amount of backup data and estimate the load that file backup jobs impose on the network.

Top Proxy Servers by Weekly Backup Window

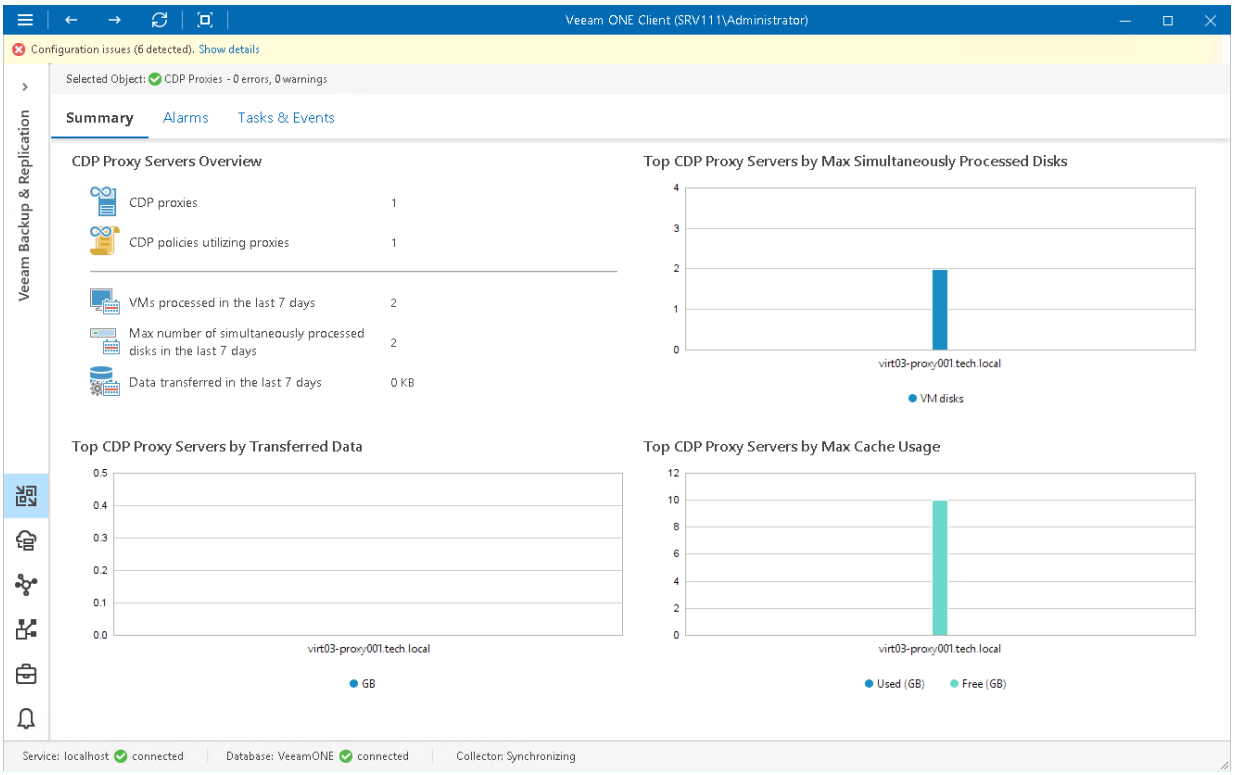
The chart allows you to detect the most 'busy' proxy servers over the last 7 days.

For every proxy, the chart shows the cumulative amount of time that the proxy was retrieving, processing and transferring unstructured data.

The chart can help you reveal possible resource bottlenecks. If the backup window on the chart is abnormally large, this can evidence of low source data retrieval speed, high proxy CPU load or insufficient network throughput.

CDP Proxy Servers Overview

The summary dashboard for the **CDP Proxies** node provides a configuration overview and performance analysis for CDP proxies managed by a backup server.



CDP Proxy Servers Overview

The section provides the following details:

- Number of CDP proxies configured on the backup server.
- Number of CDP policies configured to use proxies
- Number of VMs that CDP proxies have processed in the last 7 days
- Maximum number of VM disks that proxies have simultaneously processed in the last 7 days
- Total amount of data that proxies have processed during the last 7 days

Top CDP Proxy Servers by Max Simultaneously Processed Disks

The chart shows 5 CDP proxies that simultaneously processed the greatest number of VM disks over the last 7 days.

To draw the chart, Veeam ONE analyzes how many disks were successfully processed by every proxy.

The chart helps you detect the most heavily loaded CDP proxies and optimize the performance of your backup infrastructure. If specific proxies are overloaded with disk processing tasks, and the tasks often need to wait for proxy resources, you may need to deploy additional proxies or balance the processing load by assigning policies to other proxies.

Top CDP Proxy Servers by Transferred Data

The chart shows 5 CDP proxies that transferred the greatest amount of VM data to the target host over the last 7 days.

For every proxy, the chart shows the total amount of data that the proxy transferred over the network after the source-side deduplication and compression. The chart can help you detect proxies that transfer the greatest amount of data and estimate the load that CDP sessions impose on the network.

Top CDP Proxy Servers by Max Cache Usage

The chart shows 5 CDP proxies that used the maximum amount of space allocated for storing cache over the last 7 days.

For every proxy, the chart shows the amount of free and used space allocated for cache storage. The chart can help you detect proxies that store the greatest amount of temporary cached data and estimate which proxies require allocating more storage space.

Backup Proxy Summary

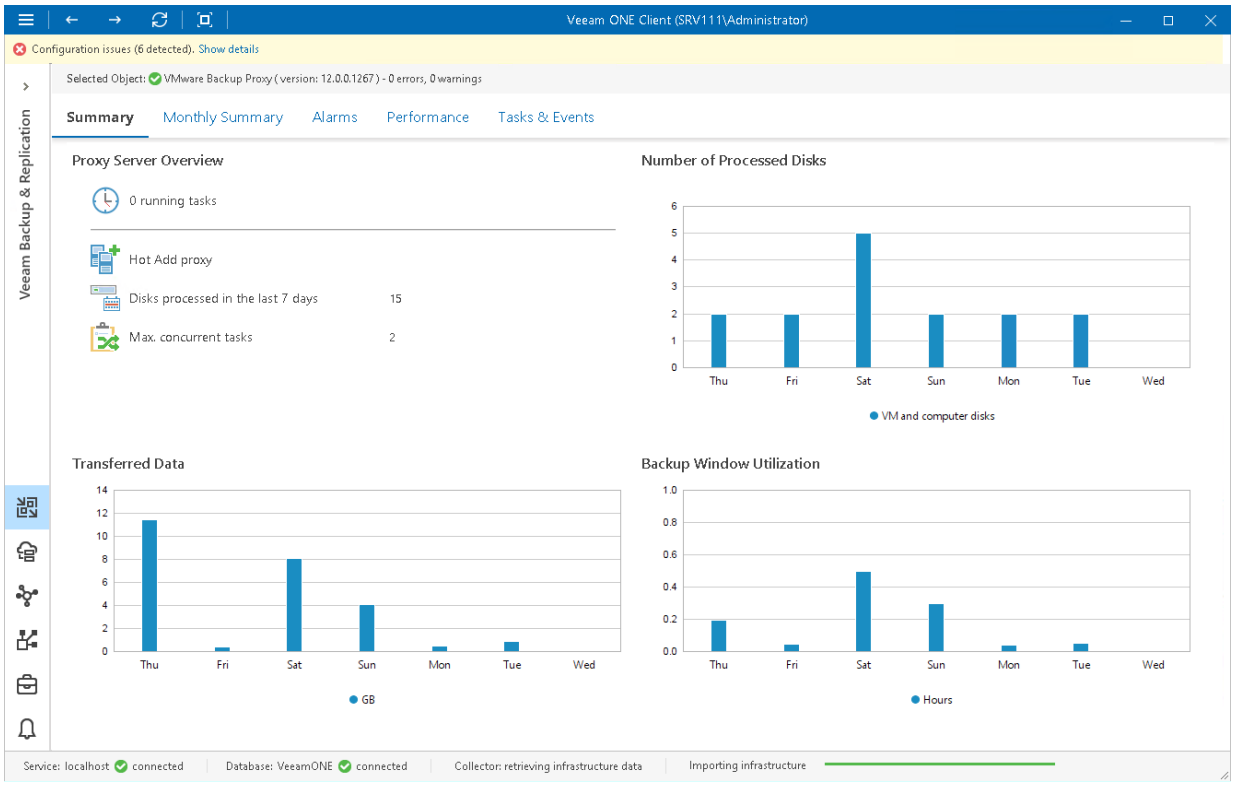
Veeam ONE Client offers the following types of summary dashboards for proxy servers:

- VM proxy summary
- General-purpose proxy summary
- CDP proxy summary

VM Proxy Summary

The VM proxy summary dashboard provides overview details and performance analysis for a chosen VM backup proxy for the last week or month.

> **NOTE:**
>
> Veeam Cloud Connect service providers cannot see performance data for proxies used by tenant data protection jobs.



Proxy Server Overview

The section provides the following details:

- Number of tasks that the proxy is currently processing
- Mode that the proxy uses to process VM disks (Direct SAN Access, Hot Add or Network for VMware backup proxies; on-host or off-host for Hyper-V proxies)
- Number of VM disks that the proxy has processed during the last 7 days

- Number of concurrent VM disk processing tasks that can be assigned to the proxy (as configured in proxy settings)

Number of Processed Disks

The chart shows how many VM disks the proxy processed over the last 7 days.

To draw the chart, Veeam ONE Client analyzes how many disk processing tasks were successfully performed by the proxy; failed tasks are not taken into account.

The chart helps you to analyze workload on the proxy and optimize the performance of your backup infrastructure. If the proxy is overloaded with processing tasks, and the tasks often need to wait for the proxy resources, you may need to deploy additional proxies or balance the processing load by assigning jobs to other proxies.

Transferred Data

The chart shows the amount of backup data that the proxy transferred to the target destination (backup repository or replica, datastore/volume) over the last 7 days.

The chart shows the total amount of data that the proxy transferred over the network after the source-side deduplication and compression. The chart can help you measure the amount of backup traffic coming from the proxy.

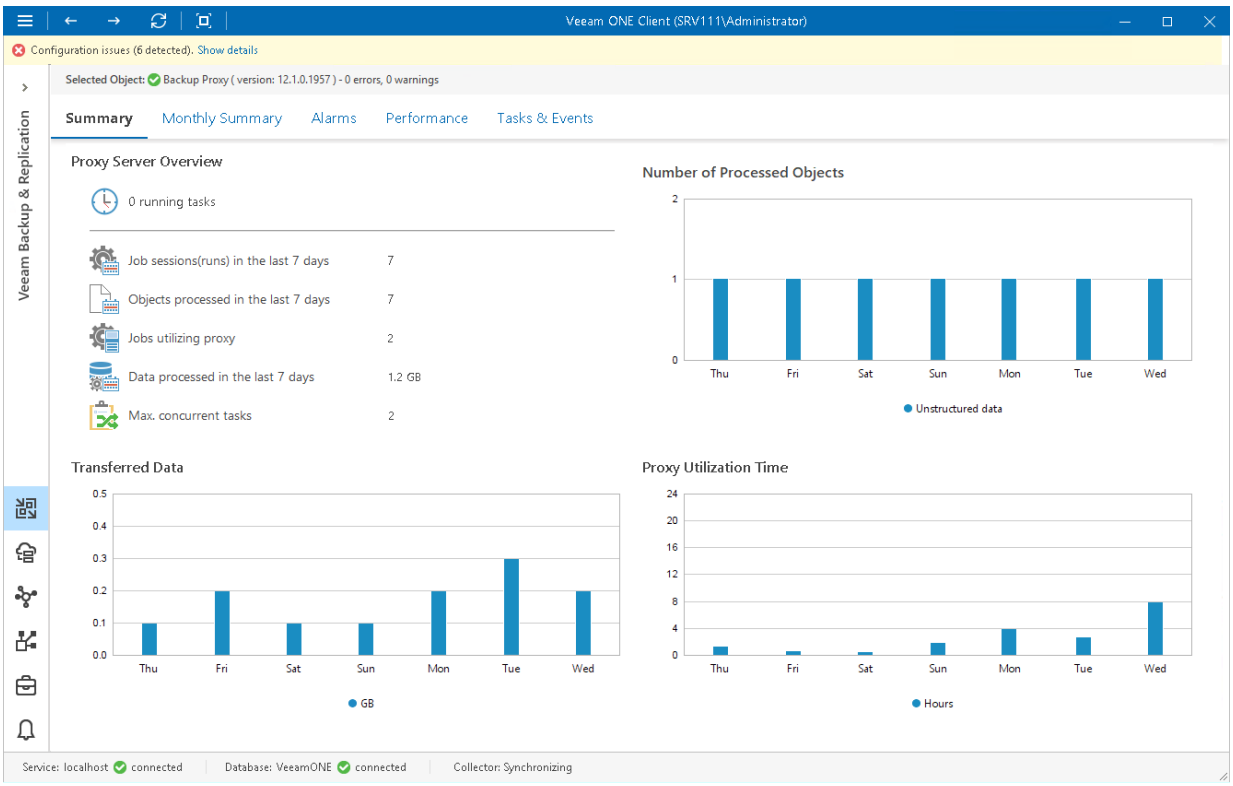
Backup Window Utilization

The chart allows you to estimate how 'busy' the proxy was during the last 7 days. The chart shows the cumulative amount of time that the proxy was retrieving, processing and transferring VM data.

The chart can help you reveal possible resource bottlenecks. If the backup window on the chart is abnormally large, this can evidence of low source data retrieval speed, high proxy CPU load or insufficient network throughput. To identify performance bottlenecks, you can switch to proxy Veeam Backup & Replication Performance Charts.

General-Purpose Proxy Summary

The general-purpose proxy summary dashboard provides overview details and performance analysis for a chosen general-purpose proxy for the last week or month.



Proxy Server Overview

The section provides the following details:

- Number of tasks that the proxy is currently processing
- Number of job sessions that the proxy has processed during the last 7 days
- Number of objects that the proxy has processed during the last 7 days
- Number of file and object storage backup jobs configured to use the proxy
- Total amount of data that the proxy has processed during the last 7 days
- Number of concurrent object processing tasks that can be assigned to the proxy (as configured in proxy settings)

Number of Processed Files

The chart shows how many objects the proxy processed over the last 7 days.

To draw the chart, Veeam ONE Client analyzes how many objects were successfully processed by the proxy.

The chart helps you to analyze workload on the proxy and optimize the performance of your backup infrastructure. If the proxy is overloaded with processing tasks, and the tasks often need to wait for the proxy resources, you may need to deploy additional proxies or balance the processing load by assigning jobs to other proxies.

Transferred Data

The chart shows the amount of backup data that the proxy transferred to the target destination (backup repository) over the last 7 days.

The chart shows the total amount of data that the proxy transferred over the network after the source-side deduplication and compression. The chart can help you measure the amount of backup traffic coming from the proxy.

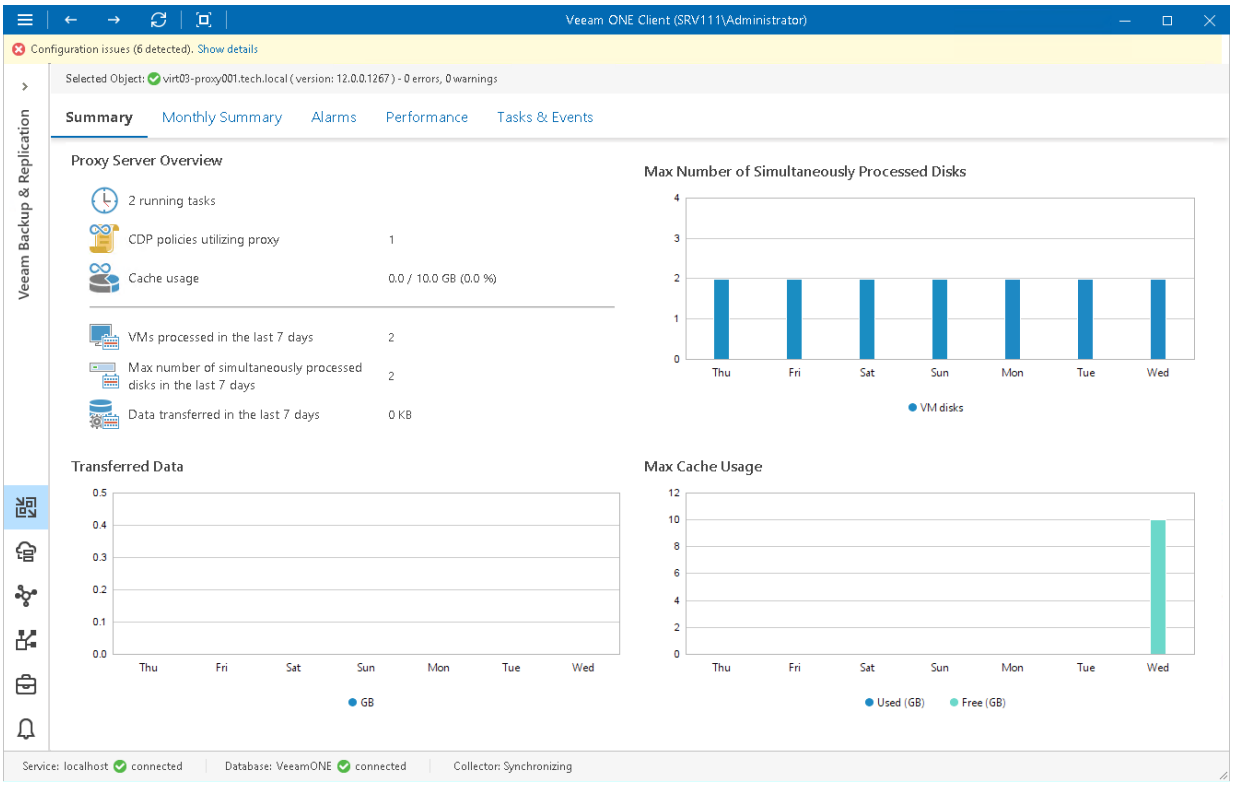
Proxy Utilization Time

The chart allows you to estimate how 'busy' the proxy was during the last 7 days. The chart shows the cumulative amount of time that the proxy was retrieving, processing and transferring file share data.

The chart can help you reveal possible resource bottlenecks. If the utilization time on the chart is abnormally large, this can evidence of low source data retrieval speed, high proxy CPU load or insufficient network throughput. To identify performance bottlenecks, you can switch to proxy Veeam Backup & Replication Performance Charts.

CDP Proxy Summary

The CDP proxy summary dashboard provides overview details and performance analysis for a chosen CDP proxy for the last week or month.



Proxy Server Overview

The section provides the following details:

- Number of tasks that the proxy is currently processing
- Number of CDP policies configured to use the proxy

- Total amount of cache data used by the proxy
- Number of VMs that the proxy has processed in the last 7 days
- Maximum number of VM disks that the proxy has simultaneously processed in the last 7 days
- Total amount of data that the proxy has processed during the last 7 days

Max Number of Simultaneously Processed Disks

The chart shows how many VM disks the proxy processed over the last 7 days.

To draw the chart, Veeam ONE Client analyzes how many VM disks were successfully processed by the proxy.

The chart helps you to analyze workload on the proxy and optimize the performance of your backup infrastructure. If the proxy is overloaded with processing tasks, and the tasks often need to wait for the proxy resources, you may need to deploy additional proxies or balance the processing load by assigning jobs to other proxies.

Transferred Data

The chart shows the amount of VM data that the proxy transferred to the target host over the last 7 days.

The chart shows the total amount of data that the proxy transferred over the network after the source-side deduplication and compression. The chart can help you measure the amount of traffic coming from the proxy.

Max Cache Usage

The chart shows the amount of temporary cached data that the proxy offloaded to the cache folder and the amount of free space in this folder over the last 7 days. If the size of the offloaded cache changed during the day, the chart will show the maximum size.

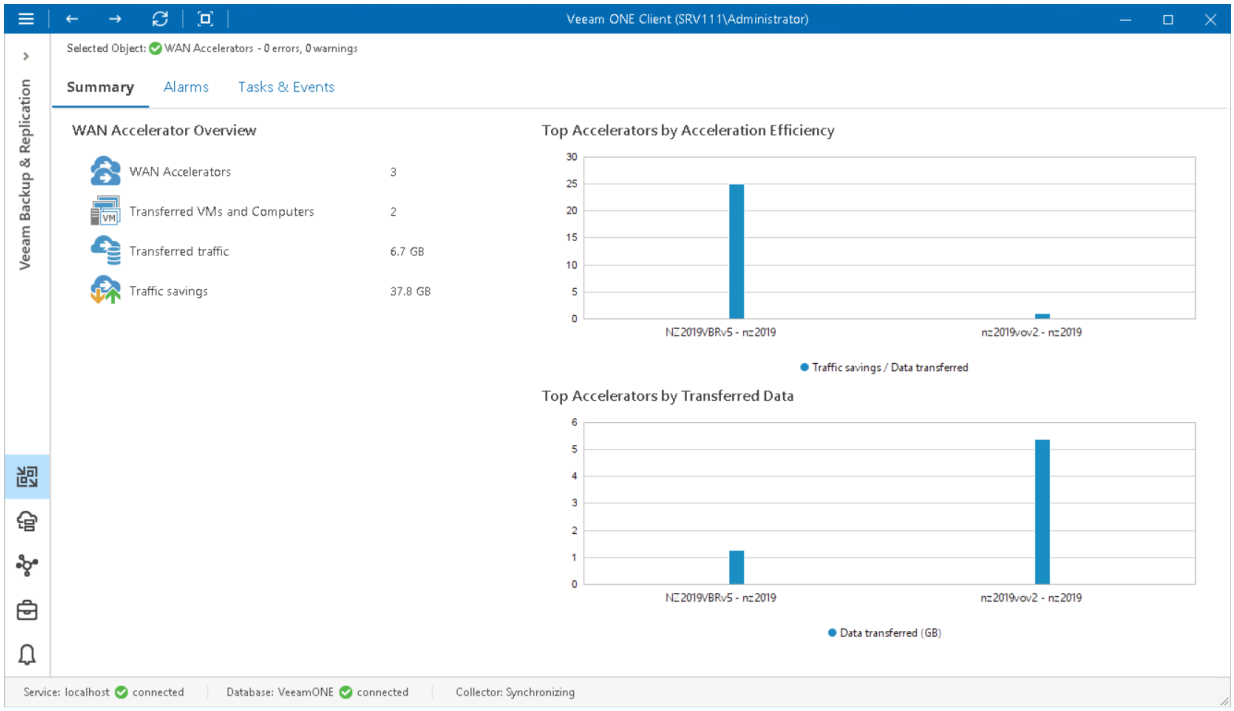
The chart can help you analyze how data blocks of continuously replicated VMs change during the week and estimate if the proxy require allocating more storage space.

WAN Accelerators Overview

The summary dashboard for the **WAN Accelerators** node provides a configuration overview and performance analysis for WAN accelerators managed by a backup server.

> **NOTE:**
>
> For WAN accelerators used in Veeam Cloud Connect jobs, performance data is available only if the target WAN accelerator is present in the Veeam ONE infrastructure.

Charts in this dashboard can help you estimate the efficiency of VM and computer data transfer over WAN links. Comparing the amount of transferred and saved traffic, you can measure how the amount of VM and computer traffic was reduced by means of Veeam WAN acceleration.



WAN Accelerator Overview

The section provides the following details:

- Number of WAN accelerators managed by the backup server
- Number of VMs and computers stored in restore points transferred by WAN accelerators during backup copy job and replication job sessions
- Cumulative amount of network traffic transferred by WAN accelerators to the target destination (secondary repositories or replica datastore/volume)
- Cumulative amount of saved traffic — that is, the difference between the amount of VM or computer data that was read from the source location (source repository or datastore/volume) and the amount of data that was actually transferred to the target destination (secondary repository or replica datastore/volume)

Top Accelerators by Acceleration Efficiency

The chart shows 5 pairs of WAN accelerators that saved the greatest amount of traffic over the past 7 days.

To draw the chart, Veeam ONE analyzes the difference between the amount of VM or computer data read from the source location (source repository or datastore/volume) and the amount of data that was actually transferred to the target destination (secondary repository or replica datastore/volume) over the past 7 days.

Top Accelerators by Transferred Data

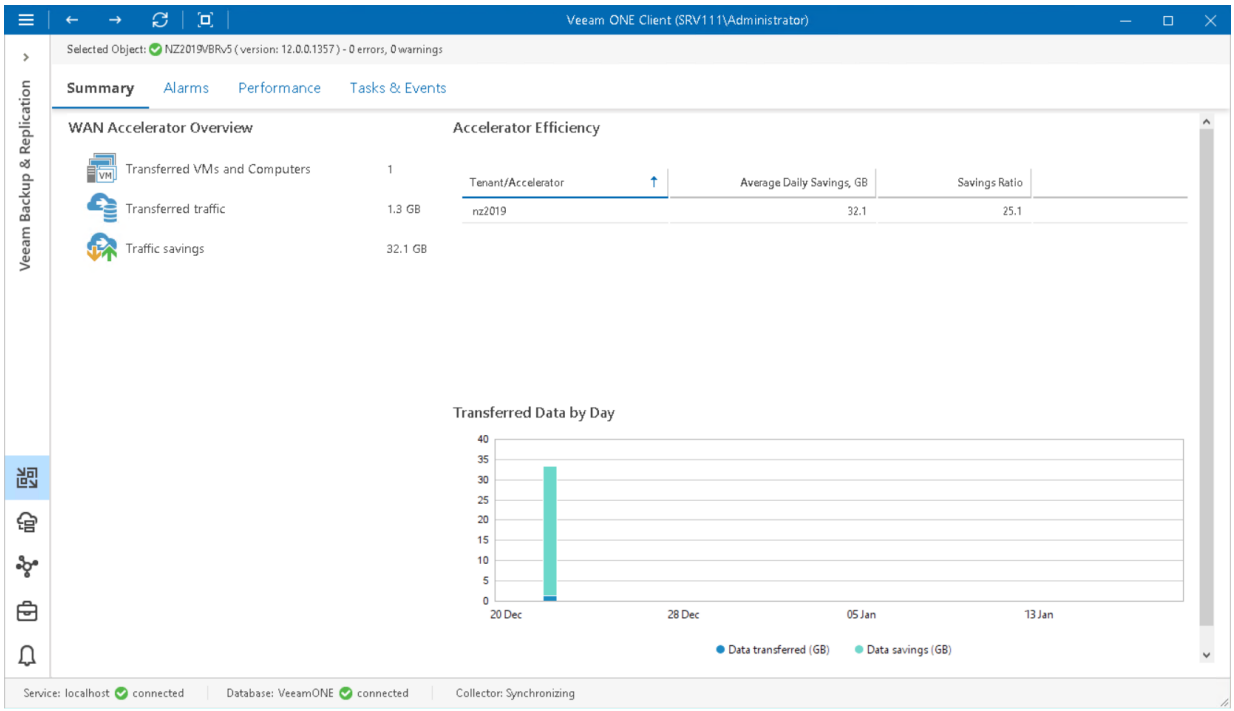
The chart shows 5 pairs of WAN accelerators that transferred the greatest amount of VM and computer data over the past 7 days.

Every graph in the chart shows the total amount of VM and computer data that was sent from the source-side accelerator to the target-side accelerator over the network.

WAN Accelerator Summary

The WAN accelerator summary dashboard presents overview details and performance analysis for the chosen WAN accelerator.

> **NOTE:**
>
> For WAN accelerators used in Veeam Cloud Connect jobs, performance data is available only if the target WAN accelerator is present in the Veeam ONE infrastructure.



WAN Accelerator Overview

The section provides the following details:

- Number of VMs and computers stored in restore points transferred or received by the WAN accelerator during backup copy job or replication job sessions.

  If the same server acts as a target- and source-side accelerator at the same time, the dashboard will show aggregate values for transferred and received restore points.

- Amount of network traffic transferred from the accelerator to target.
- Amount of saved traffic — the difference between the amount of VM and computer data that was read from the source location (source repository or datastore/volume) and the amount of data that was actually transferred to the target destination (secondary repository or replica datastore/volume).

Accelerator Efficiency

The chart shows WAN accelerators that saved the greatest amount of traffic over the past period.

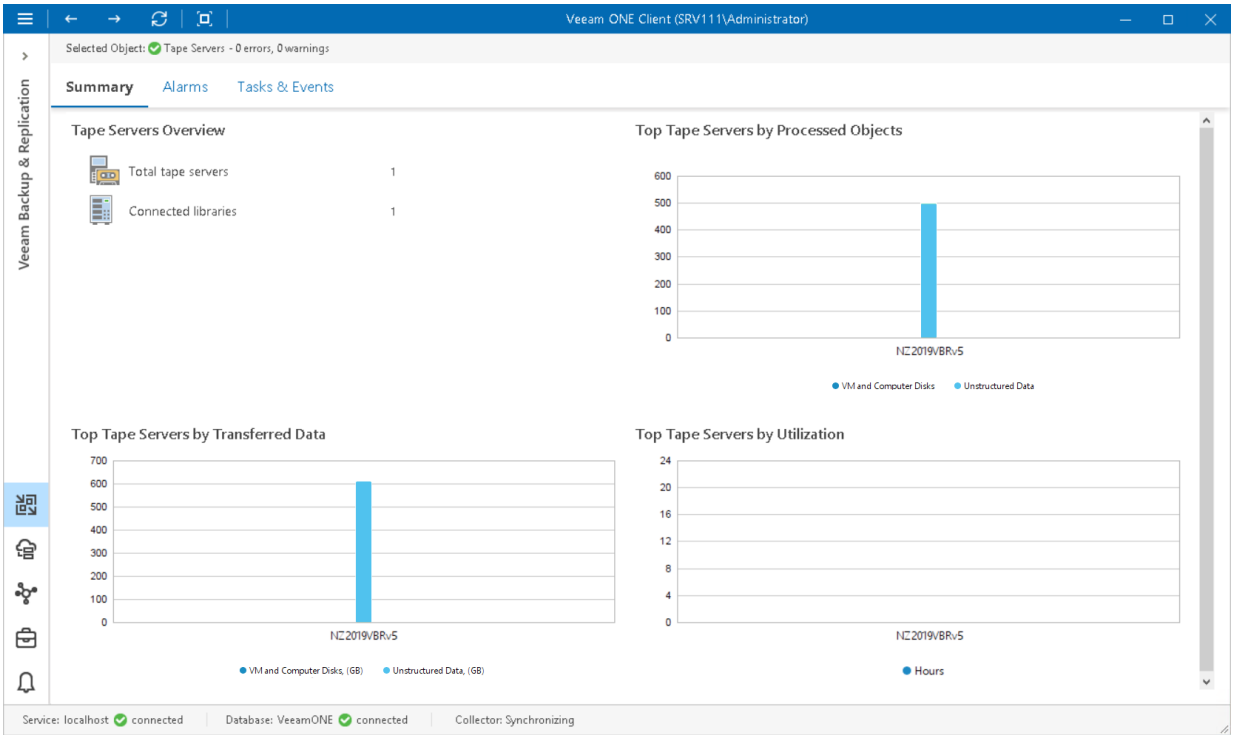
The chart lists tenant or accelerator IP, the average amount of traffic the accelerator saves daily in GB, and the ratio between the amount of VM and computer data read from the source location and the amount of data that was transferred to the destination.

Transferred Data by Day

The chart shows the amount of VM and computer data that was read from the source location (source repository or datastore/volume) and the amount of data that was actually transferred to the target destination (secondary repository or replica datastore/volume) over the past period.

Tape Servers Overview

The summary dashboard for the **Tape Servers** node presents a configuration overview and performance analysis for tape servers managed by a backup server.



Tape Servers Overview

The section shows the number of tape servers managed by a Veeam Backup & Replication server, and tape libraries connected to these servers.

Top Tape Servers by Processed Objects

The chart shows 5 tape servers that processed and archived to tape the greatest number of VM and computer disks and unstructured data items over the past 7 days. To draw the chart, Veeam ONE calculates the total number of VM and computer disks and unstructured data items in all backup restore points archived to tape.

Top Tape Servers by Transferred Data

The chart shows 5 tape servers that transferred the greatest amount of data to tape devices over the past 7 days.

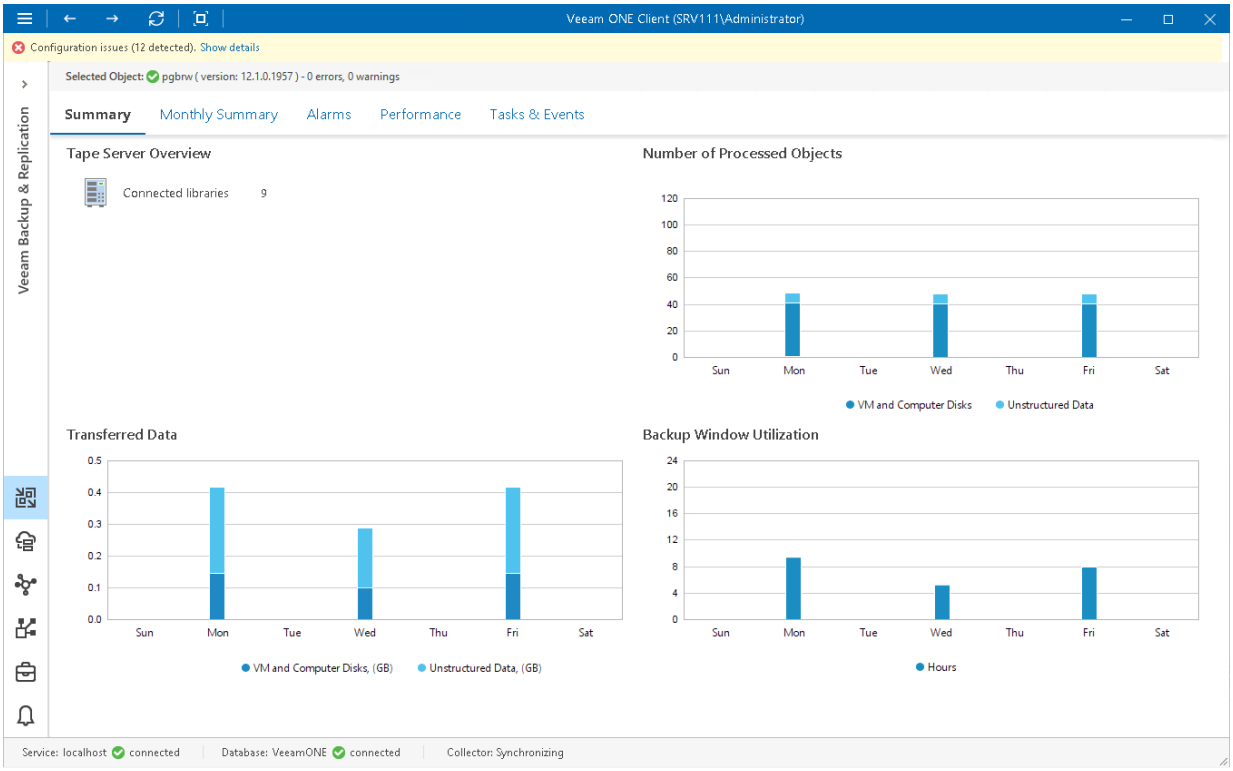
Top Tape Servers Utilization

The chart allows you to detect the most 'busy' tape servers over the past 7 days. For every tape server, the chart shows the cumulative amount of time that the server was retrieving, processing and transferring data.

The chart can help you reveal possible resource bottlenecks. If the graph on the chart is abnormally large, this can evidence of low data retrieval speed, high CPU load or insufficient network throughput.

Tape Server Summary

The tape server summary dashboard provides overview information and performance analysis for the chosen tape server.



Tape Server Overview

The section outlines the number of tape libraries connected to the tape server.

Number of Processed Objects

The chart shows how many VM and computer disks and unstructured data items the tape server processed and archived to tape over the past 7 days. To draw the chart, Veeam ONE calculates the total number of VM and computer disks and unstructured data items in all backup restore points archived to tape.

Transferred Data

The chart shows the amount of data that the tape server transferred to tape devices over the past 7 days. The chart can help you measure the amount of traffic coming from the tape server.

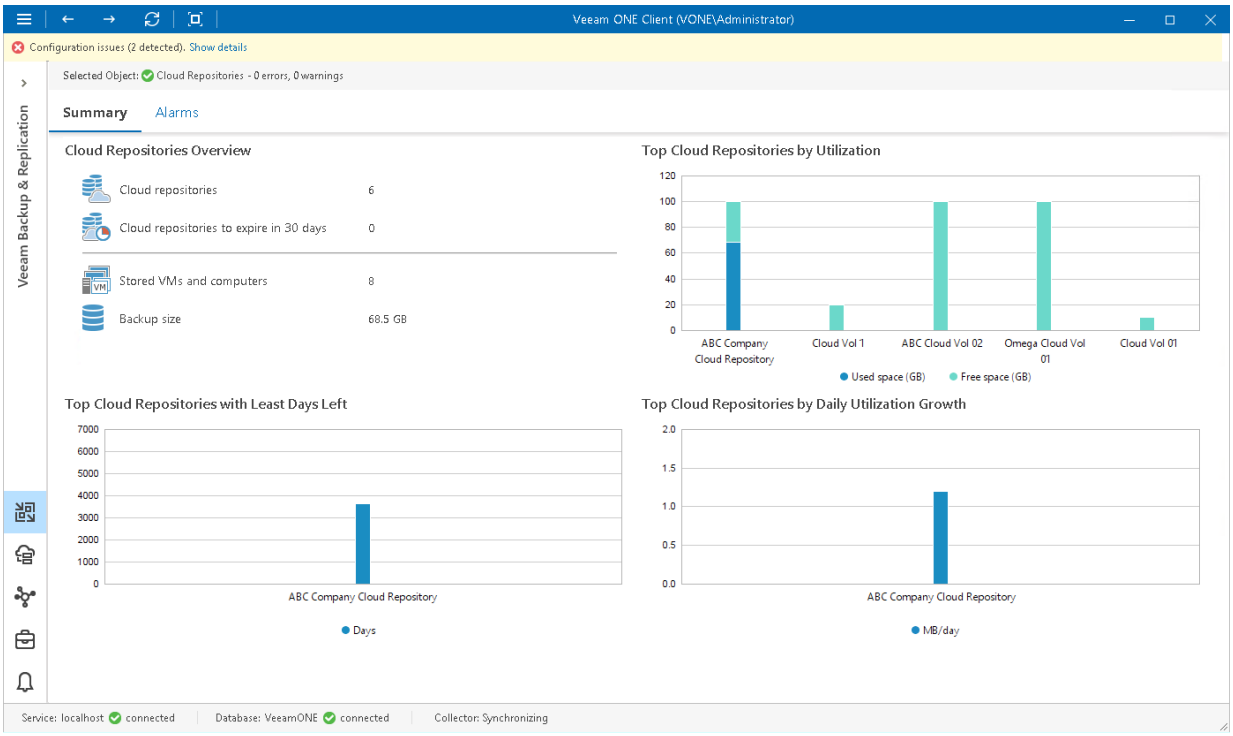
Backup Window Utilization

The chart allows you to estimate how 'busy' the tape server was during the past 7 days. The chart shows the cumulative amount of time that the tape server was retrieving, processing and transferring data.

The chart can help you reveal possible resource bottlenecks. If the backup window on the chart is abnormally large, this can evidence of low source data retrieval speed, high CPU load or insufficient network throughput.

Cloud Repositories Overview

The summary dashboard for the **Cloud Repositories** node presents a configuration overview and storage utilization analysis for cloud repositories (repositories allocated for users by Veeam Cloud Connect Service Providers).



Cloud Repositories Overview

The section provides the following details:

- Number of cloud repositories created for Veeam Cloud Connect users
- Number of cloud repository leases that will expire within 30 days
- Number of VMs and computers whose data is stored in backups on cloud repositories
- Cumulative amount of storage space occupied by VM and computer backups on all managed cloud repositories

Top Cloud Repositories by Utilization

The chart shows 5 cloud repositories with the greatest amount of used storage space.

For every repository in the chart, you can see the amount of used storage space against the amount of available space. If free space on the repository is running low, you may need to increase the repository quota.

Top Cloud Repositories with Least Days Left

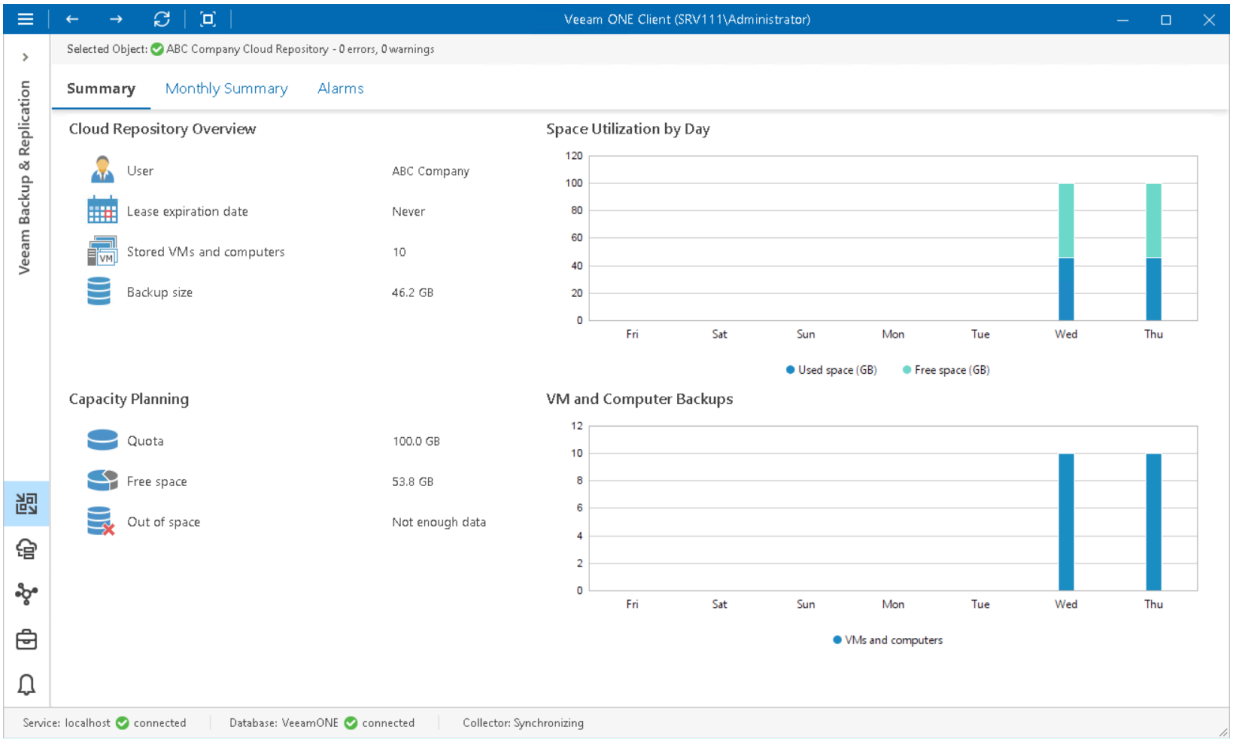
The chart shows 5 cloud repositories that can run low on storage space sooner than others. To draw the chart, Veeam ONE analyzes historical data and checks how fast free space on repositories has been decreasing in the past. Veeam ONE uses historical statistics to forecast how soon the repository will run out of space.

Top Cloud Repositories by Daily Utilization Growth

The chart allows you to detect how fast the amount of used space on repositories increased over the past 7 days. For every repository, the chart shows the daily disk space growth usage rate (the average increase in GB per day).

Cloud Repository Summary

The cloud repository summary dashboard provides overview details and space utilization analysis for the chosen cloud repository (repository allocated for a user by a Veeam Cloud Connect Service Provider).



Cloud Repository Overview

The section provides the following details:

- Name of the user that owns the cloud repository
- Date when the repository lease is set to expire
- Number of VMs and computers whose data is stored in backups stored on the cloud repository
- Cumulative amount of storage space occupied by VM and computer backups on the cloud repository

Capacity Planning

The section outlines the following details:

- User quota, that is the amount of space allocated to a user
- Amount of free storage space on the cloud repository
- Number of days before the cloud repository runs out of free space

To forecast the value, Veeam ONE uses a trend that is calculated based on historical statistics — it analyzes how fast the amount of free space on the repository was decreasing in the past and uses historical statistics to forecast how soon the repository will run out of space.

Space Utilization by Day

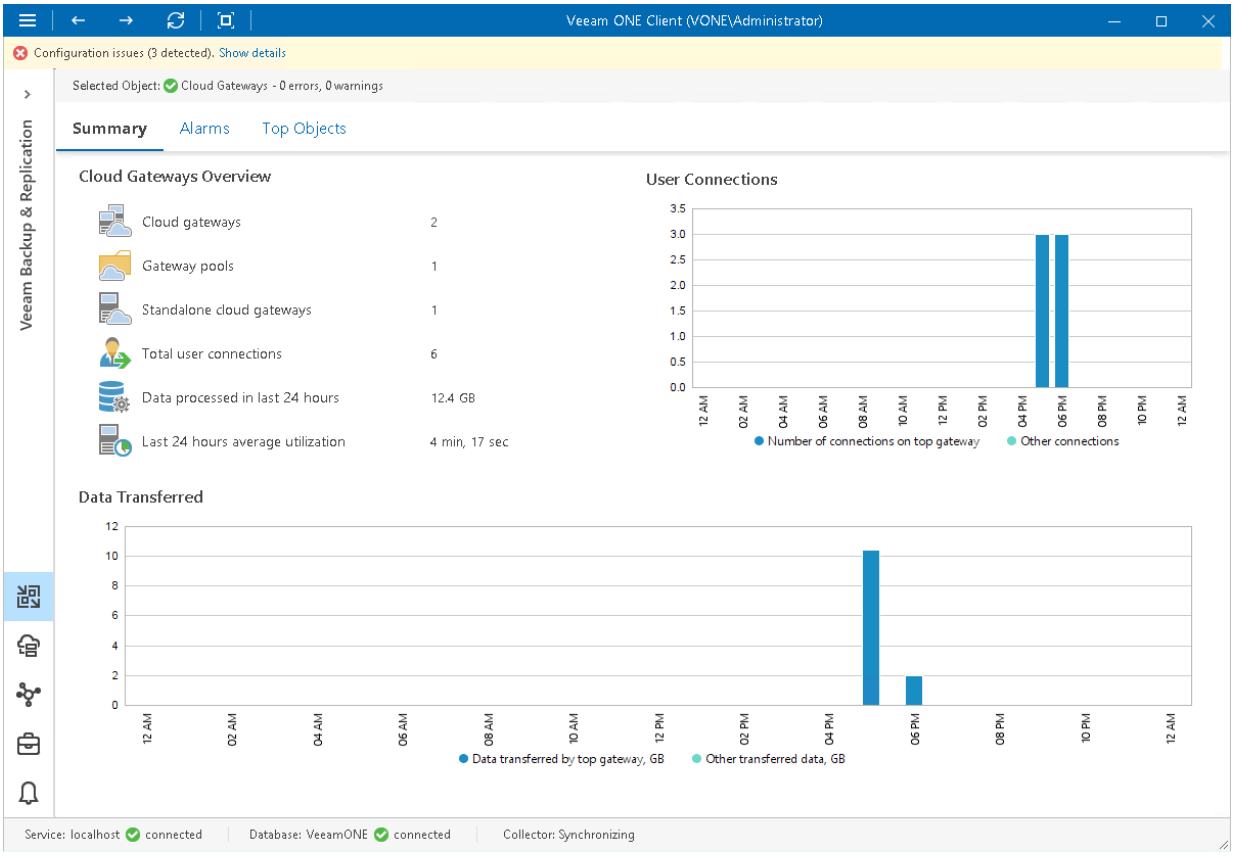
The chart shows the amount of used storage space against the amount of available space on the cloud repository. If free space on the repository is running low, you may need to increase the repository quota.

VM and Computer Backups

The chart shows the number of VMs and computers whose backups were written to the repository during the past period.

Cloud Gateways Overview

The summary dashboard for the **Cloud Gateways** node presents a configuration overview and performance analysis for cloud gateways managed by a backup server.



Cloud Gateways Overview

The section provides the following details:

- Number of cloud gateways managed by the backup server
- Number of gateway pools configured on the backup server
- Number of standalone cloud gateways configured on the backup server
- Number of connections to the gateways over the past 24 hours
- Amount of backup data that was transferred through all cloud gateways
- Average amount of time during which the gateways were utilized over the past 24 hours

User Connections

The chart shows the most loaded cloud gateways in terms of user connections. The chart shows the number of connections to the most utilized gateways, as well as connections to other gateways.

To draw the chart, Veeam ONE calculates how many connections were established to each cloud gateway over the past 24 hours.

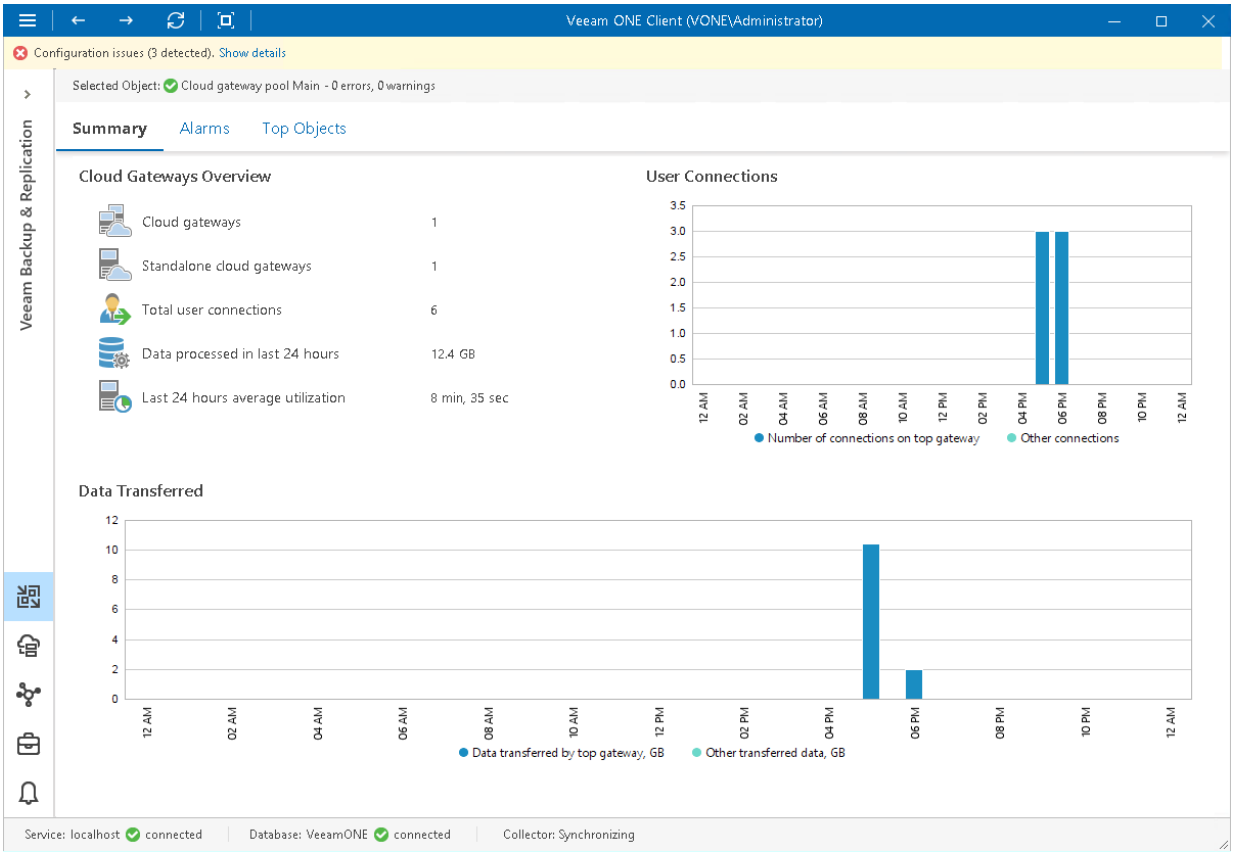
Data Transferred

The chart shows the amount of data transferred by the most utilized gateways, as well as data transferred by other gateways.

The chart can help you detect cloud gateways that transfer the greatest amount of backup data and estimate the load on gateways.

Cloud Gateway Pool Summary

The cloud gateway pool summary dashboard provides overview information and performance analysis for the chosen gateway pool over the past day, week or month.



Cloud Gateways Overview

The section outlines the following details:

- Number of cloud gateways in a pool
- Number of users that connected to the gateways in the pool over the last 24 hours
- Amount of backup data that the cloud gateways in a pool processed over the last 24 hours
- Amount of time that the cloud gateways in the pool were retrieving, processing and transferring data

User Connections

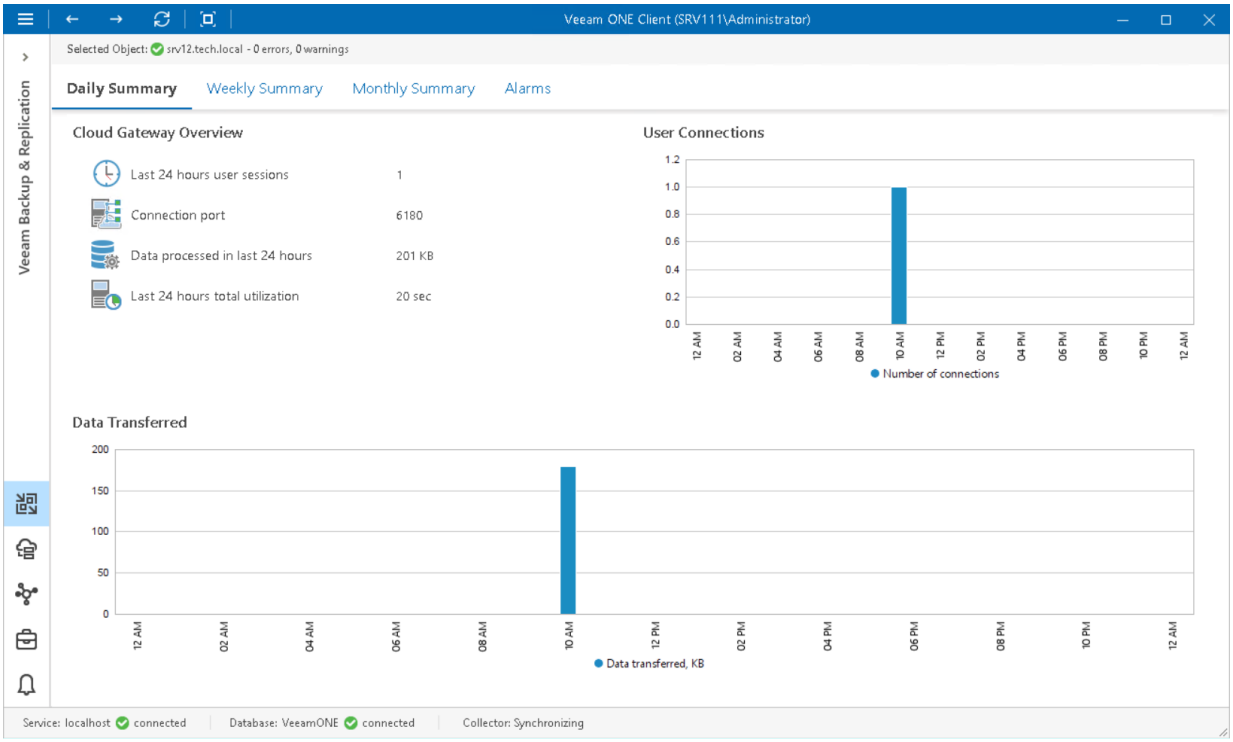
The chart shows how many times the connection to the top cloud gateway and other gateways in a pool was established to transfer backup traffic over the past period.

Data Transferred

The chart shows the amount of backup data that the to the top cloud gateway and other gateways in a pool transferred to the cloud repository over the past period. The chart can help you measure the total amount of backup traffic coming through the cloud gateways in a pool.

Cloud Gateway Summary

The cloud gateway summary dashboard provides overview information and performance analysis for the chosen gateway over the past day, week or month.



Cloud Gateway Overview

The section outlines the following details:

- Number of users that connected to the gateway over the past day, week or month
- Port configured for external connections on the cloud gateway
- Amount of backup data that the cloud gateway processed over the last 24 hours, 7 days or month
- Amount of time that the cloud gateway was retrieving, processing and transferring data

User Connections/Sessions

The chart shows how many times the connection to the cloud gateway was established to transfer backup traffic over the past period.

Data Transferred/Processed Data

The chart shows the amount of backup data that the cloud gateway transferred to the cloud repository over the past period. The chart can help you measure the total amount of backup traffic coming through the cloud gateway.

[Weekly/Monthly Summary] Utilization

The chart allows you to estimate how 'busy' the cloud gateway was during the past period. The chart shows the cumulative amount of time that the cloud gateway was retrieving, processing and transferring backup data.

The chart can help you reveal possible resource bottlenecks. If the utilization graph on the chart is abnormally large, this can evidence of high CPU load or insufficient throughput.

Veeam Backup & Replication Alarms

Veeam ONE includes a set of alarms monitor the efficiency of Veeam Backup & Replication data protection in the virtual environment.

Predefined data protection alarms are configured to warn you about events or issues that can cause loss of data or prevent Veeam Backup & Replication infrastructure from functioning properly:

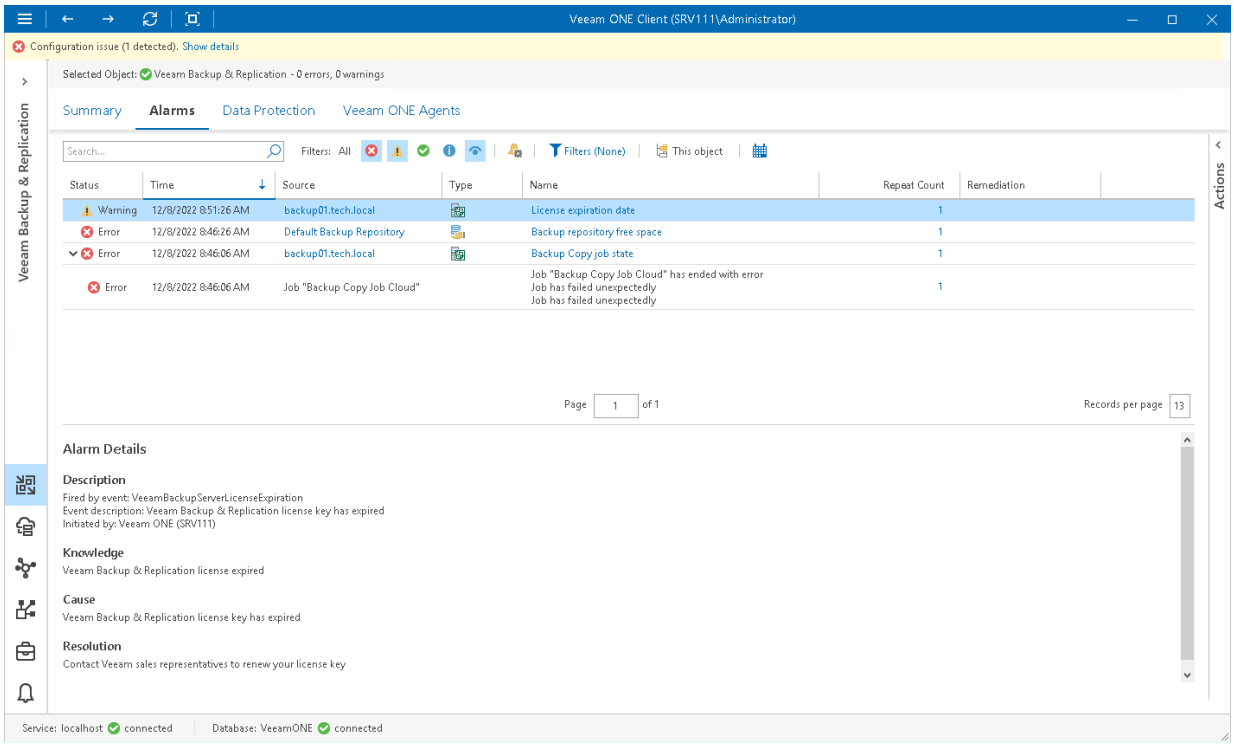
- Connectivity issues and inability of backup infrastructure components to communicate with each other
- State of Veeam Backup & Replication software installed on backup infrastructure components
- Failing jobs or jobs finished with warnings
- Configuration issues, such as fast decreasing space on backup repositories or cloud repositories
- Long-running jobs that exceed the backup window
- Product license and prepaid support contract

To view the list of data protection alarms:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.
2. At the bottom of the inventory pane, click **Veeam Backup & Replication**.
3. In the inventory pane, select the necessary backup infrastructure node.
4. Open the **Alarms** tab.

On the **Alarms** dashboard, you can view triggered alarms, track alarm history, resolve and acknowledge alarms and perform other actions. For details on available actions, see Working with Triggered Alarms.



Data Protection

Veeam ONE Client allows you to track jobs and policies configured to protect the following workloads:

- Virtual Machines
- Computers
- Unstructured Data
- Databases
- Networks

By analyzing job details, you can reveal potential problems with the efficiency of data protection operations.

For example, if job duration has significantly increased in comparison with the average monthly duration value, while there are no noticeable changes to the amount of transferred data, you may need to investigate the root cause. Such a behavior may evidence that the job has to wait for proxy resources, which increases the backup window.

Virtual Machines

Veeam ONE Client allows you to track jobs and policies configured to protect on-premises virtual machines and cloud virtual machines and instances with Veeam Backup & Replication.

You can track real-time job and policy statistics at different levels of your backup infrastructure:

- Jobs on a specific backup server
- Jobs on all backup servers controlled by Veeam Backup Enterprise Manager
- All jobs across the entire backup infrastructure

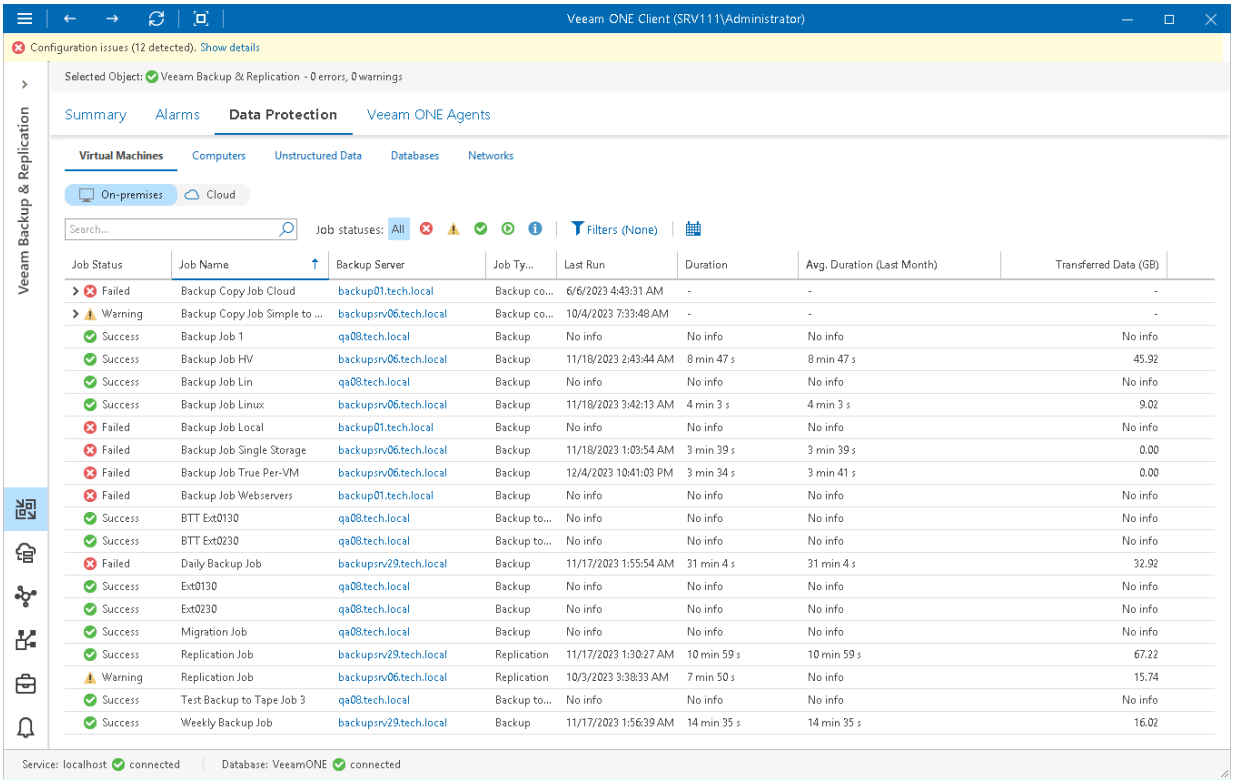
Viewing VM Job Details

To view the list of VM jobs at the necessary backup infrastructure level:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.
2. At the bottom of the inventory pane, click **Veeam Backup & Replication**.
3. In the inventory pane, select the necessary backup infrastructure node.
4. Open the **Data Protection** tab and navigate to **Virtual Machines > On-premises**.
5. To find the necessary job, you can use filters at the top of the job list:
   - To show or hide jobs that ended with a specific status, use the status buttons at the top of the list (*Show all jobs*, *Show failed jobs*, *Show jobs with warnings*, *Show successful jobs*, *Show running jobs* or *Show jobs with no status*).
   - To show or hide jobs of a specific type, use the job type filter at the top of the list (*Backup*, *Replication*, *Backup copy*, *Backup to tape*, *CDP policy*, *VM copy*, *SureBackup*, *Microsoft SQL database transaction log backup*, *Oracle Database transaction log backup*, *PostgreSQL transaction log backup*, or *Snapshot-only*).
   - To show or hide jobs that protect VMs residing on a specific hypervisor, use the platform filter at the top of the list (*VMware vSphere*, *VMware Cloud Director*, *Microsoft Hyper-V*, *Nutanix AHV*, *oVirt KVM and ProxMox VE*).
   - To set the time interval when jobs ran for the last time, use the **Filter jobs by time period** button. Release the button to discard the time period filter.
   - To find jobs by name, use the search field at the top of the list.

The list of jobs shows all types of VM jobs for the backup infrastructure level that you selected in the inventory pane.



Each job in the list is described with a set of properties. To show or hide properties, right-click the list header and choose properties that must be displayed.

- **Job Status** – latest status of the job session (*Success*, *Warning*, *Failed*, *Running*, or jobs with no status).
- **Job Name** – name of the job.
- **Backup Server** – name of the backup server on which the job is configured. Click the server name link to drill down to the list of alarms for a chosen backup server.
- **Job Type** – type of the job (*Backup*, *Replication*, *Backup copy*, *Backup to tape*, *CDP policy*, *VM copy*, *SureBackup*, *Microsoft SQL database transaction log backup*, *Oracle Database transaction log backup*, *PostgreSQL transaction log backup*, or *Snapshot-only*).
- **Last Run** – date and time of the latest job run.
- **Duration** – time taken to complete the job during its latest run.
- **Avg. Duration (Last Month)** – average time taken to complete the job (total job duration time for the previous month divided by the number of times the job ran).
- **Transferred Data (GB)** – amount of backup data that was transferred to the target destination (backup repository or replication target datastore/volume) during the latest job run.

> **NOTE:**
>
> The "*No info*" label indicates that no information is available for the job because data has not been collected yet.

Viewing Cloud VM Job Details

To view the list of cloud VM policies and jobs at the necessary backup infrastructure level:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click **Veeam Backup & Replication**.

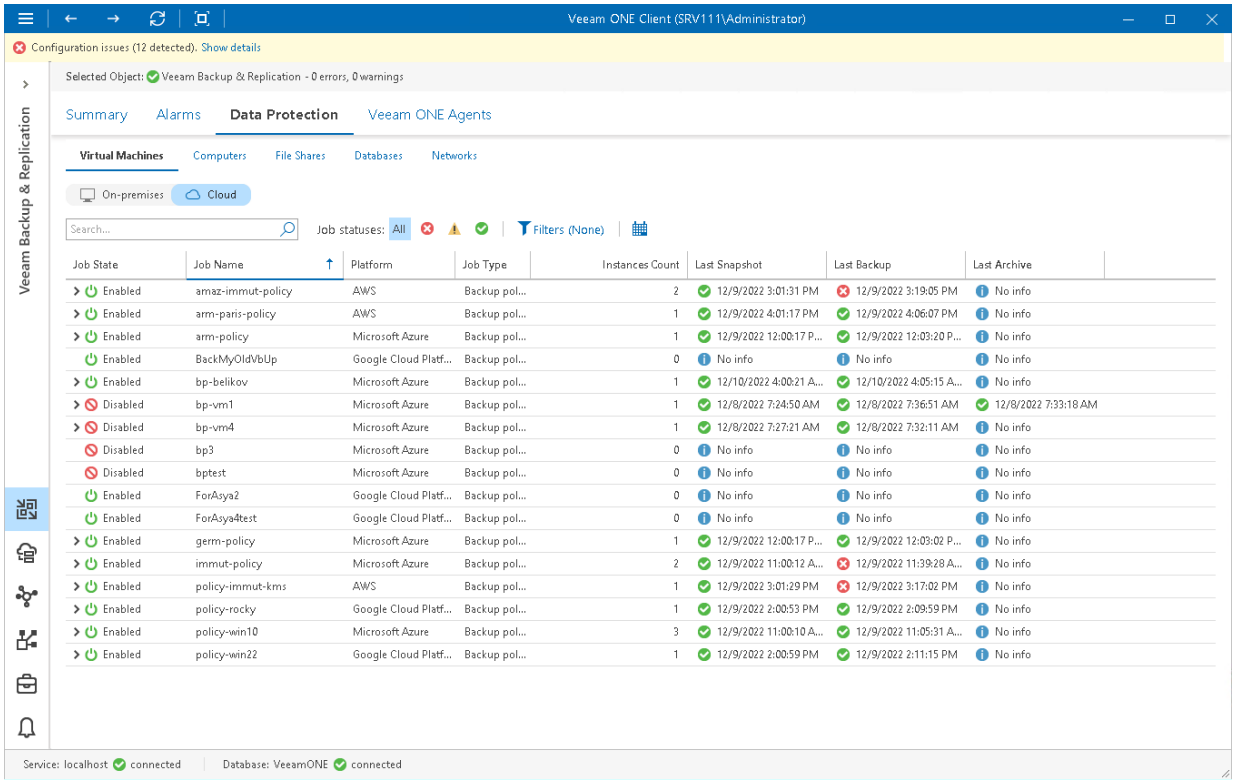
3. In the inventory pane, select the necessary backup infrastructure node.

4. Open the **Data Protection** tab and navigate to **Virtual Machines > Cloud**.

5. To find the necessary job or policy, you can use filters at the top of the policies list:

   - To show or hide jobs and policies whose sessions ended with a specific status, use the status buttons at the top of the list (*Show all jobs*, *Show jobs with errors*, *Show jobs with warnings*, *Show successful jobs*).
   - To show or hide jobs and policies of a specific type, use the job type filter at the top of the list (*Backup policy, Backup copy, Backup to tape*).
   - To show or hide jobs and policies configured for a specific platform, use the platform type filter at the top of the list (*AWS*, *Microsoft Azure*, *Google Cloud Platform*).
   - To set the time interval when jobs and policies ran for the last time, use the **Filter jobs by time period** button. Release the button to discard the time period filter.
   - To find jobs and policies by name, use the search field at the top of the list.

The list of jobs shows all Veeam Backup for Microsoft Azure, Veeam Backup for AWS and Enter value policies and jobs for the backup infrastructure level that you selected in the inventory pane.



Each job in the list is described with a set of properties. To show or hide properties, right-click the list header and choose properties that must be displayed.

- **Job State** — state of the cloud policy or job schedule (*Enabled*, *Disabled*).

  Click the > icon to show details of the last cloud protection sessions based on a specific policy.

- **Job Status** — latest status of the cloud policy or job session (*Success*, *Warning*, *Failed*, *Running*, or jobs with no status).
- **Job Name** — name of the cloud policy or job.
- **Platform** — name of the cloud platform for which the policy or job is configured.
- **Job Type** — backup job or policy type (*Backup policy*, *Backup copy*, *Backup to tape*).
- **Instance Type** — type of a protected instance.
- **Backup Server** — name of a backup server to which external repository with cloud backups is connected.

  Click the server name link to drill down to the list of alarms for a chosen backup server.

- **Instances Count** — number of Microsoft Azure VMs, AWS EC2 or Google Cloud instances processed during the last cloud protection session.
- **Last Snapshot** — date and time when the latest cloud-native snapshot was created for a Microsoft Azure VM, AWS EC2 or Google Cloud instance.
- **Last Backup** — date and time of the latest backup restore point was created for a Microsoft Azure VM, AWS EC2 or Google Cloud instance.
- **Last Replication** — date and time of the latest replication restore point was created for AWS EC2 instance.
- **Last Archive** — date and time of the latest archive restore point was created for a cloud instance.
- **Last Run** — date and time of the latest policy run.
- **Instance ID** — id of a Microsoft Azure VM, AWS EC2 or Google Cloud instance.
- **Duration** — time taken to complete the job during its latest run.
- **Avg. Duration (Last Month)** — average time taken to complete the job (total job duration time for the previous month divided by the number of times the job ran).
- **Transferred Data (GB)** — amount of backup data that was transferred to the target destination during the latest job run.

> **NOTE:**
>
> The "*No info*" label indicates that no information is available for the job because data has not been collected yet.

Computers

Veeam ONE Client allows you to track Veeam backup agent jobs and policies managed by Veeam Backup & Replication servers connected to Veeam ONE.

You can view real-time job statistics at different levels of your backup infrastructure:

- Jobs managed by a specific backup server
- Jobs managed by all backup servers controlled by Veeam Backup Enterprise Manager
- All jobs across the entire backup infrastructure

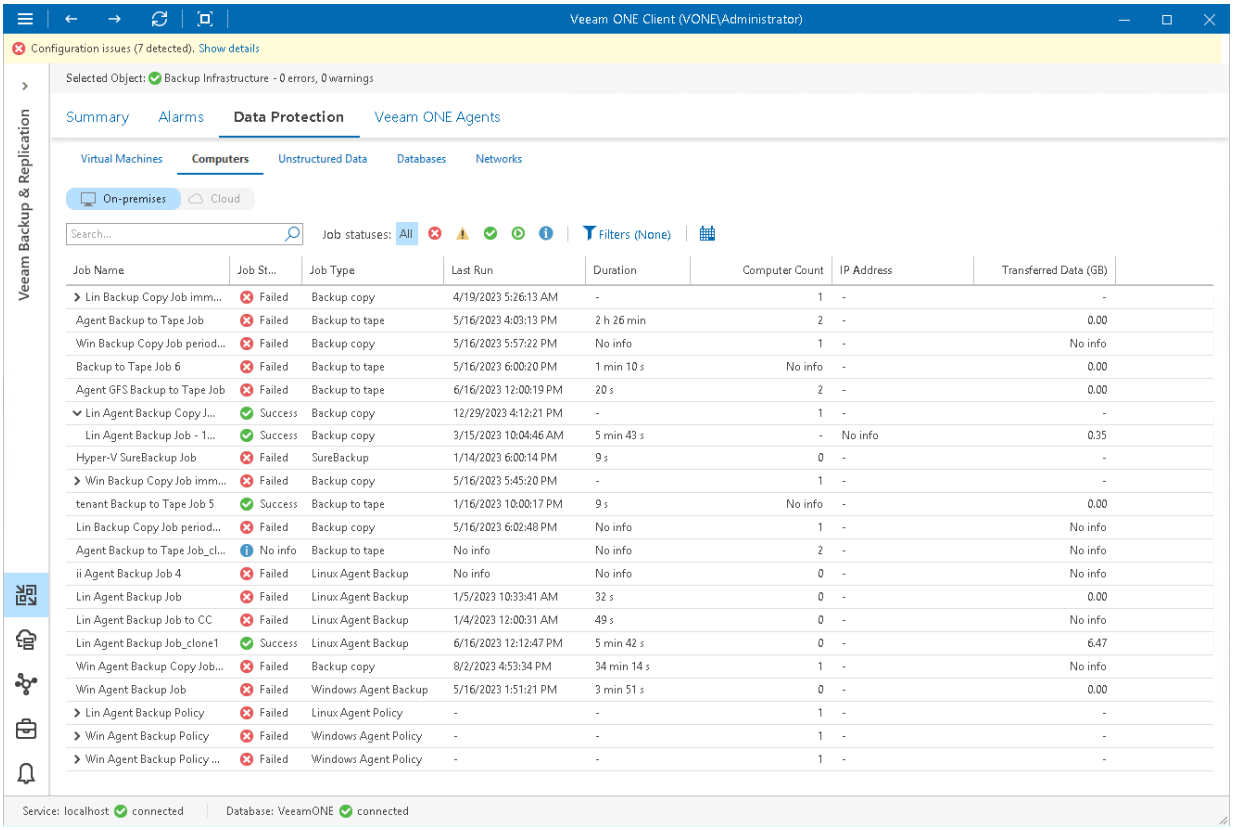
Viewing Job Details

To view the list of Veeam backup agent jobs and policies at the necessary backup infrastructure level:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.
2. At the bottom of the inventory pane, click **Veeam Backup & Replication**.
3. In the inventory pane, select the necessary backup infrastructure node.
4. Open the **Data Protection** tab and navigate to **Computers**.
5. To find the necessary job or policy, you can use filters at the top of the job list:
   - To show or hide jobs that ended with a specific status, use the status buttons at the top of the list (*Show all jobs*, *Show failed jobs*, *Show jobs with warnings*, *Show successful jobs*, *Show running jobs* or *Show jobs with no status*).
   - To show or hide jobs and policies by type, use the filters at the top of the list (*Agent backup*, *Agent backup policy*, *Backup copy*, *Backup to tape*, *SureBackup*, *Microsoft SQL transaction log backup*, *Oracle Database transaction log backup*, *PostgreSQL transaction log backup*).
   - To show or hide jobs and policies by platform of Veeam backup agent, use the filters at the top of the list (*Microsoft Windows*, *Linux*, *masOS*, *IBM AIX*, *Oracle Solaris*).
   - To set the time interval when jobs ran for the last time, use the **Filter jobs by time period** button. Release the button to discard the time period filter.
   - To find jobs and policies by name, use the search field at the top of the list.

The list of jobs shows all Veeam backup agent jobs and policies for the backup infrastructure level that you selected in the inventory pane.



Each job in the list is described with a set of properties. To show or hide properties, right-click the list header and choose properties that must be displayed.

- **Job Name** — name of the job or policy.

  Click the > icon to show details of agent job sessions based on a specific backup policy.

- **Job Status** — the latest status of the job or policy session (*Success*, *Warning*, *Failed*, *Running*, or jobs with no status).

- **Backup Server** — name of the backup server on which the job or policy is configured. Click the server name link to drill down to the list of alarms for a chosen backup server.

- **Job Type** — backup job type (*Agent backup*, *Agent backup policy*, *Backup copy*, *Backup to tape*, *SureBackup*, *Microsoft SQL transaction log backup*, *Oracle Database transaction log backup*, *PostgreSQL transaction log backup*).

- **Computer** — name of the computer for which the job or policy is configured.

- **Last Run** — date and time when the backup job was performed for the last time.

- **Duration** — time taken to complete the backup job during its latest run.

- **Computer Count** — number of computers included in the backup job.

- **IP Address** — IP addresses of computers to which the backup policy was applied.

- **Transferred Data (GB)** — amount of backup data that was transferred to the target destination during the latest job run.

- **Avg. Duration (Last Month)** — average time taken to complete the backup job (total job duration time for the previous month divided by the number of times the job ran).

NOTE:

The "*No info*" label indicates that no information is available for the job because data has not been collected yet.

Unstructured Data

Veeam ONE Client allows you to track object storage backup, object storage backup copy, object storage to tape, file backup, file backup copy, file to tape and file copy jobs configured to protect object storage items and on-premises and cloud file shares.

You can track real-time job statistics at different levels of your backup infrastructure:

- Jobs managed by a specific backup server
- Jobs on all backup servers controlled by Veeam Backup Enterprise Manager
- All jobs across the entire backup infrastructure

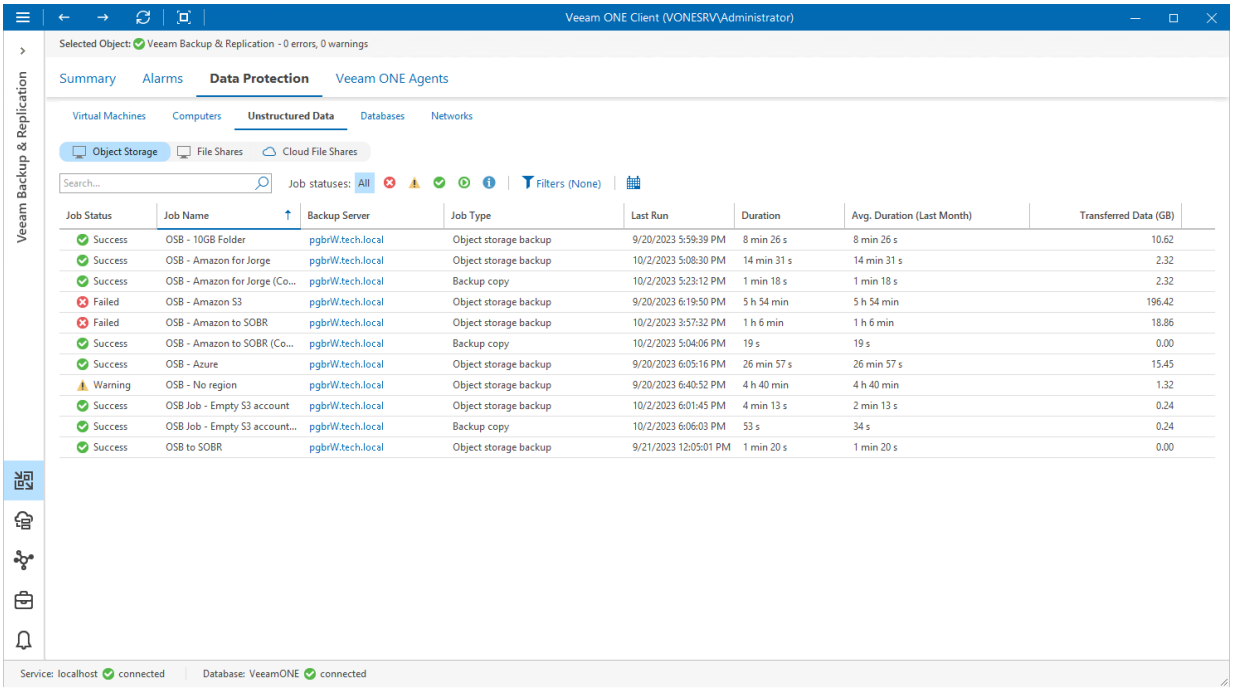
Viewing Object Storage Job Details

To view the list of object storage jobs at the necessary backup infrastructure level:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.
2. At the bottom of the inventory pane, click **Veeam Backup & Replication**.
3. In the inventory pane, select the necessary backup infrastructure node.
4. Open the **Data Protection** tab and navigate to **Unstructured Data > Object Storage**.
5. To find the necessary job, you can use filters at the top of the job list:
   - To show or hide jobs that ended with a specific status, use the status buttons at the top of the list (*Show all jobs*, *Show failed jobs*, *Show jobs with warnings*, *Show successful jobs*, *Show running jobs* or *Show jobs with no status*).
   - To show or hide jobs of a specific type, use the job type filter at the top of the list (*Object storage backup*, *Backup copy*, *Object storage to tape*).
   - To set the time interval when jobs ran for the last time, use the **Filter jobs by time period** button. Release the button to discard the time period filter.
   - To find jobs by name, use the search field at the top of the list.

The list of jobs shows all object storage backup, object storage backup copy and object storage to tape jobs for the backup infrastructure level that you selected in the inventory pane.



Each job in the list is described with a set of properties. To show or hide properties, right-click the list header and choose properties that must be displayed.

- **Job Status** — the latest status of the job session (*Success*, *Warning*, *Failed*, *Running*, or jobs with no status).
- **Job Name** — name of an object storage job.
- **Backup Server** — name of a backup server on which the job is configured. Click the server name link to drill down to the list of alarms for the chosen backup server.
- **Job Type** — job type (*Object storage backup*, *Backup copy*, *Object storage to tape*).
- **Last Run** — date and time of the latest job run.
- **Duration** — time taken to complete the job during its latest run.
- **Avg. Duration (Last Month)** — average time taken to complete the job (total job duration time for the previous month divided by the number of times the job ran).
- **Transferred Data (GB)** — amount of backup data that was transferred to the target destination (backup repository or tape) during the latest job run.

> **NOTE:**
>
> The "*No info*" label indicates that no information is available for the job because data has not been collected yet.

Viewing File Share Job Details

To view the list of file jobs at the necessary backup infrastructure level:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click **Veeam Backup & Replication**.

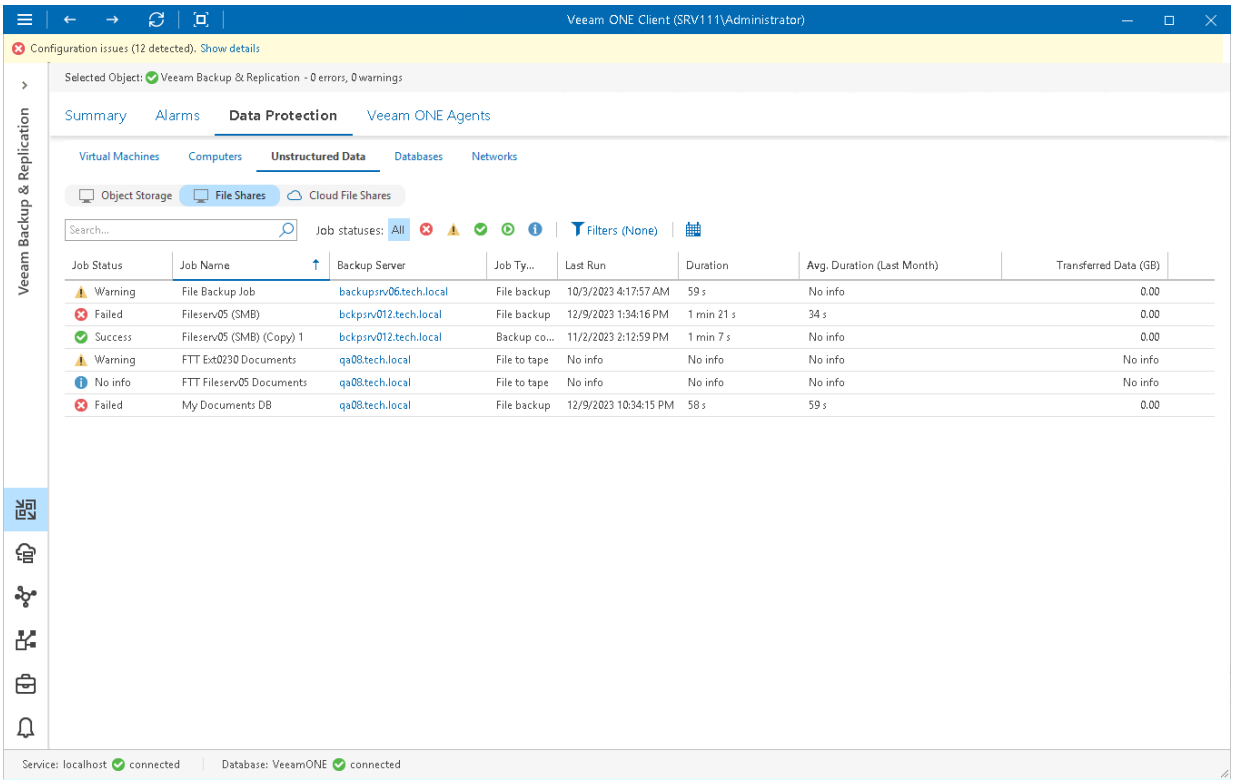
3. In the inventory pane, select the necessary backup infrastructure node.

4. Open the **Data Protection** tab and navigate to **Unstructured Data > File Shares**.

5. To find the necessary job, you can use filters at the top of the job list:

   - To show or hide jobs that ended with a specific status, use the status buttons at the top of the list (*Show all jobs*, *Show failed jobs*, *Show jobs with warnings*, *Show successful jobs*, *Show running jobs* or *Show jobs with no status*).
   - To show or hide jobs of a specific type, use the job type filter at the top of the list (*File backup*, *Backup copy*, *Backup to tape*, *File to tape* or *File copy*).
   - To set the time interval when jobs ran for the last time, use the **Filter jobs by time period** button. Release the button to discard the time period filter.
   - To find jobs by name, use the search field at the top of the list.

The list of jobs shows all file backup, file backup copy, file to tape and file copy jobs for the backup infrastructure level that you selected in the inventory pane.



Each job in the list is described with a set of properties. To show or hide properties, right-click the list header and choose properties that must be displayed.

- **Job Status** – the latest status of the job session (*Success*, *Warning*, *Failed*, *Running*, or jobs with no status).

- **Job Name** — name of a file share job.
- **Backup Server** — name of a backup server on which the job is configured. Click the server name link to drill down to the list of alarms for the chosen backup server.
- **Job Type** — job type (*File backup*, *Backup copy*, *Backup to tape*, *File to tape* or *File copy*).
- **Last Run** — date and time of the latest job run.
- **Duration** — time taken to complete the job during its latest run.
- **Avg. Duration (Last Month)** — average time taken to complete the job (total job duration time for the previous month divided by the number of times the job ran).
- **Transferred Data (GB)** — amount of backup data that was transferred to the target destination (backup repository or tape) during the latest job run.

> **NOTE:**
>
> The "*No info*" label indicates that no information is available for the job because data has not been collected yet.

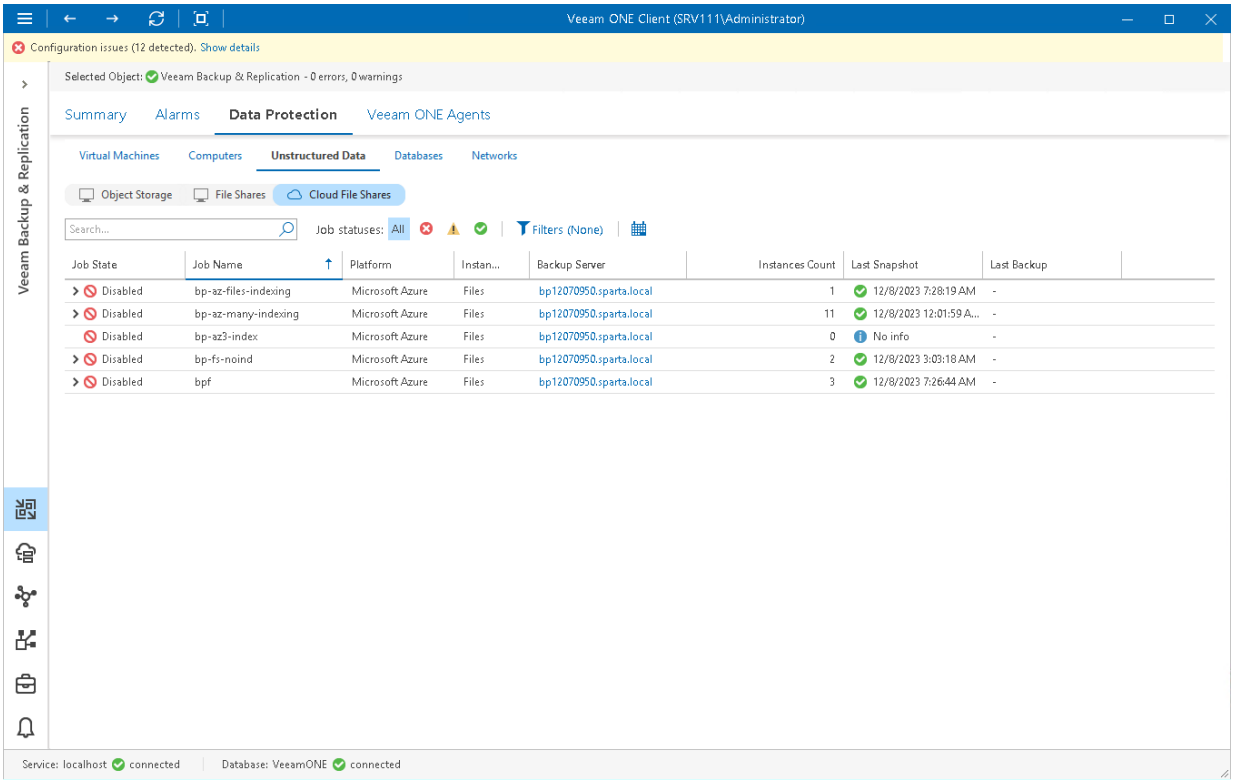
Viewing Cloud File Share Job Details

To view the list of file jobs at the necessary backup infrastructure level:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.
2. At the bottom of the inventory pane, click **Veeam Backup & Replication**.
3. In the inventory pane, select the necessary backup infrastructure node.
4. Open the **Data Protection** tab and navigate to **Unstructured Data > Cloud File Shares**.
5. To find the necessary job, you can use filters at the top of the job list:
   - To show or hide jobs that ended with a specific status, use the status buttons at the top of the list (*Show all jobs*, *Show jobs with errors*, *Show jobs with warnings*, *Show successful jobs*).
   - To show or hide jobs for a specific platform, use the job type filter at the top of the list (*AWS* or *Microsoft Azure*).
   - To set the time interval when jobs ran for the last time, use the **Filter jobs by time period** button. Release the button to discard the time period filter.
   - To find jobs by name, use the search field at the top of the list.

The list of jobs shows all file backup policies for the backup infrastructure level that you selected in the inventory pane.



Each job in the list is described with a set of properties. To show or hide properties, right-click the list header and choose properties that must be displayed.

- **Job State** — the latest status of the job session (*Success*, *Warning*, *Failed*, *Running*, or jobs with no status).
- **Job Name** — name of the file share job.
- **Platform** — name of the cloud platform for which file job is configured.
- **Instance Type** — type of the protected instance.
- **Backup Server** — name of the backup server on which the job is configured. Click the server name link to drill down to the list of alarms for a chosen backup server.
- **Instances Count** — number of Microsoft Azure Files or AWS EFS instances processed during the last cloud protection session.
- **Last Snapshot** — date and time when the latest cloud-native snapshot was created for a Microsoft Azure Files or AWS EFS instance.
- **Last Backup** — date and time of the latest backup restore point was created for a Microsoft Azure Files or AWS EFS instance.
- **Last Backup Copy** — date and time of the latest backup copy restore point was created for a Microsoft Azure Files or AWS EFS instance.
- **Instance ID** — id of the Microsoft Azure Files or AWS EFS instance.

> **NOTE:**
>
> The "*No info*" label indicates that no information is available for the job because data has not been collected yet.

Databases

Veeam ONE Client allows you to track database jobs and policies configured to protect on-premises and cloud databases.

You can track real-time job statistics at different levels of your backup infrastructure:

- Jobs managed by a specific backup server
- Jobs on all backup servers controlled by Veeam Backup Enterprise Manager
- All jobs across the entire backup infrastructure

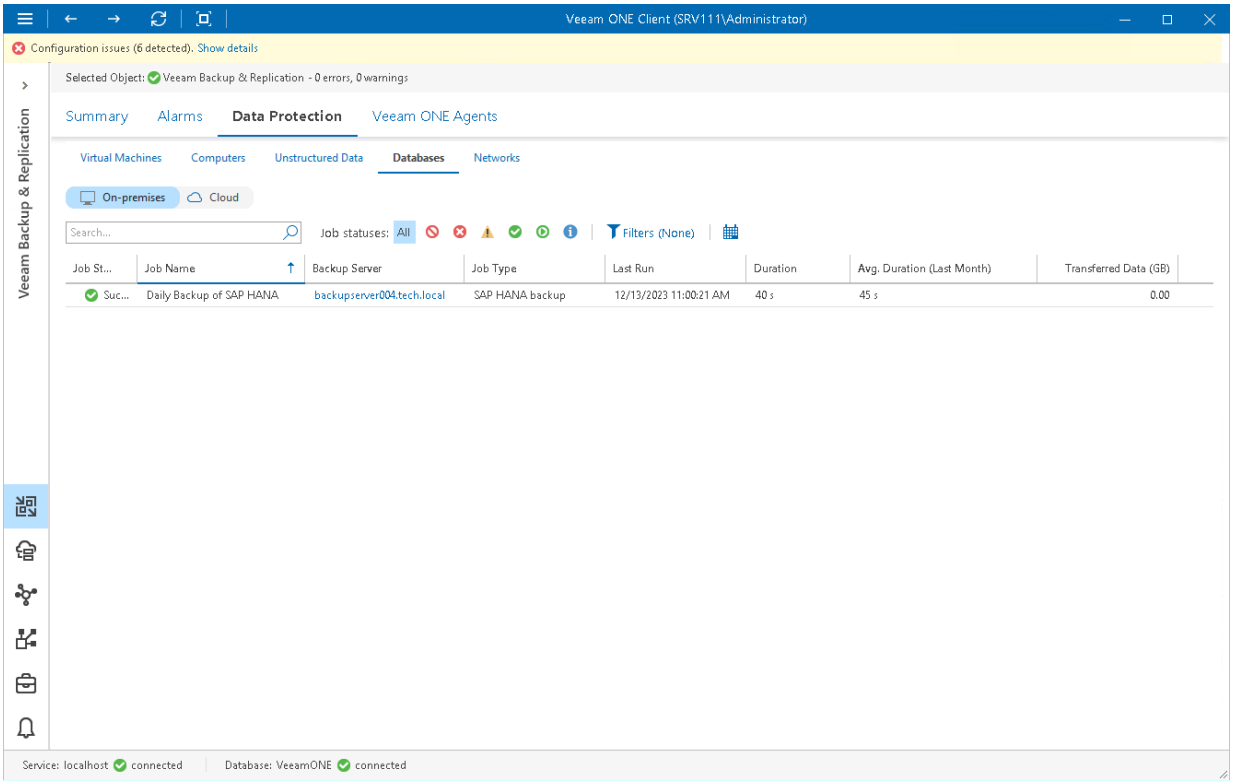
Viewing Database Job Details

To view the list of database protection jobs at the necessary backup infrastructure level:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.
2. At the bottom of the inventory pane, click **Veeam Backup & Replication**.
3. In the inventory pane, select the necessary backup infrastructure node.
4. Open the **Data Protection** tab and navigate to **Databases > On-premises**.
5. To find the necessary job, you can use filters at the top of the job list:
   - To show or hide jobs that ended with a specific status, use the status buttons at the top of the list (*Show all jobs*, *Show disabled jobs*, *Show failed jobs*, *Show jobs with warnings*, *Show successful jobs*, *Show running jobs* or *Show jobs with no status*).
   - To show or hide jobs of a specific type, use the job type filter at the top of the list (*Backup policy*, *Backup copy*, *Transaction log backup*).
   - To show or hide jobs for a specific platform, use the platform filter at the top of the list (*Oracle Database*, *SAP HANA*, *SAP on Oracle Database, Microsoft SQL Server, SAP on MaxDB*)
   - To set the time interval when jobs ran for the last time, use the **Filter jobs by time period** button. Release the button to discard the time period filter.
   - To find jobs by name, use the search field at the top of the list.

The list of jobs shows all policies, backup copy and transaction log backup jobs for the backup infrastructure level that you selected in the inventory pane.



Each job in the list is described with a set of properties. To show or hide properties, right-click the list header and choose properties that must be displayed.

- **Job Status** — the latest status of the job session (*Success*, *Warning*, *Failed*, *Running*, or *jobs with no status*).
- **Job Name** — name of the database protection job.
- **Backup Server** — name of a backup server on which the job is configured. Click the server name link to drill down to the list of alarms for the chosen backup server.
- **Job Type** — type of the database protection job (*Backup policy*, *Backup copy*, *Transaction log backup*)
- **Last Run** — date and time of the latest job run.
- **Duration** — time taken to complete the job during its latest run.
- **Avg. Duration (Last Month)** — average time taken to complete the job (total job duration time for the previous month divided by the number of times the job ran).
- **Transferred Data (GB)** — amount of backup data that was transferred to the target destination during the latest job run.

> **NOTE:**
>
> The "*No info*" label indicates that no information is available for the job because data has not been collected yet.

Viewing Cloud Database Job Details

To view the list of database protection jobs at the necessary backup infrastructure level:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click **Veeam Backup & Replication**.

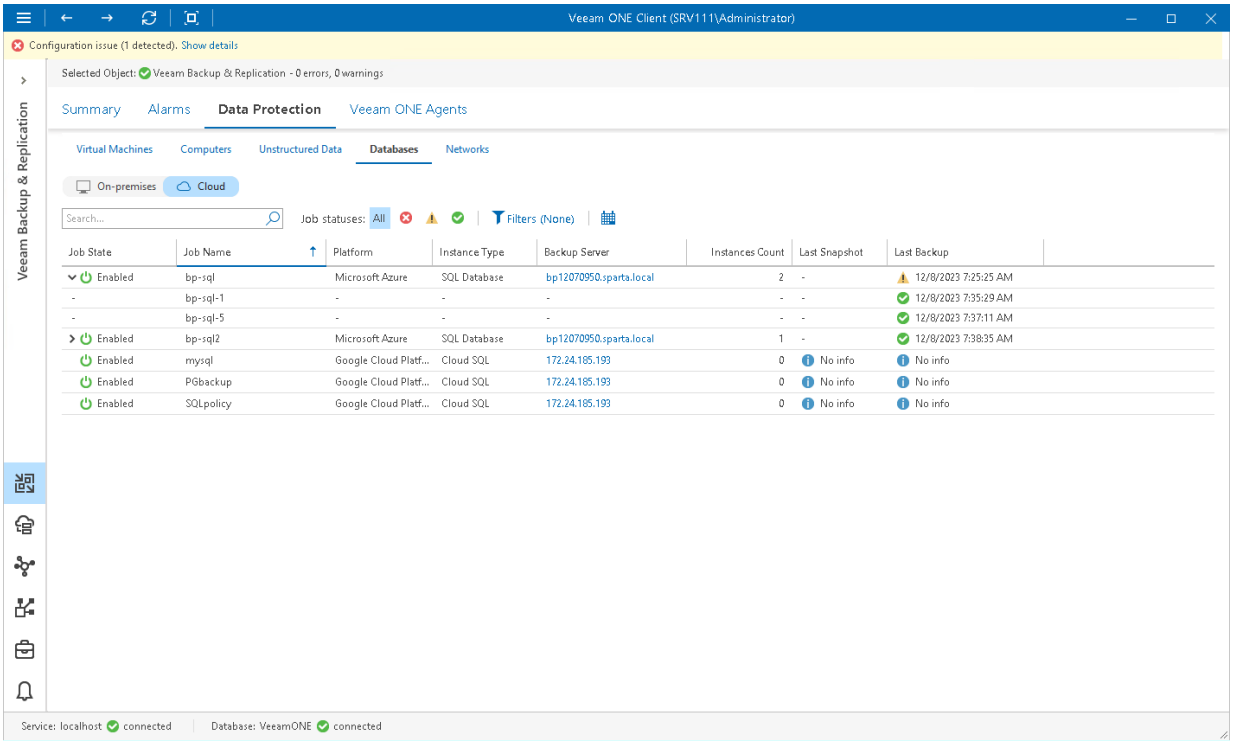
3. In the inventory pane, select the necessary backup infrastructure node.

4. Open the **Data Protection** tab and navigate to **Databases > Cloud**.

5. To find the necessary job, you can use filters at the top of the job list:

   - To show or hide jobs that ended with a specific status, use the status buttons at the top of the list (*Show all jobs*, *Show jobs with errors*, *Show jobs with warnings*, *Show successful jobs*).
   - To show or hide jobs for a specific platform, use the platform filter at the top of the list (*AWS*, *Microsoft Azure*, *Google Cloud Platform*)
   - To set the time interval when jobs ran for the last time, use the **Filter jobs by time period** button. Release the button to discard the time period filter.
   - To find jobs by name, use the search field at the top of the list.

The list of jobs shows all database protection jobs for the backup infrastructure level that you selected in the inventory pane.



Each job in the list is described with a set of properties. To show or hide properties, right-click the list header and choose properties that must be displayed.

- **Job State** – state of the Microsoft Azure SQL Database, AWS RDS or Google Cloud SQL policy schedule (*Enabled*, *Disabled*).

  Click the > icon to show details of the last cloud protection sessions based on a specific policy.

- **Job Name** — name of the Microsoft Azure SQL Database, AWS RDS or Google Cloud SQL policy.
- **Platform** — name of the cloud platform for which policy is configured.
- **Instance Type** — type of the protected instance.
- **Backup Server** — name of a backup server to which external repository with cloud backups is connected.

  Click the server name link to drill down to the list of alarms for a chosen backup server.
- **Instances Count** — number of Microsoft Azure SQL Database, AWS RDS or Google Cloud SQL instances processed during the last cloud protection session.
- **Last Snapshot** — date and time when the latest cloud-native snapshot was created for the AWS RDS or Google Cloud SQL instance.
- **Last Backup** — date and time of the latest backup restore point was created for the Microsoft Azure SQL Database or Google Cloud SQL instance.
- **Last Replication** — date and time of the latest replication restore point was created for the AWS RDS instance.
- **Last Archive** — date and time of the latest archive restore point was created for the Microsoft Azure SQL Database or Google Cloud SQL instance.
- **Instance ID** — id of the Microsoft Azure SQL Database, AWS RDS or Google Cloud SQL instance.

NOTE:

The "*No info*" label indicates that no information is available for the job because data has not been collected yet.

Networks

Veeam ONE Client allows you to track AWS policies configured to protect cloud networks.

You can track real-time job statistics at different levels of your backup infrastructure:

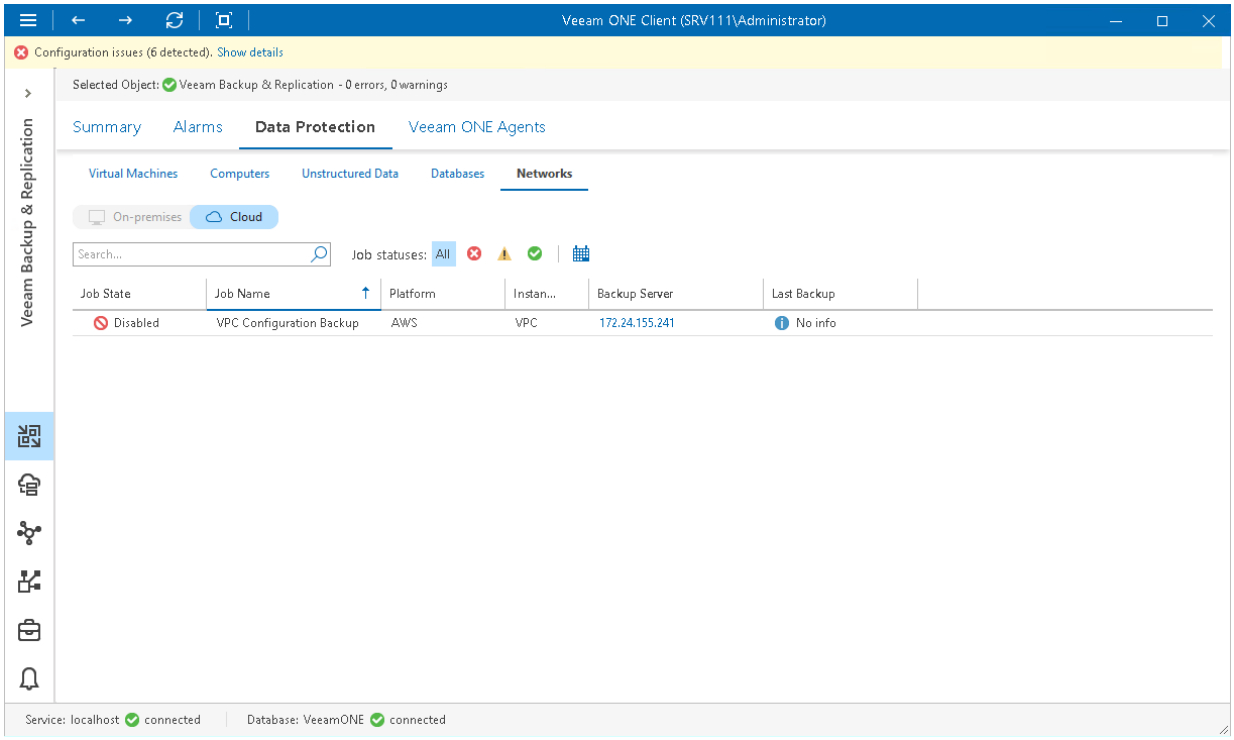
- Jobs managed by a specific backup server
- Jobs on all backup servers controlled by Veeam Backup Enterprise Manager
- All jobs across the entire backup infrastructure

To view the list of network protection policies at the necessary backup infrastructure level:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.
2. At the bottom of the inventory pane, click **Veeam Backup & Replication**.
3. In the inventory pane, select the necessary backup infrastructure node.
4. Open the **Data Protection** tab and navigate to **Networks**.
5. To find the necessary job, you can use filters at the top of the job list:
   - To show or hide jobs that ended with a specific status, use the status buttons at the top of the list (*Show all policies*, *Show policies with errors*, *Show policies with warnings*, *Show successful policies*).
   - To set the time interval when jobs ran for the last time, use the **Filter jobs by time period** button. Release the button to discard the time period filter.
   - To find jobs by name, use the search field at the top of the list.

The list of jobs shows all policies for the backup infrastructure level that you selected in the inventory pane.



Each job in the list is described with a set of properties. To show or hide properties, right-click the list header and choose properties that must be displayed.

- **Job State** – state of the cloud policy schedule (*Enabled*, *Disabled*).

  Click the > icon to show details of the last cloud protection sessions based on a specific policy.
- **Job Name** – name of the cloud backup policy.
- **Platform** – name of the cloud platform for which policy is configured.
- **Instance Type** – type of the protected instance.
- **Backup Server** – name of the backup server to which external repository with cloud backups is connected.

  Click the server name link to drill down to the list of alarms for a chosen backup server.
- **Last Backup** – date and time when the latest backup restore point was created for a cloud instance.

> **NOTE:**
>
> The "*No info*" label indicates that no information is available for the job because data has not been collected yet.

Veeam Backup & Replication Performance Charts

To identify performance bottlenecks within the backup data flow, you can drill down to the following performance charts:

- CPU Performance Chart
- Memory Performance Chart
- Disk Performance Chart
- Network Performance Chart
- Cache Performance Chart

To draw the charts, Veeam ONE gathers Windows Performance Monitor metrics from the guest OS of backup infrastructure components (for this reason, performance charts for Linux-based repositories are not available). You can track performance metrics for physical and virtual backup servers, proxies, repositories, WAN accelerators or Enterprise Manager servers.

To drill down to a performance chart for a backup infrastructure component:

1. Open Veeam ONE Client.

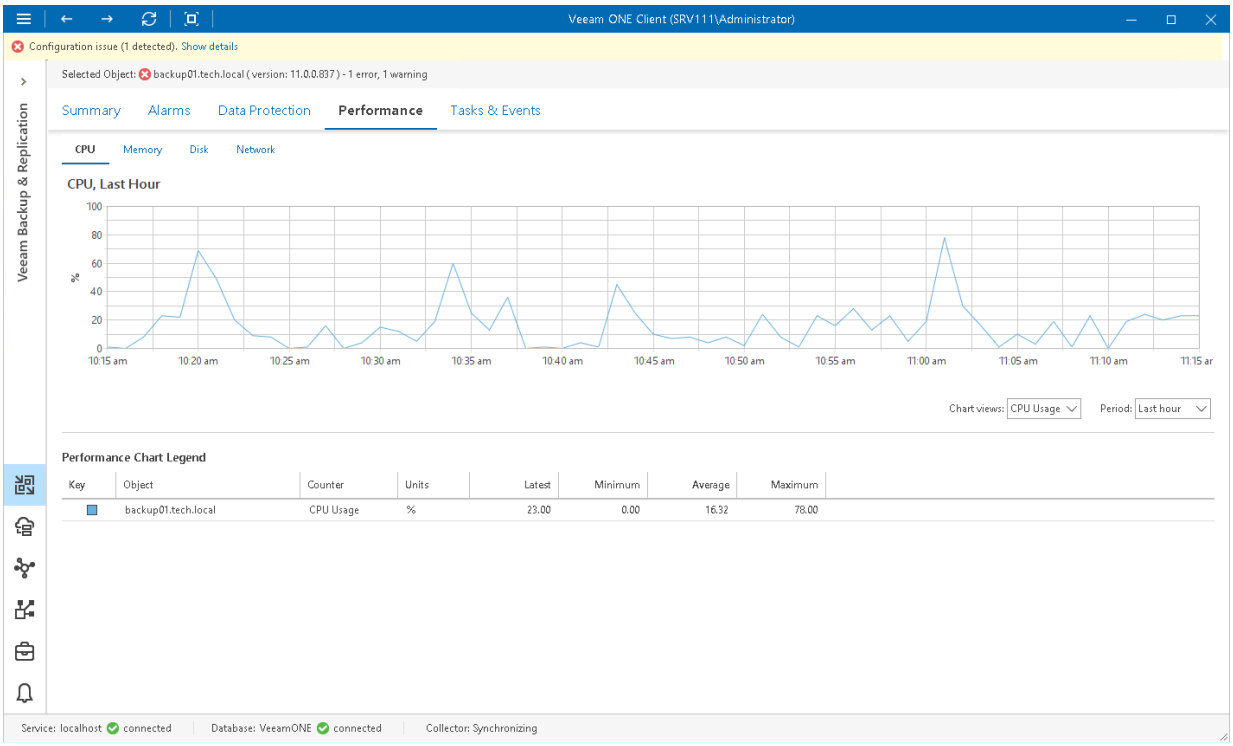
   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click **Veeam Backup & Replication**.
3. Select the necessary backup infrastructure component.
4. Open the necessary performance chart tab.

For performance charts in the **Veeam Backup & Replication**, you can change chart views and set time intervals, define objects to show on charts or select custom metrics.

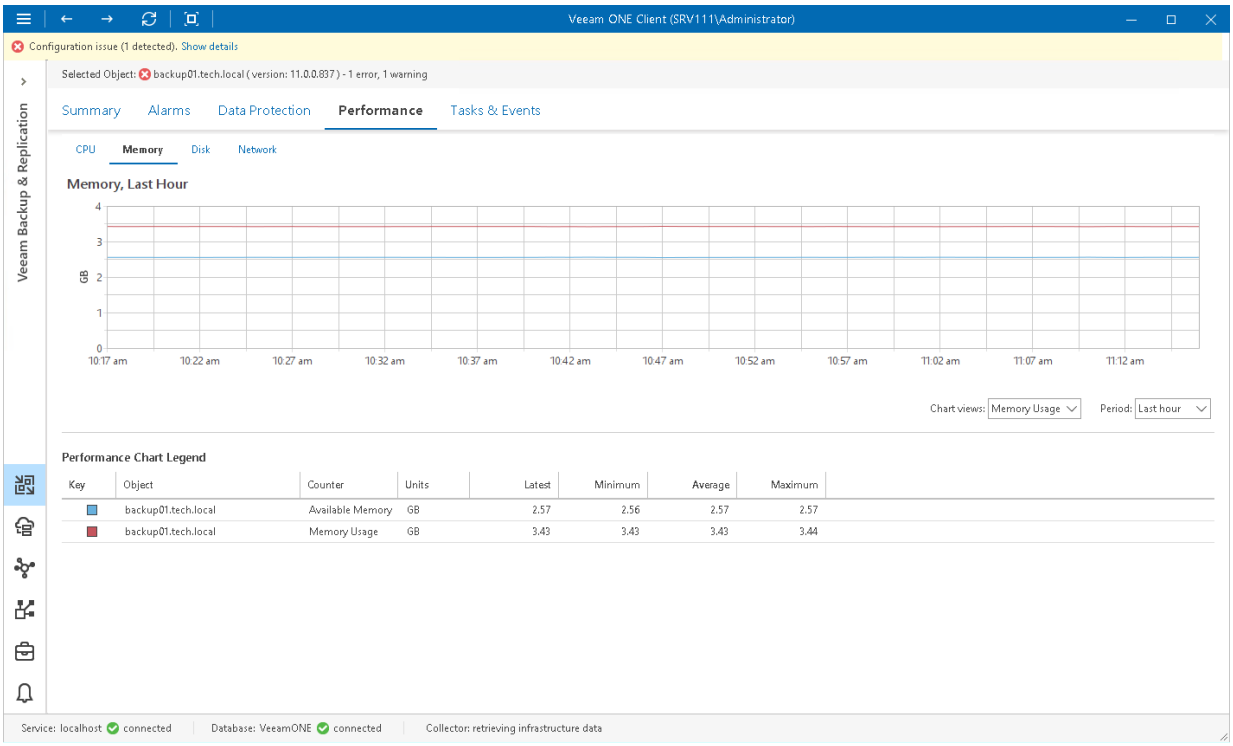
CPU Performance Chart

The **CPU** chart shows the amount of used processor resources on a machine where a backup infrastructure component runs. Graphs in the **CPU** chart illustrate the level of processor usage for every separate CPU on the machine. The **Total** graph shows the cumulative processor utilization for all CPUs.



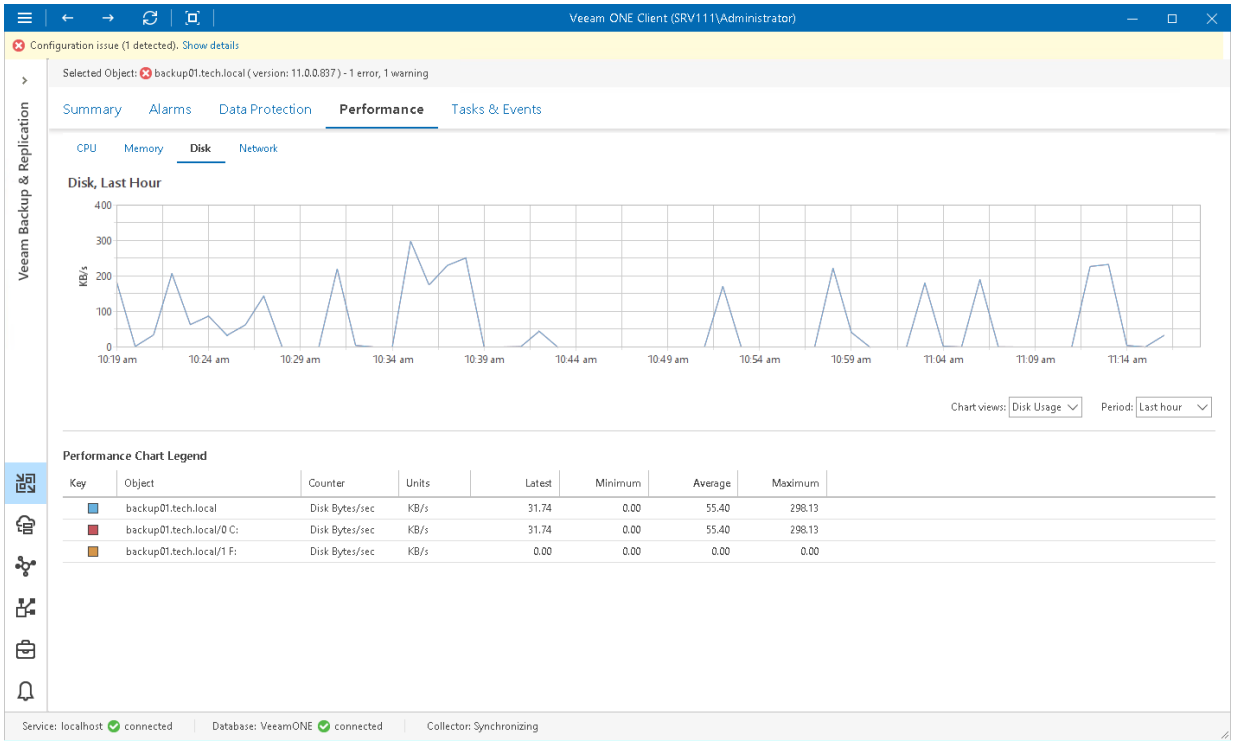
Memory Performance Chart

The **Memory** chart shows the amount of used memory resources on a machine where a backup infrastructure component runs. Graphs in the **Memory** chart illustrate the amount of total available memory and memory that is currently used on the machine.



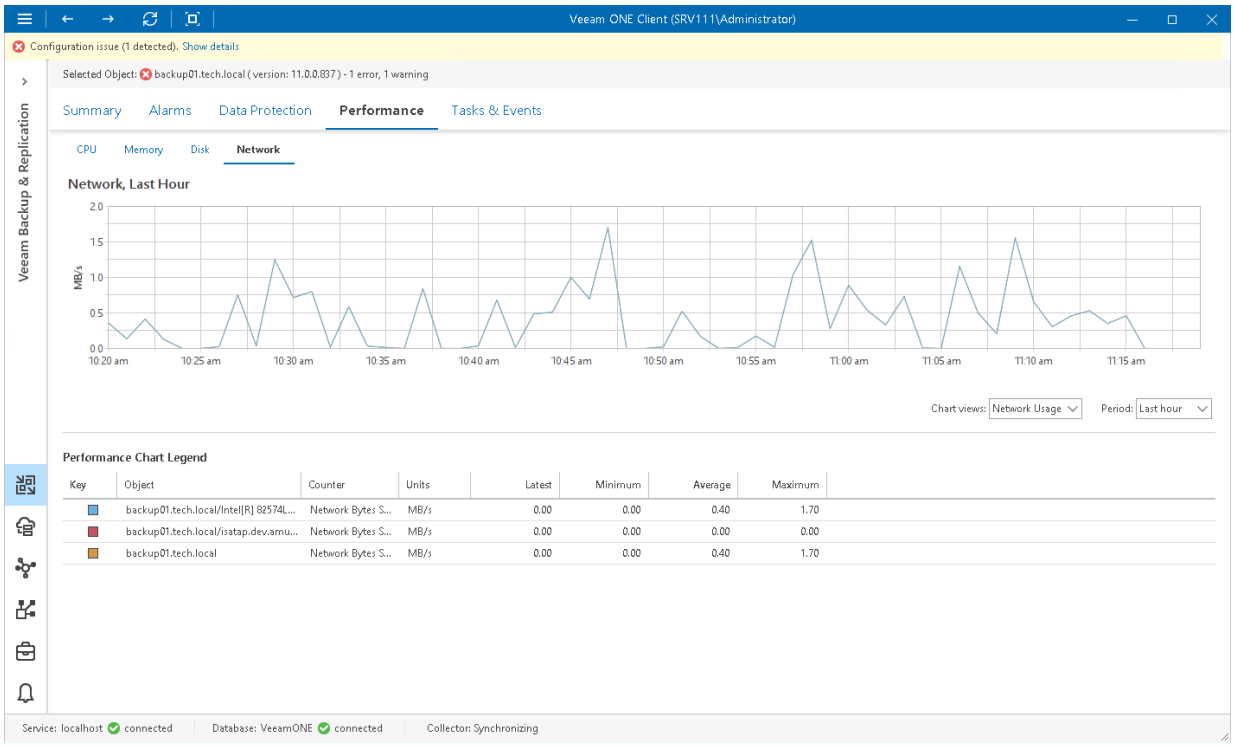
Disk Performance Chart

The **Disk** chart shows the rate at which the disk is transferring data during read and write operations. Disk usage is shown as an average for all physical disks on a machine where a backup infrastructure component runs.



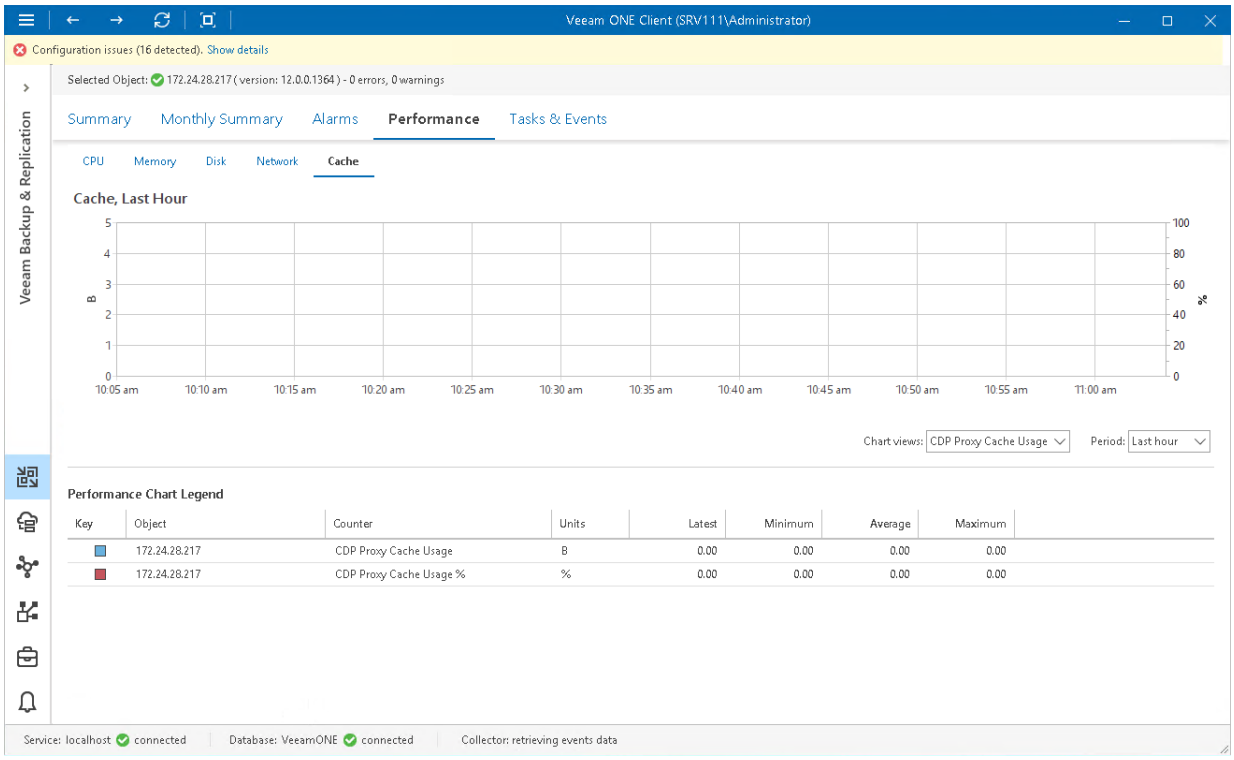
Network Performance Chart

The **Network** chart shows the throughput for NICs on a machine where a backup infrastructure component runs. Graphs in the **Network** chart illustrate the rate at which data is sent on the network interface for each separate NIC. A separate graph shows the cumulative rate for all NICs on the machine.



Cache Performance Chart

The **Cache** chart shows the amount of space consumed by the data processed during CDP operations. Graphs in the chart display how much data is stored in the cache folder on the machine where CDP Proxy component runs and the percentage of allocated cache space consumed by this data.



Data Transfer

The **Data Transfer** dashboard provides detailed information on data transfer sessions for the chosen scale-out backup repository and helps to monitor the amount of data transferred between the repository extents.

To view data transfer details for a specific repository:

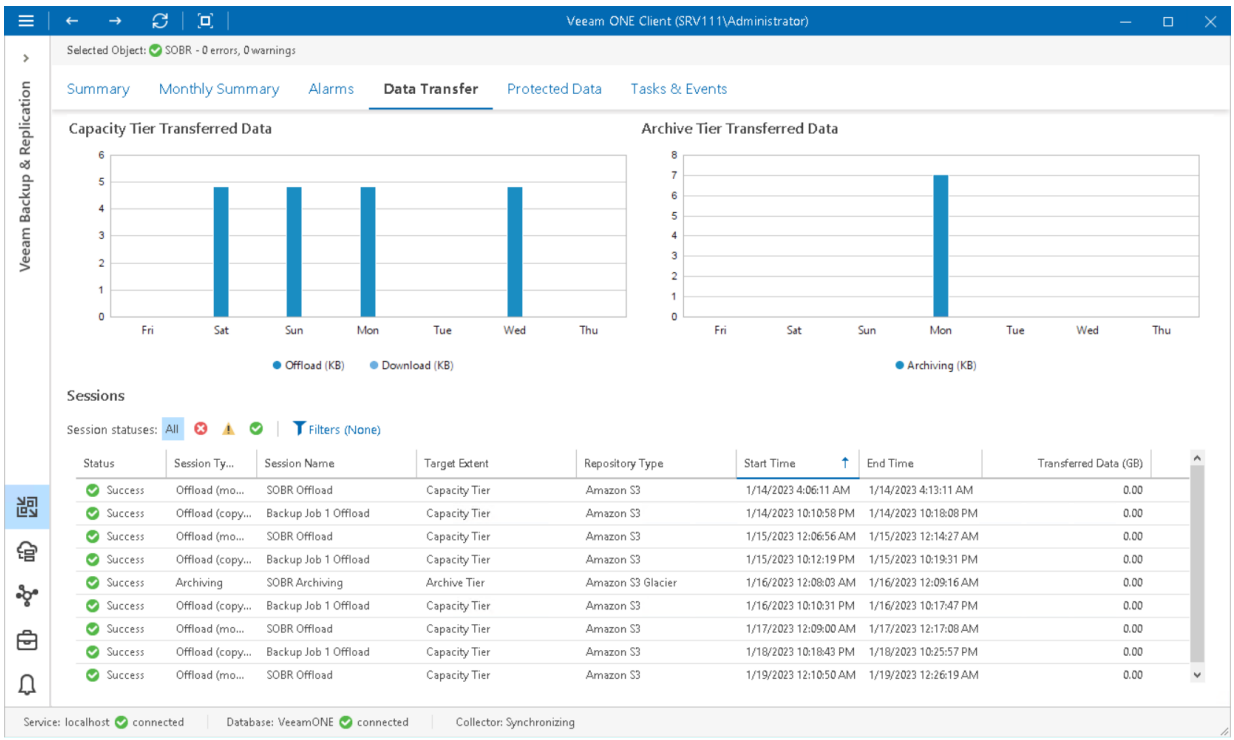
1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. In the inventory pane, click **Veeam Backup & Replication**.

3. In the inventory pane, select the necessary scale-out backup repository.

4. Open the **Data Transfer** tab.



Capacity Tier Transferred Data

The chart shows the amount of data transferred during capacity tier offload and download sessions.

Archive Tier Transferred Data

The chart shows the amount of data transferred during archive tier data transfer sessions.

Sessions

The list of sessions shows all types of data transfer sessions for the scale-out backup repository that you selected in the inventory pane. Each session in the list is described with a set of properties. To show or hide properties, right-click the list header and choose properties that must be displayed. To quickly find the necessary session, use the session status and session type filters at the top of the list.

- **Status** – latest status of the data transfer session (*Success*, *Warning*, *Failed*).

- **Session Type** – type of the data transfer session (*Offload (copy policy)*, *Offload (move policy)*, *Download*, *Archiving*, *Retrieval*).
- **Session Name** – name of the data transfer session.
- **Target Extent** – type of extent to which data transfer session is targeted (*Archive Tier*, *Capacity Tier*).
- **Repository Type** – type of the object storage repository used as the scale-out backup repository tier.
- **Start Time** – date and time when the data transfer session started.
- **End Time** – date and time when the data transfer session completed.
- **Transferred Data (GB)** – amount of data transferred between the tiers during the session.

Protected Data

The **Protected Data** tab allows you to view backups on repositories for the following workloads:

- Virtual Machines
- Computers
- Unstructured Data

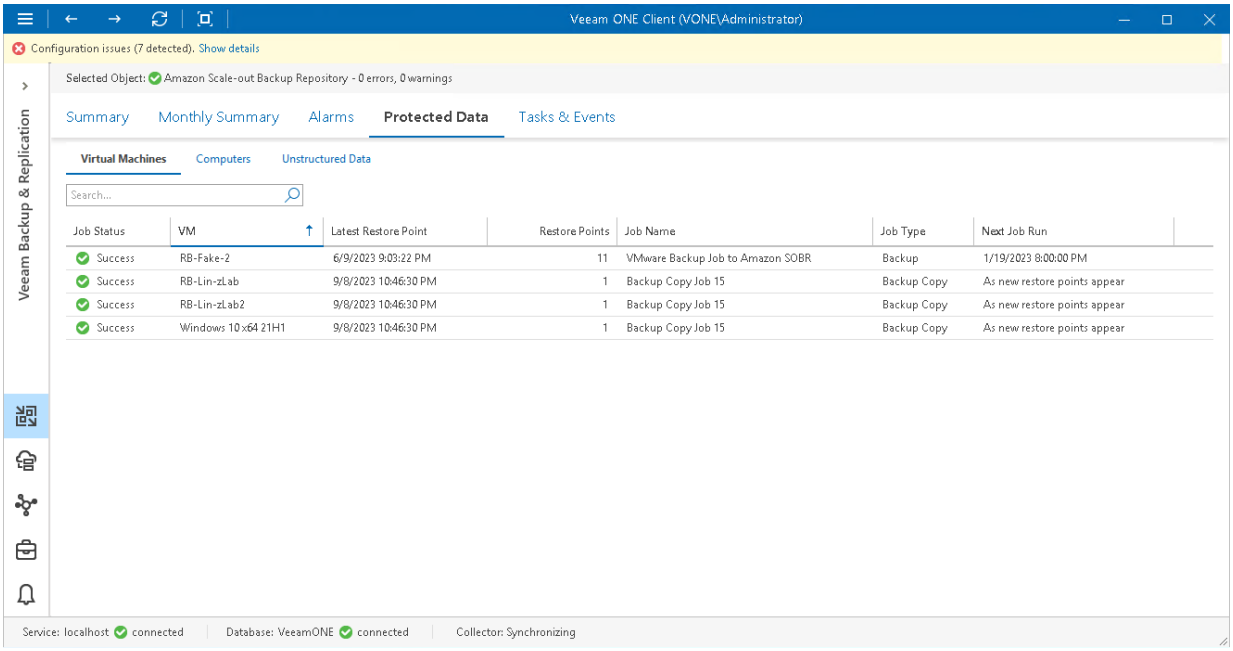
Virtual Machines

To view the list of VMs stored in backups on repositories:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click **Veeam Backup & Replication**.
3. In the inventory pane, select the necessary repository.
4. Open the **Protected Data** tab and navigate to **Virtual Machines**.
5. To quickly find VMs by name, use the **Search** field at the top of the list.



For every VM in the list, the following details are shown:

- **Job Status** – the latest status of the job that created the VM backup (*Success*, *Warning*, *Failed* or *Running*).
- **VM** – name of the VM stored in a backup on the repository.
- **Latest Restore Point** – date and time when the latest restore point was created for the VM.
- **Restore Points** – number of restore points created for the VM.
- **Job Name** – name of a backup or backup copy job that created VM backup.
- **Job Type** – type of the job that created the VM backup (*Backup job* or *Copy job*).
- **Next Job Run** – schedule according to which the job will start next time.

You can click column names to sort VMs by a specific parameter. For example, to view what VMs do not have recent backups, you can sort VMs in the list by **Latest Restore Point**.

Computers

To view the list of computers stored in backups on repositories:

1. Open Veeam ONE Client.

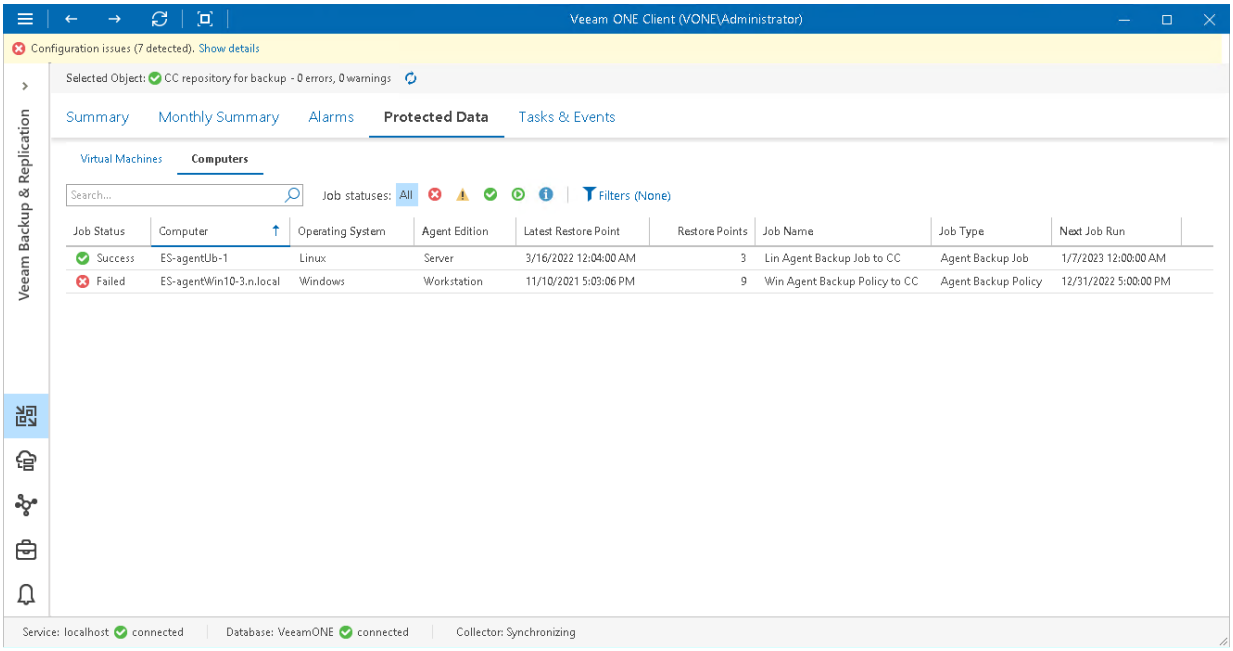
   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click **Veeam Backup & Replication**.

3. In the inventory pane, select the necessary repository.

4. Open the **Protected Data** tab and navigate to **Computers**.

5. To quickly find computers by name, use the filters and **Search** field at the top of the list.



For every computer in the list, the following details are shown:

- **Job Status** – the latest status of the job session that created the computer backup (*Success*, *Warning*, *Failed* or *Running*).
- **Computer** – name of the computer stored in a backup on the repository.
- **Operating System** – type of computer operating system (*Windows*, *Linux*, *Mac*, *AIX*, *Solaris*).
- **Agent Edition** – mode in which the backup agent job or policy operates (*Server*, *Workstation*, *Free*).
- **Latest Restore Point** – date and time when the latest restore point was created for the computer.
- **Restore Points** – number of restore points created for the computer.
- **Job Name** – name of the backup policy, backup or backup copy job that created computer backup.
- **Job Type** – type of the job that created the VM backup (*Agent Backup Policy*, *Agent Backup Job*, *Backup Copy*).
- **Next Job Run** – schedule according to which the job or policy will start next time.

You can click column names to sort computers by a specific parameter. For example, to view what computers do not have recent backups, you can sort computers in the list by **Latest Restore Point**.

Unstructured Data

To view the list of unstructured data stored in backups on repositories:

1. Open Veeam ONE Client.

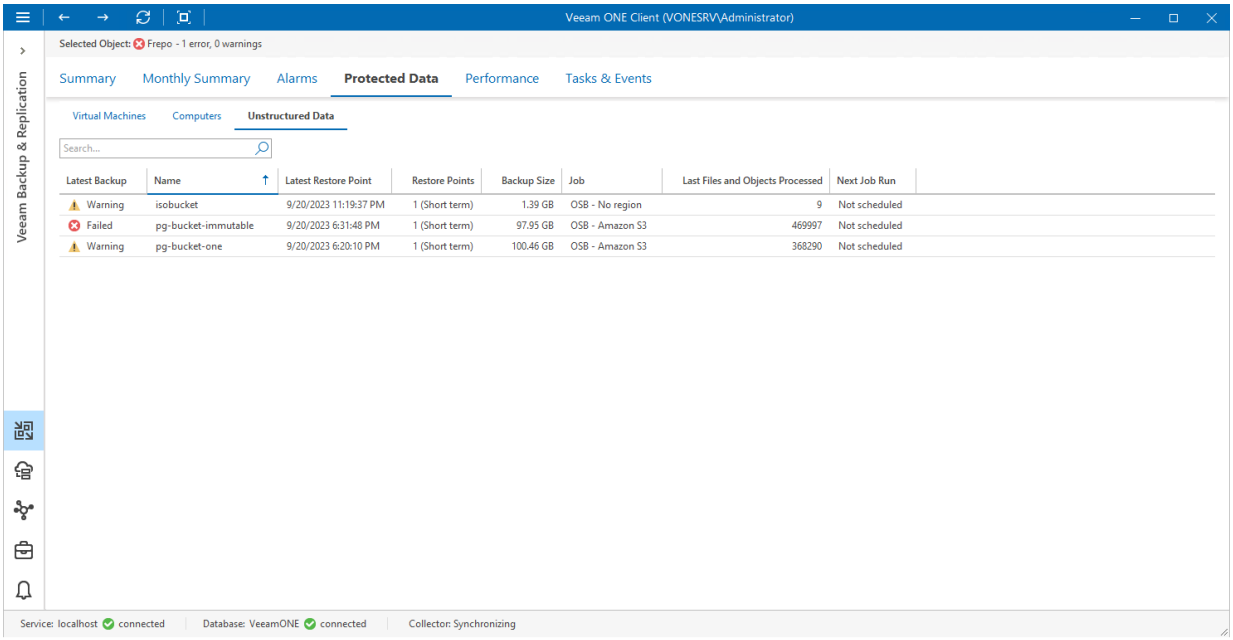
   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click **Veeam Backup & Replication**.

3. In the inventory pane, select the necessary repository.

4. Open the **Protected Data** tab and navigate to **Unstructured Data**.

5. To quickly find unstructured data by name, use the **Search** field at the top of the list.



For every unstructured data item in the list, the following details are shown:

- **Latest Backup** – the latest status of the job that created the unstructured data backup (*Success*, *Warning*, *Failed* or *Running*).
- **Name** – name of the protected file share or object storage.
- **Latest Restore Point** – date and time when the latest restore point was created for the unstructured data.
- **Restore Points** – number of short term and long term restore points stored on the repository.
- **Backup Size** – total size of unstructured data on the repository.
- **Job** – name of the job that created file share or object storage backup.
- **Last Files and Objects Processed** – number of files/objects processed during the last backup job session.
- **Next Job Run** – schedule according to which the job will start next time.

You can click column names to sort unstructured data by a specific parameter. For example, to view what unstructured data does not have recent backups, you can sort unstructured data in the list by **Latest Restore Point**.

Veeam Backup & Replication Events

The **Tasks & Events** dashboard shows the history of events that triggered Veeam Backup & Replication alarms. For the list and detailed description of data protection alarms, see Veeam Backup & Replication Alarms.

To view the list of events for a specific level:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click **Veeam Backup & Replication**.

3. In the inventory pane, select the necessary backup infrastructure node.

4. Open the **Tasks & Events** tab.

5. The **Tasks & Events** list can display up to 1000 tasks and events at a time. To find the necessary task or event, you can use the following controls:

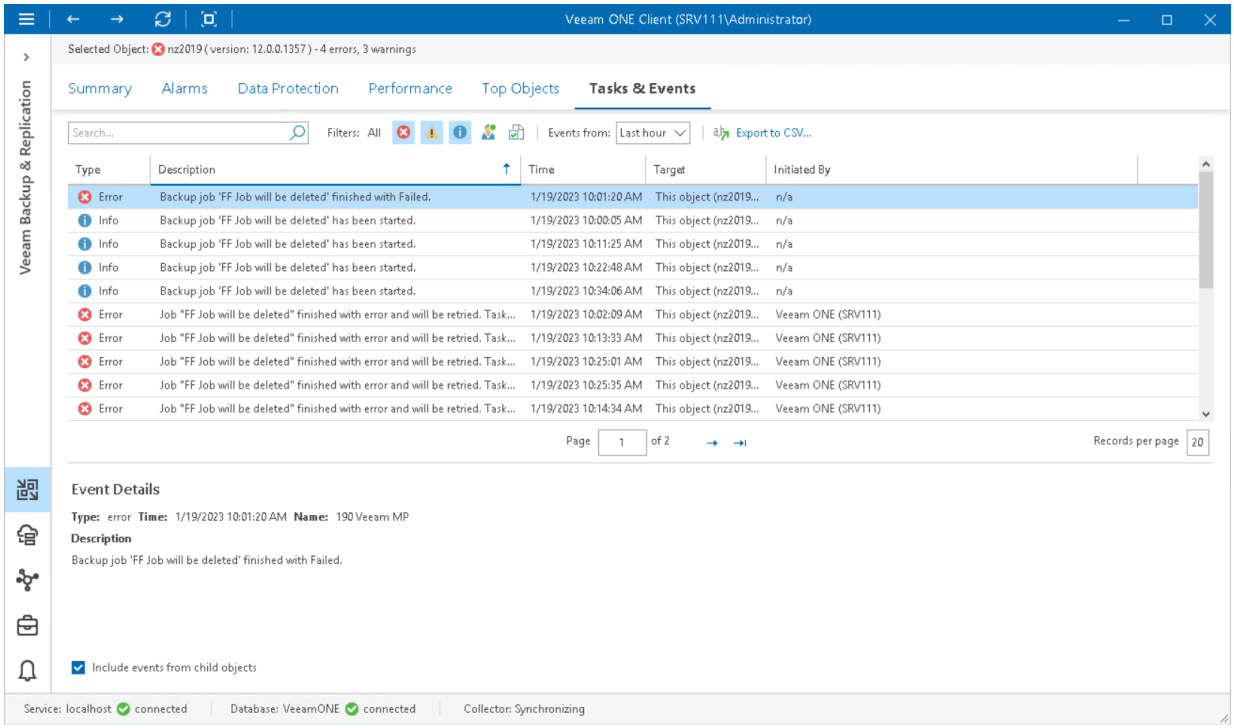
   - To display tasks or events for a specific period, select the necessary time interval from the **Events from** list.
   - To show or hide tasks or events, use filter buttons at the top of the list — *Show all events*, *Show errors*, *Show warnings*, *Show info messages*, *Show user events*, *Show tasks*.
   - To find the necessary tasks or events by description, use the **Search** field at the top of the list.

6. To view the detailed description of an event, click it in the list.

   The event description will be shown in the **Event Details** pane at the bottom.

   When you choose a virtual infrastructure container in the inventory pane, you can view events for the selected object and events for its child objects. To hide events related to child objects, clear the **Include events from child objects** check box at the bottom of the **Event Details** section.

7. To export displayed events to a CSV file, click **Export to CSV** at the top of the list and specify the location where the file will be saved.



Top Cloud Tenants

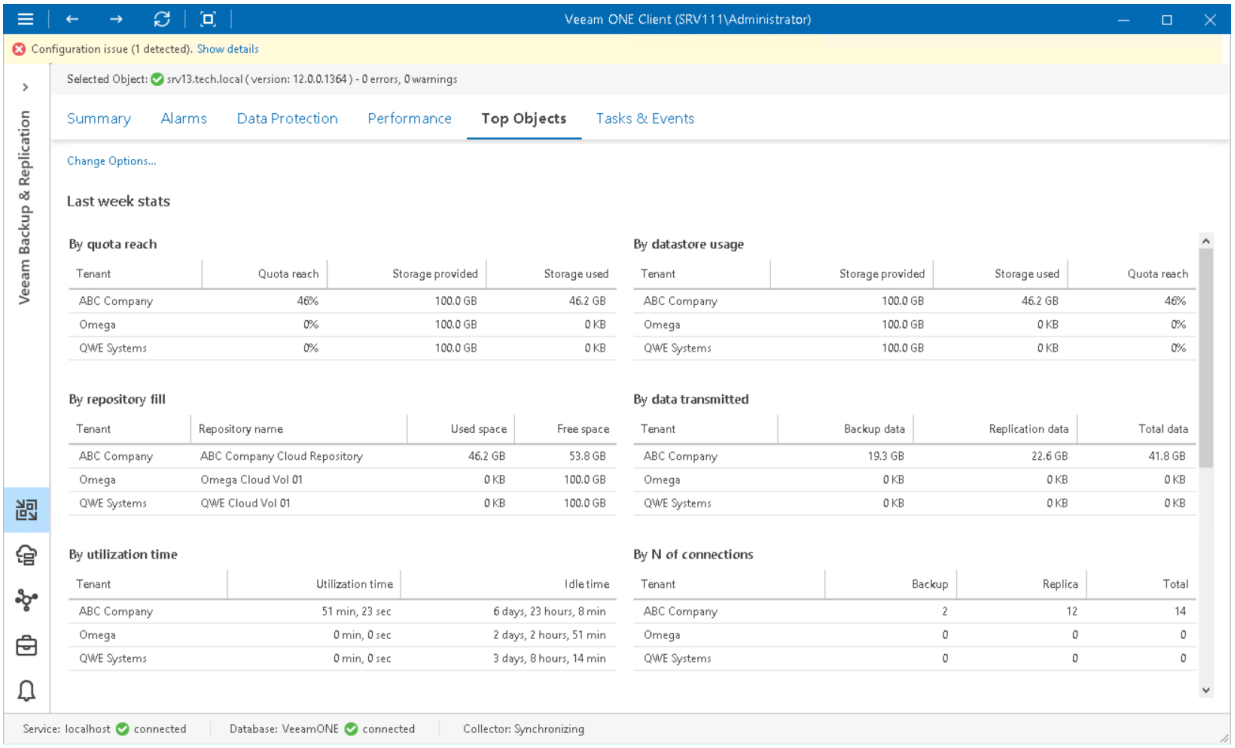
The **Top Objects** dashboard helps you detect top Veeam Cloud Connect users.

The dashboard displays top users in terms of transmitted data, used cloud storage space, number of connections, amount of gateway utilization time, traffic savings, peak transmission rate, number of failovers, number of replicated VMs and so on. By default, the dashboard displays top 3 user accounts ranged by consumed cloud repository space. You can change the number of displayed used accounts in the dashboard settings:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click **Veeam Backup & Replication**.
3. In the inventory pane, select the necessary backup server.
4. Open the **Top Objects** tab.
5. Click the **Change Options** link in the top left corner of the dashboard and select the necessary number of tenants to display.
6. Click **OK**.



Top Cloud Gateways

The **Top Objects** dashboard provides performance data of the most utilized cloud gateways for the selected server or gateway pool over the last week. The dashboard shows the most 'busy' cloud gateways for the last 7 days in terms of:

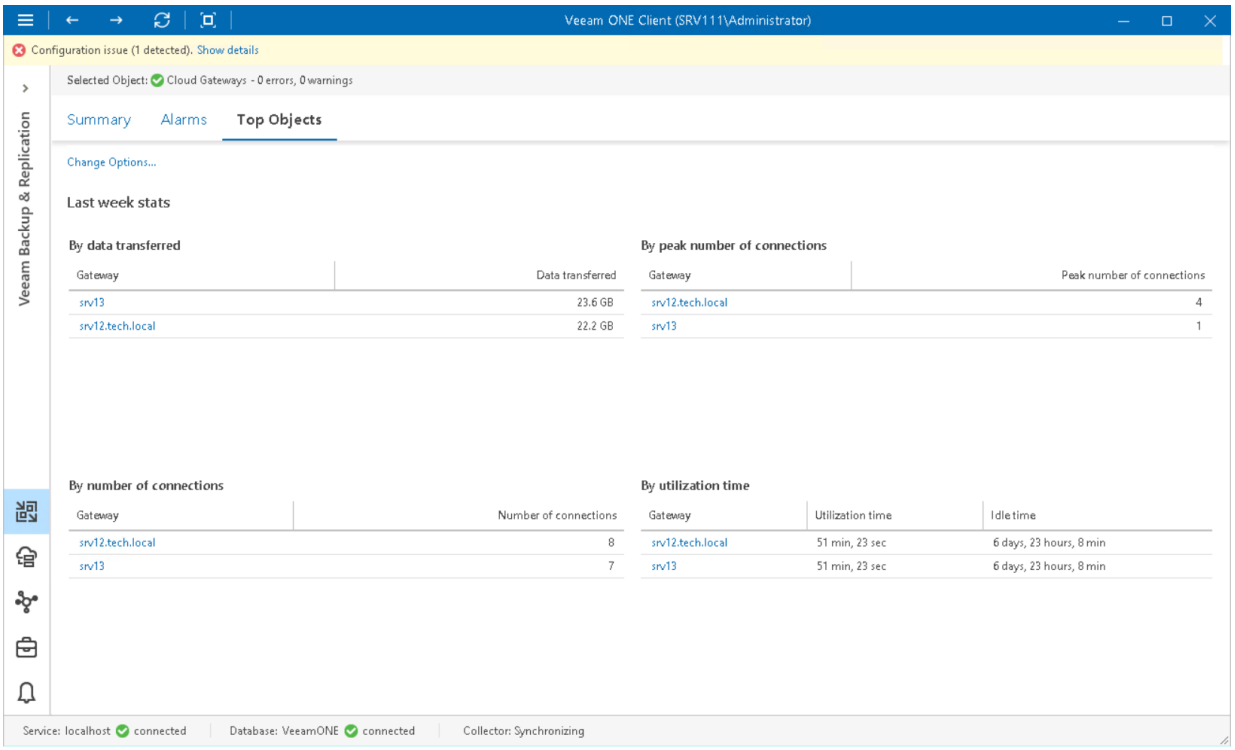
- Amount of data transferred to cloud repositories
- Number unique users connected to each cloud gateway
- Maximum number of user connections to the gateway
- Total amount of time the gateway was utilized

To view the list of the most loaded cloud gateways:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click **Veeam Backup & Replication**.
3. In the inventory pane, expand select the necessary node:
   - To view the most utilized standalone gateways, select the **Cloud Gateways** node under the necessary backup server.
   - To view the most utilized gateways from a gateway pool, select the necessary gateway pool under the **Cloud Gateways** node.
4. Open the **Top Objects** tab.



Veeam Backup for Microsoft 365 Monitoring

Veeam ONE Client offers advanced functionality for monitoring Veeam Backup for Microsoft 365 infrastructure and data protection operations in the managed virtual environment.

With Veeam ONE Client, you can:

1. **Monitor the overall state of the backup infrastructure**.

   Check the **Summary** dashboards to reveal hotspots in the Veeam Backup for Microsoft 365 infrastructure.

   Quickly review the latest status of data protection jobs, examine configuration and performance of your backup infrastructure components, detect the most loaded proxies and repositories and check whether your jobs complete within the backup window.

   Summary dashboards help you quickly reveal issues that can lead to job failure, and cause loss of valuable data.

2. **View triggered alarms**.

   Go to the **Alarms** dashboard to see details on issues and problems in your backup infrastructure.

   Data protection alarms allow you to instantaneously react to potentially dangerous situations with ongoing data protection and take immediate actions to eliminate the risk of data loss.

3. **Check the latest job status**.

   Track the status of your backup jobs.

   Get up-to-date information on the efficiency of data protection in your virtual environment and address problems with jobs as soon as they appear.

4. **Work with performance charts**.

   Drill down to performance charts to diagnose performance problems with backup infrastructure components and identify bottlenecks.

   Track CPU, memory, disk and network performance for Veeam Backup for Microsoft 365 servers and proxies to make sure the backup data flow is efficient, and all resources engaged in the backup process are optimally used.

5. **View the list of events**.

   View the full list of events that triggered Veeam Backup for Microsoft 365 alarms, and events notifying about connection problems with Veeam Backup for Microsoft 365 servers.

Prerequisites

Before you start monitoring the Veeam Backup for Microsoft 365 infrastructure, make sure you have configured connections to Veeam Backup for Microsoft 365 servers from which Veeam ONE will collect data. For details on configuring server connections, see Connecting Veeam Backup for Microsoft 365 Servers.

> **NOTE:**
>
> Veeam ONE monitors cloud Organizations protection only, monitoring of hybrid and on-premise (Exchange) platform protection is not supported.

In This Section

- Veeam Backup for Microsoft 365 Summary Dashboards
- Veeam Backup for Microsoft 365 Alarms
- Veeam Backup for Microsoft 365 Data Protection
- Veeam Backup for Microsoft 365 Performance Charts
- Veeam Backup for Microsoft 365 Protected Data
- Veeam Backup for Microsoft 365 Events

Veeam Backup for Microsoft 365 Summary Dashboards

Veeam Backup for Microsoft 365 summary dashboards serve as the 'launch point' for monitoring the backup infrastructure and data protection operations. The dashboards reflect the latest state of backup jobs, and help you analyze the performance and configuration of backup infrastructure components.

Veeam ONE Client offers the following types of summary dashboards for Veeam Backup & Replication infrastructure components:

- Veeam Backup for Microsoft 365 Infrastructure Summary
- Veeam Backup for Microsoft 365 Repositories Overview
- Veeam Backup for Microsoft 365 Repository Summary
- Veeam Backup for Microsoft 365 Proxies Overview
- Veeam Backup for Microsoft 365 Proxy Summary
- Veeam Backup for Microsoft 365 Proxy Pools Summary

Veeam Backup for Microsoft 365 Infrastructure Summary

The Veeam Backup for Microsoft 365 infrastructure summary dashboard shows the latest state of data protection operations and indicates the most intensively used resources in the infrastructure.

The dashboard is available for the following nodes:

- Veeam Backup for Microsoft 365 Infrastructure
- Veeam Backup for Microsoft 365 server



Protected Objects by Object Type

The section provides the following details:

- Number of organizations with object backups
- Number of objects (*Users*, *Groups*, *Sites*, *Teams*) with backups

Job Status

The charts reflect the latest status of Veeam Backup for Microsoft 365 protection jobs for the selected level of the infrastructure hierarchy.

Every chart segment shows how many jobs ended with a specific status — failed jobs (red), jobs that ended with warnings (yellow), successfully performed jobs (green), and jobs that are currently running (blue). Click the necessary chart segment or a legend label to drill down to the list of jobs that ended up with the corresponding status.

Backup Repositories Overview

The section provides the following details:

- Total number of backup repositories for the selected infrastructure node
- Number of repositories extended with an object storage
- Number of object storage repositories

Backup Proxies Overview

The section provides the following details:

- Number of proxies for the selected infrastructure node
- Number of jobs that the proxies are currently processing
- Number of jobs queued for processing

Top Repositories by Used Space

The chart shows 5 backup repositories with the greatest amount of used storage space.

For every repository in the chart, you can track the amount of used storage space against the amount of available space. If free space on the repository is running low, you may need to free up storage space, revise your backup retention policy or even move your backups from the repository and point backup jobs to a new location.

To display object storage data in this widget, you must first set the capacity limit for these repositories in your Veeam Backup for Microsoft 365 configuration. To do this, select the **Limit object storage consumption to** check box and specify the limit value in GB, TB or PB. For details on see Adding Object Storage Repositories.

Top Backup Proxies by Weekly Transferred Data

The chart shows 5 backup proxies that processed the greatest amount of data over the past 7 days.

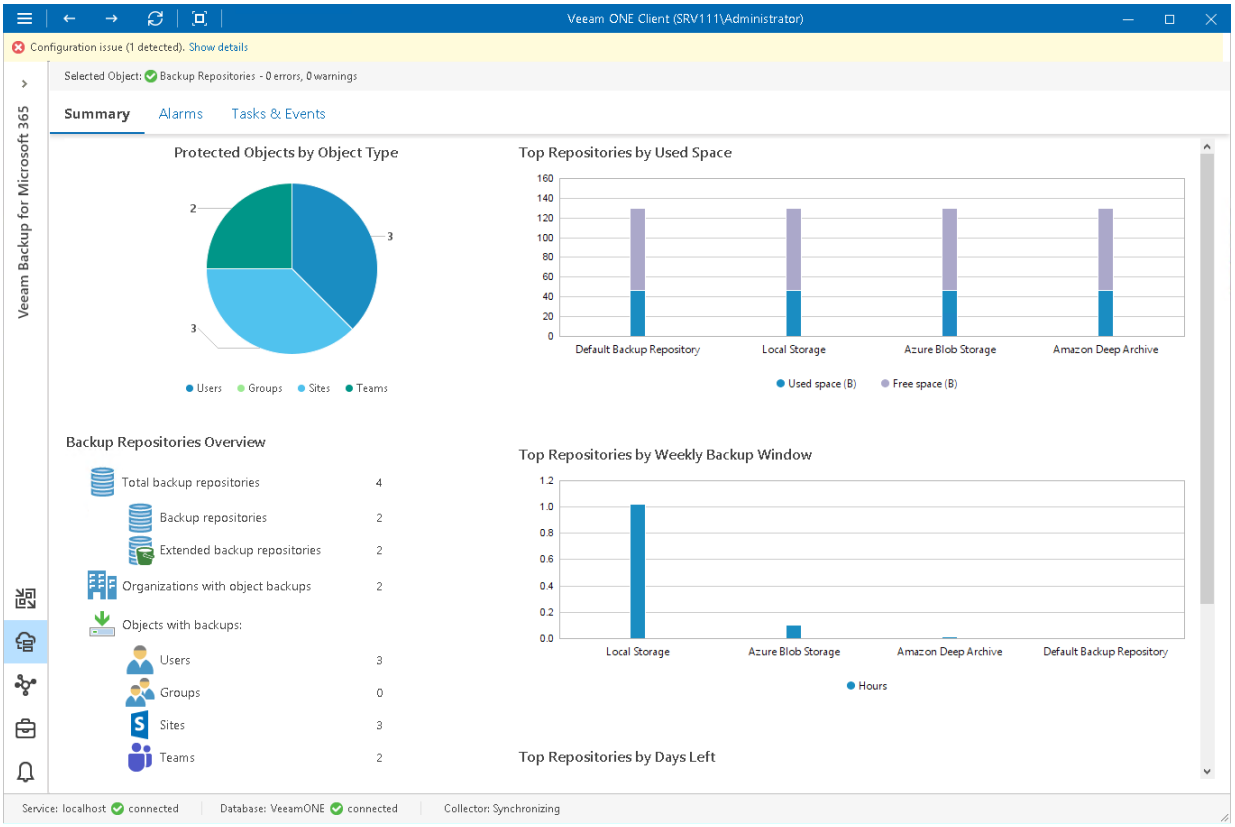
To draw the chart, Veeam ONE analyzes how many object processing tasks were successfully performed by every proxy; failed tasks are not taken into account.

The chart helps you detect the most heavily loaded proxies and optimize the performance of your backup infrastructure. If specific proxies are overloaded with processing tasks, and the jobs often need to wait for proxy resources, you may need to deploy additional proxies or balance the processing load by assigning jobs to other proxies.

Veeam Backup for Microsoft 365 Repositories Overview

The summary dashboard for the **Repositories** node provides a configuration overview and performance analysis for backup repositories and object storage extents managed by Veeam Backup for Microsoft 365 server.

Backup Repositories



Protected Objects by Object Type

The chart displays types of objects protected with Veeam Backup for Microsoft 365 jobs and policies.

Every chart segment shows the number of objects of a specific type — the number of protected Users, Groups, Sites or Teams.

Backup Repositories Overview

The section provides the following details:

- Total number of repositories managed by Veeam Backup for Microsoft 365 server
- Number of backup repositories and repositories extended with object storage
- Number of organizations with object backups that reside on backup repositories
- Number of Users, Groups, Sites and Teams backups that reside on backup repositories

Top Repositories by Used Space

The chart shows backup repositories with the greatest amount of used storage space.

For every repository in the chart, you can see the amount of storage space used by Microsoft 365 object backups against the amount of available space. If free space on the repository is running low, you may need to free up storage space on the repository or revise your backup retention policy.

To display object storage data in this widget, you must first set the capacity limit for these repositories in your Veeam Backup for Microsoft 365 configuration. To do this, select the **Limit object storage consumption to** check box and specify the limit value in GB, TB or PB. For details on see Adding Object Storage Repositories.

Top Repositories by Weekly Backup Window

The chart allows you to detect the most 'busy' repositories over the past 7 days.

For every repository, the chart shows the cumulative amount of time that the repository was busy with backup job tasks.

Top Repositories by Days Left

The chart shows backup repositories that can run low on storage space sooner than others.

To draw the chart, Veeam ONE analyzes historical data and checks how fast free space on repositories has been decreasing in the past. Veeam ONE uses historical statistics to forecast how soon the repository will run out of space.

To display object storage data in this widget, you must first set the capacity limit for these repositories in your Veeam Backup for Microsoft 365 configuration. To do this, select the **Limit object storage consumption to** check box and specify the limit value in GB, TB or PB. For details on see Adding Object Storage Repositories.

Object Storage

Protected Objects by Object Type

The chart displays types of objects protected with Veeam Backup for Microsoft 365 jobs and policies.

Every chart segment shows the number of objects of a specific type — the number of protected Users, Groups, Sites or Teams.

Object Storage Overview

The section provides the following details:

- Total number of object storage extents
- Number of organizations with object backups that reside on object storage extents
- Number of Users, Groups, Sites and Teams backups that reside on object storage extents

Space Usage

The chart shows the amount of used storage space in object storage.

If free space in the object storage is running low, you may need to free up storage space, revise your backup retention policy, or consider pointing jobs to another repository.

Top Object Storage by Used Space

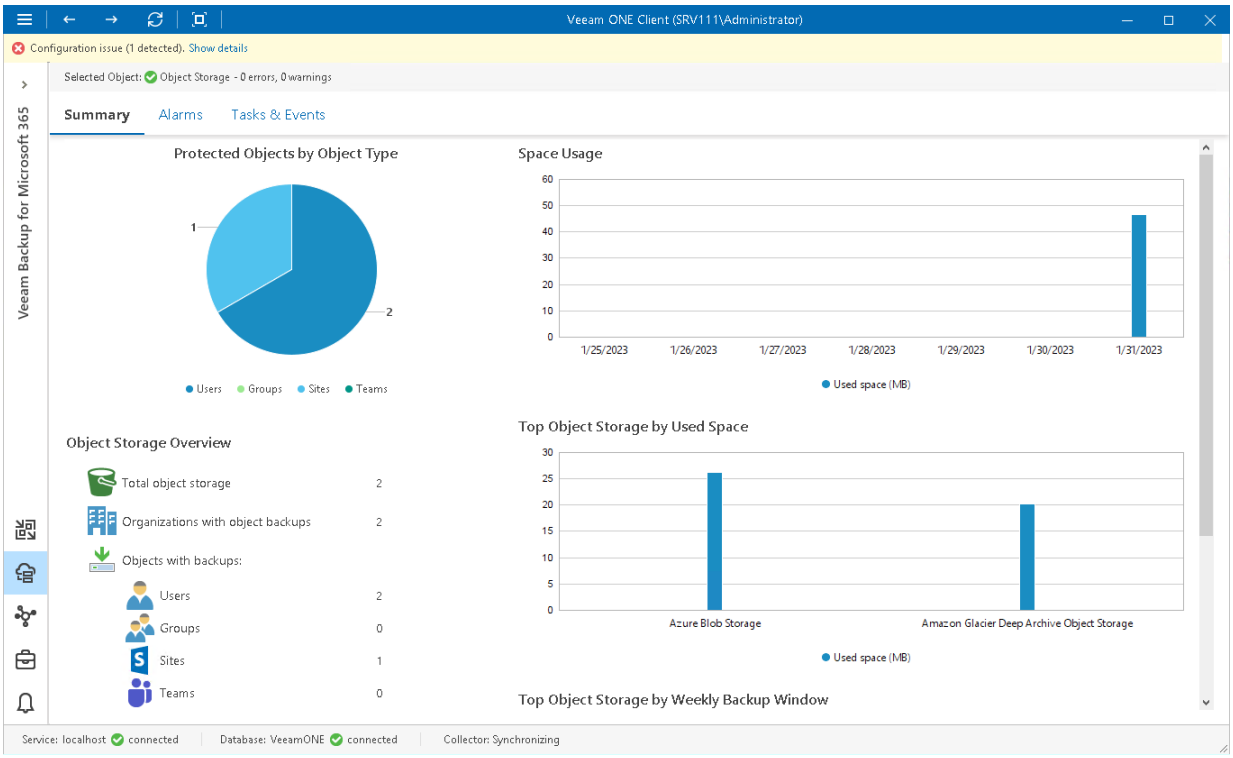
The chart shows object storage extents with the greatest amount of used storage space.

For every object storage in the chart, you can see the amount of storage space used by Microsoft 365 object backups. If free space in the object storage is running low, you may need to free up storage space or revise your backup retention policy.

Top Object Storage by Weekly Backup Window

The chart allows you to detect the most 'busy' object storage extents over the past 7 days.

For every repository, the chart shows the cumulative amount of time that the repository was busy with backup job tasks.

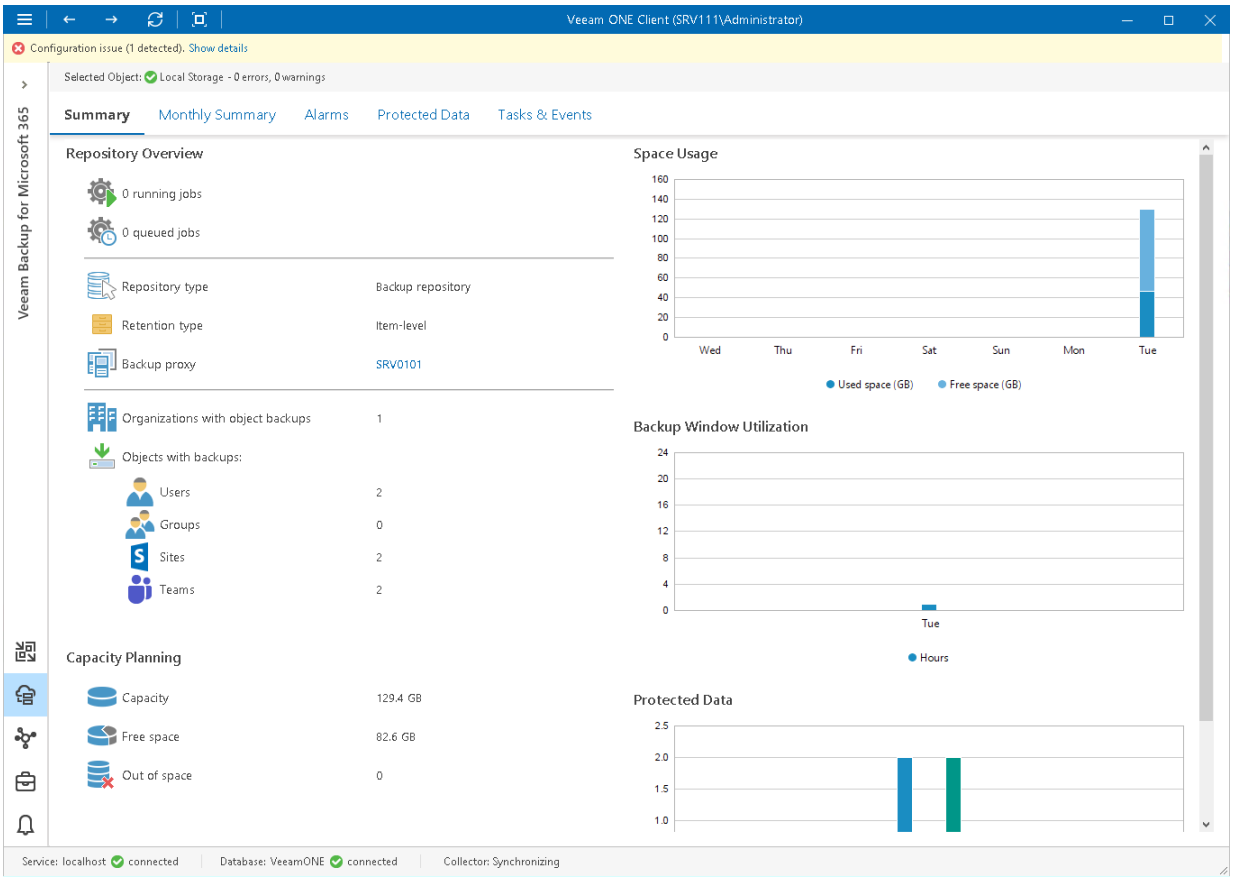


Veeam Backup for Microsoft 365 Repository Summary

Veeam ONE Client offers the following types of summary dashboards for backup repositories and object storage extents managed by Veeam Backup for Microsoft 365 server.

Backup Repository

The backup repository summary dashboard provides overview details, capacity planning information and performance analysis for a chosen backup repository for the last week or month.



Repository Overview

The section provides the following details:

- Number of jobs that are currently running and queued on the repository
- Repository type: Backup repository
- Backup proxy that processes jobs targeted to the repository
- Type of retention configured in the repository settings
- Number of organizations with object backups that reside on the repository
- Number of Users, Groups, Sites and Teams backups that reside on the repository

Capacity Planning

The section provides the following details:

- Storage capacity of the repository
- Amount of free space on the repository
- Number of days before the repository runs out of free space

To forecast the value, Veeam ONE uses a trend that is calculated based on historical statistics — it analyzes how fast the amount of free space on the repository was decreasing in the past and uses historical statistics to forecast how soon the repository will run out of space.

To display object storage data in this widget, you must first set the capacity limit for these repositories in your Veeam Backup for Microsoft 365 configuration. To do this, select the **Limit object storage consumption to** check box and specify the limit value in GB, TB or PB. For details on see Adding Object Storage Repositories.

Space Usage

The chart shows the amount of used storage space on the repository.

If free space on the repository is running low, you may need to free up storage space, revise your backup retention policy, or consider pointing jobs to another repository.

To display object storage data in this widget, you must first set the capacity limit for these repositories in your Veeam Backup for Microsoft 365 configuration. To do this, select the **Limit object storage consumption to** check box and specify the limit value in GB, TB or PB. For details on see Adding Object Storage Repositories.

Backup Window Utilization

The chart shows the cumulative amount of time that the repository was busy with backup job tasks during the past week or month.

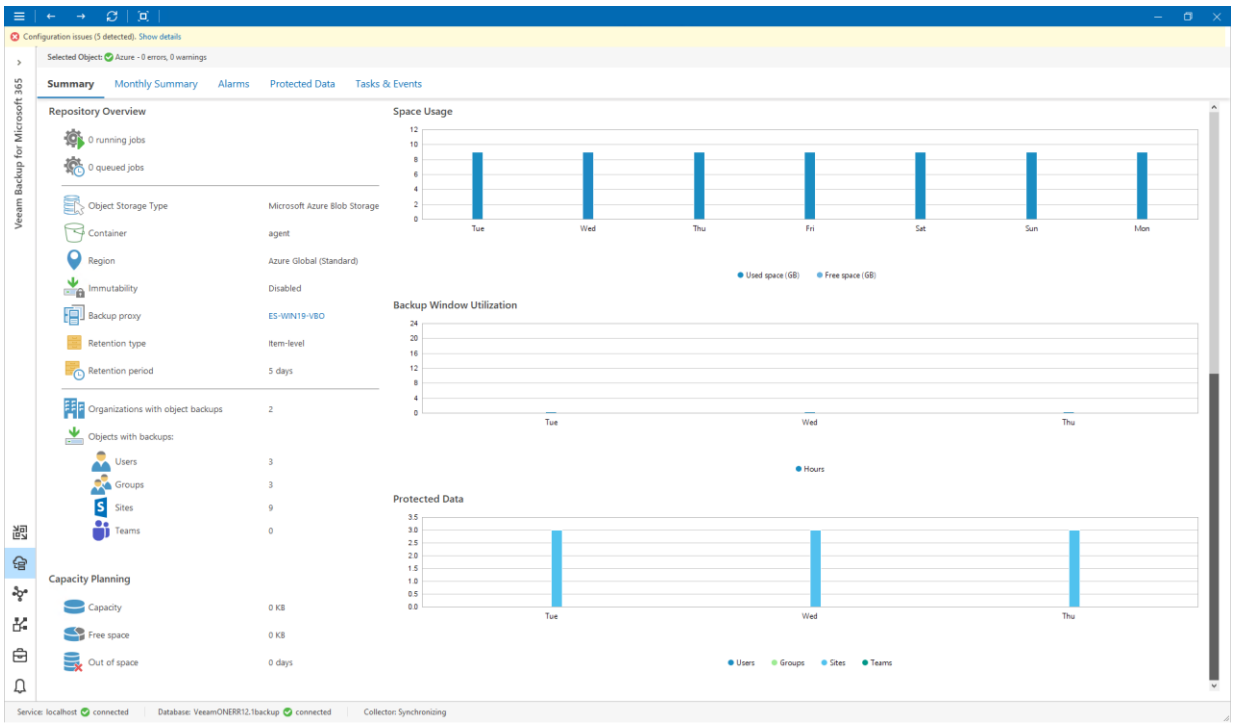
The chart can help you reveal possible resource bottlenecks on the repository side. If the backup window on the chart is abnormally large, this may evidence that the required I/O operations cannot complete fast enough, and your target is presenting a bottleneck for the whole backup data processing conveyor. To identify performance bottlenecks, you can switch to repository Veeam Backup for Microsoft 365 Performance Charts.

Protected Data

The chart shows the number of Microsoft 365 objects (Users, Groups, Sites, Teams) whose data was backed up to the repository during the past week or month.

Object Storage

The object storage summary dashboard provides overview details, capacity planning information and performance analysis for a chosen object storage repository for the last week or month.



Repository Overview

The section provides the following details depending on the repository type:

- Number of jobs that are currently running and queued on the object storage
- Object storage type
- Name of bucket or container
- Region at which the storage is located
- Immutability feature state (Enabled, Disabled, N/A)
- Governance mode (Enabled, Disabled, N/A)
- Backup proxy that processes jobs targeted to the repository
- Retention type configured in the object storage settings
- Retention period
- Connected object storage
- Storage consumption limit (Enabled, Disabled, N/A)
- Class of the infrequent access storage
- Number of organizations with object backups that reside on the repository
- Number of Users, Groups, Sites and Teams backups that reside on the repository

Capacity Planning

The section provides the following details:

- Amount of used space in the object storage
- Number of days before the object storage runs out of free space

To forecast the value, Veeam ONE uses a trend that is calculated based on historical statistics — it analyzes how fast the amount of used space in the object storage was increasing in the past and uses historical statistics to forecast how soon the object storage will run out of space.

Space Usage

The chart shows the amount of used space in the object storage.

If free space in the object storage is running low, you may need to free up storage space, revise your backup retention policy, or consider pointing jobs to another repository.

Backup Window Utilization

The chart shows the cumulative amount of time that the object storage was busy with backup job tasks during the past week or month.

The chart can help you reveal possible resource bottlenecks on the object storage side. If the backup window on the chart is abnormally large, this may evidence that the required I/O operations cannot complete fast enough, and your target is presenting a bottleneck for the whole backup data processing conveyor.

Protected Data

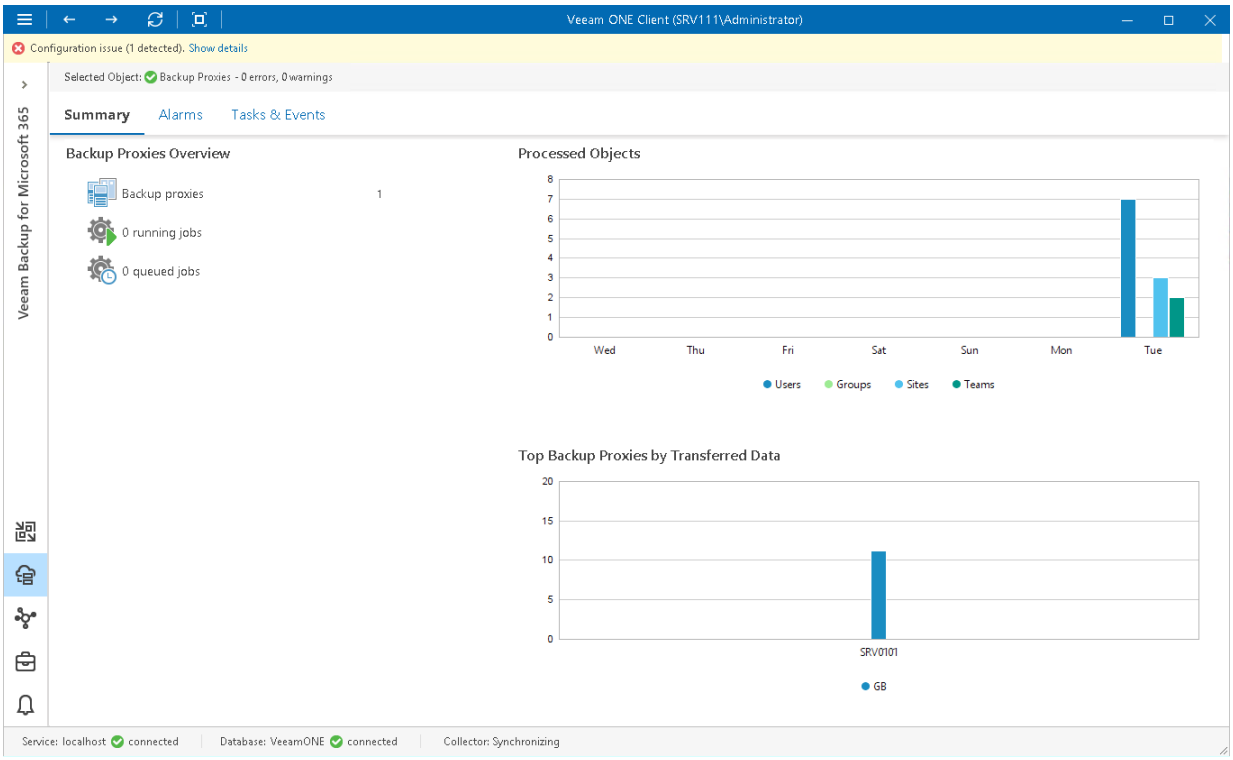
The chart shows the number of Microsoft 365 objects (Users, Groups, Sites, Teams) whose data was backed up to the repository during the past week or month.

Veeam Backup for Microsoft 365 Proxies Overview

The summary dashboard for the **Backup Proxies** node provides a configuration overview and performance analysis for backup proxies managed by a Veeam Backup for Microsoft 365 server.

This dashboard can help you detect configuration inefficiencies in your data protection infrastructure. If the same proxy server appears to process a great number of objects, transfer the greatest amount of backup data and use the largest backup window, you may need to re-balance the processing load across your backup proxies. The charts may also help you reveal 'lazy' proxies that you may decide to decommission.

Proxies can also be grouped together into proxy pools in order to operate as a single point of entry for your processing load. The backup proxy pool is a logical entity that groups any number of backup proxy servers.



Backup Proxies Overview

The section provides the total number of backup proxies for the chosen Veeam Backup for Microsoft 365 infrastructure node and the total number of running and queued jobs that these proxies process.

Processed Objects

The chart shows the number of Microsoft 365 objects (Users, Groups, Sites, Teams) whose data the proxies processed during the past week.

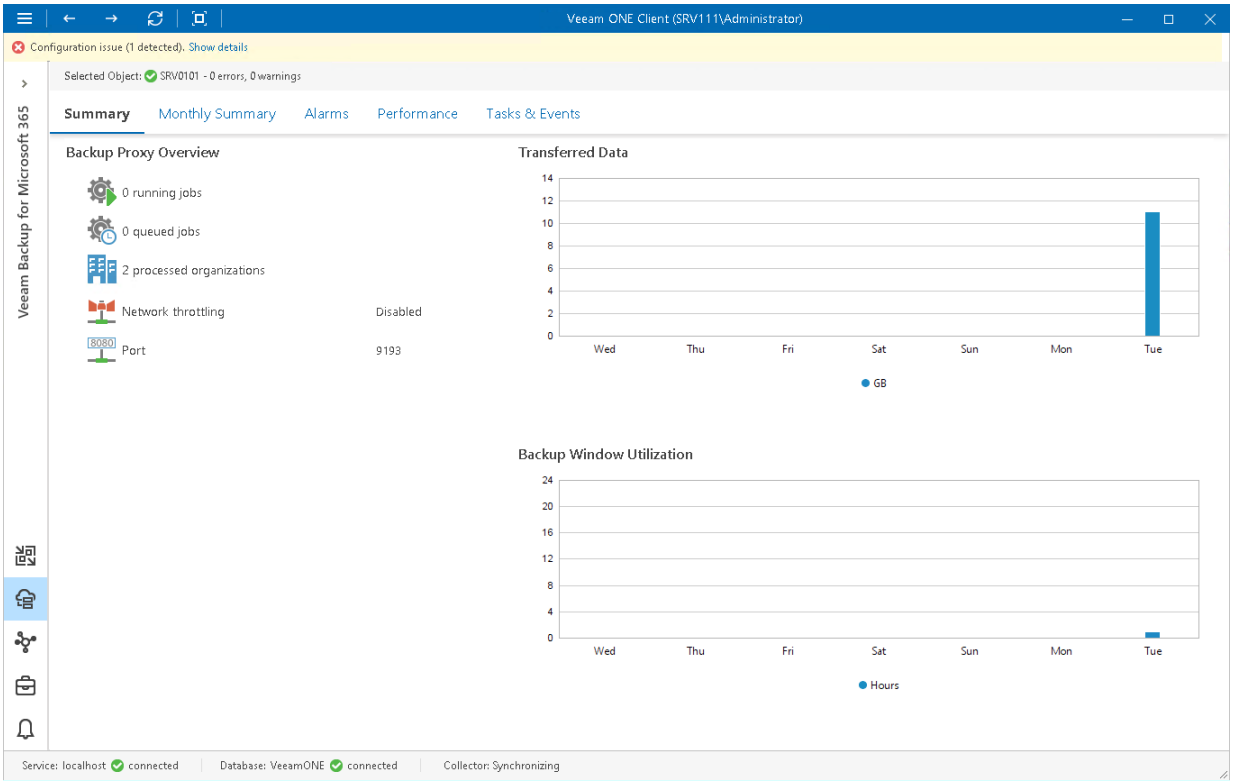
Top Backup Proxies by Transferred Data

The chart shows backup proxies that transferred the greatest amount of backup data to the target destination over the past 7 days.

For every proxy, the chart shows the total amount of data that the proxy transferred over the network after the source-side deduplication and compression. The chart can help you detect backup proxies that transfer the greatest amount of backup data and estimate the load that backup jobs impose on the network.

Veeam Backup for Microsoft 365 Proxy Summary

The proxy summary dashboard provides overview details and performance analysis for a chosen backup proxy for the last week or month.



Backup Proxy Overview

The section provides the following details:

- Number of jobs that the proxy is currently processing
- Number of jobs queued for processing
- Number of Microsoft 365 organizations that are proxy processed
- Local Network throttling settings configured in the backup proxy settings
- Port through which the proxy communicates with Veeam Backup for Microsoft 365 server

Transferred Data

The chart shows the amount of backup data that the proxy transferred to the target destination (backup repository or object storage) over the last 7 days.

The chart shows the total amount of data that the proxy transferred over the network after the source-side deduplication and compression. The chart can help you measure the amount of backup traffic coming from the proxy.

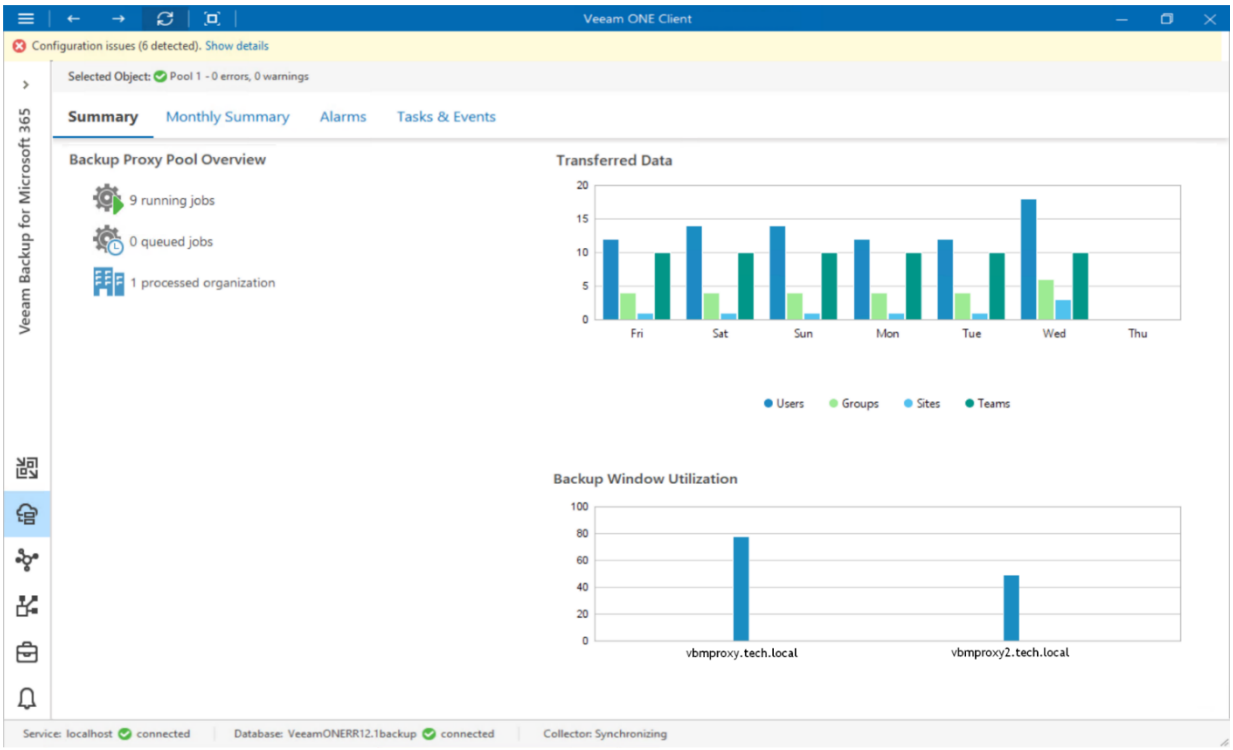
Backup Window Utilization

The chart allows you to estimate how 'busy' the proxy was during the last 7 days. The chart shows the cumulative amount of time that the proxy was retrieving, processing and transferring Veeam Backup for Microsoft 365 data.

The chart can help you reveal possible resource bottlenecks. If the backup window on the chart is abnormally large, this can evidence of low source data retrieval speed, high proxy CPU load or insufficient network throughput. To identify performance bottlenecks, you can switch to proxy Veeam Backup for Microsoft 365 Performance Charts.

Veeam Backup for Microsoft 365 Proxy Pools Summary

The proxy pool summary dashboard provides overview details and performance analysis for a chosen backup proxy pool for the last week or month.



Backup Proxy Overview

The Proxy Pools section provides the following details:

- Number of jobs that the proxy pool is currently processing
- Number of jobs queued for processing
- Number of processed Microsoft 365 organizations

Transferred Data

The chart shows the amount of backup data that the proxies in the pool transferred to the target destination (backup repository or object storage) over the last 7 days.

The chart shows the total amount of data that the proxy pool transferred over the network after the source-side deduplication and compression. The chart can help you measure the amount of backup traffic coming from the proxy pool.

Backup Window Utilization

The chart allows you to estimate how 'busy' the proxy pool was during the last 7 days. The chart shows the cumulative amount of time that the proxies in the pool was retrieving, processing and transferring Veeam Backup for Microsoft 365 data.

The chart can help you reveal possible resource bottlenecks. If the backup window on the chart is abnormally large, this can evidence of low source data retrieval speed, high proxy CPU load or insufficient network throughput.

Veeam Backup for Microsoft 365 Alarms

Veeam ONE includes a set of alarms to monitor the efficiency of Veeam Backup for Microsoft 365 data protection.

Predefined data protection alarms are configured to warn you about events or issues that can cause loss of data or prevent Veeam Backup for Microsoft 365 infrastructure from functioning properly:

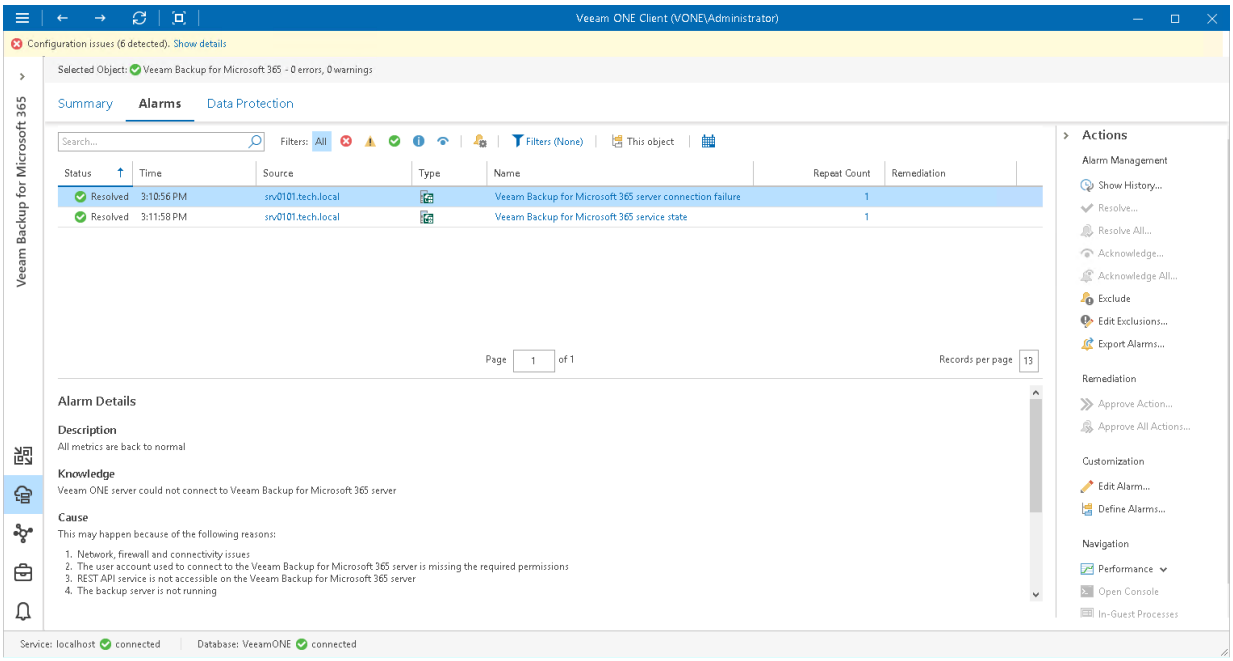
- Connectivity issues and inability of backup infrastructure components to communicate with each other
- State of Veeam Backup for Microsoft 365 software installed on backup infrastructure components
- Failing jobs or jobs finished with warnings
- Configuration issues, such as fast decreasing space on backup repositories
- Long-running jobs that exceed the backup window
- Product license and prepaid support contract

To view the list of data protection alarms:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.
2. At the bottom of the inventory pane, click **Veeam Backup for Microsoft 365**.
3. In the inventory pane, select the necessary backup infrastructure node.
4. Open the **Alarms** tab.

On the **Alarms** dashboard, you can view triggered alarms, track alarm history, resolve and acknowledge alarms and perform other actions. For details on available actions, see Working with Triggered Alarms.



Veeam Backup for Microsoft 365 Data Protection

Veeam ONE Client allows you to track jobs configured to protect Microsoft 365 objects with Veeam Backup for Microsoft 365.

You can track real-time job statistics at different levels of your infrastructure:

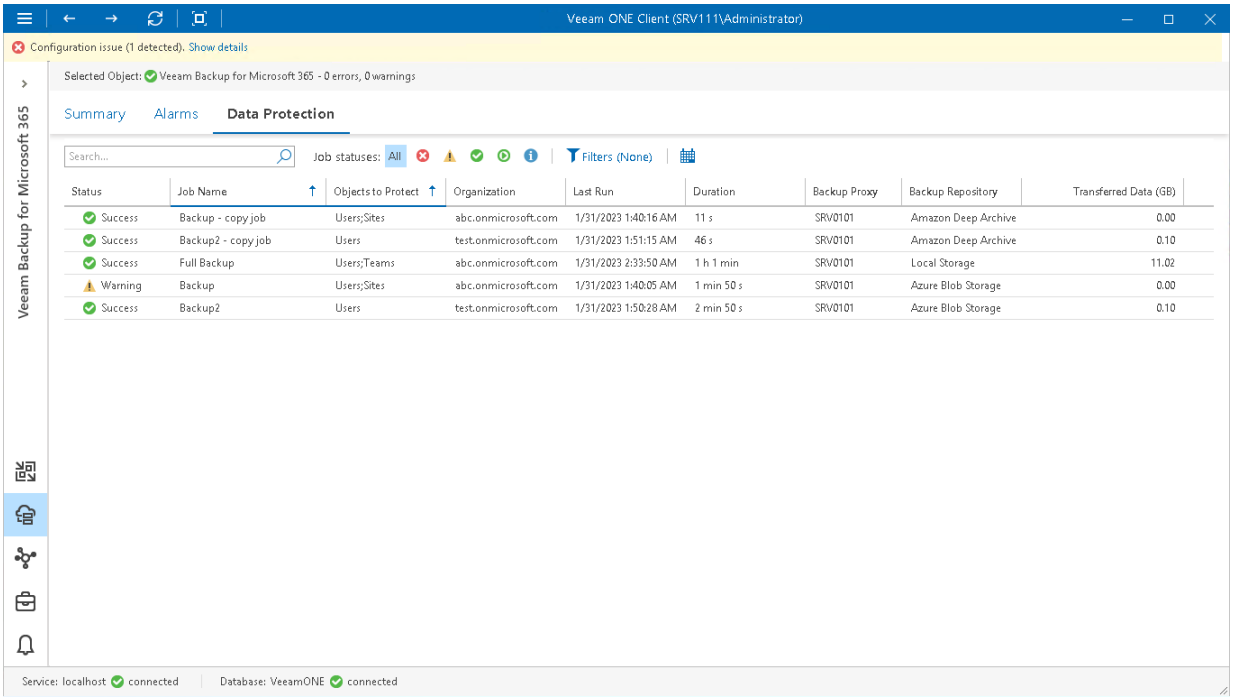
- Jobs on a specific Veeam Backup for Microsoft 365 server
- All jobs across the entire Veeam Backup for Microsoft 365 infrastructure

To view the list of jobs at the necessary backup infrastructure level:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.
2. At the bottom of the inventory pane, click **Veeam Backup for Microsoft 365**.
3. In the inventory pane, select the necessary infrastructure node.
4. Open the **Data Protection** tab.
5. To find the necessary job, you can use filters at the top of the job list:
   - To show or hide jobs that ended with a specific status, use the status buttons at the top of the list (*Show failed jobs*, *Show jobs with warnings*, *Show successful jobs*, *Show running jobs* or *Show jobs with no status*).
   - To show or hide jobs of a specific type, use the job type filter at the top of the list (*Backup*, *Backup copy*).
   - To show or hide jobs that protect specific object types, use the objects filter at the top of the list (*Entire organization, Users, Groups, Sites, Teams*).
   - To set the time interval when jobs ran for the last time, use the **Filter jobs by time period** button. Release the button to discard the time period filter.
   - To find jobs by name, use the search field at the top of the list.

The list of jobs shows all types of VM jobs for the backup infrastructure level that you selected in the inventory pane.



For every job, the following details are available:

- **Status** – the latest status of the job session (*Success*, *Warning*, *Failed*, *Running*, or jobs with no status).
- **Job Name** – name of a job.
- **Objects to Protect** – list of objects included in the job.
- **Organization** – name of Microsoft organization to which protected objects belong.
- **Last Run** – date and time of the latest job run.
- **Duration** – time taken to complete the job during its latest run.
- **Backup Proxy** – name of the backup proxy configured in job settings.
- **Backup Repository** – name of the target backup repository.
- **Transferred Data (GB)** – amount of backup data that was transferred to the target destination during the latest job run.

Veeam Backup for Microsoft 365 Performance Charts

To identify performance bottlenecks within the backup data flow, you can drill down to the following performance charts:

- CPU Performance Chart
- Memory Performance Chart
- Disk Performance Chart
- Network Performance Chart

To draw the charts, Veeam ONE gathers Windows Performance Monitor metrics from the guest OS of Veeam Backup for Microsoft 365 infrastructure components . You can track performance metrics for Veeam Backup for Microsoft 365 servers and proxies.

To drill down to a performance chart for a backup infrastructure component:

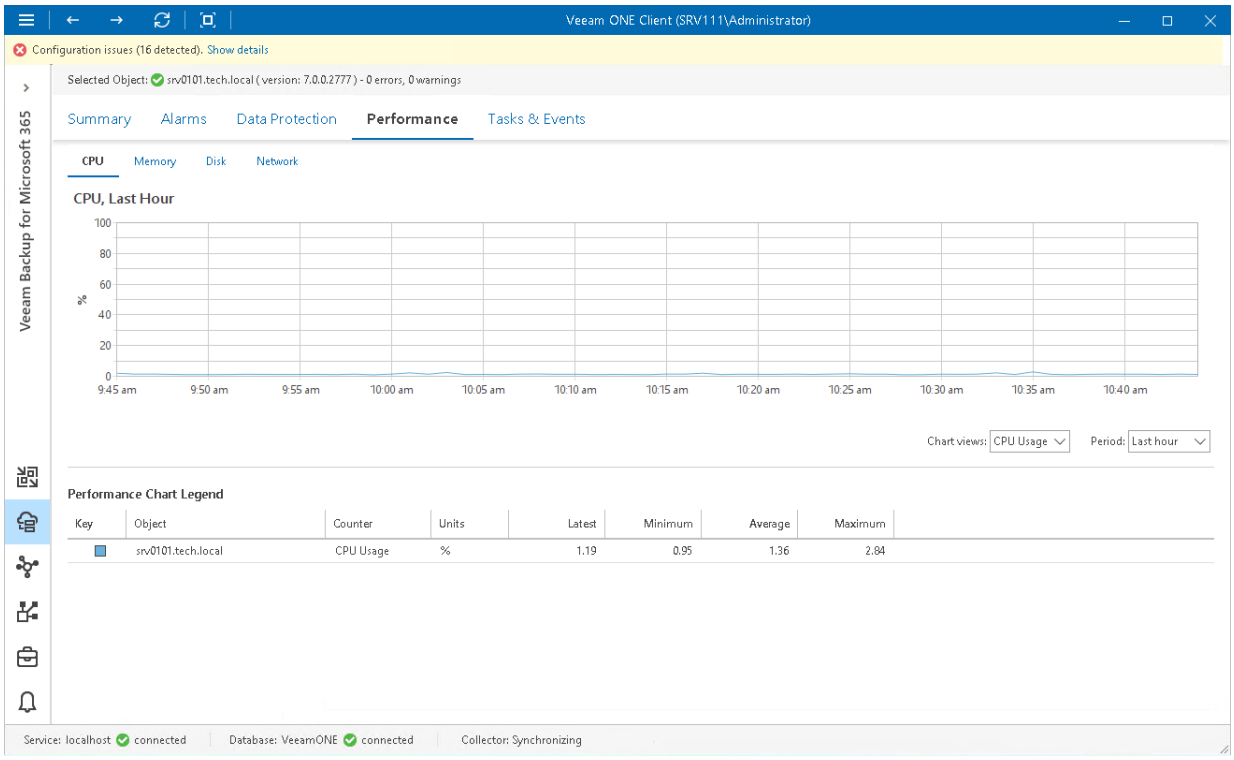
1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.
2. At the bottom of the inventory pane, click Veeam Backup for Microsoft 365.
3. Select the necessary backup infrastructure component.
4. Open the necessary performance chart tab.

For Veeam Backup for Microsoft 365 performance charts, you can change chart views and set time intervals, define objects to show on charts or select custom metrics.

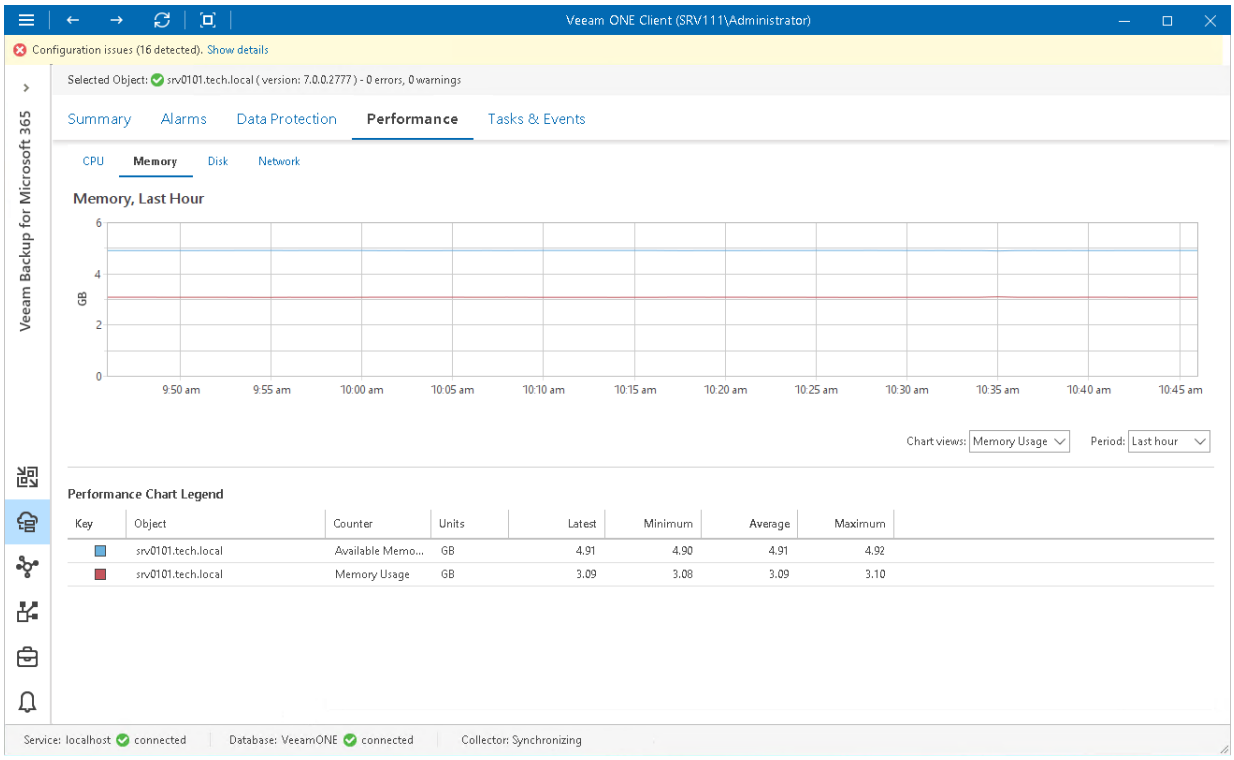
CPU Performance Chart

The **CPU** chart shows the amount of used processor resources on a machine where a backup infrastructure component runs. Graphs in the **CPU** chart illustrate the level of processor usage for every separate CPU on the machine. The **Total** graph shows the cumulative processor utilization for all CPUs.



Memory Performance Chart

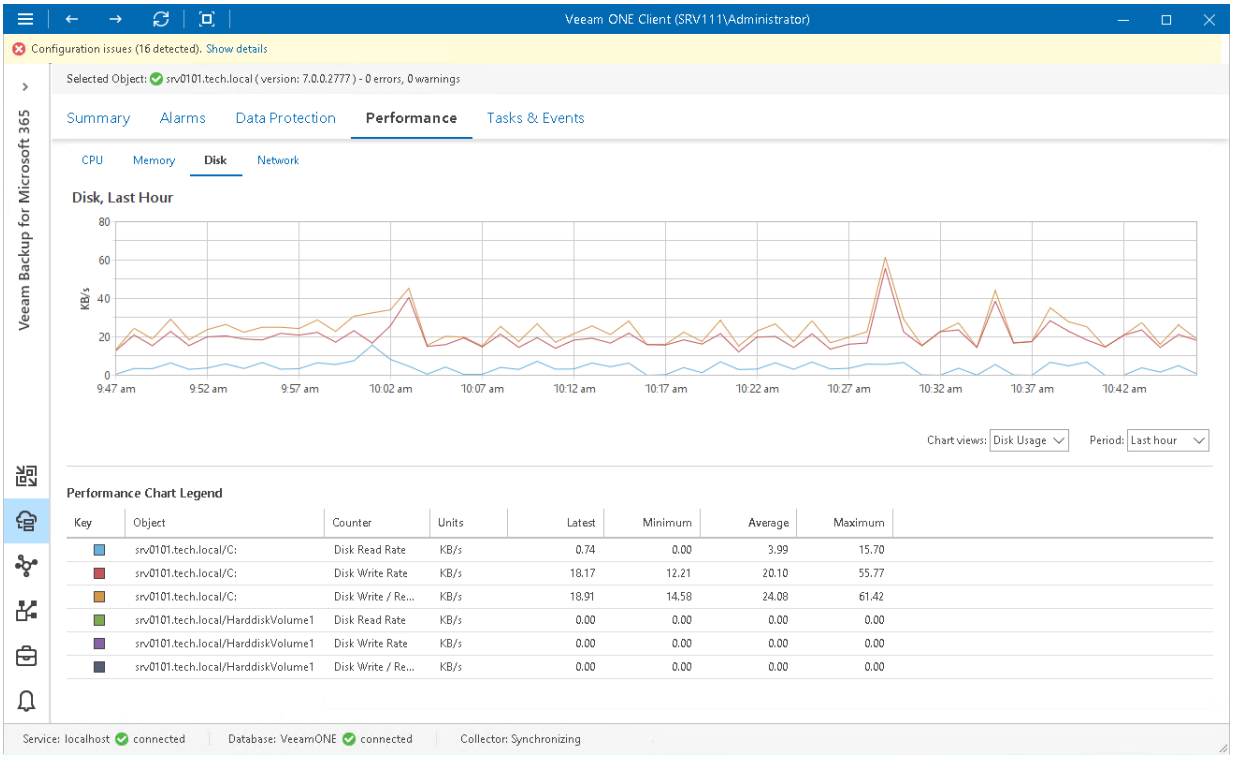
The **Memory** chart shows the amount of used memory resources on a machine where a backup infrastructure component runs. Graphs in the **Memory** chart illustrate the amount of total available memory and memory that is currently used on the machine.



Disk Performance Chart

The **Disk** chart shows the rate at which the disk is transferring data during read and write operations. Disk usage is shown as an average for all physical disks on a machine where a backup infrastructure component runs.

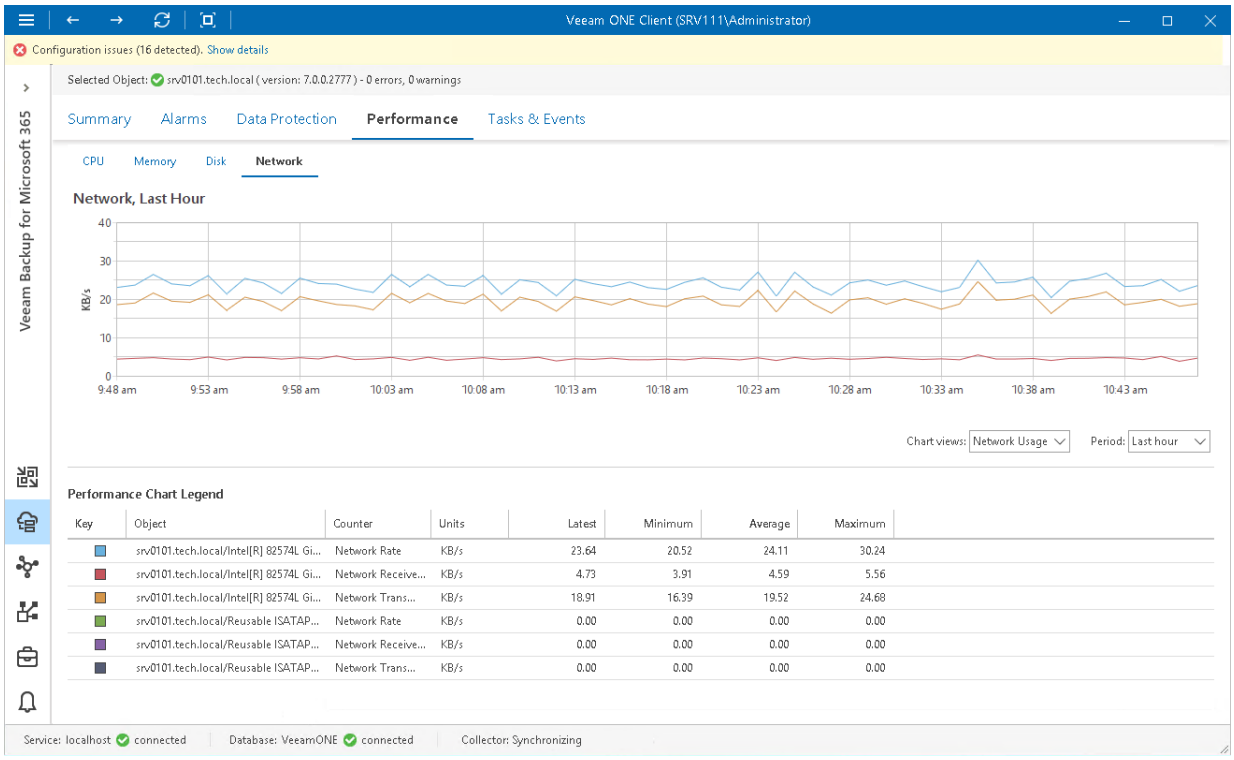
> **NOTE:**
>
> The **Disk** and **Network** tabs are not available for Linux-based proxies.



Network Performance Chart

The **Network** chart shows the throughput for NICs on a machine where a backup infrastructure component runs. Graphs in the **Network** chart illustrate the rate at which data is sent on the network interface for each separate NIC. A separate graph shows the cumulative rate for all NICs on the machine.

> **NOTE:**
>
> The **Disk** and **Network** tabs are not available for Linux-based proxies.



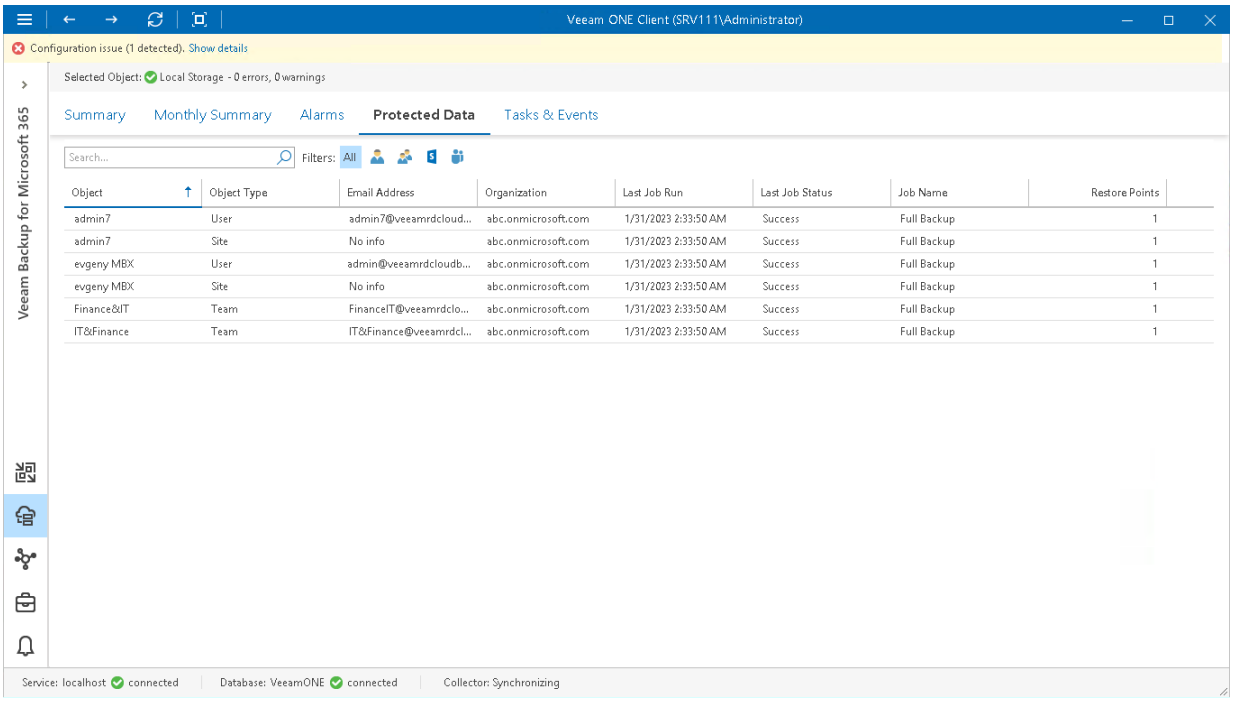
Veeam Backup for Microsoft 365 Protected Data

The **Protected Data** tab allows you to view the list of protected Microsoft 365 objects stored in backups on backup and object storage repositories:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click **Veeam Backup for Microsoft 365**.
3. In the inventory pane, select the necessary repository.
4. Open the **Protected Data** tab.
5. To quickly find the necessary object, use the **Search** field and object type filter at the top of the list.



For every object in the list, the following details are shown:

- **Object** – name of the Microsoft 365 object stored in a backup on the repository.
- **Object Type** – type of Microsoft 365 object (*Users*, *Groups*, *Sites*, *Teams*).
- **Email Address** – address of the Microsoft 365 object.
- **Organization** – name of the Microsoft 365 to which the object belongs.
- **Last Job Run** – date and time of the latest job session.
- **Last Job Status** – status of the latest job session.
- **Job Name** – name of the data protection job to which the object is included.
- **Restore Points** – number of restore points stored on the backup repository.

Veeam Backup for Microsoft 365 Events

The **Tasks & Events** dashboard shows the history of events that triggered Veeam Backup for Microsoft 365 alarms. For the list and detailed description of data protection alarms, see Veeam Backup for Microsoft 365 Alarms.

To view the list of events for a specific level:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click **Veeam Backup for Microsoft 365**.
3. In the inventory pane, select the necessary backup infrastructure node.
4. Open the **Tasks & Events** tab.
5. The **Tasks & Events** list can display up to 1000 tasks and events at a time. To find the necessary task or event, you can use the following controls:
   - To display tasks or events for a specific period, select the necessary time interval from the **Events from** list.
   - To show or hide tasks or events, use filter buttons at the top of the list — *Show all events*, *Show errors*, *Show warnings*, *Show info messages*, *Show user events*, *Show tasks*.
   - To find the necessary tasks or events by description, use the **Search** field at the top of the list.
6. To view the detailed description of an event, click it in the list.

   The event description will be shown in the **Event Details** pane at the bottom.

   When you choose a virtual infrastructure container in the inventory pane, you can view events for the selected object and events for its child objects. To hide events related to child objects, clear the **Include events from child objects** check box at the bottom of the **Event Details** section.

7. To export displayed events to a CSV file, click **Export to CSV** at the top of the list and specify the location where the file will be saved.

VMware vSphere Monitoring

Veeam ONE Client offers a variety of tools for monitoring the VMware vSphere environment from any perspective and with any level of detail.

With Veeam ONE Client, you can:

1. **Monitor health status of the virtual environment.**
   - Start with the **Summary** dashboards to check the overall health status of the virtual environment and reveal hotspots.

     Quickly review the state of virtual infrastructure components, see the latest alarms, detect the most problematic objects and drill down to the problem source for further investigation.
   - Use the **Virtual Machines** dashboard to view the list of VMs in a virtual infrastructure container and check additional details for every VM — VM current state, parent host, IP address, DNS name and the amount of resources currently consumed by the VM.
   - Use the **Top Objects** dashboard to detect the most and less loaded components in the virtual environment.

     Detect what virtual infrastructure objects are consuming the most and the least amount of CPU, memory, disk, network, and swap resources, or select additional counters to detect resource consumers in other areas.
2. **View triggered alarms.**

   Switch to the **Alarms** dashboard to see details on breached thresholds, events and problems that occurred in the virtual environment.

   Use the **Actions** pane on the alarms dashboard to detect root causes — drill down to performance charts, open VM console or view the list of in-guest processes.
3. **Work with performance charts and track events.**

   Drill down to performance charts to diagnose performance problems. You can change predefined views, quickly switch between charts and view events occurring in your environment to get all-round statistics.
4. **Investigate problems from within the guest OS.**

   Open the VM console or view the list of in-guest processes to diagnose problems related to a specific service, module or application.

Prerequisites

Before you start monitoring your virtual environment, make sure you have configured connections to virtual servers from which Veeam ONE will collect data. For details on configuring server connections, see Connecting VMware vSphere Servers.

VMware vSphere Summary Dashboards

VMware vSphere infrastructure summary dashboards serve as the starting point for monitoring and troubleshooting. Summary dashboards reflect the health status of the selected infrastructure object or infrastructure segment.

The following types of summary dashboards are available for virtual infrastructure objects:

- VMware vSphere Infrastructure Summary
- Host Summary
- Virtual Machine Summary
- Datastore Summary

To access a summary dashboard for a virtual infrastructure object or virtual infrastructure segment:

1. Open Veeam ONE Client.

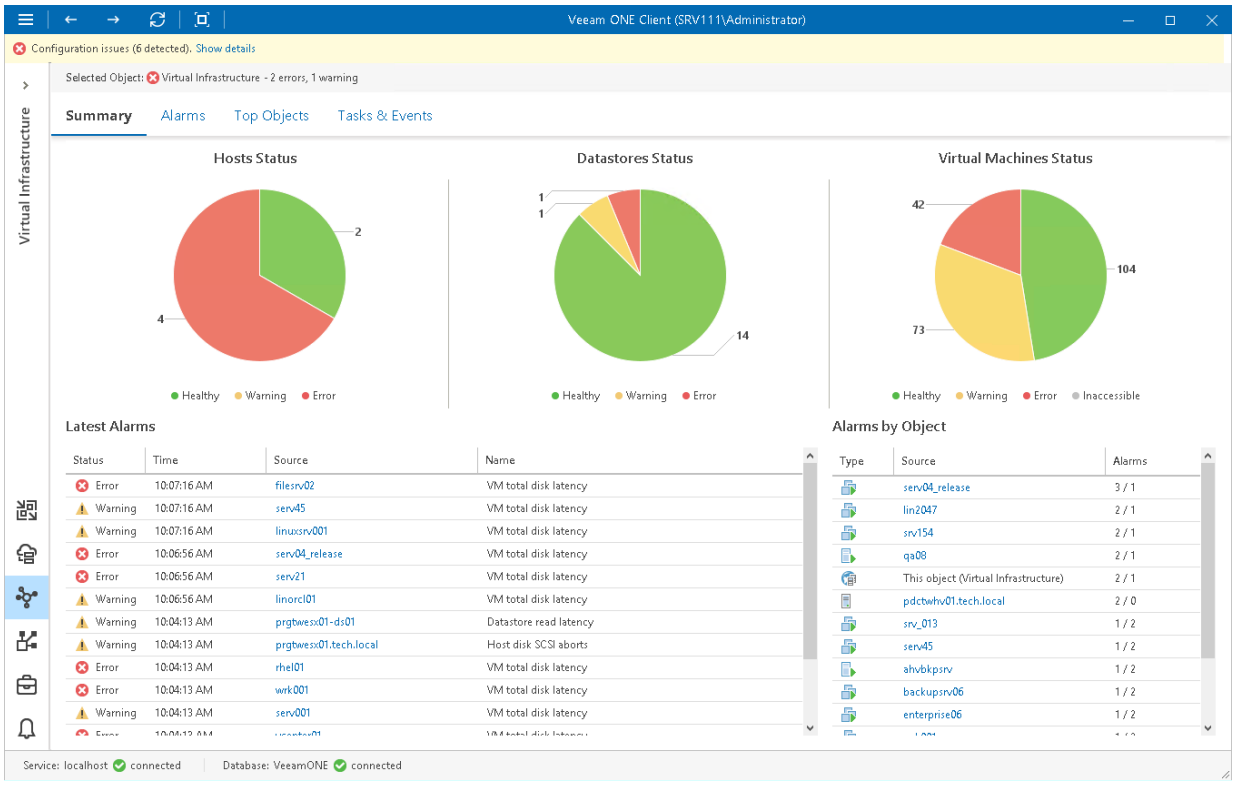
   For details, see Accessing Veeam ONE Components.
2. At the bottom of the inventory pane, click **Virtual Infrastructure**.
3. In the inventory pane, select the necessary infrastructure object or segment.
4. Open the **Summary** tab.

VMware vSphere Infrastructure Summary

The VMware vSphere infrastructure summary dashboard provides the health status overview for the selected virtual environment segment.

The dashboard is available for the following infrastructure levels:

- Virtual infrastructure (root node)
- Virtual infrastructure container (such as folder, resource pool, host, cluster, datacenter or vCenter Server)



Host Status, Datastores Status, Virtual Machines Status

The charts reflect the status of virtual infrastructure objects.

Every chart segment represents the number of objects in a certain state — objects with errors (red), objects with warnings (yellow) and healthy objects (green). Click a chart segment or a legend label to drill down to the list of alarms with the corresponding status for the selected type of virtual infrastructure objects.

Latest Alarms

The list displays the latest 15 alarms that were triggered for objects in the selected virtual environment segment. Click a link in the **Source** column to drill down to the list of alarms triggered for a specific virtual infrastructure object.

Alarms by Object

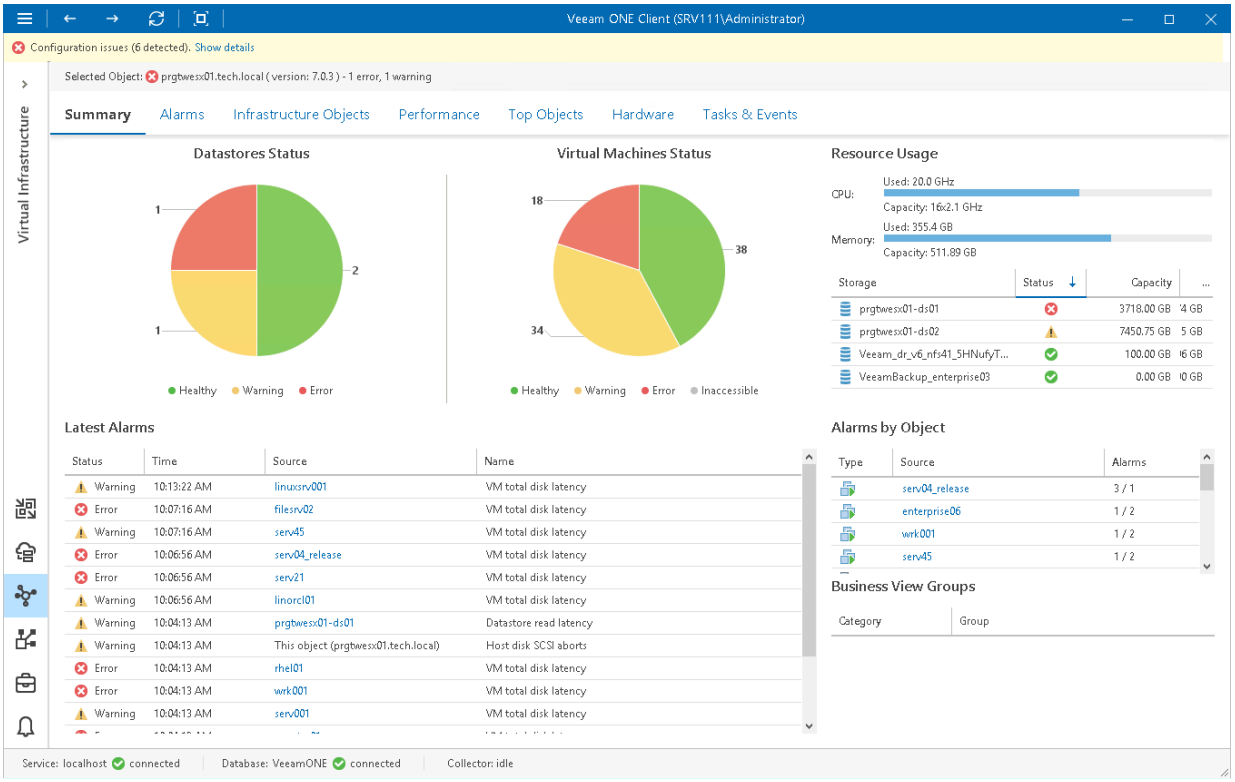
The list displays 15 objects with the highest number of alarms.

The value in the **Alarms** column shows the number of errors and warnings for an object. For example, 3/1 means that there are 3 error alarms and 1 warning alarm triggered for the object. Click a link in the **Source** column to drill down to the list of alarms related to a specific virtual infrastructure object.

For more information, see Working with Triggered Alarms.

Host Summary

The host summary dashboard provides the health status and performance overview for the selected ESXi host and its child objects.



Datastores Status, Virtual Machines Status

The charts reflect the status of datastores connected to the host and the state of VMs running on the host.

Every chart segment represents the number of objects with a certain status — objects with errors (red), objects with warnings (yellow) and healthy objects (green). Click a chart segment or a legend label to drill down to the list of alarms with the corresponding status for host child objects.

Resource Usage

The section displays capacity and performance summary for host CPU and memory. It also shows an overview for datastores connected to the host — status of the datastore, its capacity and the amount of free space on the datastore.

Latest Alarms

The list displays the latest 15 alarms triggered for the host and its child objects. Click a link in the **Source** column to drill down to the list of alarms for the host and its child objects.

Alarms by Object

The list displays 15 objects with the greatest number of alarms (including the host and its child objects).

The value in the **Alarms** column shows the number of errors and warnings for an object. For example, 3/1 means that there are 3 error alarms and 1 warning alarm triggered for the object. Click a link in the **Source** column to drill down to the list of alarms related to the host and its child objects.

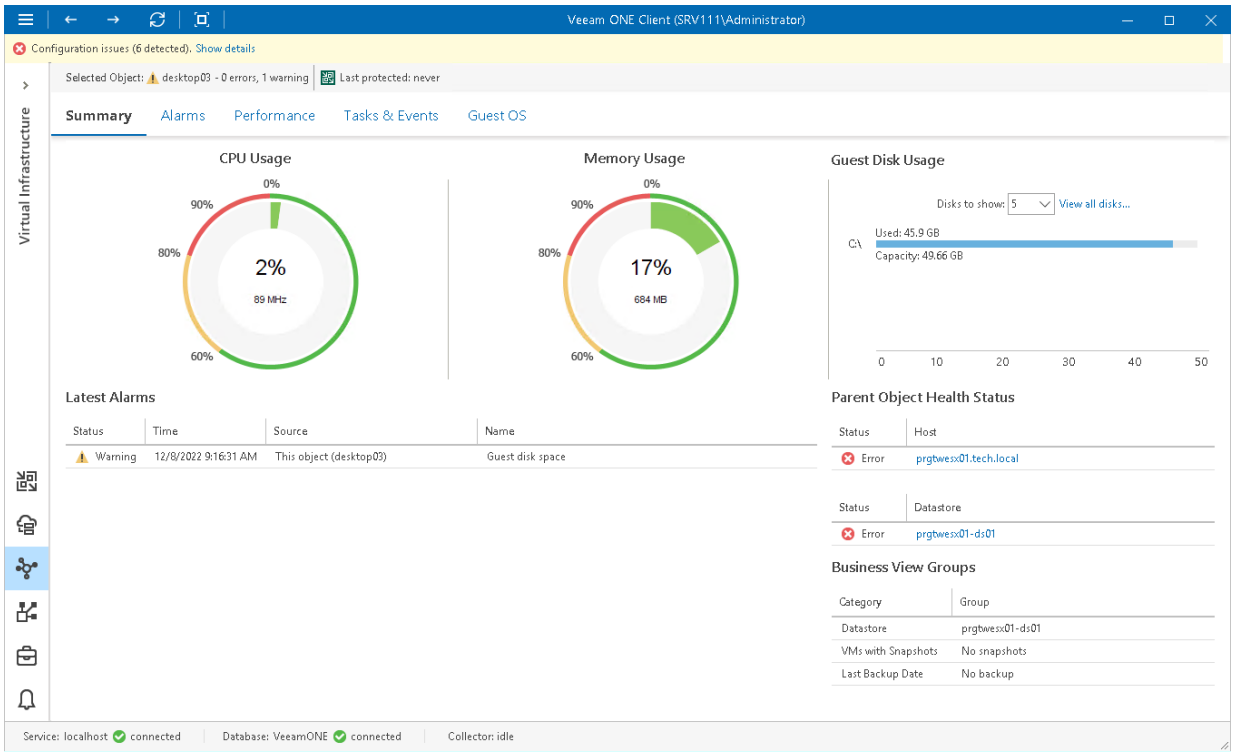
For more information, see Working with Triggered Alarms.

Business View Groups

The section displays the list of categories and groups to which the host is included.

Virtual Machine Summary

The VM summary dashboard provides the health status and performance overview for the selected VM. In addition, this dashboard shows the state of objects that can affect the VM performance — the parent host and the datastores where VM files are located.



Selected Object

The section at the top of the dashboard shows the VM health status (number of warnings and errors) and the date when the latest backup or replica restore point was created for the VM with Veeam Backup & Replication.

CPU Usage, Memory Usage

The charts display the amount of CPU and memory resources currently consumed by the VM.

Guest Disk Usage

The chart displays the amount of available and used guest disk space with a breakdown by disks. By default, 5 guest disks with the greatest amount of used space are displayed.

Use the **Disks to show** list to change the number of disks to display on the chart. Click the **View all disks** link to view details for all guest disks. In the **Guests Disks** window, you can suppress *Guest disk space* alarms for specific disks. To suppress alarms for a disk, select the **Suppress alarms** check boxes next to the disk name.

> **NOTE:**
>
> Details on the guest disk usage are available only for VMs with VMware Tools installed.

Parent Object Health Status

The section displays the current state of the host where the VM resides and the state of datastores that host VMs files. Information available in this section may help you estimate how the state of parent objects impacts the VM performance. Click the host or datastore link to drill down to the list of alarms for the host or datastore.

Latest Alarms

The list displays the latest 15 alarms for the VM.

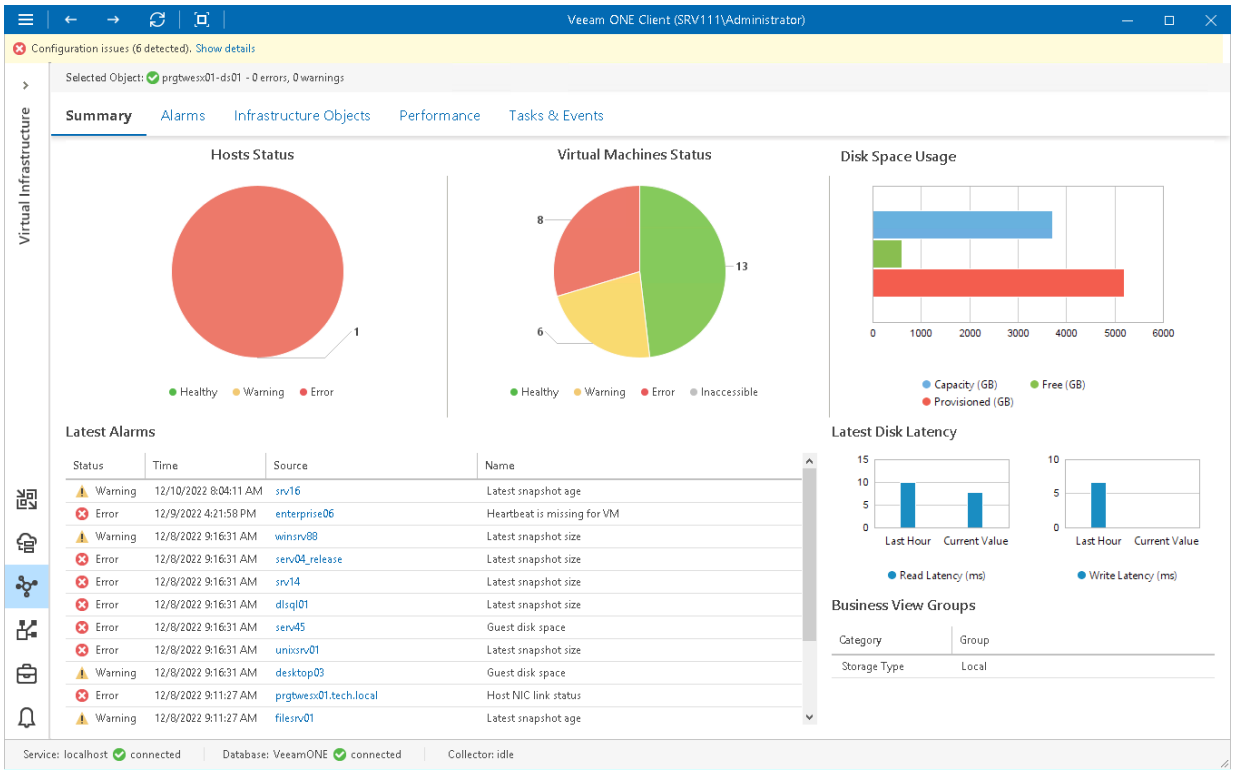
For more information, see Working with Triggered Alarms.

Business View Groups

The section displays the list of categories and groups to which the VM is included.

Datastore Summary

The datastore summary dashboard provides the health status and performance overview for the selected datastore. In addition, it shows the status of objects that can affect the datastore performance — hosts that work with the datastore and VMs whose files reside on the datastore.



Hosts Status, Virtual Machines Status

The charts reflect the health status of hosts that work with the datastore and VMs whose files reside on the datastore.

Every chart segment represents the number of objects with a certain status — objects with errors (red), objects with warnings (yellow) and healthy objects (green). Click a chart segment or a legend label to drill down to the list of alarms with the corresponding status for hosts or VMs.

Disk Space Usage

The chart shows the amount of available, used and provisioned disk space on the datastore.

Latest Disk Latency

The section displays the current read and write latency values as well as the average latency values for the past hour.

Latest Alarms

The list displays the latest 15 alarms for the datastore and for objects that work with this datastore. Click a link in the **Source** column to drill down to the list of alarms for the selected object.

For more information, see Working with Triggered Alarms.

Business View Groups

The section displays the list of categories and groups to which the datastore is included.

VMware vSphere Alarms

Veeam ONE includes a set of alarms for monitoring VMware vSphere virtual environment. These alarms warn you about events or changes that can affect performance of operations and services in the virtual environment.

To view the list of triggered VMware vSphere alarms:

1. Open Veeam ONE Client.

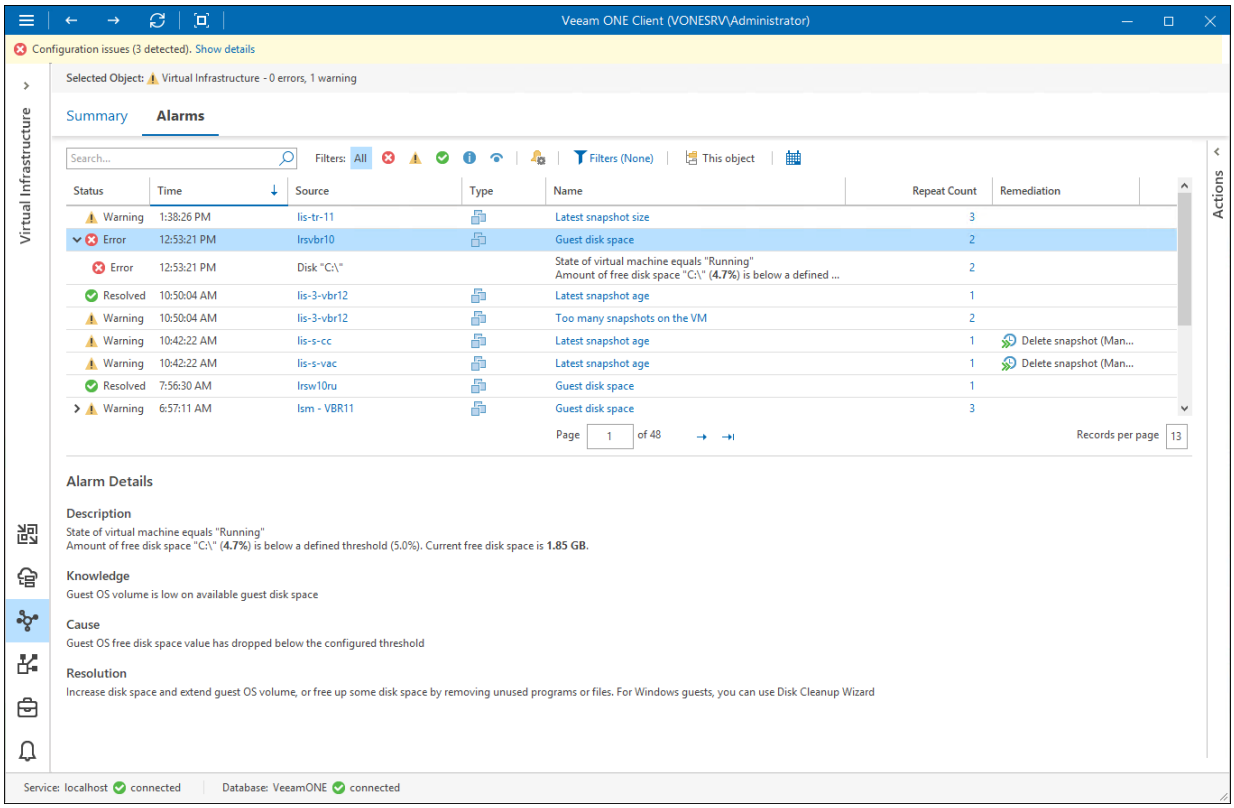
   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click **Virtual Infrastructure**.

3. In the inventory pane, select the necessary virtual infrastructure node.

4. Go to the **Alarms** tab.

On the **Alarms** dashboard, you can view triggered alarms, track alarm history, resolve and acknowledge alarms and perform other actions. For details on available actions, see Working with Triggered Alarms.



VMware vSphere Performance Charts

Performance charts show how key performance counters have been changing over time to help you diagnose performance issues and perform root cause analysis.

> **NOTE**
>
> Performance statistics for VMs are gathered and displayed from the VMware vSphere environment and not from within the Guest OS. This is because the guest OS is unaware of the hypervisor's resource allocations and cannot recognize when the hypervisor temporarily de-schedules VM resources during periods of inactivity.

Performance charts include the following elements:

- **Axes**

  Performance charts display data for a particular time period (the horizontal axis) using two scales of measurement units (vertical axes). The measurement units may vary depending on selected performance counters. However, the number of units is always limited to two.

- **Graphs**

  Performance charts include one or more graphs. Every graph on a performance chart visualizes a specific counter for an infrastructure object or a container of infrastructure objects.

- **Legend**

  The chart legend shows details about objects and counters displayed in the chart. The details include key color, object name, list of counters and units of measurement, the latest, minimum, average, and maximum counter values.

- **Chart views**

  Performance charts come with a number of predefined chart views. Every view logically groups related counters to display the most valuable data and help you speed up troubleshooting and root cause analysis of performance problems.

Performance charts can be easily customized. For details on customization options, see Customizing VMware vSphere Performance Charts.

Accessing Performance Charts

To access a performance chart for an infrastructure object or infrastructure segment:

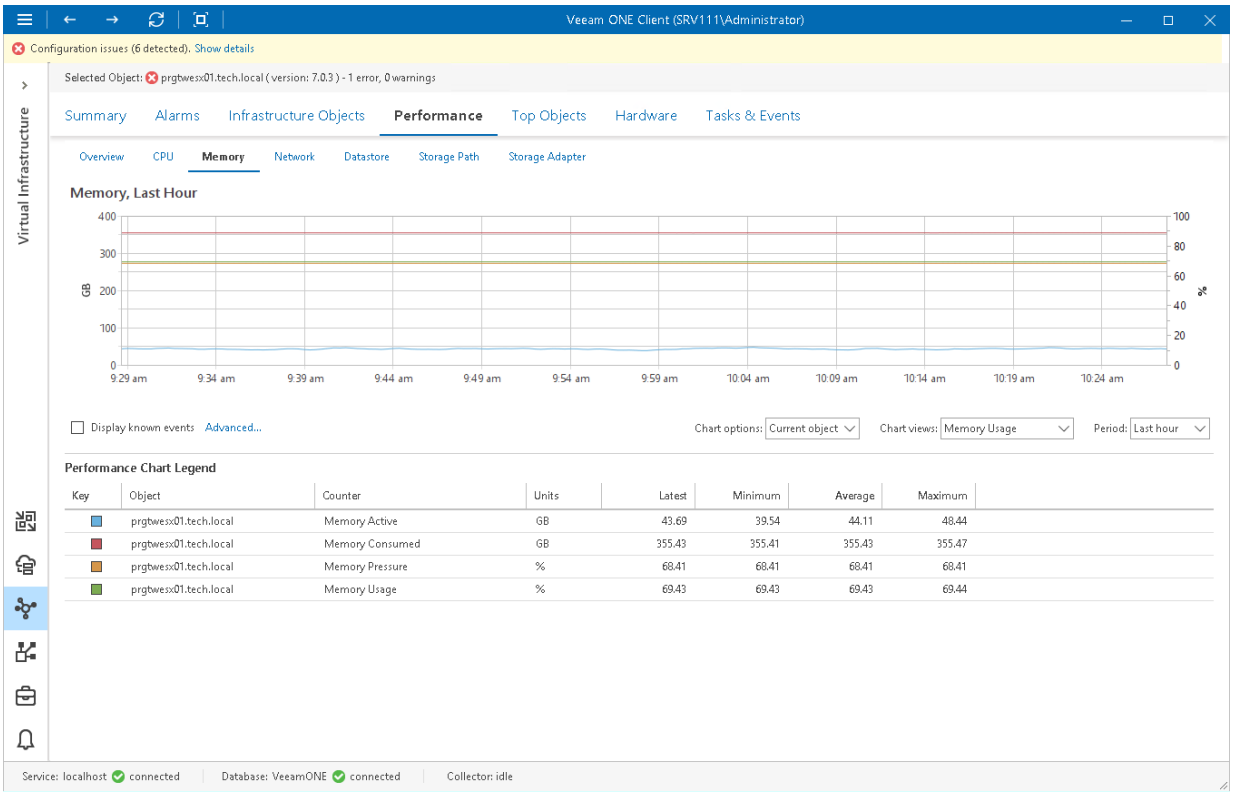
1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click **Virtual Infrastructure**.

3. In the inventory pane, select the necessary infrastructure object or segment.

4. Open the **Performance** tab.

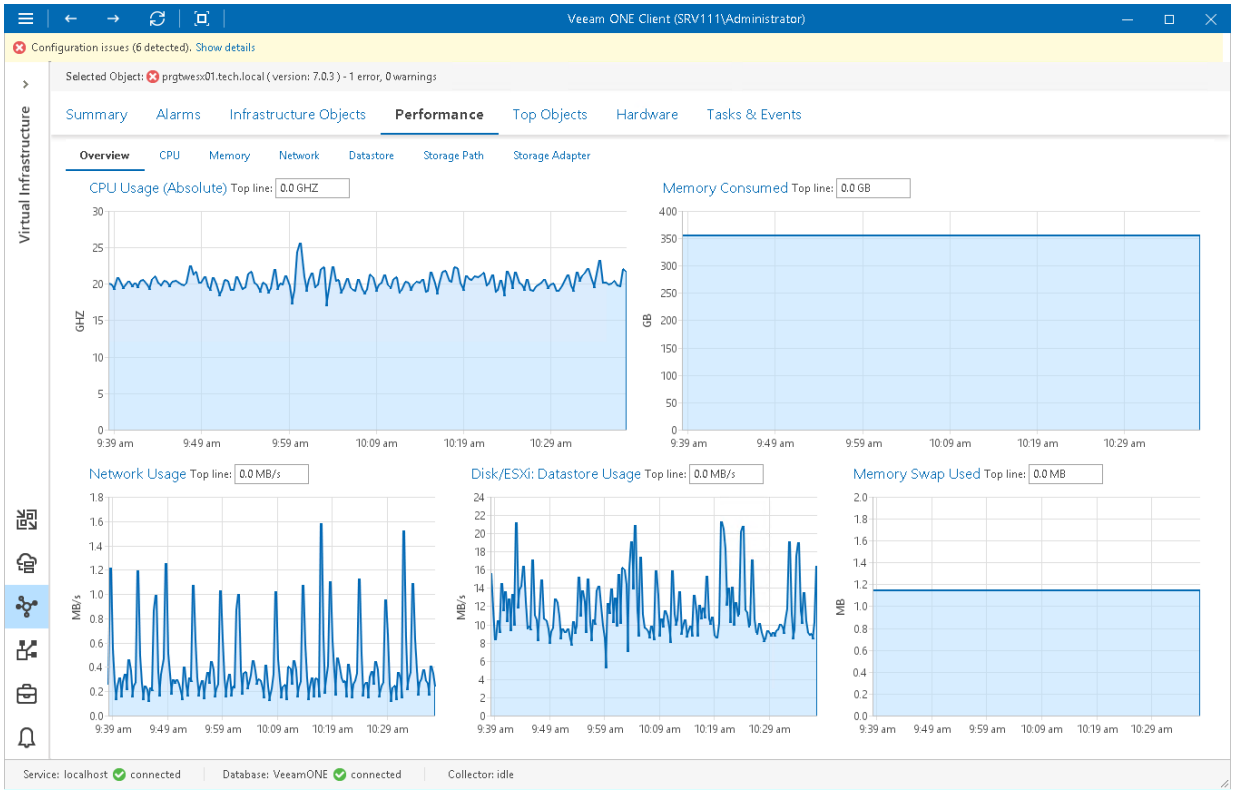


Overview

The **Overview** page shows aggregated performance data for the selected infrastructure object or segment: CPU usage, memory usage, memory swapped, network and datastore usage. Performance data is shown for the previous 60 minutes.

In the **Top line** field, you can set a threshold value. The top line is displayed as the red dotted line in the chart to help you monitor whether resource usage exceeds the healthy value range. If you do not need to display the top line, enter '0' (zero) in the **Top line** field or disable top lines in Veeam ONE Client chart settings. With the top line disabled, the Y-axis will scale automatically to match the range of the displayed data.

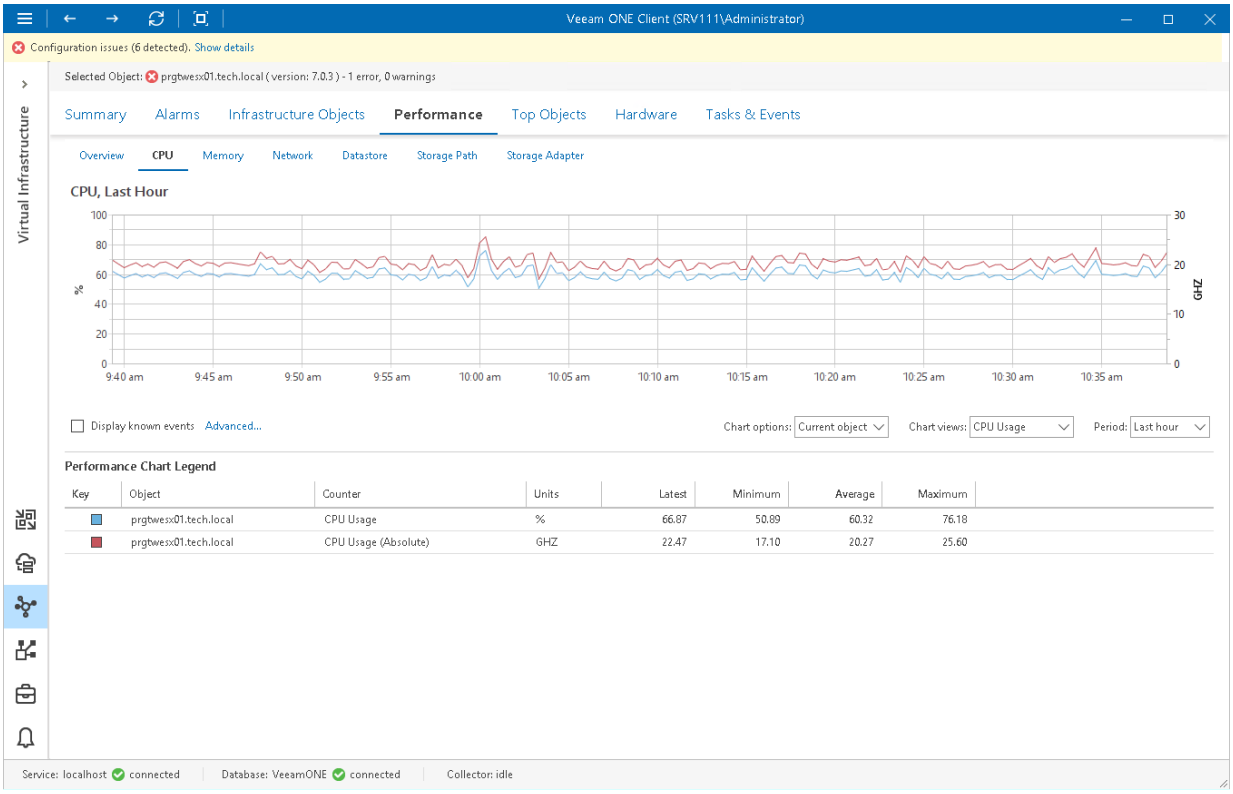
To drill down to performance chart details, click the counter link above a performance widget. A corresponding performance chart for the selected virtual infrastructure object will open.



CPU Performance Chart

The **CPU** chart displays historical statistics on CPU utilization for the selected infrastructure object.

> **NOTE**
>
> Performance statistics for VMs are gathered and displayed from the VMware vSphere environment and not from within the Guest OS. This is because the guest OS is unaware of the hypervisor's resource allocations and cannot recognize when the hypervisor temporarily de-schedules VM resources during periods of inactivity.



Host

The following table provides information on predefined views and counters that apply to hosts.

Chat View	Counter	Measurement Unit	Description
CPU Usage	CPU Usage	Percent	CPU actively used on a host, as a percentage of total available CPU.
	CPU Usage (Absolute)	GHZ	Sum of actively used CPU for all powered on VMs on a host.
CPU Bottlenecks	Average CPU Ready	Percent	Average CPU Ready value for all VMs on a host.

Virtual Machine

The following table provides information on predefined views and counters that apply to VMs.

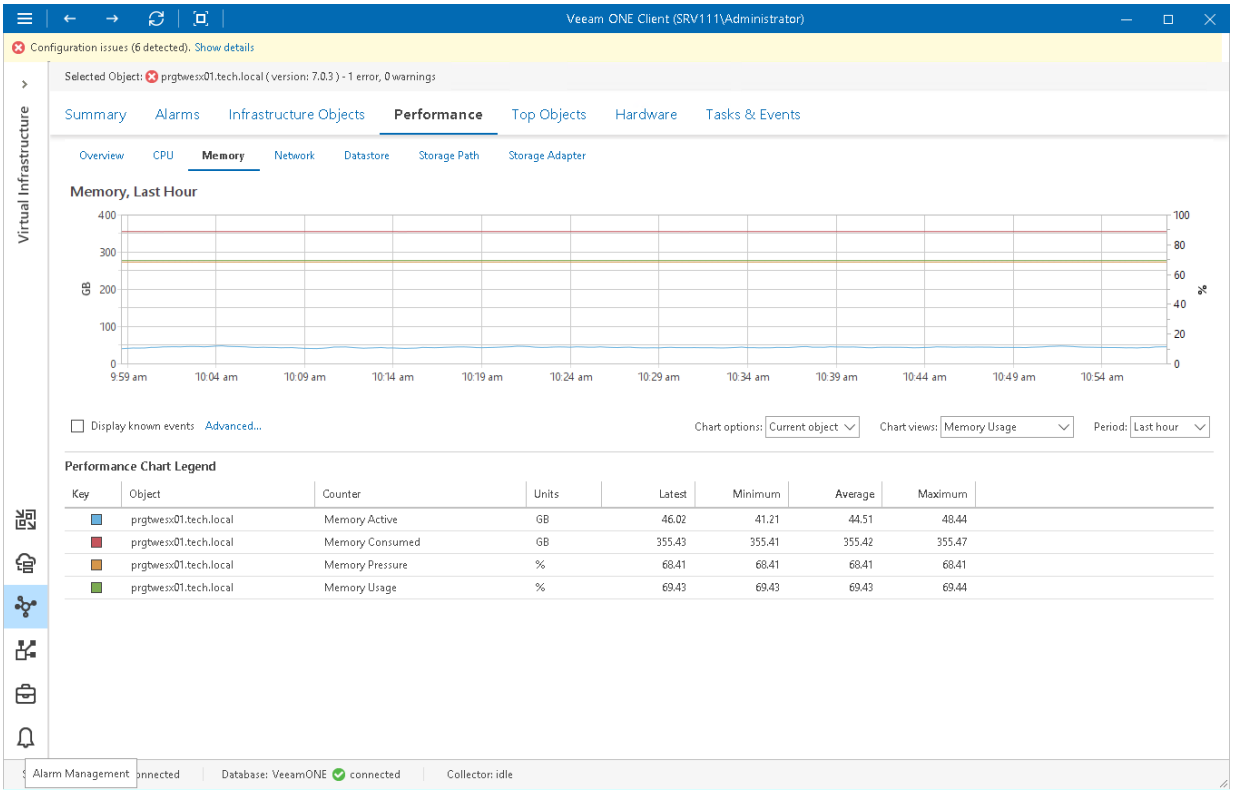
Chat View	Counter	Measurement Unit	Description
CPU Usage	CPU Usage	Percent	Amount of actively used virtual CPU resources, as a percentage of total available CPU (this is the host view, not the guest OS view).
	CPU usage (Absolute)	GHZ	Amount of actively used virtual CPU resources (this is the host view, not the guest OS view).
CPU Bottlenecks	Average CPU Idle All cores	Percent	Average amount of time all CPU cores spent in an idle state.
	Average CPU Ready All cores	Percent	Average CPU Ready value across all cores on a host.
	Average CPU Standstill All cores	Percent	Average amount of time all CPU cores spent in a standstill state.
	Average CPU Wait All cores	Percent	Time spent waiting for hardware or VMKernel lock thread locks.
	CPU Co-stop all cores	Percent	Average amount of time a VM was ready but unable to run due to co-scheduling constraints.

For objects that are parent to ESXi hosts and VMs, Veeam ONE displays rollup values.
Charts for folders, clusters, datacenters, vCenter Servers display rollup values for all hosts in the container. Chart for a resource pool displays rollup values for all VMs in the resource pool.

Memory Performance Chart

The **Memory** chart displays historical statistics on memory utilization for the selected infrastructure object.

> **NOTE**
>
> Performance statistics for VMs are gathered and displayed from the VMware vSphere environment and not from within the Guest OS. This is because the guest OS is unaware of the hypervisor's resource allocations and cannot recognize when the hypervisor temporarily de-schedules VM resources during periods of inactivity.



Host

The following table provides information on predefined views and counters that apply to hosts.

Chart View	Counter	Measurement Unit	Description
Memory Usage	Memory Active	GB	Sum of all active memory metrics for all powered-on VMs and vSphere services (such as COS, vpxa) on a host, as estimated by VMkernel based on recently touched memory pages.
	Memory Consumed	GB	Amount of physical memory used on a host, including memory used by the Service Console, VMkernel, vSphere services and total memory consumed by running VMs.

Chart View	Counter	Measurement Unit	Description
	Memory Pressure	Percent	Potential memory demand that is based on total allocated memory for running VMs, memory overhead, effects of memory Transparent Page Sharing and total available memory.
	Memory Usage	Percent	Memory usage as percentage of available machine memory.
Memory Swap Rate	Memory Swap Used	B	Amount of memory swapped to disk: sum of memory swapped for all powered on VMs and vSphere services on a host.
	Swap In Rate	B/s	Rate at which memory is swapped from disk into host active memory during the current interval.
	Swap Out Rate	B/s	Rate at which memory is swapped from host active memory to disk during the current interval.
Memory Management	Memory Balloon	B	Amount of memory allocated by the VM memory control driver (vmmemctl).
	Memory Compressed	B	Amount of RAM pages memory compressed by a host instead of swapping to disk.
	Memory Overhead	B	Total amount of memory overhead metrics for all powered-on VMs, plus memory overhead of running vSphere services on a host.
Memory Sharing	Memory Shared	MB	Sum of memory shared metrics for all powered-on VMs, and memory consumed by vSphere services on a host.
	Memory Shared Common	MB	Amount of memory shared by all powered-on VMs and vSphere services on a host.
Memory Latency	Memory Latency	Percent	Percentage of time a VM is waiting to access swapped or compressed memory.

Virtual Machine

The following table provides information on predefined views and counters that apply to VMs.

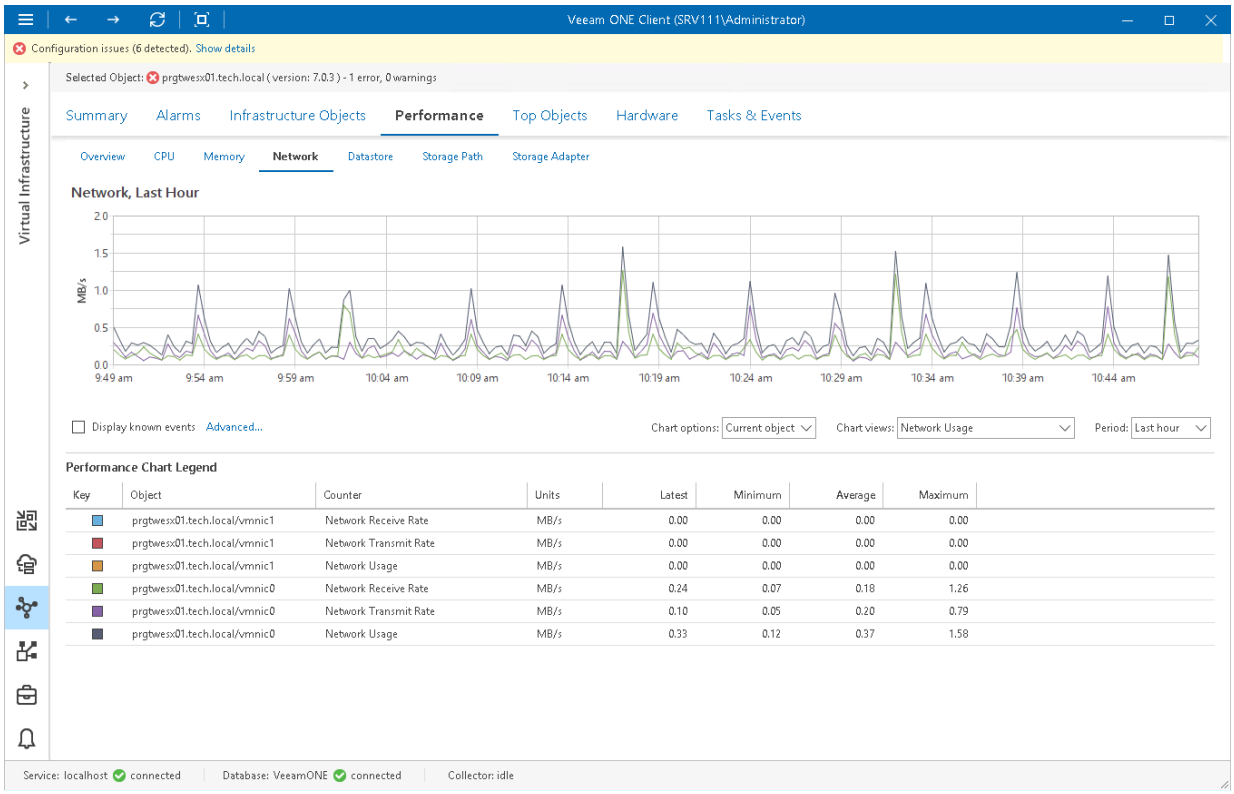
Chart View	Counter	Measurement Unit	Description
Memory Usage	Memory Active	GB	Amount of guest physical memory actively used, as estimated by VMkernel based on recently touched memory pages.
	Memory Consumed	GB	Amount of guest physical memory consumed by a VM. The value includes the shared and memory that might be reserved but not actually used; overhead memory is not taken into account.
	Memory Entitlement	GB	Amount of host physical memory a VM is entitled to, as determined by the ESXi scheduler.
	Memory Usage	Percent	Memory usage as percentage of configured physical memory for a VM.
Memory Swap Rate	Memory Swapped	B	Amount of guest physical memory swapped out to the VM swap file by the VMkernel. The metrics refers to VMkernel swapping, not to guest OS swapping.
	Swap In Rate	B/s	Rate at which memory is swapped from disk into active memory during the current interval.
	Swap Out Rate	B/s	Rate at which memory is swapped from active memory to disk during the current interval.
Memory Management	Memory Balloon	MB	Amount of memory allocated by the VM memory control driver (vmmemctl).
	Memory Compressed	MB	Amount of RAM pages compressed by a host instead of swapping to disk.
	Memory Overhead	MB	Amount of machine memory used by VMkernel to run a VM.
	Memory Saved by Zipping	MB	Amount of memory saved by memory zipping.

Chart View	Counter	Measurement Unit	Description
Memory Sharing	Memory Shared	B	Amount of guest physical memory that a VM shares with other virtual machines (through VMkernel Transparent Page Sharing and RAM deduplication).
Memory Latency	Memory Latency	Percent	Percentage of time a VM is waiting to access swapped or compressed memory.

For objects that are parent to ESXi hosts and VMs, Veeam ONE Client displays rollup values.
Charts for folders, clusters, datacenters, vCenter Servers display rollup values for all hosts in the container. Chart for a resource pool displays rollup values for all VMs in the resource pool.

Network Performance Chart

The **Network** chart displays historical statistics on network usage for the selected infrastructure object.



Host

The following table provides information on predefined views and counters that apply to hosts.

Chart View	Counter	Measurement Unit	Description
Network Usage	Network Receive Rate	KB/s	Rate at which data is received across each physical NIC instance on a host. The counter represents the bandwidth of the network.
	Network Transmit Rate	KB/s	Rate at which data is transmitted across each physical NIC instance on a host.
	Network Usage	KB/s	Network utilization, sum of data received and transmitted across all physical NIC instances connected to a host.
	Received Packets per Second	Number	Average number of packets received per second across each physical NIC instance on a host.

Chart View	Counter	Measurement Unit	Description
Network Transfer Rate (Packets)	Transmitted Packets per Second	Number	Average number of packets transmitted per second across each physical NIC instance on a host.
Dropped and Error Packets	Packet Receive Errors	Number	Number of packets with errors received.
	Packet Transmit Errors	Number	Number of packets with errors transmitted.
	Receive Packets Dropped	Number	Number of receives dropped.
	Total Errors	Number	Total number of packets with errors received and transmitted.
	Total Packets Dropped	Number	Total number of dropped packets.
	Transmit Packets Dropped	Number	Number of transmits dropped.

Virtual Machine

The following table provides information on predefined views and counters that apply to VMs.

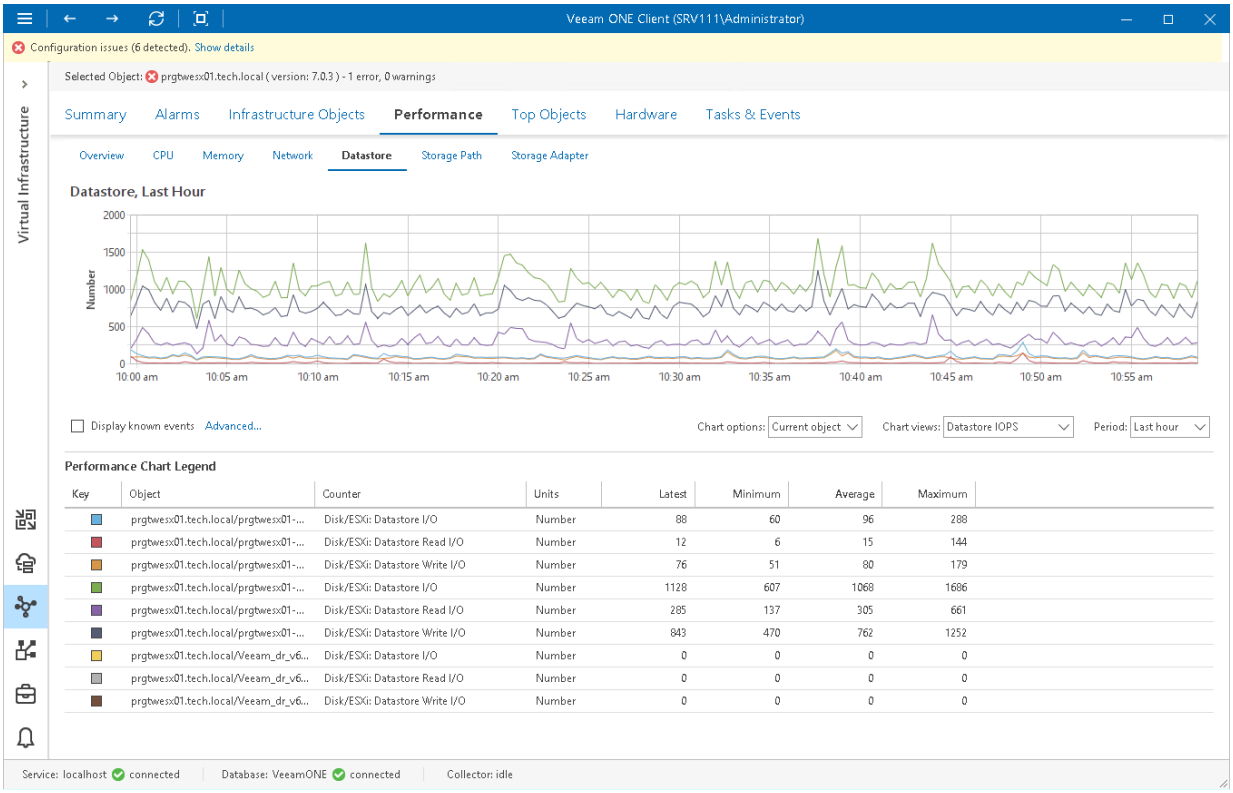
Chart View	Counter	Measurement Unit	Description
Network Usage	Network Receive Rate	KB/s	Rate at which data is received across the vNIC instance on a VM. The counter represents the bandwidth of the network.
	Network Transmit Rate	KB/s	Rate at which data is transmitted across the vNIC instance on a VM.
	Network Usage	KB/s	Network utilization, sum of data received and transmitted across all vNIC instances on a VM.
	Received Packets per Second	Number	Average number of packets received per second by each vNIC instance on a VM.

Chart View	Counter	Measurement Unit	Description
Network Transfer Rate (Packets)	Transmitted Packets per Second	Number	Average number of packets transmitted per second by each vNIC instance on a VM.

For objects that are parent to ESXi hosts and VMs, Veeam ONE Client displays rollup values.
Charts for folders, clusters, datacenters, vCenter Servers display rollup values for all hosts in the container. Chart for a resource pool displays rollup values for all VMs in the resource pool.

Datastore Performance Chart

The **Datastore** chart displays historical statistics for all datastores (including vSAN datastores) used by the selected infrastructure component and its child objects.



Host

The following table provides information on predefined views and counters that apply to hosts.

Chart View	Counter	Measurement Unit	Description
Datastore IOPS	Disk/ESXi: Datastore I/O	Number	Aggregate number of I/O operations on a datastore.
	Disk/ESXi: Datastore Read I/O	Number	Average number of read commands per second to a datastore.
	Disk/ESXi: Datastore Write I/O	Number	Average number of write commands per second to a datastore.
Datastore Usage Rates	Disk/ESXi: Datastore Read Rate	MB/s	Rate at which data is read from a datastore.

Chart View	Counter	Measurement Unit	Description
	Disk/ESXi: Datastore Usage	MB/s	Sum of read and write rates to a datastore.
	Disk/ESXi: Datastore Write Rate	MB/s	Rate at which data is written to a datastore.
Datastore Latency	Disk/ESXi: Datastore Highest Latency	Millisecond	Highest latency value across all datastores used by a host.
	Disk/ESXi: Datastore Latency Observed by VMs	Millisecond	Average datastore latency as seen by VMs.
	Disk/ESXi: Datastore Read Latency	Millisecond	Average amount of time that a read from the datastore takes.
	Disk/ESXi: Datastore Write Latency	Millisecond	Average amount of time that a write operation to a datastore takes.
Datastore Issues	Disk/ESXi: Datastore Bus Resets	Number	Number of SCSI bus reset commands.
	Disk/ESXi: Datastore Command Aborts	Number	Number of aborted SCSI commands.
	Disk/ESXi: Datastore Maximum Queue Depth	Number	Number of outstanding requests to a storage device.

Virtual Machine

The following table provides information on predefined views and counters that apply to VMs.

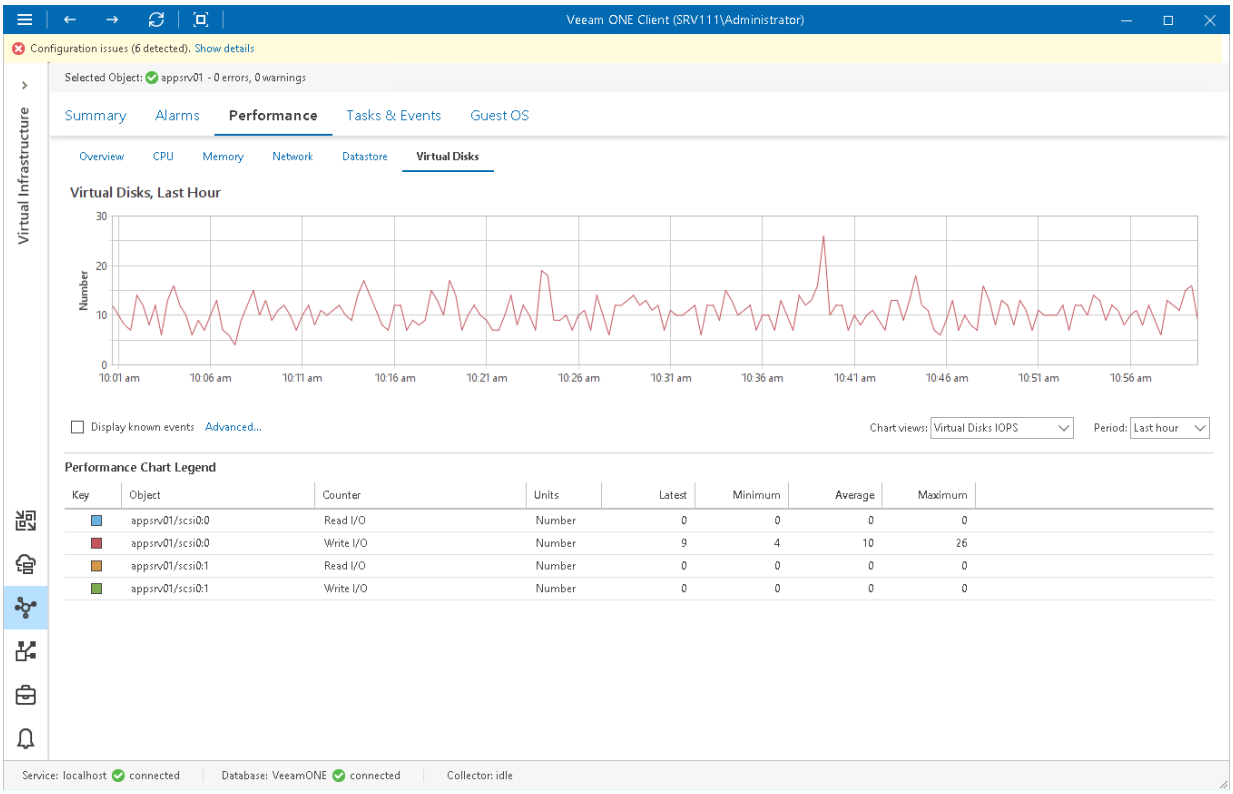
Chart View	Counter	Measurement Unit	Description
Datastore IOPS	Datastore I/O	Number	Aggregate number of I/O operations on a datastore.
	Datastore Read I/O	Number	Average number of read commands per second to a datastore.

Chart View	Counter	Measurement Unit	Description
	Datastore Write I/O	Number	Average number of write commands per second to a datastore.
	Disk/vSAN: Recovery Write I/O	Number	Average number of write commands per second to a vSAN datastore disk that contains copy of VM data.
Datastore Usage Rates	Datastore Read Rate	MB/s	Rate at which data is read from a datastore.
	Datastore Usage	MB/s	Sum of read and write rates for a datastore.
	Datastore Write Rate	MB/s	Rate at which data is written to a datastore.
	Disk/vSAN: Recovery Write Rate	MB/s	Rate of writing data to a vSAN datastore disk that stores copy of VM data.
Datastore Latency	Datastore Highest Latency	Millisecond	Highest latency value across all datastores used by a host.
	Datastore Read Latency	Millisecond	Average amount of time that a read operation from a datastore takes.
	Datastore Write Latency	Millisecond	Average amount of time that a write operation to a datastore takes.
	Disk/vSAN: Recovery Write Latency	Millisecond	Average amount of time that a write operation to a vSAN datastore disk storing copy of VM data takes.
Datastore Issues	Datastore Bus Resets	Number	Number of SCSI bus reset commands.
	Datastore Command Aborts	Number	Number of aborted SCSI commands.

For objects that are parent to ESXi hosts and VMs, Veeam ONE Monitor displays rollup values.
Charts for folders, clusters, datacenters, vCenter Servers display rollup values for all hosts in the container. Chart for a resource pool displays rollup values for all VMs in the resource pool.

Virtual Disks Performance Chart

The **Virtual Disks** chart displays historical statistics for partitions of all disks on the selected VM.

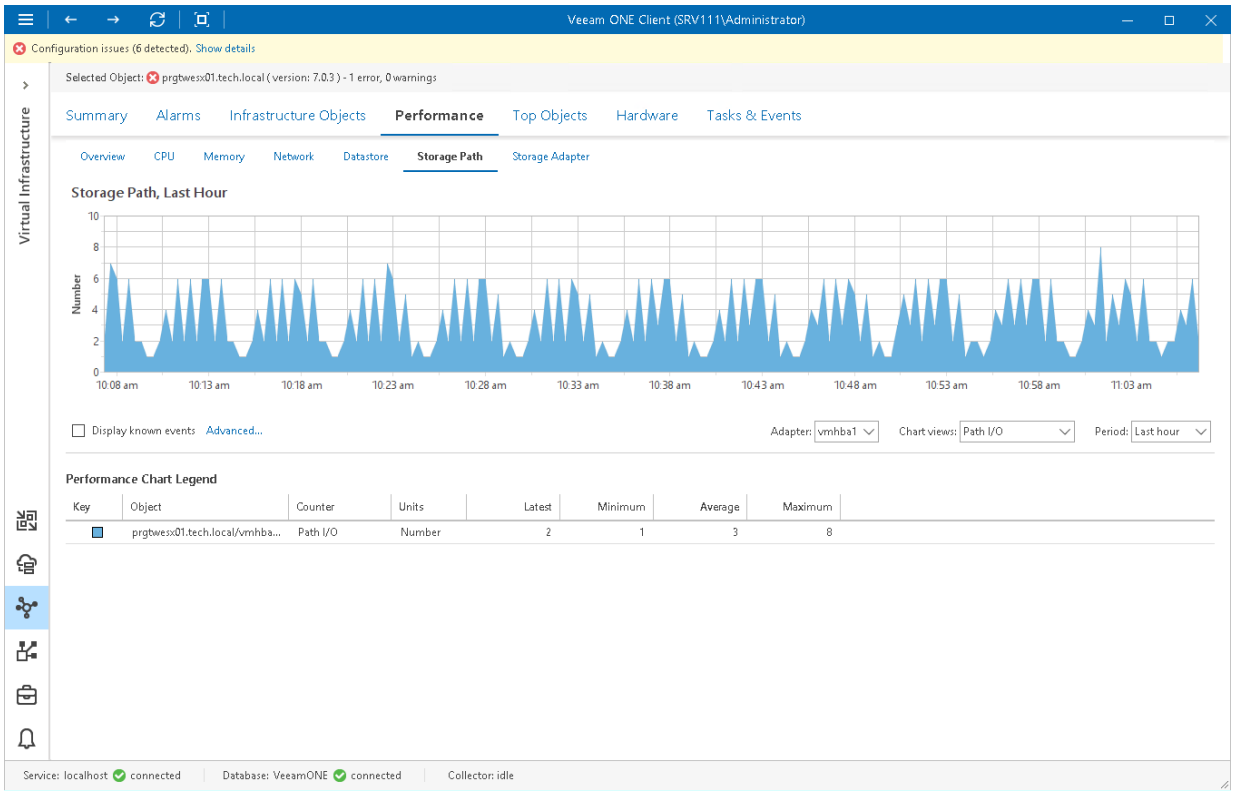


The following table provides information on predefined views and counters.

Chat View	Counter	Measurement Unit	Description
Virtual Disks IOPS	Read I/O	Number	Average number of read operations issued per second to a virtual disk.
	Write I/O	Number	Average number of write operations issued per second to a virtual disk.
Virtual Disks Usage Rates	Read Rate	MB/s	Rate at which data is read from a virtual disk.
	Write Rate	MB/s	Rate at which data is written to a virtual disk.
Virtual Disks Latency	Read Latency	Millisecond	Average amount of time that a read operation from a virtual disk takes.
	Write Latency	Millisecond	Average amount of time that a write operation to a virtual disk takes.

Storage Path Performance Chart

The **Storage Path** chart displays historical statistics for paths used by the storage adapter on the selected host.



You can switch between adapters using the **Adapter** list below the performance chart.

The name of each storage device connected to the storage adapter through the selected path is specified after the host address (separated by a forward slash). It has the following format: *<HBA>:<SCSI target>:<SCSI LUN>:<disk partition>*

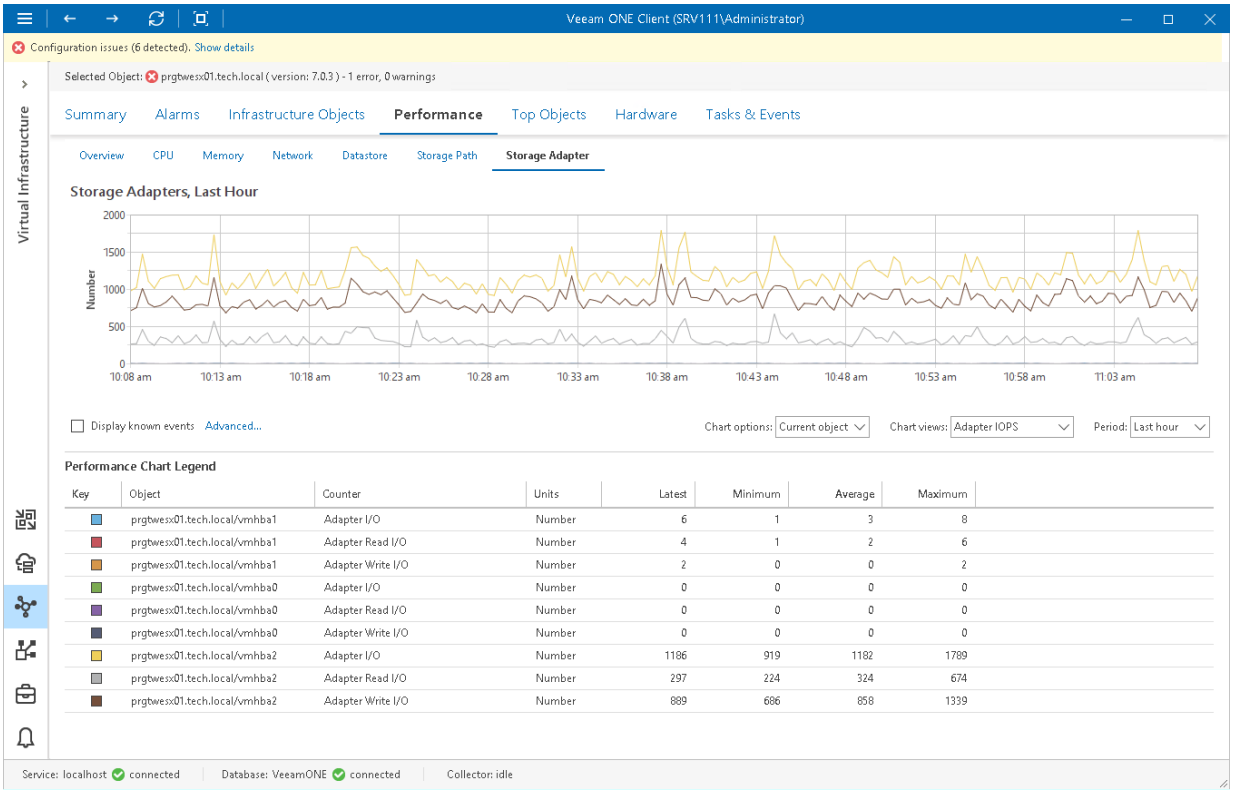
The following table provides information on predefined views and counters.

Chart View	Measurement Unit	Description
Path I/O	Number	Average number of commands issued per second through a path.
Path Read I/O	Number	Average number of read commands issued per second through a path.
Path Write I/O	Number	Average number of write commands issued per second through a path.
Path Read Rate	MB/s	Rate at which data is read through a path.
Path Write Rate	MB/s	Rate at which data is written through a path.

Chart View	Measurement Unit	Description
Path Read Latency	Millisecond	Average amount of time taken for a read operation through a path.
Path Write Latency	Millisecond	Average amount of time that a write operation through a path takes.

Storage Adapter Performance Chart

The **Storage Adapter** chart displays historical statistics for the storage adapters on the selected host.



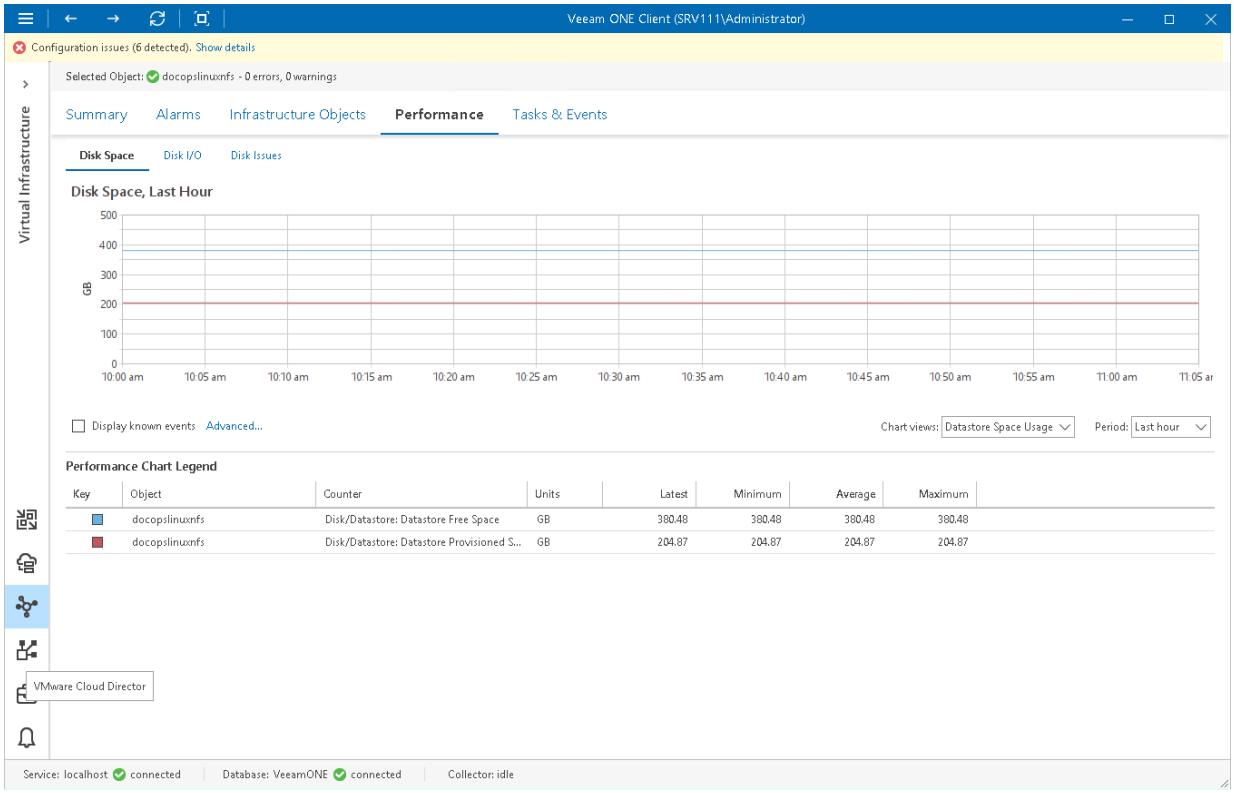
The following table provides information on predefined views and counters.

Chart View	Counter	Measurement Unit	Description
Adapter IOPS	Adapter I/O	Number	Average number of commands issued per second on a storage path during the collection interval.
	Adapter Read I/O	Number	Average number of read commands issued per second on a storage path during the collection interval.
	Adapter Write I/O	Number	Average number of write commands issued per second on a storage path during the collection interval.
Adapter Usage Rates	Adapter Read Rate	MB/s	Rate at which data is read on a storage path.
	Adapter Write Rate	MB/s	Rate at which data is written on a storage path.
Adapter Latency	Adapter Read Latency	Millisecond	Average amount of time that a read operation on a storage path takes.

Chart View	Counter	Measurement Unit	Description
	Adapter Write Latency	Millisecond	Average amount of time that a write operation on a storage path takes.

Disk Space Chart

The **Disk Space** chart is available for datastores and datastore clusters. It displays historical statistics on disk space resources and usage for the selected datastore or datastore cluster.

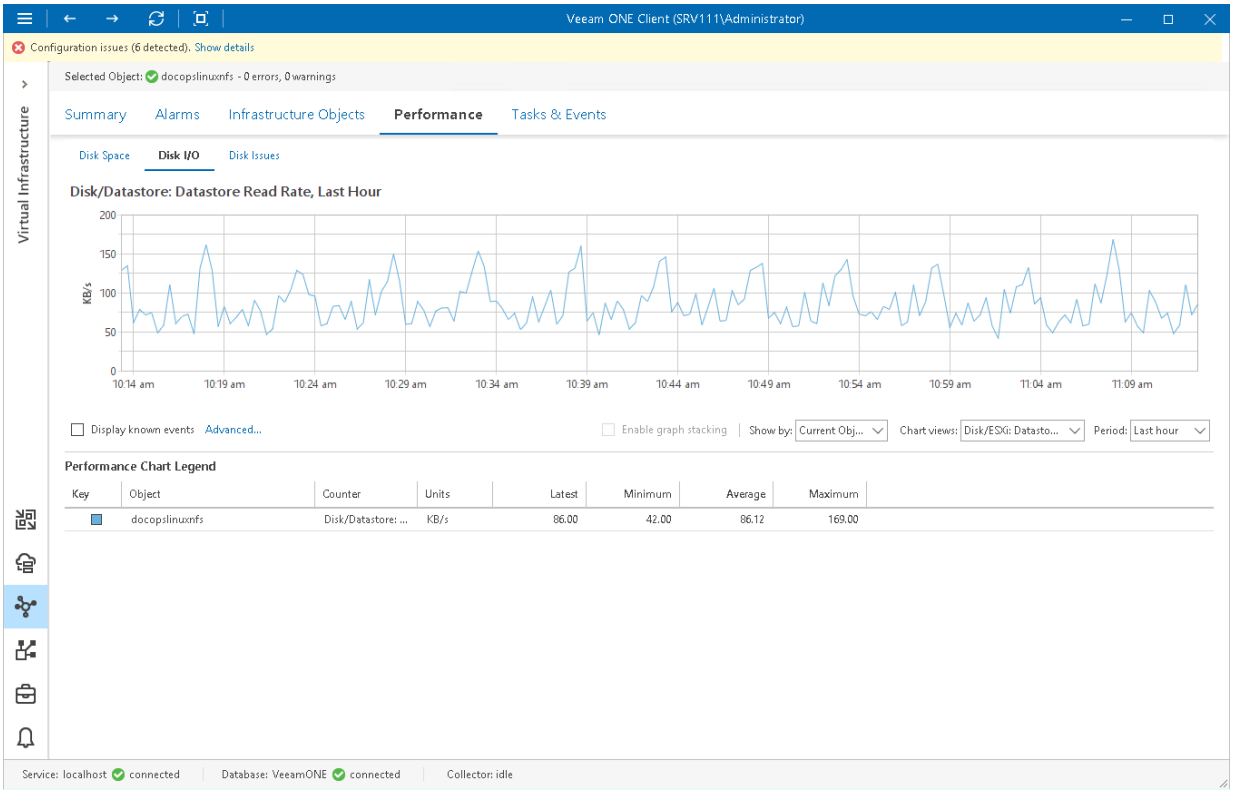


The following table provides information on predefined views and counters.

Chart View	Counter	Measurement Unit	Description
Datastore Space Usage	Disk/Datastore: Datastore Free Space	TB/GB	Amount of free space on a datastore.
	Disk/Datastore: Datastore Provisioned Space	TB/GB	Amount of storage allocated for a datastore. Size of files on the datastore cannot exceed this value.

Disk I/O Chart

The **Disk I/O** chart is available for datastores and datastore clusters. It displays historical statistics on the read and write load.



Use the **Chart options** list to display graphs for the current object (for example, a specific datastore or a virtual infrastructure container), for VMs or hosts that work with the selected datastore. For VMs or for hosts, this chart displays stacked graphs to let you see actual cumulative load on a particular datastore. If you choose to view the chart for the top **Datastore** parent object, you will also be able to stack graphs by all available datastores.

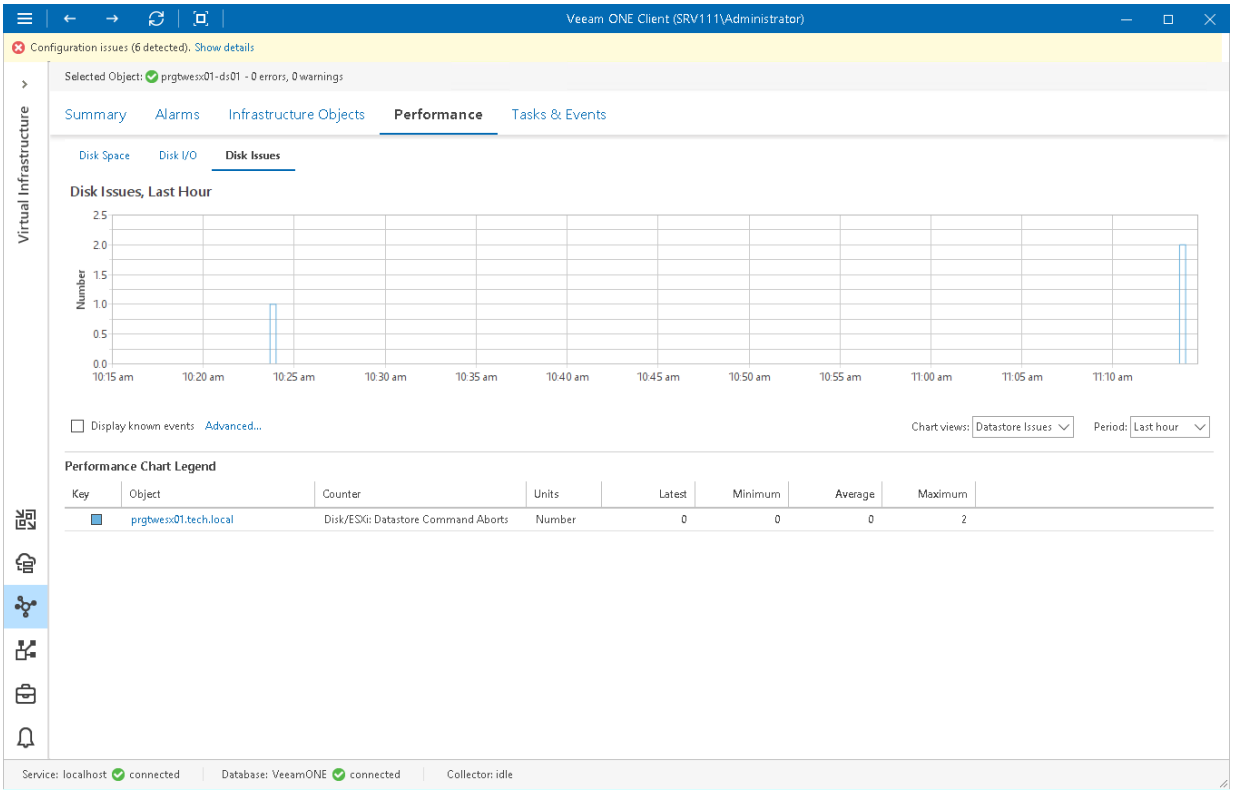
The following table provides information on predefined views and counters.

Chart View	Measurement Unit	Description
Disk/ESXi: Datastore Read Rate	MB/s	Rate at which data is read from a datastore.
Disk/ESXi: Datastore Write Rate	MB/s	Rate at which data is written to a datastore.
Disk/ESXi: Datastore Usage	MB/s	Sum of read and write rates for a datastore.
Disk/ESXi: Datastore Read I/O	Number	Number of times data was read from the disk by all VMs residing on a datastore.

Chart View	Measurement Unit	Description
Disk/ESXi: Datastore Write I/O	Number	Number of times data was written to the disk by all VMs residing on a datastore.
Disk/ESXi: Datastore I/O	Number	Average number of commands issued per second to a storage device by the adapter.
Disk/ESXi: Datastore Read Latency	Millisecond	Average amount of time that a read operation from a datastore takes (from the perspective of an ESXi host).
Disk/ESXi: Datastore Write Latency	Millisecond	Average amount of time that a write operation to a datastore takes (from the perspective of an ESXi host).

Disk Issues Chart

The **Disk Issues** chart displays historical statistics on the number of disk bus resets and disk command aborts that have occurred in the defined interval. This chart is available for datastores and datastore clusters.



The following table provides information on predefined views and counters.

Chart View	Measurement Unit	Counter	Description
Datastore Issues	Disk/ESXi: Datastore Bus Resets	Number	Number of aborted SCSI commands.
	Disk/ESXi: Datastore Command Aborts	Number	Number of SCSI bus reset commands.

Customizing VMware vSphere Performance Charts

You can customize performance charts to select specific objects, time intervals or performance counters to display on the charts.

Selecting Objects to Chart

By default, all performance charts display data for an infrastructure object selected in the inventory pane. You can also choose to display performance data on charts for:

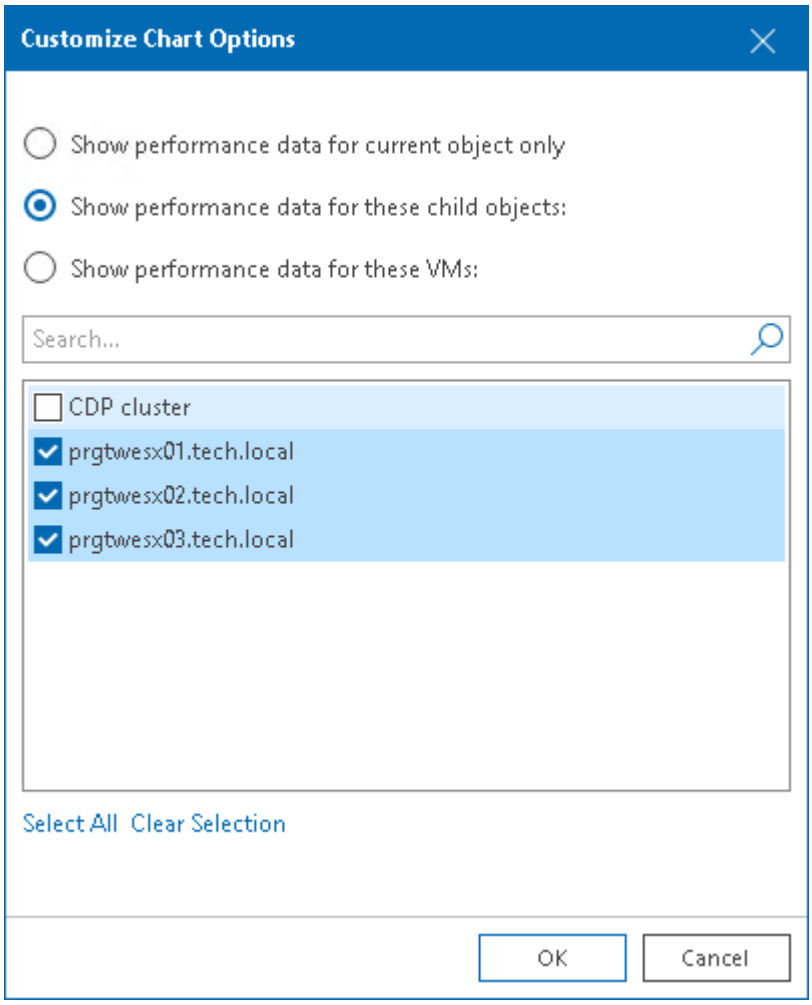
- Child components or objects of the selected virtual infrastructure object (for example, all hosts in the cluster)
- Child VMs for the selected virtual infrastructure object or segment

To display performance data for direct children of the selected virtual infrastructure object:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.
2. At the bottom of the inventory pane, click **Virtual Infrastructure**.
3. In the inventory pane, select the necessary infrastructure object.
4. Open the necessary performance chart tab.
5. From the **Chart options** list, select *Custom*.
6. In the **Customize Chart Options** window, choose **Show performance data for these child objects**.
7. Select check boxes next to child objects that should be included in the chart scope.

8. Click **OK**.



To display performance data for a set of VMs in the selected infrastructure segment:

1. Open Veeam ONE Client.

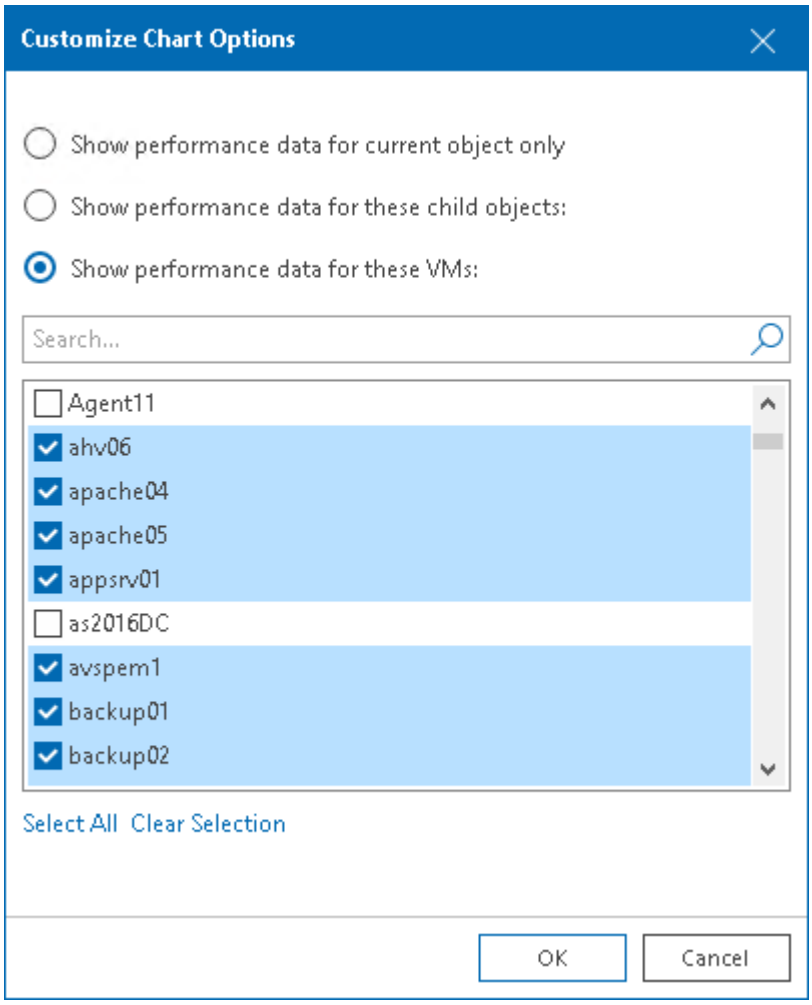
   For details, see Accessing Veeam ONE Components.

2. In the inventory pane, select the necessary infrastructure object.
3. Open the necessary performance chart tab.
4. From the **Chart options** list, select *Custom*.
5. In the **Customize Chart Options** window, choose **Show performance data for these VMs**.

   You can select both direct and indirect children (children of children) of the selected virtual infrastructure object.

6. Select check boxes next to VMs that should be included in the chart scope.

7. Click **OK**.



NOTE:

The legend pane displays objects for which data is available for the selected time interval.

Selecting Chart Views and Performance Counters

Performance charts come with a set of predefined chart views that logically group related performance counters. You can switch between chart views using the **Chart view** list at the top of the chart legend.

Instead of using predefined views, you can choose a custom set of performance counters to show on the chart:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click **Virtual Infrastructure**.
3. In the inventory pane, select the necessary infrastructure object.
4. Open the necessary performance chart tab.
5. From the **Chart views** list, select the *Custom* option to open the **Select Devices and Counters** window.

6. From the **Devices** list, select the necessary resource device(s).

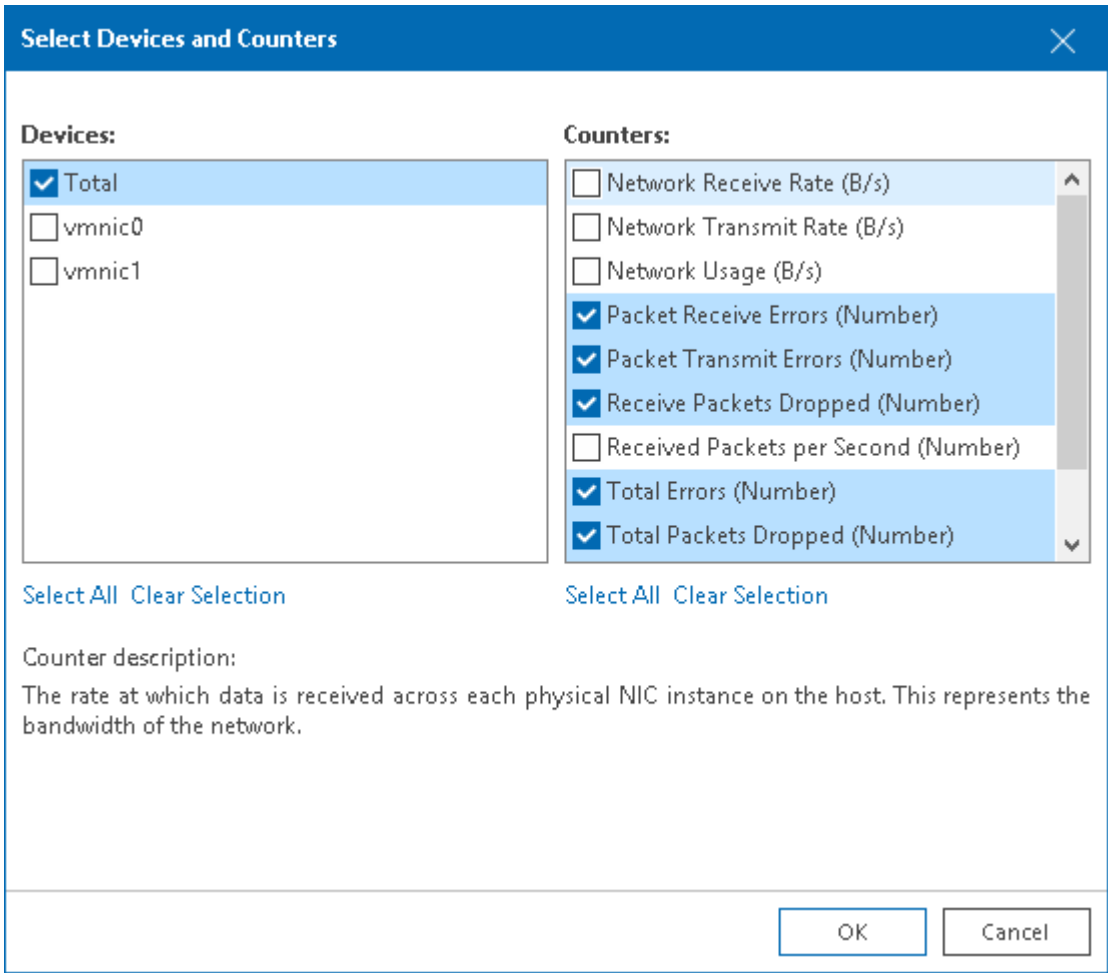
   Select *Total* to display all available devices on the chart.

> **NOTE:**
>
> The list of devices is not available for some performance charts. For example, for the **CPU** or **Memory** performance chart, you can only choose counters to display.

7. From the **Counters** list, select counters to display on the chart.

   When you select a counter, its description appears in the **Counter description** section of the window.

8. Click **OK**.



Selecting Time Interval

You can choose the time interval for which performance data on the chart will be displayed. Available options are:

- Last hour (real-time information)
- Last day
- Last week
- Last month

- Last year
- Custom time range (you can choose any time interval within the specified number of hours, days, or weeks, or specify any from/to period)

To specify a time interval for which performance data should be displayed:

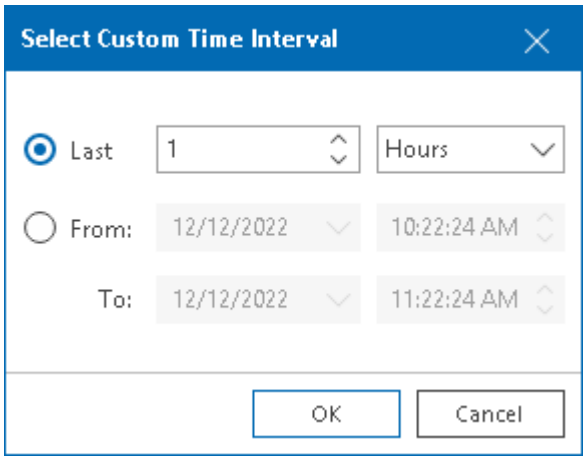
1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click **Virtual Infrastructure**.
3. In the inventory pane, select the necessary infrastructure object.
4. Open the necessary performance chart tab.
5. From the **Period** list, select *Last hour*, *Last day*, *Last week*, *Last month* or *Last year*.

   To define a custom time range, select *Custom*. In the **Select Custom Time Interval** window, define the necessary interval and click **OK**.

When you change the time interval, the time scale (X-axis) of the performance chart and the chart will change respectively.



VMware vSphere Tasks & Events

You can view information about tasks and events that occur in the virtual environment within the selected time interval. Veeam ONE loads tasks and events from vCenter Server. For each loaded task, it creates two events — one informs you when the task starts and the other informs you when the task ends.

To view the list of tasks and events:

1. Open Veeam ONE Client.

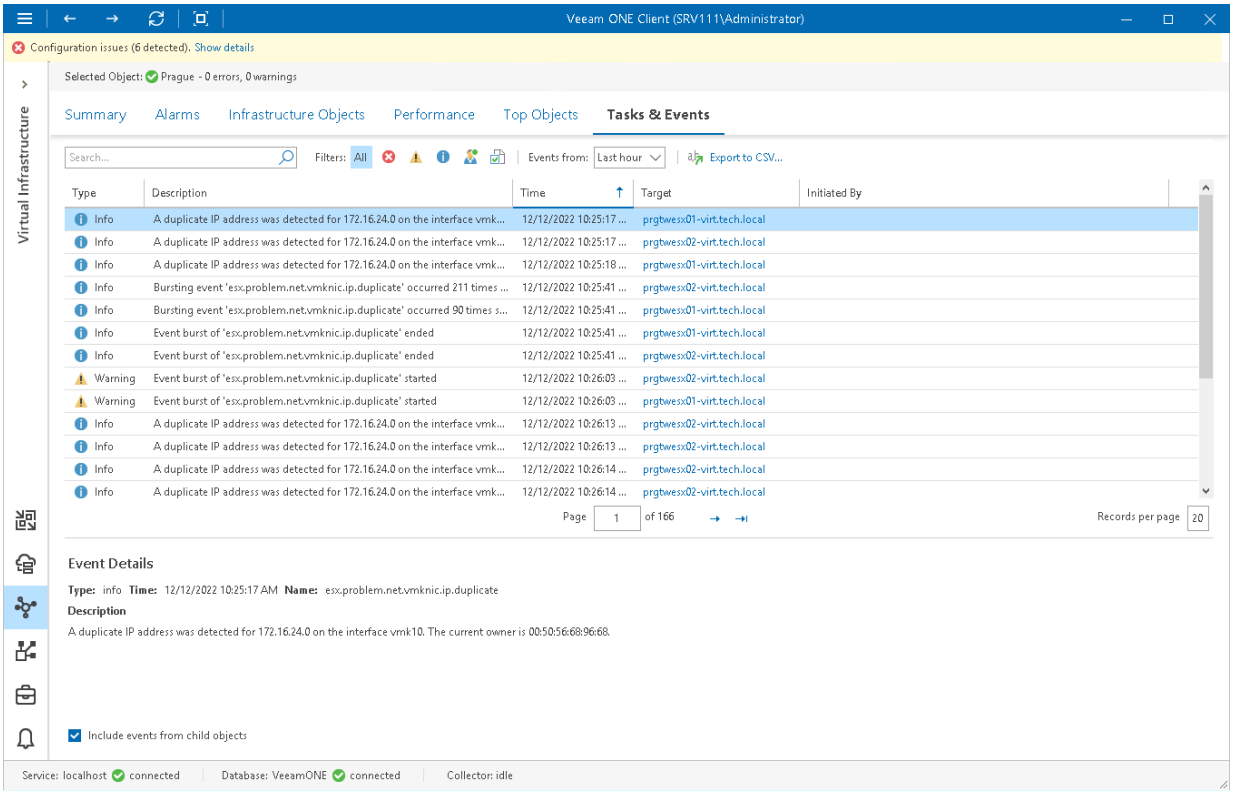
   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click **Virtual Infrastructure**.
3. In the inventory pane, select the necessary infrastructure object.
4. Open the **Tasks & Events** tab.
5. The **Tasks & Events** list can display up to 1000 tasks and events at a time. To find the necessary task or event, you can use the following controls:
   - To display tasks or events for a specific period, select the necessary time interval from the **Events from** list.
   - To show or hide tasks or events, use filter buttons at the top of the list — *Show all events*, *Show errors*, *Show warnings*, *Show info messages*, *Show user events*, *Show tasks*.
   - To find the necessary tasks or events by description, use the **Search** field at the top of the list.
6. To view the detailed description of an event, click it in the **Tasks & Events** list.

   The event description will be shown in the **Event Details** pane at the bottom.

   When you choose a virtual infrastructure container in the inventory pane, you can view events for the selected object and events for its child objects. To hide events related to child objects, clear the **Include events from child objects** check box at the bottom of the **Event Details** section.

7. To export displayed events to a CSV file, click **Export to CSV** at the top of the list and specify the location where the file will be saved.



For every task or event in the list, the following details are available:

- Event type (*User*, *Task*, *Info*, *Warning* or *Error*)
- Short description
- Time of occurrence
- Object to which the task or event relates
- Object or user that caused or initiated the event

Viewing Events on Performance Charts

Performance charts for VMware vSphere infrastructure objects allow you to display the following resource-consuming events:

- Live Migration (vMotion)
- Snapshot creation events
- Snapshot removal events
- Veeam Backup & Replication events

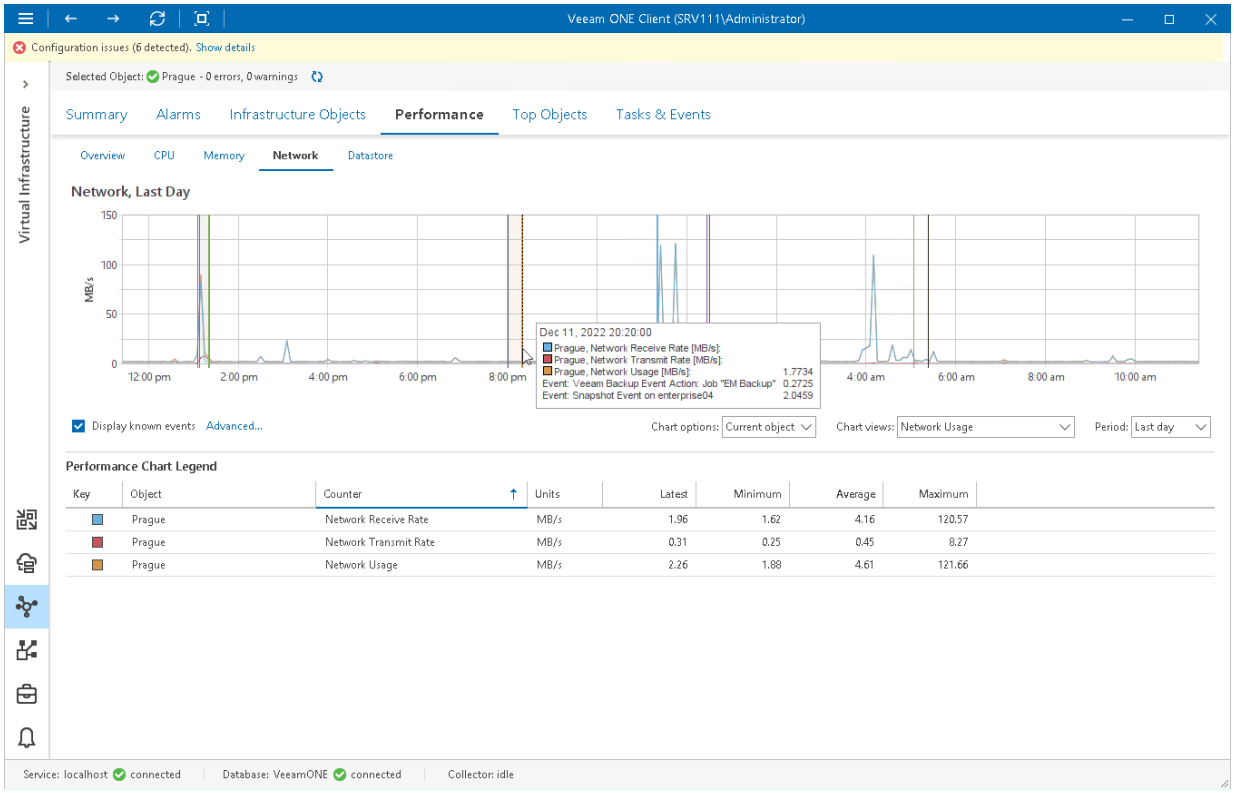
This option can help you detect events that caused performance degradation. For example, you can see what was the reason for a steep increase in the network resources usage.

To display events on a performance chart:

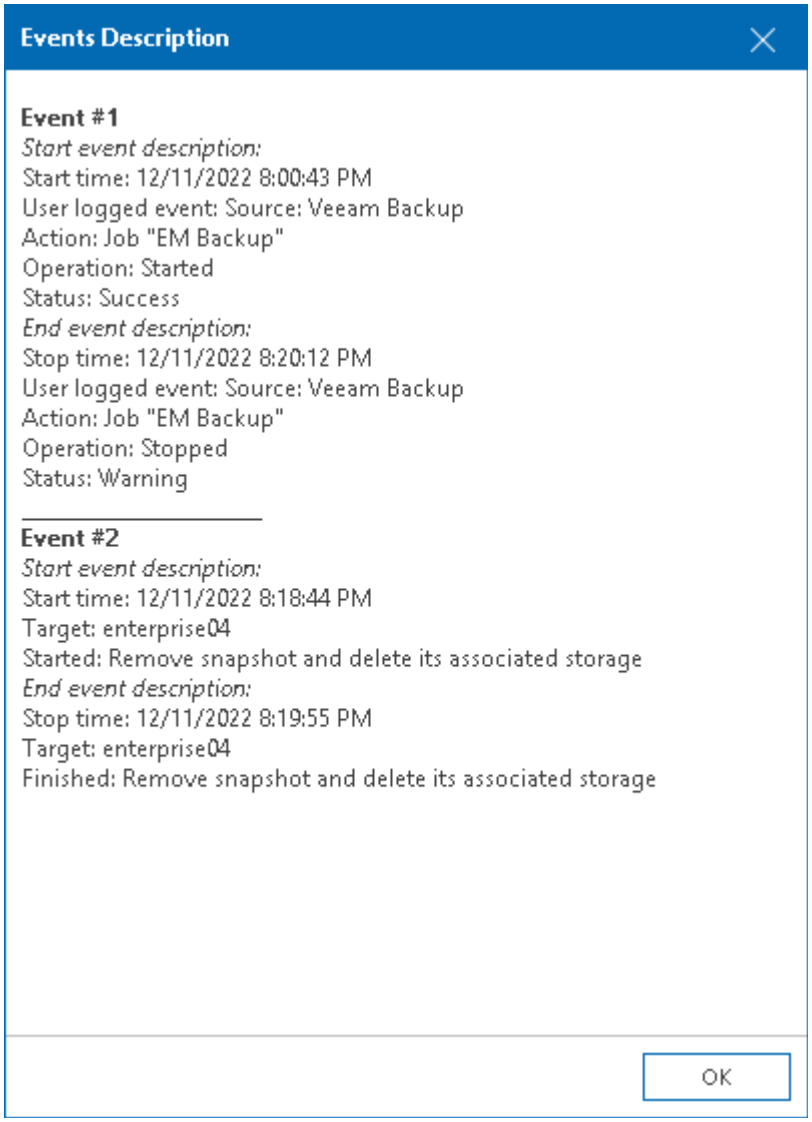
1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click **Virtual Infrastructure**.
3. In the inventory pane, select the necessary infrastructure object.
4. Open the necessary performance chart tab.
5. At the bottom of the performance chart, select the **Display known events** check box.
6. To choose what type of events to show on the performance chart, click the **Advanced** link next to the **Display known events** check box, and select the necessary events.



Events are shown as vertical lines crossing the performance graphs. To learn more about an event, hover the mouse cursor over it to see a tooltip, or click the line in the graph. The **Events Description** window will provide detailed information about the event.



NOTE:

The **Display known events** option is available only for time intervals not greater than 3 days. You will not be able to view events on the performance chart if a longer time interval is selected.

VMware vSphere Virtual Machines

You can view the list of VMs within a virtual infrastructure container — on a host, on a datastore, in a folder and so on.

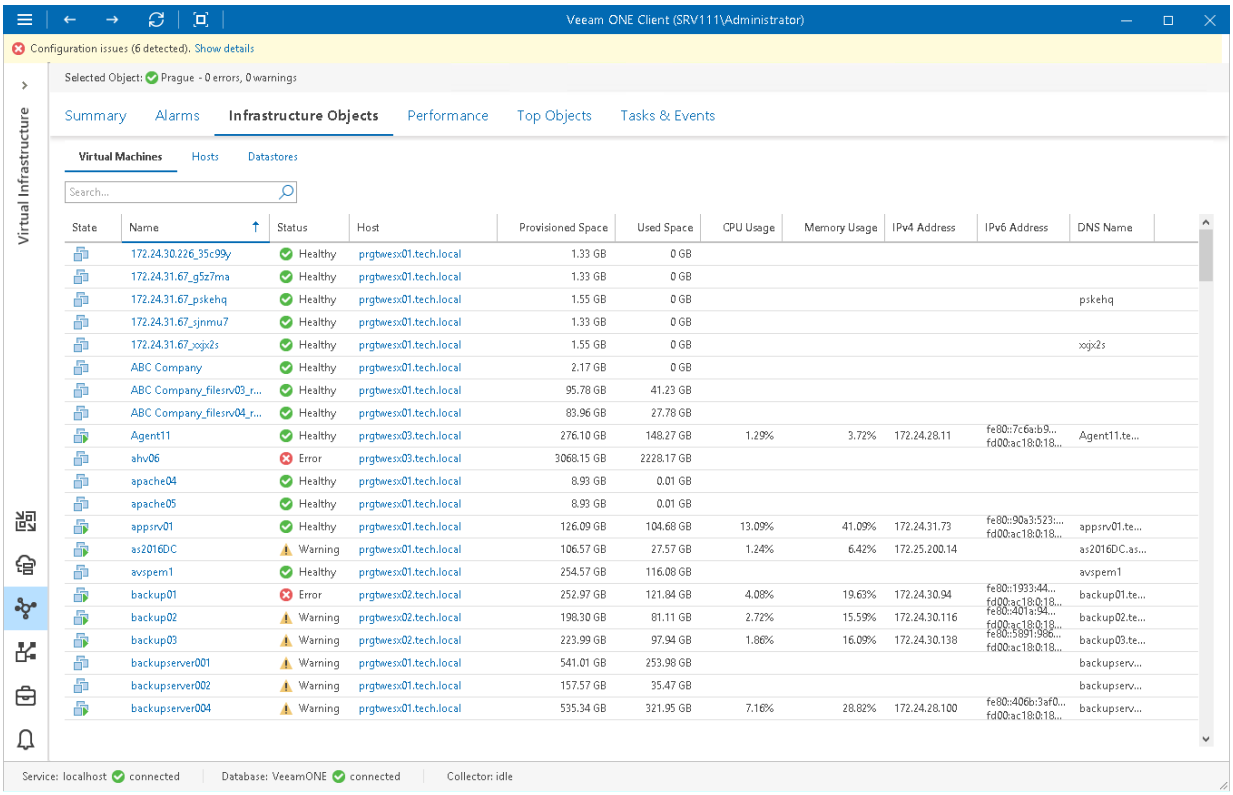
To view the list of VMs:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click **Virtual Infrastructure**.
3. In the inventory pane, select the necessary infrastructure container.
4. Open the **Infrastructure Objects** tab and navigate to **Virtual Machines**.
5. To find the necessary VM by name, use the **Search** field at the top of the list.
6. Click column names to sort VMs by a specific parameter.

   For example, to view what VMs are consuming the greatest amount of memory, you can sort VMs in the list by **Memory Usage**.



For every VM in the list, the following details are available:

- **State** — state of the VM (*powered on*, *powered off*, *suspended*)
- **Name** — name of the VM
- **Status** — current status of the VM in terms of alarms (*healthy*, *warning* or *error*)
- **Host** — name of the host on which the VM resides
- **Provisioned Space** — amount of storage space provisioned for the VM

- **Used Space** — amount of storage space actually used for storing VM files (for VMs with thin provisioned disks, this value is normally less than *Provisioned Space*)
- **CPU Usage** — amount of actively used virtual CPU as a percentage of total available CPU resources
- **Memory Usage** — amount of actively used memory resources as a percentage of configured VM memory
- **IP V4 Address** — IP v4 address assigned to the VM
- **IP V6 Address** — IP v6 address assigned to the VM
- **DNS Name** — DNS name of the VM
- **vCPU** — number of virtual CPUs configured for the VM
- **Assigned Memory** — amount of virtual memory allocated for the VM
- **Guest OS** — guest operating system installed in the VM
- **VMware Tools** — state of VMware Tools
- **Hardware Version** — hardware version of the VM

You can choose what columns to show or hide in the **Virtual Machines** table:

- To hide one or more columns, right-click the table header, and clear check boxes next to the corresponding data fields.
- To make hidden columns visible, right-click the table header, and select check boxes next to the corresponding data fields.

VMware vSphere Hosts

You can view the list of ESXi hosts in your VMware vSphere infrastructure — on vCenter Server or in a datacenter.

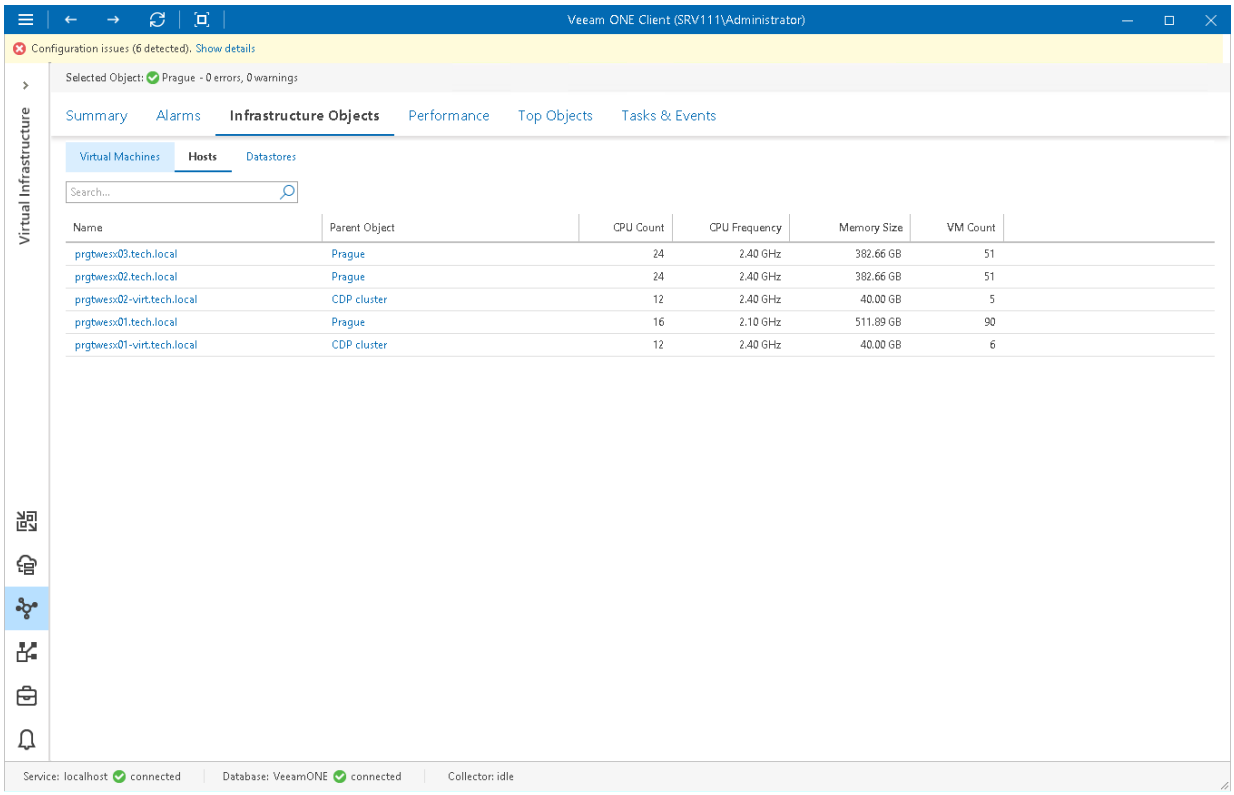
To view the list of hosts:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click **Virtual Infrastructure**.
3. In the inventory pane, select the necessary infrastructure container.
4. Open the **Infrastructure Objects** tab and navigate to **Hosts**.
5. To find the necessary host by name, use the **Search** field at the top of the list.
6. Click column names to sort hosts by a specific parameter.

   For example, to view hosts with the greatest number of VMs, you can sort VMs in the list by **VM Count**.



For every host in the list, the following details are available:

- **Object** — name of the host
- **Parent Object** — name of the parent infrastructure object
- **CPU Count** — number of CPU cores on the host
- **CPU Frequency** — frequency of the host CPU core in GHz
- **Memory Size** — amount of physical memory available on the host

- **VM Count** — number of VMs that reside on the host

You can choose what columns to show or hide in the **Hosts** table:

- To hide one or more columns, right-click the table header, and clear check boxes next to the corresponding data fields.
- To make hidden columns visible, right-click the table header, and select check boxes next to the corresponding data fields.

VMware vSphere Datastores

You can view the list of datastores in your VMware vSphere infrastructure — on vCenter Server or in a datacenter.

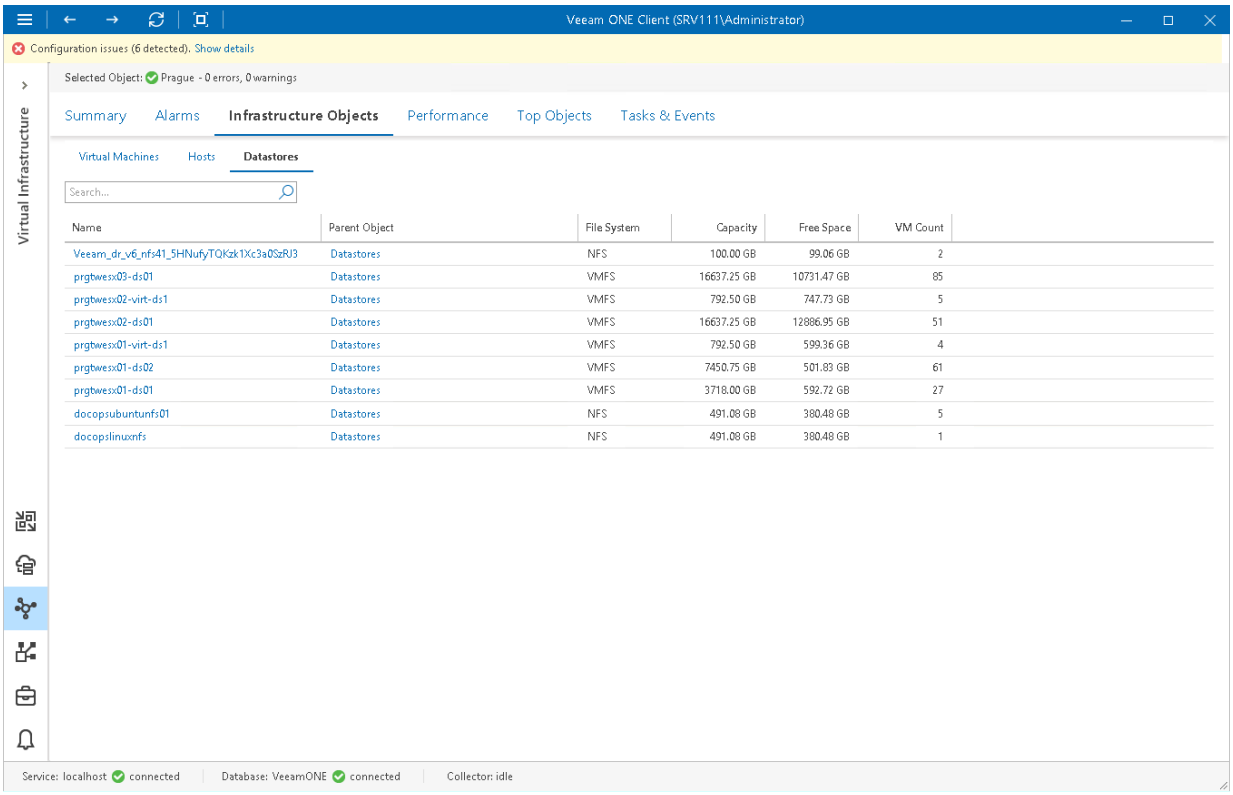
To view the list of datastores:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click **Virtual Infrastructure**.
3. In the inventory pane, select the necessary infrastructure container.
4. Open the **Infrastructure Objects** tab and navigate to **Datastores**.
5. To find the necessary datastore by name, use the **Search** field at the top of the list.
6. Click column names to sort datastores by a specific parameter.

   For example, to view what datastores have the greatest amount of free space, you can sort datastores in the list by **Free Space**.



For every host in the list, the following details are available:

- **Object** — name of the datastore
- **Parent Object** — name of the parent object in the infrastructure
- **File System** — type of the file system on the datastore
- **Capacity** — total capacity of the datastore
- **Free Space** — amount of available free space on the datastore

- **VM Count** — number of VMs that reside on the datastore

You can choose what columns to show or hide in the **Hosts** table:

- To hide one or more columns, right-click the table header, and clear check boxes next to the corresponding data fields.
- To make hidden columns visible, right-click the table header, and select check boxes next to the corresponding data fields.

VMware vSphere Top Objects

The Top Objects dashboards help you detect VMs and hosts consuming the most and the least amount of resources in the selected virtual infrastructure segment:

- **Top vSphere VMs** dashboard displays top VM consumers in terms of CPU, memory, datastore, network usage, memory swapped, active snapshot size, active snapshot age and the number of existing snapshots.
- **Top vSphere Hosts** dashboard displays top host consumers in terms of CPU, memory, datastore, network usage and swapped memory.
- **Bottom vSphere Hosts** dashboard displays least loaded hosts in terms of CPU, memory, datastore, network and memory swap used.

  You can use this dashboard to choose hosts where you can deploy new VMs or to which you can move existing VMs.

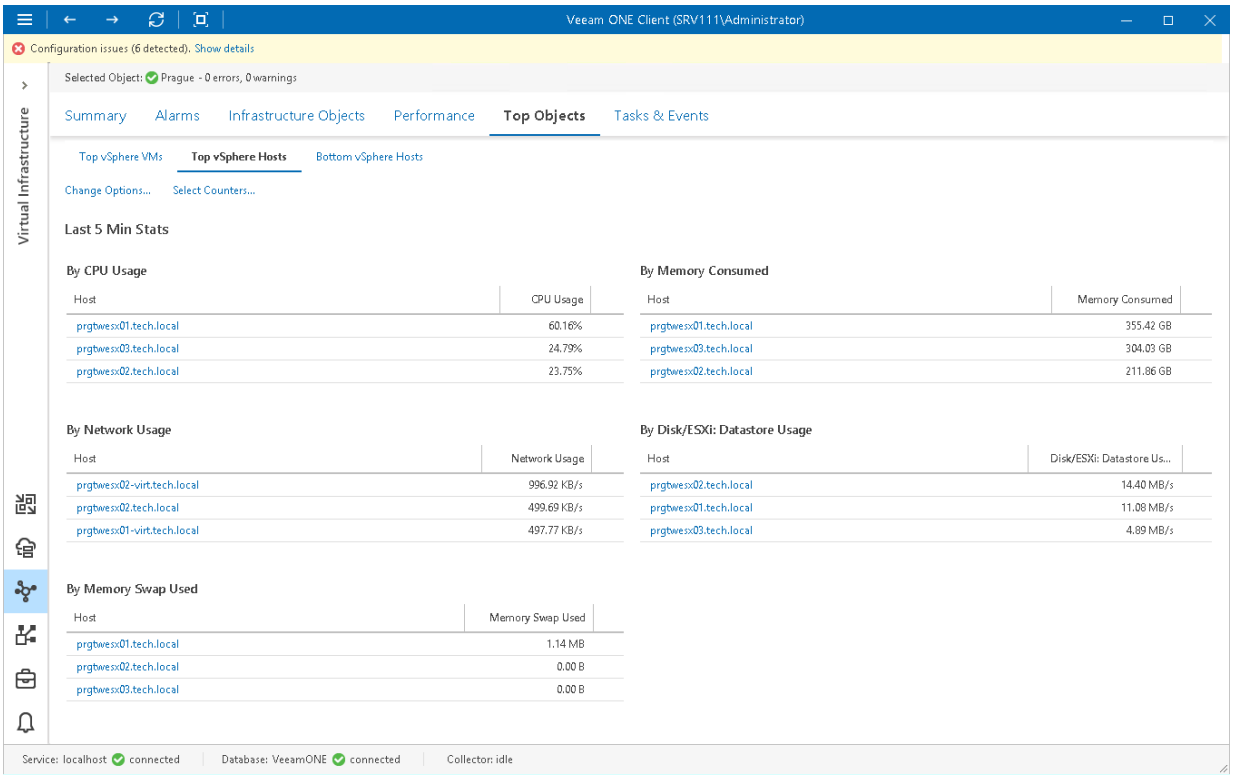
To detect the most and the least loaded hosts or VMs:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.
2. At the bottom of the inventory pane, click **Virtual Infrastructure**.
3. In the inventory pane, select the necessary infrastructure container.
4. Open the **Top Objects** tab and switch to the necessary dashboard — **Top vSphere VMs**, **Top vSphere Hosts** or **Bottom vSphere Hosts**.
5. At the top left corner of the dashboard, click the **Change Options** link.
   a. In the **Interval** field, set the time interval for which resource utilization statistics must be analyzed.
   b. In the **VMs to display/Hosts to display** field, specify the number of objects to display on the dashboard.
6. At the top left corner of the dashboard, click the **Select Counters** link.
   a. In the **Select Counters** window, choose metrics that must be included in the dashboard.

      Press and hold the `[SHIFT]` or `[CTRL]` key on the keyboard to select multiple counters.

b. Click **OK**.


Veeam ONE Client (SRV111\Administrator)
Configuration issues (6 detected). Show details
Selected Object: Prague - 0 errors, 0 warnings
Summary
Alarms
Infrastructure Objects
Performance
Top Objects
Tasks & Events
Top vSphere VMs
Top vSphere Hosts
Bottom vSphere Hosts
Change Options...
Select Counters...
Virtual Infrastructure
Last 5 Min Stats
By CPU Usage
Host
CPU Usage
prgtwesx01.tech.local
60.16%
prgtwesx03.tech.local
24.79%
prgtwesx02.tech.local
23.75%
By Memory Consumed
Host
Memory Consumed
prgtwesx01.tech.local
355.42 GB
prgtwesx03.tech.local
304.03 GB
prgtwesx02.tech.local
211.86 GB
By Network Usage
Host
Network Usage
prgtwesx02-virt.tech.local
996.92 KB/s
prgtwesx02.tech.local
499.69 KB/s
prgtwesx01-virt.tech.local
497.77 KB/s
By Disk/ESXi: Datastore Usage
Host
Disk/ESXi: Datastore Us...
prgtwesx02.tech.local
14.40 MB/s
prgtwesx01.tech.local
11.08 MB/s
prgtwesx03.tech.local
4.89 MB/s
By Memory Swap Used
Host
Memory Swap Used
prgtwesx01.tech.local
1.14 MB
prgtwesx02.tech.local
0.00 B
prgtwesx03.tech.local
0.00 B
Service: localhost connected
Database: VeeamONE connected
Collector: idle

Host Hardware State

You can monitor the health of ESXi host hardware components. Veeam ONE collects sensor details for chassis, memory, power, processors, software components, storage, system, watchdog, fan, temperature, voltage and other components.

To monitor the health status of host hardware components:

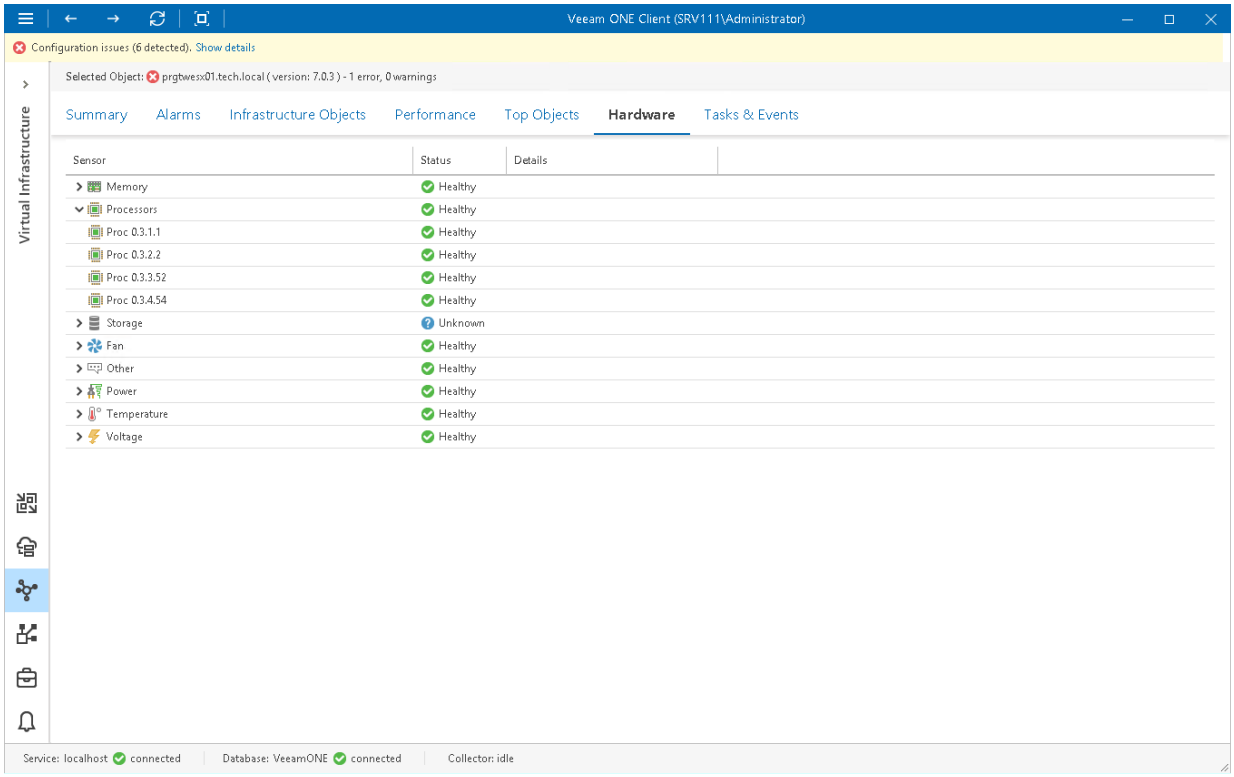
1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click **Virtual Infrastructure**.

3. In the inventory pane, select the necessary host.

4. Open the **Hardware** tab.



The color of the status indicator changes depending on the state of the corresponding component for a standalone host and on the status of a triggered vCenter Server alarm:

- *Green* — the subsystem is functioning properly.
- *Yellow* and *Red* — the performance threshold is exceeded, performance has gone down or the subsystem has stopped operating.

VMware Remote Console (VMRC)

You can access the VMware Remote Console (VMRC) right from the Veeam ONE Client interface. From within the VMware Remote Console, you can isolate the root cause of VM performance problems and perform management tasks — for example, restart an unresponsive VM.

This option requires no additional software installed on the Veeam ONE server and is available for both Window-based and Linux-based OS's.

> **NOTE:**
>
> VMware Remote Console is not included as part of Veeam ONE and Veeam Backup & Replication installation and must be installed separately. For details on VMware Remote Console, see Install the VMware Remote Console Application.

Accessing VMware Remote Console

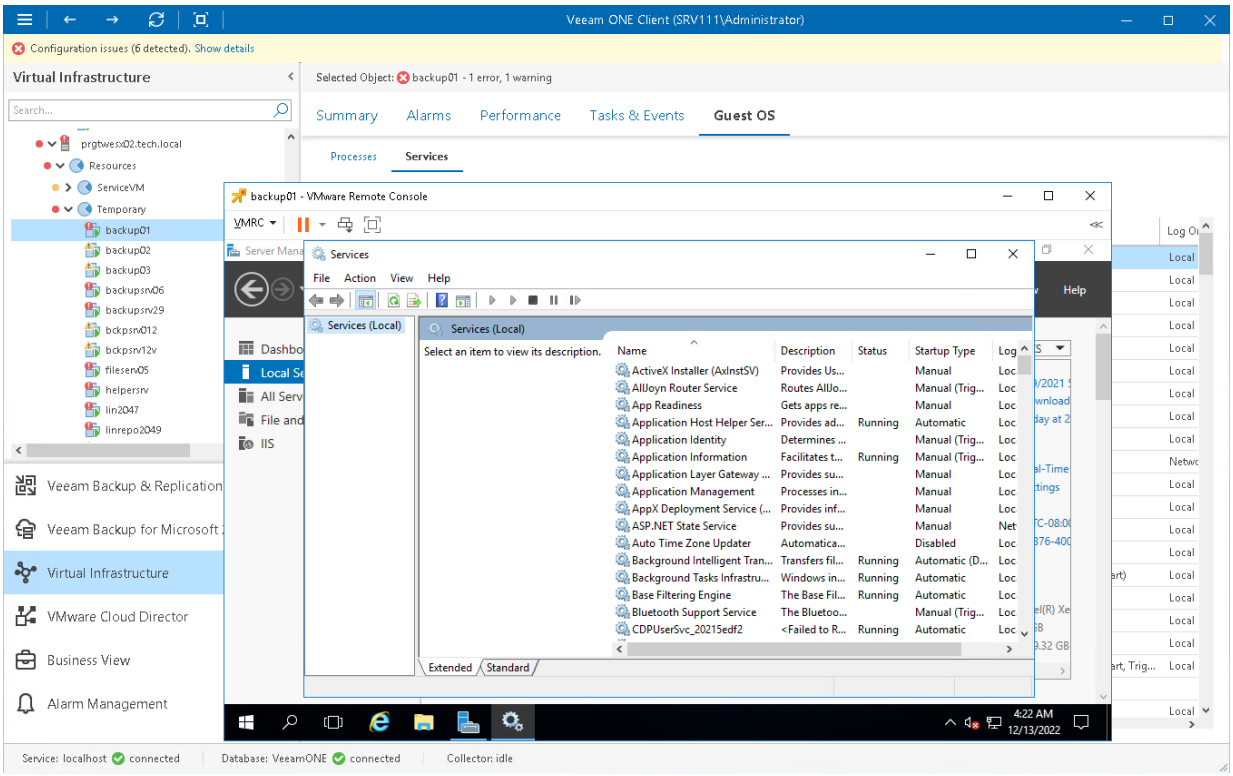
To access the VMware Remote Console:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click **Virtual Infrastructure**.

3. In the inventory pane, right-click the necessary VM and select **Open Console** from the shortcut menu.



You can use buttons at the top of the VMware Remote Console to manage the VM and change its power state.

To connect to a VM or change the VM power state, you can also right-click the VM in the inventory pane and use one of the following shortcut menu commands:

- To access the VM using Windows Remote Desktop Connection, choose **Remote Management > Connect to VM**.
- To change the VM power state, choose **Remote Management** and choose the necessary command.

VMware vSphere In-Guest Processes

You can view and control processes currently running inside a VM or vCenter Server.

- For Windows-based machines, you can view, end or restart processes.
- For Linux-based machines, you can view or end daemons.

Prerequisites

Before viewing in-guest processes, check the following prerequisites:

- Make sure that VMware Tools are installed.
- For Linux-based machines, make sure that the SSH Server is started.
- For Windows based machines make sure:
  - The Remote Registry service is *Enabled* and *Started*.
  - The Local Policy *Always wait for the network at computer startup and logon* is enabled.
  - Make sure that the fully qualified domain name (FQDN) can be resolved by the Veeam ONE server.

Viewing In-Guest Processes

To view the list of processes:

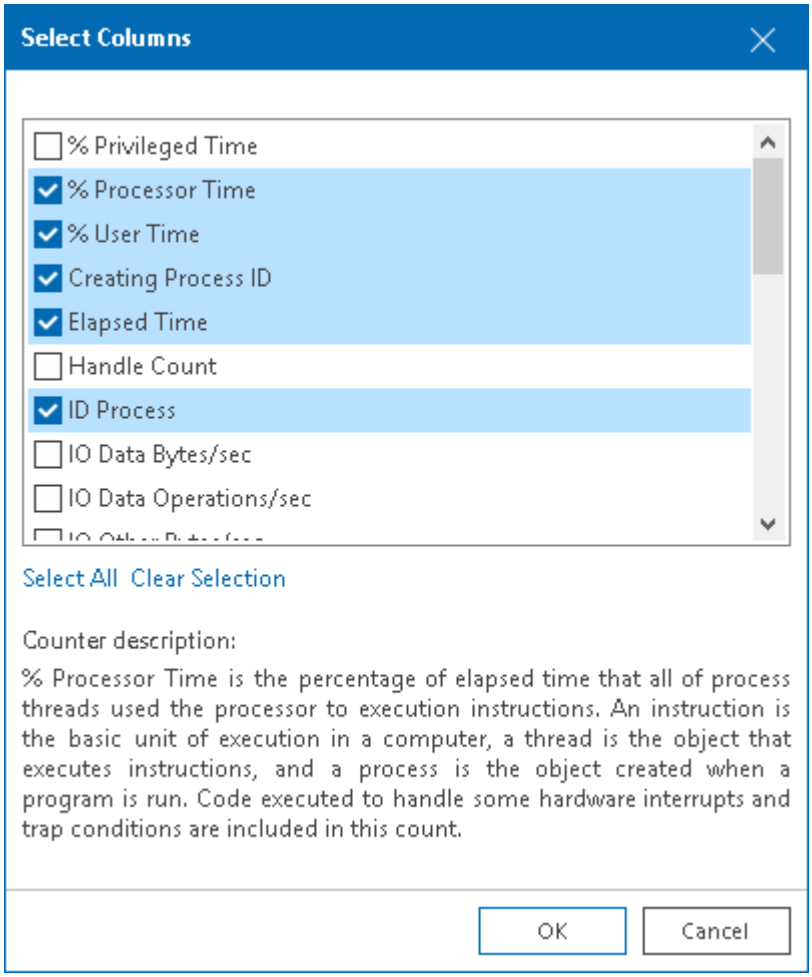
1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.
2. At the bottom of the inventory pane, click **Virtual Infrastructure**.
3. In the inventory pane, select the necessary infrastructure object.
4. Open the **Guest OS** tab and navigate to **Processes**.
5. Provide OS authentication credentials (user name and password) to access the list of running processes.

Every process is described with a set of counters that are presented as column headings. You can add or remove counters to monitor running processes:

1. In the upper right corner of the **Processes** dashboard, click the **Select Columns** link.
2. In the **Select Columns** window, select check boxes next to counters you want to display.

3. To view the detailed description of a counter, click it in the **Counters** list. The description will be displayed in the lower pane of the window.



You can end unwanted processes running on the VM or create an alarm based on the process state or object performance:

- [For Windows-based machines] To end a process, select it in the list and click the **Kill Process** button, or right-click a necessary process and select **Kill Process** from the shortcut menu.
- [For Linux-based machines] To end a daemon, select it in the list and click the **Kill Process** button and choose one of the following options:
  - **Hangup** – to send the `SIGHUP` signal
  - **Kill** – to send the `SIGKILL` signal
  - **Terminate** – to send the `SIGTERM` signal

  You can also right-click a necessary process and select **Kill Process** and choose the necessary option from the shortcut menu.
- [For Windows-based machines] To create an alarm, select one or more processes in the list, click the **Create Alarm** button, and select the type of rule on which the alarm must be based. For details on alarm rules, see Alarm Rules.

VMware vSphere In-Guest Services

You can view and control services currently running inside a VM or vCenter Server.

- For Windows-based machines, you can view, start, stop and restart services, and create alarms based on retrieved services.
- For Linux-based machines, you can view or end services.

Prerequisites

Before viewing in-guest services, check the following prerequisites:

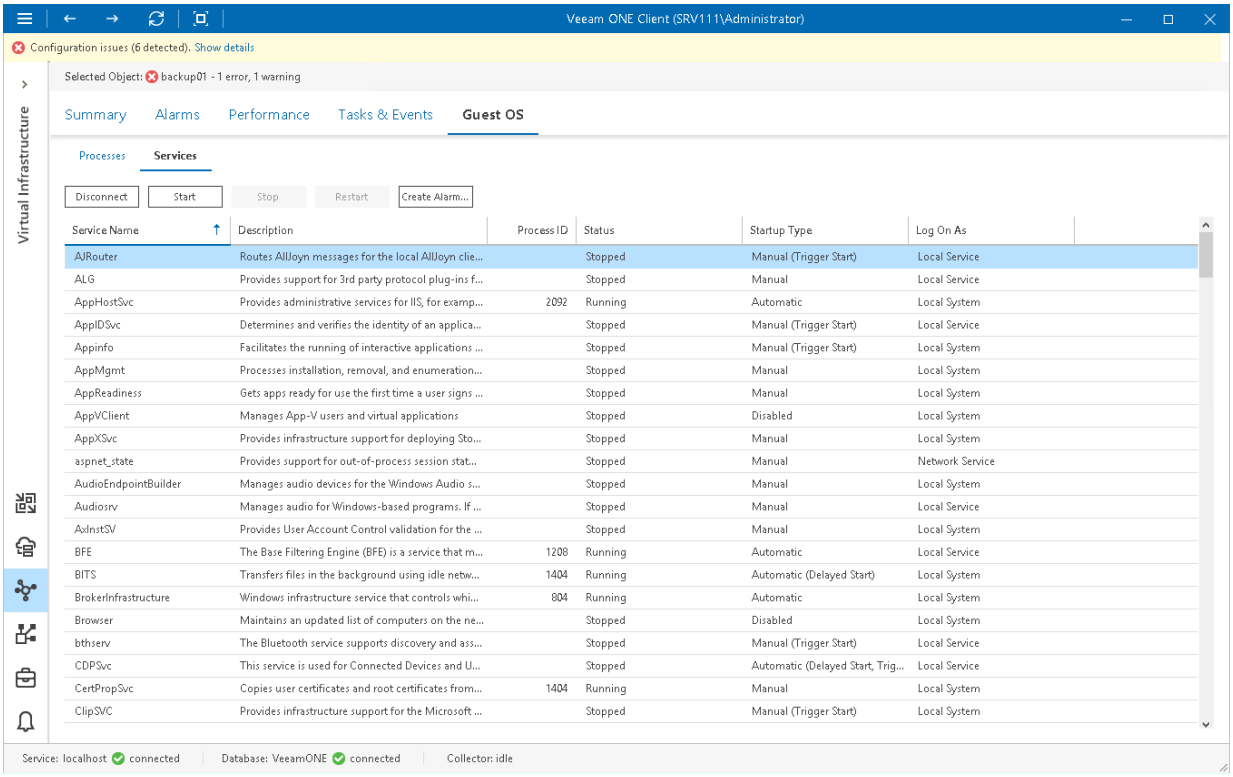
- For VMs, make sure that VMware Tools are installed.
- For Linux-based machines, make sure that the SSH Server is started.

Viewing In-Guest Services

To view the list of services:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.
2. At the bottom of the inventory pane, click **Virtual Infrastructure**.
3. In the inventory pane, select the necessary infrastructure object.
4. Open the **Guest OS** tab and navigate to **Services**.
5. Provide OS authentication credentials (user name and password) to access the list of running services.



You can start, stop and restart a running service, or create an alarm based on the service state or object performance:

- To restart a service, click the **Restart** button, or right-click a necessary service and select **Restart** from the shortcut menu.
- To disconnect from guest OS, click the **Disconnect** button.
- [For Windows-based machines] To create an alarm, select a service in the list, click the **Create Alarm** button, and select the type of rule on which the alarm must be based. For details on alarm rules, see Alarm Rules Reference.

Launching vSphere Client

You can launch vSphere Client or vSphere Web Client from within Veeam ONE Client.

Prerequisites

Before launching vSphere Client, check the following prerequisites:

- The **Open with vSphere Client** option is available only if vSphere Client is installed on the machine where the Veeam ONE Client runs.
- To launch vSphere Client from Veeam ONE Client, you must have the **x86** version of Veeam ONE Client installed.

Launching vSphere Client

To launch the vSphere Client from Veeam ONE Client:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.
2. At the bottom of the inventory pane, click **Virtual Infrastructure**.
3. In the inventory pane, right-click a vCenter Server or ESXi host and choose **Open with vSphere Client** or **Open with vSphere Web Client** from the shortcut menu.

VMware Cloud Director Monitoring

Veeam ONE Client offers a comprehensive view for the logical and physical layers of the VMware Cloud Director infrastructure. Veeam ONE collects real-time statistics from connected VMware Cloud Director servers and underlying vCenter Servers to help you track provider capacities, monitor resource usage and identify issues that may potentially result in SLA breaches.

With Veeam ONE Client, you can:

1. **Monitor health status of the VMware Cloud Director infrastructure**.

   Start with the **Summary** dashboards to check the health status of the VMware Cloud Director infrastructure and supporting VMware vSphere components.

   View the latest alarms, track pending blocking tasks and expired leases and review the overall state of vApps and VMs provisioned by Cloud Director tenants.

2. **View triggered alarms**.

   Switch to the **Alarms** dashboard to see details on issues and problems occurred in the VMware Cloud Director infrastructure. VMware Cloud Director alarms will notify you on increasing resource usage for provider and organization VDCs, expiring vApp runtime and storage leases, blocking tasks left with no response, and the health status of Cloud Director infrastructure components.

3. **Work with performance charts**.

   Drill down to performance charts to diagnose performance problems and identify resource bottlenecks.

   Track CPU, memory, disk and network performance for underlying hosts, VMs, VM containers, organizations, organization VDCs and vApps.

4. **Monitor Cloud Director capacities and resource usage**.

   Monitor available, allocated and consumed resources to make sure that VMs and vApps have enough allocated CPU, memory and storage resources, and Cloud Director tenants have enough capacities to run their workloads.

5. **Investigate problems from within the guest OS**.

   View the list of in-guest processes to diagnose problems related to a specific service, module or application within the guest OS.

Prerequisites

Before you start monitoring the VMware Cloud Director environment, make sure you have configured connections to Cloud Director servers from which Veeam ONE will collect data. For details on configuring server connections, see Connecting VMware Cloud Director Servers.

VMware Cloud Director Summary Dashboards

VMware Cloud Director summary dashboards serve as the 'launch point' for monitoring the VMware Cloud Director infrastructure state. The dashboards reflect the health status of all VMware Cloud Director infrastructure levels — from VMware Cloud Director cells to separate vApps and VMs.

The following types of summary dashboards are available for VMware Cloud Director infrastructure objects:

- VMware Cloud Director Infrastructure Summary
- Provider VDCs Overview
- Provider VDC Summary
- Organizations Overview
- Organization Summary
- Organization VDC Summary
- vApp Summary
- Virtual Machine Summary

To access a summary dashboard for a VMware Cloud Director infrastructure object or segment:

1. Open Veeam ONE Client.

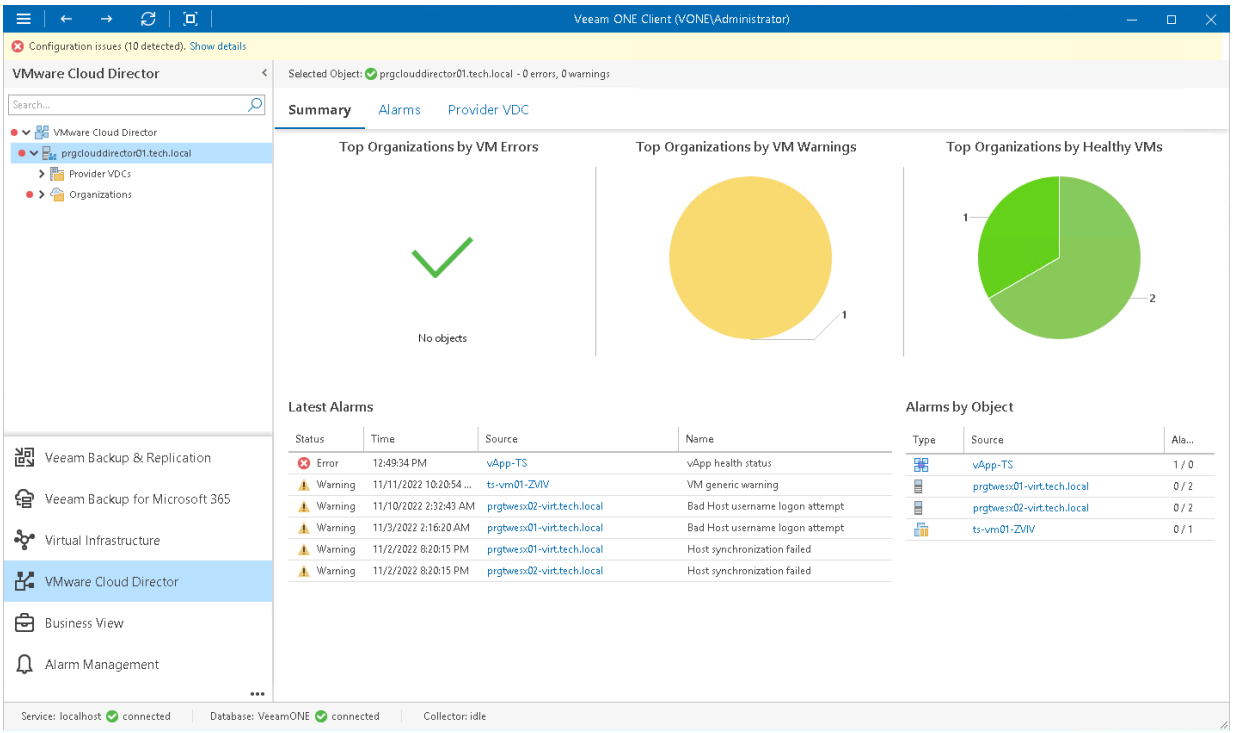
   For details, see Accessing Veeam ONE Components.
2. At the bottom of the inventory pane, click **VMware Cloud Director**.
3. In the inventory pane, select the necessary infrastructure object or segment.
4. Open the **Summary** tab.

VMware Cloud Director Infrastructure Summary

The VMware Cloud Director infrastructure summary dashboard provides the health status overview for all organizations and child VMware Cloud Director objects.

The dashboard is available for the following infrastructure levels:

- VMware Cloud Director Infrastructure (root node)
- VMware Cloud Director cell



Top Organizations by VM Errors, Top Organizations by VM Warnings, Top Organizations by Healthy VMs

The charts represent organizations with the greatest number of errors, warnings and organizations with no registered alarms. Click a chart segment or a legend label to drill down to the list of alarms with the corresponding status for the selected organization.

Latest Alarms

The list displays the latest 15 alarms for the selected VMware Cloud Director segment. Click a link in the **Source** column to drill down to the list of alarms triggered for a specific VMware Cloud Director infrastructure object.

Alarms by Object

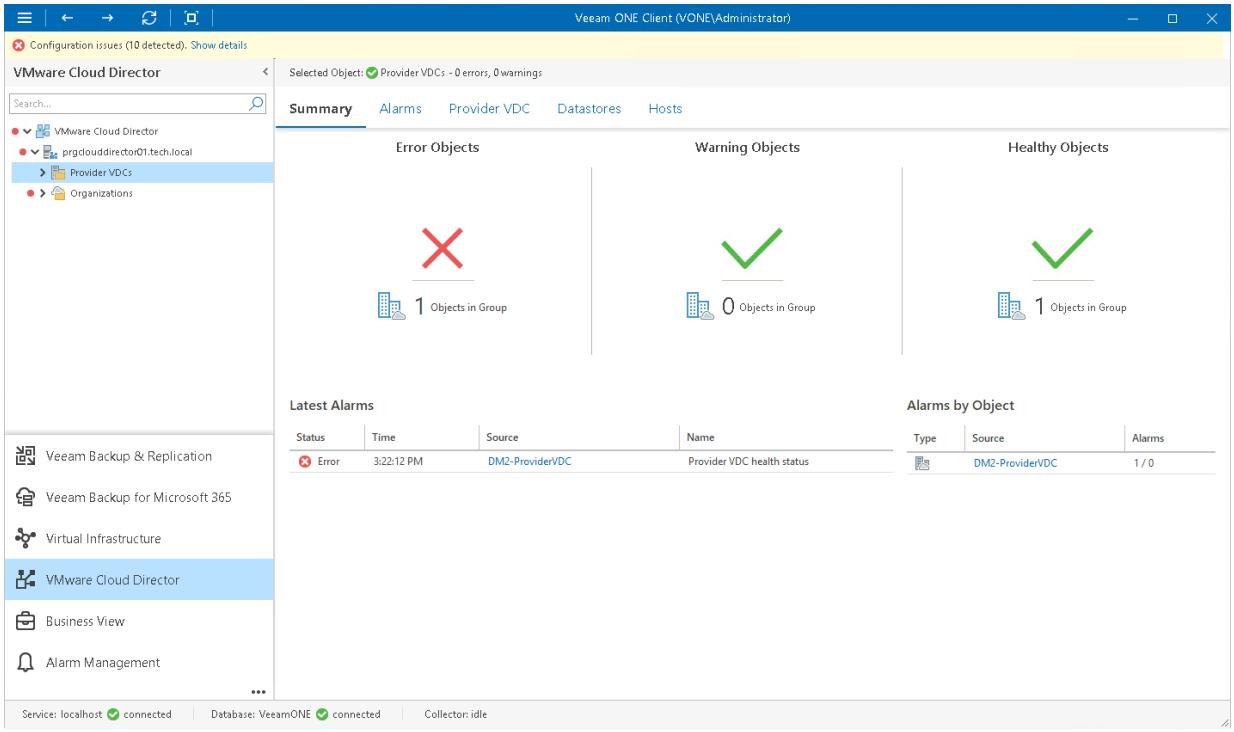
The list displays 15 objects with the greatest number of alarms.

The value in the **Alarms** column shows the number of errors and warnings for an object. For example, 3/1 means that there are 3 error alarms and 1 warning alarm triggered for the object. Click a link in the **Source** column to drill down to the list of alarms related to a specific VMware Cloud Director infrastructure object.

For details on alarms, see Working with Triggered Alarms.

Provider VDCs Overview

The summary dashboard for the **Provider VDCs** node displays the health status overview for provider virtual datacenters under a VMware Cloud Director cell.



Error Objects, Warning Objects, Healthy Objects

The charts group provider VDCs by their health status.

Every chart reflects the number of provider VDCs with a specific state — provider VDCs with errors (red), provider VDCs with warnings (yellow) and healthy provider VDCs (green). Click the problematic chart to drill down to the list of alarms for VDCs with the chosen health status.

Latest Alarms

The list displays the latest 15 alarms that were triggered for provider VDCs and underlying virtual infrastructure objects (datastores and hosts). Click a link in the **Source** column to drill down to the list of alarms triggered for a specific object.

Alarms by Object

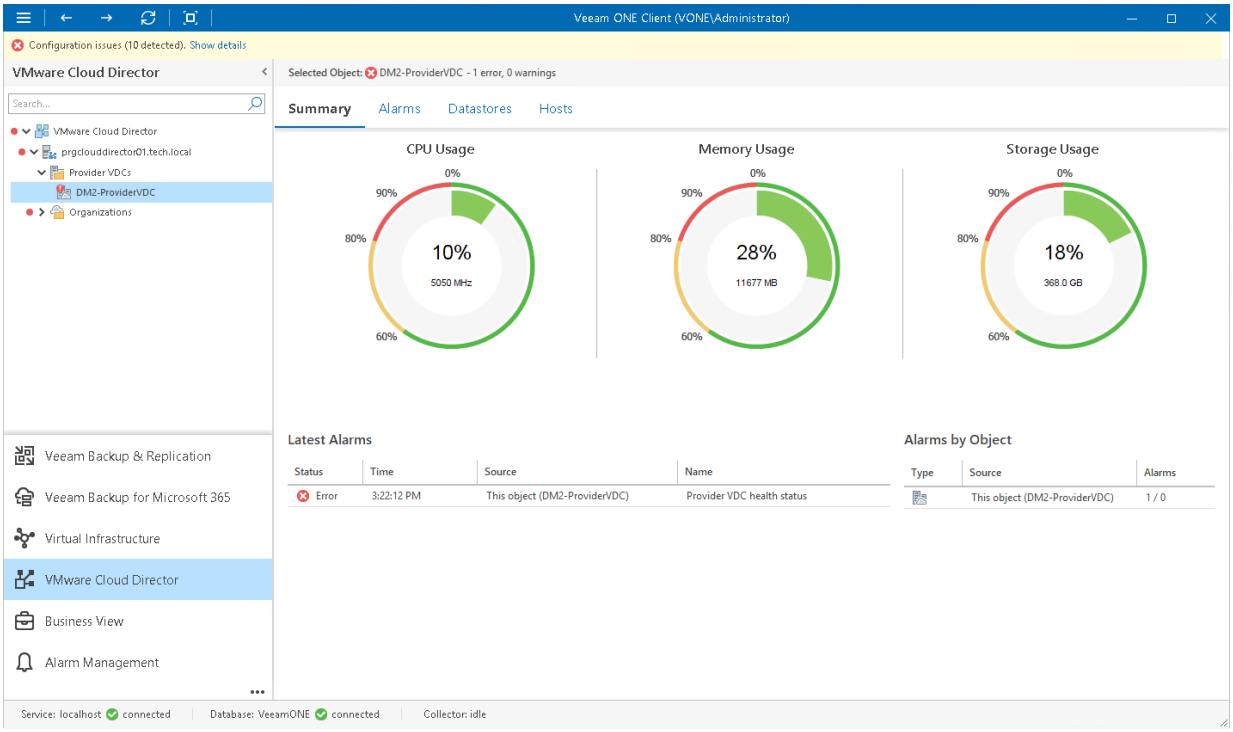
The list displays 15 objects with the greatest number of alarms.

The value in the **Alarms** column shows the number of errors and warnings for an object. For example, 3/1 means that there are 3 error alarms and 1 warning alarm triggered for the object. Click a link in the **Source** column to drill down to the list of alarms related to a specific object.

For details on alarms, see Working with Triggered Alarms.

Provider VDC Summary

The provider VDC summary dashboard reflects resource utilization analysis results and the health status overview for the chosen provider virtual datacenter and VMware vSphere resources.



CPU Usage, Memory Usage, Storage Usage

The charts reflect the amount of currently consumed CPU, memory and storage resources for the chosen provider virtual datacenter.

Latest Alarms

The list displays the latest 15 alarms for the provider VDC and underlying virtual infrastructure objects (datastores and hosts). Click a link in the **Source** column to drill down to the list of alarms triggered for a specific object.

Alarms by Object

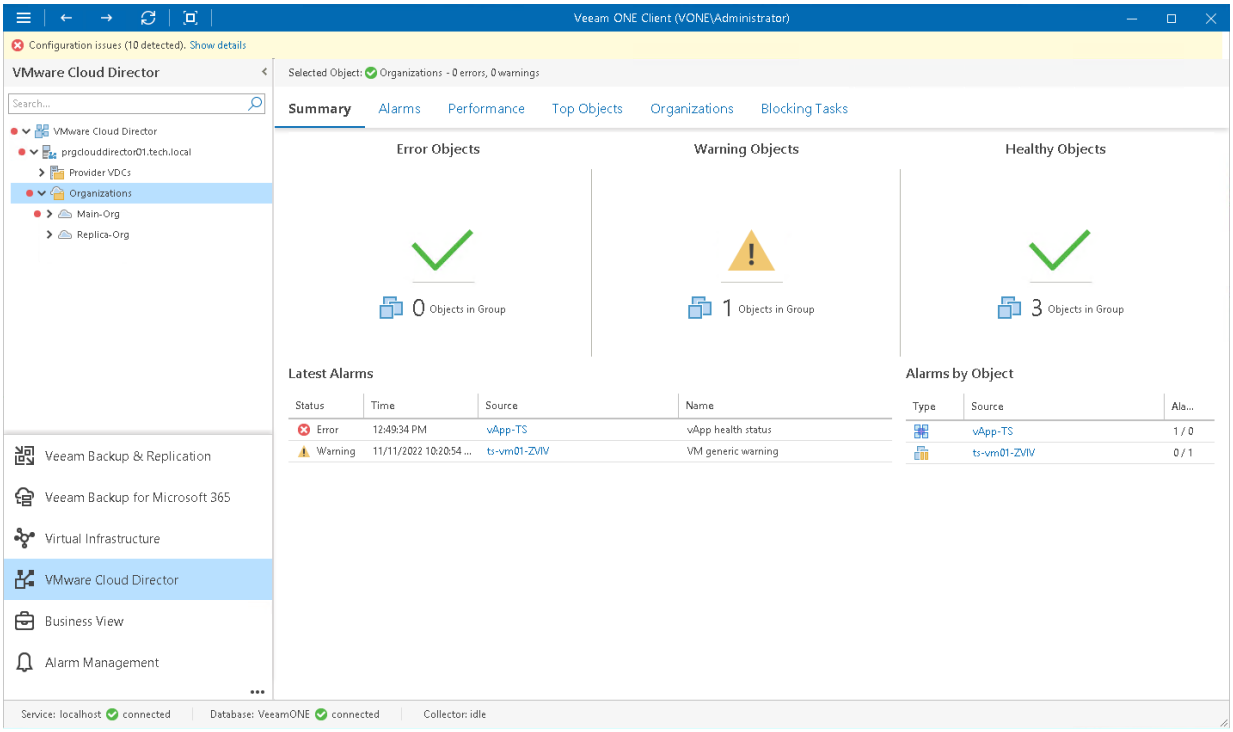
The section displays the current state of hosts and datastores that provide compute and storage resources for the provider VDC. Information in this section may help you estimate the impact of underlying VMware vSphere objects on the provider VDC and speed up root cause analysis.

The value in the **Alarms** column shows the number of errors and warnings for an object. For example, 3/1 means that there are 3 error alarms and 1 warning alarm triggered for the object. Click a link in the **Source** column to drill down to the list of alarms related to a specific object.

For details on alarms, see Working with Triggered Alarms.

Organizations Overview

The summary dashboard for the **Organizations** node provides an overview for organizations under the selected VMware Cloud Director cell.



Error Objects, Warning Objects, Healthy Objects

The charts group VMs in organizations by their health status.

Every chart reflects the number of organization VMs with a specific state — VMs with errors (red), VMs with warnings (yellow) and healthy VMs (green). Click the problematic chart to drill down to the list of alarms for VMs with the chosen health status.

Latest Alarms

The list displays the latest 15 alarms that were triggered for organizations, organization VDCs, as well as for VMs and vApps within these organizations. Click a link in the **Source** column to drill down to the list of alarms triggered for a specific object.

Alarms by Object

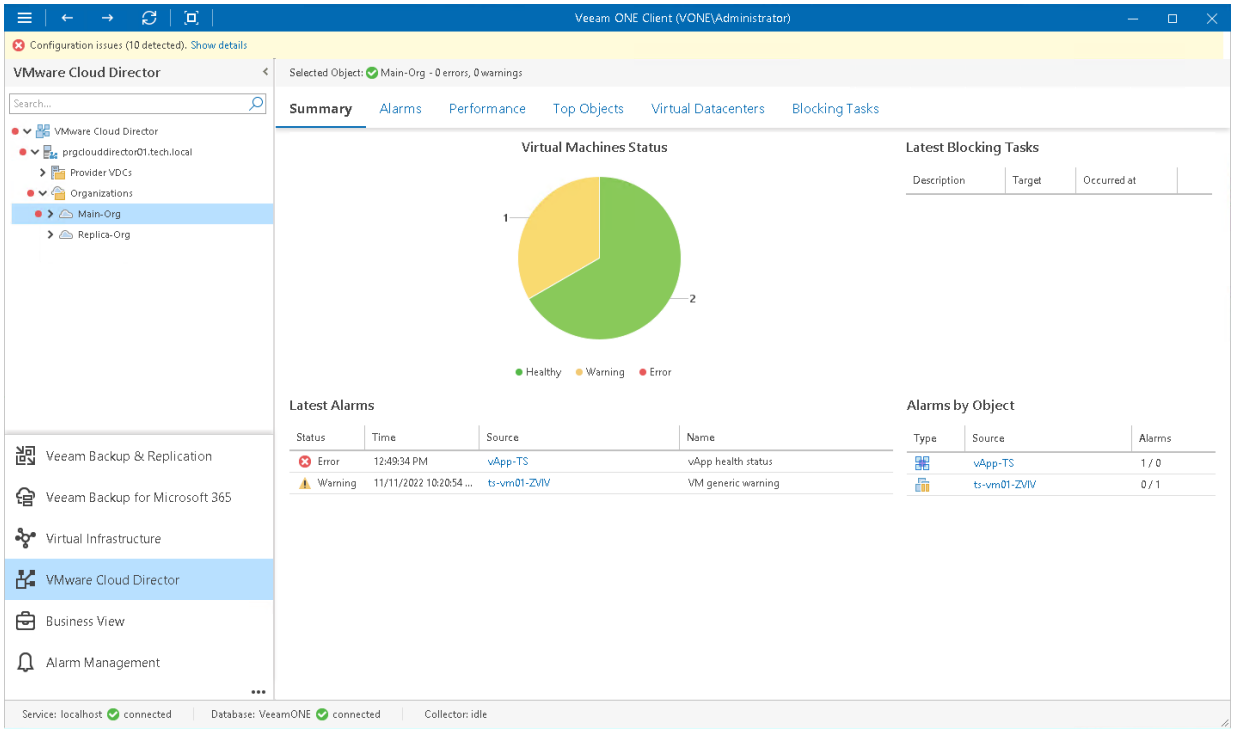
The list displays 15 objects with the greatest number of alarms.

The value in the **Alarms** column shows the number of errors and warnings for an object. For example, 3/1 means that there are 3 error alarms and 1 warning alarm triggered for the object. Click a link in the **Source** column to drill down to the list of alarms related to a specific object.

For details on alarms, see Working with Triggered Alarms.

Organization Summary

The organization summary dashboard presents the health status overview for the chosen organization and its child objects.



Virtual Machines by State

The chart reflects the summary health status of VMs in the organization.

Every colored segment represents the number of VMs in a certain state — VMs with errors (red), VMs with warnings (yellow) and healthy VMs (green). Click the chart segment or a legend label to drill down to the list of alarms triggered for organization VMs with the chosen health status.

Latest Blocking Tasks

The list displays the latest 15 suspended operations that require approval before the operation will resume.

For each pending operation, Veeam ONE Client provides a description, the organization for which the operation was initiated and the time when the operation was initiated by an organization user. Blocking tasks that expired with timeout are not included in the list.

Latest Alarms

The list displays the latest 15 alarms for the organizations, organization VDCs, as well as for VMs and vApps within these organizations. Click a link in the **Source** column to drill down to the list of alarms triggered for a specific object.

Alarms by Object

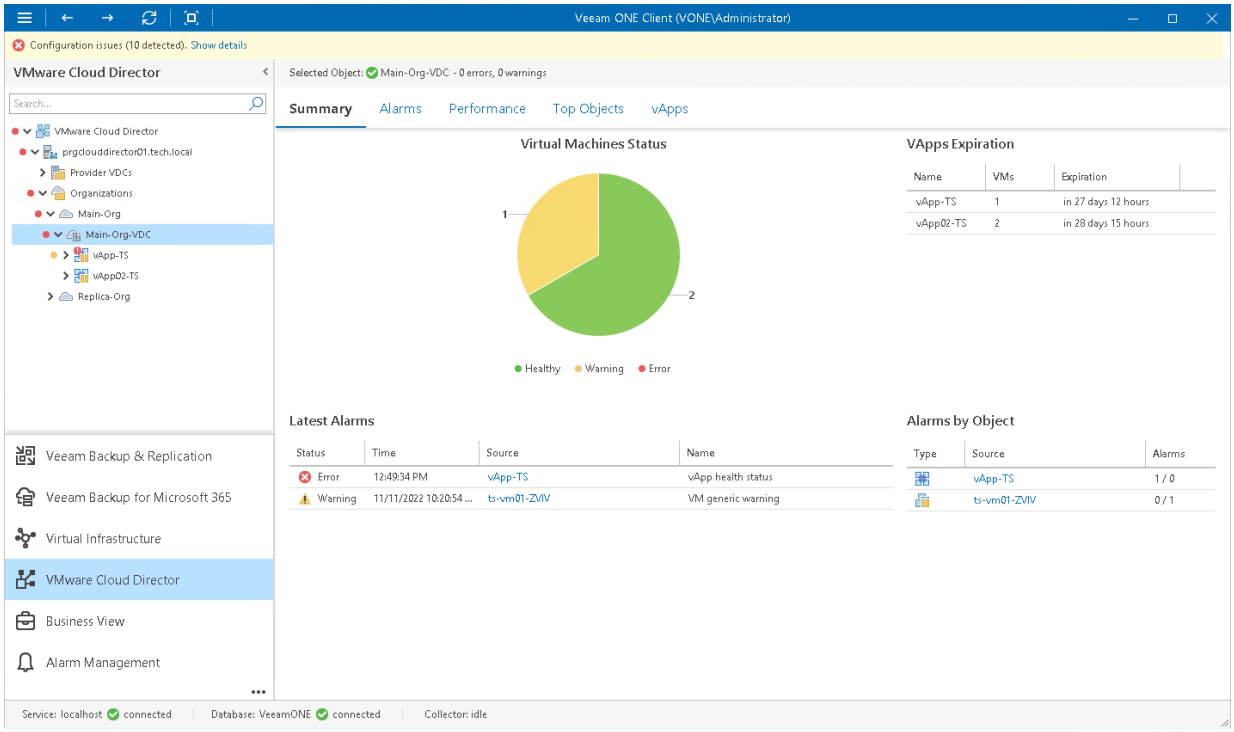
The list displays 15 objects with the greatest number of alarms.

The value in the **Alarms** column shows the number of errors and warnings for an object. For example, 3/1 means that there are 3 error alarms and 1 warning alarm triggered for the object. Click a link in the **Source** column to drill down to the list of alarms related to a specific object.

For details on alarms, see Working with Triggered Alarms.

Organization VDC Summary

The organization VDC summary dashboard presents resource utilization analysis and the health status overview for the chosen organization virtual datacenter.



Virtual Machines by State

The chart reflects the summary health status of VMs in the organization virtual datacenter.

Every colored segment represents the number of VMs in a certain state — VMs with errors (red), VMs with warnings (yellow) and healthy VMs (green). Click a chart segment or legend label to drill down to the list of alarms triggered for VMs with the chosen health status.

VApps Expiration

The list displays vApps whose runtime lease or storage lease has expired. The list shows 15 items with the recently expired lease, and is only populated if the storage lease cleanup policy for the organization is set to **Move to Expired Items**.

Latest Alarms

The list displays the latest 15 alarms for the organization VDC and its child objects (vApps and VMs). Click a link in the **Source** column to drill down to the list of alarms triggered for a specific object.

Alarms by Object

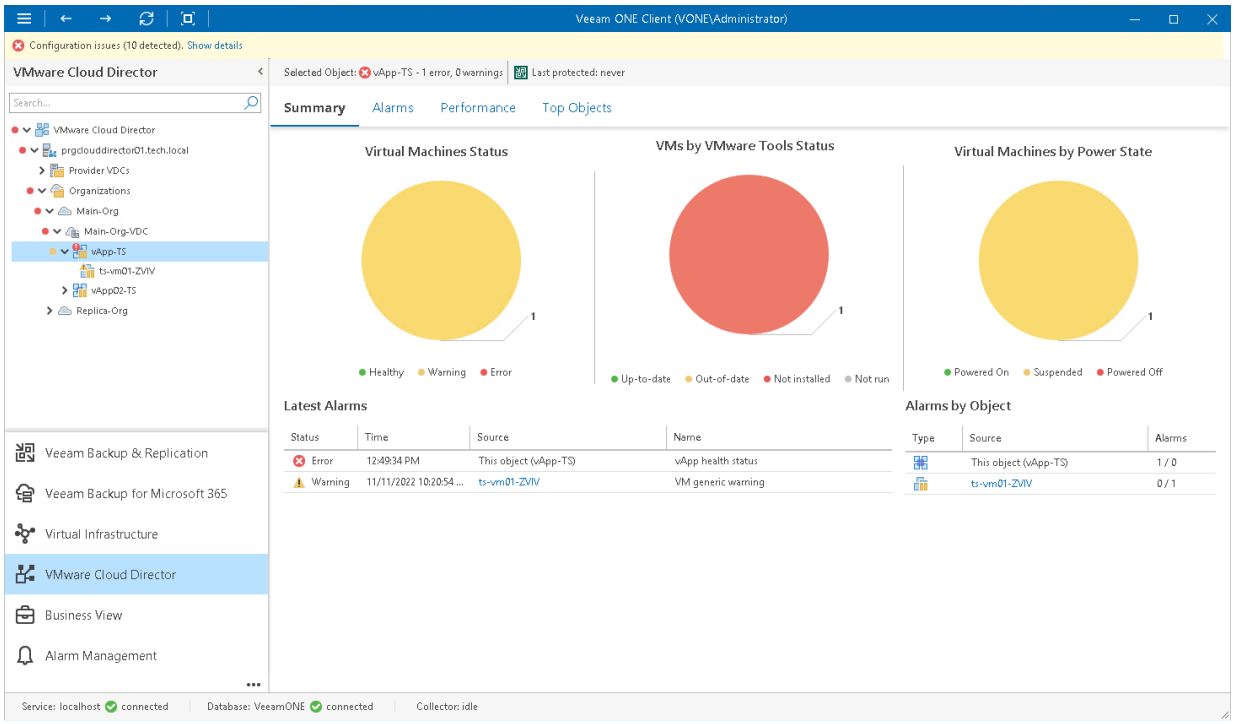
The list displays 15 objects with the greatest number of alarms.

The value in the **Alarms** column shows the number of errors and warnings for an object. For example, 3/1 means that there are 3 error alarms and 1 warning alarm triggered for the object. Click a link in the **Source** column to drill down to the list of alarms related to a specific object.

For details on alarms, see Working with Triggered Alarms.

vApp Summary

The vApp summary dashboard provides a health status overview for the chosen vApp and VMs in this vApp.



Virtual Machines by State

The chart groups VMs in the vApp by health status.

Every colored segment represents the number of VMs in a certain state — VMs with errors (red), VMs with warnings (yellow) and healthy VMs (green). Click a chart segment or a legend label to drill down to the list of alarms triggered for VMs with the chosen health status.

VMs by VMware Tools Status

The chart groups VMs in the vApp by VMware Tools status.

Every colored segment reflects the number of VMs with a specific state — VMware Tools not installed (red), VMware Tools need to be updated to the latest version (yellow), VMware Tools up-to-date and running (green) and VMware Tools installed but not running for some reason (grey).

Virtual Machines by Power State

The chart groups VMs in the vApp by power state. Every colored segment reflects the number of VMs with a specific power state — powered off VMs (red), suspended VMs (yellow) and powered on VMs (green).

Latest Alarms

The list displays the latest 15 alarms triggered for the vApp and VMs that belong to it. Click a link in the **Source** column to drill down to the list of alarms triggered for a specific object.

Alarms by Object

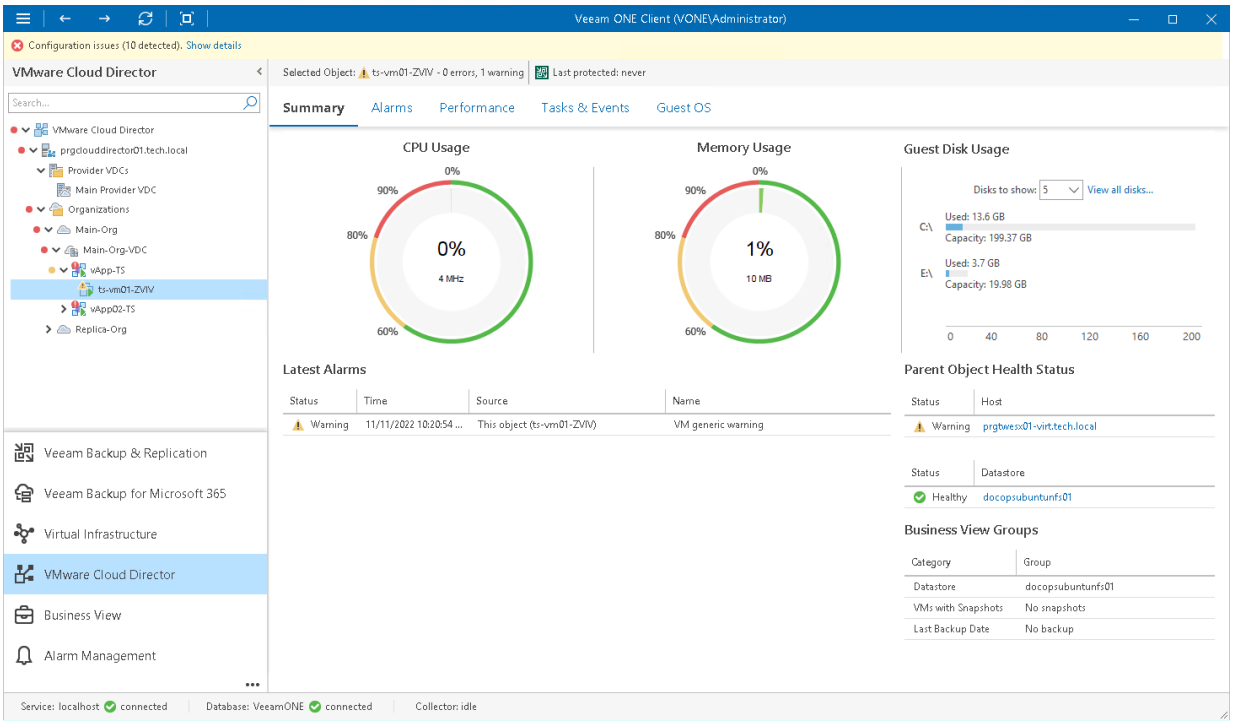
The list displays 15 objects with the greatest number of alarms.

The value in the **Alarms** column shows the number of errors and warnings for an object. For example, 3/1 means that there are 3 error alarms and 1 warning alarm triggered for the object. Click a link in the **Source** column to drill down to the list of alarms related to a specific object.

For details on alarms, see Working with Triggered Alarms.

Virtual Machine Summary

The VM summary dashboard provides the health status and performance overview for the selected VM. In addition, this dashboard shows the state of objects that can affect the VM performance — the parent host and the datastores where VM files are located.



Selected Object

The section at the top of the dashboard shows the VM health status (number of triggered warnings and errors) and the date when the latest backup or replica restore point was created for the VM with Veeam Backup & Replication.

CPU Usage, Memory Usage

The charts display the amount of CPU and memory resources currently consumed by the VM.

Guest Disk Usage

The chart displays the amount of available and used guest disk space with a breakdown by disks. By default, 5 guest disks with the greatest amount of used space are displayed.

Use the **Disks to show** list to change the number of disks to display on the chart. Click the **View all disks** link to view details for all guest disks. In the **Guests Disks** window, you can suppress *Guest disk space* alarms for specific disks. To suppress alarms for a disk, select the **Suppress alarms** check boxes next to the disk name.

> **NOTE:**
>
> Details on the guest disk usage are available only for VMs with VMware Tools installed.

Latest Alarms

The list displays the latest 15 alarms for the VM.

Parent Object Health Status

The section displays the current state of the host where the VM resides and the state of datastores that host VMs files. Information available in this section may help you estimate how the state of parent objects impacts VM performance. Click the host or datastore link to drill down to the list of alarms for the host or datastore.

For details on alarms, see Working with Triggered Alarms.

Business View Groups

The section displays the list of categories and groups to which the VM is included.

VMware Cloud Director Alarms

Veeam ONE includes a set of alarms for monitoring VMware Cloud Director health status and resource usage. Predefined VMware Cloud Director alarms are configured to warn you about events or issues that can cause disruptions in cloud service availability:

- Expiring runtime and storage leases for customers' vApps
- Pending blocking tasks left without timely response
- Breached thresholds for compute, storage and network resource utilization at various layers of the VMware Cloud Director infrastructure
- Changes in health status of VMware Cloud Director components

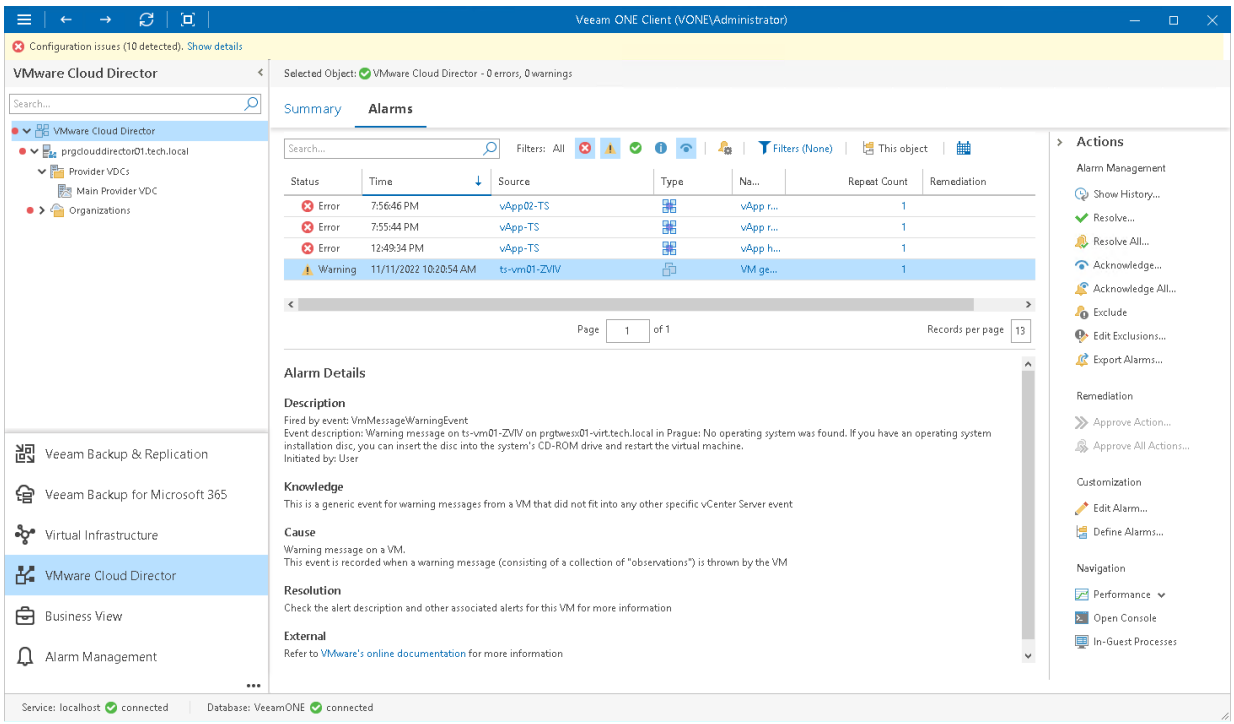
To view the list of alarms for VMware Cloud Director infrastructure:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.
2. At the bottom of the inventory pane, click **VMware Cloud Director**.
3. In the inventory pane, select the necessary infrastructure node.
4. Open the **Alarms** tab.

In addition to Cloud Director-specific alarms, the dashboard displays alarms triggered for VMware vSphere infrastructure components. Thus you can monitor both the logical cloud layer and the state of underlying VMware vSphere infrastructure components.

For details on alarms, see Working with Triggered Alarms.



VMware Cloud Director Performance Charts

To facilitate the troubleshooting process and quickly identify resource bottlenecks, you can drill down to performance charts right from the VMware Cloud Director view:

- Overview
- CPU Performance Chart
- Memory Performance Chart
- Datastore Performance Chart
- Network Performance Chart
- Virtual Disks Performance Chart

You can track performance metrics for separate VMs within an organization, for a VM container (such as vApp, organization or organization VDC) and for hosts that support provider VDCs.

To drill down to a performance chart from the VMware Cloud Director view, do one of the following:

- In the VMware Cloud Director inventory, select an infrastructure object (VM or VM container) and go to the necessary performance chart tab in the information pane.
- Open the **Alarms** dashboard. In the list of alarms, select an alarm for the necessary VM or host. Click **Performance** in the **Actions** pane on the right and choose the required performance chart.
- Open the **Alarms** dashboard. In the list of alarms, select an alarm for the necessary VM or host. Right-click the alarm, choose **Performance** and select necessary performance chart from the shortcut menu.

> **NOTE:**
>
> When you open a performance chart for a host, Veeam ONE Client automatically switches to the Virtual Infrastructure.

For performance charts in the VMware Cloud Director view, Veeam ONE supports a similar set of actions as for virtual infrastructure performance charts: you can change chart views and set time intervals, define objects to show on charts or select custom metrics. For details on customizing performance charts, see Customizing VMware vSphere Performance Charts.

VMware Cloud Director Resources

Veeam ONE Client includes a set of dashboards for monitoring resource allocation and utilization at the VMware Cloud Director infrastructure and service layers. These dashboards help you compare VMware Cloud Director capacities to the current level of resource usage and estimate the size of virtual datacenter capacities required to maintain customer workloads.

Provider VDCs

You can view a list of provider virtual datacenters configured within a Cloud Director cell:

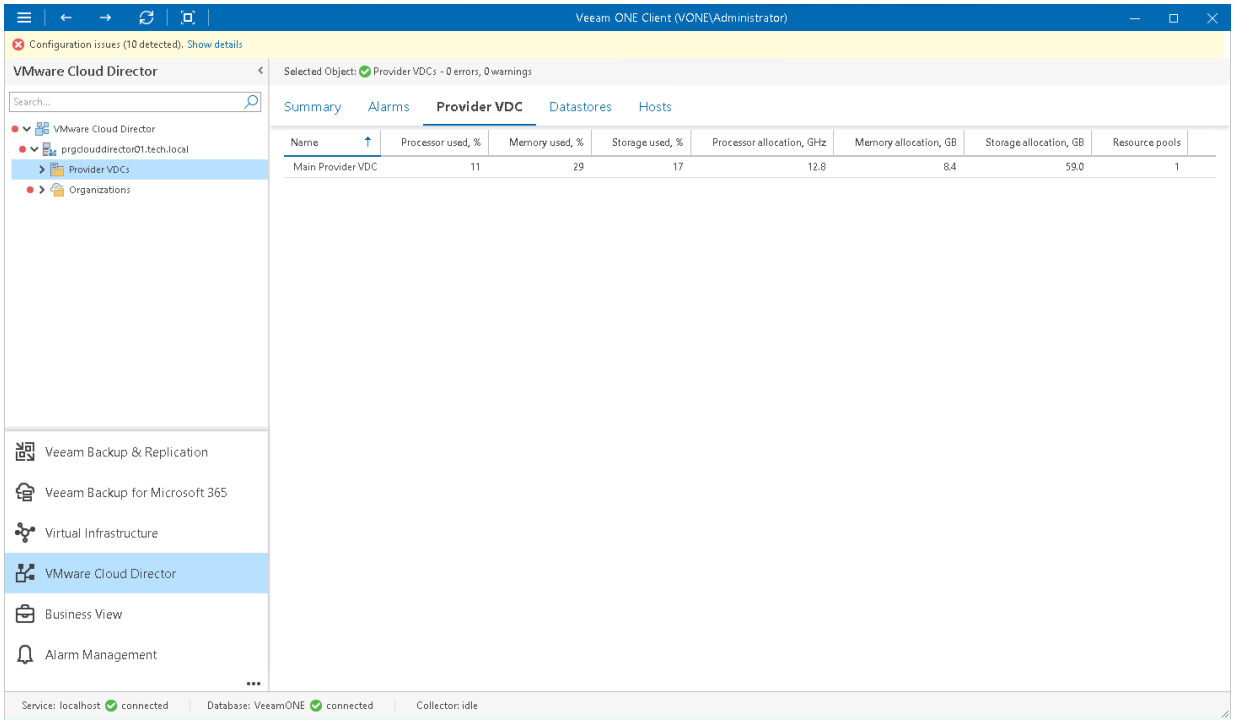
1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click **VMware Cloud Director**.

3. In the inventory pane, select a VMware Cloud Director cell or the **Provider VDCs** node.

4. Open the **Provider VDC** tab.



For every provider VDC in the list, the following details are shown:

- **Name** — name of the provider virtual datacenter
- **Processor used, %** — amount of provider VDC CPU resources that is currently used by organizations
- **Memory used, %** — amount of provider VDC memory resources that is currently used by organizations
- **Storage used, %** — amount of provider VDC storage resources that is currently used by organizations
- **Processor allocation, GHz** — amount of provider VDC CPU resources that is committed to organization VDCs
- **Memory allocation, GB** — amount of provider VDC memory resources that is committed to organization VDCs
- **Storage allocation, GB** — amount of provider VDC storage resources that is committed to organization VDCs
- **Resource pools** — number of resource pools that are backing compute resources of the provider VDC

You can click column names to sort provider VDCs by a specific parameter. For example, to identify what provider VDCs are running out of storage resources, you can sort provider VDCs in the list by **Storage used, %**.

Datastore Resources

You can view a list of datastores attached to provider virtual datacenters:

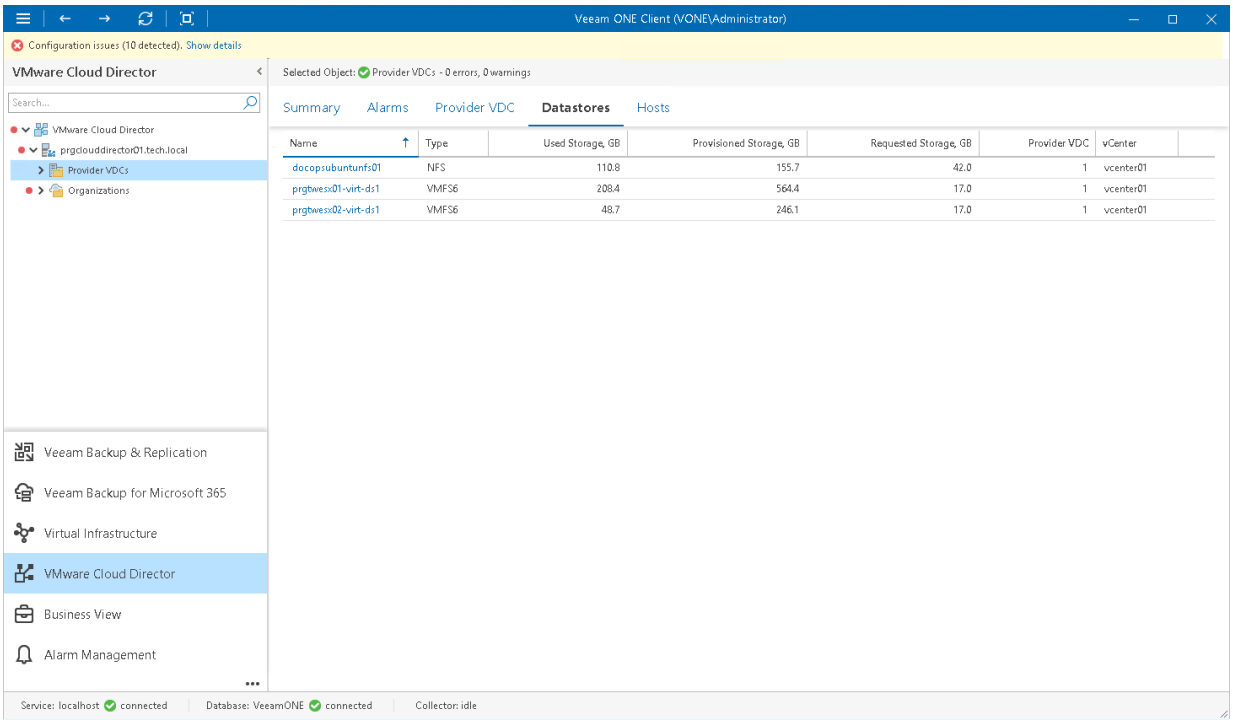
1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click **VMware Cloud Director**.

3. In the inventory pane, select a provider VDC node to view datastores attached to this provider VDC. Select the **Provider VDCs** node to view datastores attached to all provider VDCs within the VMware Cloud Director cell.

4. Open the **Datastores** tab.



For every datastore in the list, the following details are shown:

- **Name** – name of the datastore (you can click the name to switch to the summary dashboard for the datastore)
- **Type** – datastore file system (*VMFS* or *NFS*)
- **Used Storage, GB** – amount of storage resources currently consumed on the datastore
- **Provisioned Storage, GB** – amount of space provisioned to VMs. If VMs are created using thin provisioning, some of the provisioned space might not be used
- **Requested Storage, GB** – amount of provisioned storage used by Cloud Director-managed objects. If thin provisioning is enabled on Cloud Director, some of the requested space might not be used
- **Provider VDC** – number of provider VDCs to which the datastore is attached
- **vCenter** – name of the vCenter Server that manages the datastore

Host Resources

You can view a list of hosts that are backing a provider virtual datacenter:

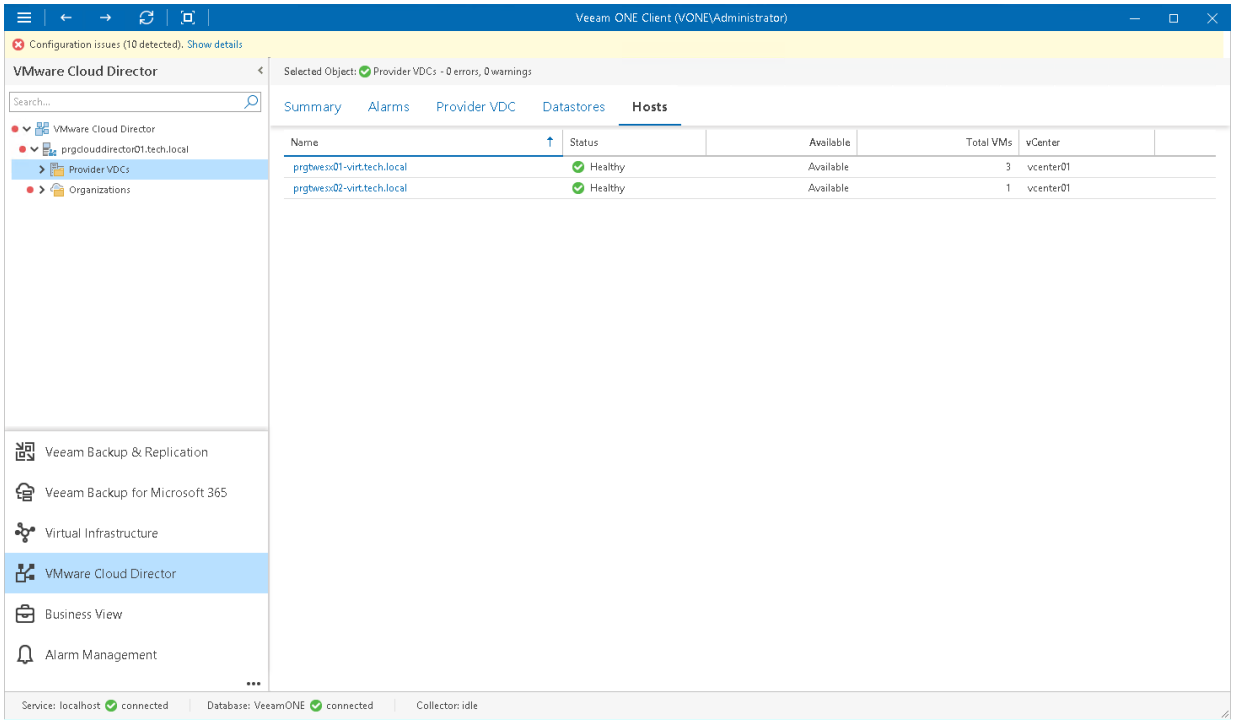
1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click **VMware Cloud Director**.

3. In the inventory pane, select a provider VDC node.

4. Open the **Hosts** tab.



For every host in the list, the following details are shown:

- **Name** – name of the host (you can click the name to switch to the summary dashboard for the host)
- **Status** – health status of the host (*Healthy*, *Warning* or *Error*)
- **Available** – flag indicating whether the host is available to VMware Cloud Director
- **Total VMs** – number of VMs currently registered on the host
- **vCenter** – name of the vCenter Server that manages the host

Organizations

You can view a list of organizations within the VMware Cloud Director cell:

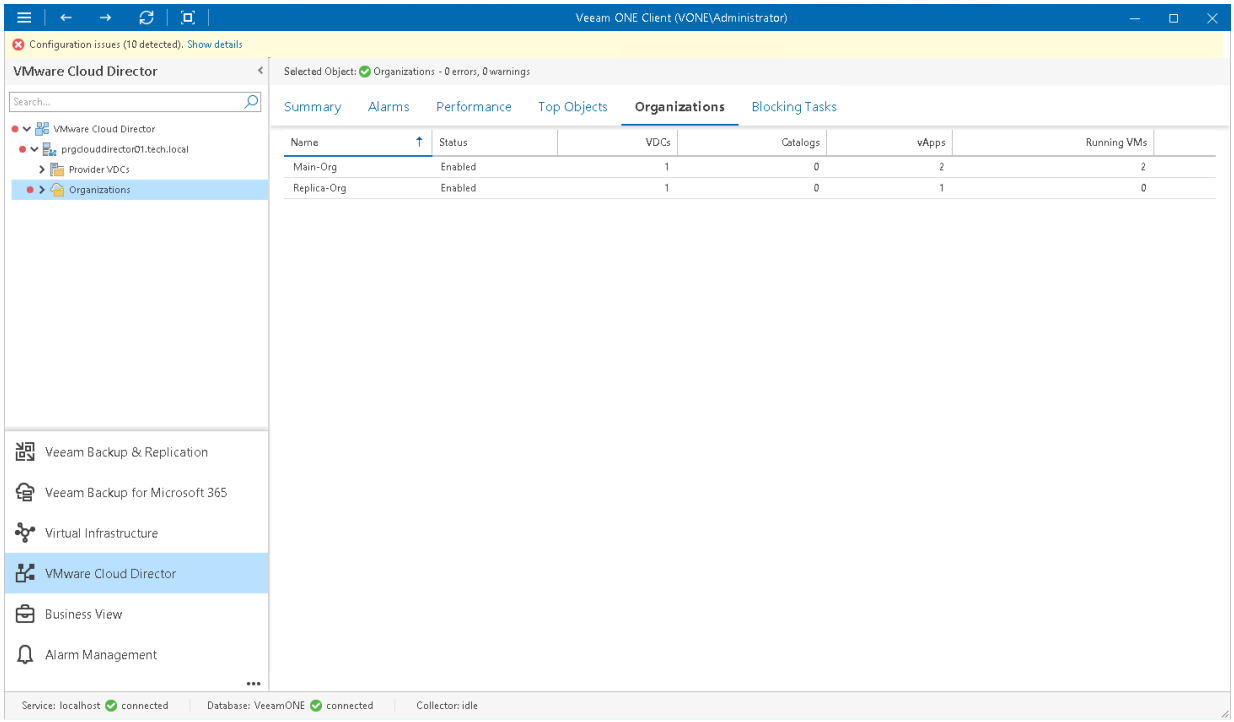
1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click **VMware Cloud Director**.

3. In the inventory pane, select the **Organizations** node.

4. Open the **Organizations** tab.



For every organization in the list, the following details are shown:

- **Name** – name of the organization
- **Status** – status of the organization indicating whether the organization is enabled (that is, users can log in to the organization and the current user sessions can run)
- **VDCs** – number of virtual datacenters configured for the organization
- **Catalogs** – number of organization's catalogs, both shared and non-shared
- **vApps** – number of vApps configured for the organization (including expired vApps)
- **Running VMs** – number of VMs currently running within this organization

Organization VDCs

You can view a list of VDCs configured for a specific organization:

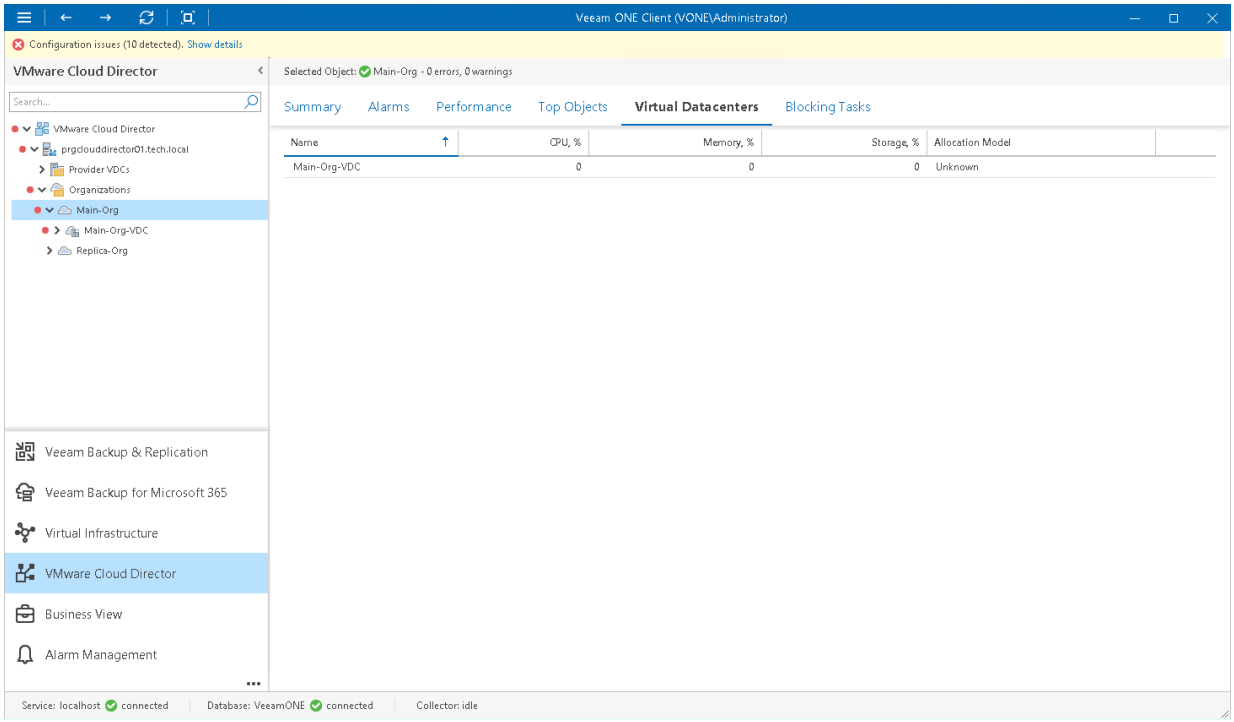
1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click **VMware Cloud Director**.

3. In the inventory pane, select an organization node.

4. Open the **Virtual Datacenters** tab.



For every virtual datacenter in the list, the following details are shown:

- **Name** — name of the organization VDC
- **CPU, %** — amount of CPU resources currently used by the organization (as a percentage of resources allocated to the organization within this virtual datacenter)
- **Memory, %** — amount of memory resources currently used by the organization (as a percentage of resources allocated to the organization within this virtual datacenter)
- **Storage, %** — amount of storage resources currently used by the organization (as a percentage of resources allocated to the organization within this virtual datacenter)
- **Allocation Model** — allocation model for the virtual datacenter (*Allocation Pool*, *Reservation Pool*, *Pay-as-you-go*, *Flex*)

vApps

You can view a list of virtual applications created within a specific organization VDC:

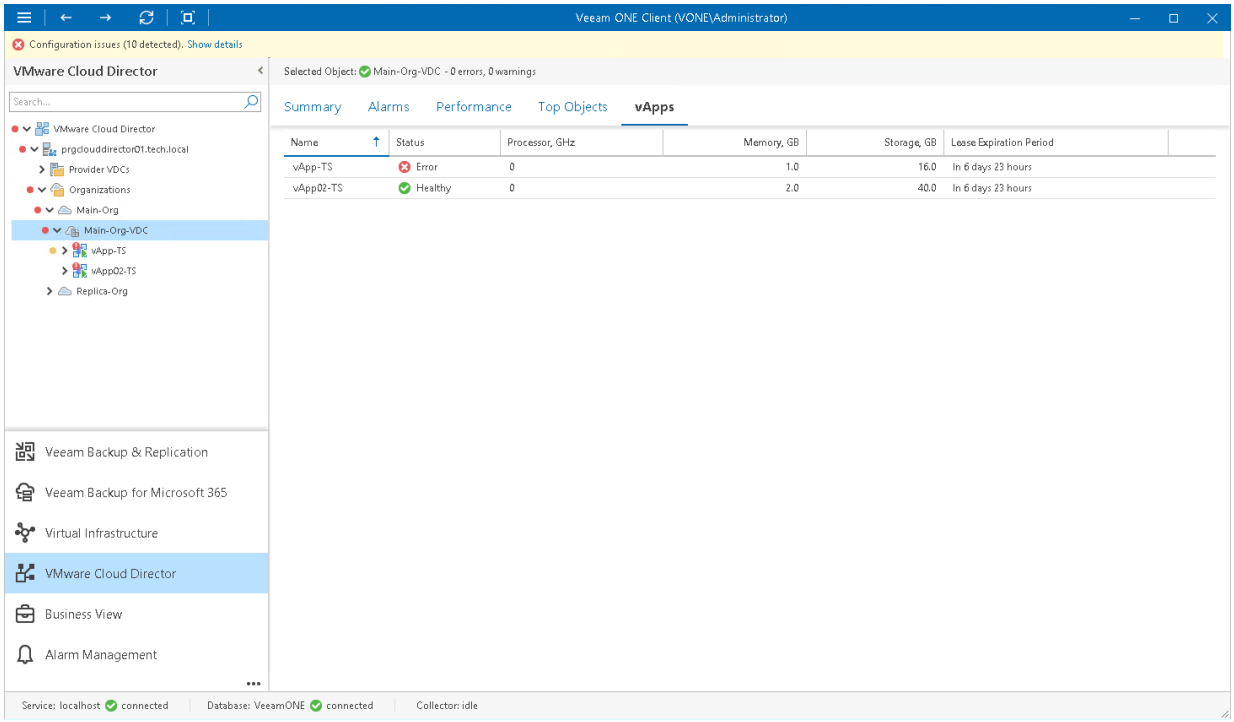
1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click **VMware Cloud Director**.

3. In the inventory pane, select an organization VDC node.

4. Open the **vApps** tab.



For every vApp in the list, the following details are shown:

- **Name** – name of the vApp
- **Status** – health status of the vApp
- **Processor, GHz** – amount of CPU resources currently consumed by the vApp and all its VMs
- **Memory, GB** – amount of memory resources currently consumed by the vApp and all its VMs
- **Storage, GB** – amount of storage resources currently consumed by the vApp and all its VMs
- **Lease Expiration Period** – amount of time left before the vApp runtime lease expires (for running vApps), or amount of time left before the vApp storage lease expires (for inactive vApps and templates)

Tracking Blocking Tasks

You can track pending blocking task requests for a specific organization or all organizations at once:

1. Open Veeam ONE Client.

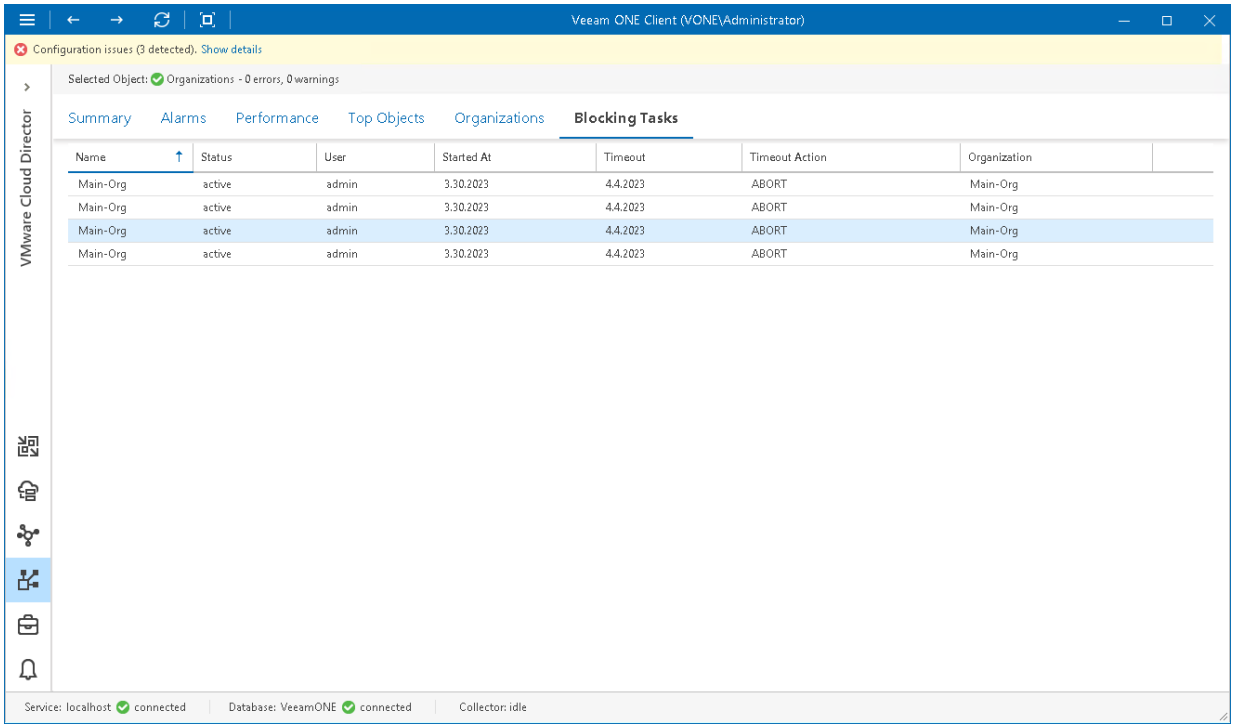
   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click **VMware Cloud Director**.

3. In the inventory pane, select an organization node to view blocking tasks pending for this organization.

   Select the **Organizations** node to view blocking tasks pending for all organizations within this VMware Cloud Director cell.

4. Open the **Blocking Tasks** tab.



For every blocking task in the list, the following details are shown:

- **Name** – name of the organization
- **Status** – current status of the blocking task
- **User** – name of the user who initiated the task
- **Started At** – date and time when the task was initiated
- **Timeout** – default timeout set for blocking tasks
- **Timeout Action** – the action that will be triggered upon the task after the timeout expires
- **Organization** – name of the organization

Troubleshooting Virtual Machine Performance

Veeam ONE Client includes a set of dashboards that give you enhanced control over VMs provisioned in the VMware Cloud Director environment, and help you facilitate the troubleshooting process:

- **Top VMs** dashboard displays the top resource consumers for CPU, memory, datastore, network usage, snapshot size and snapshot age.

  To view VMs that consume the greatest amount of compute, network and storage resources, select the necessary VM container in the inventory pane and go to the **Top VMs** tab. For more information, see VMware vSphere Top and Lowest Load.

- **Tasks & Events** dashboard shows VMware vSphere tasks and events targeted at a specific VM.

  To view the list of tasks and events for a VM, select it in the inventory pane and go to the **Tasks & Events** tab. For more information, see VMware vSphere Tasks & Events.

- **Processes** dashboard provides control over processes currently running inside the guest OS of a VM. You can view, end and restart processes on Windows- based machines. You can also view and end daemons on Linux-based machines.

  To view the list of processes, select the necessary VM in the inventory pane and go to the **Processes** tab. For more information, see VMware vSphere In-Guest Processes.

- **Services** dashboard provides control over services currently running inside the guest OS of a VM. You can view, start, stop and restart services on VMs. For Windows-based machines, you can also create alarms based on the service state or object performance.

  To view the list of processes, select the necessary VM in the inventory pane and go to the **Services** tab. For more information, see VMware vSphere In-Guest Services.

- **Console** dashboard lists running in-guest processes and helps you diagnose problems related to a specific service, module or application.

  To access a VM console, select the necessary VM in the inventory pane and go to the **Console** tab. For more information, see VMware vSphere VM Console.

Hyper-V Monitoring

Veeam ONE offers a variety of tools for monitoring the Microsoft Hyper-V environment from any perspective and with any level of detail.

With Veeam ONE Client, you can:

1. Monitor health status of the virtual environment.
   - Start with the **Summary** dashboards to check the overall health status of the virtual environment and reveal hotspots.

     Quickly review the state of virtual infrastructure components, see the latest alarms, detect the most problematic objects and drill down to the problem source for further investigation.
   - Use the **Virtual Machines** dashboard to view the list of VMs in a virtual infrastructure container and check additional details for every VM — such as VM current status, parent host, IP address, DNS name and the amount of resources currently consumed by the VM.
   - Use the **Top Objects** dashboard to detect the most and less loaded components in the virtual environment.

     Detect what virtual infrastructure objects are consuming the most and the least amount of CPU, memory, disk, network, and swap resources, or select additional counters to detect resource consumers in other areas.
2. View triggered alarms.

   Switch to the **Alarms** dashboard to see details on breached thresholds, events and problems that occurred in the virtual environment.

   Use the **Actions** pane on the alarms dashboard to detect root causes — drill down to performance charts, open VM console or view the list of in-guest processes.
3. Work with performance charts and track events.

   Drill down to performance charts to diagnose performance problems. You can change predefined views, quickly switch between charts and view events that occur in your environment to get all-round statistics.
4. Investigate problems from within the guest OS.

   Open VM console or view the list of running in-guest processes to diagnose problems related to a specific service, module or application.

Prerequisites

Before you start monitoring your virtual environment, make sure you have configured connections to virtual servers from which Veeam ONE will collect data. For details on configuring server connections, see Connecting Microsoft Hyper-V Servers.

Microsoft Hyper-V Summary Dashboards

Microsoft Hyper-V infrastructure summary dashboards serve as the starting point for monitoring and troubleshooting. Summary dashboards reflect the health status of the selected infrastructure object or infrastructure segment.

The following types of summary dashboards are available for virtual infrastructure objects:

- Microsoft Hyper-V Infrastructure Summary
- Host Summary
- Virtual Machine Summary
- Local Storage Summary
- SMB Share Summary
- Cluster Shared Volume Summary

To access a summary dashboard for a virtual infrastructure object or virtual infrastructure segment:

1. Open Veeam ONE Client.

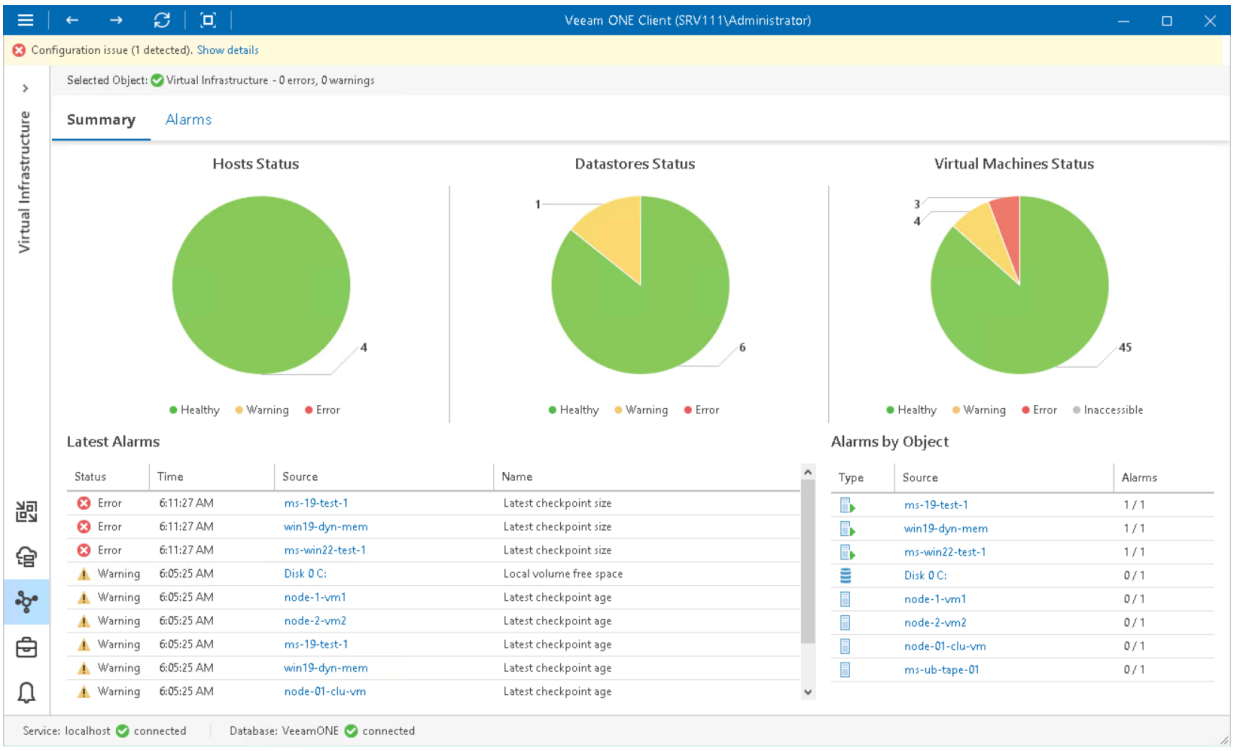
   For details, see Accessing Veeam ONE Components.
2. At the bottom of the inventory pane, click **Virtual Infrastructure**.
3. In the inventory pane, select the necessary infrastructure object or segment.
4. Open the **Summary** tab.

Microsoft Hyper-V Infrastructure Summary

The Hyper-V infrastructure summary dashboard provides the health status overview for the selected virtual environment segment.

The dashboard is available for the following infrastructure levels:

- Virtual infrastructure (root node)
- Virtual infrastructure container (such as SCVMM, cluster or storage container)



Hosts Status, Datastores Status, Virtual Machines Status

The charts reflect the status of virtual infrastructure objects.

Every chart segment represents the number of objects with a certain status — objects with errors (red), objects with warnings (yellow) and healthy objects (green). Click a chart segment or a legend label to drill down to the list of alarms with the corresponding status for the selected type of virtual infrastructure objects.

Latest Alarms

The list displays the latest 15 alarms that were triggered for objects in the selected virtual environment segment. Click a link in the **Source** column to drill down to the list of alarms triggered for a specific virtual infrastructure object.

Alarms by Object

The list displays 15 objects with the highest number of alarms.

The value in the **Alarms** column shows the number of errors and warnings for an object. For example, 3/1 means that there are 3 error alarms and 1 warning alarm triggered for the object. Click a link in the **Source** column to drill down to the list of alarms related to a specific virtual infrastructure object.

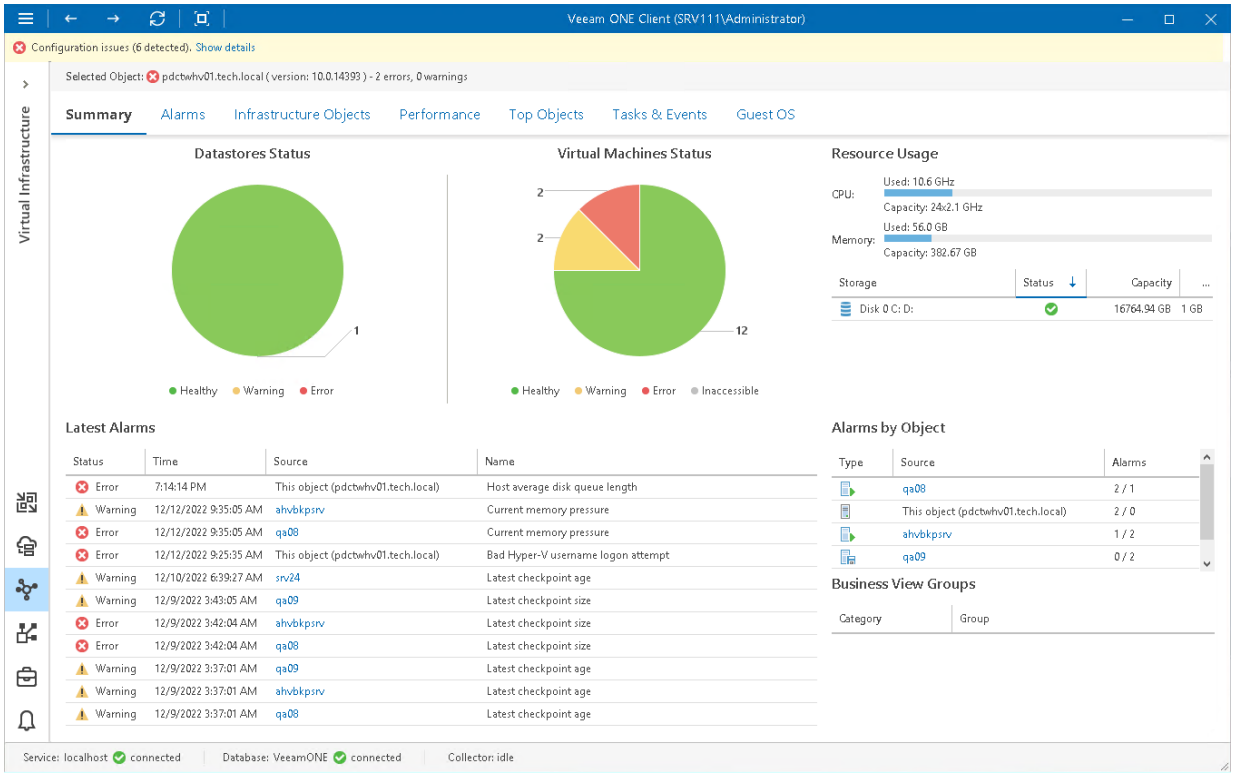
For more information, see Working with Triggered Alarms.

Business View Groups

The section displays the list of categories and groups to which the cluster is included.

Host Summary

The host summary dashboard provides the health status and performance overview for the selected Microsoft Hyper-V host and its child objects.



Datastores Status, Virtual Machines Status

The charts reflect the status of volumes connected to the host and the status of VMs running on the host.

Every chart segment represents the number of objects with a certain status — objects with errors (red), objects with warnings (yellow) and healthy objects (green). Click a chart segment or a legend label to drill down to the list of alarms with the corresponding status for host child objects.

Resource Usage

The section displays capacity and usage summary for host CPU and memory. It also shows an overview for volumes connected to the host — state of the volume, its capacity and the amount of free space on the volume.

Latest Alarms

The list displays the latest 15 alarms triggered for the host and its child objects. Click a link in the **Source** column to drill down to the list of alarms for the host and its child objects.

Alarms by Object

The list displays 15 objects with the greatest number of alarms (including the host and its child objects).

The value in the **Alarms** column shows the number of errors and warnings for an object. For example, 3/1 means that there are 3 error alarms and 1 warning alarm triggered for the object. Click a link in the **Source** column to drill down to the list of alarms related to the host and its child objects.

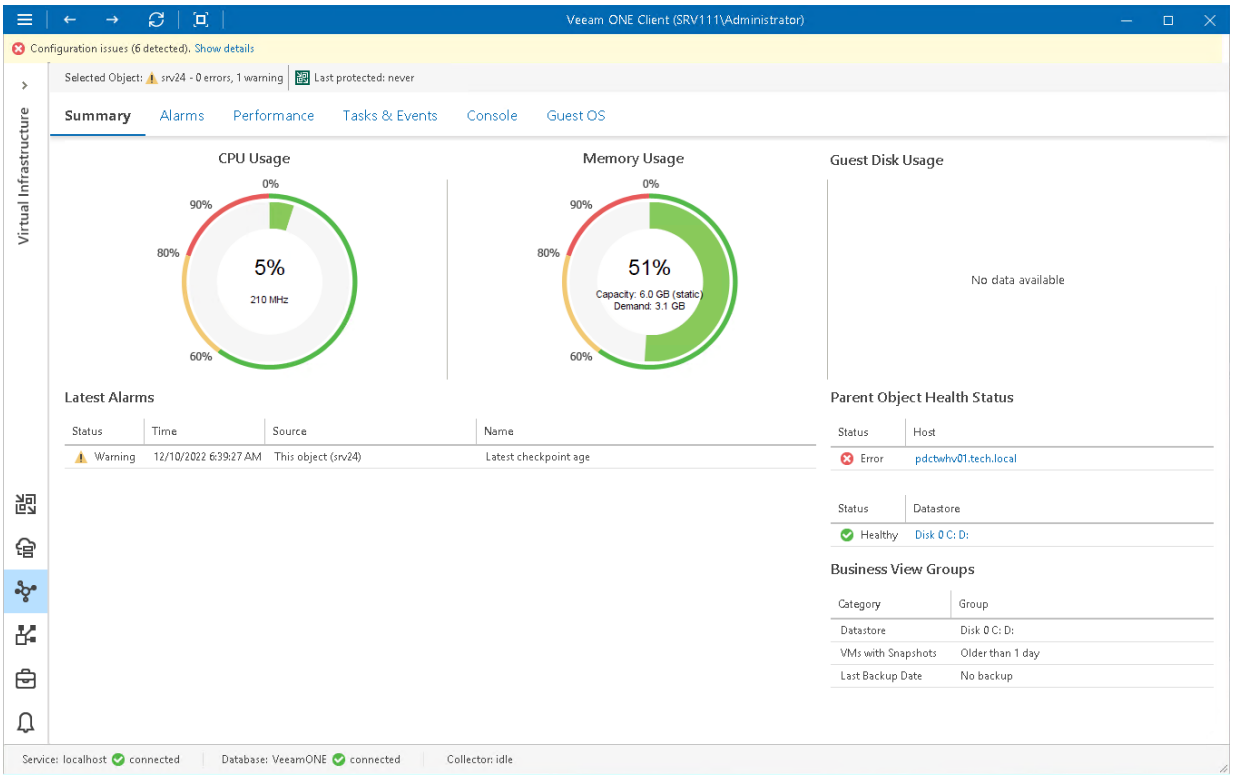
For more information, see Working with Triggered Alarms.

Business View Groups

The section displays the list of categories and groups to which the host is included.

Virtual Machine Summary

The VM summary dashboard provides the health status and performance overview for the selected VM. In addition, this dashboard shows the status of objects that can affect the VM performance — the parent host and the volumes where VM files are located.



Selected Object

The section at the top of the dashboard shows the VM health status (number of warnings and errors) and the date when the latest backup or replica restore point was created for the VM with Veeam Backup & Replication.

CPU Usage, Memory Usage

The charts display the amount of CPU and memory resources currently consumed by the VM.

NOTE:

- On Hyper-V hosts prior to version 2016, memory usage is shown as 100% for VMs with Static Memory.
- For Microsoft SQL Server or Exchange VMs running on Hyper-V 2016 hosts, memory usage can be shown to exceed 100%.
- Veeam ONE is not currently able to collect guest disk space usage data from Linux VMs running in a Hyper-V environment.

Guest Disk Usage

The chart displays the amount of available and used guest disk space with a breakdown by disks. By default, 5 guest disks with the greatest amount of used space are displayed.

Use the **Disks to show** list to change the number of disks to display on the chart. Click the **View all disks** link to view details for all guest disks. In the **Guests Disks** window, you can suppress *Guest disk space* alarms for specific disks. To suppress alarms for a disk, select the **Suppress alarms** check boxes next to the disk name.

Parent Object Health Status

The section displays the current state of the host where the VM resides and the state of volumes that host VMs files. Information in this section may help you to estimate the impact of parent objects on the VM performance. Click the host or volume name link to drill down to the list of alarms for the host or volume.

Latest Alarms

The list displays the latest 15 alarms for the VM.

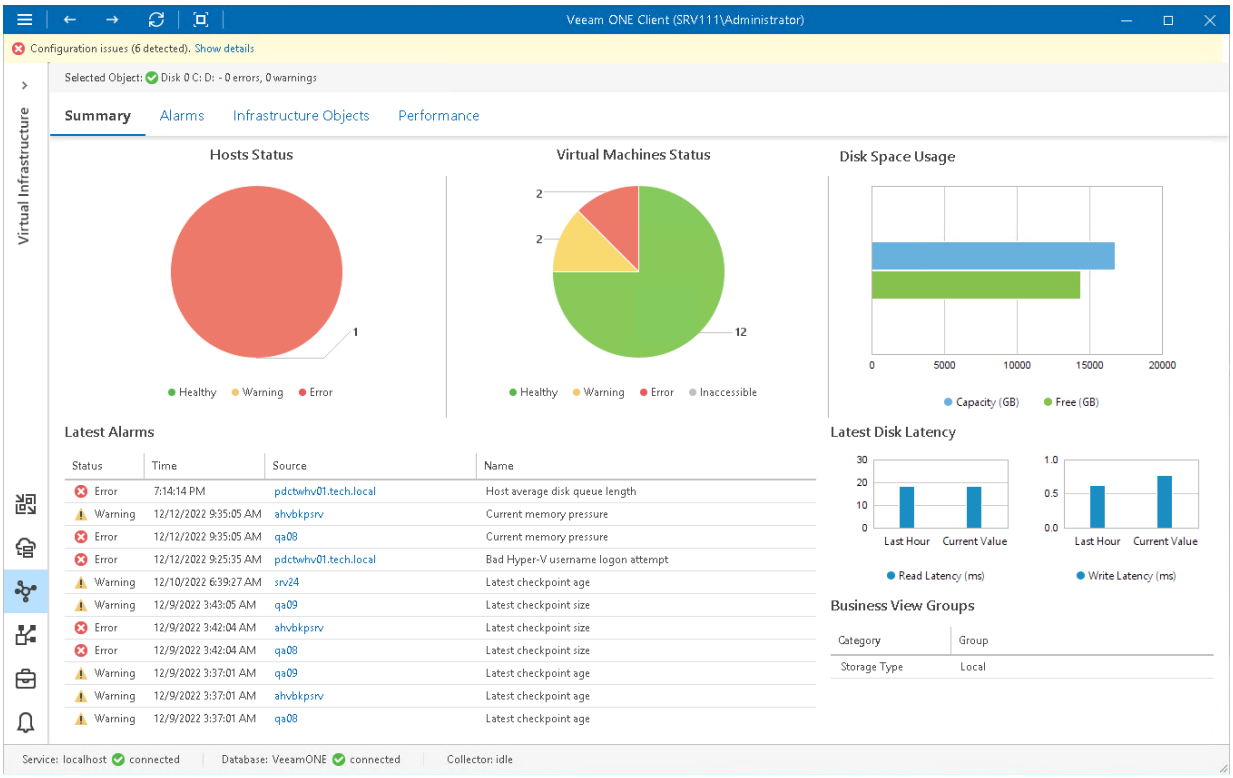
For more information, see Working with Triggered Alarms.

Business View Groups

The section displays the list of categories and groups to which the VM is included.

Local Storage Summary

The local storage summary dashboard provides the health status and performance overview for the selected host local storage. In addition, it shows the state of objects that can affect the storage performance — the parent host and VMs on the local storage.



Hosts Status, Virtual Machines Status

The charts reflect the health status of the host and VMs that work with the local storage.

Every chart segment represents the number of objects in a certain state — objects with errors (red), objects with warnings (yellow) and healthy objects (green). Click a chart segment or a legend label to drill down to the list of alarms with the corresponding status for hosts or VMs.

Disk Space Usage

The chart reflects the amount of available and used disk space on the local storage.

Latest Alarms

The list displays the latest 15 for the local storage and objects that work with the local storage. Click a link in the **Source** column to drill down to the list of alarms for the selected object.

For more information, see Working with Triggered Alarms.

Latest Disk Latency

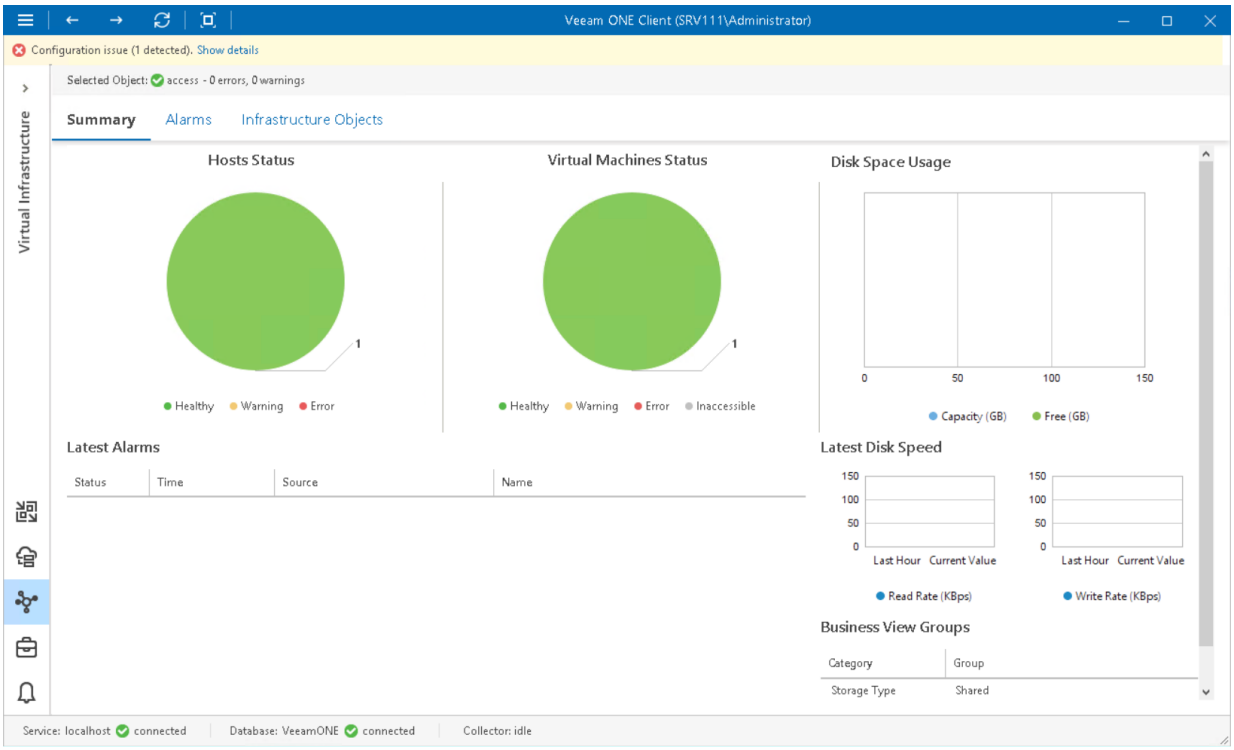
The section displays the current read and write latency values as well as the average latency values for the past hour.

Business View Groups

The section displays the list of categories and groups to which the storage is included.

SMB Share Summary

The SMB shares summary dashboard provides the health status and performance overview for the selected SMB share. In addition, it shows the state of objects that can affect SMB share performance — hosts that work with SMB shares and VMs residing on the shares.



Hosts Status, Virtual Machines Status

The charts reflect the health status of the hosts that work with the SMB share and VMs located on the share.

Every chart segment represents the number of objects with a certain status — objects with errors (red), objects with warnings (yellow) and healthy objects (green). Click a chart segment or a legend label to drill down to the list of alarms with the corresponding status for hosts or VMs.

Disk Space Usage

The chart reflects the amount of available and used disk space on the SMB share.

Latest Alarms

The list displays the latest 15 alarms for the SMB share and alarms for hosts that work with the file share and for VMs located on the share. Click a link in the **Source** column to drill down to the list of alarms for the selected object.

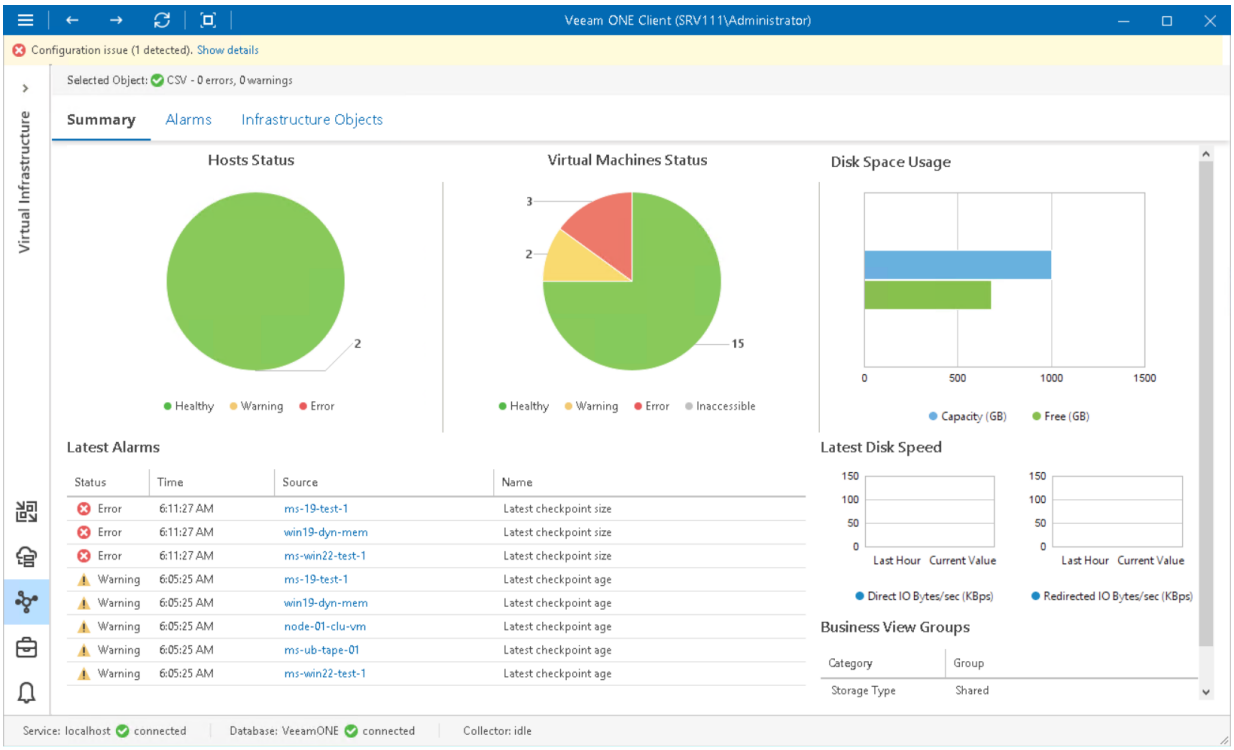
For more information, see Working with Triggered Alarms.

Latest Disk Speed

The section displays the current read and write rate as well as the average read and write rate values for the past hour.

Cluster Shared Volume Summary

The CSV summary dashboard provides the health status and performance overview for the selected Cluster Shared Volume. In addition, it shows the state of objects that can affect the volume performance — hosts that work with the CSV and VMs residing on the CSV.



Hosts Status, Virtual Machines Status

The charts reflect the health status of hosts that work with the volume and the state of VMs stored on the volume.

Every colored segment represents the number of objects with a certain status — objects with errors (red), objects with warnings (yellow) and healthy objects (green). Click a chart segment or a legend label to drill down to the list of alarms with the corresponding status for hosts or VMs.

Disk Space Usage

The chart reflects the amount of available and used disk space on the Cluster Shared Volumes.

Latest Alarms

The list displays the latest 15 alarms for the Cluster Shared Volumes and objects that work with the volumes. Click a link in the **Source** column to drill down to the list of alarms for the selected object.

For more information, see Working with Triggered Alarms.

Latest Disk Speed

The section displays the current direct and redirected I/O values as well as the average values for the past hour.

Microsoft Hyper-V Alarms

Veeam ONE includes a set of alarms for monitoring Microsoft Hyper-V virtual environment. These alarms warn you about events or changes that can affect performance of operations and services in the virtual environment.

To view the list of triggered Microsoft Hyper-V alarms:

1. Open Veeam ONE Client.

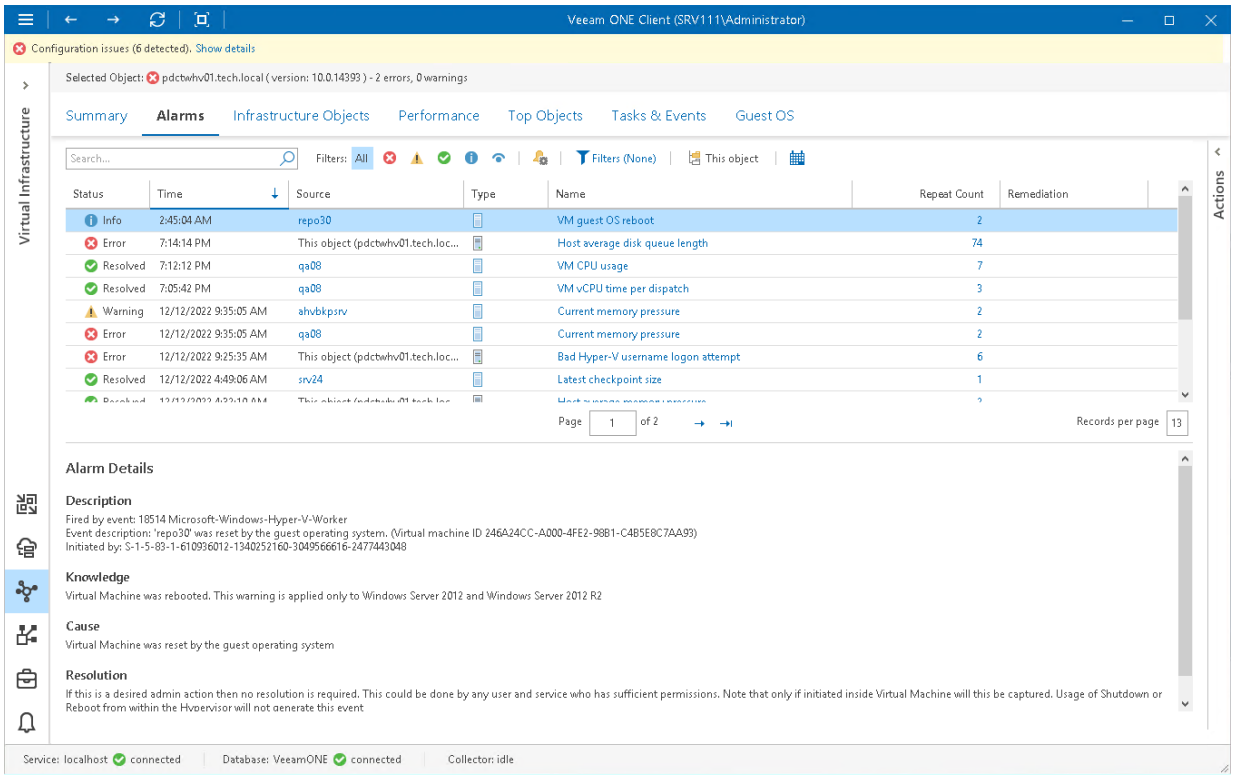
   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click **Virtual Infrastructure**.

3. In the inventory pane, select the necessary virtual infrastructure node.

4. Open the **Alarms** tab.

On the **Alarms** dashboard, you can view triggered alarms, track alarm history, resolve and acknowledge alarms and perform other actions. For details on available actions, see Working with Triggered Alarms.



Microsoft Hyper-V Performance Charts

Performance charts show how key performance counters have been changing over time to help you diagnose performance issues and perform root cause analysis.

Performance charts include the following elements:

- **Axes**

  Performance charts display data for a particular time period (the horizontal axis) using two scales of measurement units (vertical axes). The measurement units may vary depending on selected performance counters. However, the number of units is always limited to two.

- **Graphs**

  Performance charts include one or more graphs. Every graph on a performance chart visualizes a specific counter for an infrastructure object or a container of infrastructure objects.

- **Legend**

  The chart legend shows details about objects and counters displayed in the chart. The details include key color, object name, list of counters and units of measurement, the latest, minimum, average, and maximum counter values.

- **Chart views**

  Performance charts come with a number of predefined chart views. Every view logically groups related counters to display the most valuable data and help you speed up troubleshooting and root cause analysis of performance problems.

Performance charts can be easily customized. For details on customization options, see Customizing Microsoft Hyper-V Performance Charts.

Accessing Performance Charts

To access a performance chart for an infrastructure object or infrastructure segment:

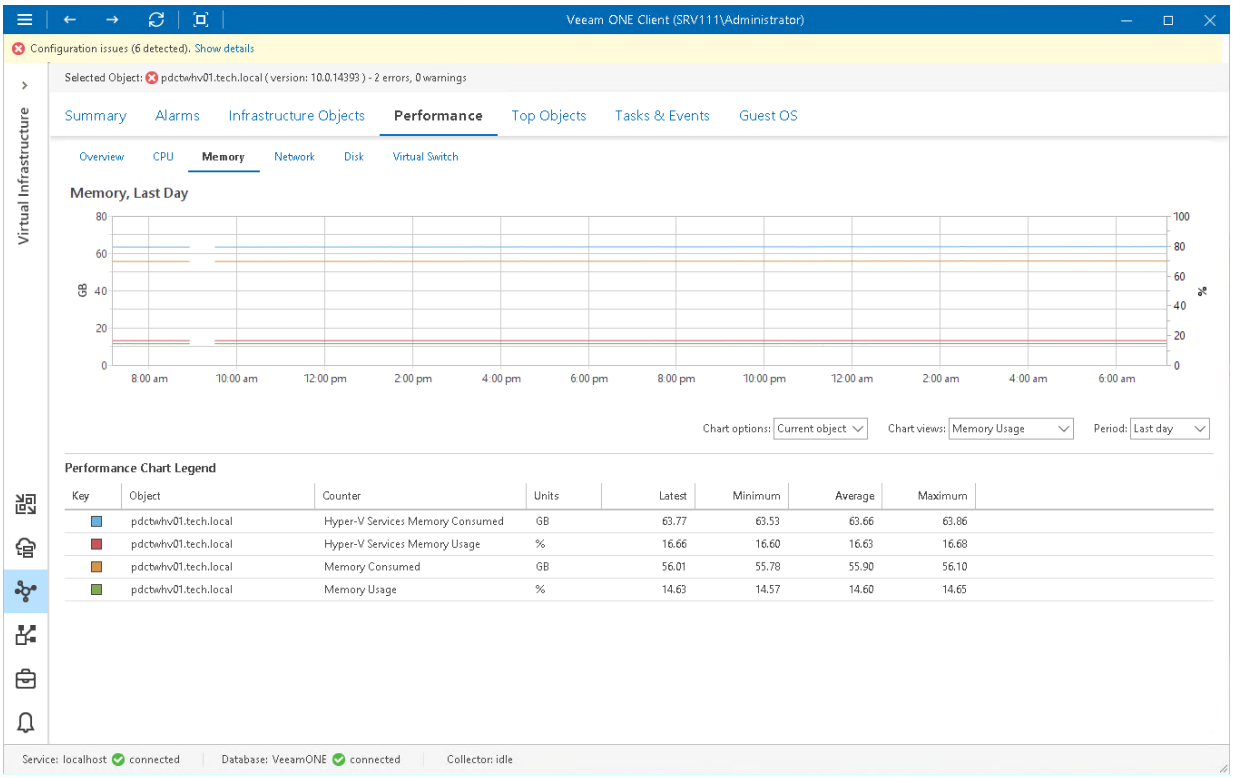
1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click **Virtual Infrastructure**.

3. In the inventory pane, select the necessary infrastructure object or segment.

4. Open the **Performance** tab.

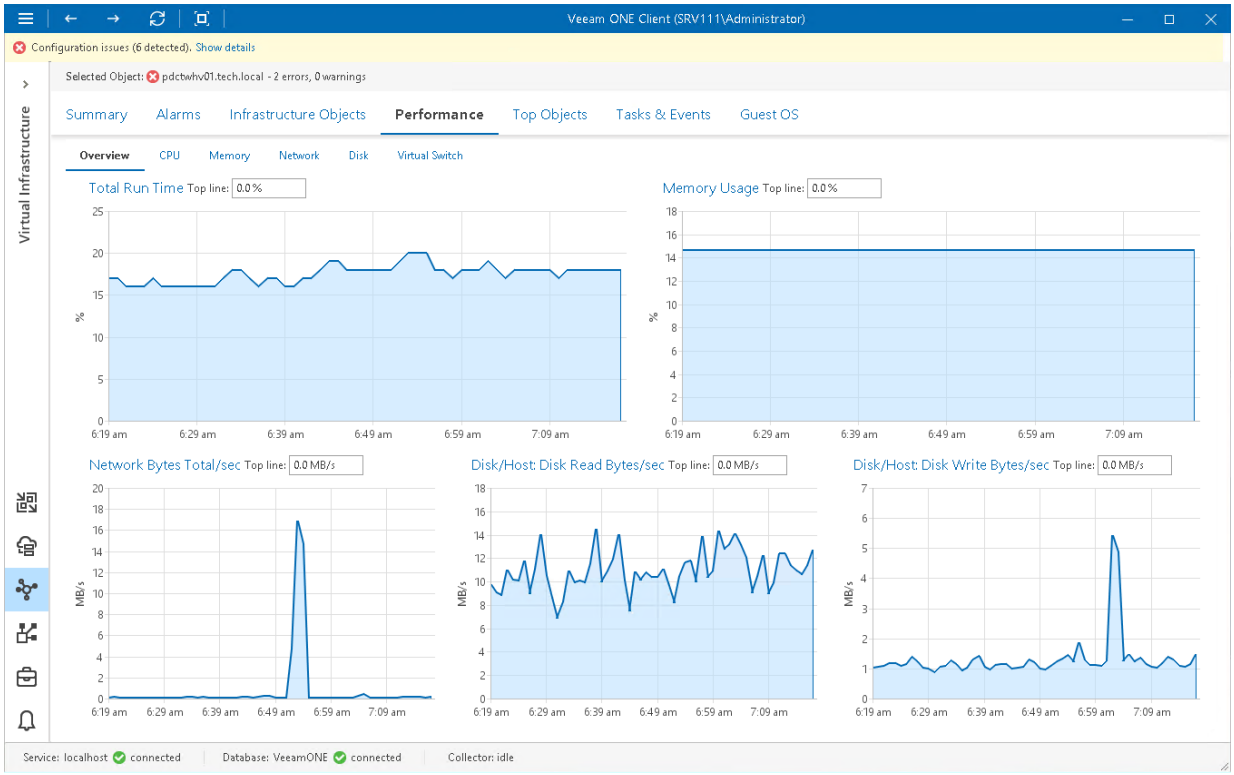


Overview

The **Overview** page shows aggregated performance data for the selected virtual infrastructure object or segment: total run time, memory usage, network, disk/host read and write speed. Performance data is shown for the previous 15 minutes.

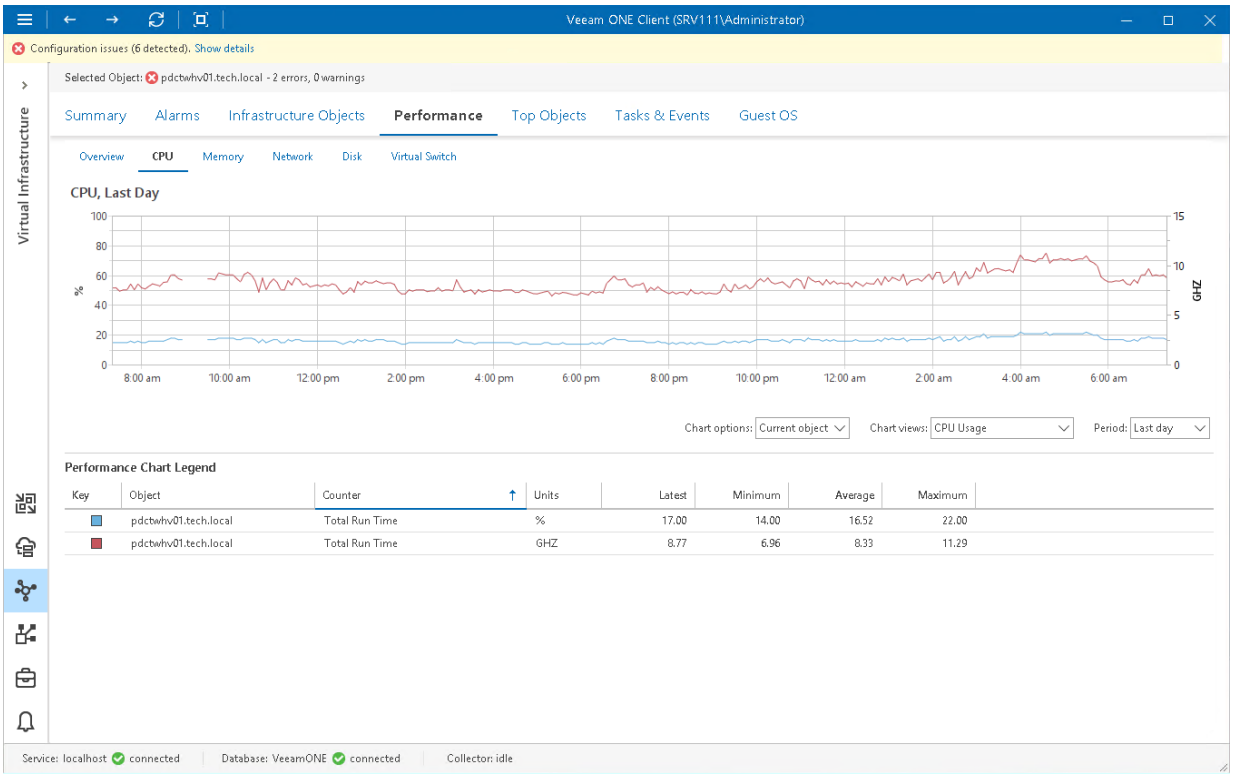
In the **Top line** field, you can set a threshold value. The top line is displayed as the red dotted line on the chart to help you monitor whether resource usage exceeds the healthy value range. If you do not need to display the top line, enter '0' (zero) in the **Top line** field or disable top lines in Veeam ONE Client chart settings. With the top line disabled, the Y-axis will scale automatically to match the range of the displayed data.

To drill down to performance chart details, click the counter link above a performance widget. A corresponding performance chart for the selected virtual infrastructure object will open.



CPU Performance Chart

The **CPU** chart displays historical statistics on CPU utilization for the selected virtual infrastructure object.



Host

The following table provides information on predefined views and counters that apply to hosts.

Chart View	Counter	Measurement Unit	Description
CPU Usage	Total Run Time	Percent	Percentage of time a physical processor required to run both VMs and the hypervisor itself.
	Total Run Time	GHz	Amount of time physical processor required to run both VMs and the hypervisor itself.
CPU Usage by Host/VMs	Guest Run Time	Percent	Percentage of time a physical processor required to run VMs.
	Hypervisor Run Time	Percent	Percentage of time a physical processor required to run a hypervisor.
	vCPU Total Run Time	Percent	Percentage of time vCPUs were used by all VMs on a host.

Chart View	Counter	Measurement Unit	Description
CPU Idle Time	Idle Time	Percent	Percentage of time a physical processor spent in an idle state.
CPU Interrupts	Total Interrupts/sec	Number	Number of interrupts to which a processor was asked to respond. Interrupts are generated from hardware components like hard disk controller adapters and network interface cards. A sustained value over 1000 usually indicates of a problem.
CPU Bottlenecks	Host CPU Wait Time	Microsecond	Average amount of time that VMs on a host spend waiting for their virtual processors to be dispatched onto a logical processor.

Virtual Machine

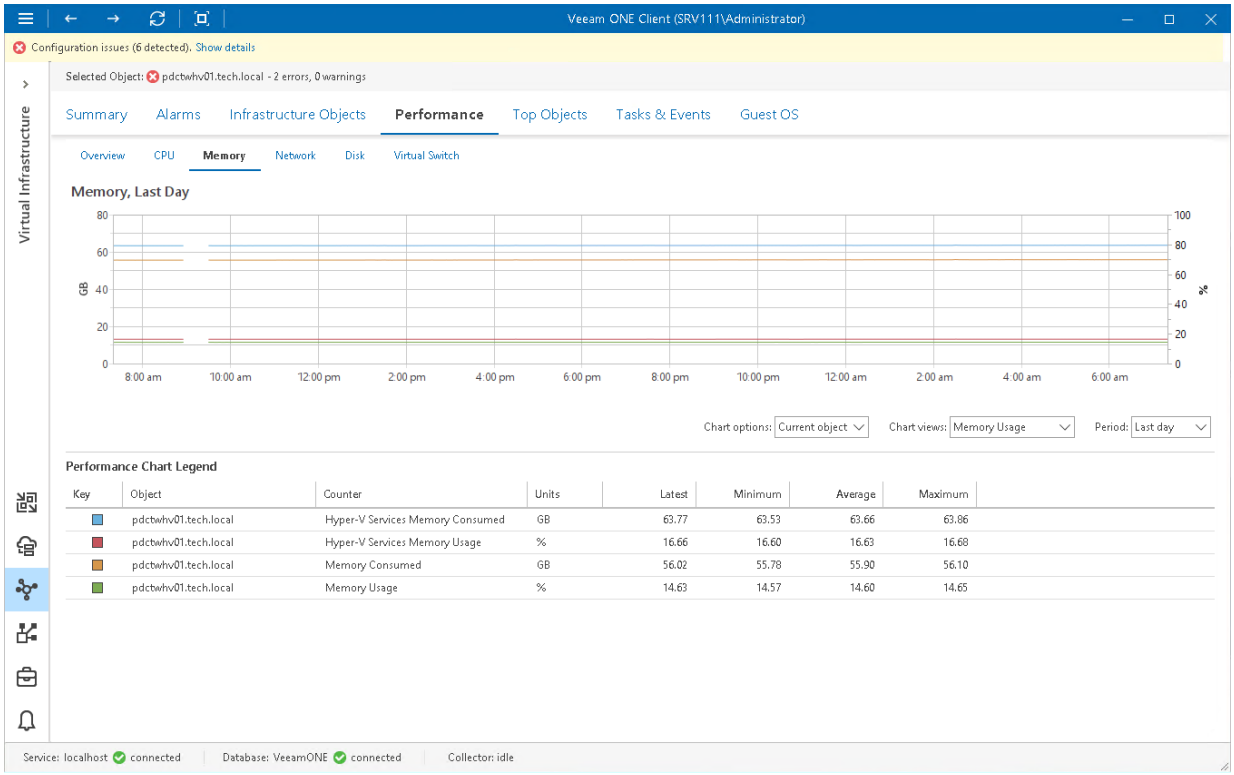
The following table provides information on predefined views and counters that apply to VMs.

Chart View	Counter	Measurement Unit	Description
CPU Usage	Guest Run Time	Percent	Percentage of time a physical processor required to run a VM.
	Guest vCPU Run Time	MHz	Amount of virtual CPU resources used by a VM.
CPU Usage by Host	Hypervisor Run Time	Percent	Percentage of physical processor time consumed by Hyper-V host for a VM.
	Total Run Time	Percent	Percentage of time a Hyper-V host required to run a VM, plus time consumed by the VM itself.
	vCPU Total Run Time	MHz	Amount of vCPU resources consumed by all VMs on a host.
CPU Bottlenecks	CPU Wait Time	Microsecond	Amount of time that a virtual processor spends waiting to be dispatched onto a logical processor.

For objects that are parent to hosts and VMs, Veeam ONE Client displays rollup values.
Charts for folders and clusters display rollup values for all hosts in the container. Chart for a resource displays rollup values for all VMs registered as shared resources.

Memory Performance Chart

The **Memory** chart displays historical statistics on memory utilization for the selected virtual infrastructure object.



Host

The following table provides information on predefined views and counters that apply to hosts.

Chart View	Counter	Measurement Unit	Description
Memory Usage	Hyper-V Services Memory Consumed	GB	Amount of memory currently consumed by Hyper-V services.
	Hyper-V Services Memory Usage	Percent	Amount of memory resources currently used by Hyper-V services.
	Memory Consumed	GB	Amount of physical memory resources used on a host.

Chart View	Counter	Measurement Unit	Description
	Memory Usage	Percent	Memory usage as percentage of available machine memory.
Memory Pressure	Average Pressure	Percent	Amount of memory resources available on a host.
Committed Memory	Committed	GB	Demand for virtual memory. The counter shows how much memory were allocated for processes and to which processes the OS has committed a RAM page frame or a page slot in the pagefile (or both). As the Committed counter grows above the available RAM, paging increases and the amount of the pagefile in use increases as well. At some point, paging activity starts to affect perceived performance significantly.
Memory Swap Faults	Page Faults/sec	Number	Page faults that occur when any process attempts to read from a virtual memory location that is marked as 'not present'. The best counter value is zero. The counter displays both hard page and soft page faults.
Memory Swap Rate	Page Reads/sec	Number	Lack of memory resources. The counter shows how often the system reads from disk because of hard page faults. The counter shows the number of read operations, not taking into account the number of pages retrieved in each operation. The counter can reveal different kinds of faults that cause system delays.
	Page Writes/sec	Number	Number of attempts taken by running the write command/operation to clear unused items out of memory. Pages are written to disk only if they change while in physical memory, so they are likely to hold data, not code. The counter shows write operations, not taking into account the number of pages written in each operation.
	Pages Input/sec	Number	Rate at which memory pages are read from disk.
	Pages Output/sec	Number	Rate at which memory pages are written to disk.
	Pages/sec	Number	Sum of Pages Input/sec and Pages Output/sec counters. The counter indicates how often the system uses a hard drive to store and retrieve memory-associated data.

Virtual Machine

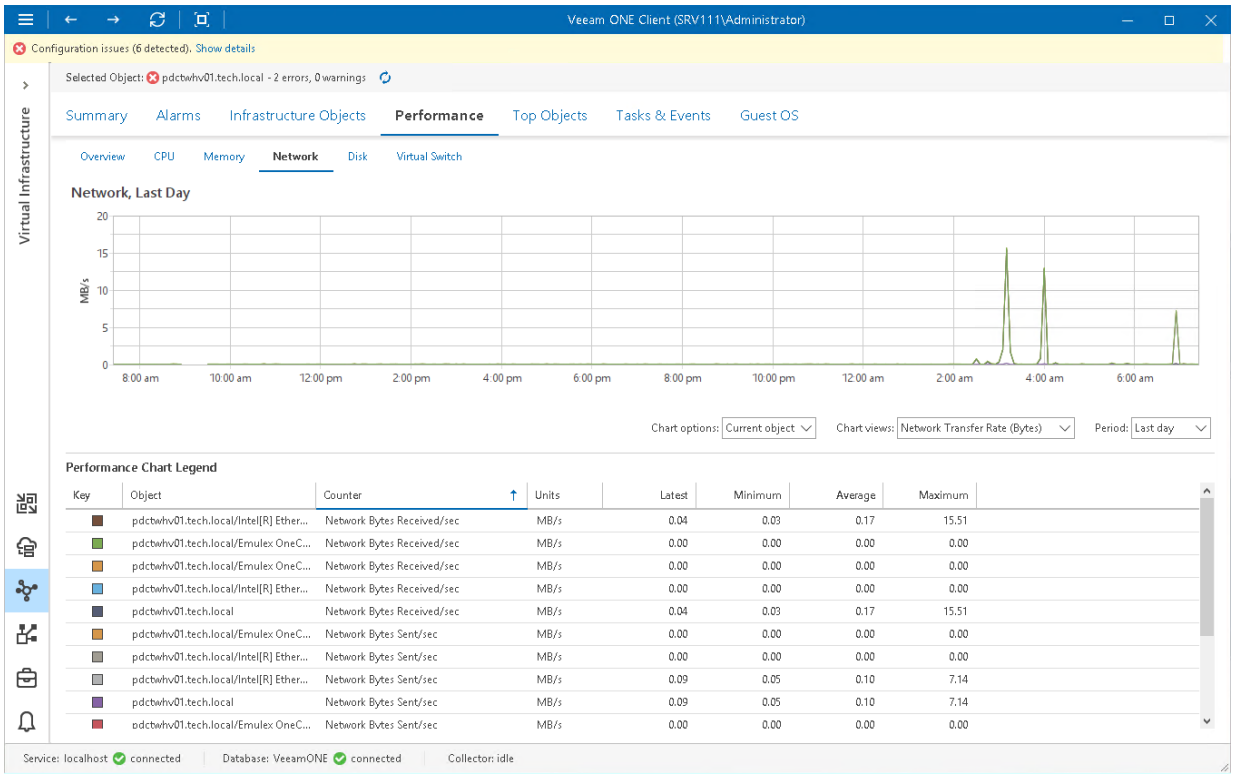
The following table provides information on predefined views and counters that apply to VMs.

Chart View	Counter	Measurement Unit	Description
Memory Usage	Guest Visible Physical Memory	GB	Amount of memory visible to the guest OS running inside a VM.
	Physical Memory	GB	Amount of memory currently used by a VM.
Memory Pressure	Demand	B	Amount of memory a VM requires to run all active processes. The counter represents the total committed memory based on data obtained from other performance counters.
	Current Pressure	Percent	Current pressure in a VM. To calculate the counter, Microsoft Hyper-V analyzes the VM total committed memory and calculates the pressure as the following ratio: the amount of memory the VM wants / the amount of memory the VM has.

For objects that are parent to hosts and VMs, Veeam ONE Client displays rollup values.
Charts for folders and clusters display rollup values for all hosts in the container. Chart for a resource displays rollup values for all VMs registered as shared resources.

Network Performance Chart

The **Network** chart displays historical statistics on network usage for the selected virtual infrastructure object.



Host

The following table provides information on predefined views and counters that apply to hosts.

Chart View	Counter	Measurement Unit	Description
Network Transfer Rate	Network Bytes Received/sec	KB/s	Rate at which data is received across each network adapter on a host. The counter represents the bandwidth of the network.
	Network Bytes Sent/sec	KB/s	Rate at which data is sent across each network adapter on a host.
	Network Bytes Total/sec	KB/s	Rate at which data is sent and received across a network interface.
Network Output Queue Length	Network Output Queue Length	Number	Length of the output queue, in packets. If the Output Queue Length value exceeds 2, it can be an indicator of delays across the network. In this case, you should find and eliminate the bottleneck to improve performance.

Chart View	Counter	Measurement Unit	Description
Network Connections	Network Offloaded Connections	Number	Number of TCP connections (over both IPv4 and IPv6) currently handled by a TCP Chimney Offload network adapter.
Network Errors	Network Outbound Errors	Number	Number of outbound packets that could not be transmitted because of errors.
	Network Received Errors	Number	Number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Network Transfer Rate (Packets)	Network Packets Received/sec	Number	Rate at which packets are received on the network interface.
	Network Packets Sent/sec	Number	Rate at which packets are sent on the network interface.
	Network Packets/sec	Number	Rate at which packets are sent and received on the network interface.

Virtual Machine

The following table provides information on predefined views and counters that apply to VMs.

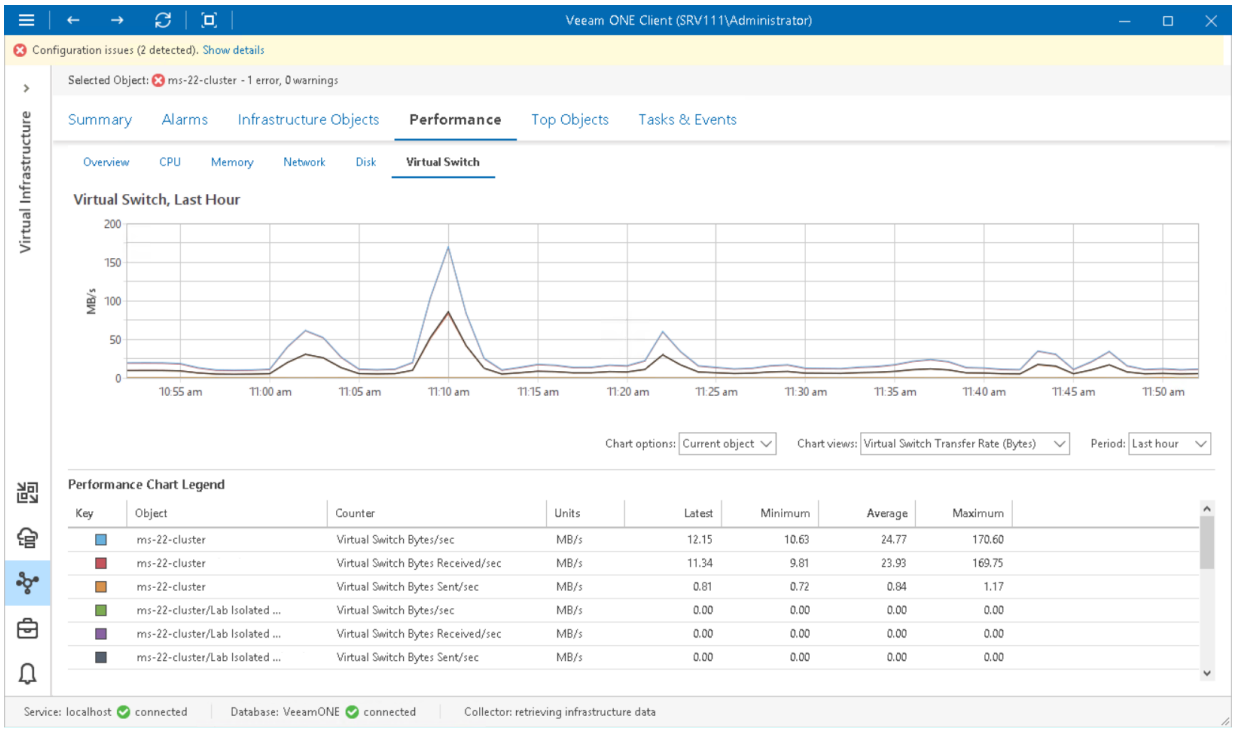
Chart View	Counter	Measurement Unit	Description
Virtual Network Usage	Virtual Network Bytes Received/sec	KB/s	Rate at which data is received across the vNIC instance on a VM. The counter represents the bandwidth of the network.
	Virtual Network Bytes Sent/sec	KB/s	Rate at which data is sent across the vNIC instance on a VM.
	Virtual Network Bytes/sec	KB/s	Network utilization, sum of data received and sent across all vNIC instances on a VM.
Virtual Network Usage (Packets)	Virtual Network Packets Received/sec	Number	Total number of packets received per second by the network adapter.
	Virtual Network Packets Sent/sec	Number	Total number of packets sent per second by the network adapter.

Chart View	Counter	Measurement Unit	Description
Legacy Network Bytes Dropped	Legacy Network Bytes Dropped	B	Amount of data dropped on the network adapter.
Legacy Network Usage	Legacy Network Bytes Received/sec	B/s	Amount of data received by the network adapter.
	Legacy Network Bytes Sent/sec	B/s	Amount of data sent by the network adapter.

For objects that are parent to hosts and VMs, Veeam ONE Client displays rollup values.
Charts for folders and clusters display rollup values for all hosts in the container. Chart for a resource displays rollup values for all VMs registered as shared resources.

Virtual Switch Performance Chart

The **Virtual Switch** chart displays historical statistics on virtual switch usage for Microsoft Hyper-V hosts.

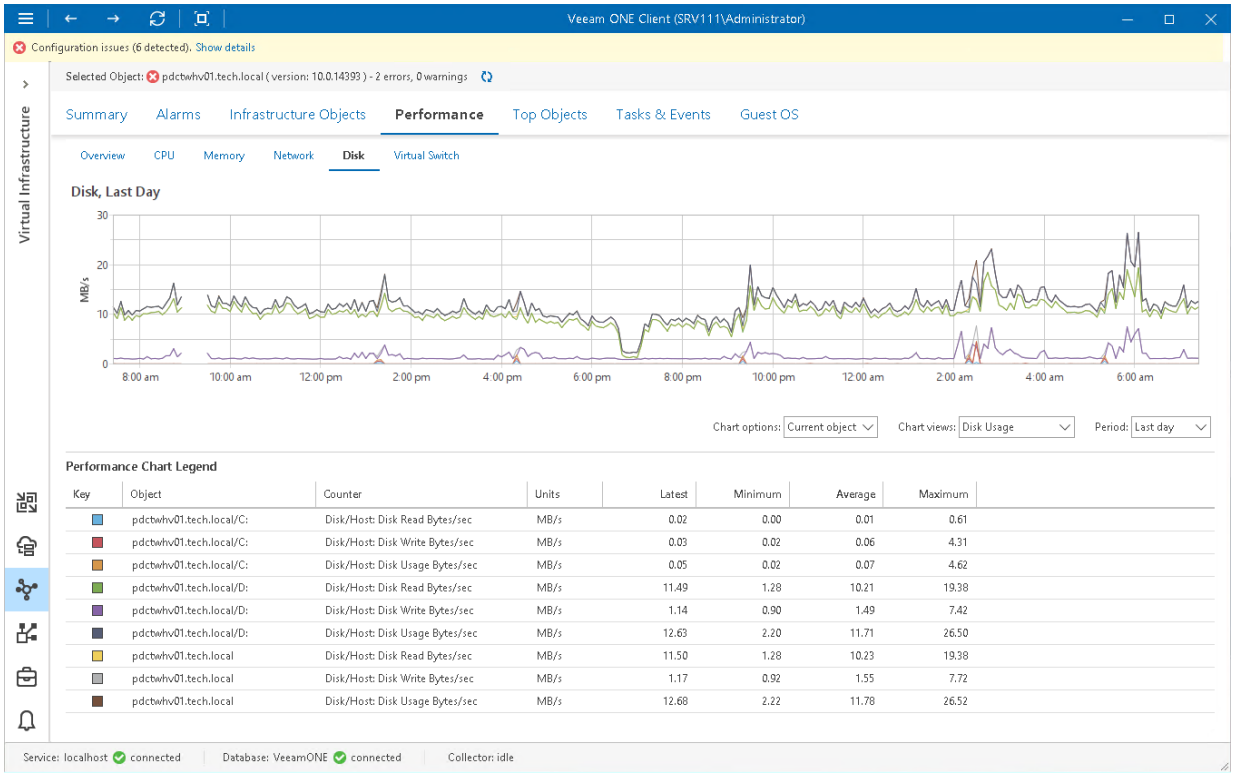


The following table provides information on predefined views and counters.

Chart View	Counter	Measurement Unit	Description
Virtual Switch Transfer Rate (Bytes)	Virtual Switch Bytes Received/sec	KB/s	Amount of data received per second by a virtual switch.
	Virtual Switch Bytes Sent/sec	KB/s	Amount of data sent per second by a virtual switch.
	Virtual Switch Bytes/sec	KB/s	Amount of data received and sent per second by a virtual switch.
Virtual Switch Transfer Rate (Packets)	Virtual Switch Packets Received/sec	Number	Total number of packets received per second by a virtual switch.
	Virtual Switch Packets Sent/sec	Number	Total number of packets sent per second by a virtual switch.
	Virtual Switch Packets/sec	Number	Total number of packets received and sent per second by a virtual switch.

Cluster/Host Disk Performance Chart

The **Disk** chart is available for Microsoft Hyper-V clusters and hosts. The chart displays historical statistics on disk usage for the selected cluster or host.



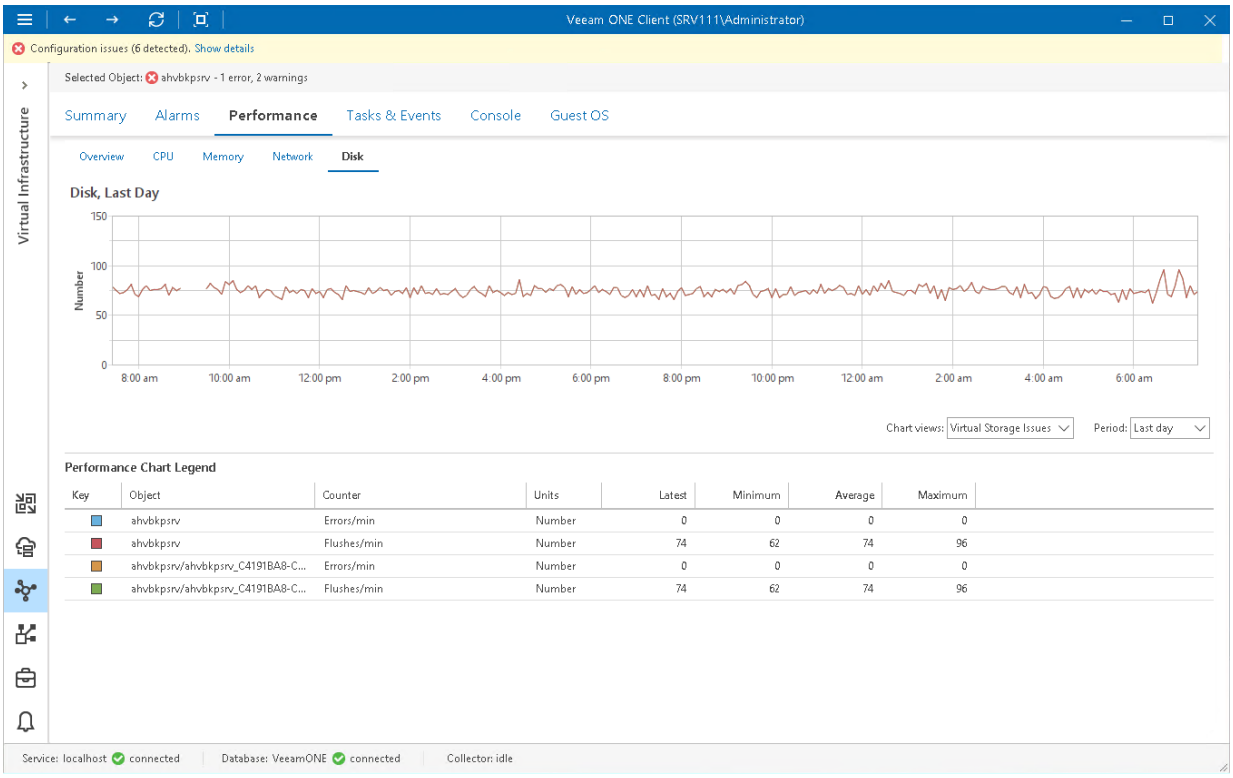
The following table provides information on predefined views and counters.

Chart View	Counter	Measurement Unit	Description
Disk Usage	Disk/Host: Disk Read	MB/s	Rate at which bytes are transferred from a disk during read operations.
	Disk/Host: Disk Write	MB/s	Rate at which bytes are transferred from a disk during write operations.
	Disk/Host: Disk Usage	MB/s	Rate at which bytes are transferred to and from a disk during read and write operations.
Disk Queue Length	Disk/Host: Avg Disk Queue Length	Number	Average number of read and write requests that were queued for a disk during the sample interval.
Disk Latency	Disk/Host: Avg Disk sec/Read	Millisecond	Average amount of time that a read operation from a disk takes.

Chart View	Counter	Measurement Unit	Description
	Disk/Host: Avg Disk sec/Write	Millisecond	Average amount of time that a write operation to a disk takes.

VM Disk Performance Chart

The **Disk** chart for VMs displays historical statistics for partitions of all disks on the selected VM.



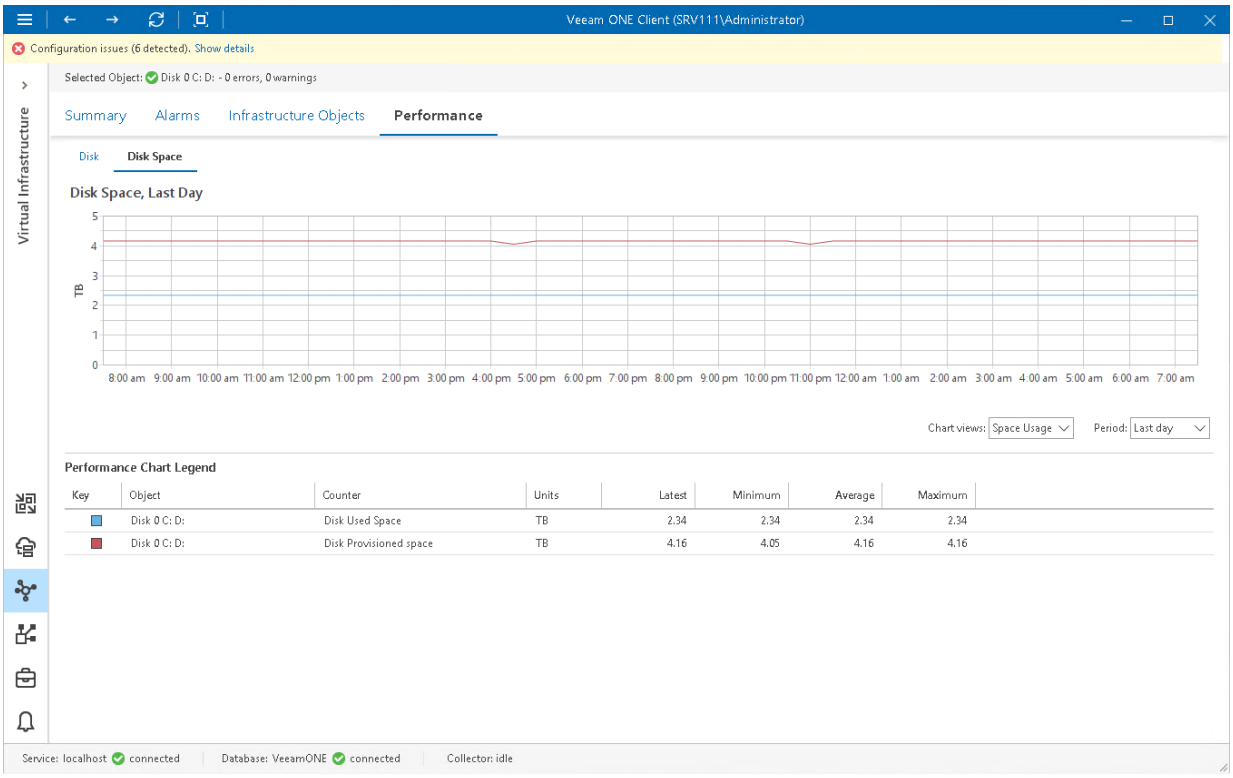
The following table provides information on predefined views and counters.

Chart View	Counter	Measurement Unit	Description
Virtual Storage Issues	Errors/min	Number	Number of virtual storage errors per minute.
	Flushes/min	Number	Number of virtual storage flush operations per minute.
Virtual Storage Usage	Virtual Storage Read	KB/s	Total number of bytes that have been read per second on a virtual storage.
	Virtual Storage Write	KB/s	Total number of bytes that have been written per second on a virtual storage.
	Virtual Storage Usage	KB/s	Rate at which bytes have been read and written per second on a virtual storage.
Virtual Storage IOPS	IOPS	Number	Average number of read and write operations per second to a virtual storage.

Chart View	Counter	Measurement Unit	Description
	Reads/sec	Number	Total number of read operations issued per second to a virtual storage.
	Writes/sec	Number	Total number of write operations issued per second to a virtual storage.

Disk Space Chart

The **Disk Space** chart it displays historical statistics on disk space resources and usage for the selected disk.

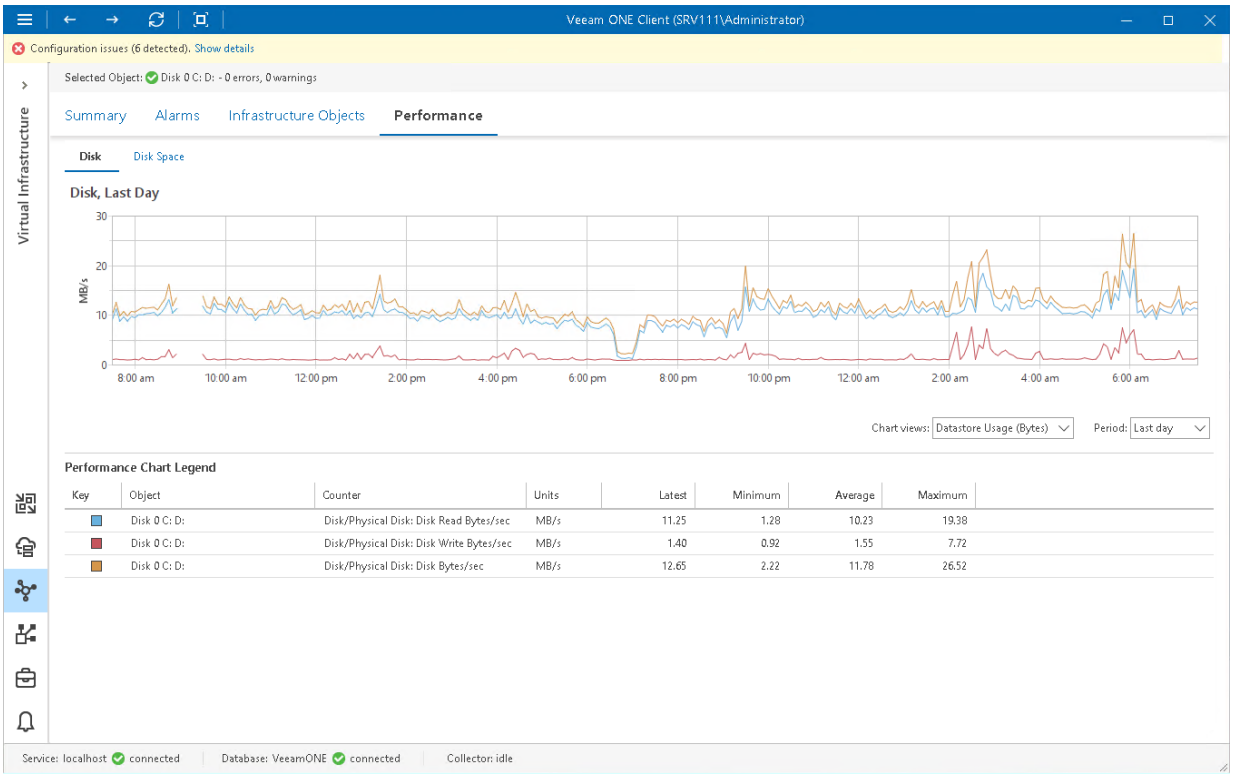


The following table provides information on predefined views and counters.

Chart View	Counter	Measurement Unit	Description
Space Usage	Disk Free Space	TB	Amount of free space on a disk.
	Disk Provisioned Space	TB	Amount of disk space provisioned to VMs.
	Disk Used Space	TB	Amount of used space on a disk.

Local Volume Performance Chart

The **Disk** chart displays historical statistics on disk usage for the selected local volume.



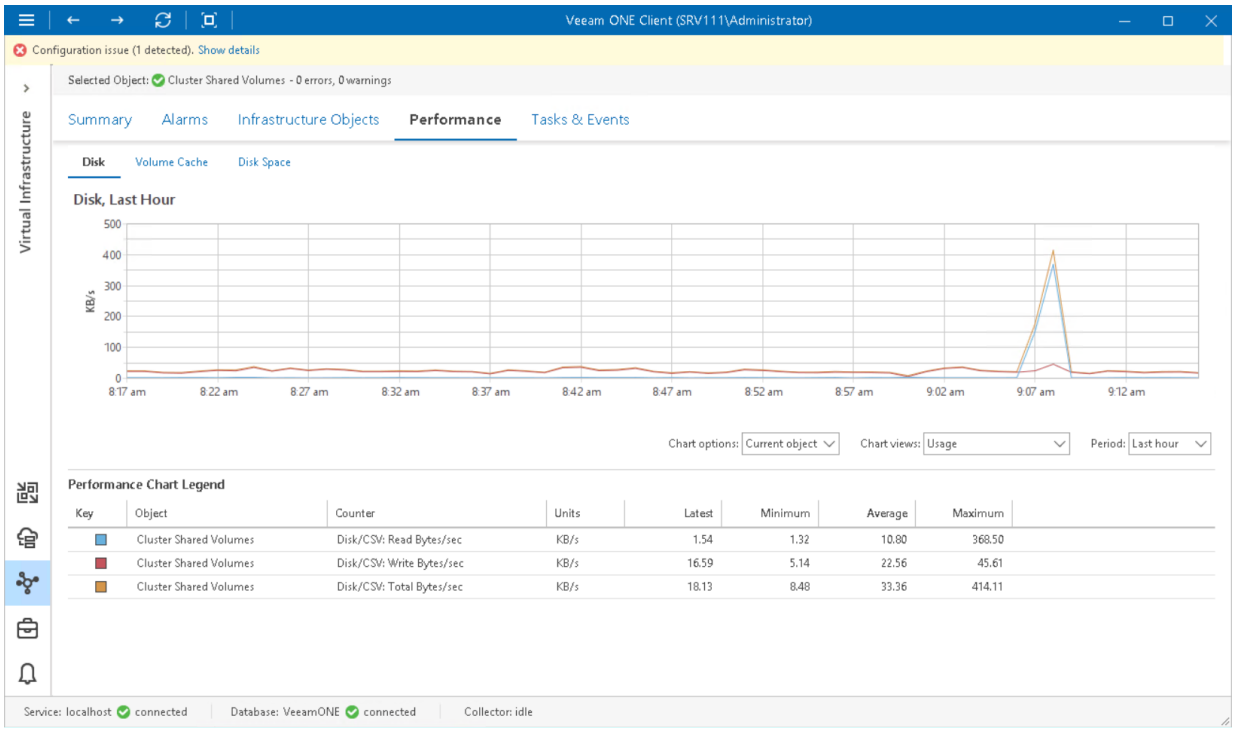
The following table provides information on predefined views and counters.

Chart View	Counter	Measurement Unit	Description
Datastore Usage	Disk/Physical Disk: Disk Read	MB/s	Rate at which data is read from a volume.
	Disk/Physical Disk: Disk Write	MB/s	Rate at which data is written to a volume.
	Disk/Physical Disk: Disk	MB/s	Sum of read and write rates for a volume.
Datastore Queue Length	Disk/Physical Disk: Avg. Disk Queue Length	Number	Average number of read and write operations queued for a volume.
Datastore IOPS	Disk/Physical Disk: Disk Transfers/sec	Number	Number of read and write operations completed per second, regardless of how much data they involve. This counter measures disk utilization. If the value exceeds 50, it can be an indicator of a bottleneck.

Chart View	Counter	Measurement Unit	Description
Datastore Latency	Disk/Physical Disk: Avg Disk sec/Read	Millisecond	Average time that a read operation from a volume takes.
	Disk/Physical Disk: Avg Disk sec/Write	Millisecond	Average time that a write operation to a volume takes.

Cluster Shared Volume Disk Performance Chart

The **Disk** chart displays historical statistics on disk usage for the selected Cluster Shared Volume.



The following table provides information on predefined views and counters.

Chart View	Counter	Measurement Unit	Description
Usage	Disk/CSV: Read Bytes/sec	KB/s	Rate at which data is read from the volume in the Direct Access or Redirected Access mode.
	Disk/CSV: Write Bytes/sec	KB/s	Rate at which data is written to the volume in the Direct Access or Redirected Access mode.
	Disk/CSV: Total Bytes/sec	KB/s	Rate at which data is read from and written to the volume in the Direct Access or Redirected Access mode.
IOPS	Disk/CSV: Reads/sec	Number	Rate at which read operations were performed directly on a volume.
	Disk/CSV: Writes/sec	Number	Rate at which write operations were performed directly on a volume.

Chart View	Counter	Measurement Unit	Description
	Disk/CSV2012: IOPS	Number	Rate at which read and write operations were performed directly on a volume.
Latency	Disk/CSV: Read Latency	Millisecond	Average latency between the time a read request arrived to a file system and the time when it was completed.
	Disk/CSV: Write Latency	Millisecond	Average latency between the time a write request arrived to a file system and the time when it was completed.
	Disk/CSV: Latency	Millisecond	Average latency required to complete read and write operations on a volume.
Datastore Queue Length	Disk/CSV: Read Queue Length	Number	Number of read operations queued for a volume.
	Disk/CSV: Write Queue Length	Number	Number of write operations queued for a volume.
	Disk/CSV: Queue Length	Number	Number of read and write operations that were queued for a volume during the sample interval.
Direct/Redirected Usage	Disk/CSV: Redirected Bytes/sec	KB/s	Average amount of data transferred to or from a disk during write or read operations over the network stack.
	Disk/CSV: Direct Bytes/sec	KB/s	Average amount of data transferred to or from a disk during write or read operations.
Direct/Redirected Latency	Disk/CSV: Direct Latency	Millisecond	Average latency required to for complete read and write operations on a volume in the Direct Access mode.
	Disk/CSV: Redirected Latency	Millisecond	Average latency required to complete read and write requests on a volume in the Redirected Access mode.
Direct/Redirected IOPS	Disk/CSV: Direct IOPS	Number	Rate at which read and write operations were performed directly on a disk.

Chart View	Counter	Measurement Unit	Description
	Disk/CSV: Redirected IOPS	Number	Rate at which read and write operations were redirected to a volume through the network.

SMB Share Disk Performance Chart

The **Disk** chart displays historical statistics on disk usage for the selected SMB file share.

The following table provides information on predefined views and counters.

Chart View	Counter	Measurement Unit	Description
Virtual Storage Issues	Errors/min	Number	Number of virtual storage errors per minute.
	Flushes/min	Number	Number of virtual storage flush operations per minute.
Virtual Storage Usage	Virtual Storage Read	KB/s	Total amount of data that have been read per second on the virtual storage.
	Virtual Storage Write	KB/s	Total amount of data that have been written per second on the virtual storage.
	Virtual Storage Usage	KB/s	Rate at which data is read and written per second on the virtual storage.
Virtual Storage IOPS	Reads/sec	Number	Total number of read operations that have occurred on the virtual storage.
	Writes/sec	Number	Total number of write operations that have occurred on the virtual storage.
	IOPS	Number	Average number of read and write operations per second during collection interval.

HA SMB Performance Chart

The **HA Disk** chart displays historical statistics on disk usage for the selected Highly Available SMB share created on Cluster Shared Volumes.

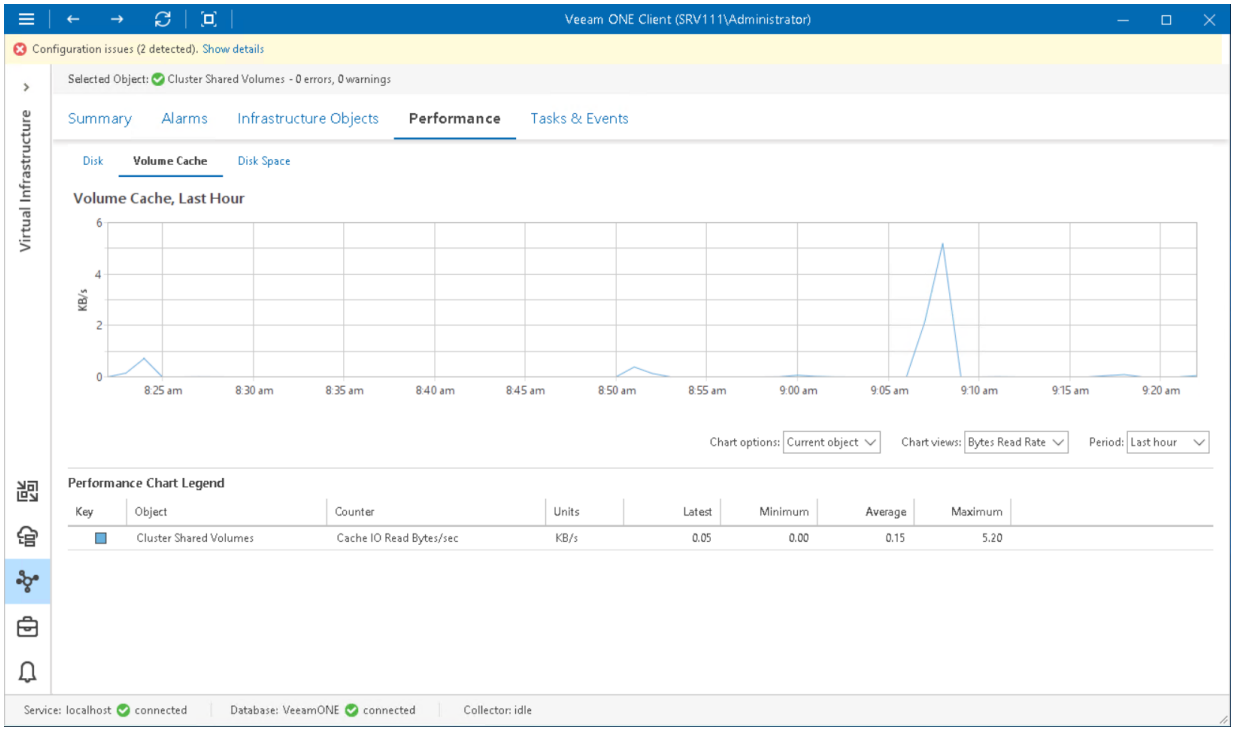
The following table provides information on predefined views and counters.

Chart View	Counter	Measurement Unit	Description
Usage	Disk/CSV: Read	KB/s	Rate at which data was read from a volume in the Direct Access or Redirected Access mode.
	Disk/CSV: Write	KB/s	Rate at which data was written to a volume in the Direct Access or Redirected Access mode.
	Disk/CSV: Total	KB/s	Rate at which data was read from and written to a volume in the Direct Access or Redirected Access mode.
IOPS	Disk/CSV: Read/sec	Number	Rate at which read operations were performed directly on a volume.
	Disk/CSV: Writes/sec	Number	Rate at which write operations were performed directly on a volume.
	Disk/CSV: IOPS	Number	Rate at which read and write operations were performed directly on a volume.
Latency	Disk/CSV: Read Latency	Millisecond	Average latency between the time a read request arrived to a file system and the time when it was completed.
	Disk/CSV: Write Latency	Millisecond	Average latency between the time a write request arrived to the file system and the time when it was completed.
	Disk/CSV: Latency	Millisecond	Average latency required to complete read and write operations on a volume.
Datastore Queue Length	Disk/CSV: Read Queue Length	Number	Number of read operations queued for a volume.
	Disk/CSV: Write Queue Length	Number	Number of write operations queued for a volume.

Chart View	Counter	Measurement Unit	Description
	Disk/CSV: Queue Length	Number	Total number of read and write operations queued for a volume during the sample interval.
Direct/Redirected Usage	Disk/CSV: Redirected Bytes/sec	KB/s	Average amount of data transferred to or from the disk during write or read operations over the network stack.
	Disk/CSV: Direct Bytes/sec	KB/s	Average amount of data transferred to or from the disk during write or read operations.
Direct/Redirected Latency	Disk/CSV: Direct Latency	Millisecond	Average latency required to complete read and write operations on a volume in the Direct Access mode.
	Disk/CSV: Redirected Latency	Millisecond	Average latency required to complete read and write operations on a volume in the Redirected Access mode.
Direct/Redirected IOPS	Disk/CSV: Direct IOPS	Number	Rate at which read and write operations were performed directly on a disk.
	Disk/CSV: Redirected IOPS	Number	Rate at which read and write operations were redirected to a volume through the network.

Volume Cache Performance Chart

The **Volume Cache** chart displays historical statistics on read requests from the cache for the selected Cluster Shared Volume with enabled CSV Cache.



The following table includes information on predefined views and counters.

Chart View	Counter	Measurement Unit	Description
Bytes Read Rate	Cache IO Read	MB/s	Rate at which data is transferred from the volume cache during read operations.
Total Read	Cache Reads/sec	Number	Number of read operations performed in the volume cache per second.

Customizing Microsoft Hyper-V Performance Charts

You can customize performance charts to select specific objects, time intervals or performance counters to display on the charts.

Selecting Objects to Chart

By default, all performance charts display data for an infrastructure object selected in the inventory pane. You can also choose to display performance data on charts for:

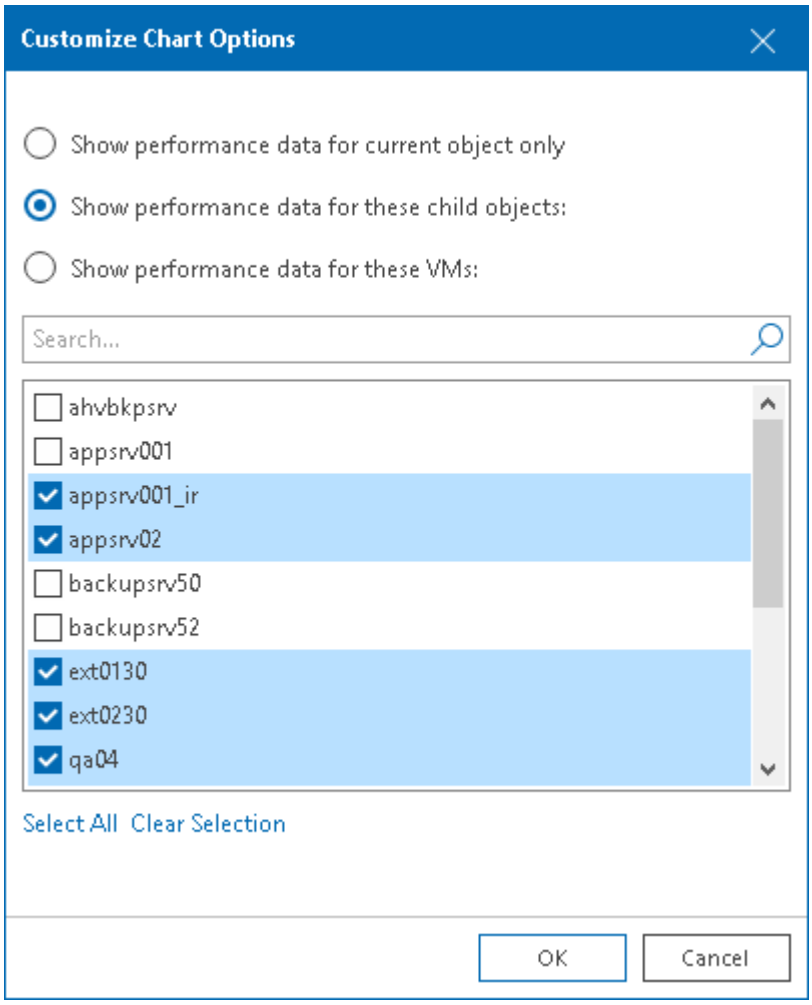
- Child components or objects of the selected virtual infrastructure object (for example, all hosts in the cluster)
- Child VMs for the selected virtual infrastructure object or segment

To display performance data for direct children of the selected virtual infrastructure object:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.
2. At the bottom of the inventory pane, click **Virtual Infrastructure**.
3. In the inventory pane, select the necessary infrastructure object.
4. Open the necessary performance chart tab.
5. From the **Chart options** list, select *Custom*.
6. In the **Customize Chart Options** window, choose **Show performance data for these child objects**.
7. Select check boxes next to child objects that should be included in the chart scope.

8. Click **OK**.



To display performance data for a set of VMs in the selected virtual infrastructure segment:

1. Open Veeam ONE Client.

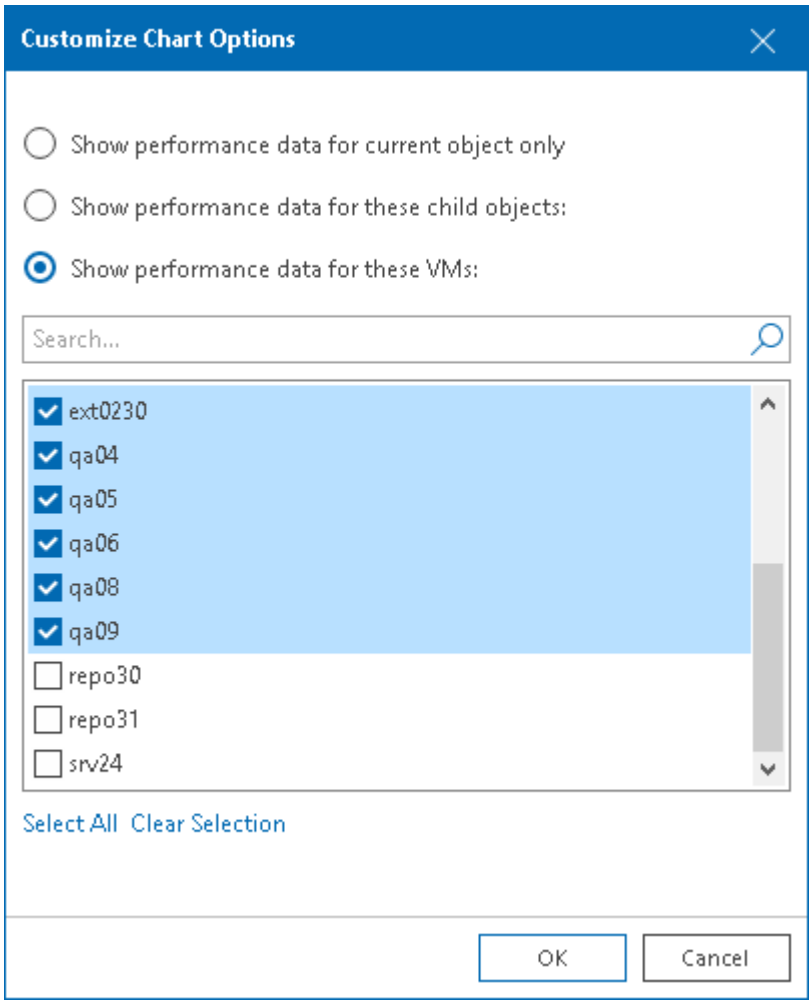
   For details, see Accessing Veeam ONE Components.

2. In the inventory pane, select the necessary infrastructure object.
3. Open the necessary performance chart tab.
4. From the **Chart options** list, select *Custom*.
5. In the **Customize Chart Options** window, choose **Show performance data for these VMs**.

   You can select both direct and indirect children (children of children) of the selected virtual infrastructure object.

6. Select check boxes next to VMs that should be included in the chart scope.

7. Click **OK**.



NOTE:

The legend pane displays objects for which data is available for the selected time interval.

Selecting Chart Views and Performance Counters

Performance charts come with a set of predefined chart views that logically group related performance counters. You can switch between chart views using the **Chart view** list at the top of the chart legend.

Instead of using predefined views, you can choose a custom set of performance counters to show on the chart:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click **Virtual Infrastructure**.
3. In the inventory pane, select the necessary infrastructure object.
4. Open the necessary performance chart.
5. In the **Chart views** list, select the *Custom* option to open the **Select Devices and Counters** window.

6. From the **Devices** list, select the necessary device(s).

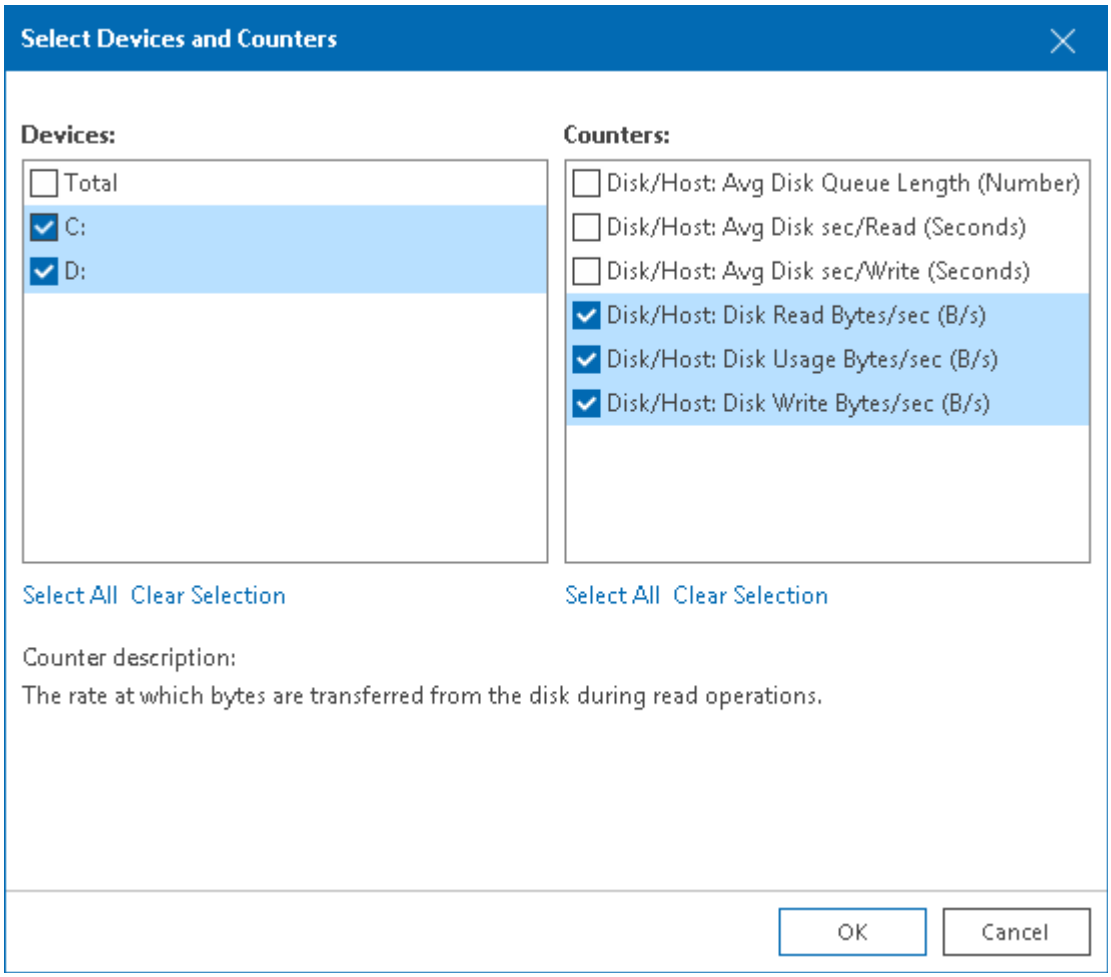
   Select *Total* to display all available devices on the chart.

> **NOTE:**
>
> The list of devices is not available for some performance charts. For example, for the **CPU** or **Memory** performance chart, you can only choose counters to display.

7. From the **Counters** list, select counters to display on the chart.

   When you select a counter, its description appears in the **Counter description** section of the window.

8. Click **OK**.



Selecting Time Interval

You can choose the time interval for which performance data on the chart will be displayed. Available options are:

- Real-time information (last hour)
- Last day
- Last week
- Last month

- Last year
- Custom time range (you can choose any time interval within the specified number of hours, days, or weeks, or specify any from/to period)

To specify a time interval for which performance data should be displayed:

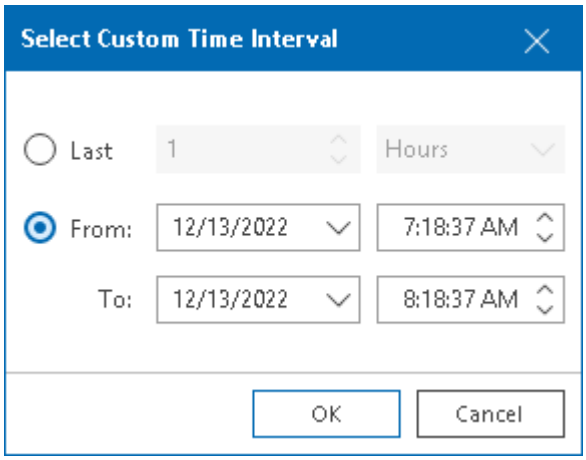
1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click **Virtual Infrastructure**.
3. In the inventory pane, select the necessary infrastructure object.
4. Open the necessary performance chart.
5. From the **Period** list, select *Last hour*, *Last day*, *Last week*, *Last month* or *Last year*.

   To define a custom time range, select *Custom*. In the **Select Custom Time Interval** window, define the necessary interval and click **OK**.

When you change the time interval, the time scale (X-axis) of the performance chart and the chart will change respectively.



Microsoft Hyper-V Tasks & Events

You can view information about events that occur in your virtual environment within the selected time interval. Veeam ONE loads information about events through the Event Viewer.

To view the list of events:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click **Virtual Infrastructure**.

3. In the inventory pane, select the necessary infrastructure object.

4. Open the **Tasks & Events** tab.

5. The **Tasks & Events** list can display up to 1000 tasks and events at a time. To find the necessary task or event, you can use the following controls:

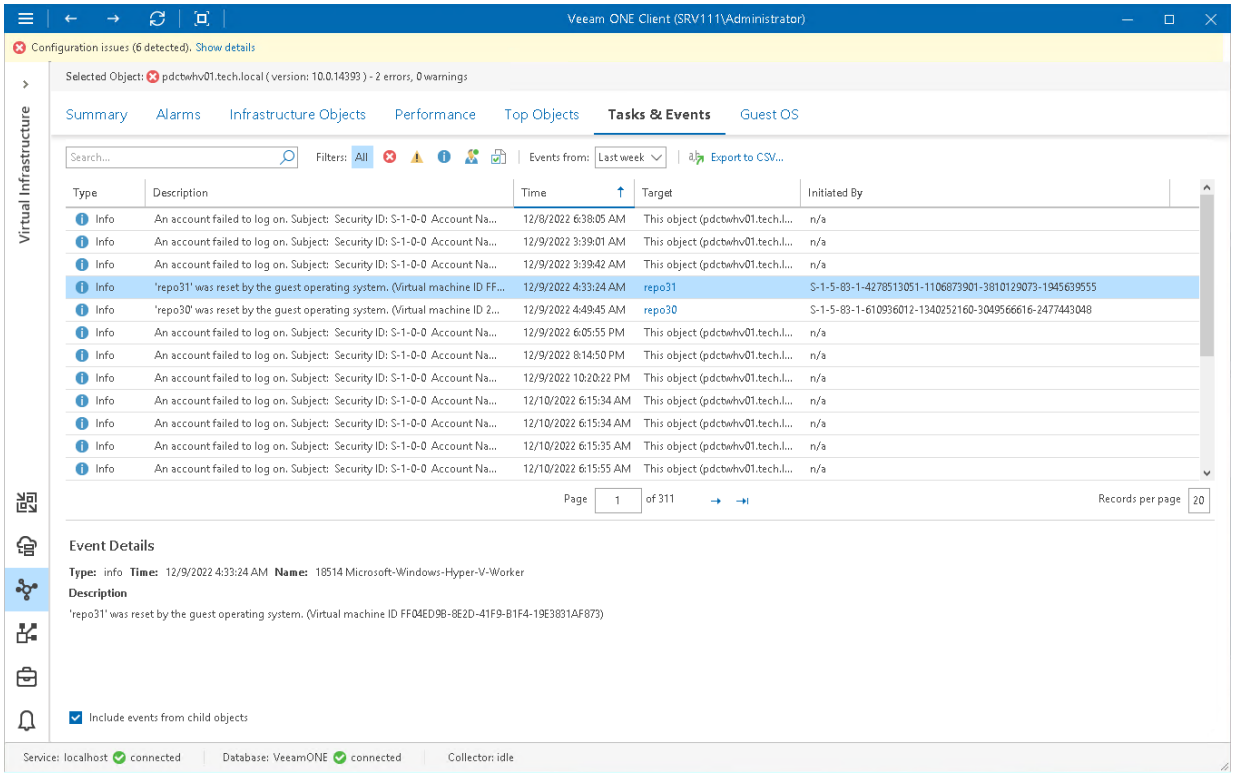
   - To display tasks or events for a specific period, select the necessary time interval from the **Events from** list.
   - To show or hide tasks or events, use filter buttons at the top of the list — *Show all events*, *Show errors*, *Show warnings*, *Show info messages*, *Show user events*, *Show tasks*.
   - To find the necessary tasks or events by description, use the **Search** field at the top of the list.

6. To view the detailed description of an event, click it in the list.

   The event description will be shown in the **Event Details** pane at the bottom.

   When you choose a virtual infrastructure container in the inventory pane, you can view events for the selected object and events for its child objects. To hide events related to child objects, clear the **Include events from child objects** check box at the bottom of the **Event Details** section.

7. To export displayed events to a CSV file, click the **Export to CSV** at the top of the list and specify the location where the file will be saved.



For every event in the list, the following details are available:

- Event type (*User*, *Info*, *Warning* or *Error*)
- Short event description
- Time of occurrence
- Event target
- Object that caused or initiated the event

Microsoft Hyper-V Virtual Machines

You can view the list of VMs within a virtual infrastructure container — on a host, on a volume, in a folder and so on.

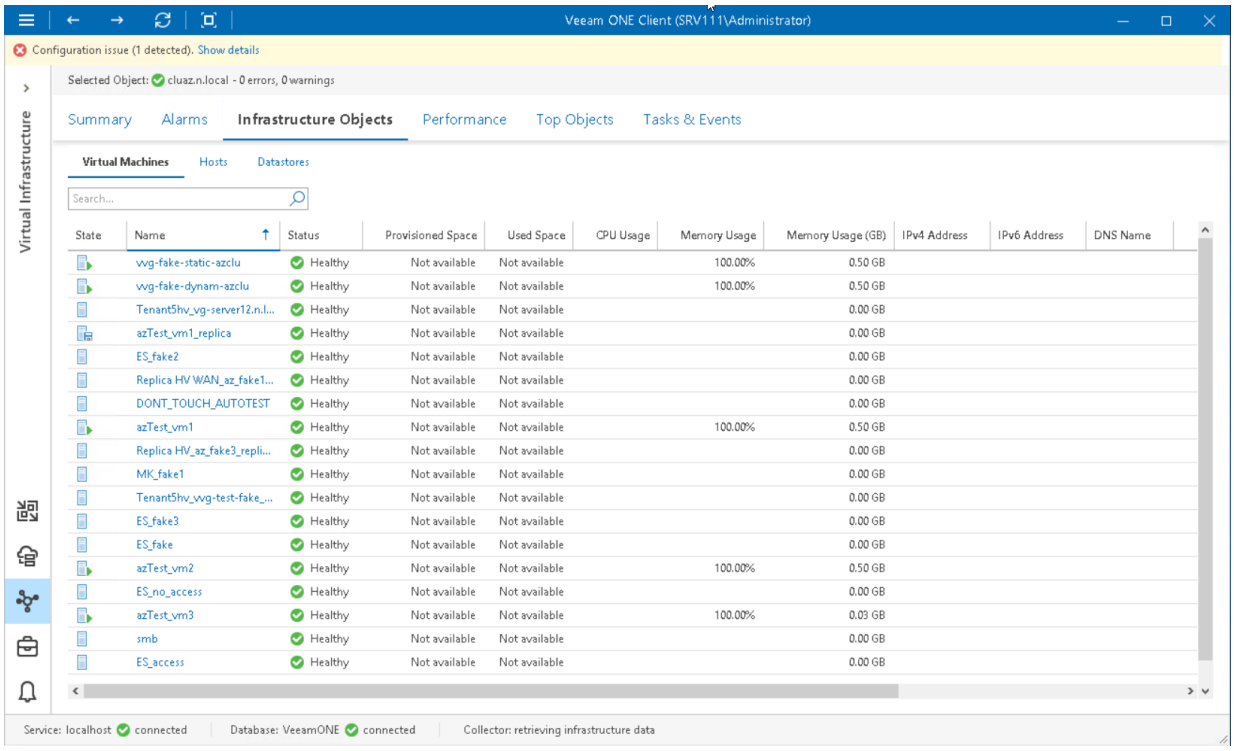
To view the list of VMs:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click **Virtual Infrastructure**.
3. In the inventory pane, select the necessary infrastructure container.
4. Open the **Infrastructure Objects** tab and navigate to **Virtual Machines**.
5. To find the necessary VM by name, use the **Search** field at the top of the list.
6. Click column names to sort VMs by a specific parameter.

   For example, to view what VMs are consuming the greatest amount of memory, you can sort VMs in the list by **Memory Usage**.



For every virtual machine in the list, the following details are available:

- **State** — state of the virtual machine (*powered on*, *powered off*, *saved*, *paused*)
- **Name** — name of the virtual machine
- **Status** — current status of the virtual machine in terms of alarms (*healthy*, *warning* or *error*)
- **Host** — name of the host where the virtual machine resides
- **Provisioned Space** — amount of storage space provisioned for the virtual machine

- **Used Space** — amount of storage space actually used for storing virtual machine files (for VMs with thin provisioned disks, this value is normally less than Provisioned Space)
- **CPU Usage** — amount of actively used virtual CPU as a percentage of total available CPU resources
- **Memory Usage** — amount of actively used memory resources as a percentage of configured VM memory
- **Memory Usage (GB)** — amount of actively used memory resources in GB
- **IP V4 Address** — IP V4 address assigned to the virtual machine
- **IP V6 Address** — IP V6 address assigned to the virtual machine
- **DNS Name** — DNS name of the virtual machine
- **vCPU** — number of virtual CPUs configured for the virtual machine
- **Assigned Memory** — amount of virtual memory allocated for the virtual machine
- **Guest OS** — guest operating system installed in the virtual machine
- **Integration Services** — number and state of Hyper-V Integration Services installed in the guest OS

You can choose what columns to show or hide in the **Virtual Machines** table:

- To hide one or more columns, right-click the table header and clear check boxes for corresponding data fields.
- To make hidden columns visible, right-click the table header and select check boxes for corresponding data fields.

Microsoft Hyper-V Hosts

You can view the list of Microsoft Hyper-V hosts in your virtual infrastructure — on System Center Virtual Machine Manager or in a cluster.

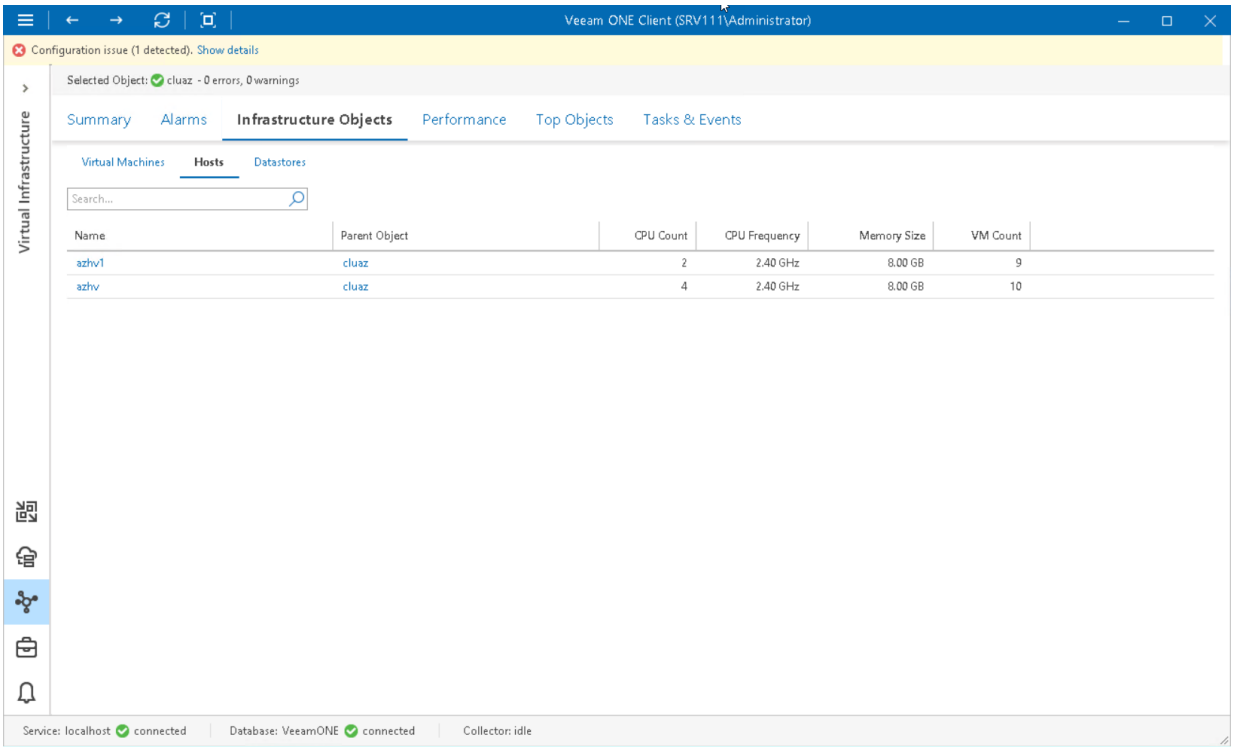
To view the list of hosts:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click **Virtual Infrastructure**.
3. In the inventory pane, select the necessary infrastructure container.
4. Open the **Infrastructure Objects** tab and navigate to **Hosts**.
5. To find the necessary host by name, use the **Search** field at the top of the list.
6. Click column names to sort hosts by a specific parameter.

   For example, to view hosts with the greatest number of VMs, you can sort VMs in the list by **VM Count**.



For every host in the list, the following details are available:

- **Name** — name of the host
- **Parent Object** — name of the parent object in the infrastructure
- **CPU Count** — number of CPU cores on a host
- **CPU Frequency** — frequency of a host CPU core in GHz
- **Memory Size** — amount of physical memory available on a host
- **VM Count** — number of VMs that reside on a host

You can choose what columns to show or hide in the **Hosts** table:

- To hide one or more columns, right-click the table header, and clear check boxes next to the corresponding data fields.
- To make hidden columns visible, right-click the table header, and select check boxes next to the corresponding data fields.

Microsoft Hyper-V Datastores

You can view the list of datastores in your Microsoft Hyper-V infrastructure — on System Center Virtual Machine Manager or in a cluster.

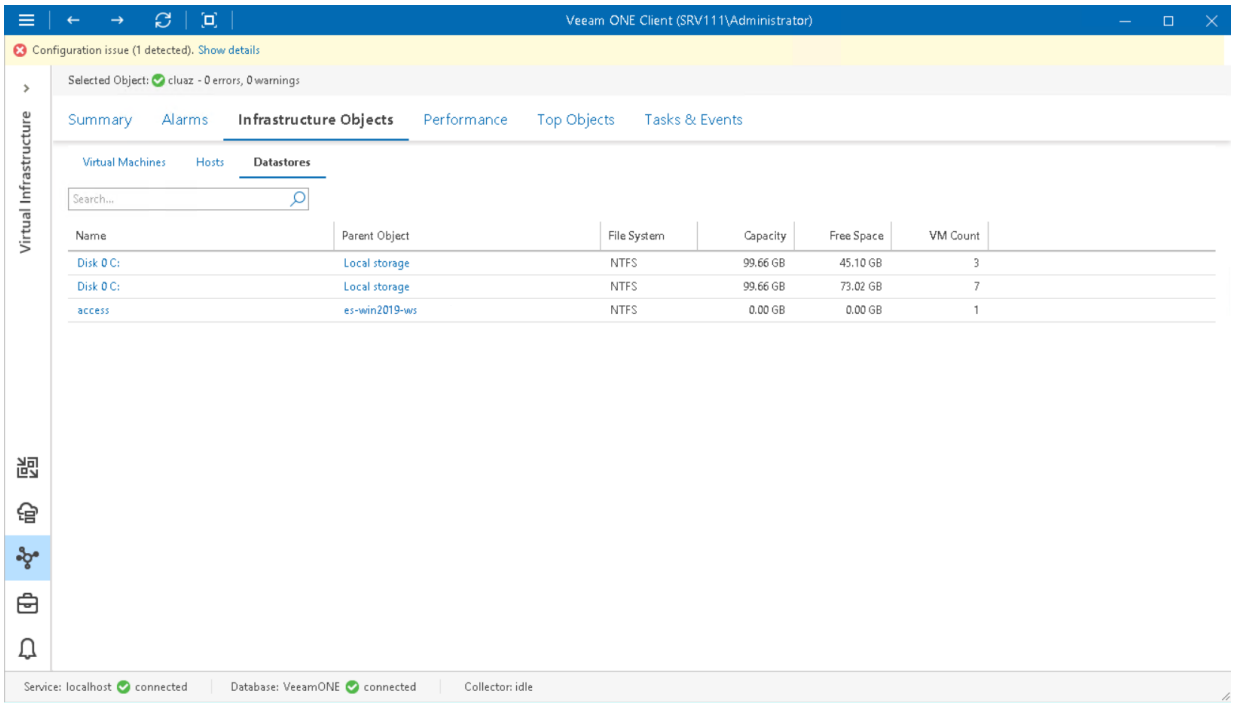
To view the list of datastores:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click **Virtual Infrastructure**.
3. In the inventory pane, select the necessary infrastructure container.
4. Open the **Infrastructure Objects** tab and navigate to **Datastores**.
5. To find the necessary datastore by name, use the **Search** field at the top of the list.
6. Click column names to sort datastores by a specific parameter.

   For example, to view what datastores have the greatest amount of free space, you can sort datastores in the list by **Free Space**.



For every datastore in the list, the following details are available:

- **Name** — name of a datastore
- **Parent Object** — name of the parent object in the infrastructure
- **File System** — type of the file system on the datastore
- **Capacity** — total capacity of a datastore
- **Free Space** — amount of available free space on a datastore
- **VM Count** — number of VMs that reside on a datastore

You can choose what columns to show or hide in the **Datastores** table:

- To hide one or more columns, right-click the table header, and clear check boxes next to the corresponding data fields.
- To make hidden columns visible, right-click the table header, and select check boxes next to the corresponding data fields.

Microsoft Hyper-V Top Objects

The top and lowest load dashboards help you detect VMs and hosts consuming the greatest or the smallest amount of resources in the selected virtual infrastructure segment.

- **Top Hyper-V VMs** dashboard displays top VM consumers in terms of CPU, memory, storage, network usage, snapshot age and size.
- **Top Hyper-V Hosts** dashboard displays top hosts in terms of CPU, memory, disk and network usage.
- **Bottom Hyper-V Hosts** dashboard displays least loaded hosts in terms of CPU, memory, disk and network resource usage.

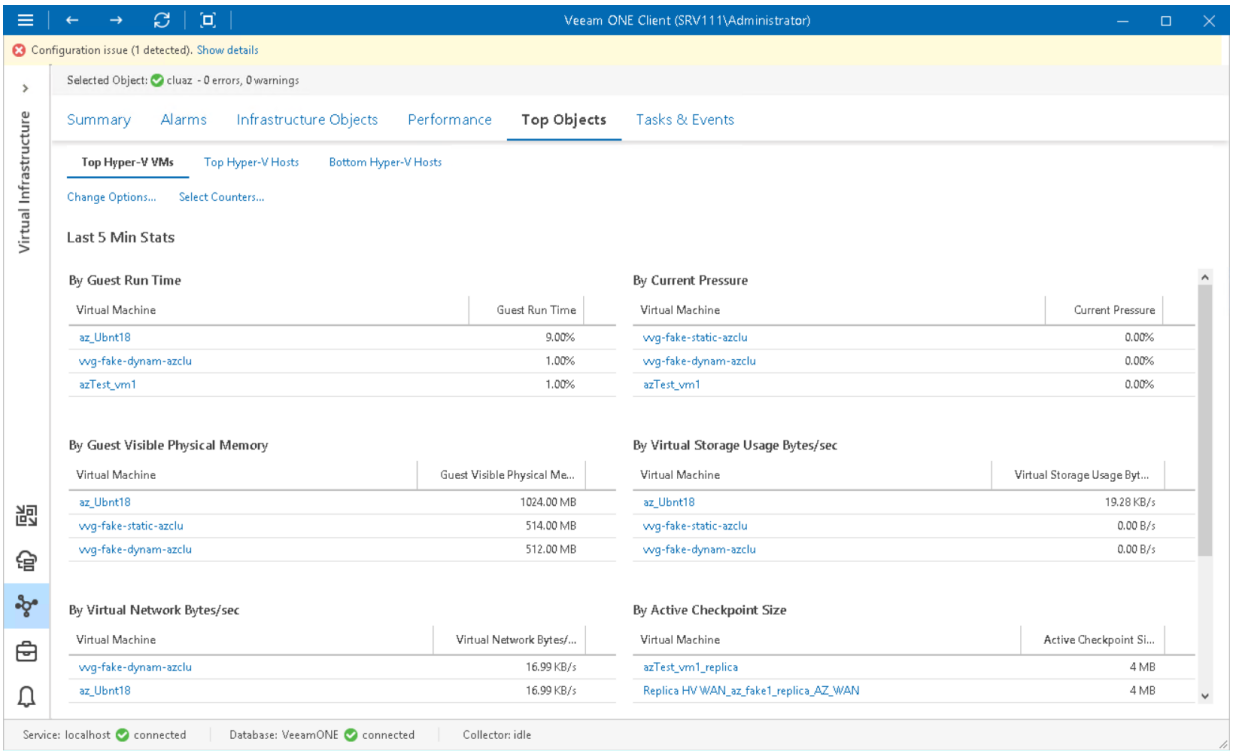
  You can use this dashboard to choose hosts where you can deploy new VMs or to which you can move existing VMs.

To detect the most or least loaded hosts or VMs:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.
2. At the bottom of the inventory pane, click **Virtual Infrastructure**.
3. In the inventory pane, select the necessary infrastructure container.
4. Open the **Top Objects** tab and navigate to necessary dashboard — **Top Hyper-V VMs**, **Top Hyper-V Hosts** or **Bottom Hyper-V Hosts**.
5. Click the **Change Options** link in the top left corner of the dashboard.
   - In the **Interval** field, set the time interval for which resource utilization statistics must be analyzed.
   - In the **VMs to display/Hosts to display** field, define the number of objects to display on the dashboard.
6. Click the **Select Counters** link in the top left right corner of the dashboard.
   a. In the **Select counters** window, choose metrics that must be included in the dashboard. Press and hold the `[SHIFT]` or `[CTRL]` key on the keyboard to select multiple counters.

b. Click **OK**.


Veeam ONE Client (SRV111\Administrator)
Configuration issue (1 detected). Show details
Selected Object: cluaz - 0 errors, 0 warnings
Summary
Alarms
Infrastructure Objects
Performance
Top Objects
Tasks & Events
Virtual Infrastructure
Top Hyper-V VMs
Top Hyper-V Hosts
Bottom Hyper-V Hosts
Change Options...
Select Counters...
Last 5 Min Stats
By Guest Run Time
Virtual Machine
Guest Run Time
az_Ubnt18
9.00%
vvg-fake-dynam-azclu
1.00%
azTest_vm1
1.00%
By Current Pressure
Virtual Machine
Current Pressure
vvg-fake-static-azclu
0.00%
vvg-fake-dynam-azclu
0.00%
azTest_vm1
0.00%
By Guest Visible Physical Memory
Virtual Machine
Guest Visible Physical Me...
az_Ubnt18
1024.00 MB
vvg-fake-static-azclu
514.00 MB
vvg-fake-dynam-azclu
512.00 MB
By Virtual Storage Usage Bytes/sec
Virtual Machine
Virtual Storage Usage Byt...
az_Ubnt18
19.28 KB/s
vvg-fake-static-azclu
0.00 B/s
vvg-fake-dynam-azclu
0.00 B/s
By Virtual Network Bytes/sec
Virtual Machine
Virtual Network Bytes/...
vvg-fake-dynam-azclu
16.99 KB/s
az_Ubnt18
16.99 KB/s
By Active Checkpoint Size
Virtual Machine
Active Checkpoint Si...
azTest_vm1_replica
4 MB
Replica HV WAN_az_fake1_replica_AZ_WAN
4 MB
Service: localhost connected
Database: VeeamONE connected
Collector: idle

Microsoft Hyper-V VM Console

From within the VM console, you can easily isolate the root cause of VM performance problems and execute management tasks — for example, restart an unresponsive VM.

This option requires no additional software installed on the Veeam ONE server and is available for both Window-based and Linux-based OS's.

Prerequisites

To access the console of a Linux-based VM, you must download PuTTY.exe and provide path to it in Veeam ONE Client client settings.

Accessing VM Console

You can access the VM console right from the Veeam ONE Client interface:

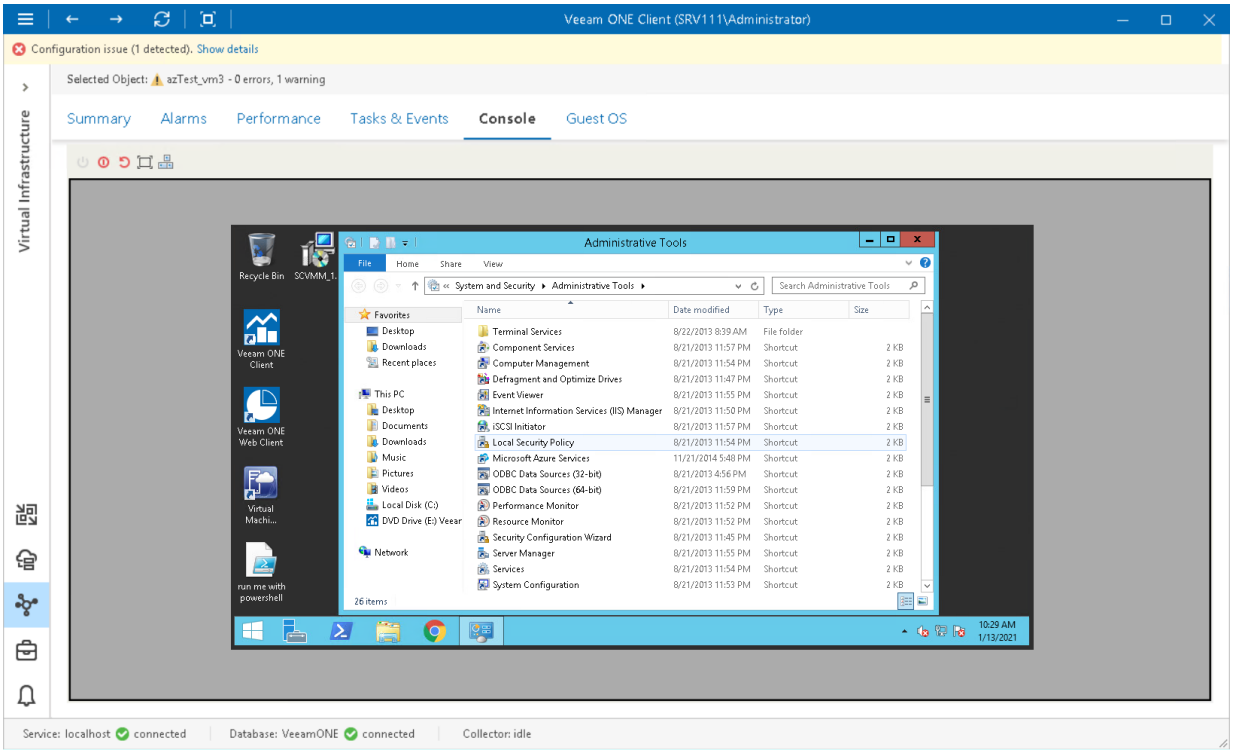
1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click **Virtual Infrastructure**.

3. In the inventory pane, select the necessary VM.

4. Open the **Console** tab.



You can use buttons at the top of the **Console** tab to change the VM power state:

- **Power on** — powers on a VM if it is powered off. Resumes a VM if it is paused.
- **Power off** — shuts down the guest OS and powers off a VM.

- **Hard reset** — resets a VM without waiting for the guest OS and VM processes to stop. It is recommended to use this option only if you want to reboot a stuck or unresponsive VM.
- **Full screen** — switches between the full screen mode and a separate window running the VM console.
- **Send Ctrl+Alt+Del** — sends the **[Ctrl+Alt+Del]** command to a VM.

To access the VM console or change the VM power state, you can also right-click the VM in the inventory pane and use one of the following shortcut menu commands:

- To access the VM using Windows Remote Desktop Connection, choose **Remote Management > Connect to VM**.
- To change the VM power state, choose **Remote Management** and click the necessary command.
- To send the [Ctrl+Alt+Del] command to the VM, choose **Send Ctrl+Alt+Del**. Note that this command is only available if the **VM Console** tab is active.

Microsoft Hyper-V In-Guest Processes

You can view and control processes that are currently running inside a virtual machine or host.

- On Windows-based machines, you can view, end or restart processes.
- On Linux-based machines, you can view or end daemons.

Prerequisites

For Linux-based machines, make sure that the SSH Server is started.

Viewing In-Guest Processes

To view the list of processes:

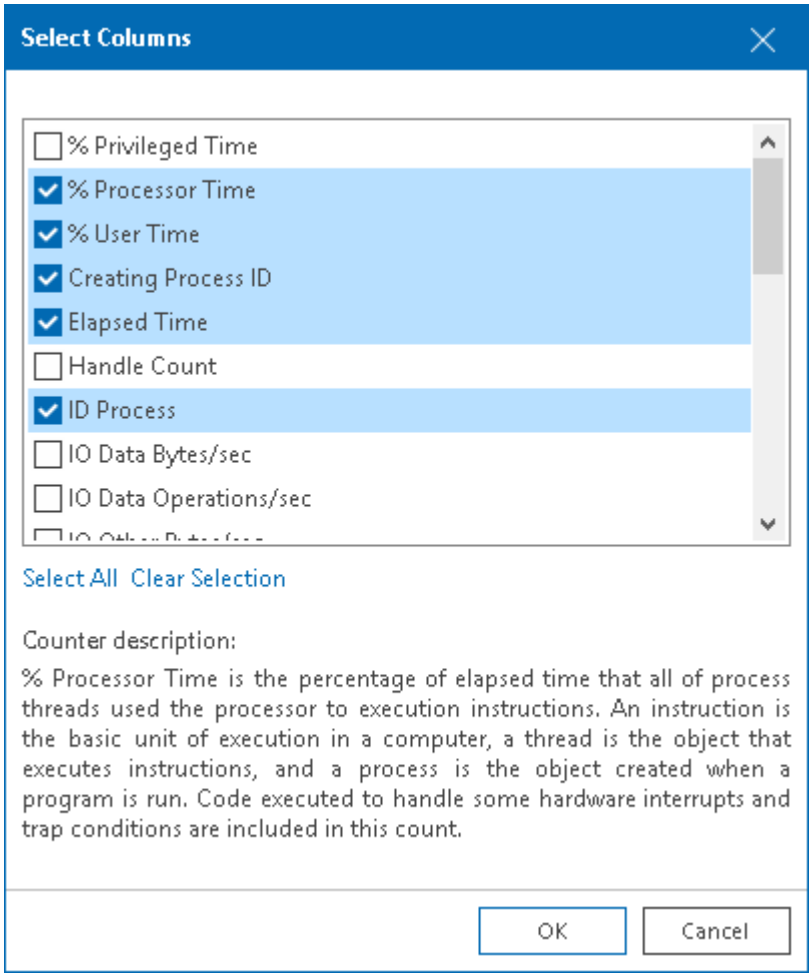
1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.
2. At the bottom of the inventory pane, click **Virtual Infrastructure**.
3. In the inventory pane, select the necessary infrastructure object.
4. Open the **Processes** tab.
5. Provide OS authentication credentials (user name and password) to access the list of running processes.

Every process is described with a set of counters that are presented as column headings. You can add or remove counters to monitor running processes:

1. In the upper right corner of the **Processes** dashboard, click the **Select columns** link.
2. In the **Select Columns** window, select check boxes next to counters you want to display.

3. To view a detailed description of a counter, click it in the **Counters** list, and the description will be displayed in the lower pane of the window.



You can end unwanted processes running on the VM or create an alarm based on the process state or object performance:

- [For Windows-based machines] To end a process, select it in the list and click the **Kill Process** button, or right-click a necessary process and select **Kill Process** from the shortcut menu.
- [For Linux-based machines] To end a daemon, select it in the list and click the **Kill Process** button and choose one of the following options:
  - **Hangup** — to send the `SIGHUP` signal
  - **Kill** — to send the `SIGKILL` signal
  - **Terminate** — to send the `SIGTERM` signal

  You can also right-click a necessary process and select **Kill Process** and choose the necessary option from the shortcut menu.
- [For Windows-based machines] To create an alarm, select one or more processes in the list, click the **Create Alarm** button, and select the type of rule on which the alarm must be based. For more information, see Alarm Rules Reference.

Microsoft Hyper-V In-Guest Services

You can view and control services currently running inside a VM.

- For Windows-based machines, you can view, start, stop and restart services, and create alarms based on retrieved services.
- For Linux-based machines, you can view, start, stop and restart services.

Prerequisites

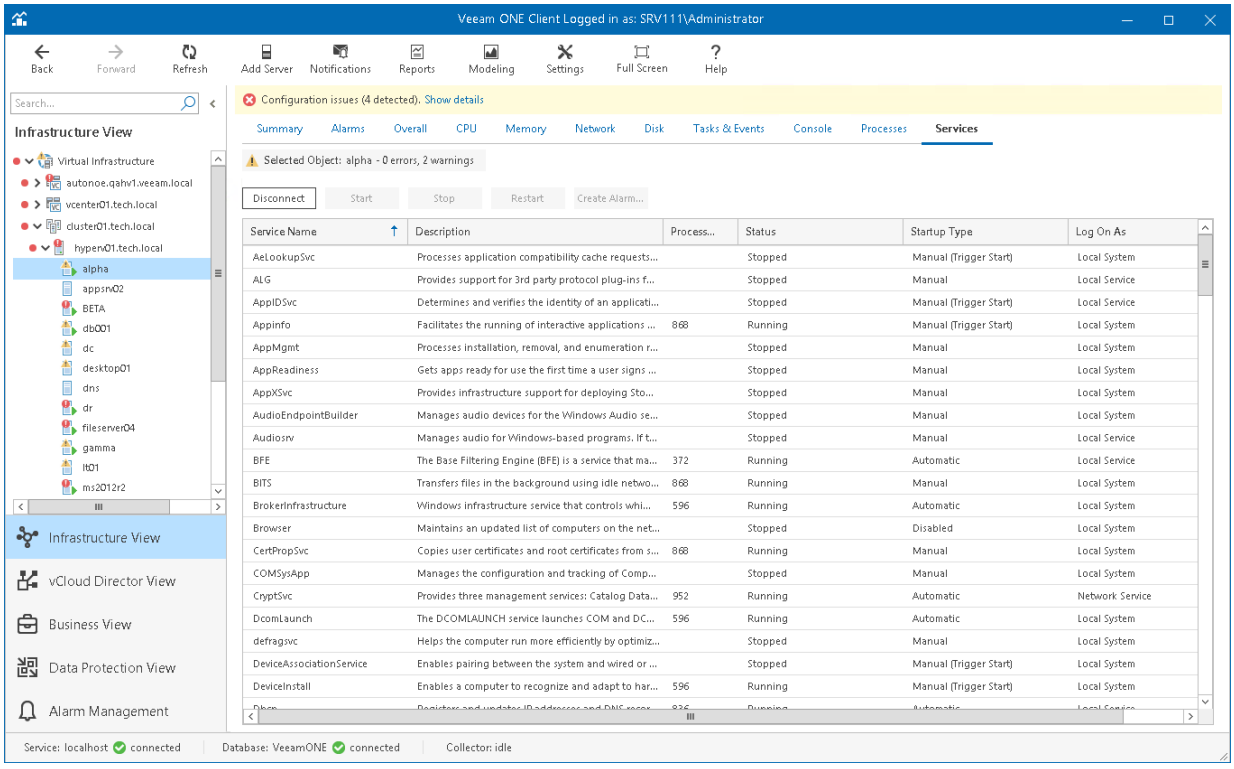
For Linux-based machines, make sure that the SSH Server is started.

Viewing In-Guest Services

To view the list of services:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.
2. At the bottom of the inventory pane, click **Virtual Infrastructure**.
3. In the inventory pane, select the necessary infrastructure object.
4. Open the **Services** tab.
5. Provide OS authentication credentials (user name and password) to access the list of running services.



You can start, stop and restart a running service, or create an alarm based on the service state or object performance:

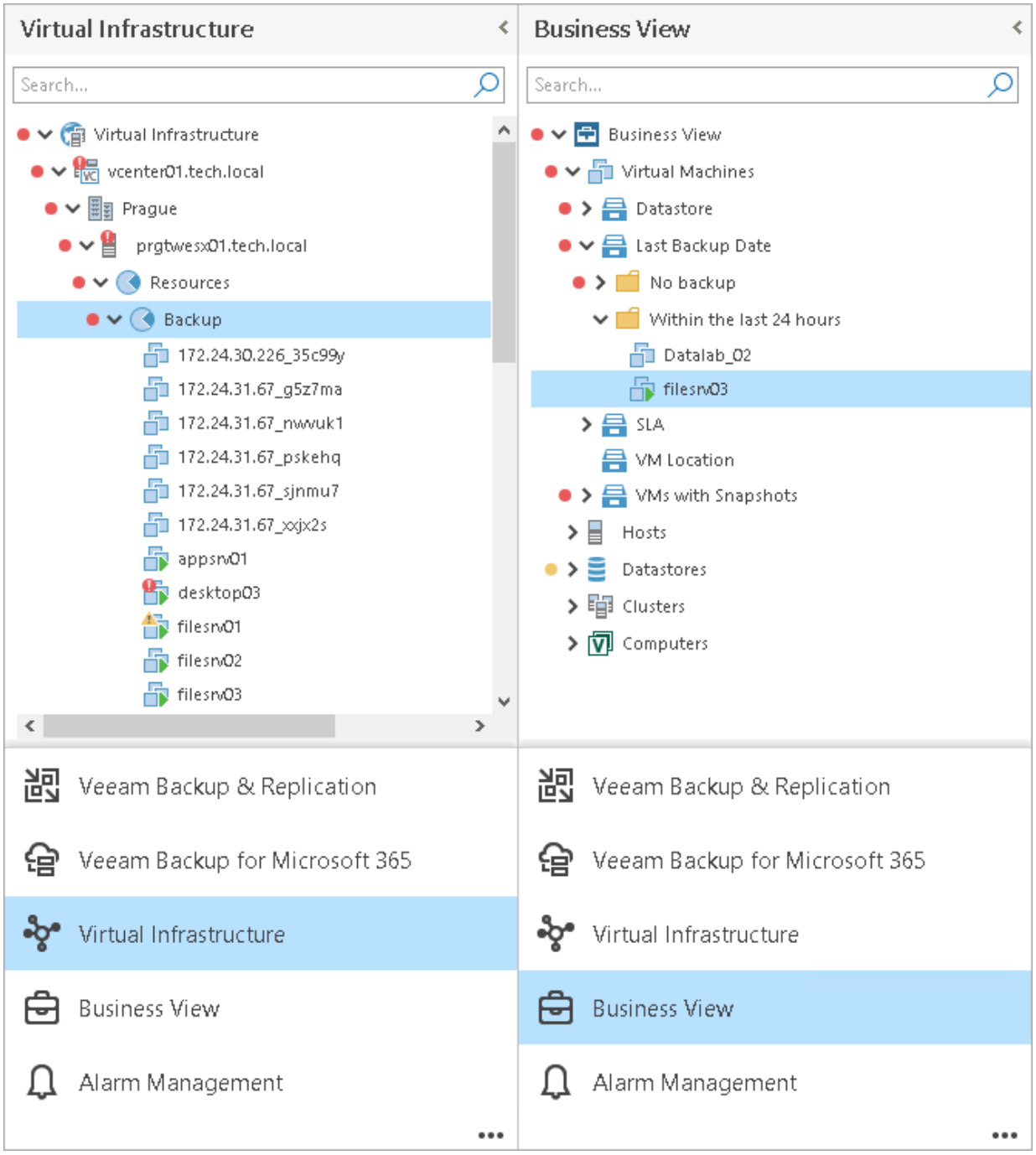
- To restart a service, click the **Restart** button, or right-click a necessary service and select **Restart** from the shortcut menu.
- To disconnect from guest OS, click the **Disconnect** button.
- [For Windows-based machines] To create an alarm, select a service in the list, click the **Create Alarm** button, and select the type of rule on which the alarm must be based. For more information, see Alarm Rules Reference.

Business View

Veeam ONE Client can present your virtual infrastructure from the technical perspective (in terms of VMware vSphere or Microsoft Hyper-V inventory), and from the business perspective (based on your company needs and priorities). Veeam ONE Client presents infrastructure objects from the business perspective using categorization capabilities provided by the embedded Business View component.

Business View allows you to categorize virtual and backup infrastructure objects — VMs, hosts, clusters, datastores, enterprise applications and computers protected with Veeam backup agents — according to constructs of your business. You can categorize virtual infrastructure objects by such criteria as business unit, department, purpose, SLA and others. Categorization data is continuously synchronized with Veeam ONE Client and Veeam ONE Web Client, and enables you to monitor, troubleshoot, resolve issues and report on business groups of infrastructure objects. For details on creating categories and groups for the objects in your infrastructure, see Configuring Categorization Model.

To work with the business view of your infrastructure in Veeam ONE Client, click **Business View** at the bottom of the inventory pane. In this view, you can use monitoring capabilities for business groups created for your virtual environment. For details on monitoring capabilities for Business View groups, see Business View Monitoring.



Configuring Categorization Model

To present the virtual infrastructure, Veeam ONE Client uses the model that includes categories, groups and objects:

- **Category** is a logical division or a sector of the infrastructure. Each category includes one or more groups.

  Categories can be static or dynamic:

  - **Static** categories include a user-defined number of groups. You can manually create groups that Veeam ONE will populate each time data collection runs.
  - **Dynamic** categories can include one or more groups that Veeam ONE creates and populates automatically each time data collection runs.

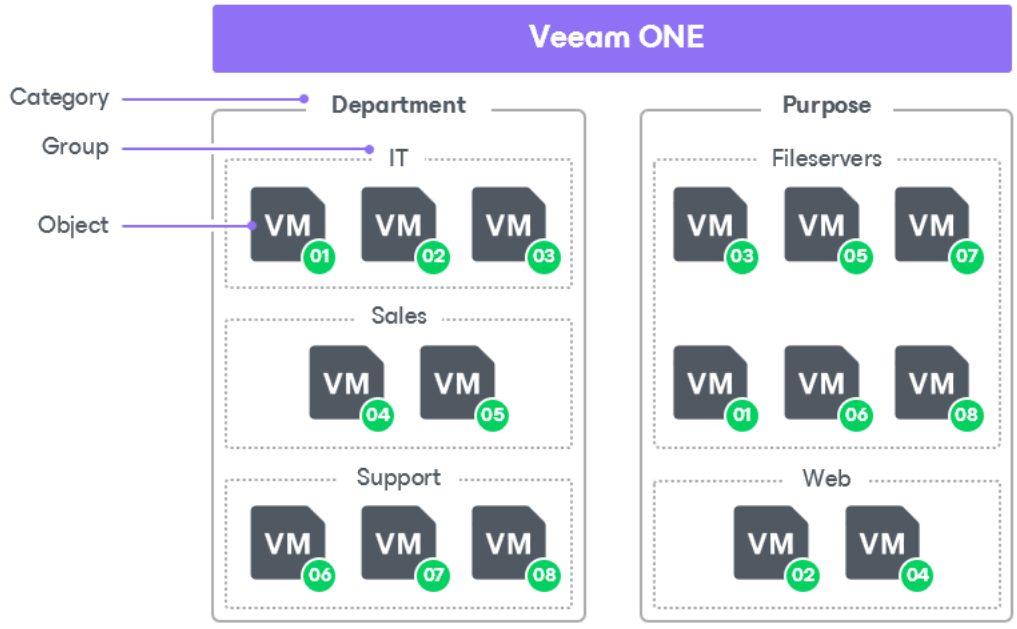
- **Group** is a collection of infrastructure objects that share same characteristics, or match same criteria. You can think of a group as a tag assigned to an object.

  Each group includes one or more objects.

- **Objects** are categorized elements of the infrastructure.

  In Veeam ONE Client you can categorize the following types of objects: clusters, hosts, storage objects, VMs, computers protected with Veeam backup agents and enterprise applications. You can include an object into one or more groups within a category.

The following picture illustrates an example of Veeam ONE categorization model.



In the example above, the categorization model includes categories *Department* and *Purpose*.

- *Department* category includes groups *IT*, *Sales* and *Support*
- *Purpose* category includes groups *Fileservers* and *Web*

Virtual machines numbered 1-8 are included in groups within both categories.

Predefined Categories

Out of the box, Veeam ONE Client comes with a number of predefined categories:

- **Datastore** — dynamically groups VMs by datastore where VM files reside.
- **Location** — dynamically groups by location computers managed by Veeam Backup & Replication.
- **Last Backup Date** — dynamically groups VMs, computers and enterprise applications by the age of the latest restore point.
- **SLA** — category with static groups for all types of virtual infrastructure objects. Includes two predefined groups: *Mission Critical* and *Other*.
- **Storage Type** — dynamically groups storage objects by type.
- **VM Location** — dynamically groups by location VMs protected with Veeam Backup & Replication.
- **VMs with Snapshots** — dynamically groups VMs with snapshots by the snapshot age.

You can use predefined categories for your categorization model. If predefined categories are not enough, you can create custom categories and edit predefined categories or import an existing categorization model.

Creating Business View Categories and Groups

To categorize objects into groups automatically, you can use the following methods:

- Configuring Single-Parameter Categorization — the method that allows you to configure dynamic categories. Veeam ONE will create groups automatically based on the values of a single property of an object.
- Configuring Multiple-Condition Categorization — the method that allows you to configure static categories and create groups manually by combining multiple object properties and logical operators.
- Configuring Categorization Using Grouping Expressions — the method that allows you to configure dynamic categories. Veeam ONE will create groups automatically based on object properties, operators and methods included into expression.

Configuring Single-Parameter Categorization

Single-parameter categorization is based on object properties specified within a hypervisor and Veeam Backup & Replication server. When you select a property as a categorization condition, Veeam ONE automatically creates a group for each unique value of the selected property. All objects with the same property value will fall into one group.

Groups created using the single property method have dynamic membership. If the property value changes, the object can be moved into another group or excluded from categorization when the next data collection runs.

For example, you can categorize VMs based on their power state. After data collection, Veeam ONE will create three groups: **Powered On**, **Powered Off** and **Suspended**. If a VM power state changes, this VM will be moved into another group next time data collection runs.

To categorize objects using a single property:

1. Open Veeam ONE Client.

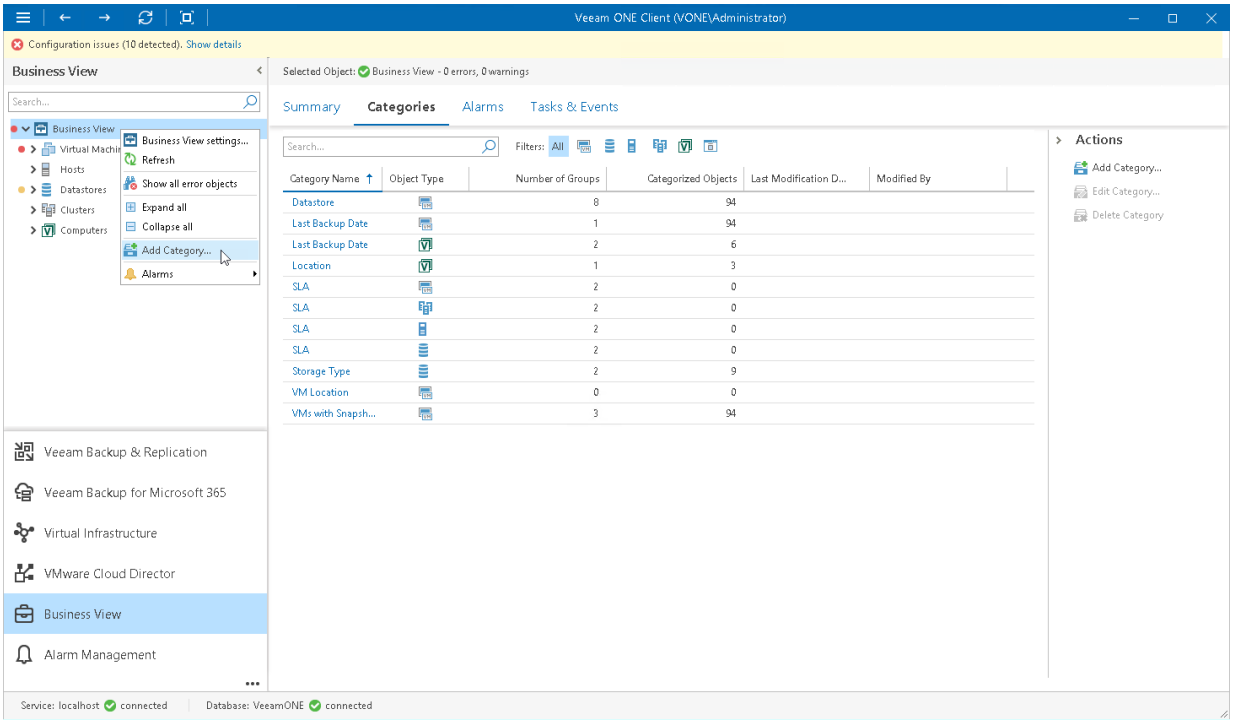
   For details, see Accessing Veeam ONE Components.

2. In the inventory pane, navigate to the **Business View** node.
3. Launch the **Categorization Wizard**:

   a. In the information pane, switch to the **Categories** tab.

b. In the **Actions** pane, click **Add Category**.

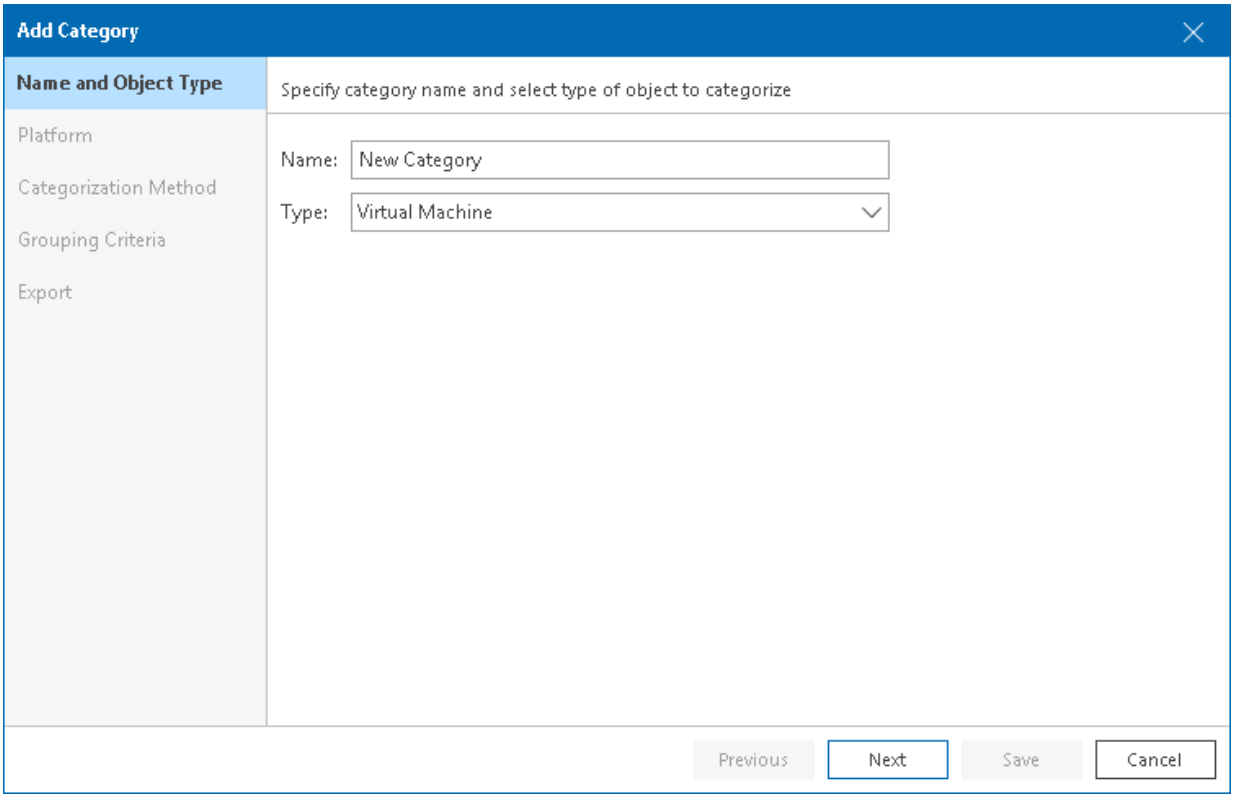
Alternatively, in the **Business View** tree, right-click the main node and select **Add Category**.



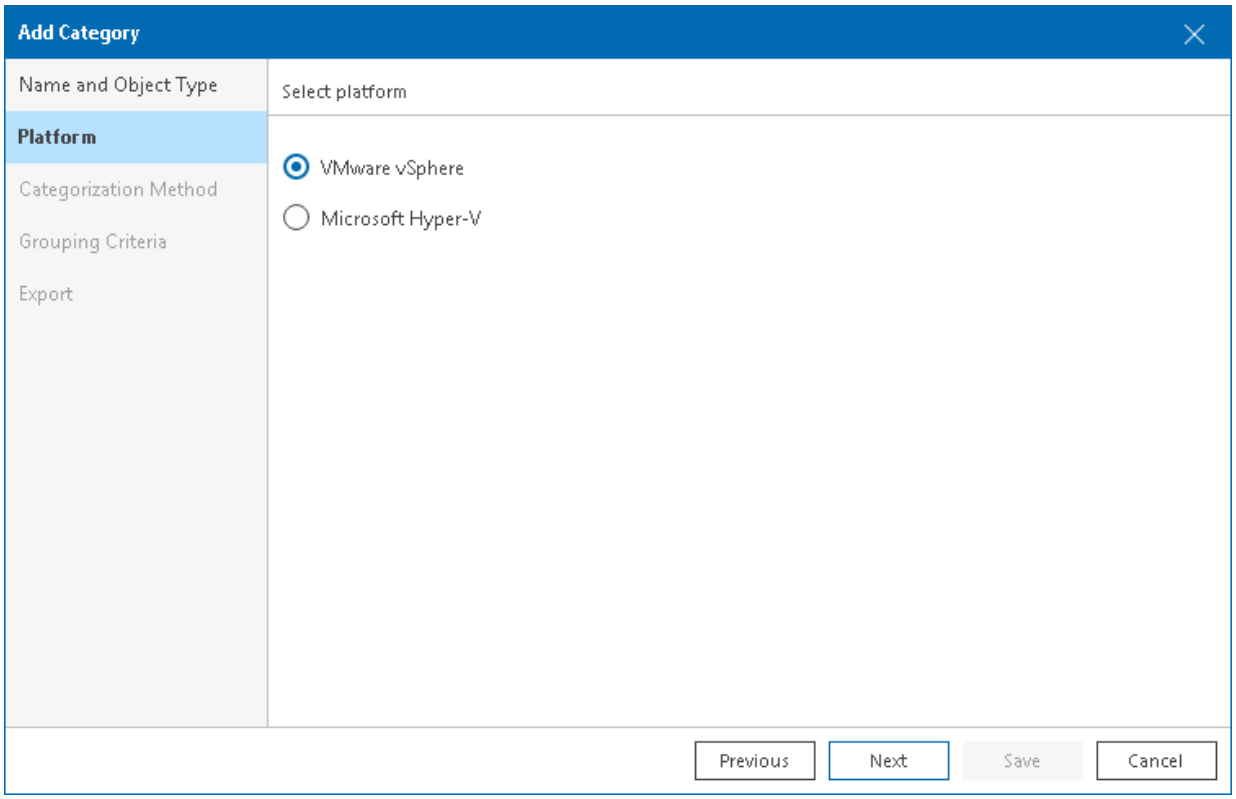
4. At the **Name and Object Type** step of the wizard, enter a category name and select an object type.

   You can select the following types of objects: *Virtual Machine*, *Host*, *Cluster*, *Storage*, *Computer*, *Enterprise Application*.

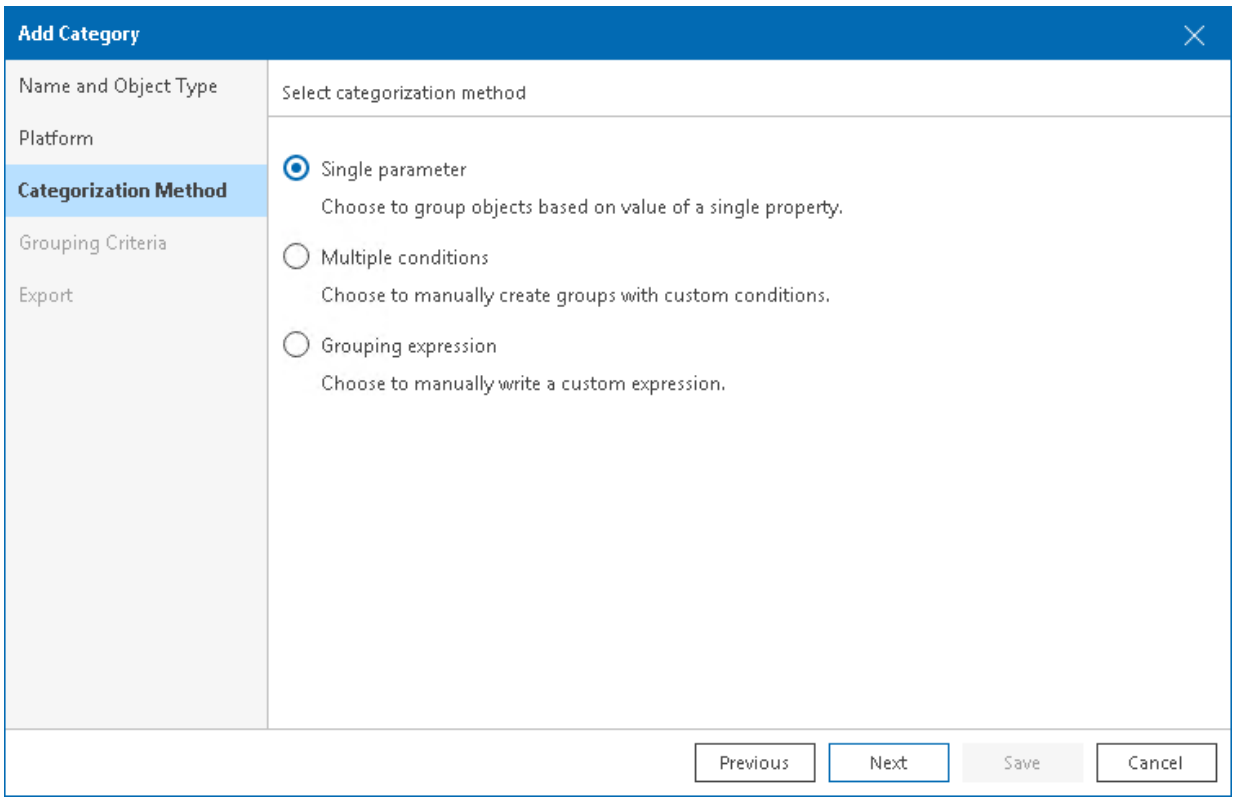
   If you select the *Computer* or *Enterprise Application* object type, continue with step 6 of this procedure.



5. At the **Platform** step of the wizard, select the platform for which you want to categorize objects: *VMware vSphere* or *Microsoft Hyper-V*.

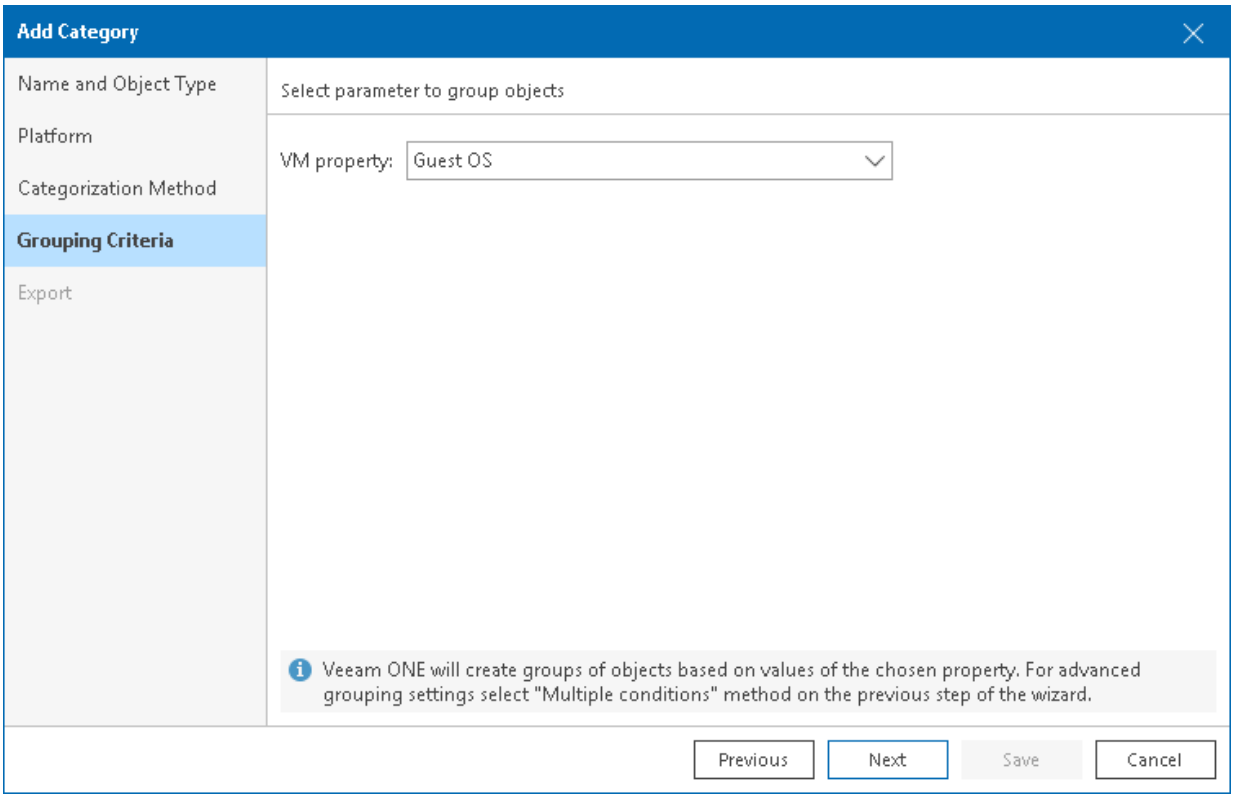


6. At the **Categorization Method** step of the wizard, select *Single parameter*.



7. At the **Grouping Criteria** step of the **Categorization Wizard**, select an object property.

   If you selected the *Computer* or *Enterprise Application* object type, click **Save** to finish working with the wizard.



8. At the **Export** step of the wizard, choose whether you want to export Business View categorization data:

   - [For VMware vSphere objects] Select **Create vSphere tags** if you want to display Business View categories and groups in vCenter Server.

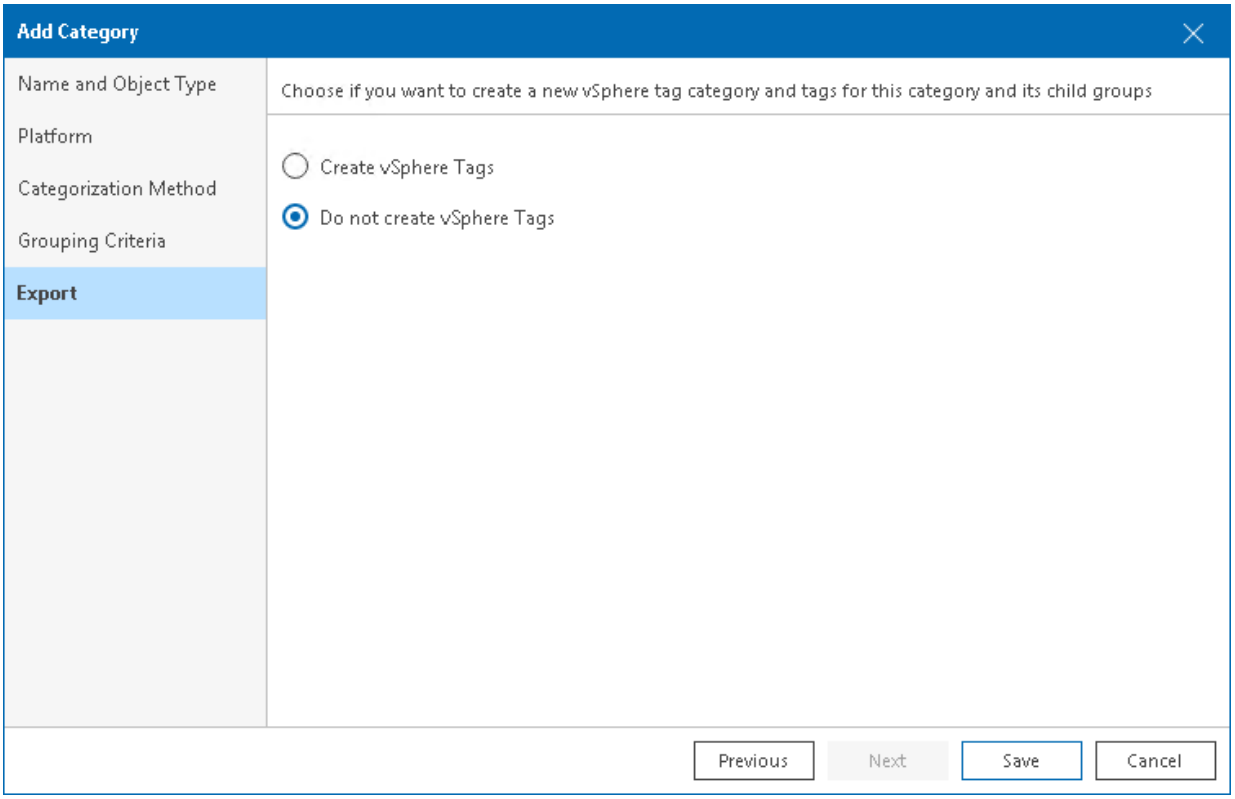
     Veeam ONE will export categories as tag categories and groups as tags.

   - [For Microsoft Hyper-V objects] Select **Create Hyper-V custom properties** if you want to display Business View categories and groups in System Center Virtual Machine Manager.

     Veeam ONE will export categories as custom properties and groups as property values.

   Veeam ONE will periodically overwrite created tags and custom properties to keep categorization data in synchronization with vCenter Server and System Center Virtual Machine Manager.

> **NOTE:**
>
> This step is not available if you enable import of categorization data from vCenter Server, System Center Virtual Machine Manager. For details on importing categorization model, see Selecting Categorization Model.



9. Click **Save**.

   Veeam ONE will create an individual group for each unique value of the selected property.

Configuring Multiple-Condition Categorization

Multiple-condition categorization allows you to combine multiple conditions that evaluate object properties for creating groups. This method makes categories highly customizable, as each group within a category can have its own condition. Conditions can be based on different object properties and logical operators. For one group, you can specify one or more conditions and link them with the **AND** and **OR** operators.

Groups created with the multiple-condition method have dynamic membership. If the property value changes, the object can be moved into another group or excluded from categorization after the next data collection.

For example, you can categorize VMs based on their power state, datacenter name and guest OS at the same time. If any of these properties change, the VM will be moved into another group or excluded from categorization.

To create groups using multiple conditions:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

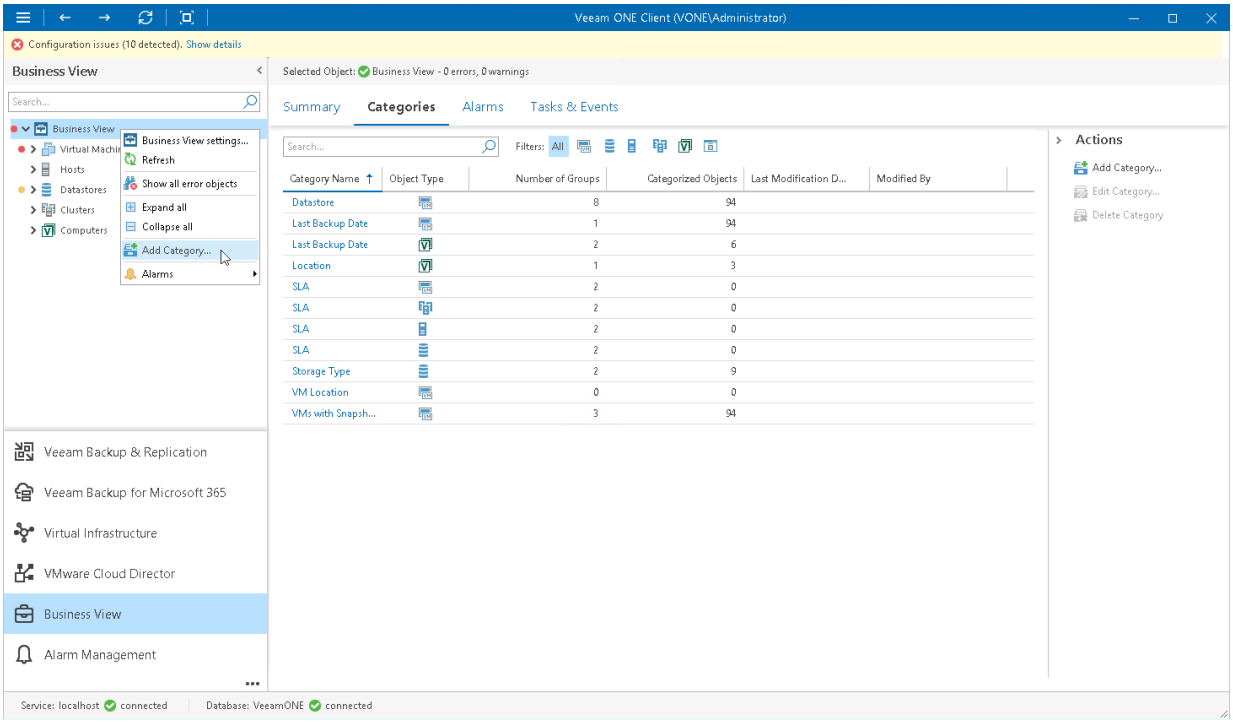
2. In the inventory pane, navigate to the **Business View** node.

3. Launch the **Categorization Wizard**:

   a. In the information pane, switch to the **Categories** tab.

b. In the **Actions** pane, click **Add Category**.

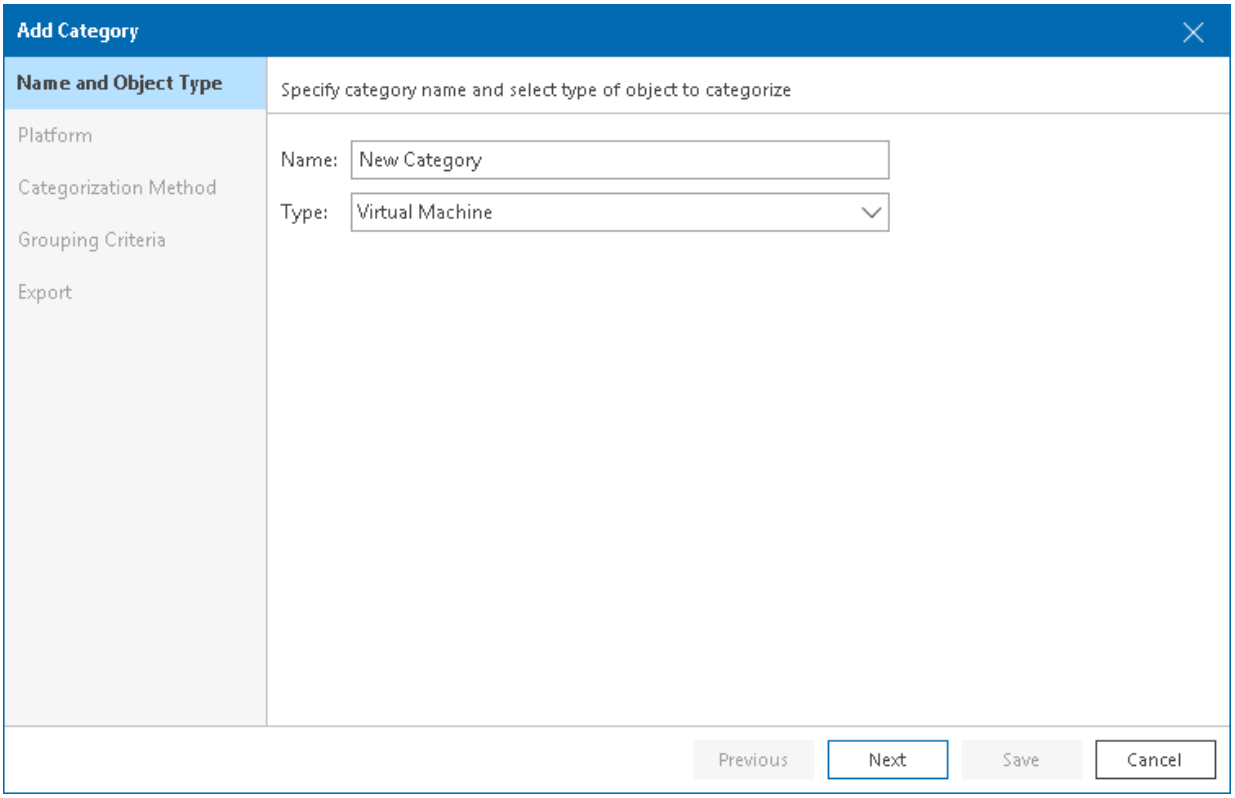
Alternatively, in the **Business View** tree, right-click the main node and select *Add Category*.



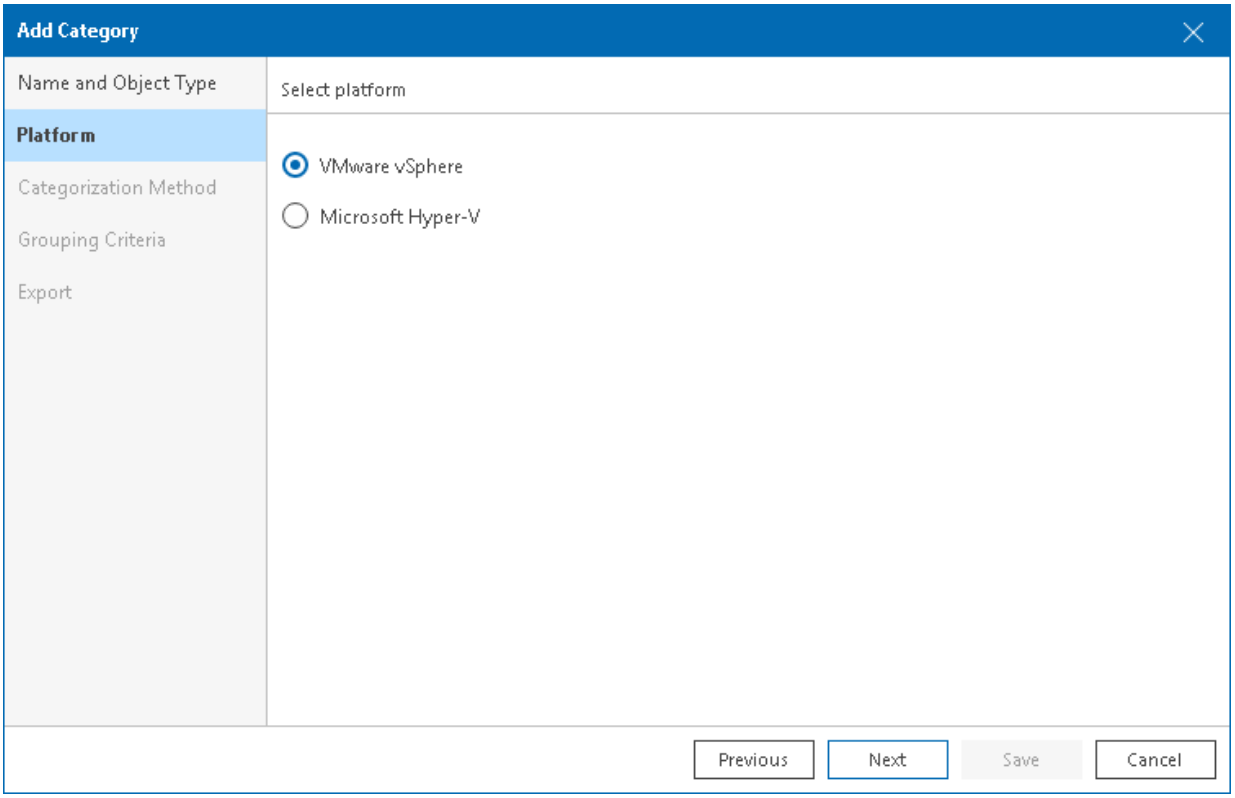
4. At the **Name and Object Type** step of the wizard, enter a category name and select an object type.

   You can select the following types of objects: *Virtual Machine*, *Host*, *Cluster*, *Storage*, *Computer*, *Enterprise Application*.

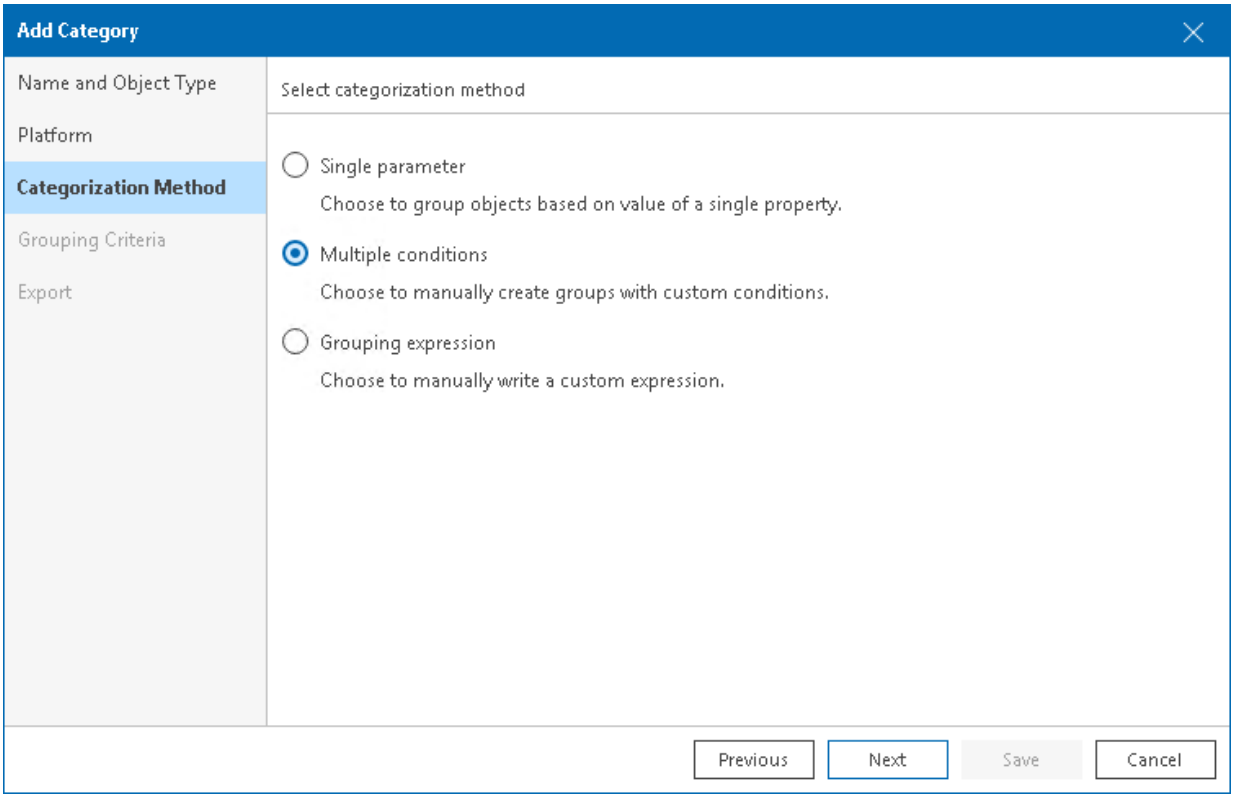
   If you select the *Computer* or *Enterprise Application* object type, continue with step 6 of this procedure.



5. At the **Platform** step of the wizard, select the platform for which you want to categorize objects.

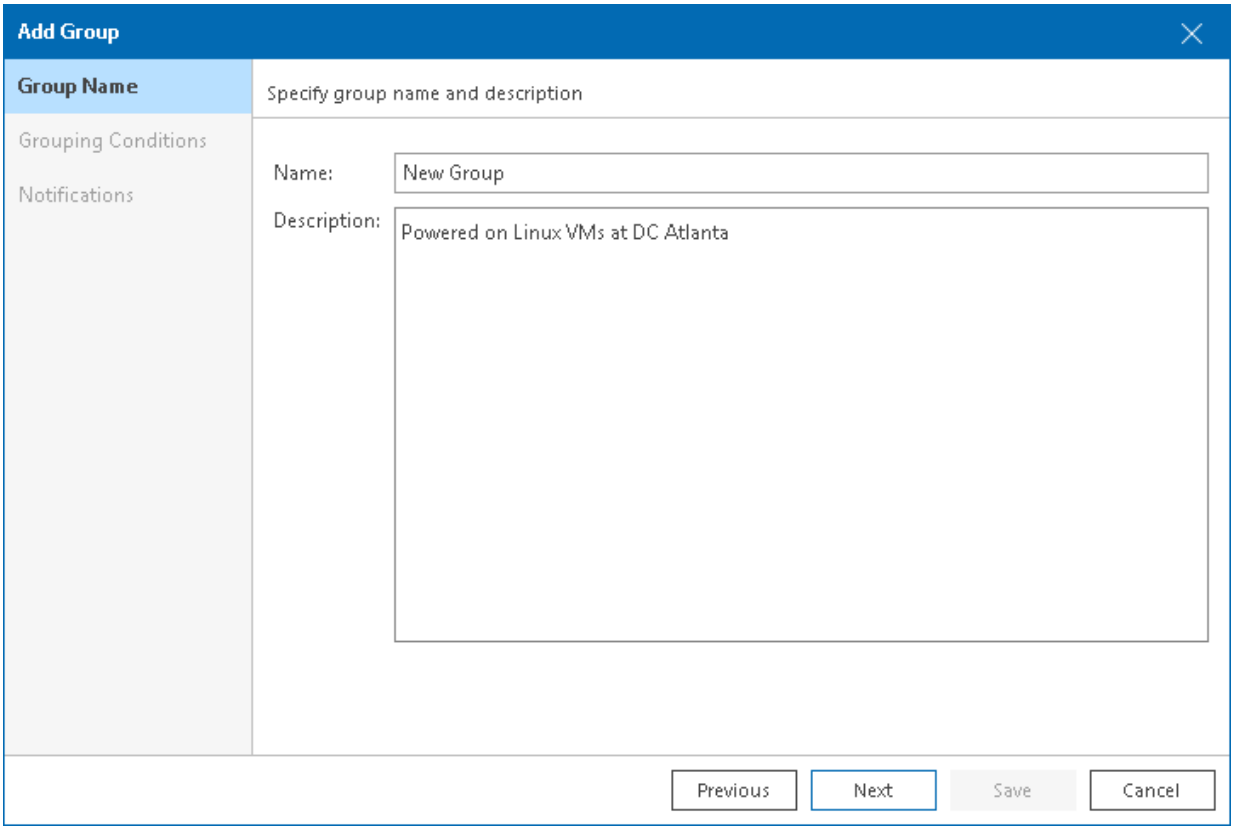


6. At the **Categorization Method** step of the wizard, select *Multiple conditions*.



7. At the **Grouping Criteria** step of the wizard, click **Add** to create groups based on multiple conditions. The **Add Group** wizard will open.

8. At the **Group Name** step of the wizard, specify a group name and description.



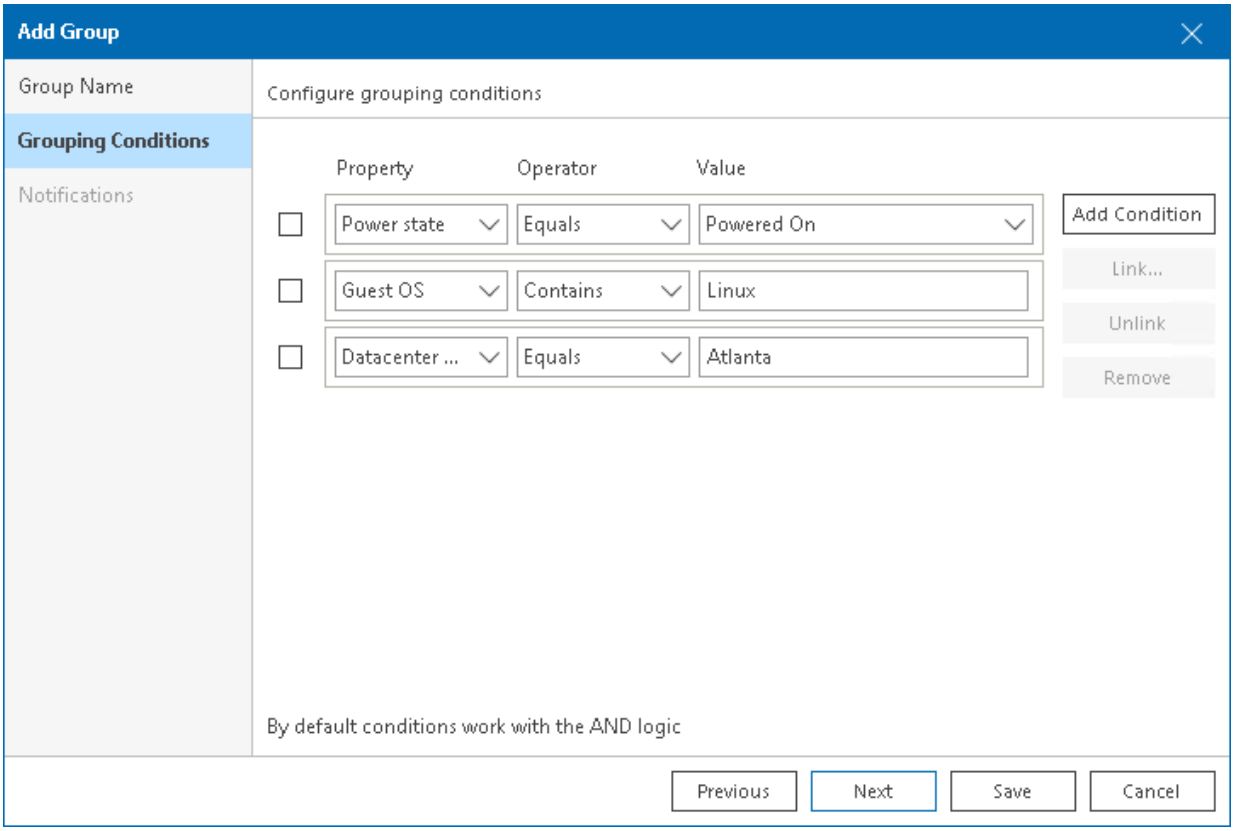
9. At the **Grouping Conditions** step of the **Add Group** wizard, set up categorization conditions:
   - From the **Property** drop-down list, select an object property.

     The list contains all object properties that Veeam ONE collects from a hypervisor and Veeam Backup & Replication servers.
   - From the **Operator** drop-down list, select a conditional operator.

     The list contains the following operators: *Equals*, *Does not equal*, *Starts with*, *Contains*, *Does not contain*.

- In the **Value** field, specify a value that will be checked in the condition.

The condition will be evaluated against discovered objects. To add another condition, click **Add Condition**.



By default, conditions are linked by the **AND** operator. That is, an object falls into a group when all specified conditions are met. You can change this behavior by linking conditions with the **OR** operator. In this case, an object will fall into a group when a condition for any of the linked rules is met.

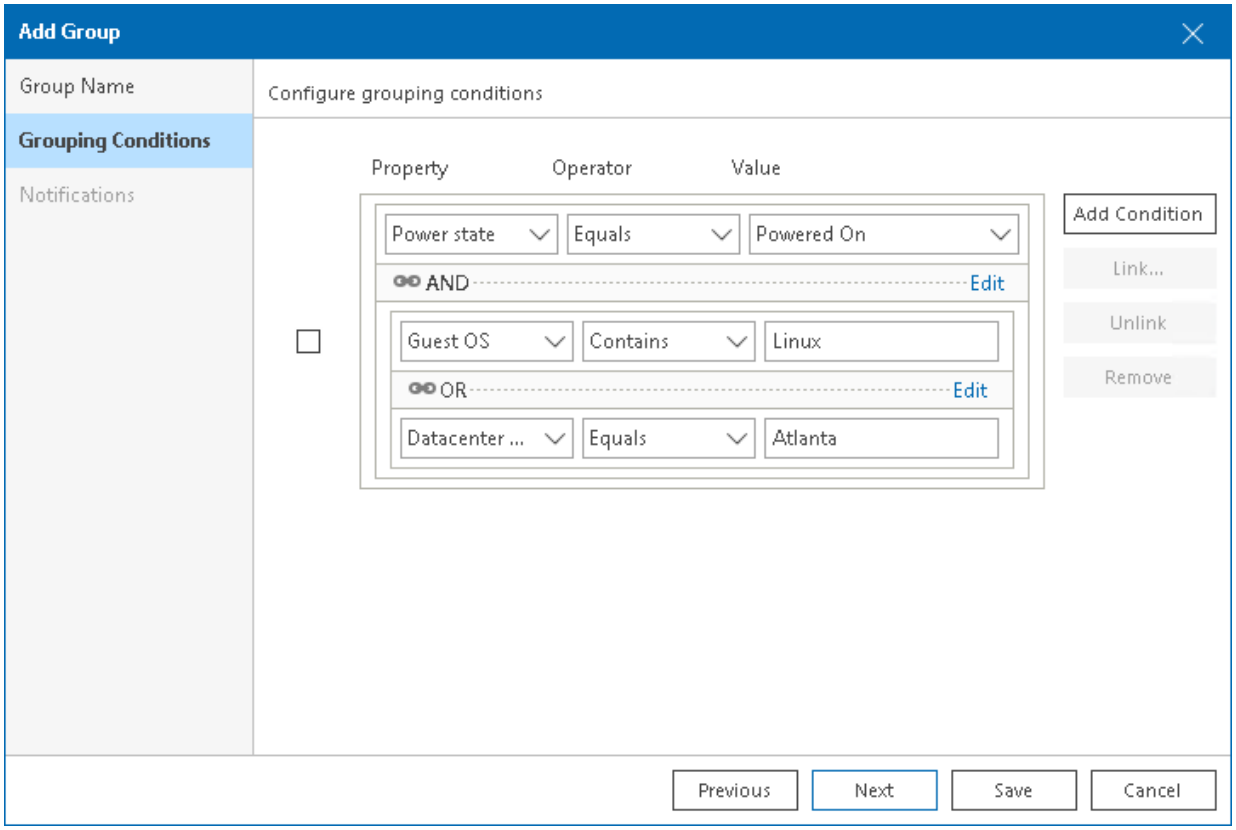
For example, you can create a group which will include VMs based on their power state, datacenter name and guest OS. If you want the group to include all powered on VMs that reside in datacenter Atlanta or run Linux as their guest OS, you must link these conditions. The second and the third conditions will be linked to each other with the **OR** operator. The first condition will be linked to them with the **AND** operator.

> **NOTE:**
>
> Linking supports 3 levels of nesting.

To link conditions:

a. Select check boxes next to the necessary conditions and click **Link**.

b. In the **Rule condition** window, select a link operator and click **OK**.



10. [Optional] At the **Notifications** step of the wizard, specify notification settings:

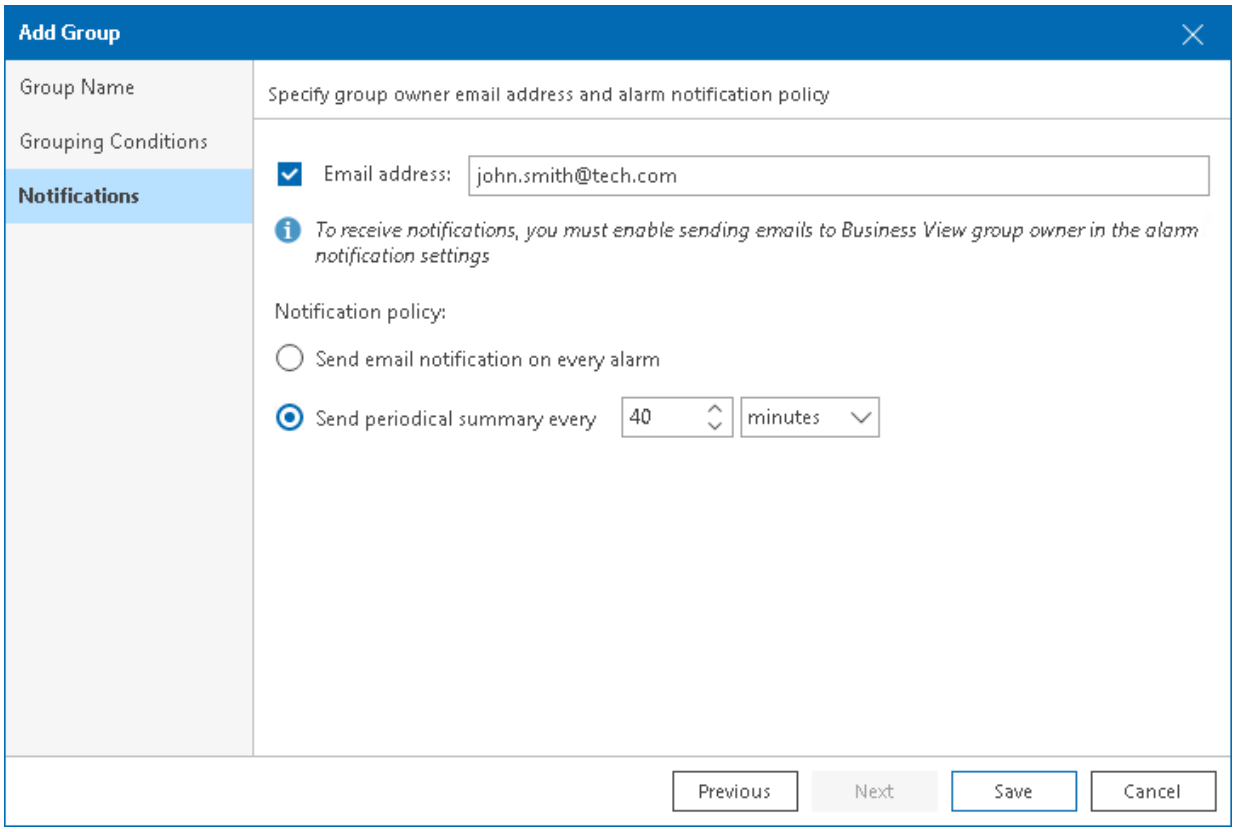
    a. Select the **Email address** check box and specify an email address of a person who will receive notifications about alarms triggered for the objects in a group (group owner).

    To receive alarm notifications, enable the **Send email to Business View group owner** option in alarm settings. For details on configuring alarm notification settings, see Specify Alarm Notification Options.

    b. Choose the notification policy:

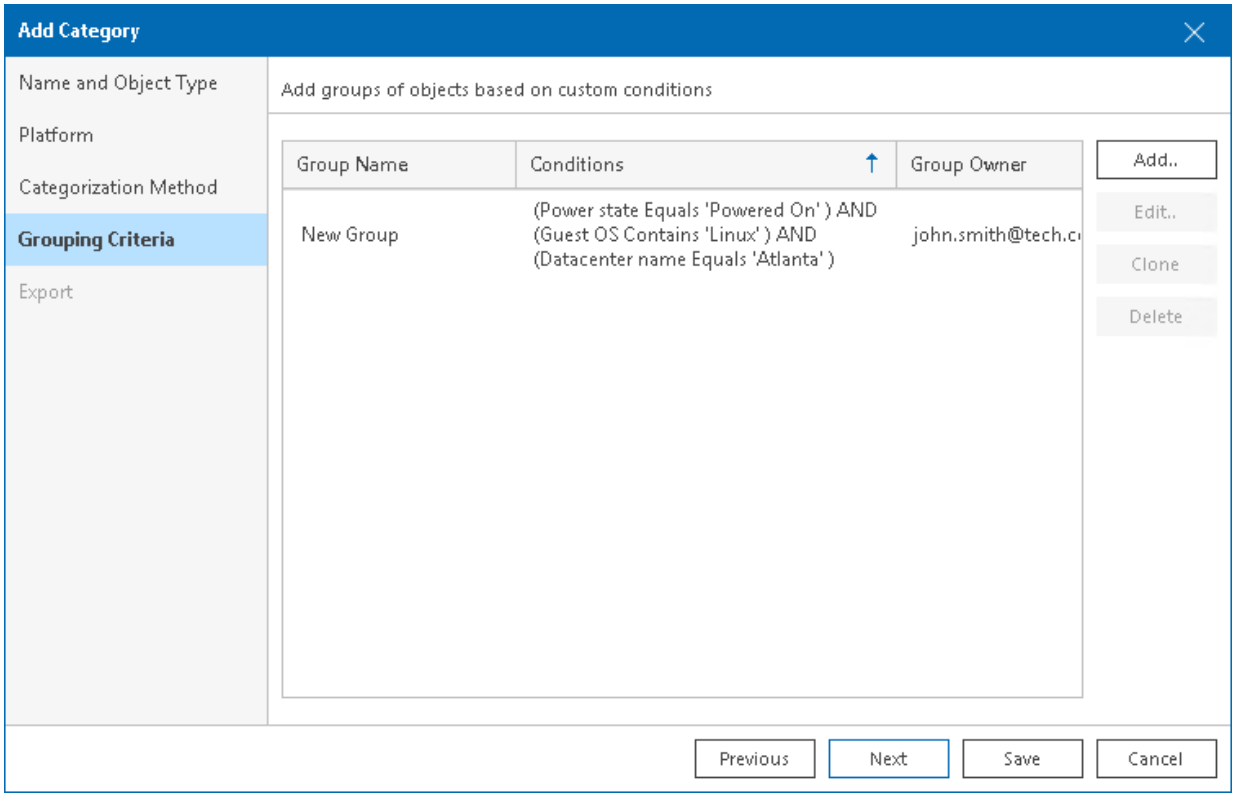
    - **Send email notification on every alarm** — select this option if you want to send an email notification every time a new alarm is triggered or the status of an existing alarm changes.

- **Send periodical summary every** – select this option and if you want to accumulate information about alarms and send an email notification once within a specific time interval. You can specify the time interval in minutes or hours.



11. Click **Save** to save a group configuration and close the **Add Group** wizard.

Group settings will appear in the **Categorization Wizard**.



12. Repeat steps **7-11** for each group you want to configure in the category.

    If you selected the *Computer* or *Enterprise Application* object type, click **Save** to finish working with the wizard.

13. At the **Export** step of the wizard, choose whether you want to export Business View categorization data:

    - [For VMware vSphere objects] Select **Create vSphere tags** if you want to display Business View categories and groups in vCenter Server.

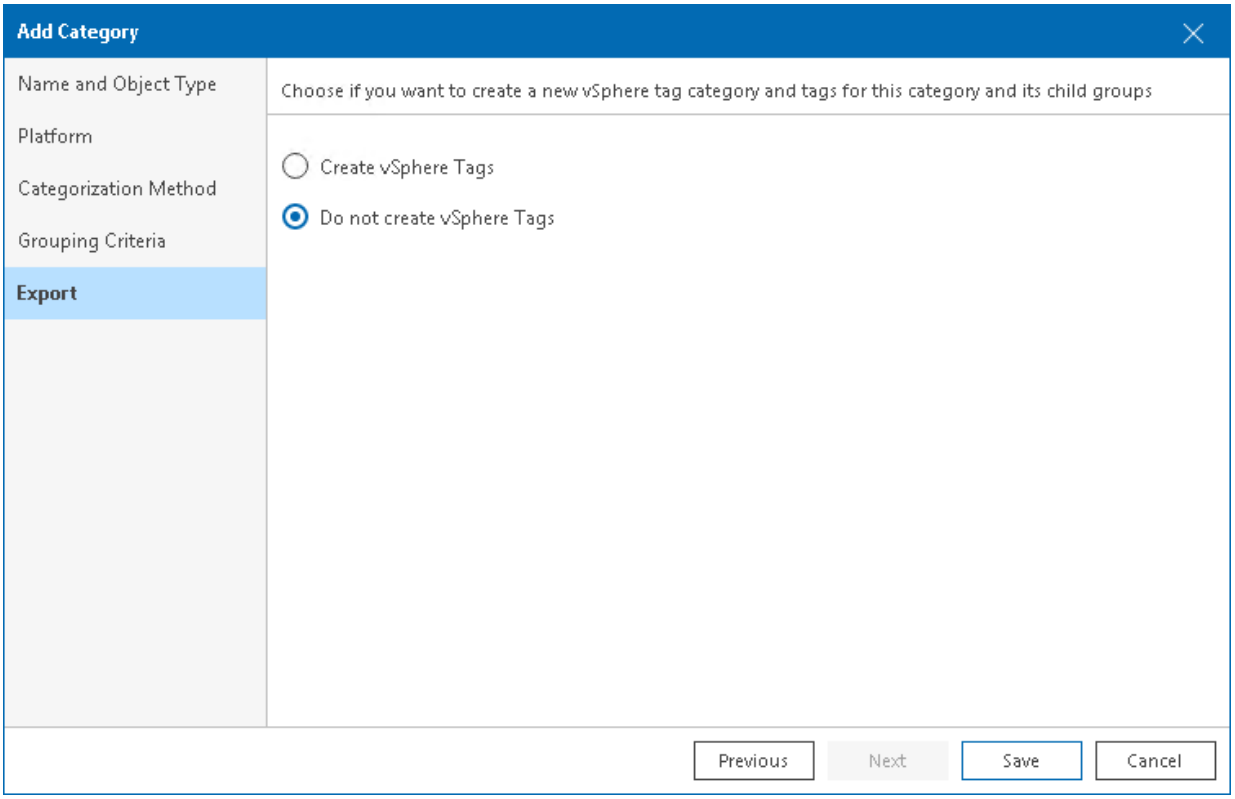
      Veeam ONE will export categories as tag categories and groups as tags.

    - [For Microsoft Hyper-V objects] Select **Create Hyper-V custom properties** if you want to display Business View categories and groups in System Center Virtual Machine Manager.

      Veeam ONE will export categories as custom properties and groups as property values.

    Veeam ONE will periodically overwrite created tags and custom properties to keep categorization data in synchronization with vCenter Server and System Center Virtual Machine Manager.

> **NOTE:**
>
> This step is not available if you enable import of categorization data from vCenter Server, System Center Virtual Machine Manager. For details on importing categorization model, see Selecting Categorization Model.



14. Click **Save**.

Configuring Categorization Using Grouping Expressions

Grouping expressions are used to find objects that share common properties. When you configure categorization with grouping expression, Veeam ONE creates a set of groups, and includes objects with matching attributes into these groups.

Groups created with grouping expressions have dynamic membership. If the property value changes, the object can be moved into another group or excluded from categorization after the next data collection.

For example, you can create an expression that will divide VMs into groups by the guest OS name. Veeam ONE will create groups with the names of guest OSes that VMs in your infrastructure run. Each group will include VMs with the same guest OS.

To create groups using expressions:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

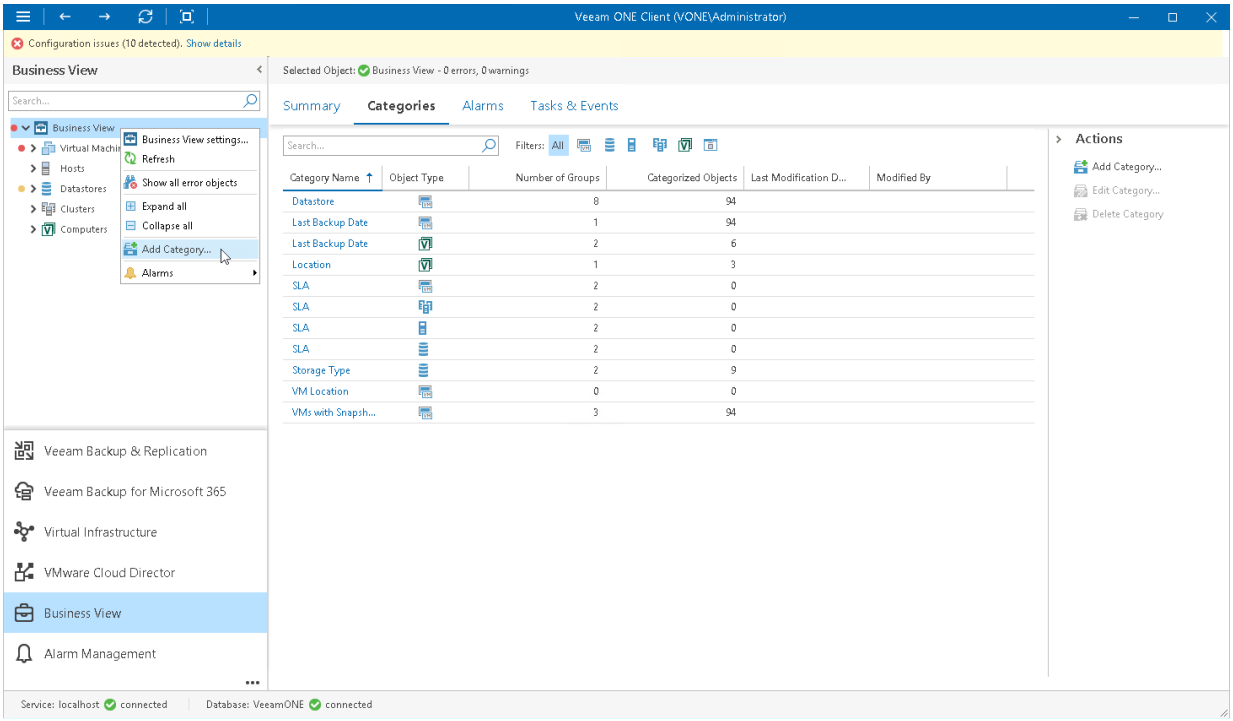
2. In the inventory pane, navigate to the **Business View** node.

3. Launch the **Categorization Wizard**:

   a. In the information pane, switch to the **Categories** tab.

   b. In the **Actions** pane, click **Add Category**.

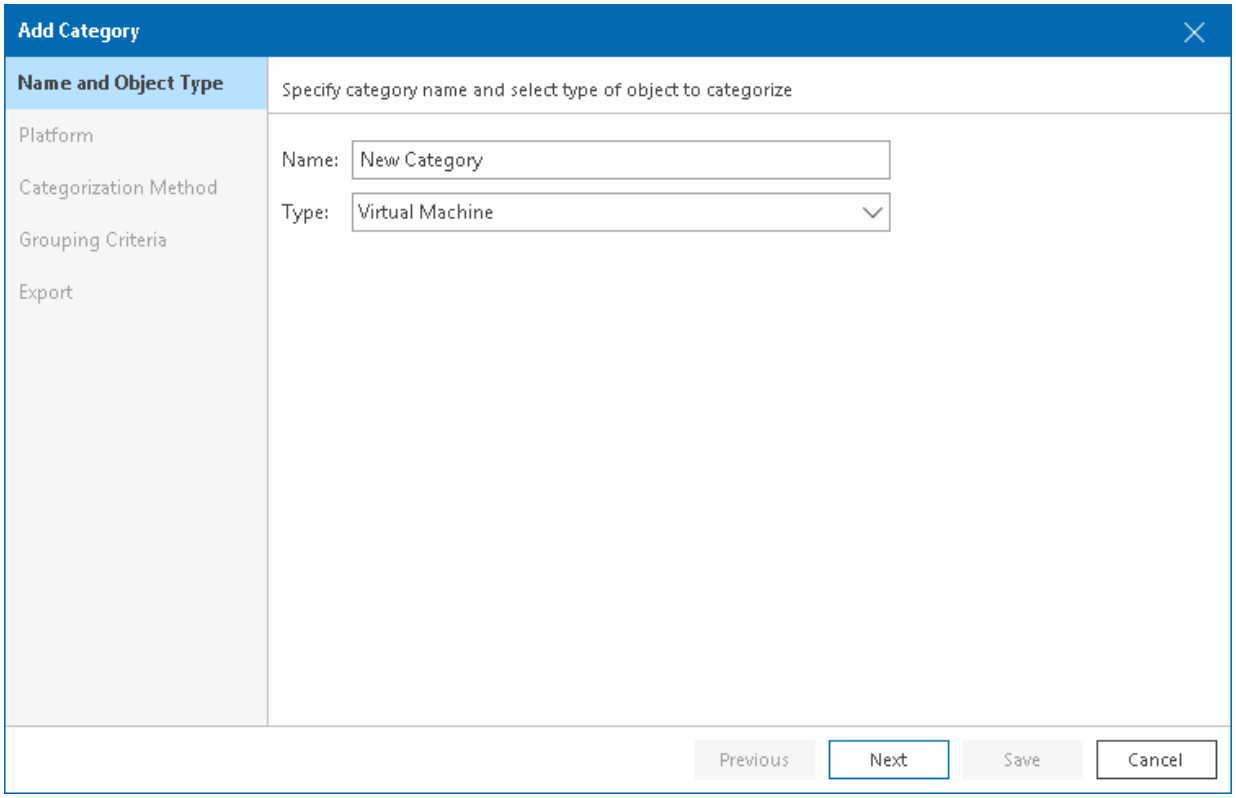
   Alternatively, in the **Business View** tree, right-click the main node and select *Add Category*.



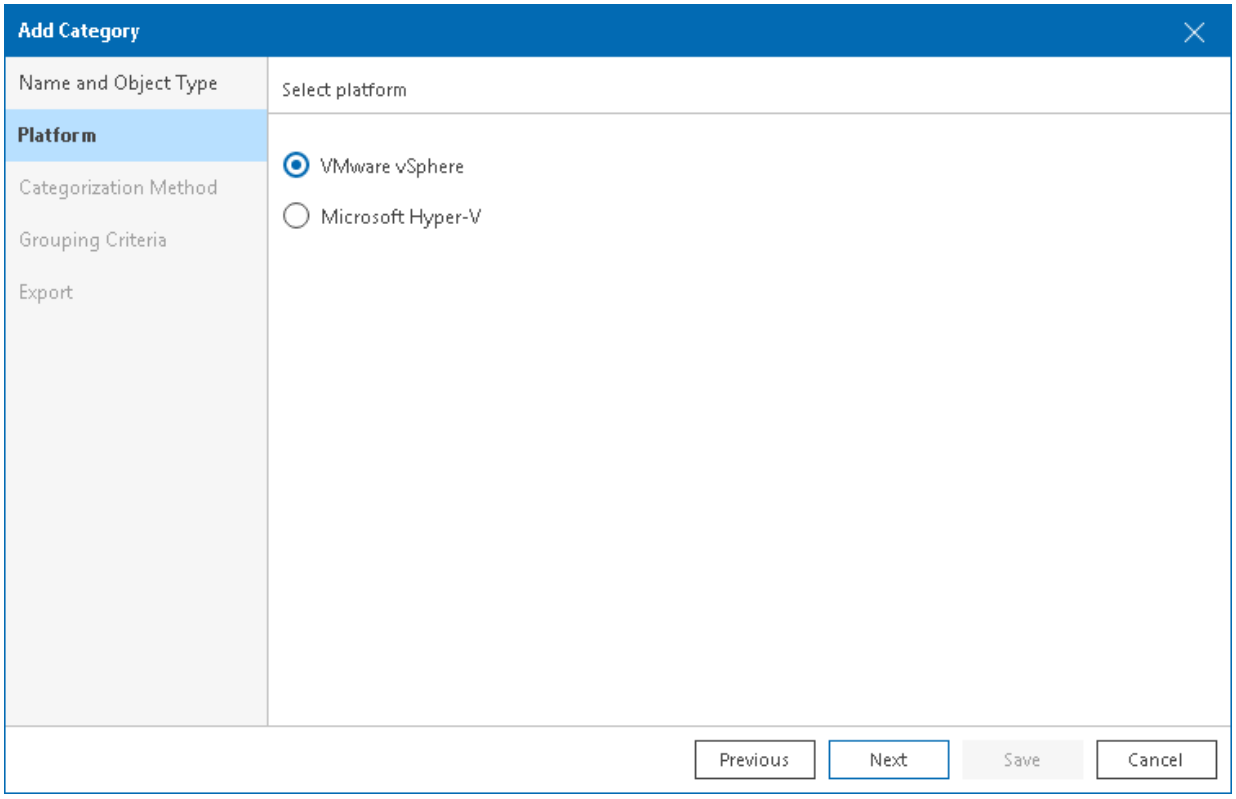
4. At the **Name and Object Type** step, enter category name, select object type and click **Next**.

   You can select the following types of objects: *Virtual Machine*, *Host*, *Cluster*, *Storage*, *Computer*, *Enterprise Application*.

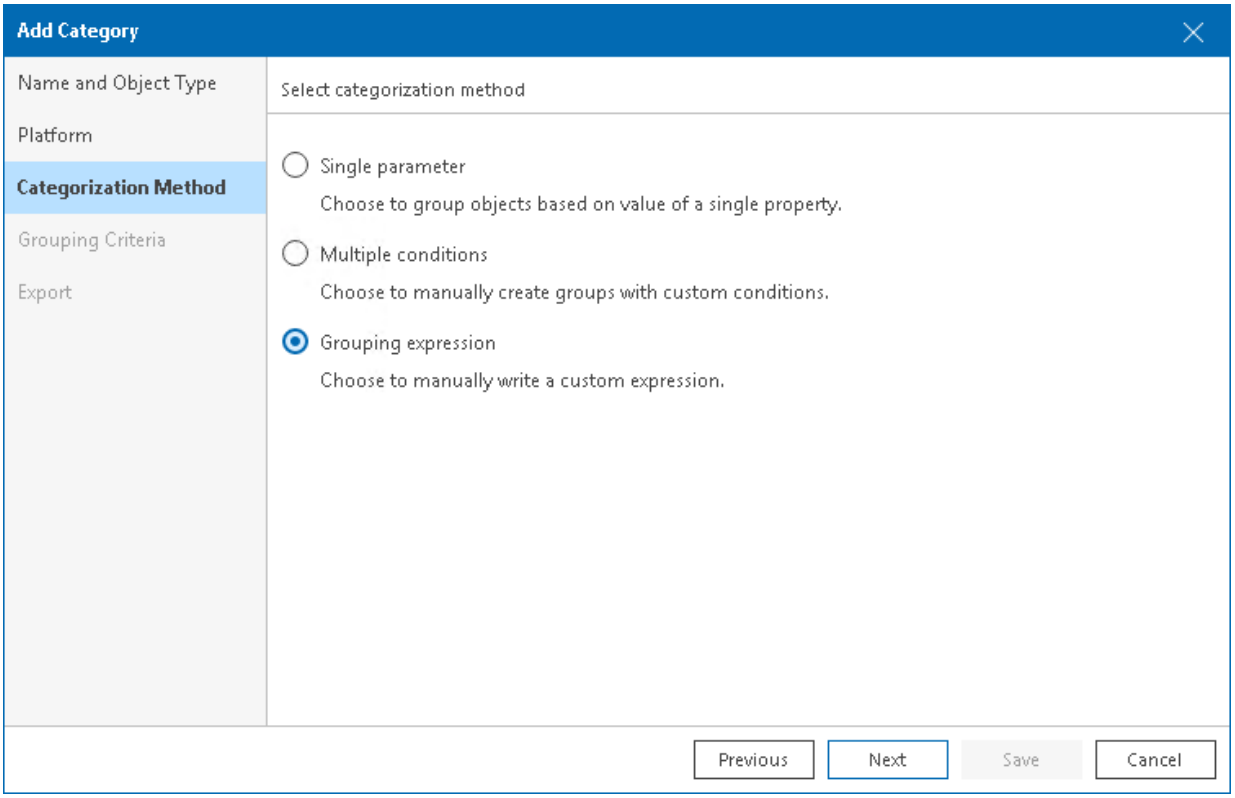
If you select the *Computer* or *Enterprise Application* object type, continue with step 6 of this procedure.



5. At the **Platform** step of the wizard, select the platform for which you want to categorize objects.



6. At the **Categorization Method** step of the wizard, select *Grouping expression*.

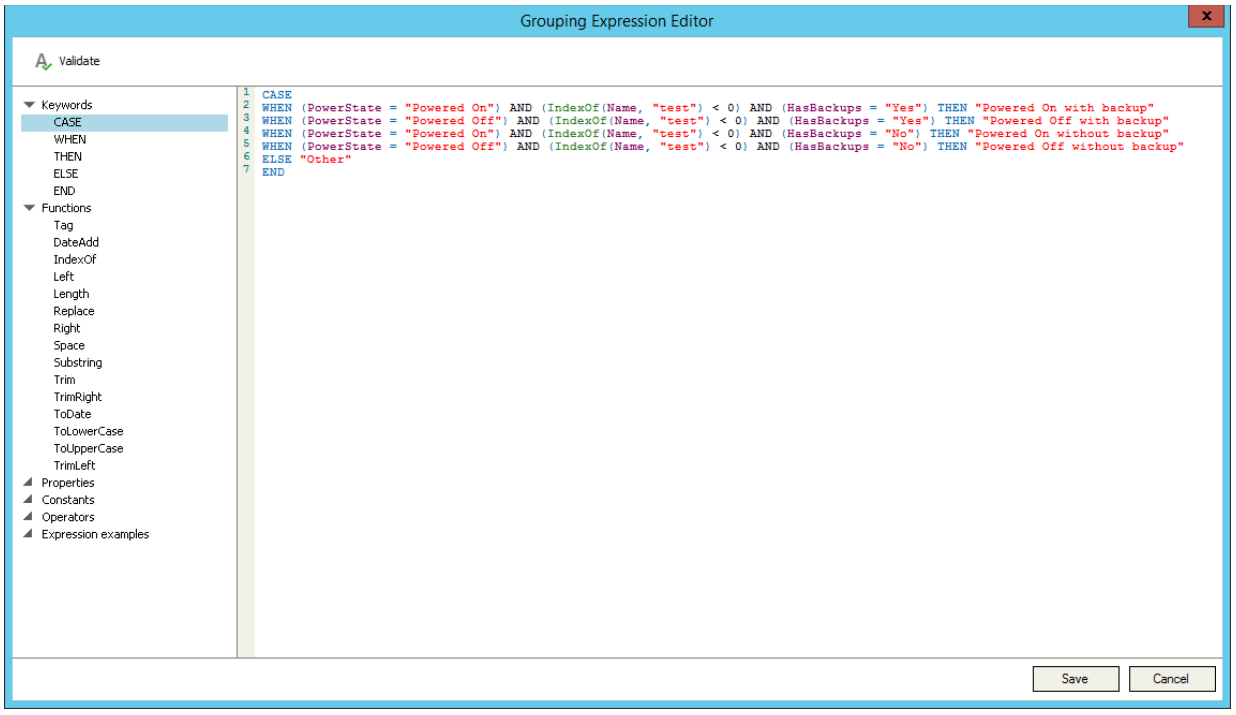


7. At the **Grouping Criteria** step of the wizard, specify an expression that Veeam ONE must use to create groups and distribute infrastructure objects in these groups:

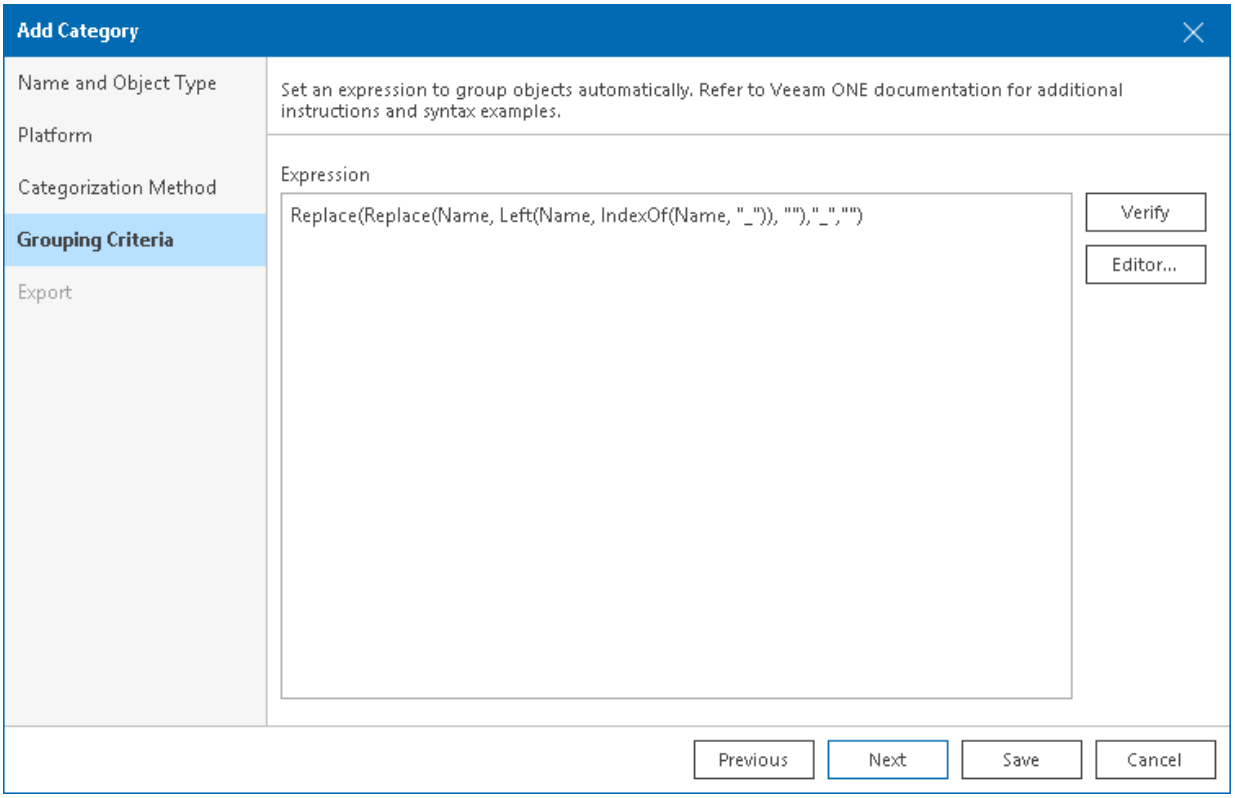
   a. Click the **Editor** button to open the **Grouping Expression Editor**.

   b. In the menu on the left, double click an item to add it to the **Expression** field.

   c. Click **Save** to save the expression and exit the editor.



To check the created script, click the **Verify** button.



For details on the syntax of grouping expressions, see Grouping Expressions Syntax.

If you selected the *Computer* or *Enterprise Application* object type, click **Save** to finish working with the wizard.

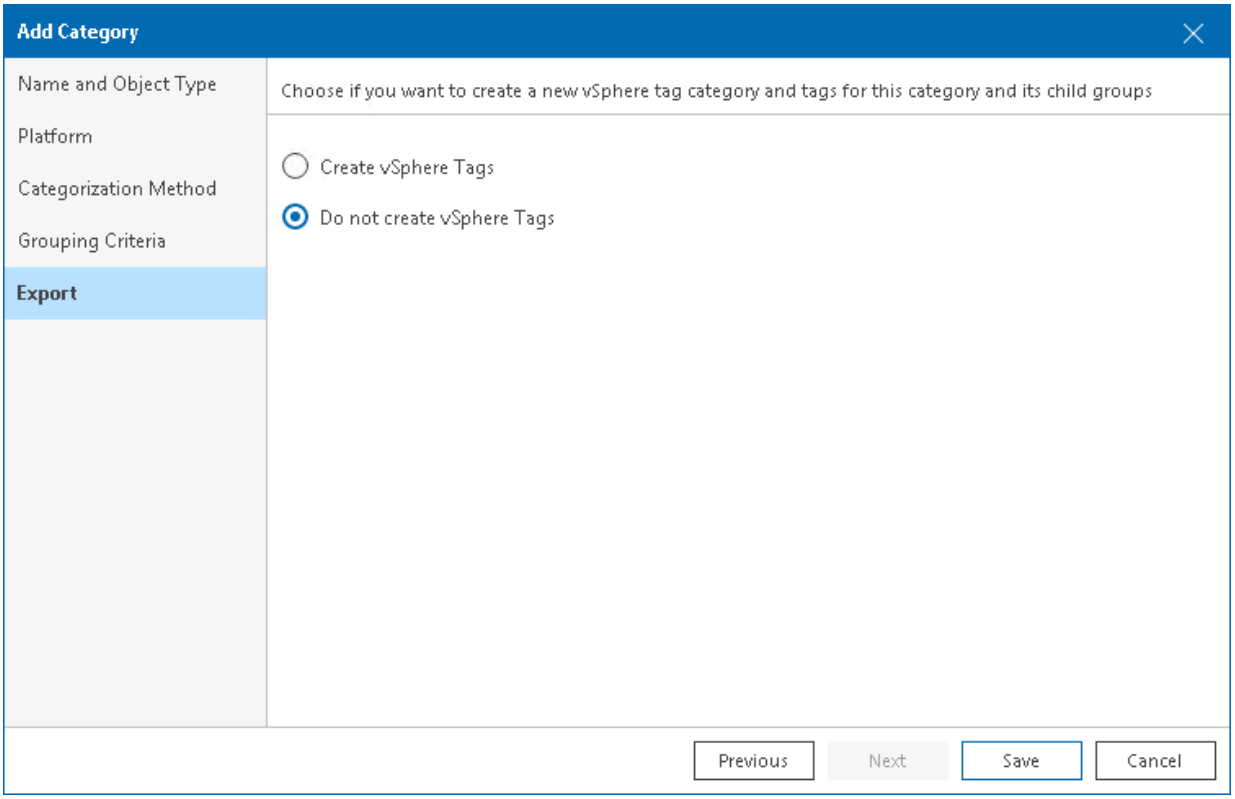
8. At the **Export** step of the wizard, choose whether you want to export Business View categorization data:
   - [For VMware vSphere objects] Select **Create vSphere tags** if you want to display Business View categories and groups in vCenter Server.

     Veeam ONE will export categories as tag categories and groups as tags.
   - [For Microsoft Hyper-V objects] Select **Create Hyper-V custom properties** if you want to display Business View categories and groups in System Center Virtual Machine Manager.

     Veeam ONE will export categories as custom properties and groups as property values.

NOTE:

This step is not available if you enable import of categorization data from vCenter Server, System Center Virtual Machine Manager or a 3rd party application. For details on importing categorization model, see Selecting Categorization Model.


Add Category
Name and Object Type
Platform
Categorization Method
Grouping Criteria
Export
Choose if you want to create a new vSphere tag category and tags for this category and its child groups
Create vSphere Tags
Do not create vSphere Tags
Previous
Next
Save
Cancel

9. Click **Save**.

Adding Objects to Groups Manually

You can manually add objects to groups in static categories — categories created with multiple-condition method and imported manually from a CSV file. When you map an object to a group, Veeam ONE adds the **Manual selection** condition to the group configuration. The name of an object acts as condition value. Mapped objects have static group membership, that is, they remain in the group until you manually reset categorization values. For details on resetting, see Resetting Categorization Values.

> **TIP:**
>
> To add objects to groups within multiple categories in a batch, you can describe these objects and groups in a CSV file and import this file to Veeam ONE Client. For details on importing categorization data from a CSV file, see Importing and Exporting Using CSV File.

Mapping Objects to Groups

To add objects to a group:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. In the inventory pane, navigate to the **Business View** node.

3. In the **Business View** tree, select the necessary object type — Virtual Machines, Hosts, Datastores, Clusters, Computers or Enterprise Applications.

4. Open the tab with the name of the object: *Virtual Machines*, *Hosts*, *Datastores*, *Clusters*, *Computers*, *Enterprise Applications*.

5. Select objects that you want to add to a group.

   To quickly find necessary objects, use the scope drop-down list and search field at the top of the objects list.

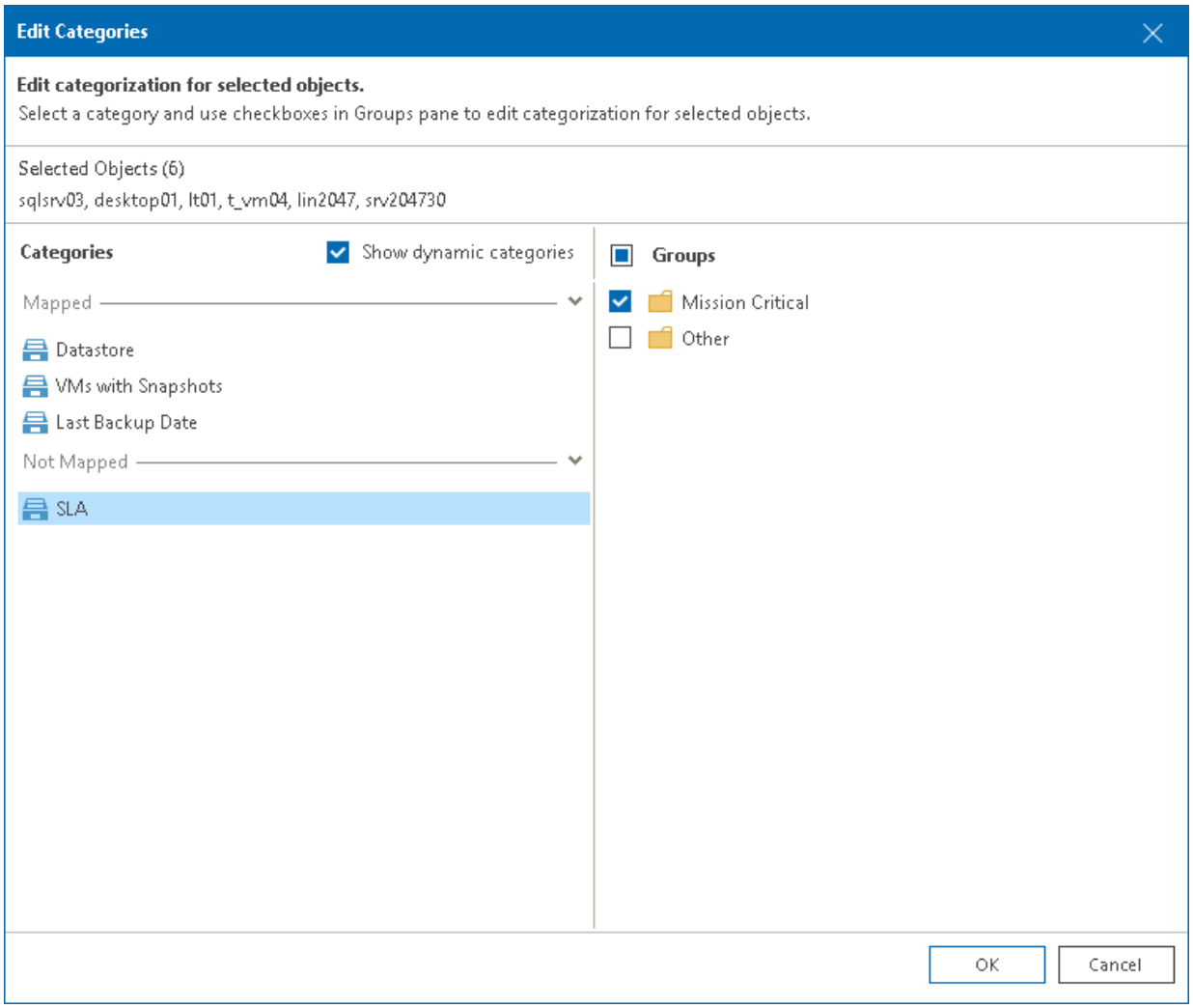
   Press and hold the `[CTRL]` or `[SHIFT]` key on the keyboard to select multiple objects.

6. In the **Actions** pane, click **Manual Categorization**.

7. In the **Edit Categories** window, select a category and groups to which you want to add objects.

   The **Categories** section lists static categories to which you can add objects. To display all categories for the selected object type, select the **Show dynamic categories** check box.

8. Click **OK** to save the settings.



Resetting Categorization Values

You can remove objects from categories and groups to which you manually added these objects.

To remove objects from groups:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. In the inventory pane, navigate to the **Business View** node.

3. In the **Business View** tree, select the necessary object type — *Virtual Machines*, *Hosts*, *Datastores*, *Clusters*, *Computers* or *Enterprise Applications*.

4. Open the tab with the name of the object: *Virtual Machines*, *Hosts*, *Datastores*, *Clusters*, *Computers*, *Enterprise Applications*.

5. Select objects for which you want to reset categorization.

   To quickly find necessary objects, use the scope drop-down list and search field at the top of the objects list.

   Press and hold the `[CTRL]` or `[SHIFT]` key on the keyboard to select multiple objects.

6. In the **Actions** pane, click **Reset Categorization**.
7. In the **Reset Manual Categorization** window, click **OK** to confirm object removal.

Importing and Exporting Categorization Data

You can import and export categorization data and synchronize it with other applications. Veeam ONE offers the following synchronization possibilities:

- Importing Categorization Model from vCenter Server and System Center Virtual Machine Manager

  If you use vCenter Server tags and System Center Virtual Machine Manager custom properties to categorize virtual infrastructure objects on the vCenter Server or Microsoft Hyper-V side, you can import these tags and properties to create Business View groups in Veeam ONE. Each time data collection runs, tag categories and custom properties are imported as Business View categories, tags and property values are assigned to groups within these categories.

- Importing and Exporting Using CSV File

  You can synchronize Business View categorization data with categorization data from 3rd party software. In Veeam ONE, you can import categorization data from and export categorization data to a CSV file that acts as a medium between the two systems.

Importing Categorization Model from vCenter Server and System Center Virtual Machine Manager

You can import categorization model from vCenter Server and System Center Virtual Machine Manager.

When you enable synchronization of categorization data from virtualization servers, Veeam ONE Client imports tags and custom properties and creates categories and groups according to the values of imported tags and properties. Every time data collection runs, Veeam ONE Client overwrites created categories and groups to keep categorization data in synchronization with vCenter Server and System Center Virtual Machine Manager.

> **NOTE:**
>
> Consider the following:
>
> - Categories imported from vCenter Server and System Center Virtual Machine Manager are read-only, you cannot edit or delete them. To remove such categories from Business View tree, disable the option in Server Settings. For details on Business View Server Settings, see Business View.
> - If Veeam ONE detects tags and custom properties with names that are already assigned to categories in Business View, it will exclude such tags and properties from synchronization.
> - While in categorization model imported from vCenter Server and System Center Virtual Machine Manager, if you create a new category, you will not be able to export it to tags.

To import tags and custom properties:

1. Open Veeam ONE Client.

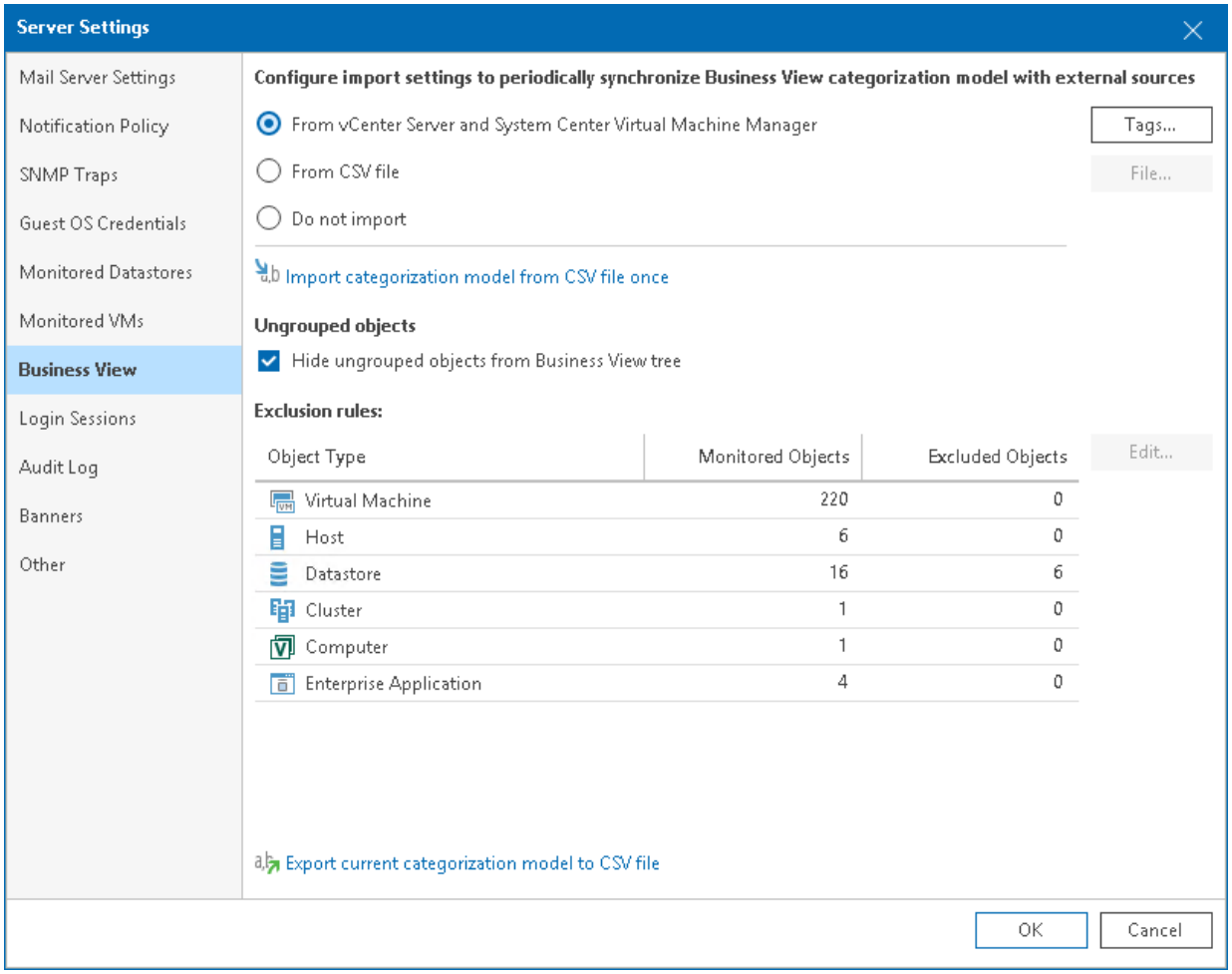
   For details, see Accessing Veeam ONE Components.

2. In the main menu, click **Settings > Server Settings**.

   Alternatively, press `[CTRL + S]` on the keyboard.

3. In the **Server Settings** window, open the **Business View** tab.

4. Select **From vCenter Server and System Center Virtual Machine Manager**.

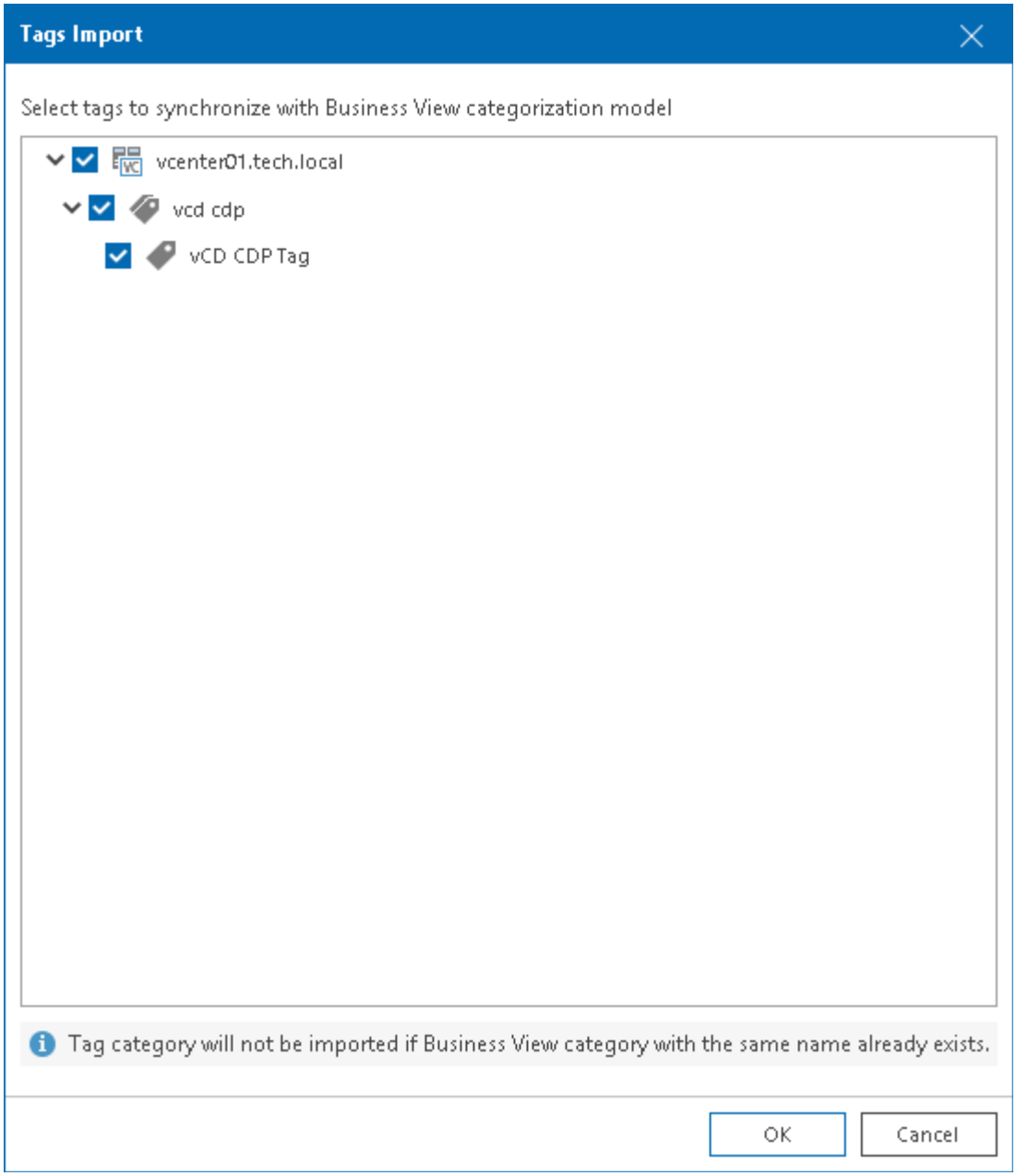


By default, Veeam ONE Client imports all tags and custom properties available on the vCenter Server and System Center Virtual Machine Manager side.

To select which tags and properties to import:

a. Click the **Tags** button.

b. Clear the check boxes next to tags that you want to exclude from import.



c. Click **OK** to save settings.

5. Click **OK** to close the **Server Settings** window.

Veeam ONE will import selected vCenter Server tags and System Center Virtual Machine Manager properties to create Business View categories and groups.

Importing and Exporting Using CSV File

In Veeam ONE, you can import and export categorization model using a CSV file.

Importing Categorization Data Manually

If you already categorized the virtual infrastructure objects outside Veeam ONE, you can describe categorization model using a CSV file and then import this file to Veeam ONE.

When you import a CSV file manually, Veeam ONE creates categories and groups specified in the file and maps objects to these groups. If Veeam ONE detects in the imported CSV file categories and groups that already exist in Business View, it will map objects specified in the CSV file to existing groups. Imported objects have static membership, that is, they remain in the group until you manually reset categorization values. For details on manual mapping and resetting categorization values, see Adding Objects to Groups Manually.

> **NOTE:**
>
> To make sure that Veeam ONE will process the CSV file without errors, check the file structure. For details on CSV file structure, see CSV File Structure.

To import categorization data from a CSV file:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. In the main menu, click **Settings > Server Settings**.

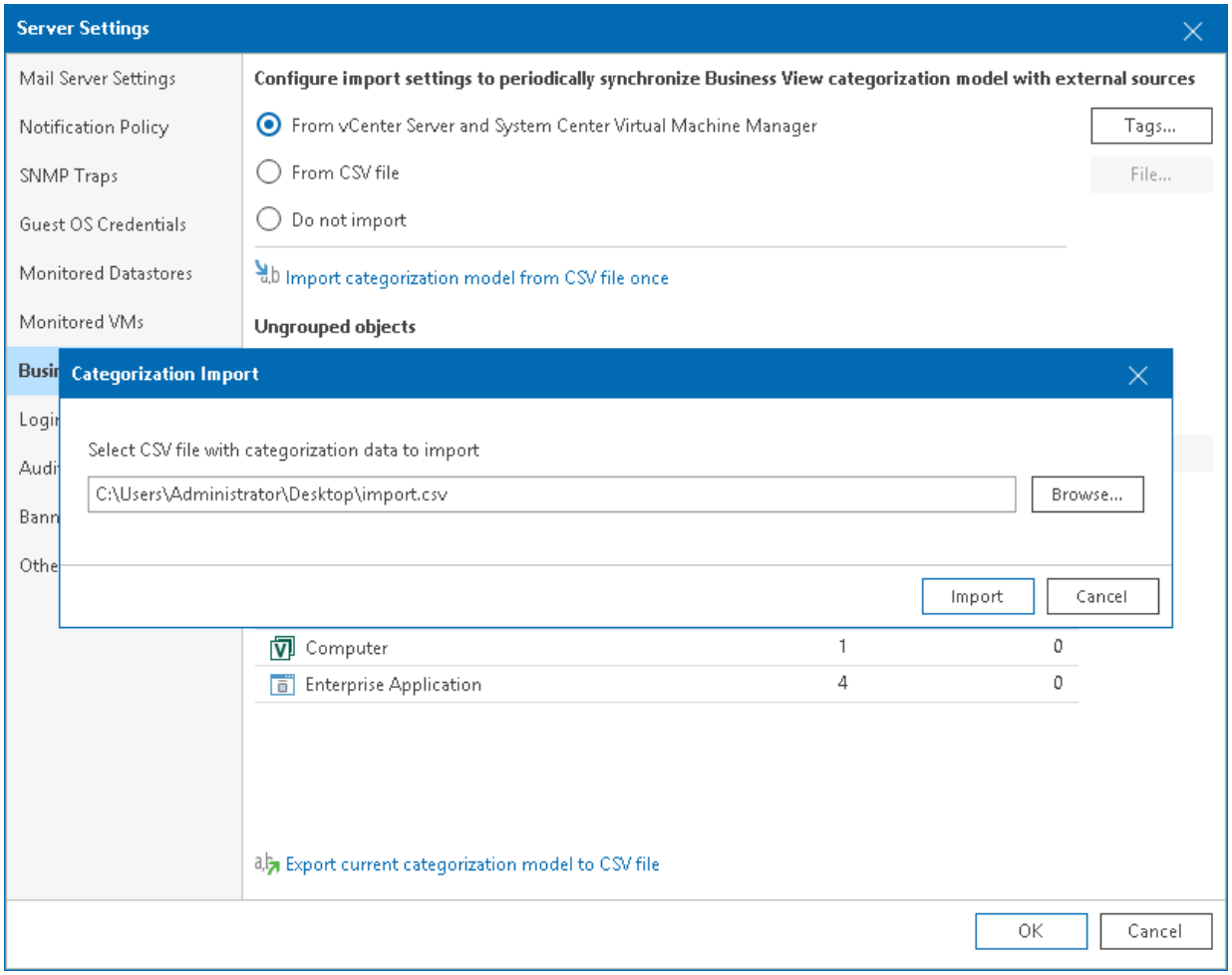
   Alternatively, press `[CTRL + S]` on the keyboard.

3. In the **Server Settings** window, open the **Business View** tab.

4. Click the **Import categorization model from CSV file once** link.

5. In the **Categorization Import** window, specify the path to the CSV file with the categorization data you want to import.

6. Click **Import**.



Importing Categorization Data Automatically

You can synchronize categorization data between Veeam ONE and a 3rd party application every time data collection runs. To do this, you can specify a path to a CSV file with the categorization data exported from a 3rd party application. Veeam ONE will import data from this file during every data collection session.

Additionally, you can specify a path to a script that must be triggered before data from the CSV file is imported. This can be a script that creates the CSV file based on data from a 3rd party application, or updates the file. For details on structuring the file, see CSV File Structure.

> **NOTE:**
>
> If Veeam ONE detects in the specified CSV file categories that already exist in Business View, it will exclude such categories from synchronization.

To configure periodic synchronization of categorization data between Veeam ONE and a 3rd party application:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. In the main menu, click **Settings > Server Settings**.

   Alternatively, press `[CTRL + S]` on the keyboard.

3. In the **Server Settings** window, open the **Business View** tab.

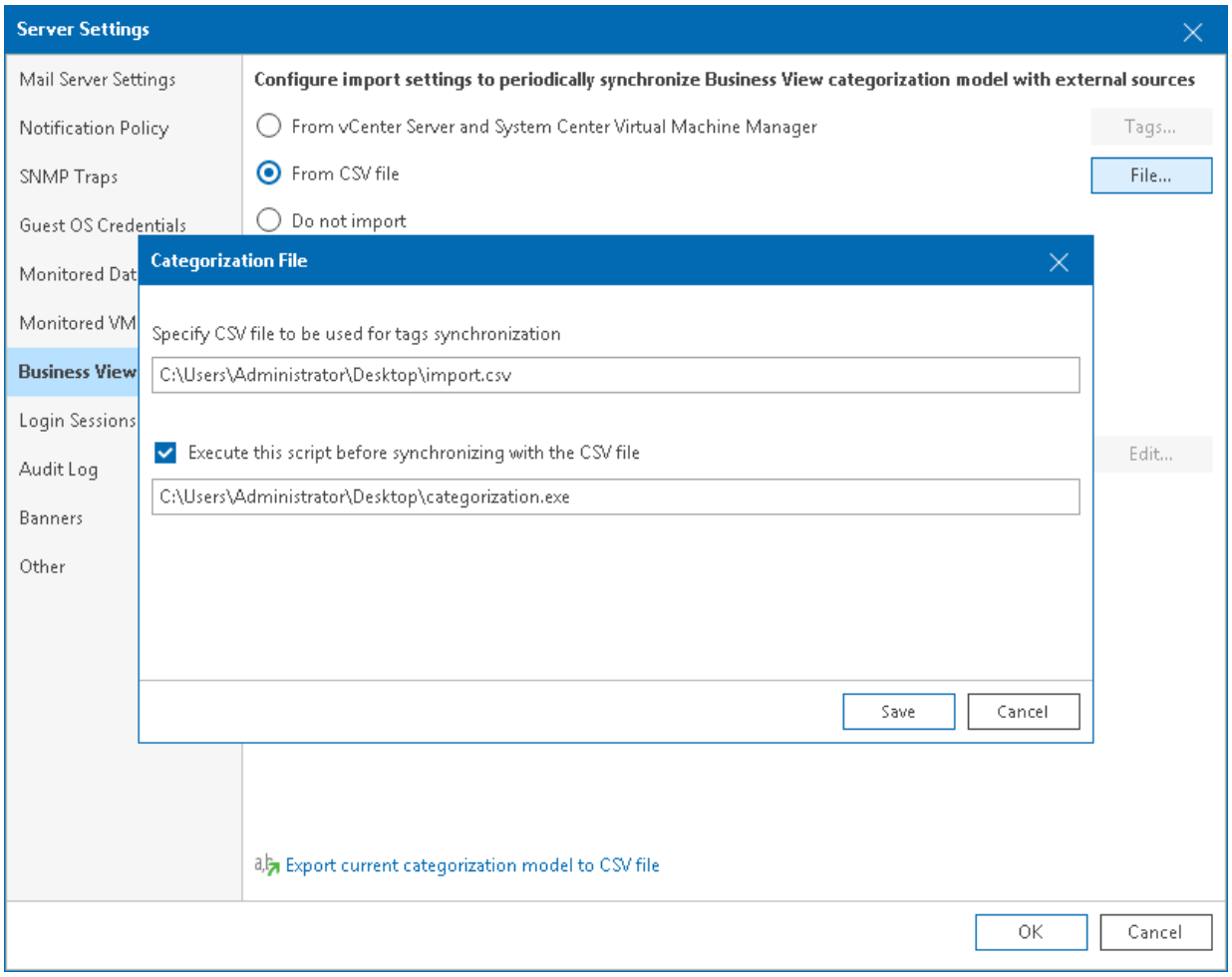
4. Select **From CSV file** and click the **File** button.

5. In the **Categorization File** window, specify the path to the CSV file with the categorization data you want to synchronize.

6. If you want to trigger a custom script before data synchronization, select the **Execute this script before synchronizing with a CSV file** check box and specify a path to the script file.

> **NOTE:**
>
> The CSV and script files must reside in a folder that is accessible by *Veeam ONE Monitoring Service*. The account under which the service runs must have read permissions on the files.

7. Click **Save**.



Exporting Categorization Data

To export Business View categorization data to a CSV file:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

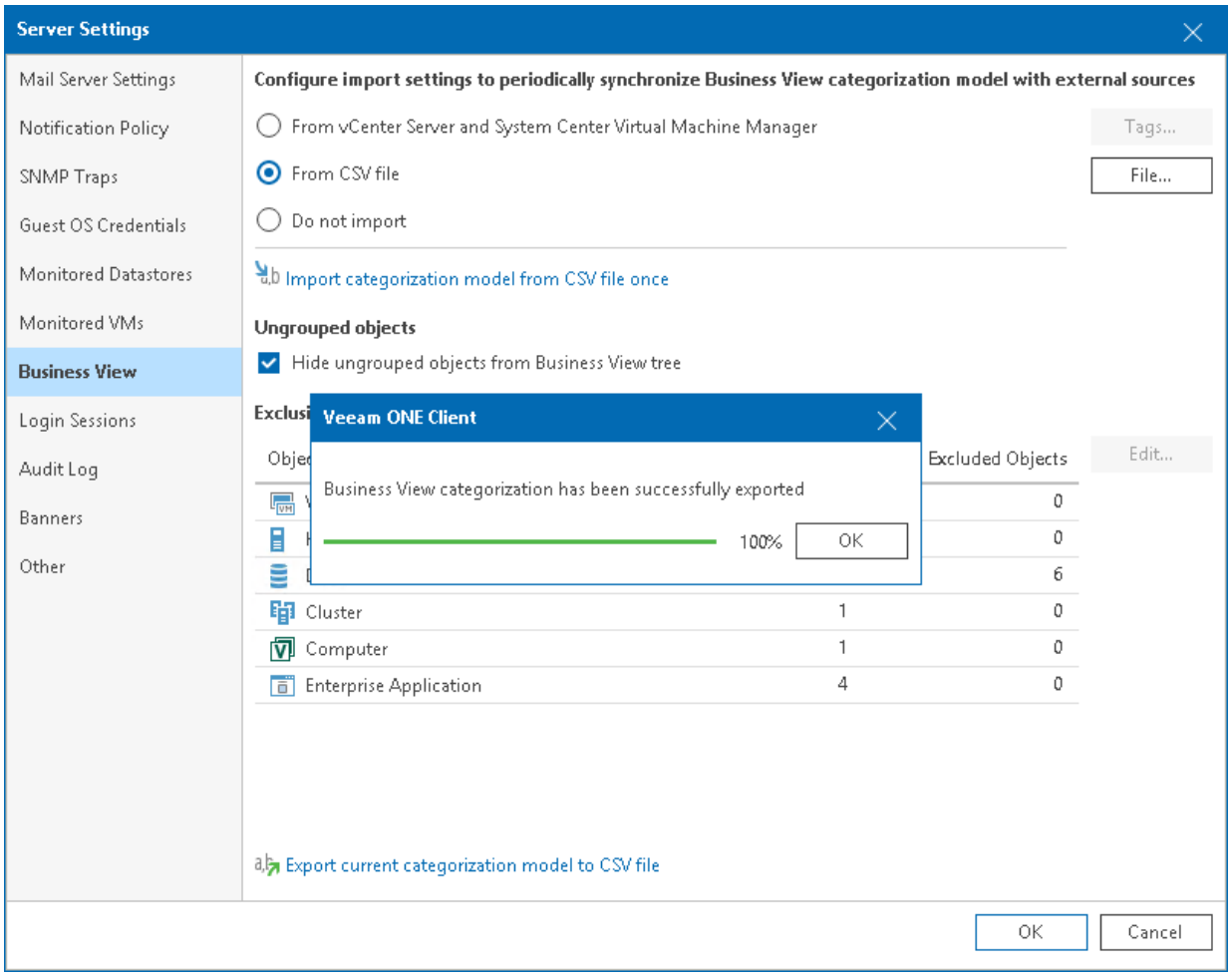
2. In the main menu, click **Settings > Server Settings**.

   Alternatively, press `[CTRL + S]` on the keyboard.

3. In the **Server Settings** window, open the **Business View** tab.

4. At the bottom of the window, click the **Export current categorization model to CSV file** link, specify the location where the file must be saved and click **Save**.

5. In the **Veeam ONE Client** window, click **OK** to acknowledge export results.



CSV File Structure

You can create a CSV file with categorization data from scratch. Every new record (row) in the file must describe an infrastructure object and its categorization data.

The following columns are mandatory for every record:

- **Server** – name of the managed virtual infrastructure or backup server to which object belongs.
- **ObjectType** – type of object (possible values are *VirtualMachine*, *HostSystem*, *Storage*, *ClusterComputerResource*, *HvCluster*, *HvCsvDisk*, *HvHost*, *HvPhysicalDisk*, *HvVirtualMachine*, *VeeamBpAgent*, *SMBShare*).
- **MoRef** – reference number of the object (for VMware vSphere), UUID or ID of the object (for Microsoft Hyper-V).

Other columns in the CSV file must be named as Business View categories. Category fields accept the following types of values:

- Name of a group within the category to which an infrastructure object belongs
- Empty field, if the object does not belong to any group within the category
- *Excluded*, if the object must be excluded from categorization

The following table shown as example of a CSV file for VMware vSphere VMs.

Server	ObjectType	MoRef	Category1
server.local	VirtualMachine	vm-01	Group1
server.local	VirtualMachine	vm-02	Excluded

Editing Business View Categories

You can edit Business View categories created in Veeam ONE Client as well as predefined categories and categories imported manually from a CSV file.

To edit a category:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. In the inventory pane, navigate to the **Business View** node.

3. Open the **Categories** tab.

4. Select a category that you want to edit.

   To quickly find the necessary category, use filters and the search field at the top of the **Categories** list.

5. In the **Actions** pane, click **Edit Category**.

   Alternatively, right-click the category and select **Edit Category** from the shortcut menu.

6. Change the required category settings.

   For details on category settings, see Creating Business View Categories and Groups.

Deleting Business View Categories

You can delete Business View categories created in Veeam ONE Client as well as predefined categories and categories imported manually from a CSV file. When you delete a category, objects from this category remain in your infrastructure.

To delete a category:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. In the inventory pane, navigate to the **Business View** node.
3. Open the **Categories** tab.
4. Select a category that you want to delete.

   To quickly find the necessary category, use filters and the search field at the top of the **Categories** list.

5. In the **Actions** pane, click **Delete Category**.

   Alternatively, right-click the category and select **Delete Category** from the shortcut menu.

Business View Monitoring

Veeam ONE Client allows you to monitor infrastructure presented from the business perspective — that is, based on Business View categories and groups of VMs, hosts, datastores, clusters, computers and enterprise applications.

With Veeam ONE, you can:

- Monitor the overall state of the categorized infrastructure
- View triggered alarms
- View objects included in categories and groups
- Work with performance charts
- View the list of events

Business View Summary Dashboards

Veeam ONE Client comes with a set of summary dashboards for business view groups that include infrastructure objects. These dashboards allow you to:

- Review the summary details for all VMs, hosts, datastores, clusters, computers and enterprise applications in custom groups
- View latest alarms
- Troubleshoot issues by drilling down to specific objects in groups

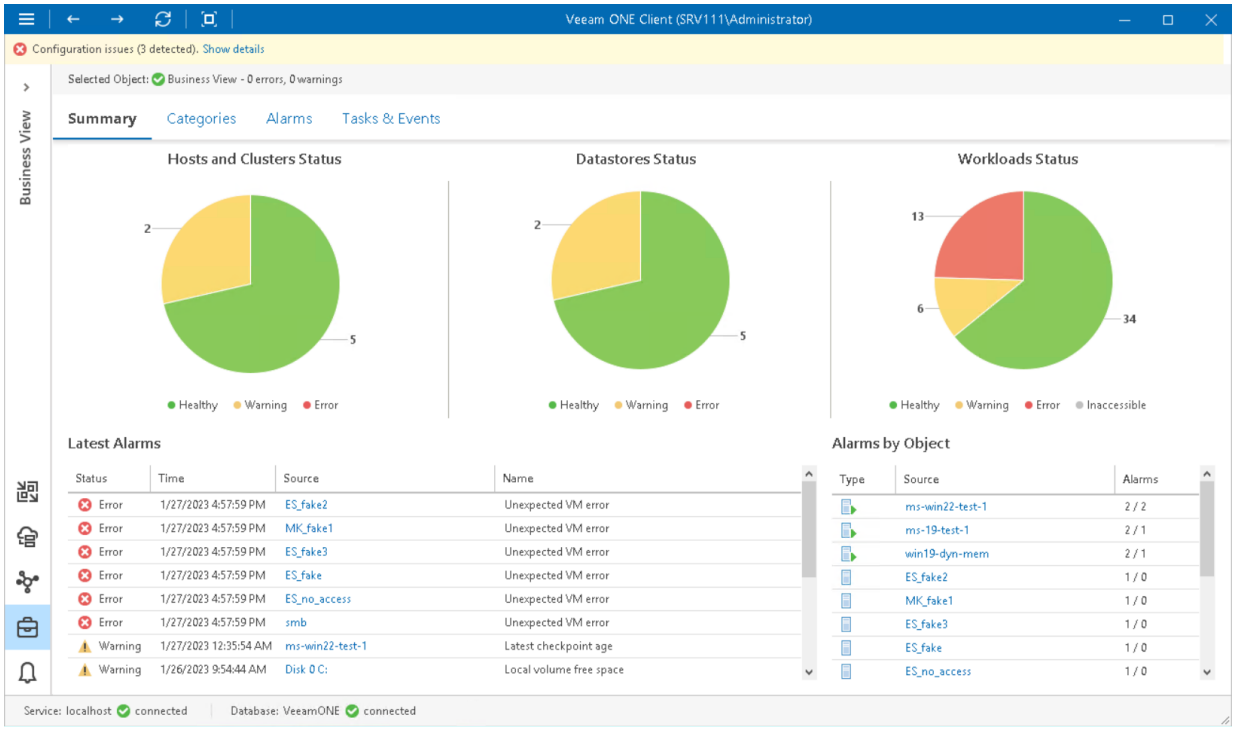
To access a summary dashboard for a virtual infrastructure object or virtual infrastructure segment:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.
2. At the bottom of the inventory pane, click **Business View**.
3. In the inventory pane, select the necessary node.
4. Open the **Summary** tab.

Business View Summary

The Business View summary dashboard presents the health status overview for objects in all available Business View groups.



Host and Clusters Status, Datastores Status, Workloads Status

The charts reflect the health status of virtual infrastructure objects in Business View groups.

Every chart segment represents the number of objects in a certain state — objects with errors (red), objects with warnings (yellow) and healthy objects (green). Click a chart segment or a legend label to drill down to the list of alarms with the corresponding status for the selected type of virtual infrastructure objects.

Latest Alarms

The list displays the latest 15 alarms for objects in available Business View groups. Click a link in the **Source** column to drill down to the list of alarms triggered for a specific virtual infrastructure object.

Alarms by Object

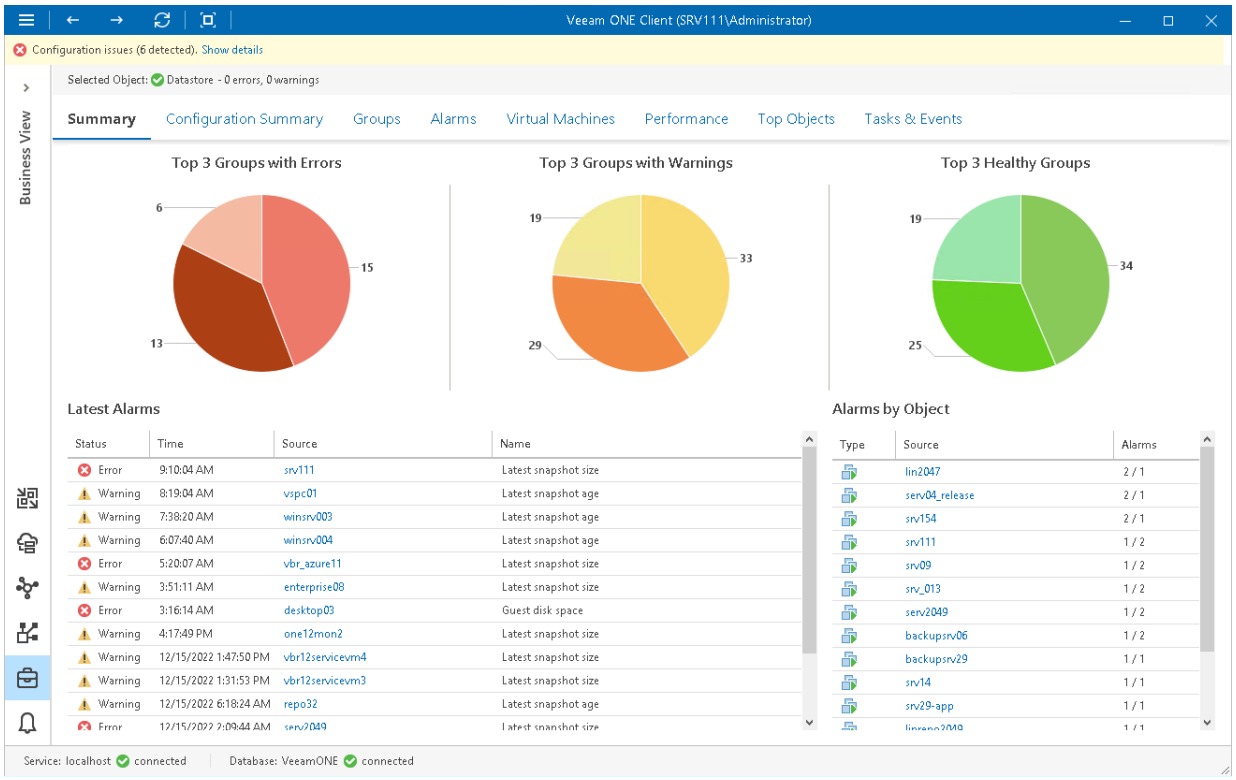
The list displays 15 objects with the greatest number of alarms.

The value in the **Alarms** column shows the number of errors and warnings for an object. For example, 3/1 means that there are 3 errors and 1 warning triggered for the object. Click a link in the **Source** column to drill down to the list of alarms triggered for a specific virtual infrastructure object.

For more information, see Working with Triggered Alarms.

Category Summary

The category summary dashboard provides an overview of the health status and performance for categorized infrastructure objects.



Top 3 Groups with Errors, Top 3 Groups with Warnings, Top 3 Healthy Groups

The charts reflect the health status of all groups within the chosen category.

Every chart segment represents groups in a certain state — groups with the greatest number of infrastructure objects with errors (red), groups with the greatest number of infrastructure objects with warnings (yellow) and groups with healthy infrastructure objects (green).

Click a chart segment to drill down to the list of alarms with the corresponding status for the selected Business View group.

Latest Alarms

The list displays the latest 15 alarms for the selected category. Click a link in the **Source** column to drill down to the list of alarms triggered for a specific infrastructure object.

Alarms by Object

The list displays 15 objects with the greatest number of alarms.

The value in the **Alarms** column shows the number of errors and warnings for an object. For example, 3/1 means that there are 3 errors and 1 warning triggered for the object. Click a link in the **Source** column to drill down to the list of alarms triggered for a specific infrastructure object.

For more information, see Working with Triggered Alarms.

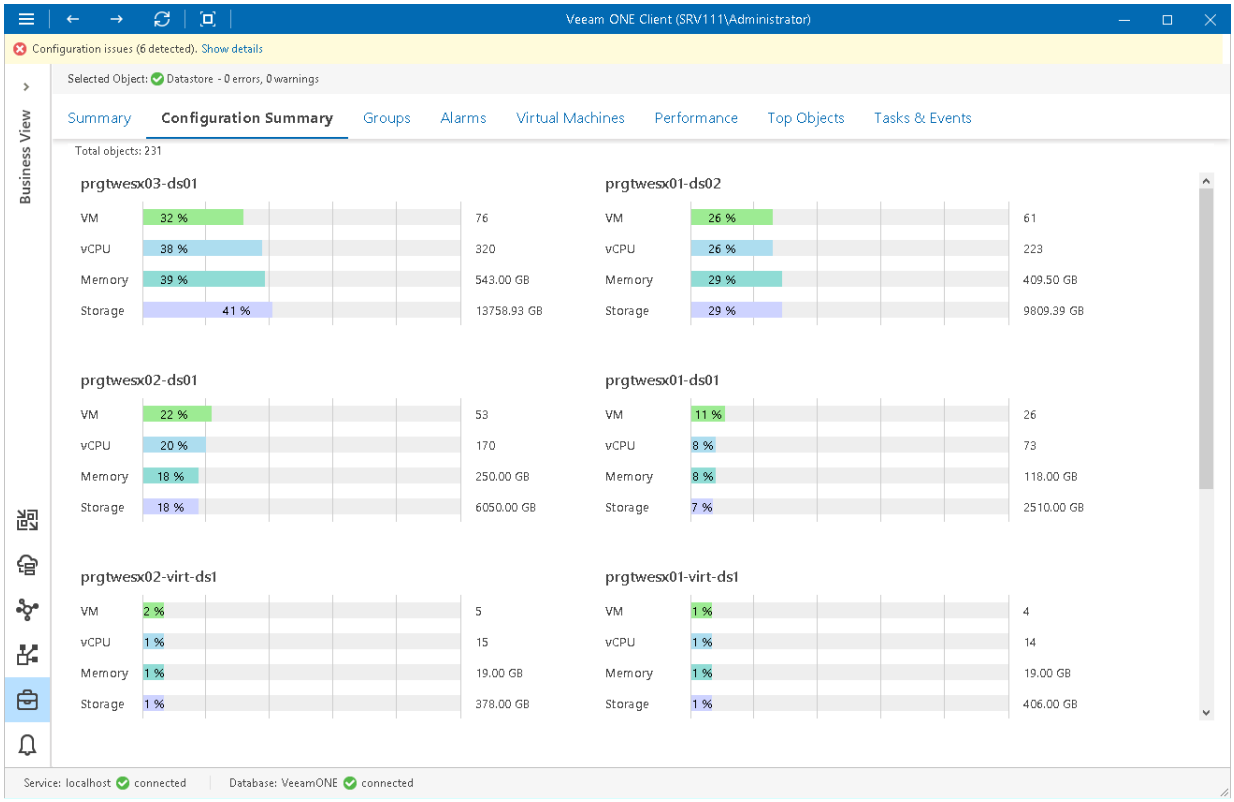
Category Configuration Summary

The **Configuration Summary** dashboard displays categorization details for different types of virtual infrastructure objects.

The dashboard acts as detailed monitoring panel: it presents virtual infrastructure objects from the perspective of business view categories. For each category, **Configuration Summary** provides information on the groups included in the category, shows how many objects belong to these groups, and provides information on the total number of objects in a group of their vCPU, memory and storage resources.

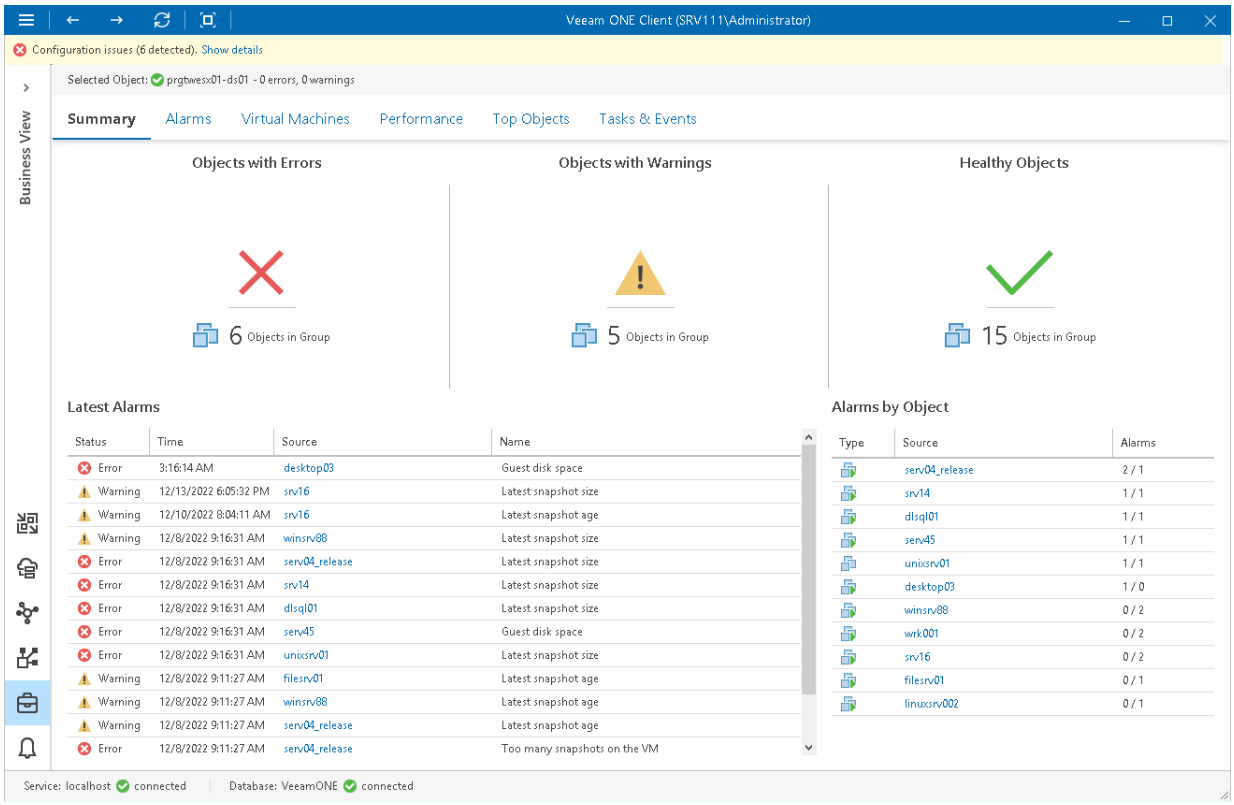
At the top of the dashboard, Veeam ONE Client displays information on the total number of objects included in a category.

> **NOTE:**
>
> This dashboard is not available for the *Computers* and *Enterprise Applications* categories.



Group Summary

The group summary dashboard provides an overview of the health status and performance for the virtual infrastructure objects that belong to the chosen group.



Error Objects, Warning Objects, Healthy Objects

The charts reflect the health status of virtual infrastructure objects in the group — objects with errors (red), objects with warnings (yellow) and healthy objects (green). Click the problematic chart to drill down to the list of alarms for objects with the chosen health status.

Latest Alarms

The list displays the latest 15 alarms for virtual infrastructure objects in the selected group. Click a link in the **Source** column to drill down to the list of alarms triggered for a specific virtual infrastructure object.

Alarms by Object

The list displays 15 objects with the greatest number of alarms.

The value in the **Alarms** column shows the number of errors and warnings for an object. For example, 3/1 means that there are 3 errors and 1 warning triggered for the object. Click a link in the **Source** column to drill down to the list of alarms triggered for a specific virtual infrastructure object.

For more information, see Working with Triggered Alarms.

Virtual Infrastructure Objects Summary

Veeam ONE allows you not only to view category and group summary, but also to monitor the summary state of categorized virtual infrastructure objects — VMs, hosts, clusters and datastores. To view a summary dashboard for a specific virtual infrastructure object:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click **Business View**.

3. In the inventory pane, select the necessary categorized object.

4. Open the **Summary** tab.

For details on virtual infrastructure summary dashboards, see VMware vSphere Summary Dashboards and Microsoft Hyper-V Summary Dashboards.

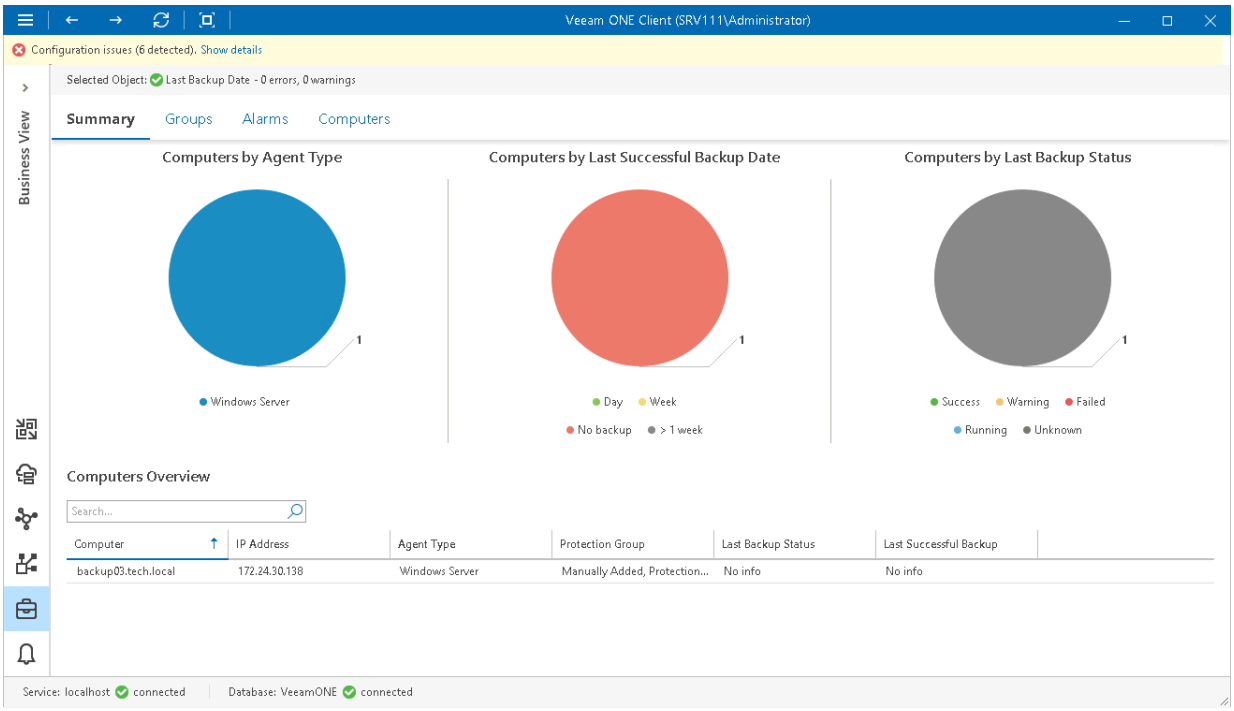
Computers Summary

The **Computers** summary dashboard presents the health status overview for computers protected with Veeam Agent for Microsoft Windows, Veeam Agent for Linux, Veeam Agent for Mac and Veeam Agent for Unix. The dashboard scope includes computers whose backups are managed by Veeam Backup & Replication servers that you monitor in Veeam ONE.

The dashboard is available for different levels of the categorization model:

- For the **Computers** node, the dashboard presents all computers from the monitored infrastructure

- For the category node, the dashboard to presents computers included in groups within the selected category



Computers by Agent Type

The chart displays types of computers protected with Veeam Agent for Microsoft Windows, Veeam Agent for Linux, Veeam Agent for Mac and Veeam Agent for Unix.

Every chart segment shows the number of computers of a specific platform and type — the number of managed Windows servers, the number of managed Windows workstations, the number of managed Linux servers, the number of managed Linux workstations, the number of managed Mac servers, the number of managed Mac workstations, the number of managed AIX servers, the number of managed Solaris servers.

Computers by Last Successful Backup Date

The chart displays the time interval when the latest successful backup was created for computers running Veeam Agent for Microsoft Windows, Veeam Agent for Linux, Veeam Agent for Mac and Veeam Agent for Unix.

Every chart segment shows the number of computers with last successful backups created within a specific interval — the number of computers with backups created not older than a day ago, computers with backups created not older than a week ago, computers with backups older than a week, and computers with no backups.

Computers by Last Backup Status

The chart displays the latest status of backup jobs for computers running Veeam Agent for Microsoft Windows, Veeam Agent for Linux, Veeam Agent for Mac and Veeam Agent for Unix.

Every chart segment shows how many jobs ended with a specific status — failed jobs, jobs that ended with warnings, successfully performed jobs, jobs that are currently running, and jobs whose status is unknown.

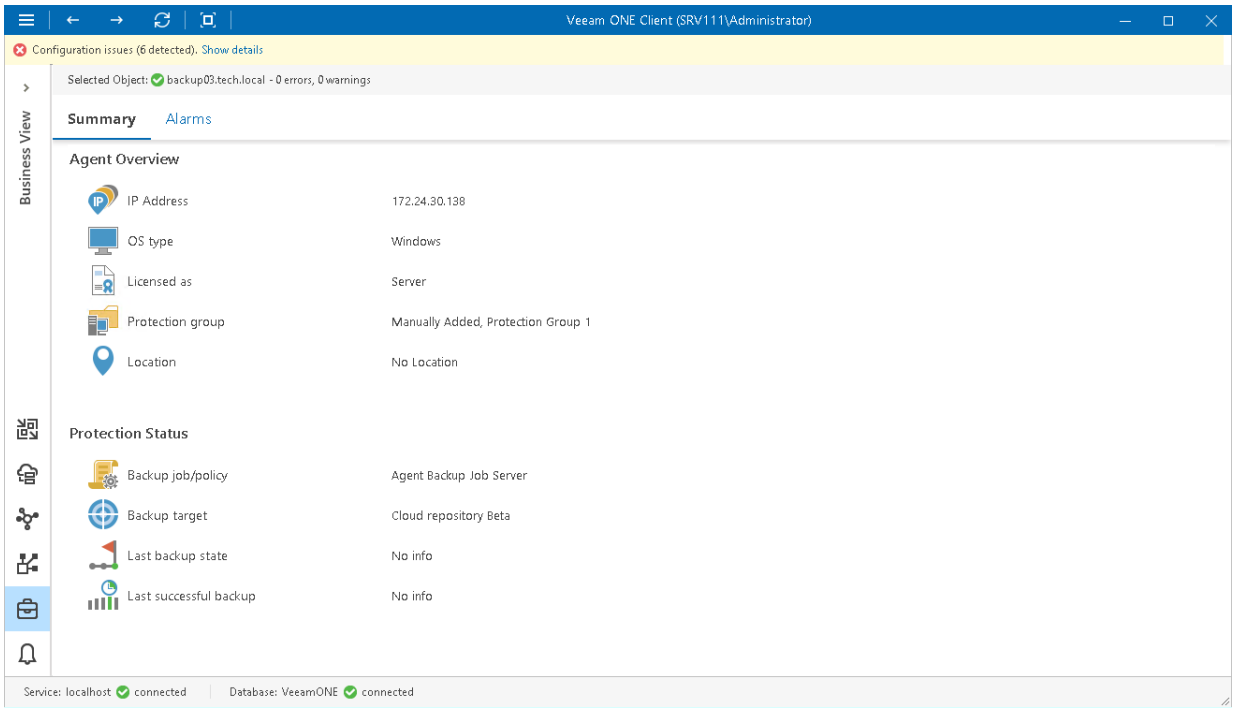
Computers Overview

The table provides details on computers running Veeam Agent for Microsoft Windows, Veeam Agent for Linux, Veeam Agent for Mac and Veeam Agent for Unix:

- **Computer** — computer name.
- **IP Address** — computer IP address.
- **Agent Type** — operation mode of a backup agent on the computer *(Windows server*, *Windows workstation*, *Linux Server*, *Linux Workstation*, *Mac Server*, *Mac Workstation*, *AIX Server*, *Solaris Server*).
- **Protection Group** — name of a protection group in which the computer is included.
- **Last Backup State** — the latest status of a backup job (*Success*, *Warning*, *Failed*, *Running*, *No Info*).
- **Last Successful Backup** — date and time when the latest successful backup was created for the computer.

Computer Details

The **Summary** dashboard for a single computer node presents an overview and protection status details for computers running Veeam Agent for Microsoft Windows, Veeam Agent for Linux, Veeam Agent for Mac and Veeam Agent for Unix.



Agent Overview

The section provides the following details:

- IP address of the computer running Veeam Agent for Microsoft Windows, Veeam Agent for Linux, Veeam Agent for Mac or Veeam Agent for Unix
- Type of an OS installed on the computer (*Windows*, *Linux*, *macOS*, *UNIX*)
- Operation mode in which the computer is licensed
- Name of the protection group in which the computer is included

- Location of the computer, as specified in Veeam Backup & Replication

Protection Status

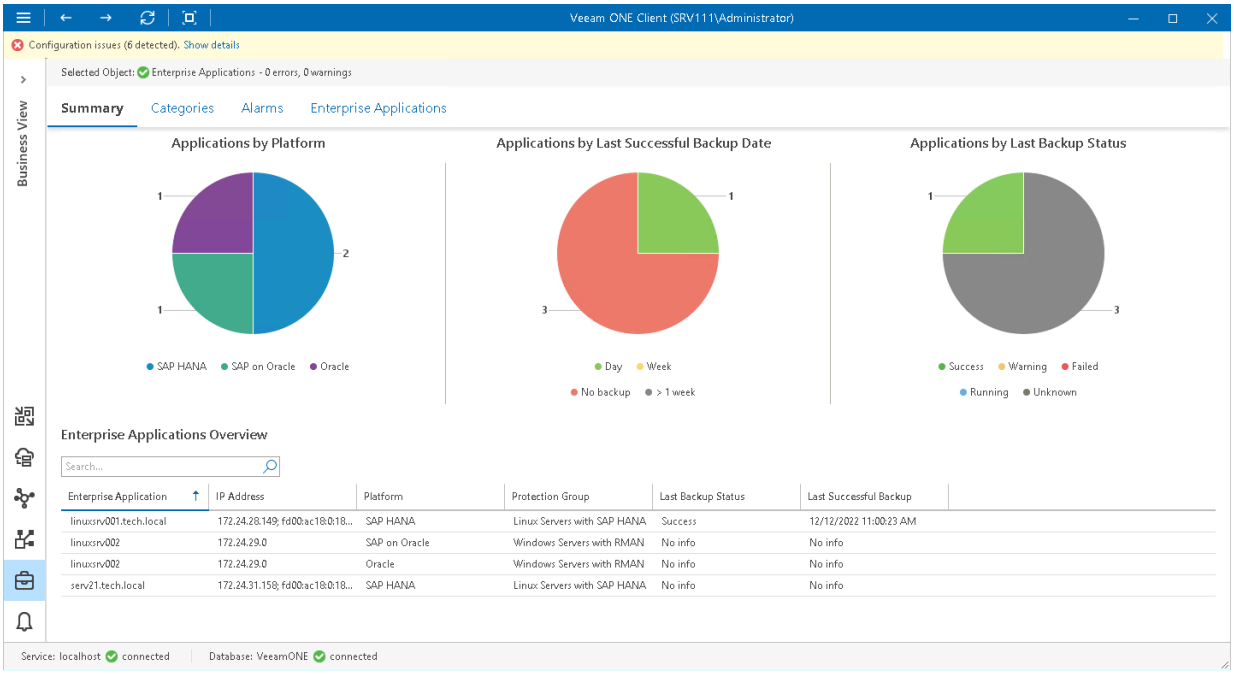
The section provides the following details:

- Name of the backup policy applied to the computer, or the backup job in which a computer is included
- Target location in which computer backups are stored
- The latest status of the backup job session (*Success*, *Warning*, *Failed*, *Running*, *No Info*)
- Date and time when the latest successful backup was created for the computer

Enterprise Applications Summary

The **Enterprise Applications** summary dashboard presents the health status overview for applications protected with Veeam Plug-ins for SAP HANA, SAP on Oracle, Oracle RMAN and Microsoft SQL Server. The dashboard scope includes applications whose backups are managed by Veeam Backup & Replication servers that you monitor in Veeam ONE.

> **NOTE:**
>
> To be able to see enterprise application data in Veeam ONE, you must add the application into a protection group and configure a backup policy in Veeam Backup & Replication. For details on protection groups and application backup policies, see section Veeam Plug-in Management of the Veeam Plug-ins for Enterprise Applications Guide.



Applications by Platform

The chart displays types of application protected with enterprise application plug-ins.

Every chart segment shows the number of applications of a specific platform — the number of protected SAP HANA, SAP on Oracle, Oracle RMAN and Microsoft SQL Server applications.

Applications by Last Successful Backup Date

The chart displays the time interval when the latest successful backup was created for enterprise applications.

Every chart segment shows the number of computers with last successful backups created within a specific interval — the number of applications with backups created not older than a day ago, applications with backups created not older than a week ago, applications with backups older than a week, and applications with no backups.

Applications by Last Backup Status

The chart displays the latest status of backup jobs for enterprise applications.

Every chart segment shows how many jobs ended with a specific status — failed jobs, jobs that ended with warnings, successfully performed jobs, jobs that are currently running, and jobs whose status is unknown.

Enterprise Applications Overview

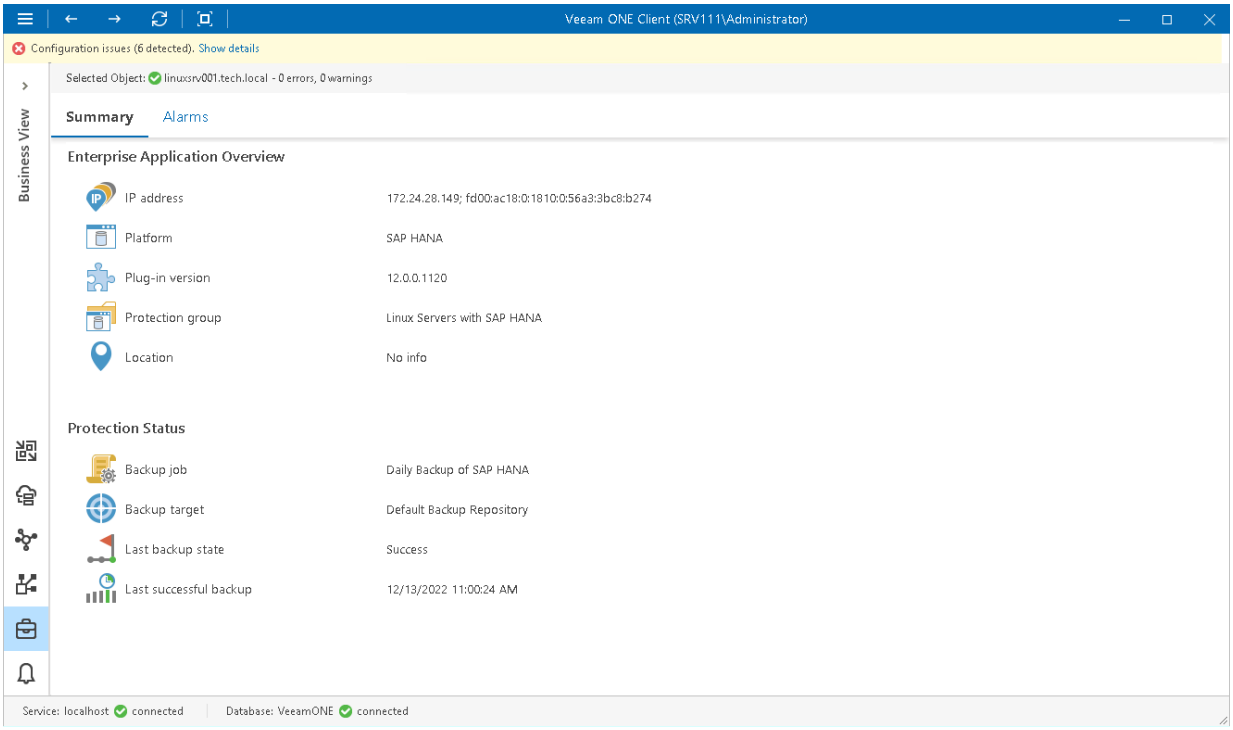
The table provides details on protected enterprise applications:

- **Enterprise Application** — name of the machine on which the enterprise application is installed.
- **IP Address** — IP address of the machine on which the enterprise application is installed.
- **Platform** — enterprise application platform (*SAP HANA*, *SAP on Oracle*, *Oracle*, *Microsoft SQL Server*).
- **Protection Group** — name of a protection group in which an application is included.
- **Last Backup Status** — the latest status of a backup job (*Success*, *Warning*, *Failed*, *Running*, *No Info*).
- **Last Successful Backup** — date and time when the latest successful backup was created for the enterprise application.

Enterprise Application Details

The **Summary** dashboard for a single application node presents an overview and protection status details for applications protected with Veeam Plug-ins for SAP HANA, SAP on Oracle, Oracle RMAN and Microsoft SQL Server.

> **NOTE:**
>
> To be able to see enterprise application data in Veeam ONE, you must add the application into a protection group and configure a backup policy in Veeam Backup & Replication. For details on protection groups and application backup policies, see section Veeam Plug-in Management of the Veeam Plug-ins for Enterprise Applications Guide.



Enterprise Application Overview

The section provides the following details:

- IP address of a machine on which the enterprise application is installed
- Enterprise application platform (*SAP HANA*, *SAP on Oracle*, *Oracle*, *Microsoft SQL Server*)
- Version of the enterprise application plug-in
- Name of the protection group in which the enterprise application is included
- Location of the enterprise application, as specified in Veeam Backup & Replication

Protection Status

The section provides the following details:

- Name of the backup job in which the enterprise application is included
- Target location in which enterprise application backups are stored
- The latest status of the backup job session (*Success*, *Warning*, *Failed*, *Running*, *No Info*)
- Date and time when the latest successful backup was created for the enterprise application

Business View Alarms

You can create and manage alarms for virtual infrastructure objects organized into Business View groups. For example, you can group your virtual infrastructure objects by a department to which these objects belong. For each group, you can configure alarms with severity levels and thresholds corresponding to requirements of a specific department.

For Business View, Veeam ONE supports all alarms that apply to categorized objects — VMs, hosts, clusters, datastores, computers and enterprise applications.

To view the list of alarms for categorized objects:

1. Open Veeam ONE Client.

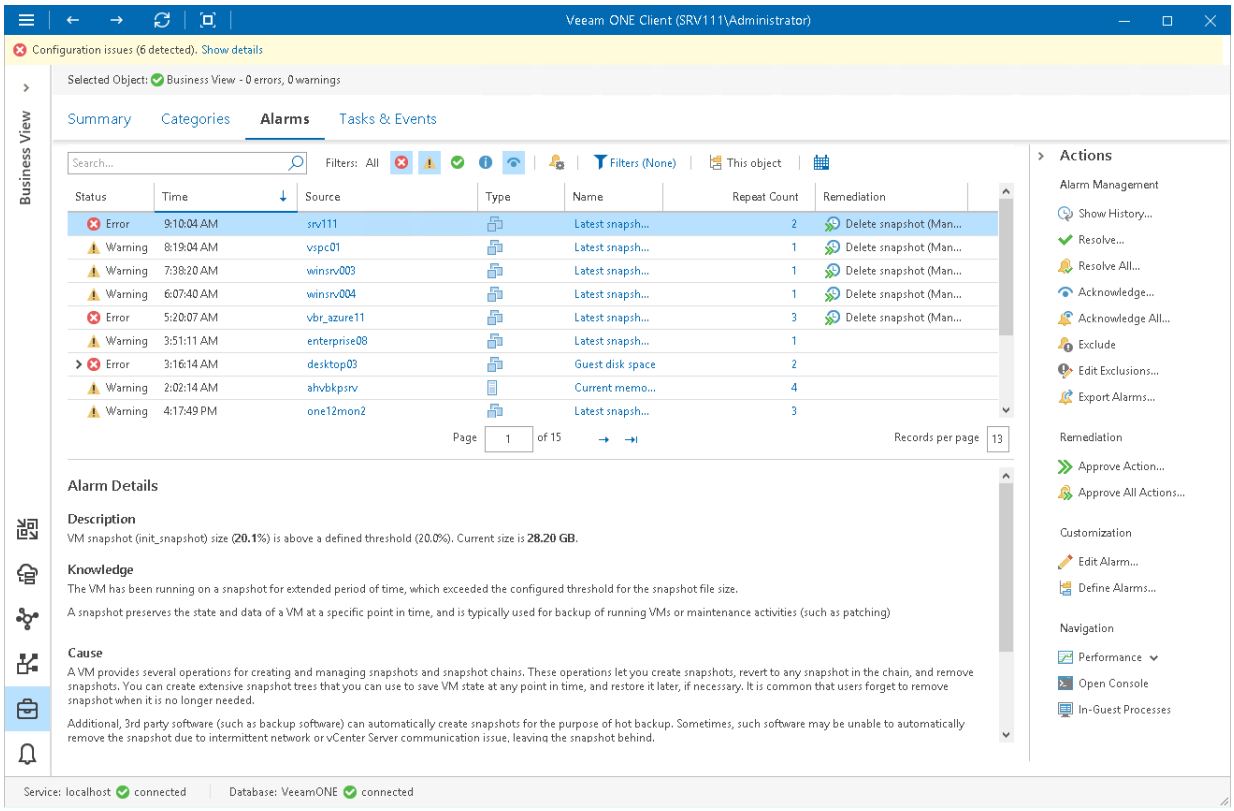
   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click **Business View**.

3. In the inventory pane, select the necessary category, group or object.

4. Open the **Alarms** tab.

For more information, see Working with Triggered Alarms.



Business View Objects

You can view the list of infrastructure objects within the Business View node — object type, platform, category and group.

To view the list of objects:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click **Business View**.

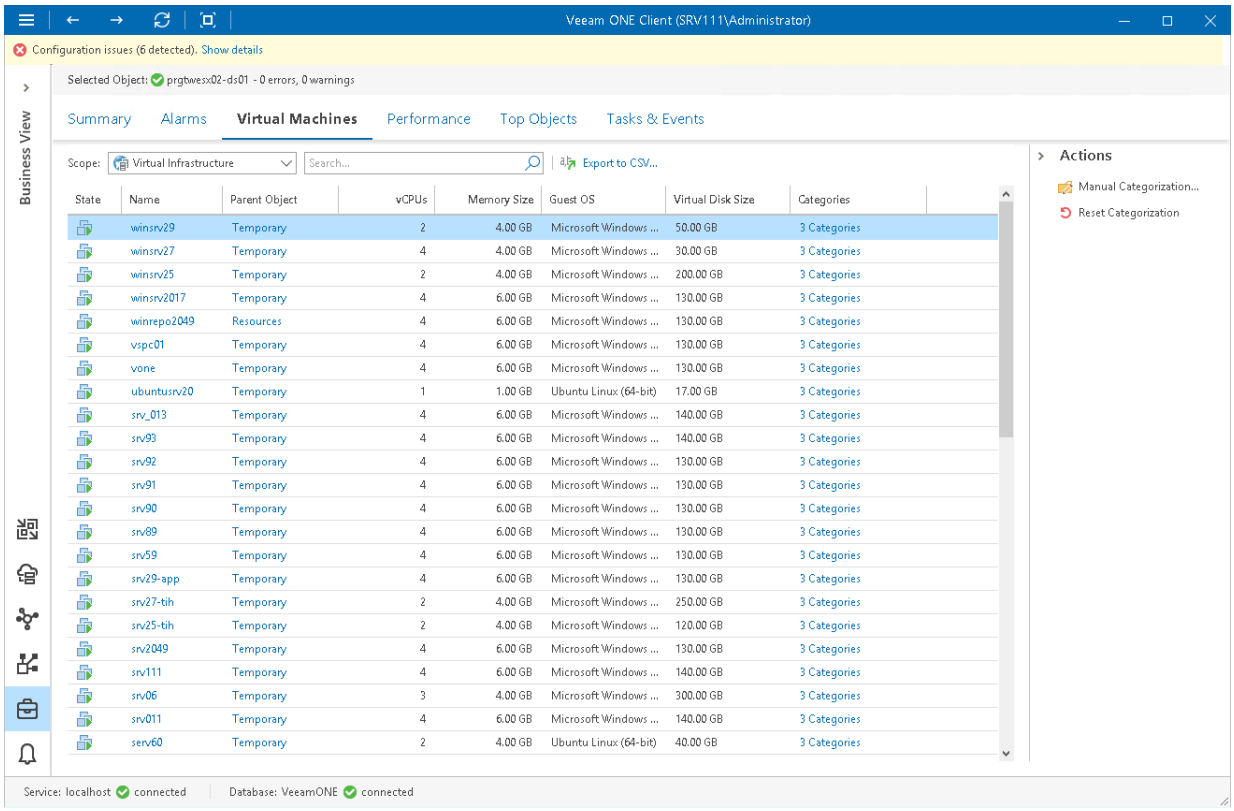
3. In the inventory pane, select the necessary node.

4. Open the tab with the name of the object: *Virtual Machines*, *Hosts*, *Datastores*, *Clusters*, *Computers*, *Enterprise Applications*.

5. To find the necessary object by name, use the **Search** field at the top of the list.

   To display objects of a specific virtual infrastructure node, select the necessary node in the **Scope** field at the top of the list.

6. Click column names to sort objects by a specific parameter.



For every object in the list, the following details are available.

Virtual Machines

- **State** — state of the VM (*powered on*, *powered off*, *suspended*)
- **Name** — name of the VM

- **Parent Object** — name of the parent object for the VM

  Click a link in this column to switch to the **Virtual Infrastructure** for the parent object.
- **vCPUs** — number of virtual CPUs configured for the virtual machine
- **Memory Size** — amount of memory resources allocated to the VM
- **Guest OS** — guest operating system installed on the VM
- **Virtual Disk Size** — size of the VM virtual disk
- **Categories** — number of categories to which the VM is included

  Click a link in this column to see all categories and groups in which the VM is included.

Hosts

- **Name** — name of the host
- **Parent Object** — name of the parent object for the host

  Click a link in this column to switch to the **Virtual Infrastructure** for the parent object.
- **CPU Count** — number of CPU cores on the host
- **CPU Speed** — frequency of CPU cores on the host
- **Memory Size** — total capacity of the host
- **VM Count** — number of VMs residing on the host
- **Categories** — number of categories to which the host is included

  Click a link in this column to see all categories and groups in which the host is included.

Datastores

- **Datastores** — name of the datastore
- **Parent Object** — name of the parent object for the datastore

  Click a link in this column to switch to the **Virtual Infrastructure** for the parent object.
- **File System** — type of the file system on the datastore
- **Capacity** — total capacity of the datastore
- **Free Space** — free space remaining on the datastore
- **VM Count** — number of VMs residing on the datastore
- **Categories** — number of categories to which the datastore is included

  Click a link in this column to see all categories and groups in which the datastore is included.

Clusters

- **Clusters** — name of the cluster
- **Parent Object** — name of the parent object for the cluster

  Click a link in this column to switch to the **Virtual Infrastructure** for the parent object.

- **CPU Count** — number of CPU cores in the cluster
- **CPU Speed** — total frequency of all CPU cores in the cluster
- **Memory Size** — total size of memory available for the cluster
- **Host Count** — number of hosts in the cluster
- **VM Count** — number of VMs residing on the cluster
- **Categories** — number of categories to which the cluster is included

  Click a link in this column to see all categories and groups in which the cluster is included.

Computers

- **Name** — name of the computer on which Veeam backup agent is installed
- **IP Address** — IP address of the computer on which Veeam backup agent is installed
- **Cluster** — name of a failover cluster added to a protection group
- **Agent Type** — type of the computer OS and mode in which Veeam backup agent job runs (*Windows Server*, *Windows Workstation*, *Linux Server*, *Linux Workstation*, *Mac Server*, *Mac Workstation*, *Solaris Server* or *AIX Server*)
- **Location** — location assigned to the computer in Veeam Backup & Replication
- **Agent Version** — version of the Veeam backup agent
- **Protection Group** — name of the protection group to which the computer is included
- **Backup Server** — name of the Veeam Backup & Replication server that manages the Veeam backup agent
- **Backup Job / Policy** — name of the backup job or policy assigned to the Veeam backup agent on the computer
- **Last Backup State** — state of the latest job session
- **Last Successful Backup** — date and time when the latest restore point was created
- **Categories** — number of categories to which the computer is included

  Click a link in this column to see all categories and groups in which a computer is included.

Enterprise Applications

- **Name** — name of the machine on which the enterprise application plug-in is installed
- **IP Address** — IP address of the machine on which the enterprise application plug-in is installed
- **Platform** — enterprise application platform
- **Location** — location assigned to the application in Veeam Backup & Replication
- **Plug-in Version** — version of the Veeam Plug-in
- **Protection Group** — name of the protection group to which the application is included
- **Backup Server** — name of the Veeam Backup & Replication server that manages the Veeam Plug-in
- **Backup Policy** — name of the backup job or policy assigned to the Veeam Plug-in

- **Last Backup State** — state of the latest job session
- **Last Successful Backup** — date and time when the latest restore point was created
- **Categories** — number of categories to which the application is included

  Click a link in this column to see all categories and groups in which a computer is included.

You can choose what columns to show or hide in the objects table:

- To hide one or more columns, right-click the table header, and clear check boxes next to the corresponding data fields.
- To make hidden columns visible, right-click the table header, and select check boxes next to the corresponding data fields.

Exporting Object Details to CSV

You can export categorization data to a CSV file and save it for documenting purposes:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.
2. At the bottom of the inventory pane, click **Business View**.
3. In the inventory pane, select the necessary node.
4. Open the tab with the name of the object: *Virtual Machines*, *Hosts*, *Datastores*, *Clusters*, *Computers*, *Enterprise Applications*.
5. To find the necessary object by name, use the **Search** field at the top of the list.
6. At the top of the list, click **Export to CSV** and save the file.

Business View Performance Charts

You can launch performance charts for infrastructure objects organized into business groups. You can view the performance of objects in custom groups, and identify whether there are enough resources allocated to these objects.

For Business View, Veeam ONE supports all dashboards that apply to categorized virtual infrastructure objects — VMs, hosts, clusters and datastores.

To access a performance chart for a categorized virtual infrastructure object:

1. Open Veeam ONE Client.

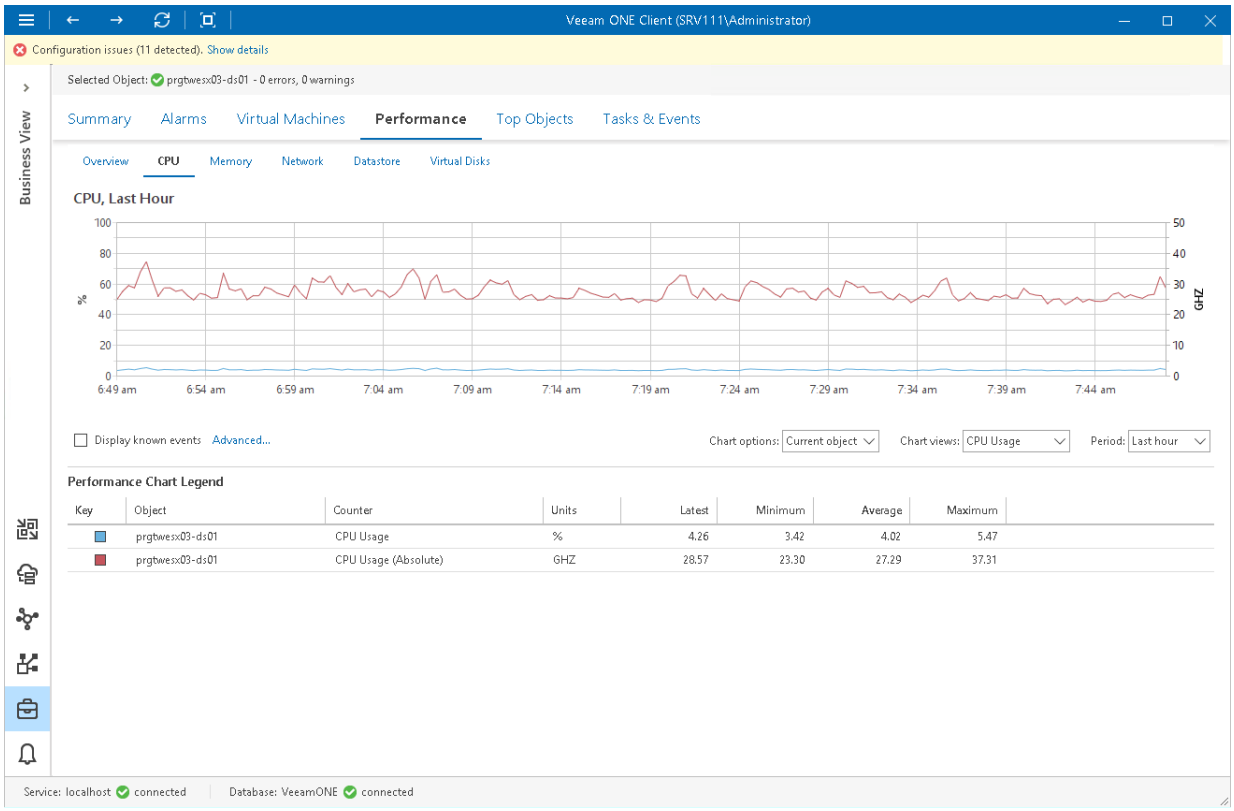
   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click **Business View**.

3. In the inventory pane, select the necessary object.

4. Open the necessary performance chart tab.

For details on performance charts, see VMware vSphere Performance Charts and Microsoft Hyper-V Performance Charts.



Troubleshooting Performance of Categorized Objects

Veeam ONE Client includes a set of dashboards that give you enhanced control over categorized virtual infrastructure objects and facilitate the troubleshooting process:

- Top N dashboards display top and bottom resource consumers in a group:
  - To view VMs that consume the greatest amount of compute, network and storage resources, choose the necessary VM group in the inventory pane and go to the **Top Objects** tab.
  - To view the most loaded hosts, choose the necessary host group in the inventory pane and navigate to **Top Objects** > **Top Hosts**.
  - To view the least loaded hosts, choose the necessary host group in the inventory pane and navigate to **Top Objects** > **Bottom Hosts**.

  For details on the **Top and Lowest Load** dashboards, see VMware vSphere Top Objects and Microsoft Hyper-V Top Objects.
- **Tasks & Events** dashboard shows tasks and events targeted for categorized objects.

  To view the list of tasks and events for a categorized virtual infrastructure object, select it in the inventory pane and go to the **Tasks & Events** tab.
- **Processes** dashboard provides control over processes and services running inside the guest OS of a VM.
  - For Windows- based machines, you can view, end or restart processes.
  - You can view or end daemons on Linux-based machines.

  To view the list of processes, select the necessary VM in the inventory pane and go to the **Processes** tab.

  For details on VM processes, see VMware vSphere In-Guest Processes and Microsoft Hyper-V In-Guest Processes.
- **Console** view allows you to access the VM guest OS right from the Veeam ONE Client interface.

  To access a VM console, select the necessary VM in the inventory pane and go to the **Console** tab.

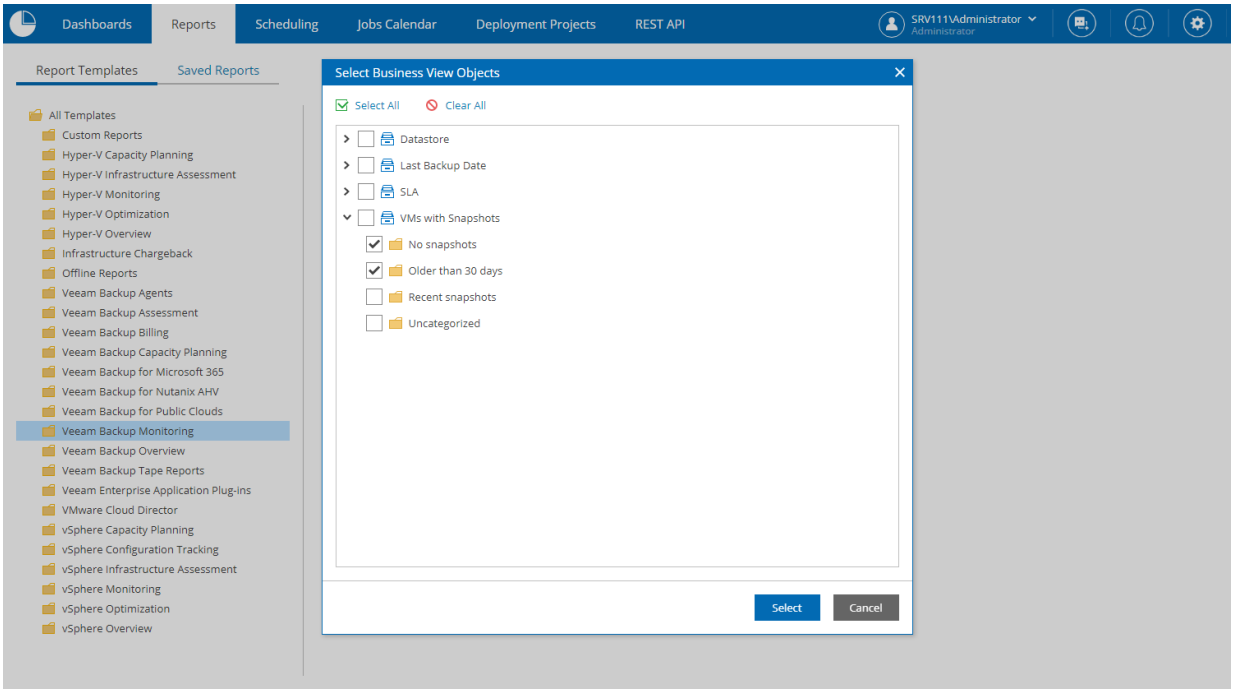
  For details on working with VM console, see VMware vSphere VM Console and Microsoft Hyper-V VM Console.

Business View Reporting

Veeam ONE Web Client integrates with Business View and allows you to create reports and dashboards for business view groups. For example, if you group VMs by department, you can create reports for a specific department in your organization.

The following example shows how you can create the **Protected VMs** report for specific business view groups:

1. Open Veeam ONE Web Client.
2. Open the **Reports** section.
3. In the hierarchy on the left, select the **Veeam Backup Monitoring** folder.
4. In the displayed list of reports, click the **Protected VMs** report.
5. From the **Business view objects** list, select business groups for which you want to create a report.
6. Specify other report parameters and click **Preview**.



Veeam ONE Web Client will present data from the business point of view — that is, for the selected business groups.



Protected VMs

Description

This report lists protected and unprotected VMware vSphere and Microsoft Hyper-V VMs including their last backup job status.
Note: VM replicas not protected by any Veeam Backup & Replication job are not accounted in this report.

Report Parameters

Scope:	Virtual Infrastructure
RPO:	24 hours (12/19/2022 8:00:00 AM)
VM exclusion rule:	
Job types:	VM backup, Replication, Backup copy, Cloud Director backup, Cloud Director replication
Business View objects:	VMs with Snapshots: Older than 30 days, No snapshots
Analyze VM templates:	No
Excluded jobs:	-

Summary

VMs Overview

Total VMs:	197
Including VM Replicas:	9
Protected VMs:	2
With Backup:	2
With Replication:	0
Unprotected VMs:	186

Protected VMs

VM Last Backup State

VM Last Backup Age

Report created: 12/20/2022 7:22:38 AM ((UTC-08:00) Pacific Time (US & Canada))

Page: 1 of 6

Working with Alarms

Veeam ONE alarms notify users about important events, changes and potential problems in the managed virtual and backup environment. Alarms speed up the process of identifying, troubleshooting and reacting to issues that may affect mission-critical services and business operations.

Out of the box, Veeam ONE comes with a set of predefined alarms so that you can start monitoring your environment immediately after deploying the solution. Predefined alarms include:

- Alarms Overview dashboard
- Veeam Backup & Replication alarms
- Veeam Backup for Microsoft 365 alarms
- VMware vSphere and VMware Cloud Director alarms
- Microsoft Hyper-V alarms
- Internal alarms for monitoring issues with Veeam ONE

Predefined alarms are based on best practices and include an extensive knowledge base. When a problem occurs, you will not only receive an alert but will also have all the necessary information for troubleshooting and finding the root cause of the issue.

About Alarms

Veeam ONE offers an extensive set of tools that will help you develop your own alarm model. Depending on your requirements for the virtual and backup environment, you can customize predefined alarms, or create new alarms. This section describes various aspects of alarms in Veeam ONE, including alarm rules, severity levels, assignment options, response actions and other.

How Alarms Work

After you connect virtual or backup servers, Veeam ONE starts collecting data about objects in your environment and their health state, and checks this data against alarm configuration in real time. If Veeam ONE detects that behavior or state of an infrastructure object meets alarm criteria, or that a specific event occurs, it triggers an alarm with the defined severity level.

After an alarm is triggered, Veeam ONE Client will display alarm details and information about the affected object. You can view, acknowledge or resolve the alarm.

If an alarm is configured to perform an action, Veeam ONE performs a response action after the alarm is triggered — sends an email notification, SNMP trap, or runs a predefined or custom script.

If the event, state or condition that triggered the alarm is resolved, Veeam ONE updates the alarm status in the console.

Alarm Rules

Every alarm has one or more associated rules that define conditions to trigger the alarm, severity of the alarm and rule suppression settings.

There are the following types of alarm rules:

- **Event-based rules** are rules for alerting about specific events that occur in the backup or virtual infrastructure. These can be events issued by the hypervisor or Veeam Backup & Replication events.
- **Rules for a specific condition or state** are rules for alerting about important conditions or changed state of infrastructure objects.
- **Rules based on existing alarms** are rules for alerting about other alarms triggered in Veeam ONE.
- **Rules based on resource usage counters** are rules for alerting about abnormal resource usage of infrastructure objects.

For the full list of available rule types, see Alarm Rules Reference.

Aggregation Type

An aggregation type defines how Veeam ONE analyzes performance data collected for a specified period of time, and compares it to the threshold.

The following table explains how Veeam ONE alarms trigger depending on the aggregation type and rule condition:

Aggregation Type	Condition	
	Above	Below
Min	Veeam ONE takes the **minimum** value across the collected performance parameters and compares it to the specified threshold. If the value is above the threshold, Veeam ONE triggers an alarm. That means that the alarm triggers only if all the values are above the threshold.	Veeam ONE takes the **minimum** value across the collected performance parameters and compares it to the specified threshold. If the value is below the threshold, Veeam ONE triggers an alarm. That means that the alarm triggers if at least one of the collected values is below the threshold.
Avg	Veeam ONE takes the **average** value across the collected performance parameters. The alarm triggers if this value is above the threshold.	Veeam ONE takes the **average** value across the collected performance parameters. The alarm triggers if this value is below the threshold.
Max	Veeam ONE takes the **maximum** value across the collected performance parameters and compares it to the specified threshold. If the value is above the threshold, Veeam ONE triggers an alarm. That means that the alarm triggers if at least one of the collected values is above the threshold.	Veeam ONE takes the **maximum** value across the collected performance parameters and compares it to the specified threshold. If the value is below the threshold, Veeam ONE triggers an alarm. That means that the alarm triggers only if all the values are below the threshold.

To learn how to configure rules based on performance counters, see Adding Rules Based on Resource Usage Counters.

Analysis Depth

Alarm rules may include the **Analysis depth** parameter. This parameter defines the number of latest performance data values among which an average value is calculated. Each newly collected value is compared to the average value. If the new value is above or below the average value according to severity levels, Veeam ONE triggers the alarm.

Linking Rules

You can link two or more rules using Boolean operators:

- **AND** — if rules are joined with this operator, an alarm is triggered when conditions for all linked rules are met.
- **OR** — if rules are joined with this operator, an alarm is triggered when a condition for any of the linked rules is met.

You can form several groups of linked rules and join them with different operators. To learn how to link rules, see Linking Rules.

Alarm Severity

Every alarm rule is associated with a specific severity level. The severity level defines how serious the state or event is and how badly it can affect an object health state.

There are four severity levels that are color-coded as follows:

- **Error (red)** indicates a critical situation or a major problem that requires immediate action.
- **Warning (yellow)** indicates a potential problem or non-critical issue that needs your attention. If the issue is left without attention, it can potentially cause a major problem.
- **Resolved (green)** indicates that the issue was eliminated because of the changed conditions, or shows that the alarm was resolved manually.
- **Information (blue)** indicates general information about a specific condition or health state of an object.

You can define different severity levels for conditions of different intensity. For example, if the level of memory usage must not exceed 75%, you can create the following alarm rules:

- If the memory usage is over 70%, an alarm with the *Warning* severity level must be triggered.
- If the memory usage is over 75%, an alarm with the *Error* severity level must be triggered.

In such situation, if the memory usage level is constantly growing and exceeds 70%, Veeam ONE will trigger a warning alarm, notifying about a potentially dangerous situation. If the memory usage level keeps on growing and exceeds the level of 75%, Veeam ONE will trigger an error alarm notifying about the severe danger.

Alarm Assignment Options

You can assign Veeam ONE alarms to objects of the backup or virtual infrastructure. There are several options to assign alarms:

- **Object-level assignment** — you can assign an alarm to a single object.

  This type of assignment can be useful if you need to customize alarms for specific objects, like separate hosts, VMs or backup infrastructure components.

- **Group-level assignment** — you can assign an alarm to a group of objects (for example, to an infrastructure container or Business View group).

  This type of assignment can be useful if you need to assign an alarm to all objects under a specific parent entity. For example, to all VMs residing on a host or to all backup proxies connected to a backup server.

- **Infrastructure-level assignment** — you can assign an alarm to all objects of a particular type in the entire managed environment.

  This is the default type of assignment used for all predefined alarms.

You can combine various assignment options. For example, you can assign an alarm to all VMs running on a chosen host, to all VMs in a Business View group and to a few single VMs at the same time.

In addition to flexible alarm assignment options, Veeam ONE offers a possibility to exclude specific objects or object groups from the assignment scope. Thus, you can easily point out what part of your environment the alarm must ignore.

Alarm Notification Options

You can configure Veeam ONE to send notifications when alarms are triggered or change their status. Depending on alarm configuration, Veeam ONE can:

- Send email notifications to the default notification group or to specific recipients
- Send SNMP traps to third-party consoles

Alarm notification options are defined in alarm settings. You can specify when Veeam ONE must notify you about alarm status change:

- Alarm severity changes to *Error*
- Alarm severity changes to *Error* or *Warning*
- Alarm is resolved
- Alarm severity changes to any level (*Error*, *Warning* or *Resolved*)

By default, all predefined alarms are configured to send email notifications to the default notification group when the alarm severity changes to any level. You can change alarm notification settings and define conditions when notifications must be sent.

Alarm Remediation Actions

To automate virtual and backup infrastructure troubleshooting, you can configure Veeam ONE to run remediation actions as soon as alarms are triggered.

> **NOTE:**
>
> To run remediation actions for the backup infrastructure, you must have Veeam ONE agents installed on connected Veeam Backup & Replication servers. For details on installing and configuring Veeam ONE agents, see Managing Veeam ONE Agents.

Veeam ONE offers the following types of remediation for alarms:

- Predefined actions that are configured for the most commonly used out-of-the-box alarms. For each alarm severity level, Veeam ONE can run only one predefined action.

  For the list of alarms with predefined remediation actions, see Remediation Actions.

- Custom scripts that you can specify in the settings of any alarm. For each severity level, Veeam ONE can run one or more custom scripts.

You can select the resolution type for alarm remediation actions:

- **Manual** – when an alarm is triggered, you must approve the remediation action manually. This type of resolution is default for alarms with predefined remediation actions.
- **Automatic** – when an alarm is triggered, Veeam ONE will automatically run a predefined remediation action or custom script.

Veeam ONE makes 3 attempts to run a remediation action or script. If the remediation is successful, the alarm status will change to Acknowledged. If for some reason Veeam ONE fails to run an action or script, the alarm will remain active.

Advanced Alarm Options

To avoid alarm storms and ensure that critical issues are not overlooked, you can use advanced alarm configuration options — alarm suppression and alarm modeling.

- **Alarm suppression** is used to disregard events and prevent sending alarms when specific activities are performed. For example, during backup Veeam ONE may send a great number of alarms informing about potential problems or increased resource pressure. Alarm suppressing allows you to pause specific alarms during such activities, or at a specific period of time when you plan to perform resource-consuming operations.
- **Alarm modeling** is used to verify the created alarm scheme and estimate the need for adjusting alarm settings. During alarm modeling, Veeam ONE applies alarm settings to collected historical data and produces a forecast on the number of alarms that will be sent over a specific period of time. If the number of alarms is too high, alarm thresholds may need to be changed to avoid numerous useless alarms. If the number is too low, the sensitivity of alarms may need to be increased so that you do not miss important issues.

Alarm Reports

In addition to receiving alarms in real-time, Veeam ONE allows you to analyze alarm statistics. You can use Veeam ONE Web Client dashboards and reports to track how the number of alarms is changing over time, identify short- and long-term alarm trends, detect the most affected infrastructure objects, troubleshoot commonly encountered issues and ensure that your infrastructure stays fully reliable and productive.

You can use the following dashboards and reports for analyzing alarms:

- **Alarms Dashboard (vSphere and Hyper-V)** analyzes alarms triggered over the previous week. The dashboard provides information on the general health state of virtual infrastructure objects, shows daily roll-ups for errors and warnings, enumerates typical problems and helps to detect the most affected VMs, clusters, hosts and datastores. For more information, see Predefined Veeam ONE Dashboards.
- **Alarms Overview Report (vSphere and Hyper-V)** provides an overview of the current health state of the virtual infrastructure, details the most common alarms and identifies the most affected infrastructure objects. The report consolidates information about raised alarms and provides a summary for the selected time interval. For more information, see Predefined Veeam ONE Reports.
- **Alarms Current State Overview Report (vSphere and Hyper-V)** provides information about all currently unresolved alarms (alarms with the *Error* or *Warning* severity level) and displays reasons why these alarms were triggered. For more information, see Predefined Veeam ONE Reports.
- **Alarms Overview Dashboard** provides a centralized view of all active and historical alarms in the environment, allowing users to quickly assess system health and identify issues. For more information, see Alarms Overview.
- **Backup Alarms Overview Report** provides a detailed report of backup-related alarms, including statuses, occurrences, and affected objects, supporting troubleshooting and compliance efforts.For more information, see Backup Alarms Overview.
- **Current Backup Alarms State Overview** provides real-time status of backup alarms, highlighting ongoing issues and their severity to enable prompt resolution. For more information, see Current Backup Alarms State Overview.

Configuring Alarms

Veeam ONE comes with a set of predefined alarms that cover most common monitoring scenarios. You can customize predefined alarms or create new alarms to meet specific monitoring conditions.

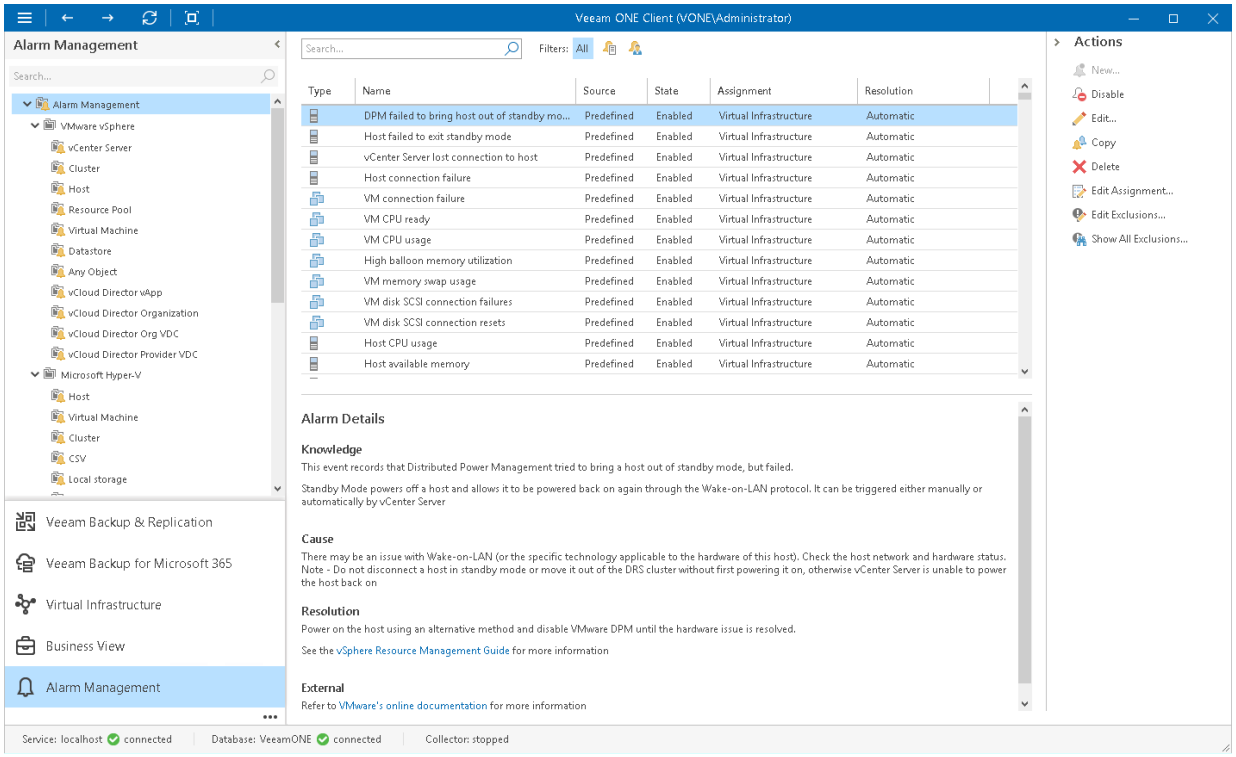
To access the list of alarms:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click **Alarm Management**.

3. To limit the list of displayed alarms, you can use filter buttons — *Show predefined alarms only*, *Show custom alarms only*, *All*.



The Alarm Management view comprises the following panes — the inventory pane, information pane, and actions pane.

- The **inventory pane** on the left shows the alarm management tree with alarm object types: virtual infrastructure components to which alarms can be applied, VMware Cloud Director components, Veeam Backup & Replication and Veeam Backup for Microsoft 365 infrastructure components, and internal alarms.

- The **information pane** contains the list of predefined and custom alarms for the type of object that is selected in the alarm management tree. Every alarm is described with the following details: type, name, source (*Predefined* or *Custom*), state (*Enabled* or *Disabled*), assignment scope and resolve action (*Automatic* or *Manual*). The bottom section of the information pane displays information on the selected alarm, such as summary, cause, resolution and external resources.

- The **Actions** pane on the right displays a list of links that you can use to perform actions with alarms.

Creating Alarms

If predefined alarms do not cover all important events, conditions or state changes about which you need to be notified, you can create custom alarms.

To create a new alarm, perform the following steps.

Step 1. Select Alarm Object Type

All alarms are applied to a certain level of the monitored infrastructure. The **Type** attribute of an alarm defines to what kind of infrastructure objects this alarm applies. The list of available alarm types is displayed in the inventory pane of the **Alarm Management** view.

To create a new alarm, select its type first:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click **Alarm Management**.
3. In the alarm management tree, select the necessary object type.
4. In the **Actions** pane on the right, click the **New** link.

   You can also right-click anywhere in the information pane and choose **New** from the shortcut menu.

> **NOTE:**
>
> Mind that you will not be able to change the alarm type later.

Creating Alarms from Tasks or Events

You can create an alarm that is based on a task or event that occurred in the monitored infrastructure. Veeam ONE will add the **Event-based** rule type to the alarm configuration, and will trigger this alarm for all events with the same name. For details on the Event-based rules, see Adding Event-Based Rules.

To create an alarm from a task or event:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. Select the necessary view (*Veeam Backup & Replication*, *Veeam Backup for Microsoft 365*, *Virtual Infrastructure*, *VMware Cloud Director*, *Business View*).
3. In the information pane, navigate to the **Tasks & Events** tab.
4. Right-click a task or event for which you want to create an alarm, select **Create new alarm** from the shortcut menu and then choose an object type.

Creating Alarms from Performance Chart Counters

You can create an alarm from a performance counter. Veeam ONE will add to the alarm configuration a rule based on resource usage counter, and will trigger this alarm every time the counter reaches the specified values. For details on the rules based on resource usage counters, see Adding Rules Based on Resource Usage Counters.

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. Select the necessary view (*Veeam Backup & Replication*, *Veeam Backup for Microsoft 365*, *Virtual Infrastructure*, *VMware Cloud Director*, *Business View*).
3. In the object tree, select an object for which you want to create an alarm.

4. Open a tab with performance parameters for which you want to create an alarm (for example, *Network*, *Memory*, *CPU*, and so on).
5. At the bottom of the performance chart, right-click the necessary counter and select **Create new alarm** from the shortcut menu.

Creating Alarms from In-Guest Processes and Services

You can create an alarm from a process or service. For details on the rules based on specific condition or state, see Adding State-Based Rules.

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.
2. Select the necessary view (*Virtual Infrastructure*, *VMware Cloud Director*, *Business View*).
3. In the object tree, select an object for which you want to create an alarm.
4. Open the **Processes** or **Services** tab.
5. Select one or more processes or services in the list.
6. Click the **Create Alarm** button.

   Alternatively, you can right-click the necessary process or service.
7. Select the type of rule on which the alarm must be based.

Step 2. Specify General Alarm Settings

On the **General** tab of the **Alarm Settings** window, specify general alarm settings:

1. In the **Alarm name** field, specify the name of the new alarm.
2. If you want to enable the alarm immediately after you save its settings, make sure that the **Enable this alarm** check box is selected.

   If you unselect this check box, the alarm settings will be saved, but the alarm will be disabled and will not raise any notifications.

Step 3. Specify Alarm Rules

On the **Rules** tab of the **Alarm Settings** window, specify rules for triggering the alarm. You can add up to 8 rules of different type and link them to each other.

Adding State-Based Rules

Alarms with state or condition-based rules alert about the important condition or state changes.

To add a rule for a specific condition or state change:

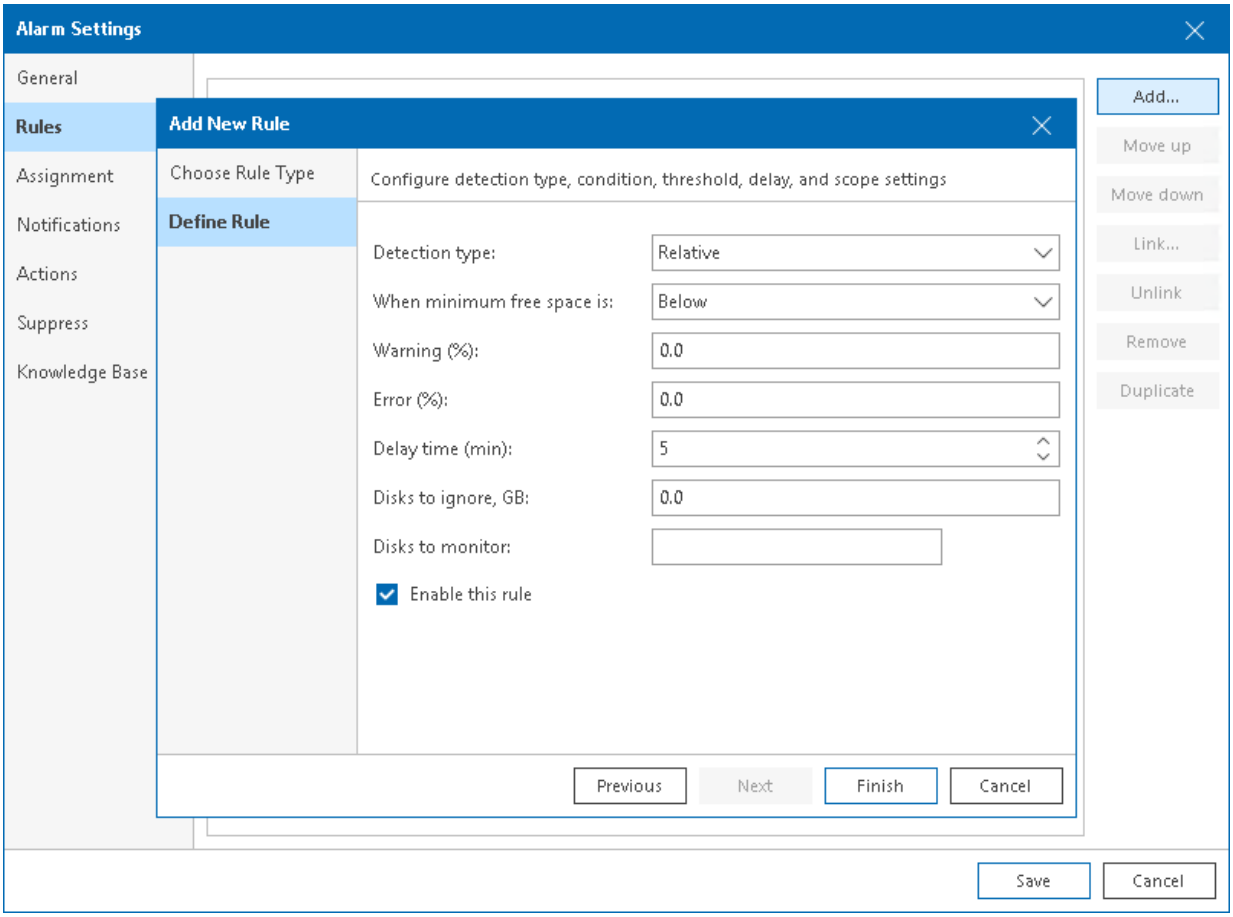
1. On the **Rules** tab, click **Add**.
2. At the **Choose Rule Type** step of the wizard, select the necessary trigger type.
3. Click **Next** and select the necessary rule condition.

   Available options depend on the alarm type. For the full list of alarm rules, see Alarm Rules Reference.
4. At the **Define Rule** step of the wizard, specify conditions (or other settings, as applicable) for the alarm rule.
5. Specify alarm severity.

   For details, see Alarm Severity.
6. If you want to put the rule in action for the alarm, make sure that the **Enable this rule** check box is selected.

   If you clear this check box, the rule settings will be saved, but the rule will be disregarded.

7. Click **Finish**.



8. Repeat steps **1–7** for every state-based rule you want to add to an alarm.

Adding Event-Based Rules

Alarms with event-based rules alert about specific events that occur in your backup or virtual infrastructure. These can be events issued by the hypervisor or Veeam Backup & Replication events.

To add an event-based rule:

1. On the **Rules** tab, click **Add**.
2. At the **Choose Rule Type** step of the wizard, select **Event-based rule**.
3. At the **Define Rule** step of the wizard, specify rule settings:
   a. In the **Event name** field, specify the name of the event that must trigger the alarm.

      For the list of Veeam Backup & Replication and Veeam Backup for Microsoft 365 events, see sections Veeam Backup & Replication Alarms and Veeam Backup for Microsoft 365 Alarms. For the list of virtual infrastructure events, see VMware vSphere Documentation or Microsoft documentation.

      Note that for VMware vSphere events, you must provide their names without prefixes. For example, for the *vim.event.VmReconfiguredEvent* event, you must specify only the *VmReconfiguredEvent* part.

b. In the **Event text** field, specify one or more keywords that an event description must contain. This can be a name of a user who initiated an action, a name of a changed object, or a specific action.

   You can use the '*' (asterisk) and '?' (question) wildcards in the **Event name** and **Event text** fields. The '*' (asterisk) character stands for zero or more characters. The '?' (question mark) stands for a single character.

   For example, if you want to receive notifications when users reconfigure VMs on the *host.domain.local* host, in the **Event name** field, specify *VmReconfiguredEvent*, and in the **Event text** field, specify '*reconfigured * on host.domain.local*'. Here the '*' (asterisk) replaces a name of a reconfigured VM. As a result, the alarm will be triggered each time any user reconfigures any VM on the host.

c. Specify the alarm severity level for the rule.

   For details, see Alarm Severity.

d. In the **Ignore after** field, enter the number of times the alarm for the same event or condition must be triggered. All further repetitive alarms are suppressed.

   For example, an alarm is configured to fire when a host loses its network connection, and the **Ignore after** value is set to 1. If a host loses its network connection, an event informing about connection loss will be raised by the hypervisor, and Veeam ONE will trigger an alarm. All further events informing about problems with host network connectivity will be ignored until you resolve the alarm that has already been triggered.

   If you want the alarm to trigger every time an event or condition occurs, set the **Ignore after** value to 0.

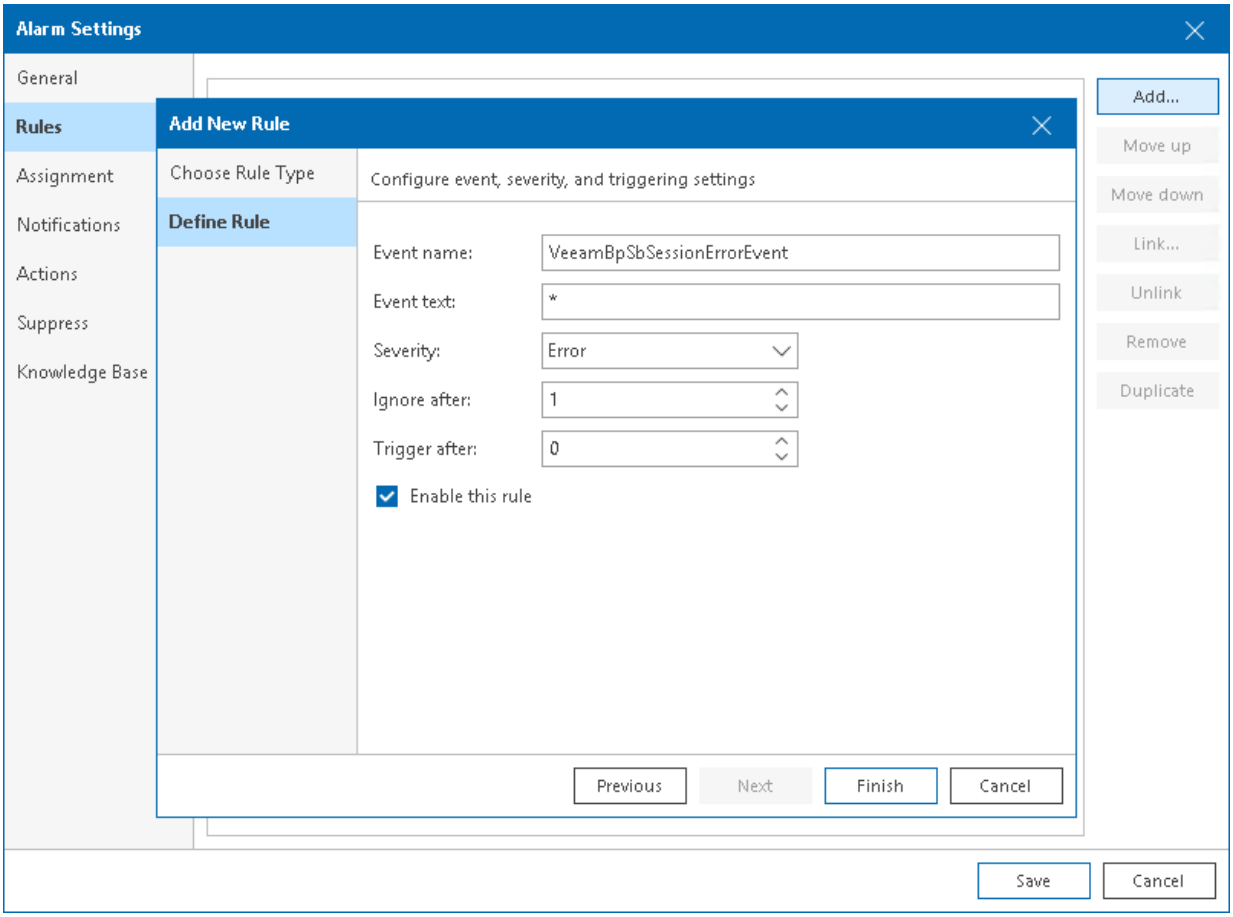
e. In the **Trigger after** field, enter the number of times an event must repeat before Veeam ONE must trigger an alarm.

   By default, this value is set to 0, which means that Veeam ONE must trigger an alarm after the first event occurrence.

f. If you want to put the rule in action for the alarm, make sure that the **Enable this rule** check box is selected.

   If you clear this check box, the rule settings will be saved, but the rule will be disregarded.

4. Click **Finish**.



5. Repeat steps **1-4** for every event-based rule you want to add.

Adding Rules Based on Existing Alarms

You can add to an alarm rules that are based on existing alarms. These rules alert if the specified alarms trigger or change their status.

To add a rule based on existing alarm:

1. On the **Rules** tab, click **Add**.
2. At the **Choose Rule Type** step of the wizard, select **Existing alarm**.
3. At the **Define Rule** step of the wizard, specify rule settings:
   a. In the **Alarm name** field, specify the name of the existing alarm that must trigger an alarm.

      This can be a predefined or custom alarm. For a list of predefined alarms, see the Predefined Alarms section.

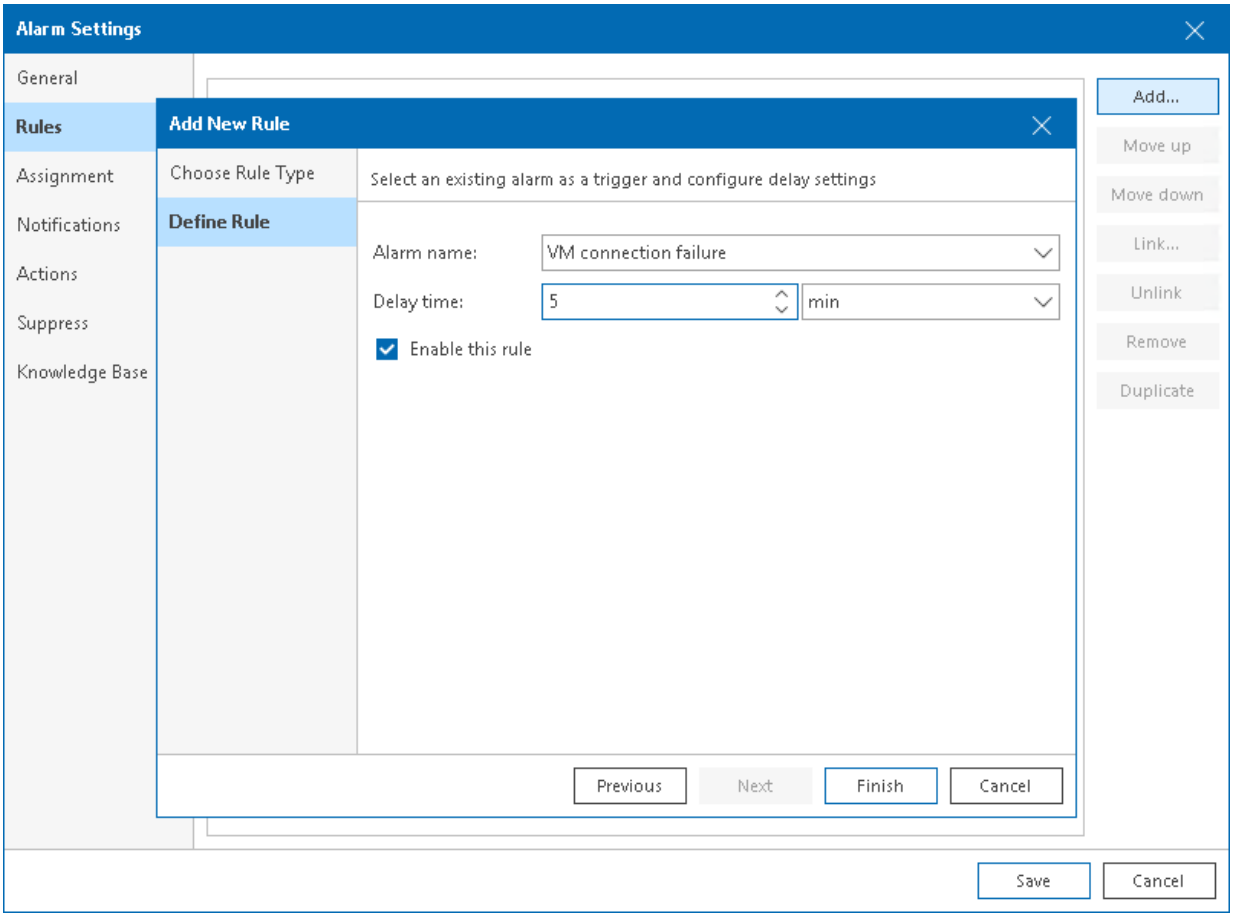
   b. In the **Delay time** field, specify the period that must pass between triggering the source and the target alarm.

      You can specify the delay time in minutes, hours, or days.

   c. If you want to put the rule in action for the alarm, make sure that the **Enable this rule** check box is selected.

      If you unselect this check box, the rule settings will be saved, but the rule will be disregarded.

4. Click **Finish**.



5. Repeat steps **1-4** for every alarm-based rule you want to add.

Adding Rules Based on Resource Usage Counters

Alarms with rules resource usage counters alert about the important changes in the performance of objects from the monitored infrastructure.

To add a rule based on resource usage counters:

1. On the **Rules** tab, click **Add**.
2. At the **Choose Rule Type** step of the wizard, select **Resource usage**.
3. At the **Define Rule** step of the wizard, specify conditions (or other settings, as applicable) for the alarm rule.

   If you want to put the rule in action for the alarm, make sure that the **Enable this rule** check box is selected. If you unselect this check box, the rule settings will be saved, but the rule will be disregarded.
4. [Optional] Exclude specific objects from the alarm scope.

   By default, counter-based rules apply to all storage objects in the alarm scope. For example, if you create an alarm rule for a host and select a datastore usage counter, this rule will apply to all datastores connected to the host.

   For some counter-based rules, you can exclude specific storage objects from the alarm scope. Excluded objects will not be monitored by the alarm. To exclude one or more storage objects, specify their names in the **Exclude instances** field. Separate object names with a semicolon (;).

NOTE:

- When you specify objects to exclude, use object display names. To learn the exact display name of an object, navigate to a performance chart for the necessary object in Veeam ONE Client, and choose a chart view with the necessary counter. You can check the object display name either in the chart legend or in the **Select Devices and Counters** window > **Devices** list. For details, see Selecting Chart Views and Performance Counters.
- Names of drives must be specified with the backward slash, for example, `C:\; Z:\`.

5. Click **Finish**.
6. Repeat steps **1–5** for every alarm-based rule you want to add.

Linking Rules

If you add multiple rules to one alarm, Veeam ONE will trigger the alarm when conditions for at least one rule are met. You can change the default way of evaluating alarm rules and link rules using Boolean AND or OR operators. For example, if an alarm must be triggered when conditions for two rules are met simultaneously, you can link these rules with Boolean AND.

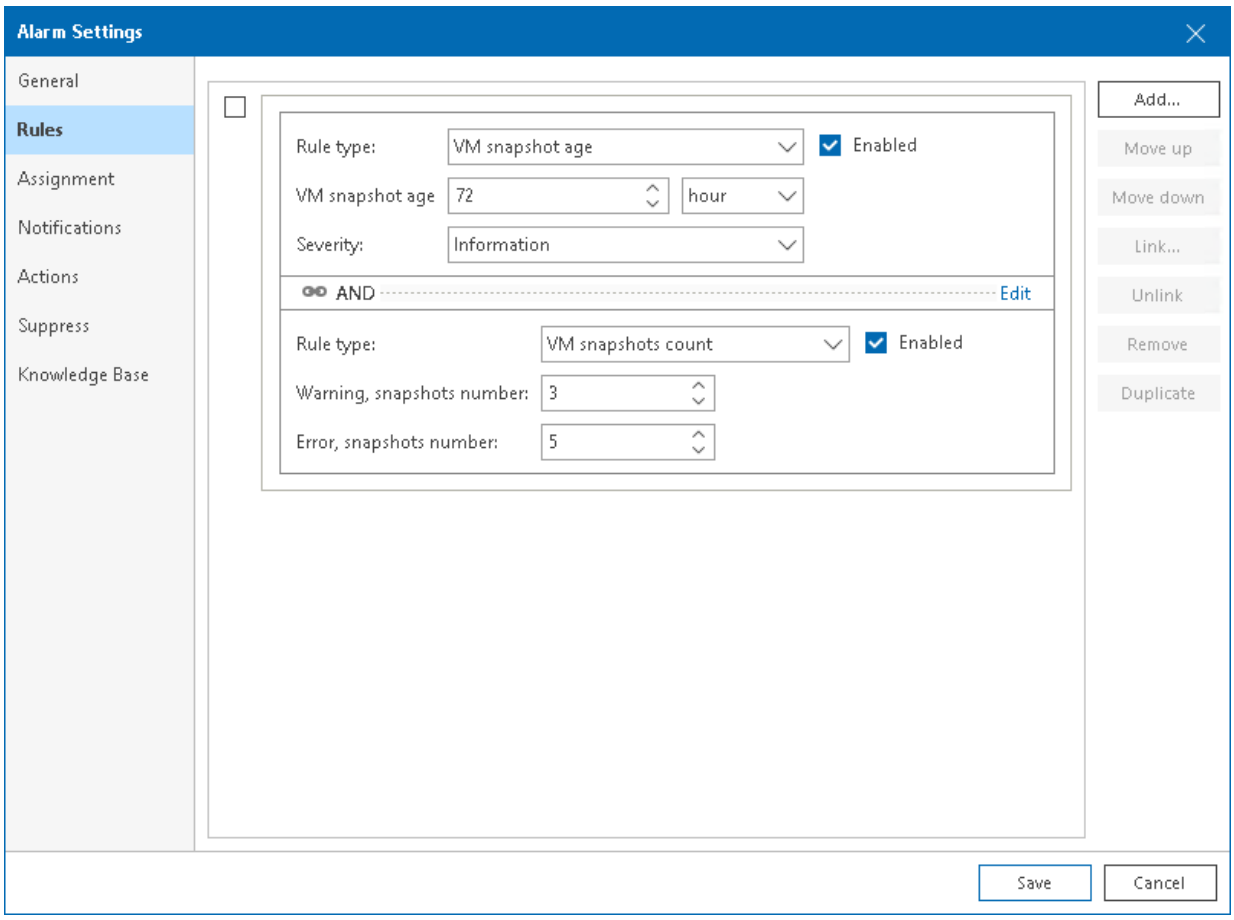
To link alarm rules:

1. Choose the rules you want to link and place them one after another. You cannot link rules that do not follow one another in the list. For example, you cannot link the first and the fifth rule.

   To move a rule one position up, select the check box next to the rule and click **Move up**. To move a rule one position down, select the check box next to the rule and click **Move down**.
2. Select check boxes next to rules you want to link, and click **Link** on the right.
3. In the **Rule condition** window, select a condition:
   - **AND** — if rules are linked with this operator, the alarm is triggered when conditions for all linked rules are met.
   - **OR** — if rules are linked with this operator, the alarm is triggered when a condition for any of the linked rules is met.

4. Click **Apply**.

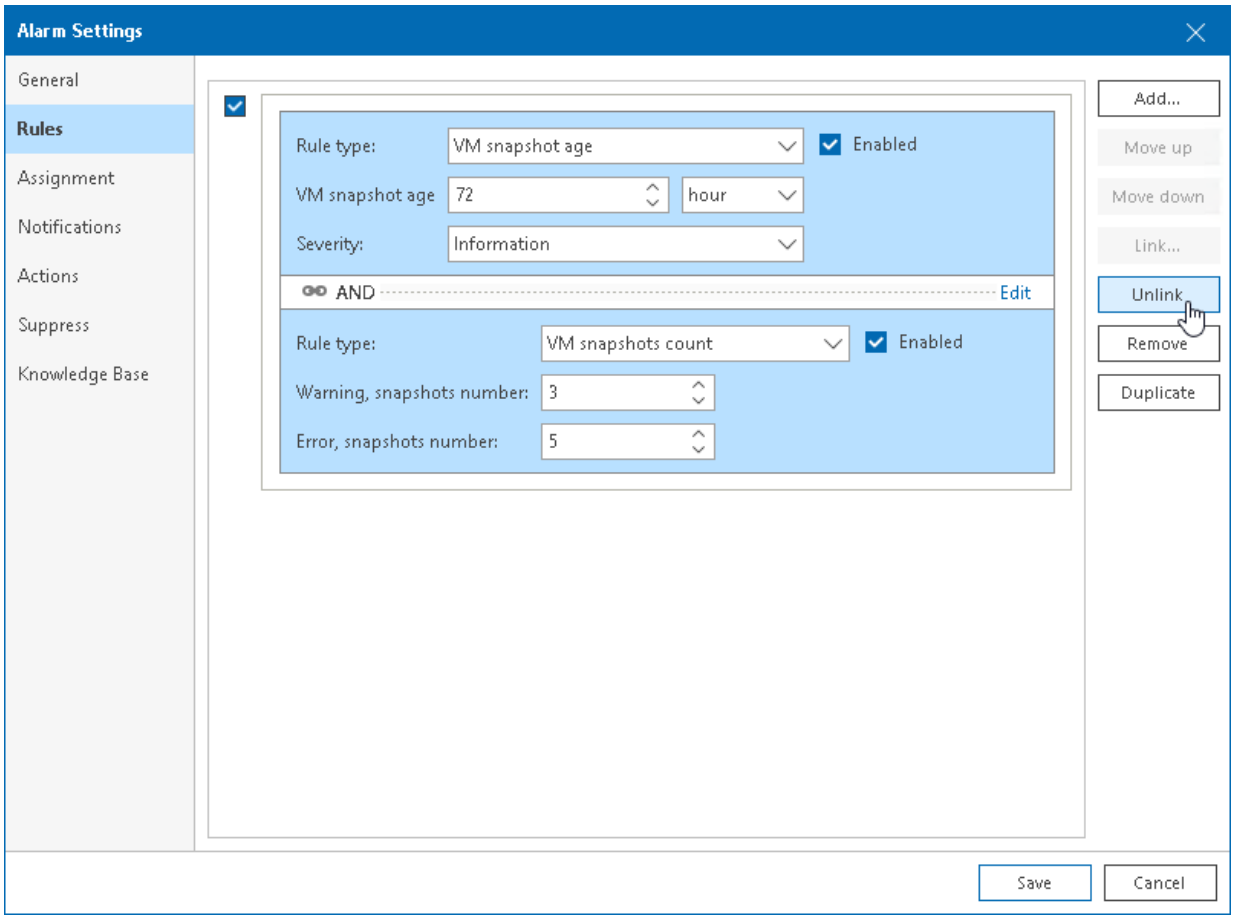
   After you link two or more rules, Veeam ONE will display a dotted line and a linking condition between the rules. Linking supports 3 levels of nesting.



To unlink rules:

1. Select the check box next to the linked rules.
2. On the right, click **Unlink**.

If you unlink rules, the alarm will be triggered each time when conditions for any alarm rule are met.

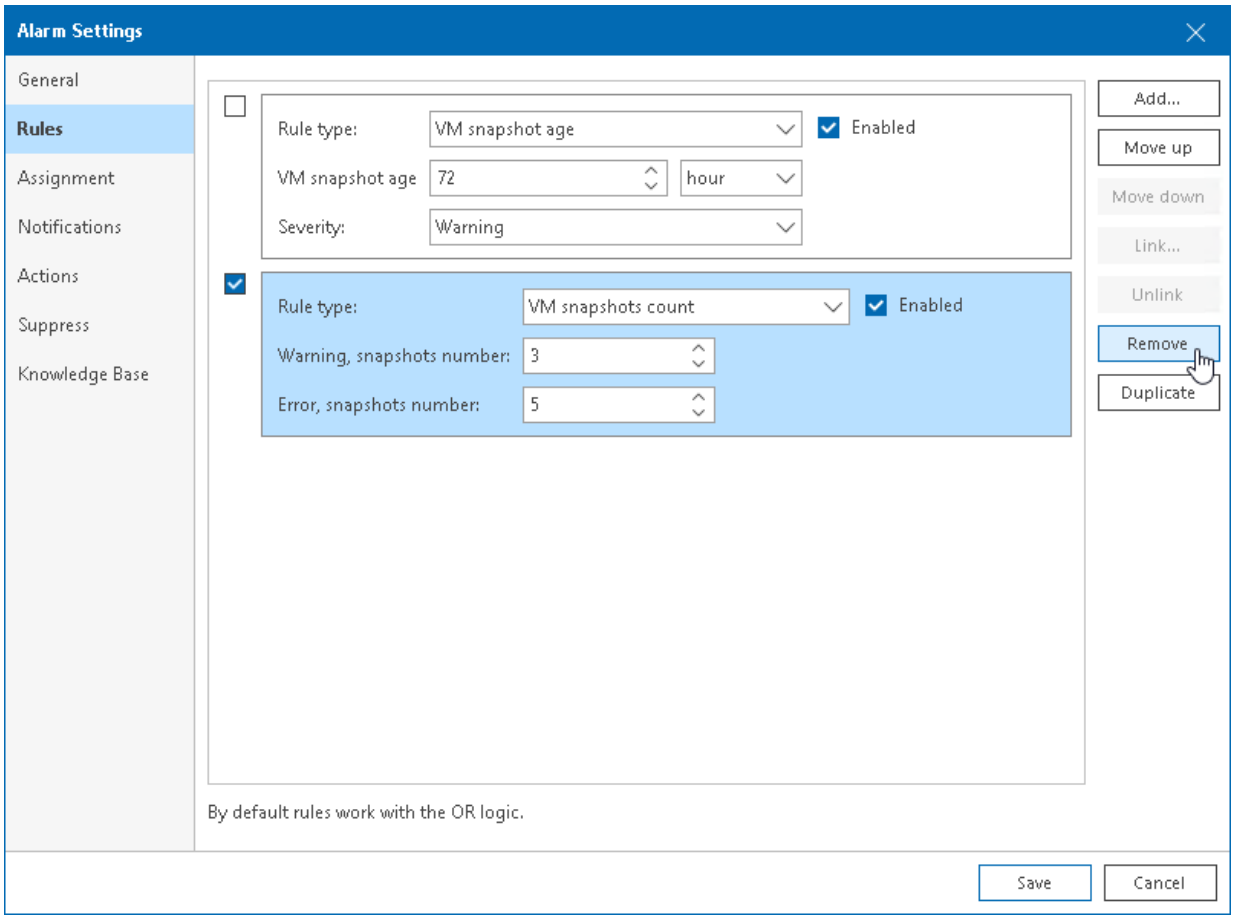


Removing Rules

To remove a rule from an alarm:

1. Select the check box next to a rule you want to remove.

2. On the right, click **Remove**.

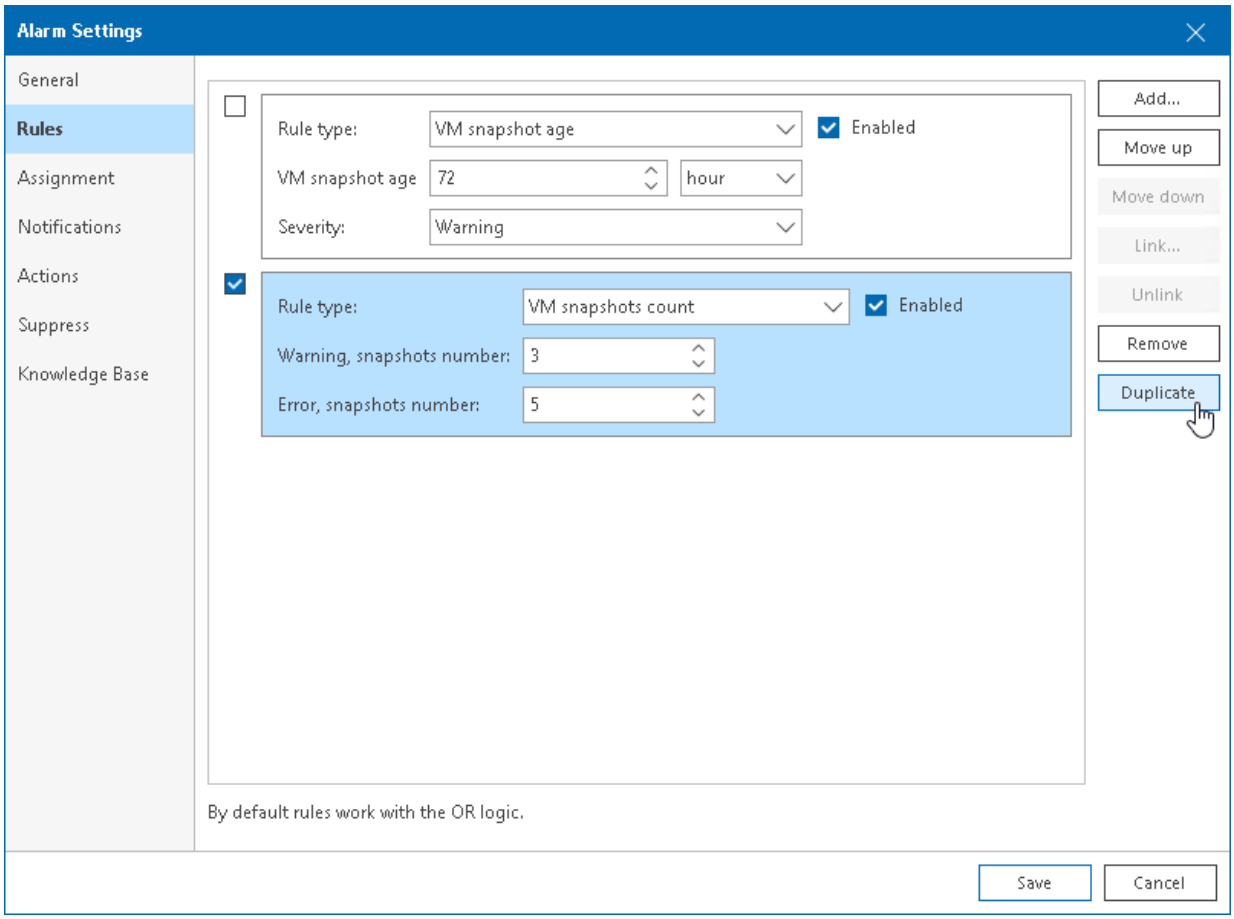


Duplicating Rules

To duplicate a rule:

1. Select the check box next to a rule you want to duplicate.

2. On the right, click **Duplicate**.



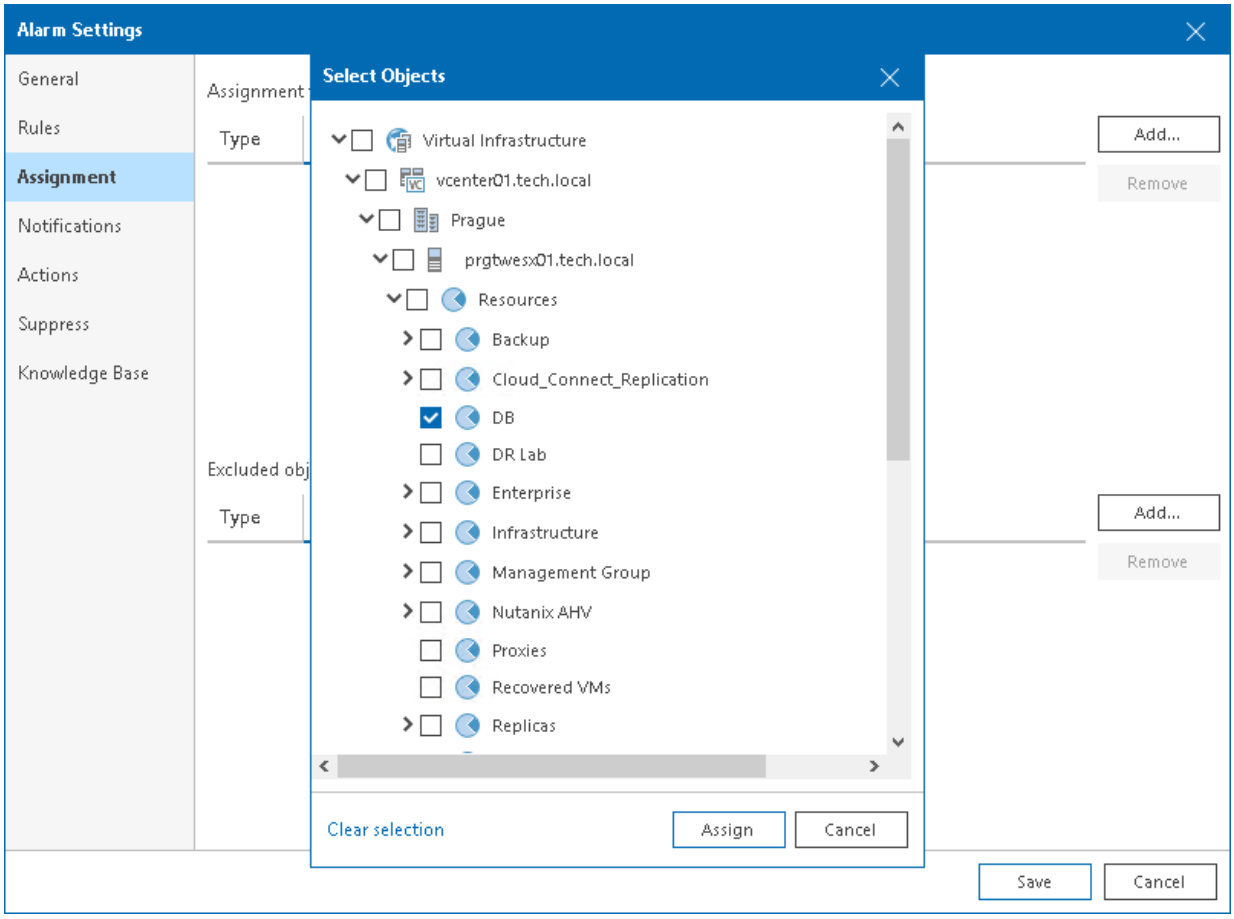
Step 4. Specify Alarm Assignment Scope

On the **Assignment tab** of the **Alarm settings** window, specify one or more infrastructure objects to which the alarm must be assigned.

Adding Objects to Alarm Assignment Scope

To add one or more objects to alarm assignment scope:

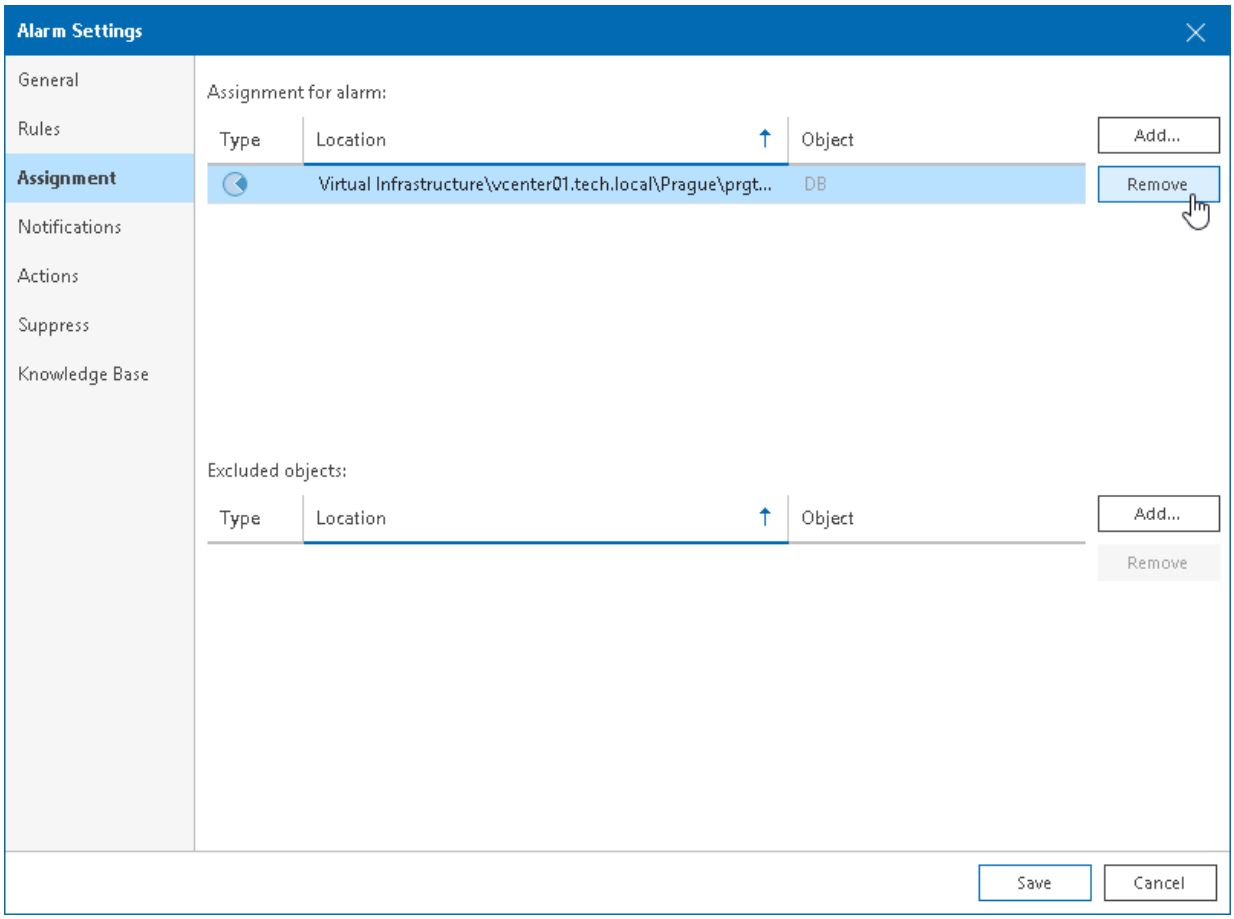
1. On the **Assignment** tab, in the **Assignment for alarm** section, click **Add** and select the necessary node (*Veeam Backup & Replication*, *Veeam Backup for Microsoft 365*, *Virtual Infrastructure*, *VMware Cloud Director*, *Business View*).
2. In the **Assign Alarm** window, select check boxes next to objects to which you want to assign the alarm.
3. Click **Assign**.



To remove an object from the alarm assignment:

1. On the **Assignment** tab, in the **Assignment for alarm** section, select an object you want to remove from the assignment.

2. On the right, click **Remove**.

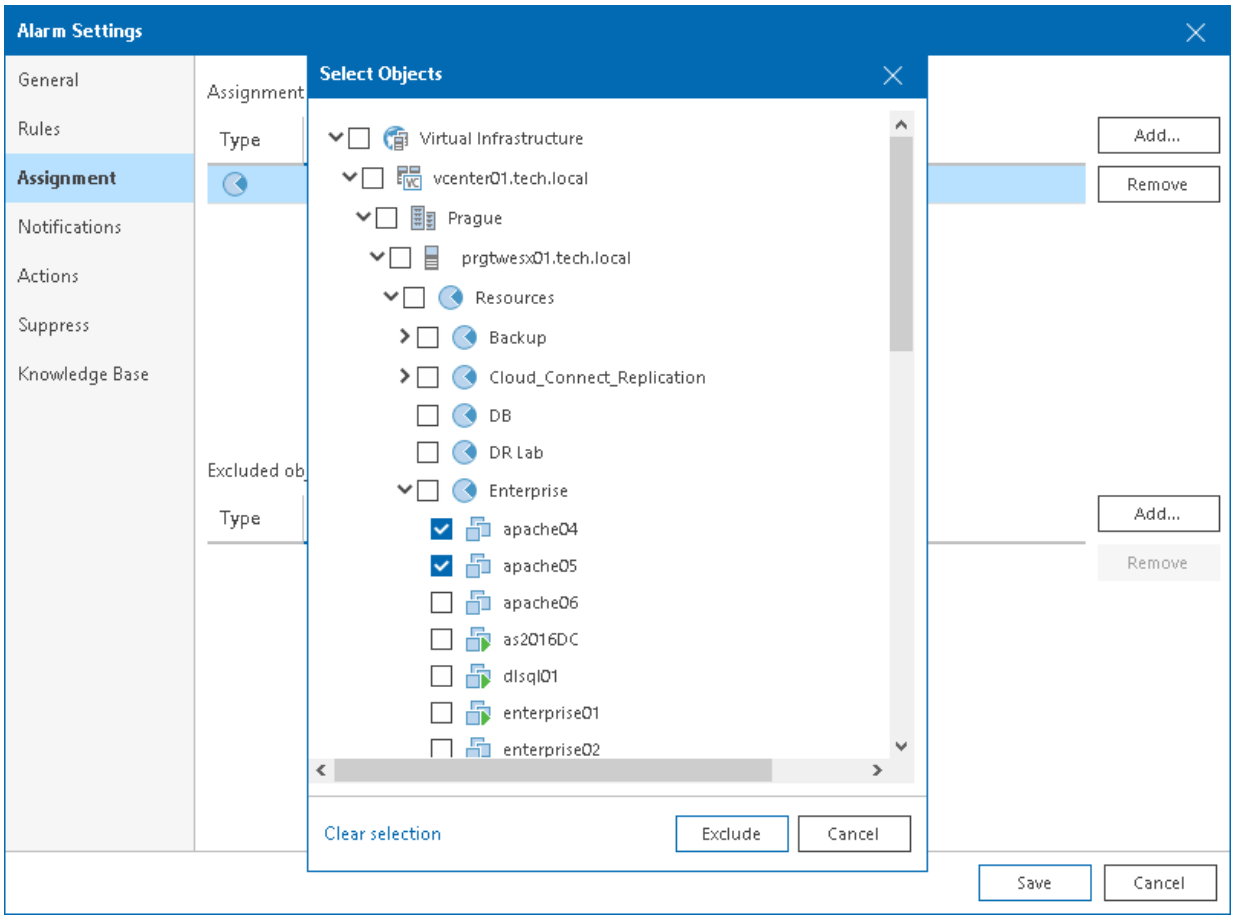


Excluding Objects from Alarm Assignment Scope

You can exclude objects from alarm assignment scope:

1. On the **Assignment** tab, in the **Excluded objects** section, click **Add** and select the necessary node (*Veeam Backup & Replication*, *Veeam Backup for Microsoft 365*, *Virtual Infrastructure*, *VMware Cloud Director*, *Business View*).
2. In the **Exclude Alarm** window, select check boxes next to objects you want to exclude from alarm assignment.

3. Click **Exclude**.



Step 5. Specify Alarm Notification Options

On the **Notifications** tab of the **Alarm settings** window, you can specify what actions must be performed after the alarm is triggered, or after the alarm status changes. You can choose to notify virtual infrastructure administrators by email, send SNMP traps or run a custom script.

> **NOTE:**
>
> To receive email and trap notifications, you must first configure email and trap notification settings in the Veeam ONE Client Configuration Wizard or in Veeam ONE Client server settings. To learn how to configure notification settings for alarms, see Configuring Alarm Notifications.

To define alarm response actions:

1. From the **Action** list, select the action you want to perform:
   - **Send email to a default group** — select this option if you want to send an email notification to all recipients included in the *default email notification group* when the alarm is triggered or when the alarm status changes. This is the default action that applies to all new and predefined alarms.

     For details, see Configuring Email Notifications.
   - **Send email to Business View group owner** — select this option if you want to send an email notification an owner of a Business View group to which the object is included.

     To receive notifications, you must specify an email address of a group owner in the Business View group settings. For details, see Configuring Multiple-Condition Categorization.
   - **Send email notification** — select this option if you want to send an email notification to specific recipients when the alarm is triggered or when the alarm status changes. In the **Value** field, enter recipients email addresses. If you want to specify several recipients, separate email addresses with a semicolon (;), comma (,) or space ( ).

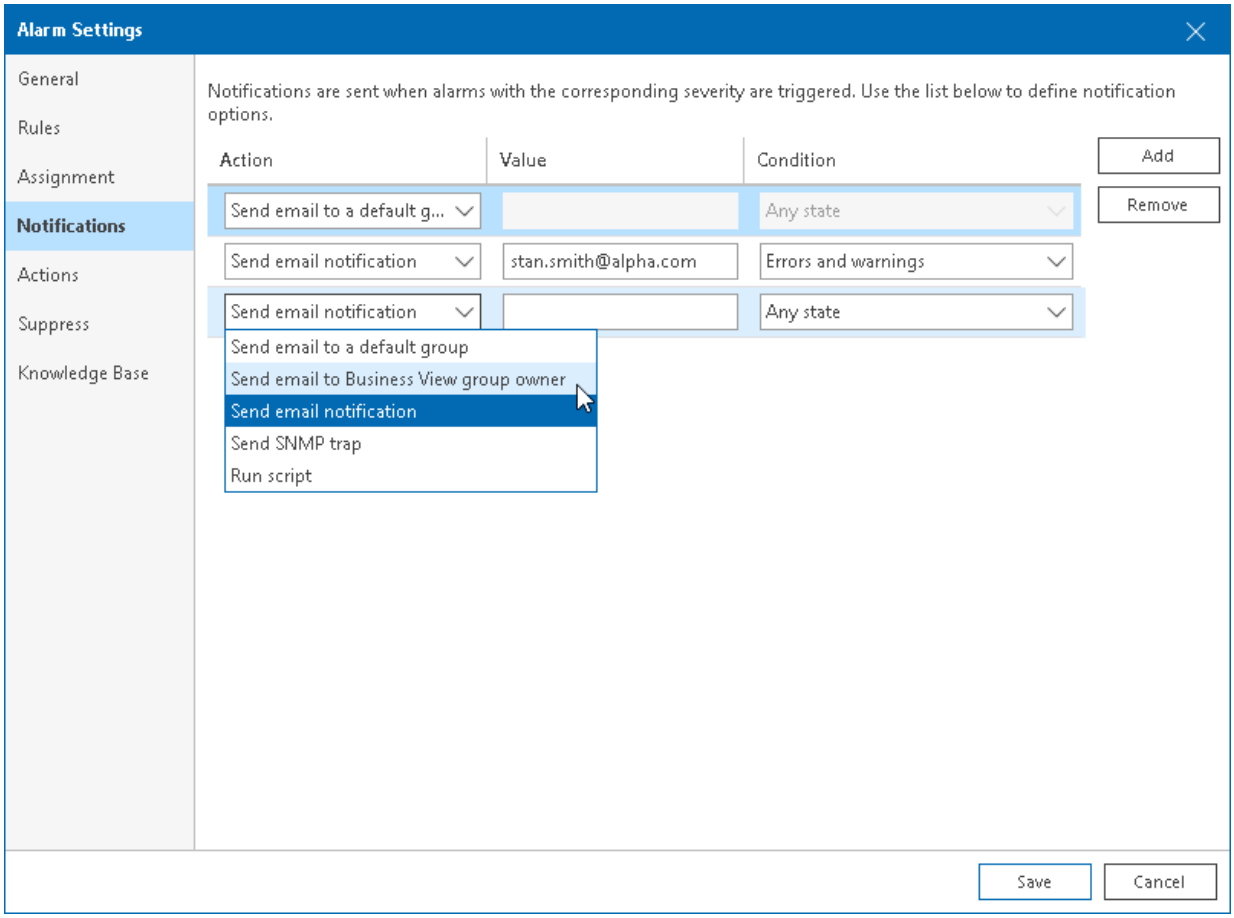
     For more information, see Configuring Email Notifications.
   - **Send SNMP trap** — select this option if you want to send a Simple Network Management Protocol (SNMP) trap when the alarm is triggered or when the alarm status changes.

     For details, see Configuring SNMP Traps.
   - **Run script** — select this option if you want to run a custom script when the alarm is triggered or when the alarm status changes. By running a script, you can automate routine tasks that you normally perform when specific alarms fire. For example, if a critical system is affected, you may need to immediately open a ticket with the in-house support or perform corrective actions that will eliminate the problem.

     In the **Value** field, specify the path to the executable file. The executable file must be located on the machine running the Veeam ONE Server component. You can use the following parameters in the command line for running the script: *%1* — alarm name; *%2* — affected node name; *%3* — alarm summary; *%4* — date and time of alarm trigger; *%5* — alarm status; *%6* — previous alarm status; *%7* — ID assigned to a combination of an affected node and an alarm; *%8* — type of a child alarm object.
2. In the **Condition** field, specify when the action must be performed:
   - **Errors and warnings** — select this option if the action must be performed every time when the alarm status changes to *Error* or *Warning*.
   - **Errors only** — select this option if the action must be performed every time when the alarm status changes to *Error*.

- **Resolved** — select this option if the action must be performed every time when the alarm status changes to *Resolved*.
- **Any state** — select this option if the action must be performed every time when the alarm status changes to *Error*, *Warning* or *Resolved*.

You can specify multiple response actions for the same alarm. To add a new action, click the **Add** button and repeat steps **1-2** for every new action.



Step 6. Specify Alarm Remediation Actions

On the **Actions** tab of the **Alarm settings** window, you can specify what actions must be performed after the alarm is triggered, or after the alarm status changes:

1. Click **Add**.
2. From the **Action** list, select **Run Script**.

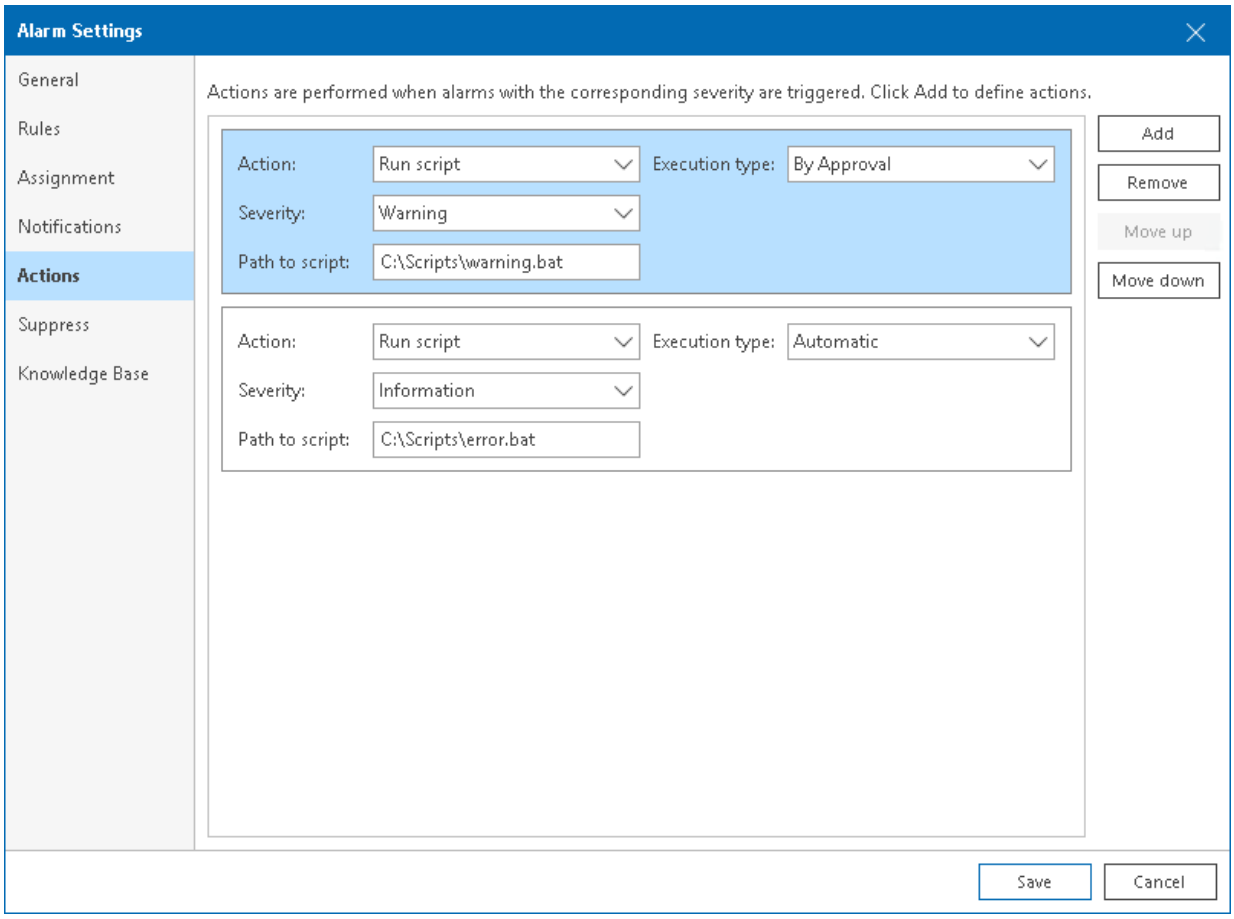
   In the **Path to script** field, specify the path to the script that must be executed after the alarm is triggered, or after the alarm status changes. The executable file must be placed at the location accessible for the Veeam ONE service account. The script is executed on the machine running Veeam ONE Server component. You can use the following parameters in the command line for running the script: *%1* — alarm name; *%2* — affected node name; *%3* — date and time of alarm trigger; *%4* — alarm status; *%5* — affected object name; *%6* — ID assigned to a combination of an affected node and an alarm.

> **NOTE:**
>
> Predefined remediation actions are available for a number of out-of-the-box alarms only. For the list of alarms with predefined remediation actions, see Remediation Actions.

3. From the **Severity** list, select alarm severity level at which an action must be taken.
4. From the **Resolution Type** list, select resolution type — manual or automatic.

   For details, see Alarm Remediation Actions.
5. Repeat steps **1–4** for every action you want to add to an alarm.

To change the position of an action relative to other actions, select the action and click **Move up** or **Move down**.



Step 7. Configure Alarm Suppression Settings

To automatically suppress alarms that occur under specific conditions or during a specific time interval, you can configure alarm suppression settings. For example, alarms informing about high resource utilization may need to be suppressed if these alarms occur during a scheduled resource-consuming operation (such as backup performed with Veeam Backup & Replication or other operations).

For suppressed alarms, Veeam ONE does not show any notifications and does not perform any response actions. If the object stays affected by the end of the suppression period, Veeam ONE will trigger the alarm and perform the alarm response actions.

On the **Suppress tab** of the **Alarm settings** window, specify alarm suppression settings.

Suppressing Alarms During Events

To suppress the alarm under specific conditions or when a specific event occurs, choose one of the following options:

- **Veeam Backup activity** — suppresses the alarm when Veeam Backup & Replication jobs are running. Veeam ONE detects which VMs are being processed and does not trigger alarms for these VMs and associated hosts and datastores.

  For example, if you select **Veeam Backup activity** check box for the *VM CPU Usage* alarm, this alarm will be suppressed for all VMs that are being backed up or replicated — until the jobs finish processing these VMs.

  If you select the **Veeam Backup activity** check box for the *Host CPU Usage* alarm, this alarm will be suppressed for the entire host where at least one VM is being backed up or replicated — until the jobs are finished.

- **Snapshot creation** — suppresses the alarm during snapshot creation for the object itself or its parent objects.

  For example, if you create an alarm for a VM, the alarm will be suppressed for a VM while a hypervisor creates a snapshot. If you create an alarm for a host, the alarm will be suppressed for the host while a snapshot is being created for any VM on this host.

- **Snapshot deletion** — suppresses the alarm during snapshot deletion for the object itself or its parent objects.

  For example, if you create an alarm for a VM, the alarm will be suppressed for a VM while a hypervisor deletes a snapshot. If you create an alarm for a host, the alarm will be suppressed for the host while a snapshot is being deleted for any VM on this host.

NOTE:

- The **Veeam Backup activity** suppression option apply to VMware vSphere and Microsoft Hyper-V alarms only. To enable the **Veeam Backup activity** option, make sure that you connected a Veeam Backup & Replication server to Veeam ONE. Otherwise, alarms will not be suppressed during Veeam Backup & Replication activity.
- **Snapshot creation** and **Snapshot deletion** suppression options apply to VMware vSphere alarms only.

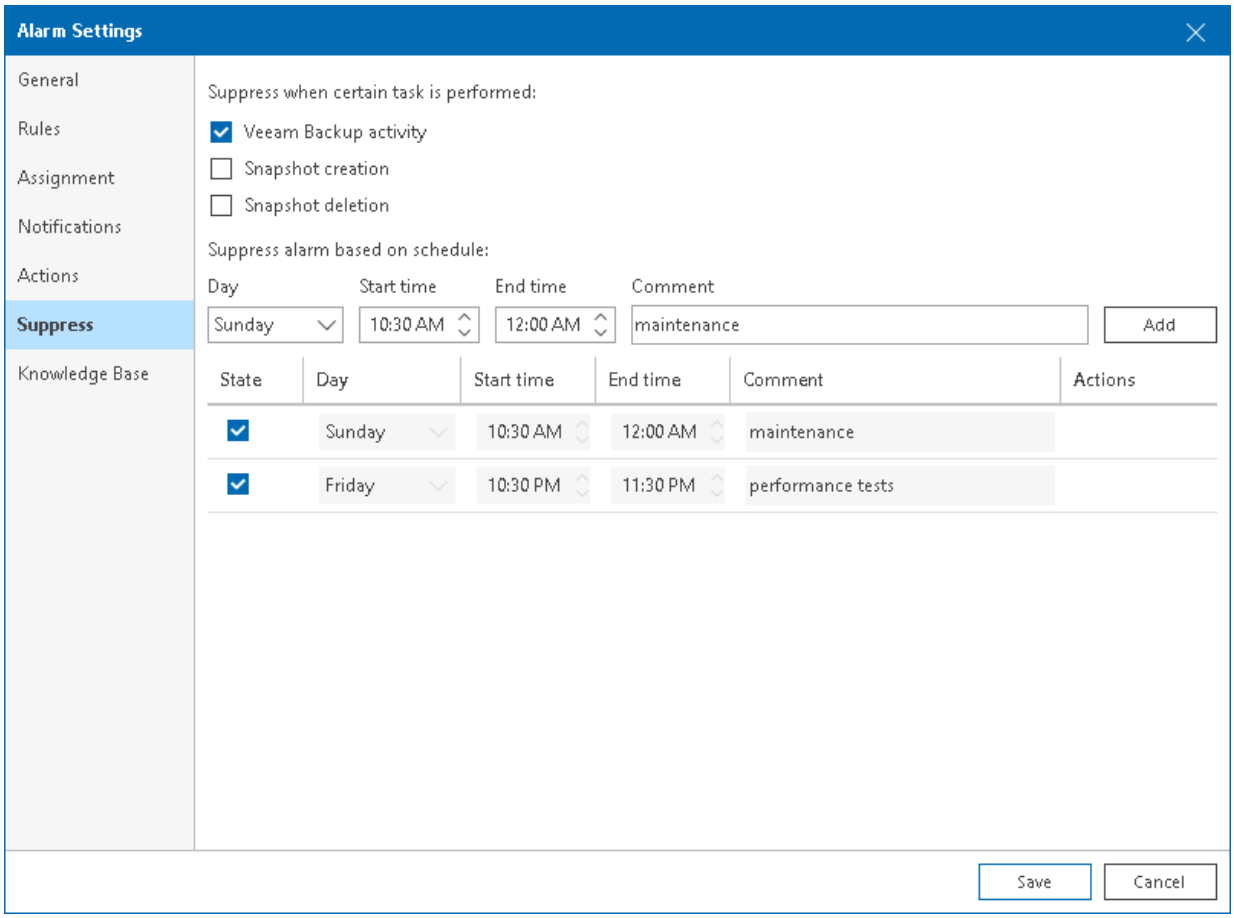
Scheduled Alarm Suppression

To suppress the alarm according to a specific schedule during the week:

1. Select the **Suppress alarm based on schedule** option.

2. Specify time intervals on specific weekdays during which the alarm must be suppressed.

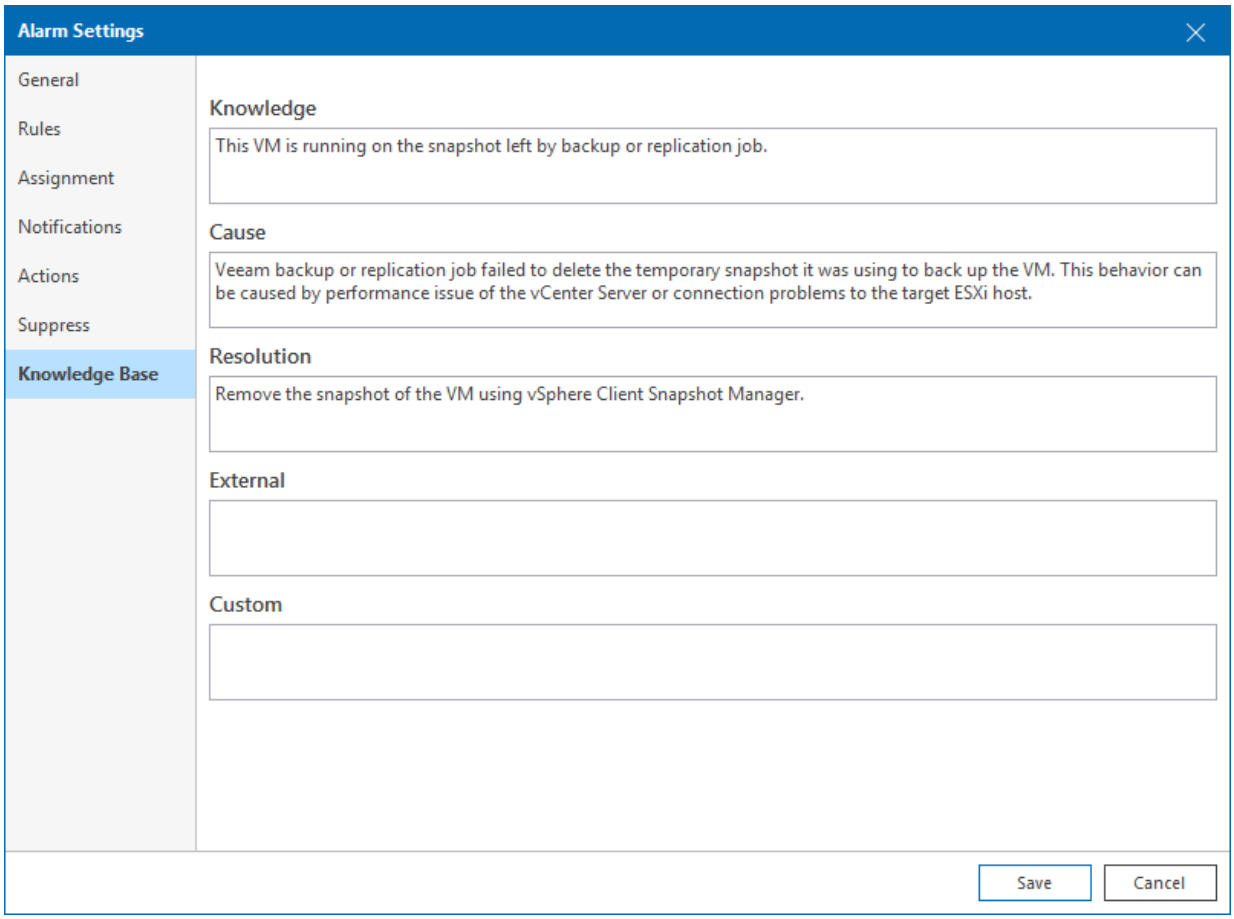
You can add more than one record for one weekday. Note that the time intervals specified for the same day must not intersect.



Step 8. Specify Alarm Details

On the **Knowledge base** tab of the **Alarm settings** window, specify alarm details. Alarm details are displayed when you select the alarm in the **Alarm Management** view or on the **Alarms** monitoring dashboard in Veeam ONE Client, and included in alarm email notifications.

1. In the **Knowledge**, **Cause** and **Resolution** fields, specify alarm details, what could cause the alarm, and steps to resolve the alarm.
2. In the **External** field, provide links to external resources containing reference information, such as VMware vSphere Documentation or Microsoft documentation.
3. In the **Custom** field, specify additional information, such as comments or additional instructions.



Step 9. Save Alarm Settings

Review the specified alarm settings and click **Save** to save the alarm.

Modifying Alarms

Veeam ONE allows you to modify settings of predefined or custom alarms.

To modify alarm settings:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click **Alarm Management**.
3. Select an alarm from the list and do either of the following:
   - Double click the alarm.
   - Right-click the alarm and choose **Edit** from the shortcut menu.
   - In the **Actions** pane, click **Edit**.
4. Change the necessary alarm settings.

   For details on alarm settings, see Creating Alarms.

Other Ways to Modify Alarms

You can also modify alarms on the **Alarms** tab of the Veeam Backup & Replication view, Veeam Backup for Microsoft 365 view, Virtual Infrastructure view, VMware Cloud Director view, Business View view.

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click the necessary view (*Veeam Backup & Replication*, *Veeam Backup for Microsoft 365*, *Virtual Infrastructure*, *VMware Cloud Director*, *Business View*).
3. In the inventory pane, select the necessary infrastructure object.
4. In the information pane, open the **Alarms** tab.
5. To open the **Alarm settings** window, do either of the following:
   - Right-click the alarm and select **Edit alarm** from the shortcut menu.
   - Select the alarm in the list and click **Edit alarm** in the **Actions** pane on the right.
6. Change the necessary alarm settings.

   For details, see Creating Alarms.

Modifying Multiple Alarms

Veeam ONE supports batch alarm editing. In the batch editing mode, you can change only the **Assignment**, **Notifications**, **Actions** and **Suppression** alarm settings.

To modify settings of several alarms in batch:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click **Alarm Management**.
3. Select the necessary alarms in the list using the [CTRL] or [SHIFT] key on the keyboard and do either of the following:
   - Right-click the selected alarms and click **Edit** in the shortcut menu.
   - Click **Edit** in the **Actions** pane on the right.
4. Change the **Actions** or **Suppression** settings.

   For details, see Creating Alarms.

Adding Alarm Rule from Task or Event

You can add to an alarm a new rule based on a task or event that occurred in the managed environment. For example, you can create a rule that monitors the *Create virtual machine* event and notifies you whenever a new VM is created.

To create a new rule from a task or event:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.
2. At the bottom of the inventory pane, click the necessary view (*Veeam Backup & Replication*, *Veeam Backup for Microsoft 365*, *Virtual Infrastructure*, *VMware Cloud Director*, *Business View*).
3. In the inventory pane on the left, select the necessary object.
4. In the information pane, open the **Tasks & Events** tab.
5. Right-click a task or event about which you want to be notified, select **Add this event to the existing alarm** from the shortcut menu, and click the necessary infrastructure object type.
6. In the **Select Alarms** window, select an alarm to which the rule must be added and click **Add**.
7. In the **Alarm Settings** window, change the rule settings, and click **Save**.

   For details on working with alarm rules, see Step 3. Specify Alarm Rules and Severity.
8. In the **Select Alarms** window, click **Close**.

Adding Alarm Rules from Performance Counters

You can add to an alarm a new rule based on a performance counter.

> **NOTE:**
>
> You can use this option with objects for which Veeam ONE collects performance data. For objects that do not have any performance data, such as datacenters and clusters, this option is not available.

To create a new rule from a performance counter:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.
2. At the bottom of the inventory pane, click the necessary view (*Veeam Backup & Replication*, *Veeam Backup for Microsoft 365*, *Virtual Infrastructure*, *VMware Cloud Director*, *Business View*).

3. In the inventory pane on the left, select the necessary object.
4. Open a tab with performance parameters for which you want to create an alarm (for example, *Network, Memory, CPU, and so on*).
5. At the bottom of the performance chart, right-click the necessary counter and select **Add this counter to the existing alarm** from the shortcut menu.
6. In the **Select Alarms** window, select an alarm to which the rule must be added and click **Add**.
7. In the **Alarm Settings** window, change the rule settings, and click **Save**.

   For details on alarm rules, see Step 3. Specify Alarm Rules and Severity.
8. In the **Select Alarms** window, click **Close**.

Changing Alarm Assignment Scope

By default, all predefined alarms are assigned to the root level of the managed infrastructure. Alarms for monitoring the virtual environment apply to the root level of the virtual infrastructure — connected vCenter Server, SCVMM, failover cluster, or host. VMware Cloud Director alarms apply to the root VMware Cloud Director level. Veeam Backup & Replication alarms apply to the root level of the backup infrastructure — connected Veeam Backup & Replication server or Veeam Backup Enterprise Manager. Veeam Backup for Microsoft 365 alarms apply to the connected Veeam Backup for Microsoft 365 server.

You can change the alarm assignment scope for predefined and custom alarms, exclude one or more objects from the alarm scope, or even exclude an object from the scope of multiple alarms at once.

Modifying Alarm Assignment Scope

To modify the assignment scope of one or more alarms:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click **Alarm Management**.
3. In the alarm management tree, select the necessary type of infrastructure objects.
4. Select one or more alarms in the list and do either of the following:
   - Right-click the alarm and select **Edit assignment** from the shortcut menu.
   - In the **Actions** pane on the right, click **Edit assignment**.
5. In the **Edit** assignment window, select the effective assignment rules and click **Remove**.
6. Click **Add** and choose one of the following options:
   - **Virtual Infrastructure tree** — choose this option if you want to assign the alarm to specific levels of the virtual infrastructure.

     You can select infrastructure objects that match the alarm type or choose containers from the virtual infrastructure hierarchy. For example, you can assign an alarm of the *Virtual Machine* type to a specific VM, resource pool, host, cluster, datacenter, or vCenter Server or SCVMM server.

   - **Business View** — choose this option if you want to assign the alarm to custom categorization groups that you have configured in Business View.

     For example, if VMs in your environment are divided into SLA groups, you can create a set of alarms that correspond to specific service level requirements and assign these alarms to the necessary SLA group.

   - **VMware Cloud Director View** — choose this option if you want to assign the alarm to a certain level of your VMware Cloud Director infrastructure.

     You can select infrastructure objects that match the alarm type or select containers from the VMware Cloud Director hierarchy. For example, you can assign an alarm of the VMware Cloud Director vApp type to a specific vApp, organization VDC, organization or vCloud Director cell.

- **Veeam Backup for Microsoft 365 View** — choose this option if you want to assign the alarm to a certain level of the Veeam Backup for Microsoft 365 infrastructure.

  You can select Veeam Backup for Microsoft 365 infrastructure objects that match the alarm type or select containers from the infrastructure hierarchy. For example, you can assign an alarm of the *Repository* type to a specific repository or Veeam Backup for Microsoft 365 server.

- **Veeam Backup & Replication View** — choose this option if you want to assign the alarm to a certain level of the Veeam Backup & Replication infrastructure.

  You can select backup infrastructure objects that match the alarm type or select containers from the backup infrastructure hierarchy. For example, you can assign an alarm of the *Repository* type to a specific repository, Veeam Backup & Replication servers or Veeam Backup Enterprise Manager.

You can combine various types of alarm assignment options for the same alarm. The type of options you can combine depends on the alarm type. For example, if an alarm has the *Virtual machine* type, you can include in the assignment scope virtual infrastructure, VMware Cloud Director and Business View objects.

7. Repeat steps **3–6** for all virtual and backup infrastructure objects or categorization groups to which the alarms must be assigned.

NOTE:

Mind the following restrictions for alarm assignment:

- Alarm can be assigned to infrastructure objects that correspond to the alarm type. For example, alarm of the VM type can be assigned to VMs or to a container that includes VMs.
- The same applies to Business View groups: the alarm type must match the Business View category type. You cannot assign an alarm of the Host type to a Business View group that is used to categorize VMs.

Excluding Single Objects from Alarm Assignment Scope

You can exclude a single infrastructure object from alarm assignment:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click the necessary view (*Veeam Backup & Replication*, *Veeam Backup for Microsoft 365*, *Virtual Infrastructure*, *VMware Cloud Director*, *Business View*).

3. In the information pane, open the **Alarms** tab.

4. Select the necessary alarm in the list and do either of the following:

   - Right-click the alarm and select **Edit Exclusions** from the shortcut menu.
   - In the **Actions** pane on the right, click **Edit Exclusions**.

   If you select a container object and choose an alarm that was triggered for its child object, Veeam ONE will provide two exclusion choices — exclude the child object only or exclude the whole container from the alarm assignment scope.

   For example, if in the inventory pane you select a cluster, the list of alarms will contain alarms on the cluster and alarms on the hosts in this cluster. If you select an alarm that was triggered for a host, you can exclude either the host (child object) or the whole cluster (container).

5. Click **OK** in the dialog box to confirm exclusion.

NOTE:

When you exclude an object from an alarm, all unresolved *Warning* or *Error* notifications that were triggered by this alarm for the object will change their status to *Resolved*.

Excluding Multiple Objects from Alarm Assignment Scope

You can exclude multiple infrastructure objects from the alarm assignment scope:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click **Alarm Management**.
3. Select the necessary alarm in the list and do either of the following:
   - Right-click the alarm and select **Edit exclusions** from the shortcut menu.
   - In the **Actions** pane on the right, click **Edit exclusions**.
4. In the **Edit exclusions** window, click **Add** and select objects that you want to exclude from the assignment scope:
   - **Virtual Infrastructure tree** — select this option if you want to assign the alarm to specific levels of the virtual infrastructure.

     You can select infrastructure objects that match the alarm type or choose containers from the virtual infrastructure hierarchy. For example, you can assign an alarm of the *Virtual Machine* type to a specific VM, resource pool, host, cluster, datacenter, or vCenter Server or SCVMM server.

   - **Business View** — select this option if you want to assign the alarm to custom categorization groups that you have configured in Business View.

     For example, if VMs in your environment are divided into SLA groups, you can create a set of alarms that correspond to specific service level requirements and assign these alarms to the necessary SLA group.

   - **VMware Cloud Director View** — select this option if you want to assign the alarm to a certain level of your vCloud Director infrastructure.

     You can select infrastructure objects that match the alarm type or select containers from the vCloud Director hierarchy. For example, you can assign an alarm of the vCloud Director vApp type to a specific vApp, organization VDC, organization or vCloud Director cell.

   - **Veeam Backup for Microsoft 365 View** — select this option if you want to assign the alarm to a certain level of the Veeam Backup for Microsoft 365 infrastructure.

     You can select Veeam Backup for Microsoft 365 infrastructure objects that match the alarm type or select containers from the infrastructure hierarchy. For example, you can assign an alarm of the *Repository* type to a specific repository or Veeam Backup for Microsoft 365 server.

   - **Veeam Backup & Replication View** — select this option if you want to assign the alarm to a certain level of the Veeam Backup & Replication infrastructure.

     You can select backup infrastructure objects that match the alarm type or select containers from the backup infrastructure hierarchy. For example, you can assign an alarm of the *Repository* type to a specific repository, Veeam Backup & Replication servers or Veeam Backup Enterprise Manager.

You can combine various types of alarm assignment options for the same alarm. The type of options you can combine depends on the alarm type. For example, if an alarm has the *Virtual machine* type, you can include in the assignment scope virtual infrastructure, vCloud Director and Business View objects.

5. Repeat steps **3–4** for all virtual and backup infrastructure objects or categorization groups you want to exclude.
6. In the **Edit exclusions** window, click **OK**.

Other Ways to Exclude Multiple Objects from Alarm Assignment

You can also exclude objects from the alarm assignment scope on the **Alarms** tab of the Virtual Infrastructure view, Business View, VMware Cloud Director view, Veeam Backup for Microsoft 365 view or Veeam Backup & Replication view.

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.
2. At the bottom of the inventory pane, click the necessary view (*Veeam Backup & Replication*, *Veeam Backup for Microsoft 365*, *Virtual Infrastructure*, *VMware Cloud Director*, *Business View*).
3. In the inventory pane, select the necessary infrastructure object.
4. In the information pane, open the **Alarms** tab.
5. Repeat steps **3–5** of the procedure above.

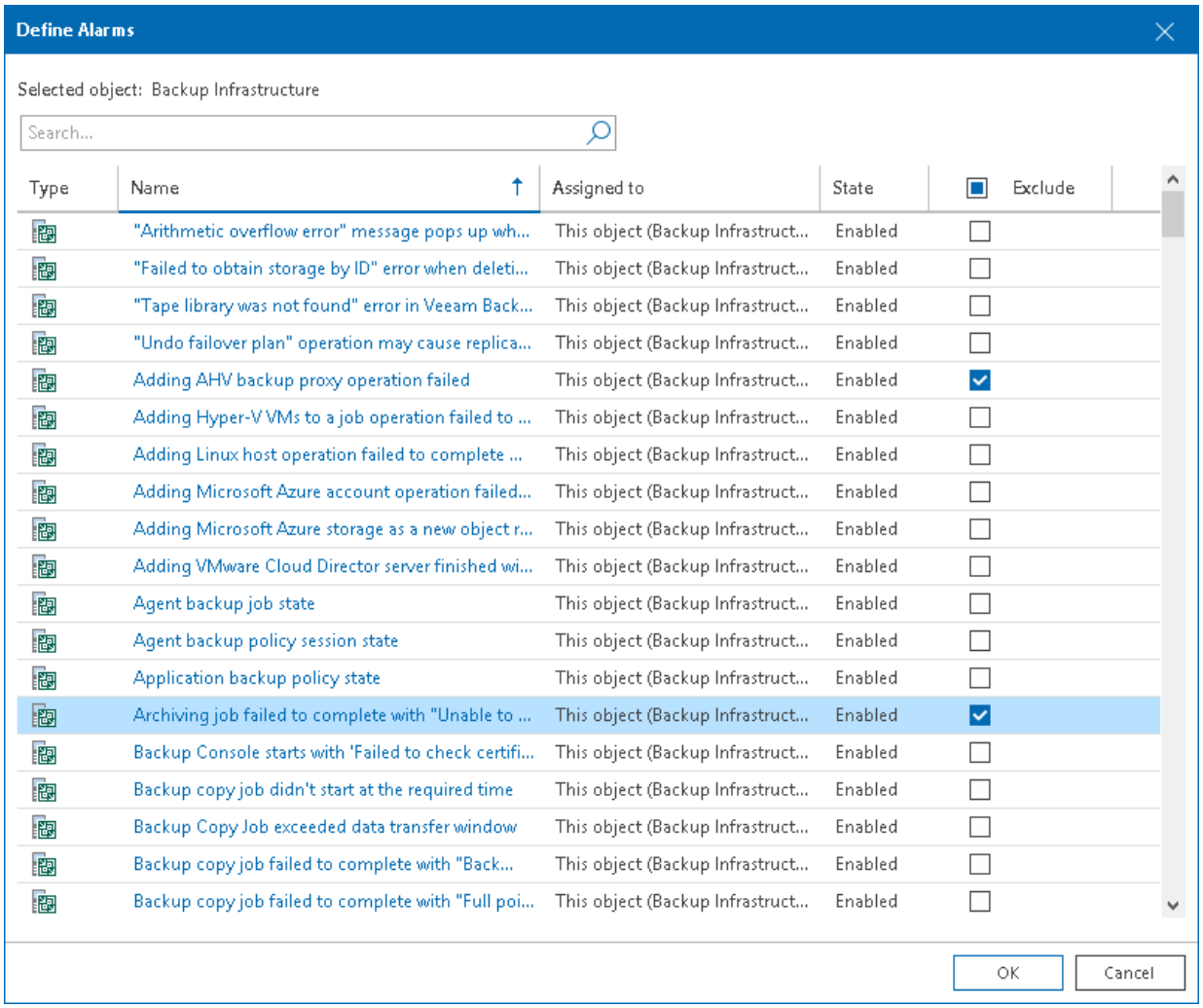
Excluding Objects from Multiple Alarms

You can exclude a single infrastructure object from the scope of multiple alarms:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.
2. At the bottom of the inventory pane, click the necessary view (*Veeam Backup & Replication*, *Veeam Backup for Microsoft 365*, *Virtual Infrastructure*, *VMware Cloud Director*, *Business View*).
3. In the inventory pane, select the necessary infrastructure object.
4. In the information pane, open the **Alarms** tab.
5. Select an alarm and do either of the following:
   - Right-click the alarm and select **Define alarms** in the shortcut menu.
   - In the **Actions** pane on the right, click **Define Alarms**.
6. In the **Define Alarms** window, select check boxes next to alarms from which you want to exclude the object.

7. Click **OK**.



Other Ways to Exclude Objects from Multiple Alarms

You can also exclude an object from multiple alarms using the object tree in the inventory pane.

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click the necessary view (*Veeam Backup & Replication*, *Veeam Backup for Microsoft 365*, *Virtual Infrastructure*, *VMware Cloud Director*, *Business View*).

3. In the inventory pane, right-click the necessary object in the inventory pane and select **Alarms** > **Define alarms** from the shortcut menu.

4. In the **Define Alarms** window, select check boxes next to alarms from which you want to exclude the object.

5. Click **OK**.

Viewing Alarm Exclusions

You can view the list of excluded objects for an alarm:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click **Alarm Management**.
3. Select the necessary alarm in the list and click **Show All Exclusions** in the **Actions** pane on the right.

Copying Alarms

Instead of creating a new alarm from scratch, you can create a copy of an existing alarm and modify its settings.

An alarm copy keeps the same settings as the original alarm, except the alarm assignment. Initially, an alarm copy is not assigned to any virtual infrastructure, VMware Cloud Director objects, Business View groups, or Veeam Backup & Replication and Veeam Backup for Microsoft 365 infrastructure components.

To copy an alarm:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click **Alarm Management**.

3. Select the necessary alarm in the list.

   Press and hold the `[CTRL]` or `[SHIFT]` key on the keyboard to select multiple alarms.

4. Do either of the following:

   - Right-click the selection and click **Copy** from the shortcut menu.
   - In the **Actions** pane on the right, click **Copy**.

What You Can Do Next

After you create an alarm copy, you can change its settings and assignment scope:

1. Select the alarm copy from the list of alarms.

   Veeam ONE uses the following pattern for names of alarm copies: *Copy of <alarm name>*.

2. Change alarm settings and alarm assignment scope.

   For details on alarm settings, see Creating Alarms.

Disabling and Enabling Alarms

You can disable and enable predefined and custom alarms.

Disabling Alarms

You can disable alarms that you do not use for monitoring:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.
2. At the bottom of the information pane, click **Alarm Management**.
3. In the information pane, select the necessary alarm.

   Press and hold the `[CTRL]` or `[SHIFT]` key on the keyboard to select multiple alarms.
4. Do either of the following:
   - Right-click the selection and select **Disable** from the shortcut menu.
   - In the **Actions** pane on the right, click **Disable**.

> **NOTE:**
>
> After you disable an alarm, all unresolved *Warning* or *Error* notifications that were triggered by this alarm will change their status to *Resolved*.

Enabling Alarms

To enable alarms that were previously disabled:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.
2. At the bottom of the information pane, click **Alarm Management**.
3. In the information pane, select the necessary alarm.

   Press and hold the `[CTRL]` or `[SHIFT]` key on the keyboard to select multiple alarms.
4. Do either of the following:
   - Right-click the selection and select **Enable** from the shortcut menu.
   - In the **Actions** pane on the right, click **Enable**.

Deleting Alarms

You can delete alarms you no longer need for monitoring:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click **Alarm Management**.
3. In the information pane, select the necessary alarm.

   Press and hold the `[CTRL]` or `[SHIFT]` key on the keyboard to select multiple alarms.

4. Do either of the following:
   - Right-click the selection and choose **Delete** from the shortcut menu.
   - In the **Actions** pane on the right, click **Delete**.
5. In the displayed dialog box, click **OK** to confirm deletion.

> **NOTE:**
>
> When you delete an alarm in the Alarm Management view, Veeam ONE retains the alarm history. All triggered alarms and alarm status changes will be available on the **Alarms** view.
>
> The status of a deleted alarm is changed to *Resolved*. To view the history of a deleted alarm, you need to apply the *Show resolved alarms* filter. For details on working with triggered alarms, see Viewing Triggered Alarms.

Exporting and Importing Alarms

You can export alarms to an XML file and import alarms from an XML file. Exporting and importing alarms can be useful if you need to back up your alarm settings, or if you want to copy alarm settings from one Veeam ONE deployment to another.

You can use export and import options to copy alarm settings between different Veeam ONE versions. Veeam ONE 13 supports import of alarm settings that were exported from Veeam ONE version 8.0 and later.

Exporting Alarms

To export alarms to an XML file:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click **Alarm Management**.
3. In the alarm management tree, select the type of infrastructure object for which you want to export alarms.
4. Right-click the object and choose **Export Alarms** from the shortcut menu.
5. Save the XML file with alarm settings.

Importing Alarms

To import alarms from an XML file:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

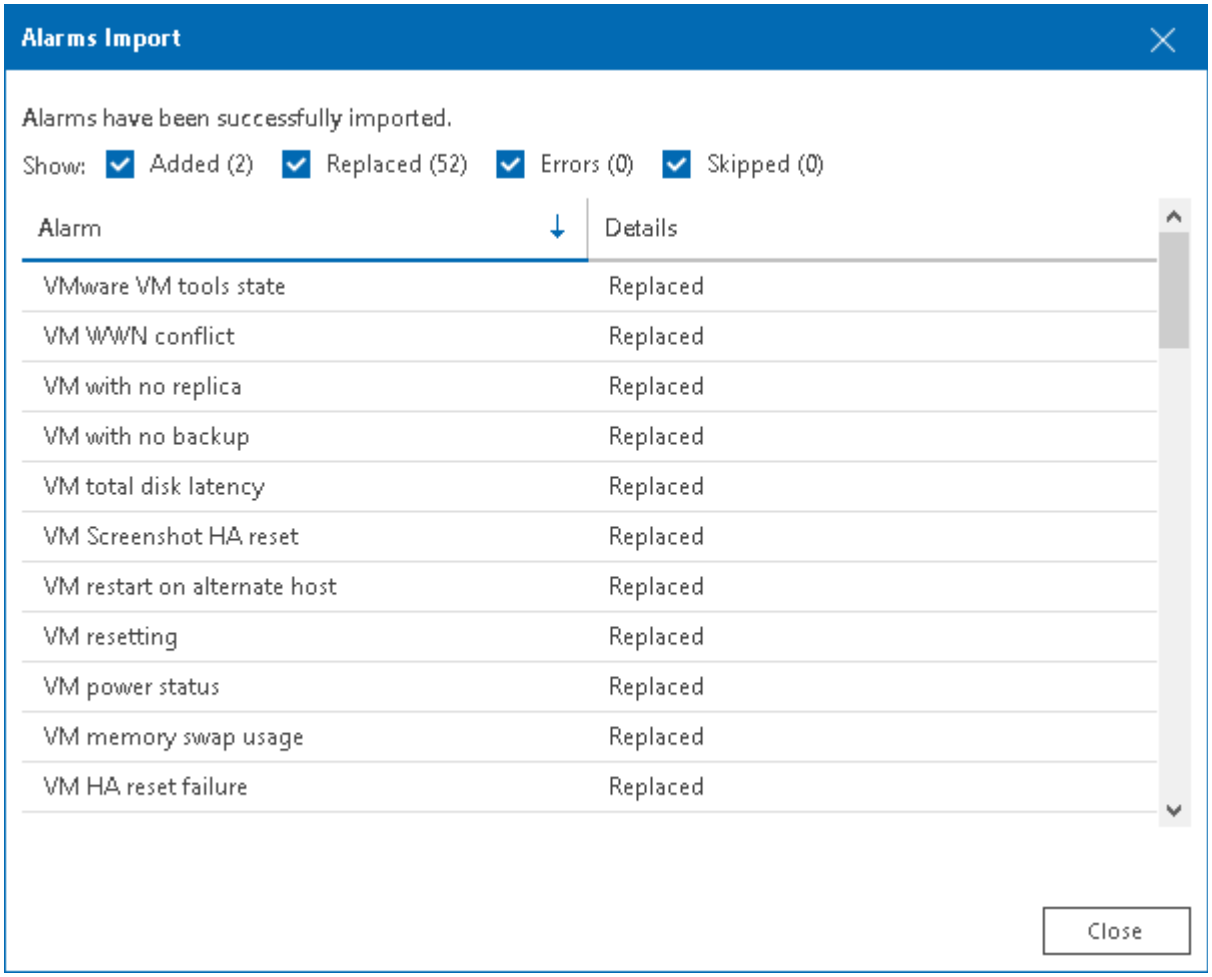
2. At the bottom of the inventory pane, click **Alarm Management**.
3. In the alarm management tree, right-click any object and choose **Import Alarms** from the shortcut menu.
4. In the **Alarms Import** window:
   - Specify a path to an XML file with alarm settings.
   - Select the **Import assignment** check box if you want to import a list of alarms together with their assignment settings.
   - Select the **Replace all existing alarms** check box if you want to replace existing alarms with imported alarms.

     If you do not select this check box, but during import Veeam ONE detects alarms with matching names, Veeam ONE will suggest you to update settings of the existing alarm with data from the XML file. You can either replace the existing alarm with the alarm from the XML file, or leave the existing alarm without any changes.

     If an alarm in the XML file does not match any existing alarm by name, Veeam ONE will create a new alarm.

5. When the import is finished, the **Alarms Import** window will display a report with the import status, the total number of added, replaced, and skipped alarms, and the number of alarms that were imported with errors.

   Review the report and click **Close** to close the **Alarms Import** window.



Suppressing Alarms

During resource-consuming operations, such as backup, Veeam ONE may send a great number of alarms informing about potential problems or increased resource pressure. If you do not want to receive notifications during specific activities or at a specific period of time, you can disable alarms for an object in your infrastructure. When alarms are suppressed, Veeam ONE disregards events and state changes to which the alarms react and does not trigger any alarms.

To suppress alarms, you can use one of the following options:

- Silence mode
- Alarm-specific suppression settings
- Suppression of guest disk space alarms

Silence Mode

Silence mode is an option used to suppress alarms for specific infrastructure objects during planned maintenance operations. After you switch an infrastructure object to the silence mode, Veeam ONE will suppress all alarms on this object.

You can enable the silence mode for single infrastructure objects or containers. When you enable the silence mode for a container, you can choose to propagate alarm suppression to its child objects. For example, if you want to perform maintenance on a host, you can enable the silence mode for the host itself and for all VMs on this host.

You can enable the silence mode manually or set a silence mode schedule.

> **NOTE:**
>
> Silence mode suppresses both alarms and Veeam Intelligent Diagnostics log analysis when active. For details, see Veeam Intelligent Diagnostics.

Enabling Silence Mode Manually

You can enable the silence mode for an infrastructure object manually. After you switch an infrastructure object to the silence mode manually, Veeam ONE will stop triggering alarms for this object until you manually disable the silence mode.

To enable the silence mode for an infrastructure object manually:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click the necessary view (*Veeam Backup & Replication*, *Veeam Backup for Microsoft 365*, *Virtual Infrastructure*, *VMware Cloud Director*, *Business View*).

3. In the inventory pane, right-click an infrastructure object and select **Silence Mode** from the shortcut menu.

   If you select an object container, you can select the scope of objects for which you want to enable the silence mode:

   - If you select **For this object**, the silence mode will be enabled for the selected object only. Alarms on its child objects will not be suppressed.

- If you select **For this and all contained objects**, the silence mode will be enabled for the container and its child objects.

After you enable the silence mode for an infrastructure object, Veeam ONE will change the infrastructure object icon, and will display the *Silence mode* label next to the object name in the inventory pane.

Scheduling Silence Mode

You can configure a silence mode schedule for infrastructure objects. When a schedule is set, the silence mode will be enabled and disabled automatically according to the schedule.

To configure a silence mode schedule:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click the necessary view (*Veeam Backup & Replication*, *Veeam Backup for Microsoft 365*, *Virtual Infrastructure*, *VMware Cloud Director*, *Business View*).

3. In the inventory pane, right-click an infrastructure object and choose **Schedule Silence Mode** from the shortcut menu.

4. In the **Schedule Silence Mode** window, configure the silence mode schedule.

   a. Click **Add**.

   b. In the **Type** field, specify how often the object must be placed into the silence mode (*once*, *monthly*, *weekly*, *daily*).

   c. In the **Day/Date** field, specify a day when the silence mode must be enabled.

   d. In the **Start time** and **End time** fields, specify the start and end time of the silence mode period.

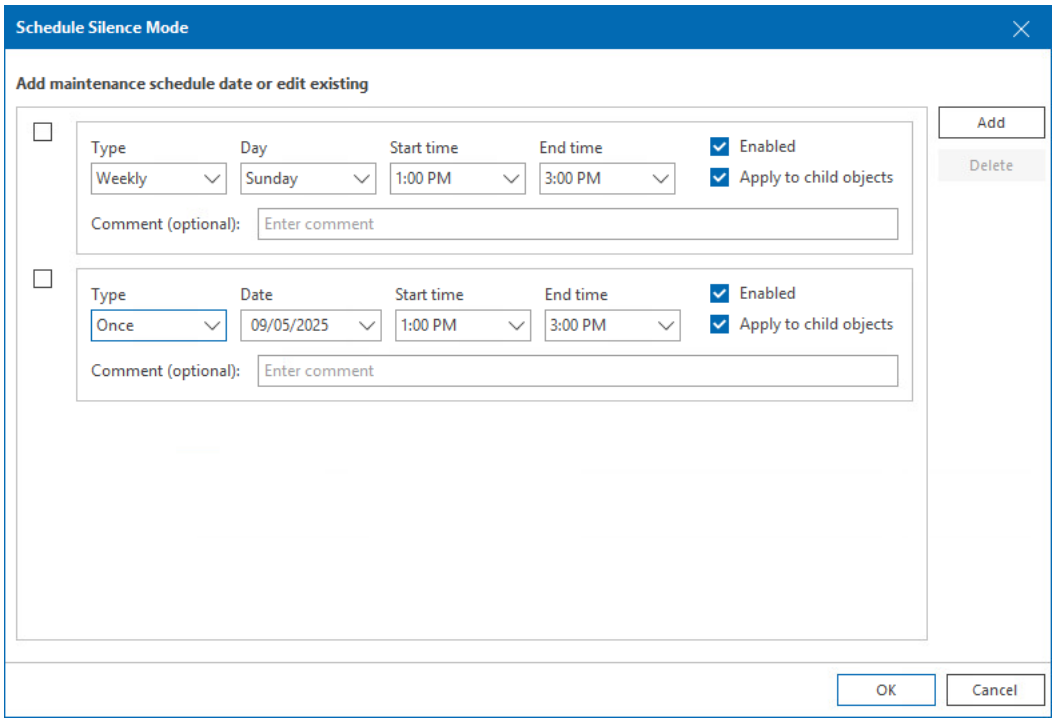
   e. Select the **Apply to child objects** check box if you want to enable the silence mode on the object itself and its child objects.

   f. In the **Comment** field, provide additional information about the planned silence mode period. You can enter up to 512 characters in this field.

   g. Select the **Enabled** check box to enable the silence mode schedule.

   h. Repeat steps **a-g** for each schedule entry you want to add.

5. Click **OK**.



To disable a silence mode schedule:

1. In the **Schedule Silence Mode** window, clear the **Enabled** check box next to the necessary schedule entry.
2. Click **OK**.

The disabled schedule will remain on the list, but it will not be applied to the object.

To delete a schedule:

1. In the **Schedule Silence Mode** window, select the check box next to the schedule entry you want to remove.
2. Click **Delete**.
3. Click **OK**.

Disabling Silence Mode

To exit a scheduled or manual silence mode period:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.
2. In the inventory pane, right-click an object in the silence mode and select **Exit Silence Mode**.

After you exit the silence mode, Veeam ONE will resume triggering alarms.

Alarm-Specific Suppression Settings

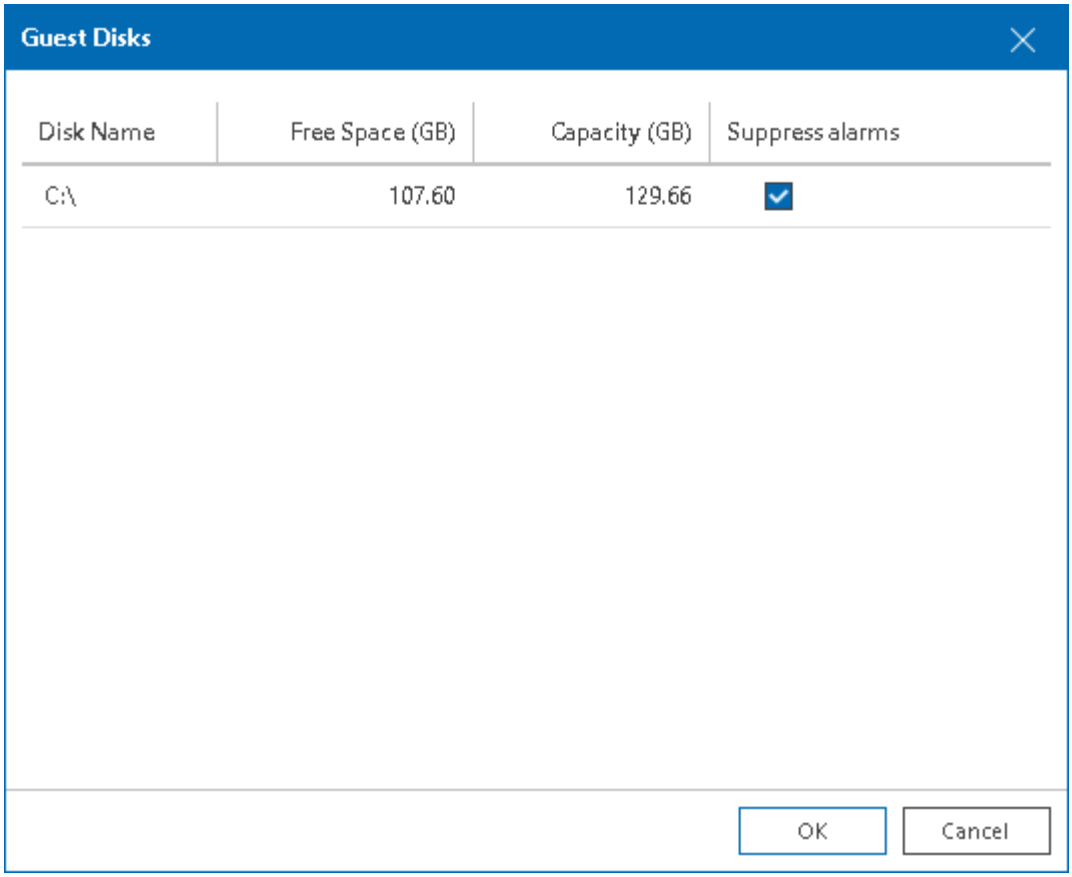
For each alarm, you can configure individual suppression settings to disable the alarm during specific resource-consuming operations. For details on configuring alarm suppression settings, see Step 7. Configure Alarm Suppression Settings.

Suppressing Guest Disk Space Alarms

You can suppress *Guest disk space* alarms for specific VM guest OS disks:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.
2. At the bottom of the inventory pane, click the necessary view (*Virtual Infrastructure*, *Business View*).
3. In the inventory pane, select the necessary VM.
4. In the information pane, open the **Summary** tab.
5. In the **Guest Disk Usage** section, click the **View all disks** link.
6. In the **Guest disks** list, select check boxes next to guest OS disks for which alarms must be suppressed.
7. Click **OK**.



Modeling Alarm Number

Alarm modeling allows you to forecast the number and type of alarms that will be sent for a specific infrastructure object within a specified time interval. To model the alarm number, Veeam ONE applies the current alarm settings to historical data collected for the selected infrastructure object, and calculates the approximate number of alarms that will be sent within the specified time interval in future.

Alarm modeling can help you avoid receiving non-significant alarms, or conversely missing important events. After you change alarm settings, you can perform alarm modeling to estimate how many alarms will be triggered for an infrastructure object if you keep the effective alarm settings. Taking into consideration the modeled number of alarms, you can consider changing alarm settings. For example, if the number is too high, you can adjust alarm rule conditions.

To forecast the number of alarms that will be sent for a specific infrastructure object:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. In the main menu, click **Modeling**.

3. In the **Alarm Modeling** window, click **Select** and choose the necessary type of infrastructure objects (*Veeam Backup & Replication*, *Virtual Infrastructure*, *VMware Cloud Director*).

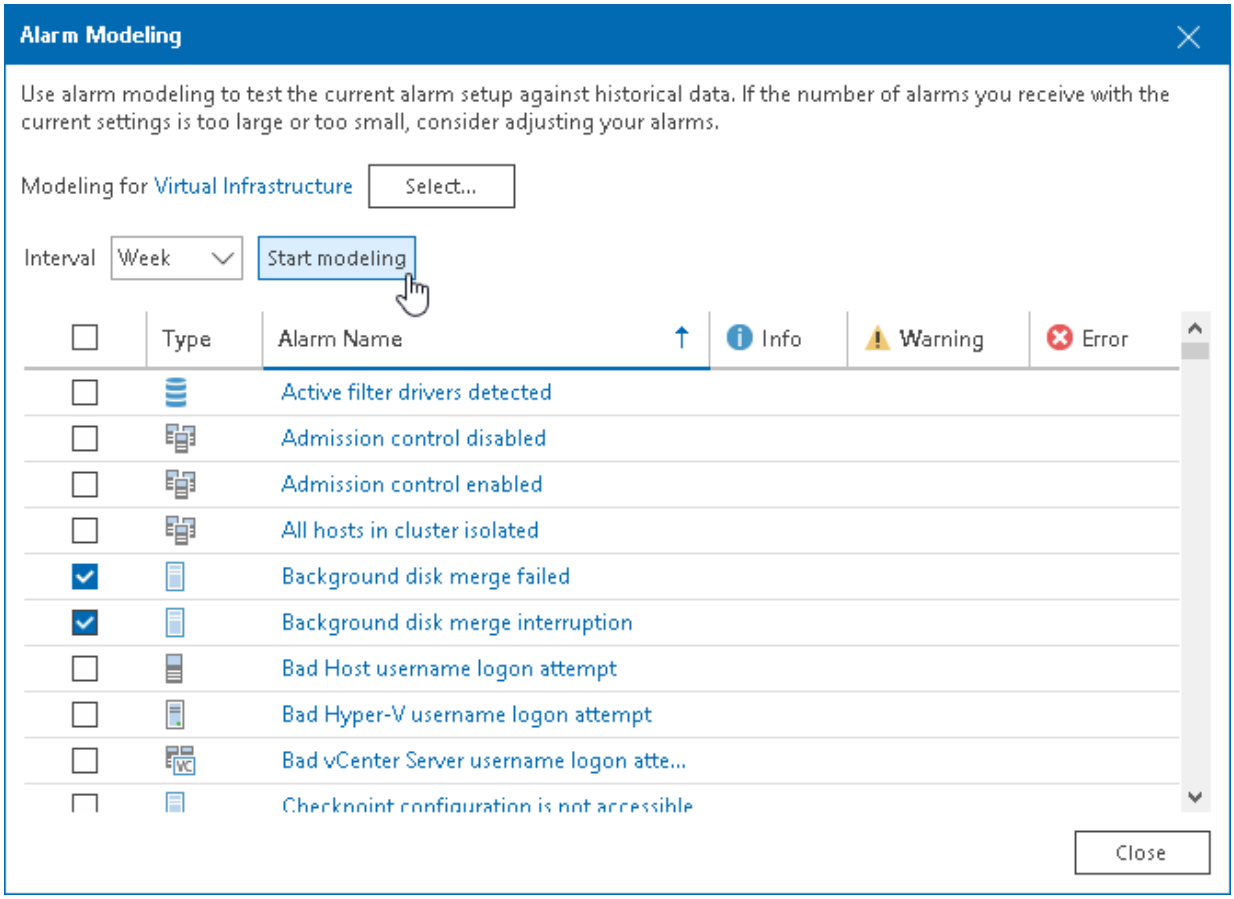
4. In the **Select Node** window, select check box next to an infrastructure object for which you want to model the number of alarms and click **Select**.

5. From the **Interval** drop-down list, select the period for which historical data must be analyzed (week, month or year).

6. In the list of alarms, select check boxes next to alarms for which you want to perform modeling.

7. Click **Start Modeling**.

Veeam ONE will forecast the number of alarms of different severity that will be sent within the selected period of time.



Other Ways to Perform Alarm Modeling

To perform alarm modeling for a selected infrastructure object:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click the necessary view (*Veeam Backup & Replication*, *Virtual Infrastructure*, *VMware Cloud Director*).

3. In the inventory pane, right-click an infrastructure object and select **Alarms** > **Modeling** from the shortcut menu.

4. From the **Interval** drop-down list, select the period for which historical data must be analyzed (week, month or year).

5. In the list of alarms, select check boxes next to alarms for which you want to perform modeling.

6. Click **Start Modeling**.

To perform alarm modeling for selected alarms:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click **Alarm Management**.

3. Select the one or more alarms in the list, right-click the selection and select **Modeling** from the shortcut menu.
4. At the bottom of the inventory pane, click the necessary view (*Veeam Backup & Replication*, *Virtual Infrastructure*, *VMware Cloud Director*).
5. In the **Select Node** window, select check box next to an infrastructure object for which you want to model the number of alarms and click **Select**.
6. From the **Interval** drop-down list, select the period for which historical data must be analyzed (week, month or year).
7. Click **Start Modeling**.

Configuring Alarm Notifications

To ensure you do not miss critical events or state changes in the managed infrastructure, you can configure Veeam ONE to send notifications when alarms are triggered. Veeam ONE supports the following types of alarm notifications:

- Configuring Email Notifications
- Configuring SNMP Traps
- Configuring ServiceNow Incidents
- Configuring Syslog Alarms

Configuring Email Notifications

To stay informed about potential problems, state changes, events, and tasks performed by users in your infrastructure, you can configure Veeam ONE to send email notifications about alarms. Email notifications contain basic information that helps to find the root cause of an issue and resolve it.

An email notification can be sent when a new alarm is triggered or when an existing alarm changes its status.

To configure alarm email notifications, perform the following steps:

1. Configure SMTP server settings.
2. Configure notification frequency.
3. Customize the email template.
4. Configure email recipients.
5. [Optional] Disable notifications about resolved alarms.

Step 1. Configure SMTP Server Settings

To deliver email notifications, Veeam ONE needs an SMTP server.

To configure SMTP settings:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. In the main menu, click **Settings** > **Server Settings**.

   Alternatively, you can press [CTRL + S] on the keyboard.

3. In the **Server Settings** window, open the **Mail Server Settings** tab.

4. Select the **Enable email notifications** check box.

5. From the drop-down list, select **Custom SMTP (Basic authentication)**.

6. In the **SMTP server** field, specify DNS name or IP address of the SMTP server that must be used for sending email notifications.

   The default SMTP port number is 25.

7. In the **From** field, enter an email address of the notification sender.

   This email address will be displayed in the **From** field of the email header.

8. To configure additional settings, click **Advanced**:

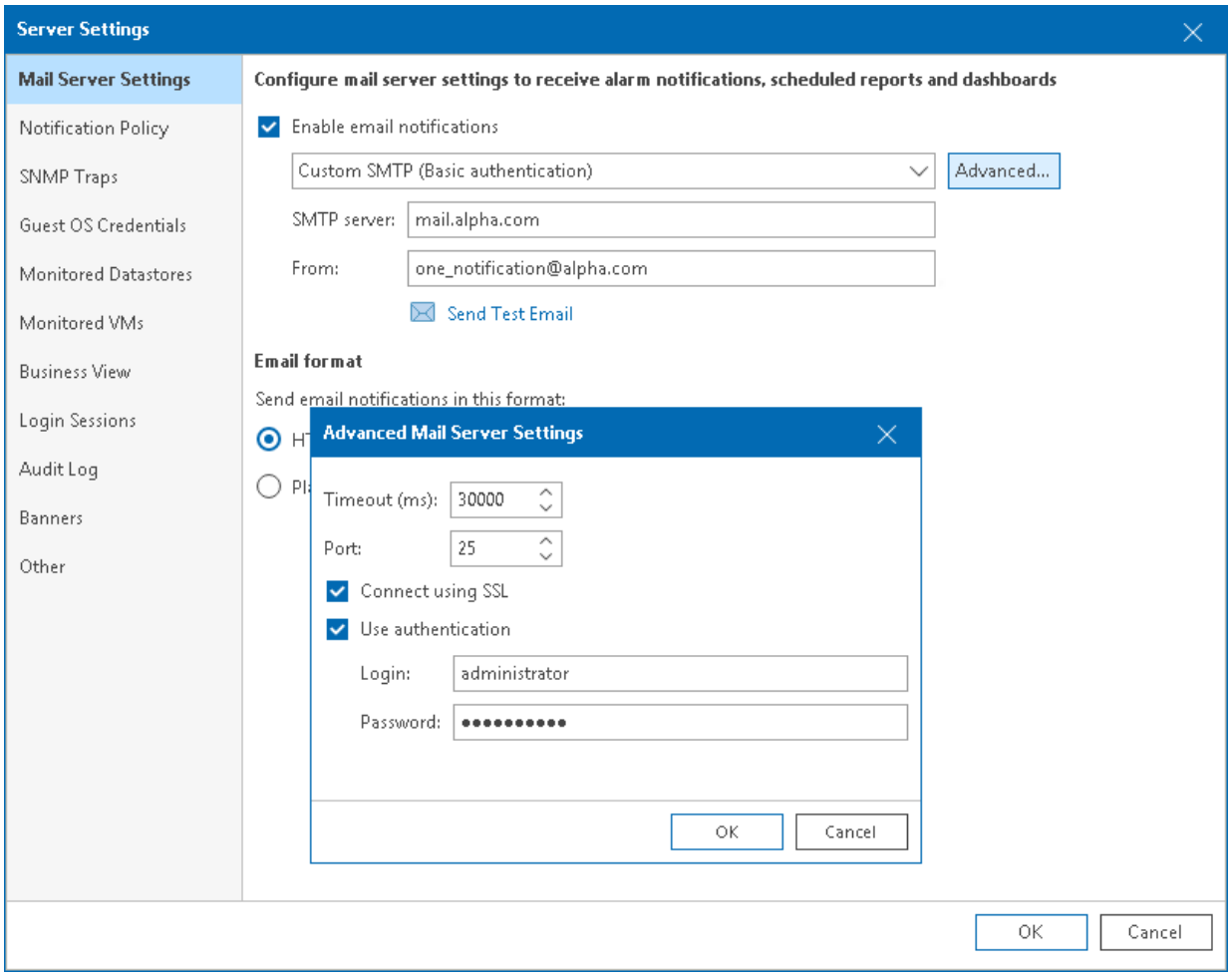
   a. In the **Timeout** field, specify server connection timeout in milliseconds.

   b. In the **Port** field, change the default SMTP communication port if required.

   c. For SMTP server with SSL support, select **Connect using SSL** to enable SSL data encryption.

   d. If your SMTP server requires authentication, select the **Use authentication** check box and specify authentication credentials in the **Login** and **Password** fields.

e. Click **OK**.

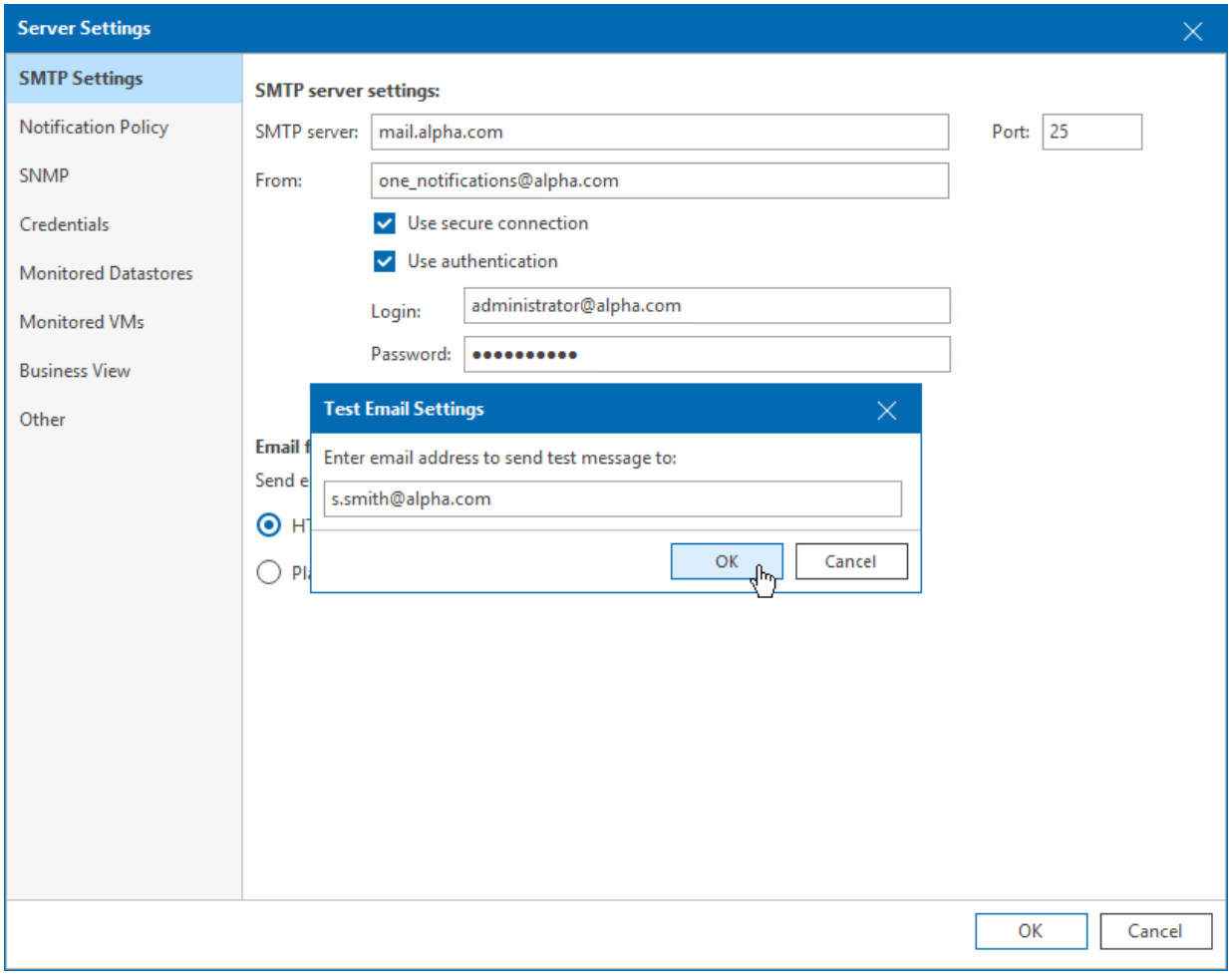


Sending Test Email

To check whether you have specified SMTP settings correctly, you can send out a test email:

1. Click **Send Test Email**.
2. In the **Test Email Settings** window, specify an email address to which a test notification must be sent.
3. Click **OK**.

The test email will be sent to the specified email address. Veeam ONE will notify you whether the message was successfully sent.



Step 2. Configure Notification Frequency

Veeam ONE sends an email notification when a new alarm is created or when the status of an existing alarm is changed. If you do not want to receive an email message each time a new alarm is triggered or alarm status changes, you can change the notification frequency.

The frequency with which Veeam ONE sends email notifications is defined by *notification policy*. There are two types of notification policies:

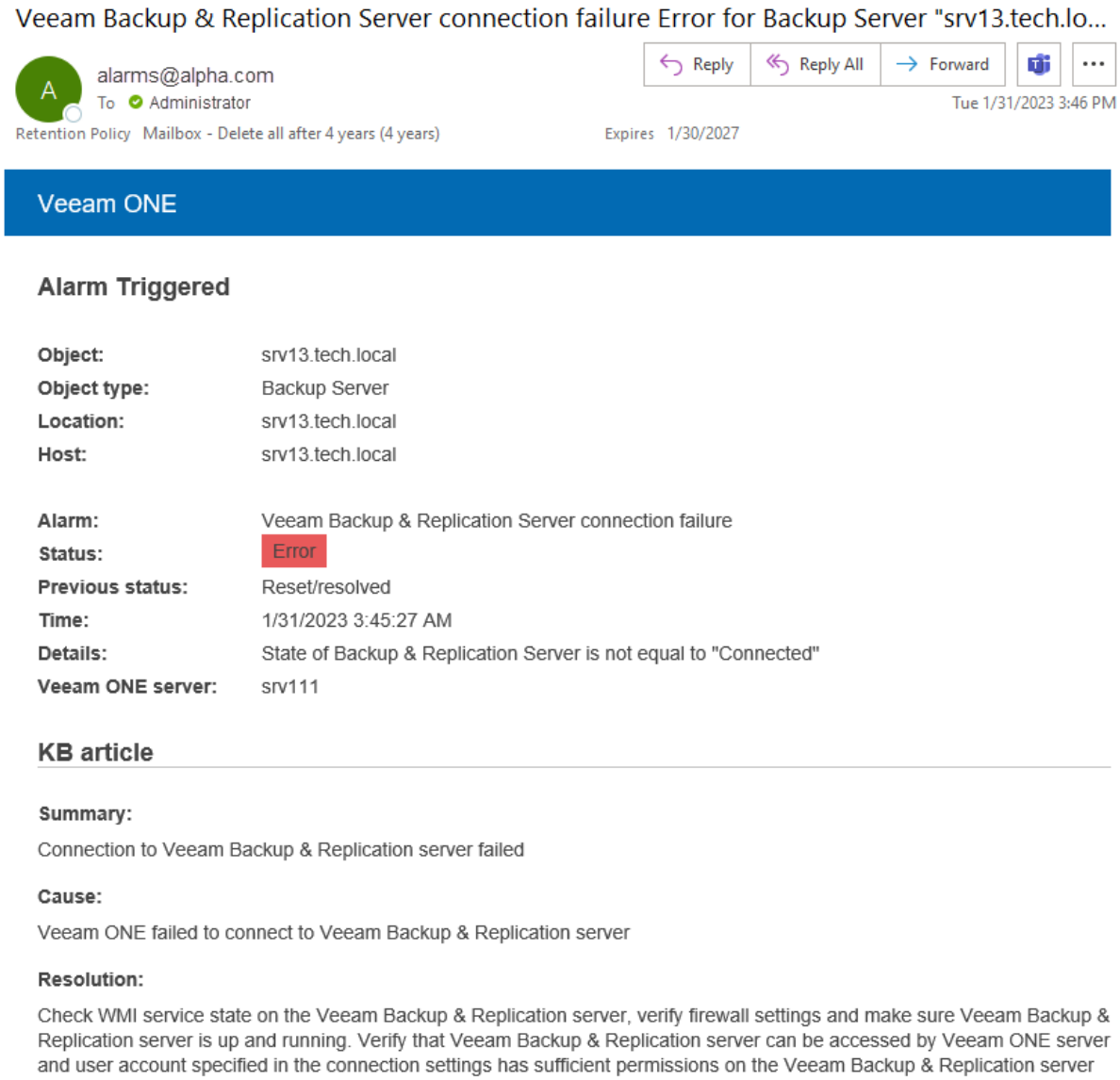
- Mission Critical
- Other

You can apply different types of notification policies to different infrastructure objects.

Enabling Mission Critical Notifications

Mission Critical notification policy is the default policy that is enabled for all infrastructure objects. This policy prescribes Veeam ONE to send an email notification every time a new alarm is created or the status of an existing alarm changes. An email notification contains details on the triggered alarm and affected object.

The following image shows an example of an email notification for the *Mission Critical* policy.



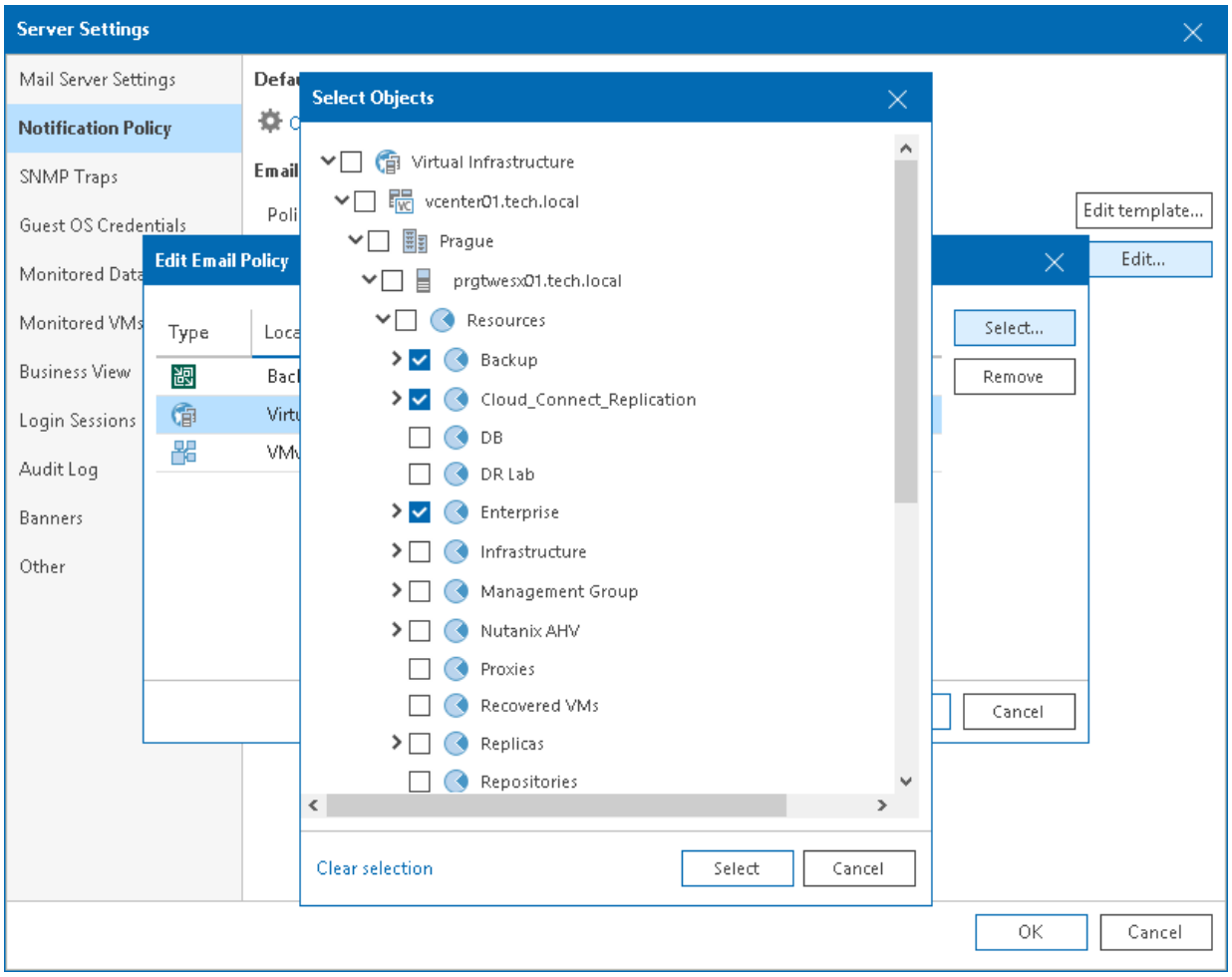
To apply the **Mission Critical** notification policy to an infrastructure object:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.
2. In the main menu, click **Settings** > **Server Settings**.

   Alternatively, you can press `[CTRL + S]` on the keyboard.
3. In the **Server Settings** window, open the **Notification Policy** tab.
4. In the **Email notification policies** section, select **Mission Critical** and click **Edit**.
5. In the **Edit Email Policy** window, click **Select** and choose one of the infrastructure types.
6. In the **Select Objects** window, click **Select**.

7. In the **Edit Email Policy** window, Click **OK**.

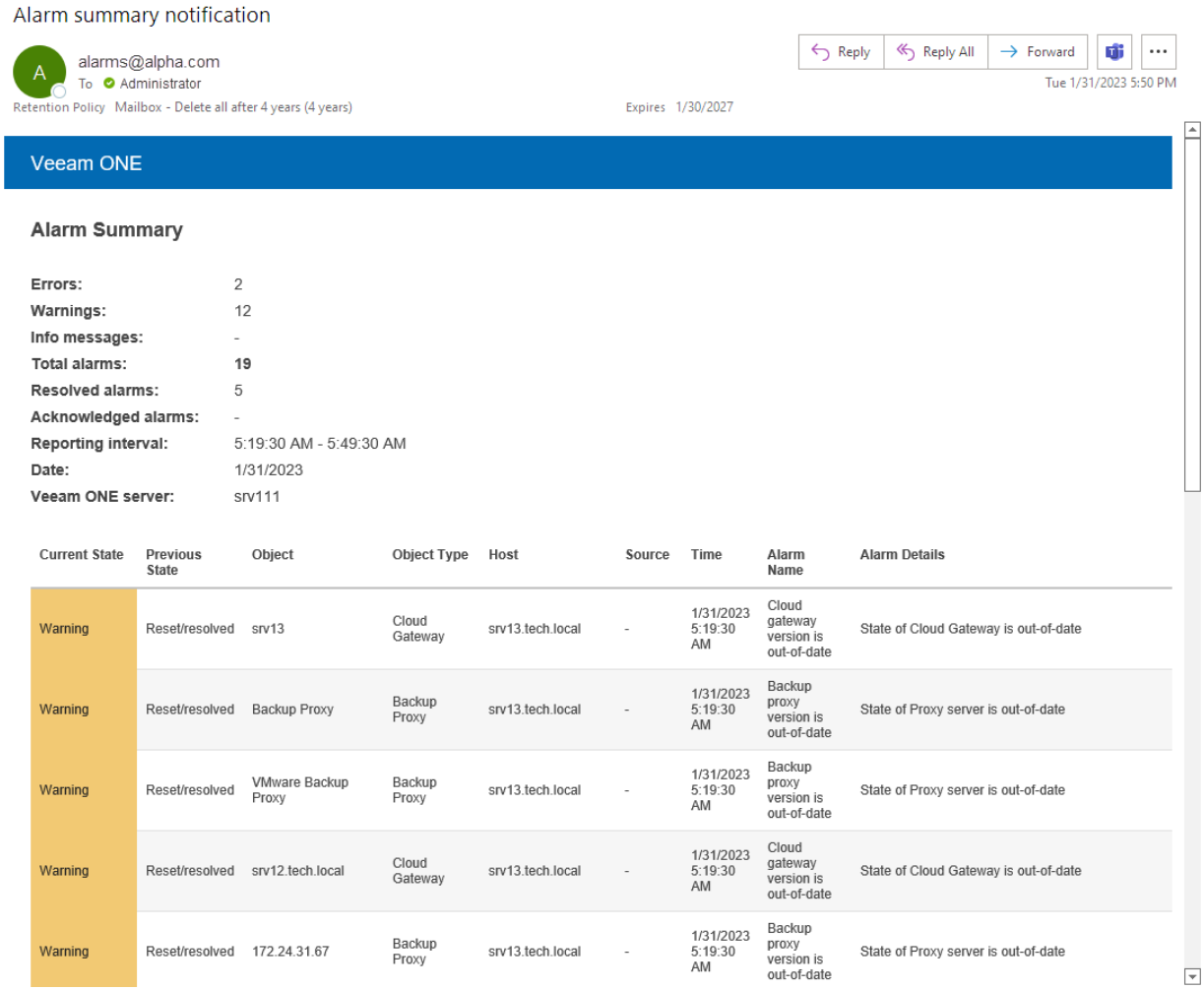


Enabling Summary Notifications

Other notification policy prescribes Veeam ONE to accumulate information about alarms and send an email notification once within a specific time interval (by default, a notification is sent once every 30 minutes). You do not receive a notification on every triggered alarm. Instead, Veeam ONE generates a message with a list of all alarms triggered over the past period.

You can choose how often you want to receive summary email notifications. For example, if you specify the time interval of 15 minutes, you will receive notifications with the list of alarms triggered over the past 15 minutes. If no alarms are triggered over the past 15 minutes, you will not receive a summary email notification.

The following image shows an example of a summary email notification for the *Other* policy.


Alarm summary notification

alarms@alpha.com
To Administrator
Retention Policy Mailbox - Delete all after 4 years (4 years)
Expires 1/30/2027

Reply | Reply All | Forward
Tue 1/31/2023 5:50 PM

Veeam ONE

Alarm Summary

Errors:	2
Warnings:	12
Info messages:	-
Total alarms:	**19**
Resolved alarms:	5
Acknowledged alarms:	-
Reporting interval:	5:19:30 AM - 5:49:30 AM
Date:	1/31/2023
Veeam ONE server:	srv111

Current State	Previous State	Object	Object Type	Host	Source	Time	Alarm Name	Alarm Details
Warning	Reset/resolved	srv13	Cloud Gateway	srv13.tech.local	-	1/31/2023 5:19:30 AM	Cloud gateway version is out-of-date	State of Cloud Gateway is out-of-date
Warning	Reset/resolved	Backup Proxy	Backup Proxy	srv13.tech.local	-	1/31/2023 5:19:30 AM	Backup proxy version is out-of-date	State of Proxy server is out-of-date
Warning	Reset/resolved	VMware Backup Proxy	Backup Proxy	srv13.tech.local	-	1/31/2023 5:19:30 AM	Backup proxy version is out-of-date	State of Proxy server is out-of-date
Warning	Reset/resolved	srv12.tech.local	Cloud Gateway	srv13.tech.local	-	1/31/2023 5:19:30 AM	Cloud gateway version is out-of-date	State of Cloud Gateway is out-of-date
Warning	Reset/resolved	172.24.31.67	Backup Proxy	srv13.tech.local	-	1/31/2023 5:19:30 AM	Backup proxy version is out-of-date	State of Proxy server is out-of-date

By default, all infrastructure objects have the *Mission Critical* policy assigned. Before you apply the *Other* notification policy to an object, you must remove the default *Mission Critical* policy assignment:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.
2. In the main menu, click **Settings** > **Server Settings**.

   Alternatively, you can press `[CTRL + S]` on the keyboard.
3. In the **Server Settings** window, open the **Notification Policy** tab.
4. In the **Email notification policies** section, select the *Mission Critical* policy and click **Edit**.
5. In the **Edit Email Policy** window, select the necessary type of infrastructure objects and click **Remove**.
6. In the **Edit Email Policy** window, click **OK**.

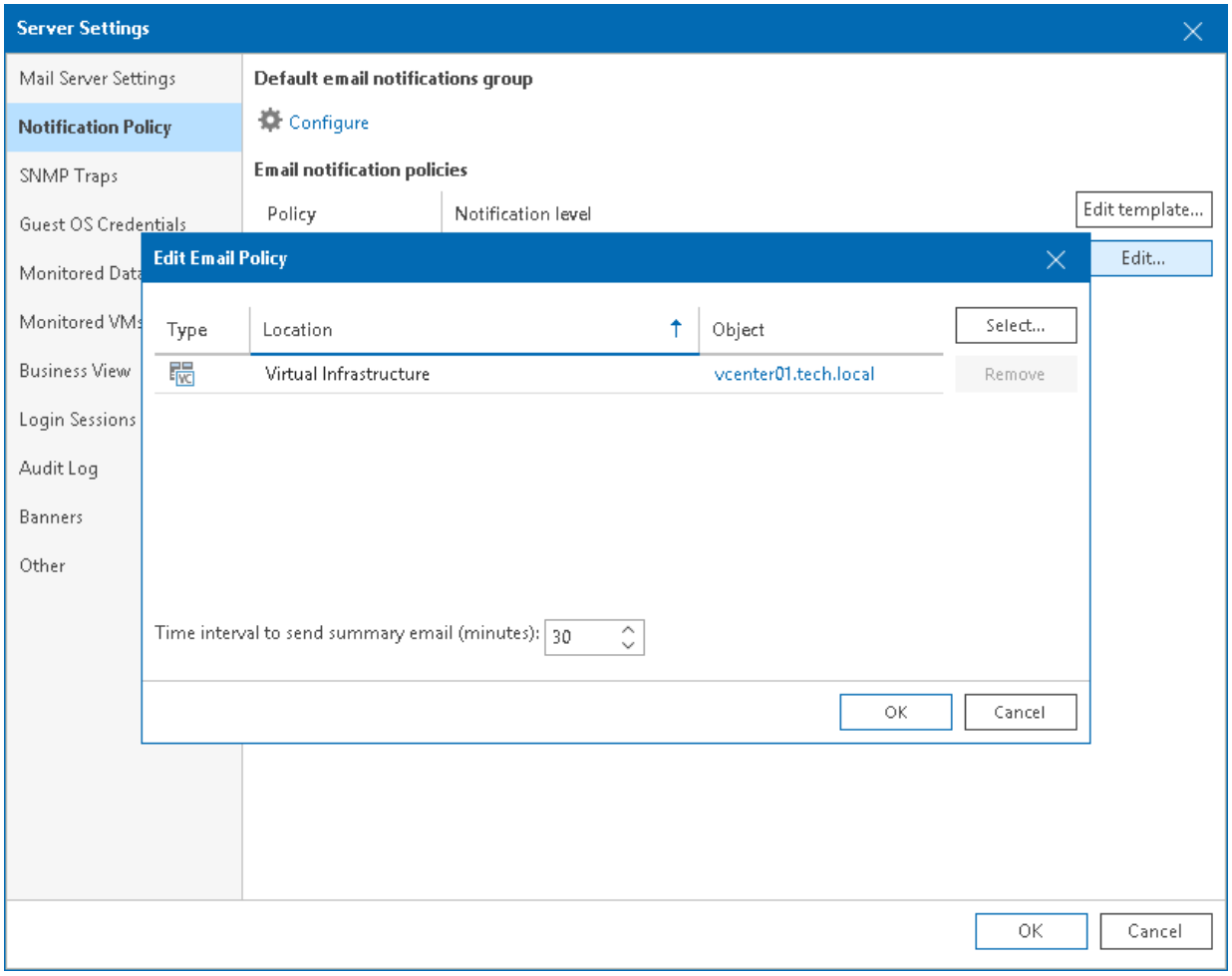
To apply the *Other* notification policy to one or more infrastructure objects:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.
2. In the main menu, click **Settings** > **Server Settings**.

   Alternatively, you can press `[CTRL + S]` on the keyboard.

3. In the **Server Settings** window, open the **Notification Policy** tab.
4. In the **Email notification policies** section, select *Other* and click **Edit**.
5. In the **Edit Email Policy** window, click **Select** and choose one of the infrastructure types.
6. In the **Select Objects** window, click **Select**.
7. In the **Time interval to send summary email (minutes)** field, specify how often Veeam ONE must send out a summary email informing about triggered alarms. The default time interval is 30 minutes.
8. In the **Edit Email Policy** window, click **OK**.



Step 3. Customize Email Template

You can customize the email template used for alarm notifications. In the template, you can change the following items:

- Email subject and body
- Email format

> **NOTE:**
>
> You can customize the email template for *Mission Critical* notifications only. You cannot modify the template for alarm summary notifications sent in accordance with the *Other* notification policy. For more information on notification policies, see Step 2. Configure Notification Frequency.

Configuring Email Subject and Body

You can customize the email notification subject:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.
2. In the main menu, click **Settings** > **Server Settings**.

   Alternatively, you can press `[CTRL + S]` on the keyboard.
3. In the **Server Settings** window, open the **Notification Policy** tab.
4. In the **Email notification policies** section, select *Mission Critical* and click **Edit template**.
5. In the **Email subject template** field, specify the subject of the notification.

   You can use the following variables in the subject text:

   - *%ALARM_NAME%* — name of the alarm
   - *%TIME%* — date and time when the alarm was triggered or when the alarm status changed
   - *%STATUS%* — current alarm status
   - *%OLD_STATUS%* — status of the alarm before its status was changed
   - *%OBJECT%* — affected infrastructure object
   - *%OBJECT_TYPE%* — type of the affected infrastructure object
   - *%SOURCE%* — affected child object
   - *%LOCATION%* — location of the object in the infrastructure tree
   - *%HOST%* — name of a vCenter Server, SCVMM server, or Veeam Backup & Replication server
6. In the **Select additional fields to include to the email notifications** section, select check boxes next to options you want to include in the body of the email message.

   General options apply to email notification for all types of alarms.

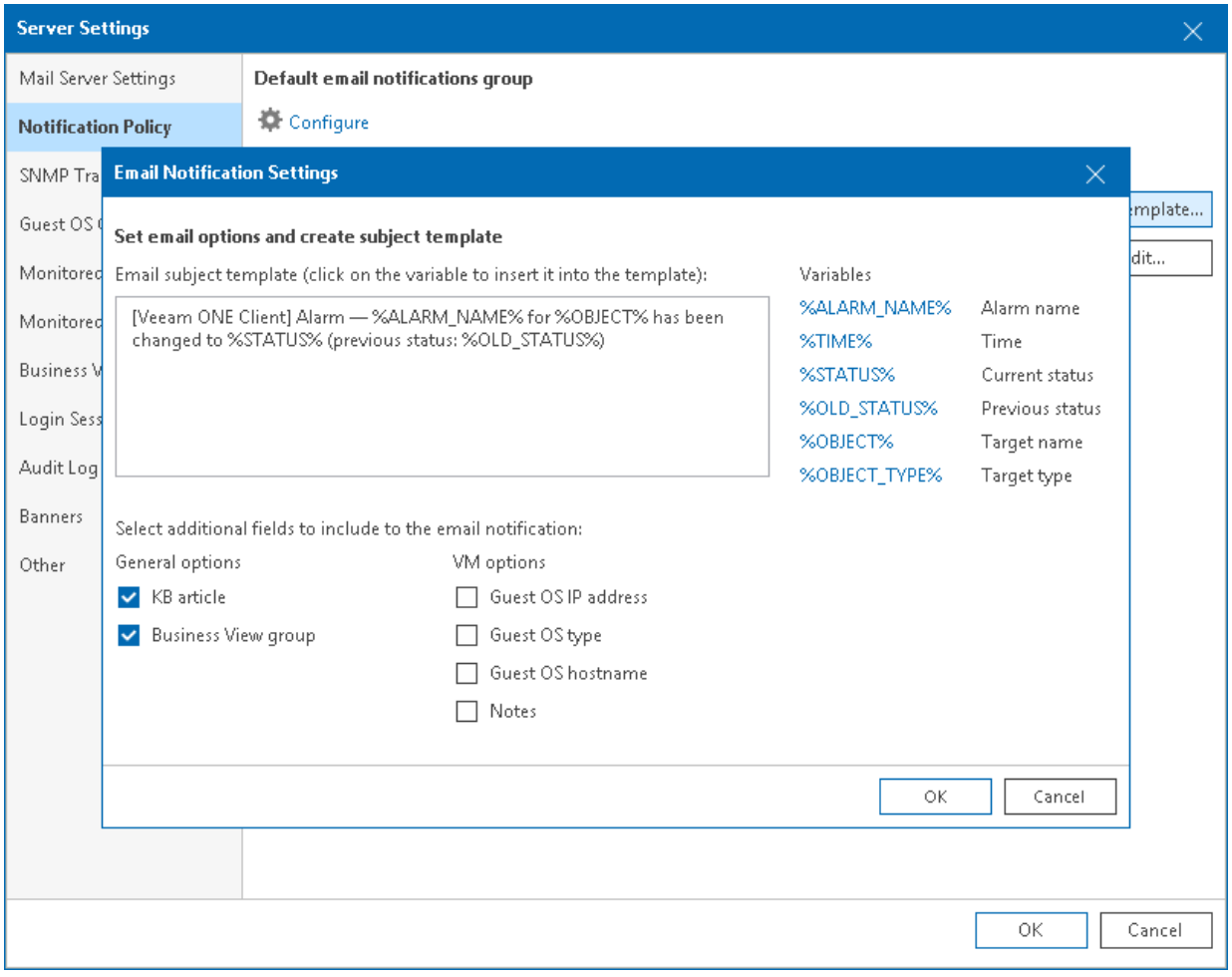
   - **KB article** — select this check box if an email notification must include a knowledge base article.

- **Business View group** – select this check box if an email notification must include a category assigned to the object in Business View.

VM options apply to email notifications for VM alarms.

- **Guest OS IP address** – select this check box if an email notification must include IP and MAC addresses of the affected VM.
- **Guest OS type** – select this check box if an email notification must include information about the guest OS of the affected VM.
- **Guest OS hostname** – select this check box if an email notification must include a DNS name of the affected VM.
- **Notes** – select this check box if an email notification must include custom notes that can be specified in alarm details.

7. Click **OK**.



Configuring Email Format

By default, Veeam ONE sends email notifications in the HTML format. You can change notification format to *plain text*. Note that plain text notifications do not support HTML elements, formatted text, colors or graphics. Plain text notifications also do not include knowledge base articles.

To choose the email notification format:

1. Open Veeam ONE Client.

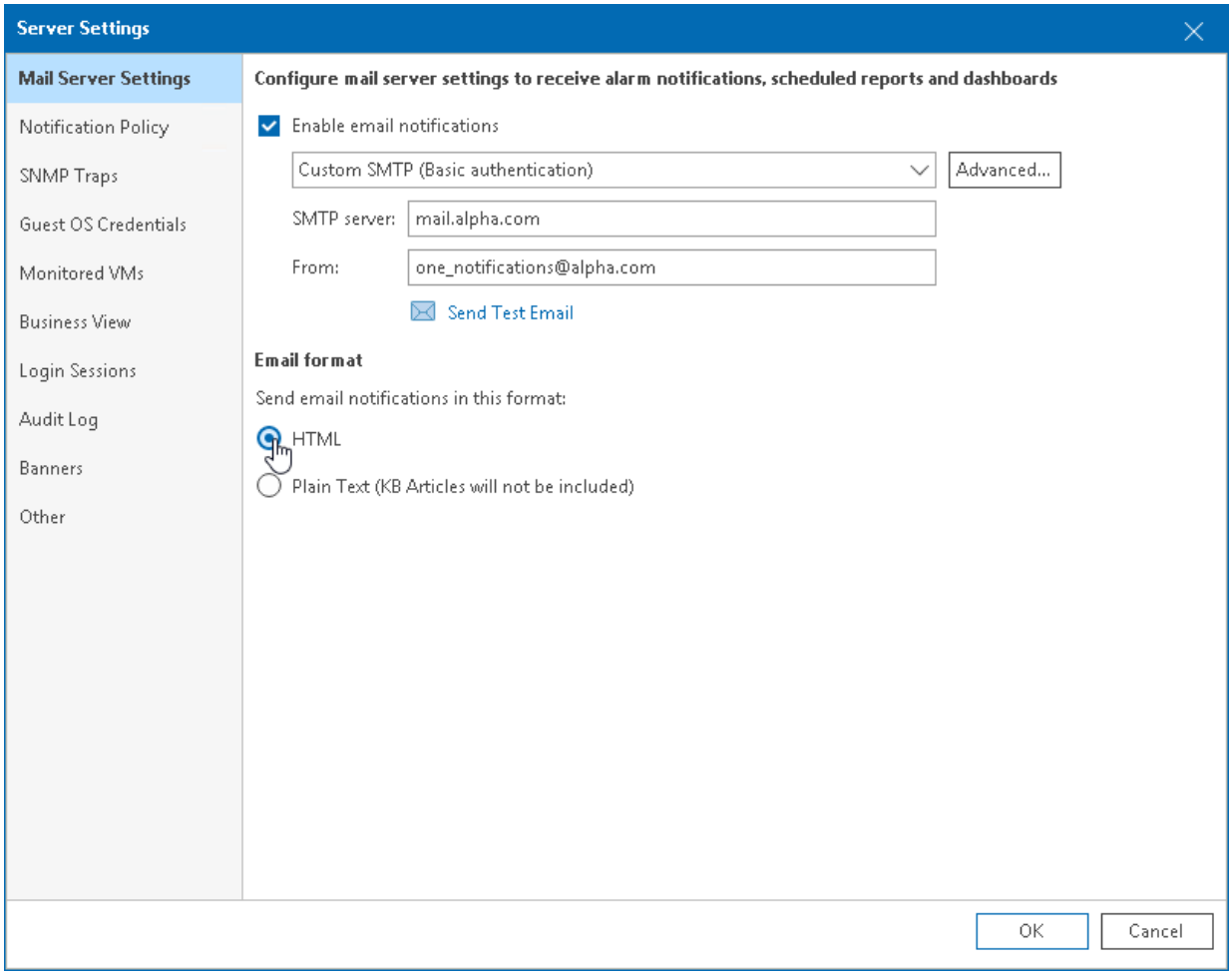
   For details, see Accessing Veeam ONE Components.

2. In the main menu, click **Settings** > **Server Settings**.

   Alternatively, you can press `[CTRL + S]` on the keyboard.

3. On the **SMTP Settings** tab, in the **Email format** section, choose a format: *HTML* or *Plain Text*.

4. Click **OK**.



Step 4. Configure Email Recipients

To report about triggered alarms by email, Veeam ONE must know where to deliver messages. When you configure alarm notifications, you must specify email addresses of users who will receive these notifications.

Veeam ONE offers the following options for configuring email notification recipients:

- You can add recipients to the default email notification group.

  This option can be useful if you want to notify responsible personnel when alarms are triggered or when alarms change their statuses.

- You can configure recipients for individual alarms.

  This option can be useful if you want to notify responsible personnel when a specific event occurs in the managed infrastructure.

Configuring Default Email Notification Group

The default email notification group includes a list of recipients who must be notified about alarms by email. All predefined alarms are configured to send email notifications to the default notification group. You can also configure custom alarms to send notifications to the default notification group.

To add recipients to the default email notification group:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. In the main menu, click **Settings** > **Server Settings**.

   Alternatively, you can press `[CTRL + S]` on the keyboard.

3. Open the **Notification Policy** tab.

4. In the **Default email notifications group** section, click **Configure**.

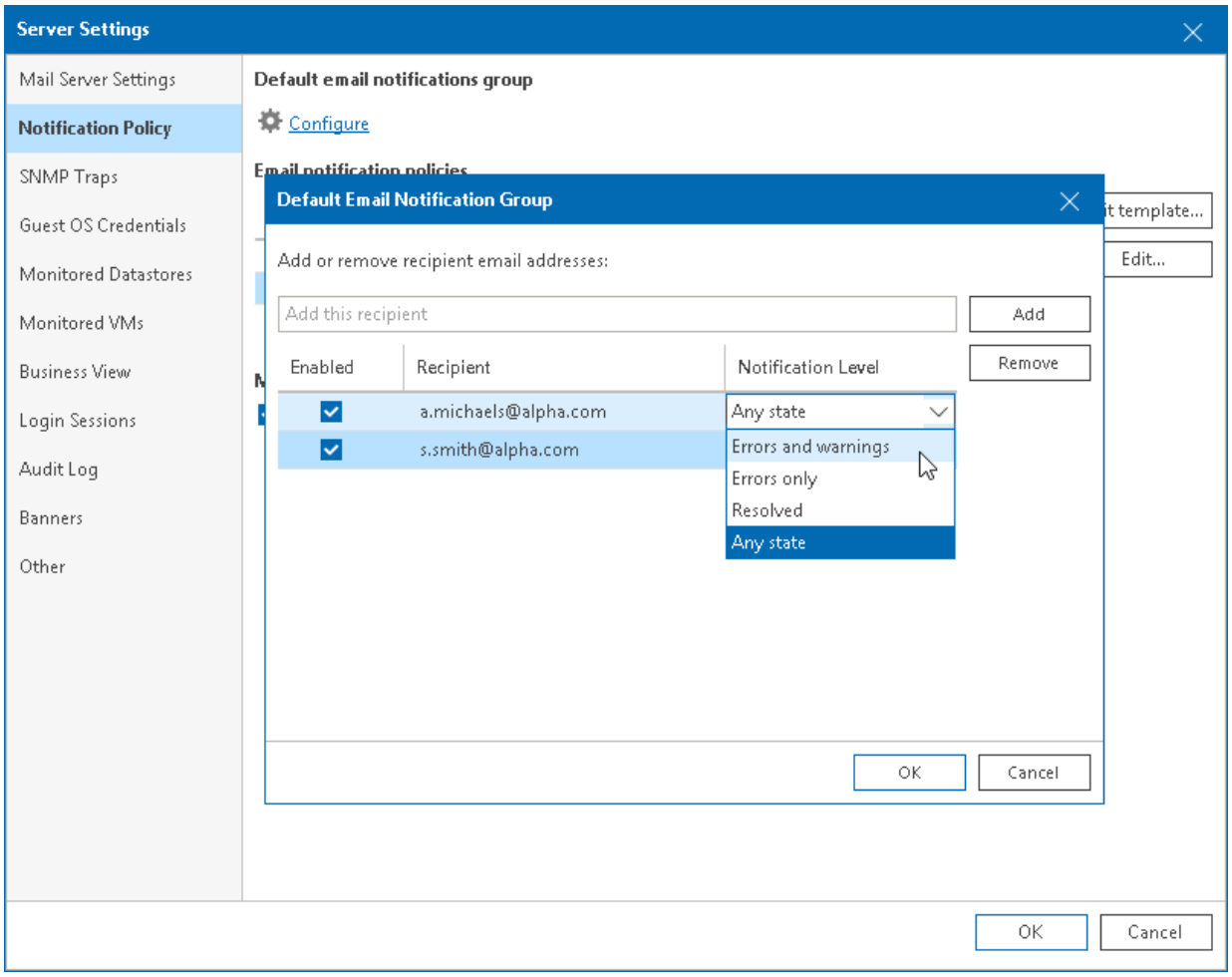
5. In the **Default Email Notification Group** window, specify email addresses of notification recipients.

   To add a recipient, in the **Add this recipient** field enter recipient email address and click **Add**. If you want to specify several recipients, separate email addresses with ";" (semicolon), "," (comma) or ", " (comma with space).

6. From the **Notification Level** list, choose the severity of alarms about which recipients must be notified:

   - **Any state** — an email notification will be sent every time when an alarm status changes to *Error*, *Warning*, *Info* or *Resolved*.
   - **Errors and warnings** — an email notification will be sent every time when an alarm status changes to *Error* or *Warning*.
   - **Resolved** — an email notification will be sent every time when an alarm status changes to *Resolved*.
   - **Errors only** — an email notification will be sent every time when an alarm status changes to *Error*.

7. Click **OK**.



You can temporarily disable email notifications for specific recipients in the default email notification group. The recipients will remain on the list, but they will no longer receive email notifications on triggered alarms.

1. In the **Default Email Notification Group** window, clear the check box next to recipient email address.
2. Click **OK**.

To permanently remove a recipient from the default email notification group:

1. In the **Default Email Notification Group** window, select an email address you want to delete and click **Remove**.
2. Click **OK**.

Configuring Recipients for Specific Alarms

You can add email notification recipients to each alarm individually and specify alarm severity about which the recipients must be notified.

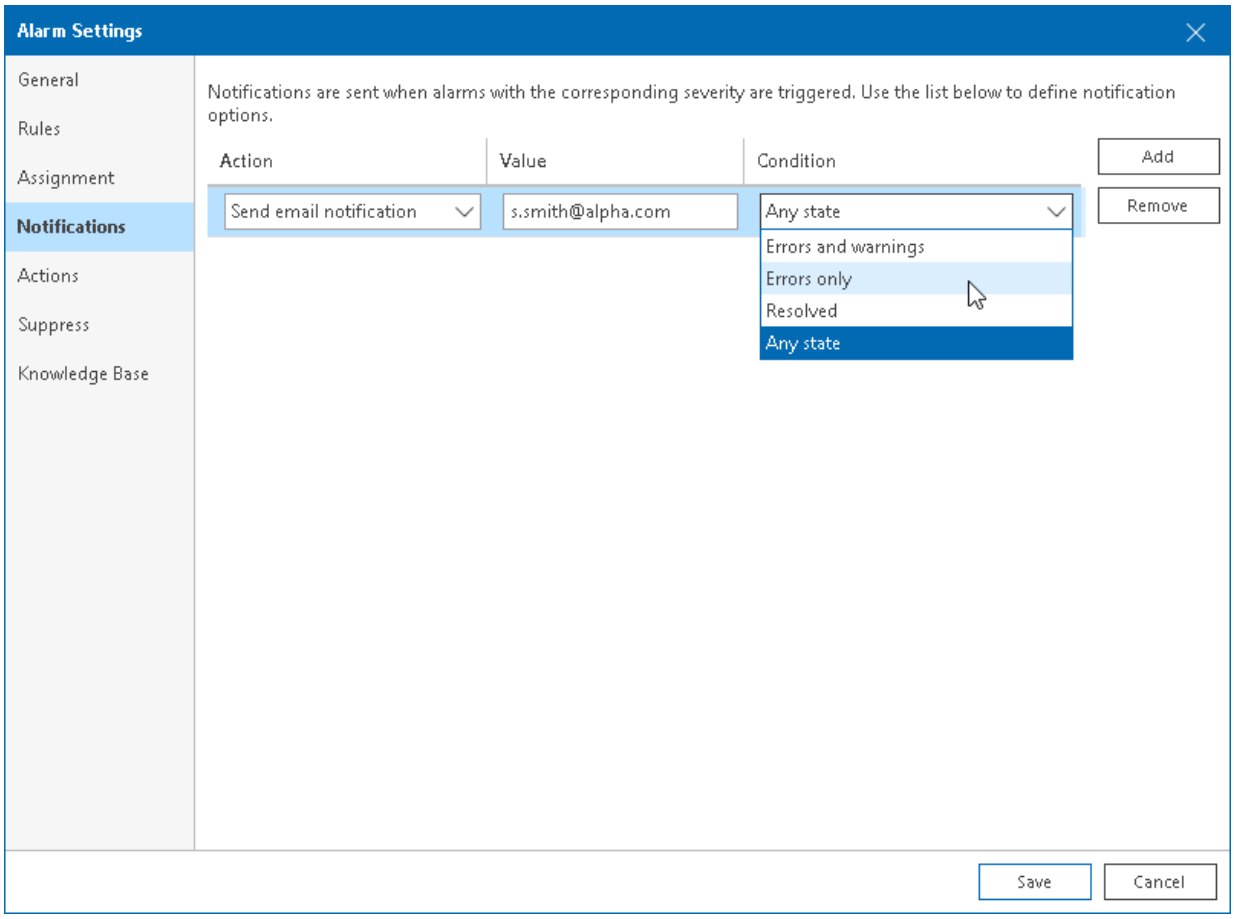
To add one or more recipients to a specific alarm:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.
2. At the bottom of the inventory pane, click **Alarm Management**.

3. To open the **Alarm Settings** window for the necessary alarm, do either of the following:
   - Double click the alarm in the list.
   - Right-click the alarm and choose **Edit** from the shortcut menu.
   - Select the alarm in the list and click **Edit** in the **Actions** pane on the right.
4. In the **Alarm Settings** window, open the **Notifications** tab.
5. On the **Notifications** tab, click **Add**.
6. From the **Action** list, select the **Send email notification** option.
7. In the **Value** field, specify an email address of the recipient.

   If you want to specify several recipients, separate email addresses with ";" (semicolon), "," (comma) or ", " (comma with space).
8. From the **Condition** list, choose the severity of alarms about which the recipient must be notified:
   - **Any state** – an email notification will be sent every time when an alarm status changes to *Error*, *Warning*, *Info* or *Resolved*.
   - **Errors and warnings** – an email notification will be sent every time when an alarm status changes to *Error* or *Warning*.
   - **Resolved** – an email notification will be sent every time when an alarm status changes to *Resolved*.
   - **Errors only** – an email notification will be sent every time when an alarm status changes to *Error*.
9. Click **Save**.



Step 5. Disable Notifications About Resolved and Acknowledged Alarms

By default, Veeam ONE sends an email notification when an alarm is triggered, when its status changes to *Error* or *Warning,* when an alarm is resolved and acknowledged. If you do not want to receive notifications on resolved and acknowledged alarms, you can disable them.

To disable email notifications on resolved and acknowledged alarms:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

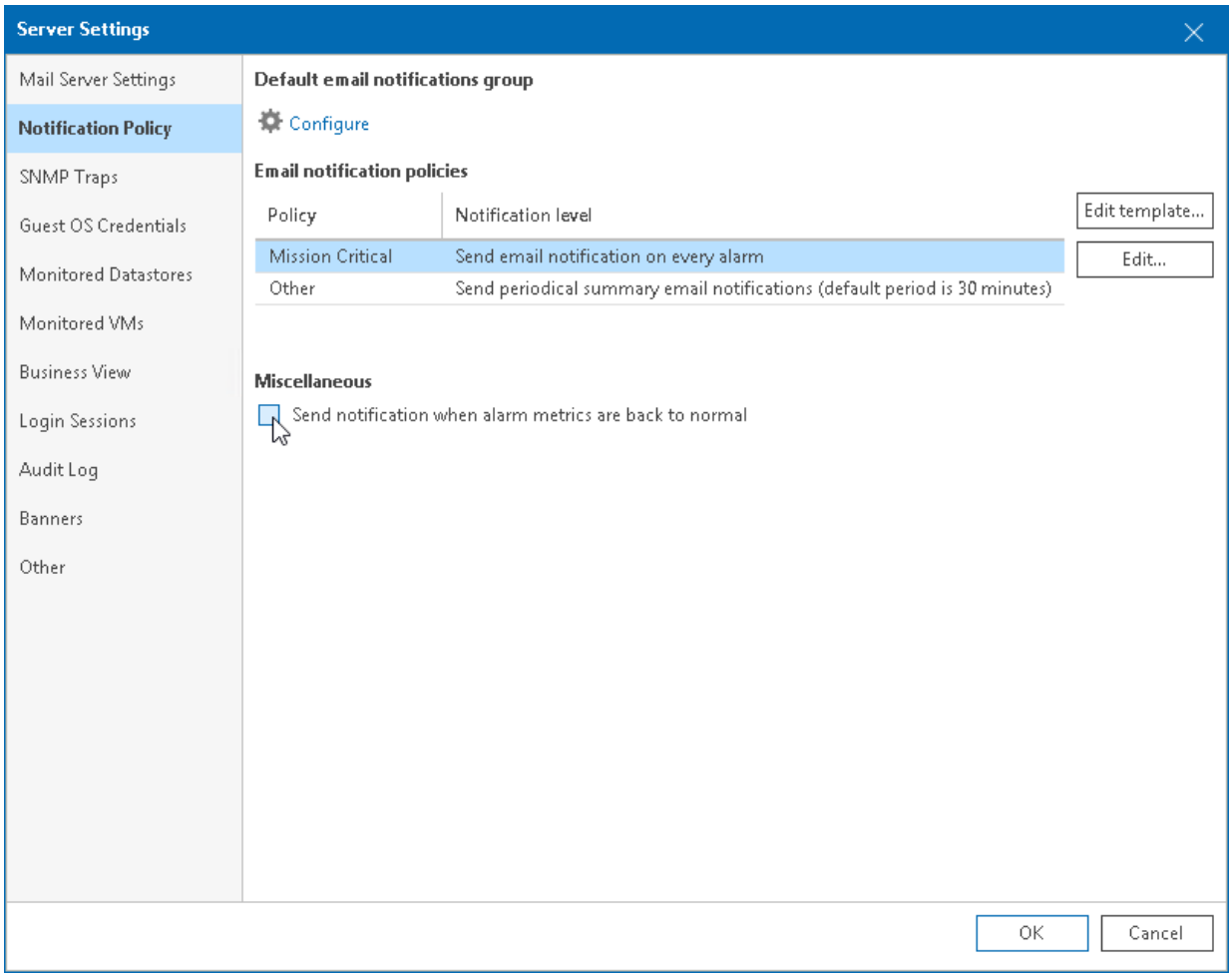
2. In the main menu, click **Settings** > **Server Settings**.

   Alternatively, you can press `[CTRL + S]` on the keyboard.

3. In the **Server Settings** window, open the **Notification Policy** tab.

4. In the **Miscellaneous** section, clear the **Send notification when alarm metrics are back to normal** check box.

5. Click **OK**.



Configuring SNMP Traps

If you use SNMP to monitor applications and devices in the managed infrastructure, you can configure Veeam ONE to report about triggered alarms by means of SNMP traps. When SNMP trap notifications are enabled, Veeam ONE acts as an agent. It generates trap messages when an alarm is triggered, and sends them to SNMP receivers. SNMP receivers can then forward the traps to a management application.

Veeam ONE sends SNMP traps with the following information:

- Date and time the alarm was triggered
- Name of the affected node
- Old alarm status
- New alarm status
- Alarm name
- Alarm summary

Veeam ONE supports SNMP versions 1, 2, and 3. For version 3, Veeam ONE sends traps based on CISCO-SNMP-USM-OIDS-MIB that complies with RFC 3414.

To configure SNMP traps, perform the following steps:

1. Configure SNMP receivers and manager.
2. Configure SNMP settings in Veeam ONE.
3. Change alarm action settings to enable SNMP traps for the necessary alarms.

Step 1. Configure SNMP Receivers and Manager

To receive and process SNMP traps generated by Veeam ONE, you must install and configure the following components:

1. SNMP receivers that will listen for traps.
2. SNMP management application that will obtain and process traps from receivers.

The configuration procedure depends on the SNMP processing solution you use to handle traps. To learn how to configure an SNMP receiver with Net-SNMP, see SNMPTRAPD.

Step 2. Configure SNMP Settings in Veeam ONE

To send SNMP traps, Veeam ONE must know trap destinations. You must specify a list of receivers to which Veeam ONE must send traps, and ports that SNMP receivers will listen.

To configure SNMP trap destination settings in Veeam ONE:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. In the main menu, click **Settings** > **Server Settings**.

   Alternatively, you can press `[CTRL + S]` on the keyboard.

3. In the **Server Settings** window, open the **SNMP Traps** tab.
4. Click **Add**
5. From the drop-down list on the left, select the preferable SNMP version.
6. Configure receiver settings. To do that:
   - For SNMP v.1 and v.2
     i. Double-click the added entry in the list.

     Alternatively, you can select the receiver entry and click **Configure**.

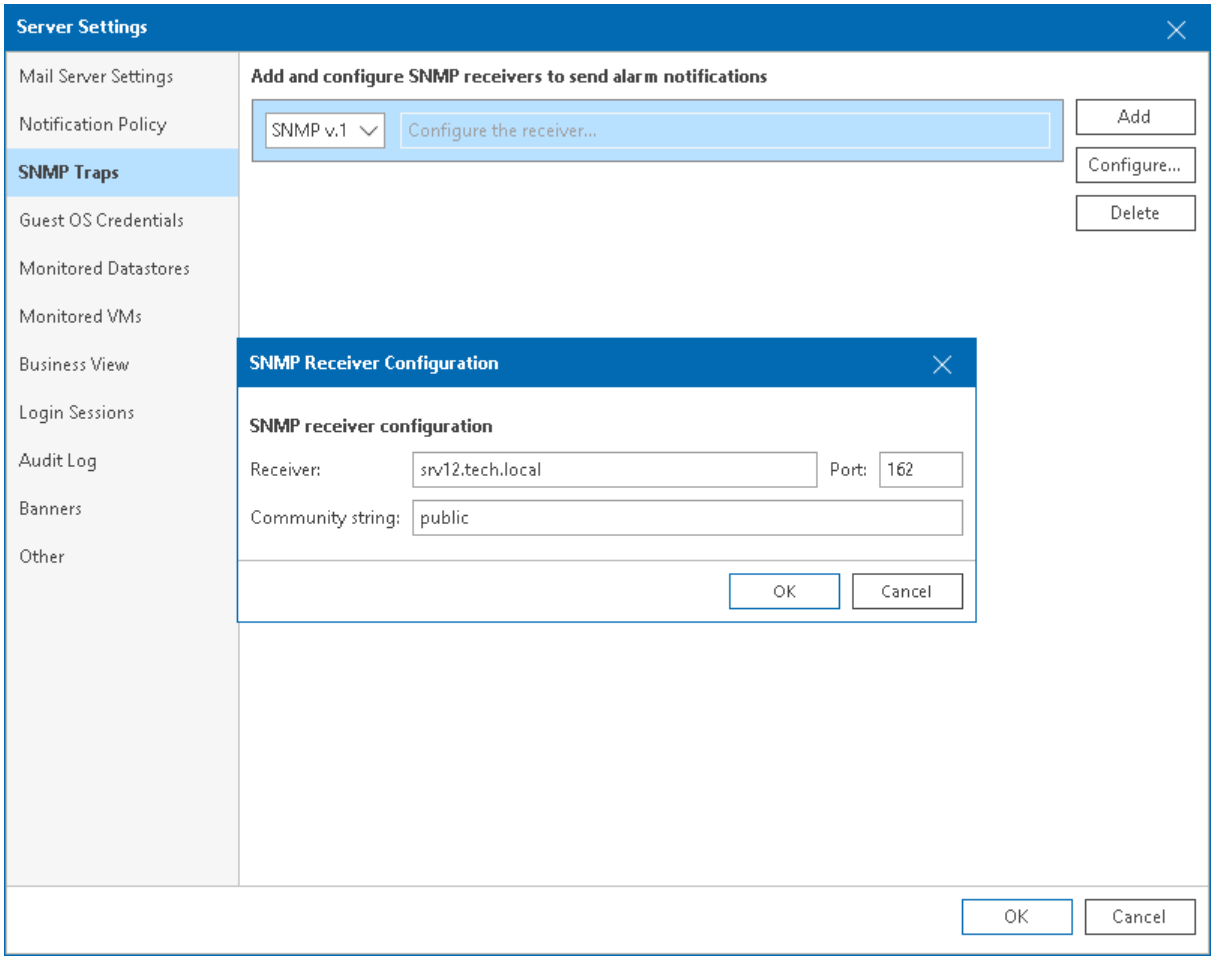
     ii. In the **Receiver** field, specify FQDN or IP address of the SNMP receiver.

     iii. In the **Port** field, specify the port number.

     iv. In the **Community string** field, specify the community identifier.

     v. Click **OK**.

vi. To add a new receiver to the list, click **Add** and repeat steps i-v.



- For SNMP v.3

  i. Double-click the added entry in the list.

  Alternatively, you can select the receiver entry and click **Configure**.

  ii. In the **Receiver** field, specify FQDN or IP address of the SNMP receiver.

  iii. In the **Port** field, specify the port number.

  iv. In the **Engine ID** field, specify an ID for an SNMP remote agent.

  v. In the **Username** and **Password** fields, specify credentials for SNMP receiver user account.

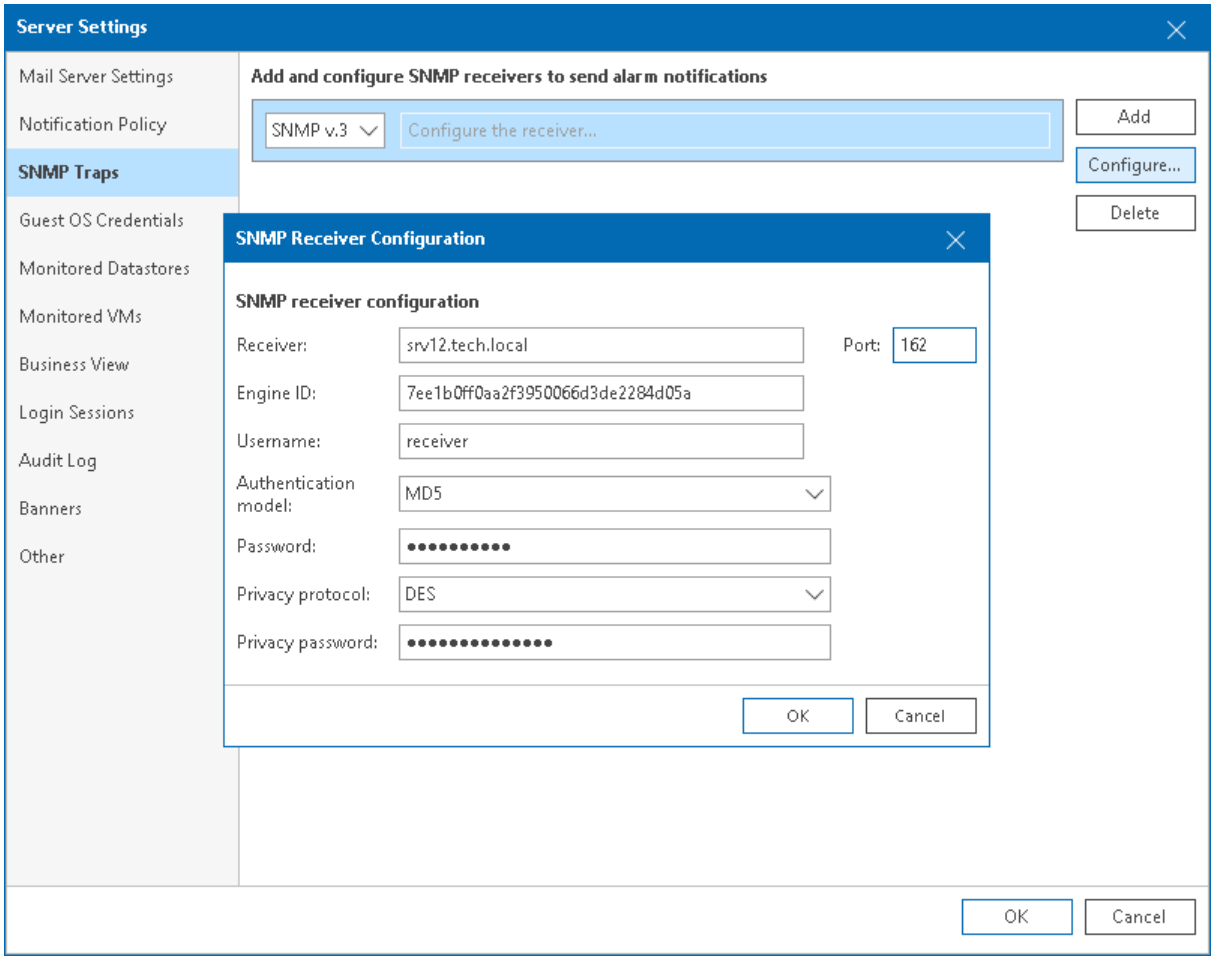
  vi. From the **Authentication model** list, select the authentication algorithm for SNMP receiver user.

  vii. From the **Privacy protocol** list, select encryption method for SNMP messages.

  viii. In the **Privacy password** field, specify a password that an SNMP receiver will use for private access.

  ix. Click **OK**.

x. To add a new receiver to the list, click **Add** and repeat steps i-ix.



7. Click **OK**.

Step 3. Enable SNMP Notification for Alarms

To receive SNMP traps when an alarm is triggered, you must set SNMP notification as a response action for every alarm manually.

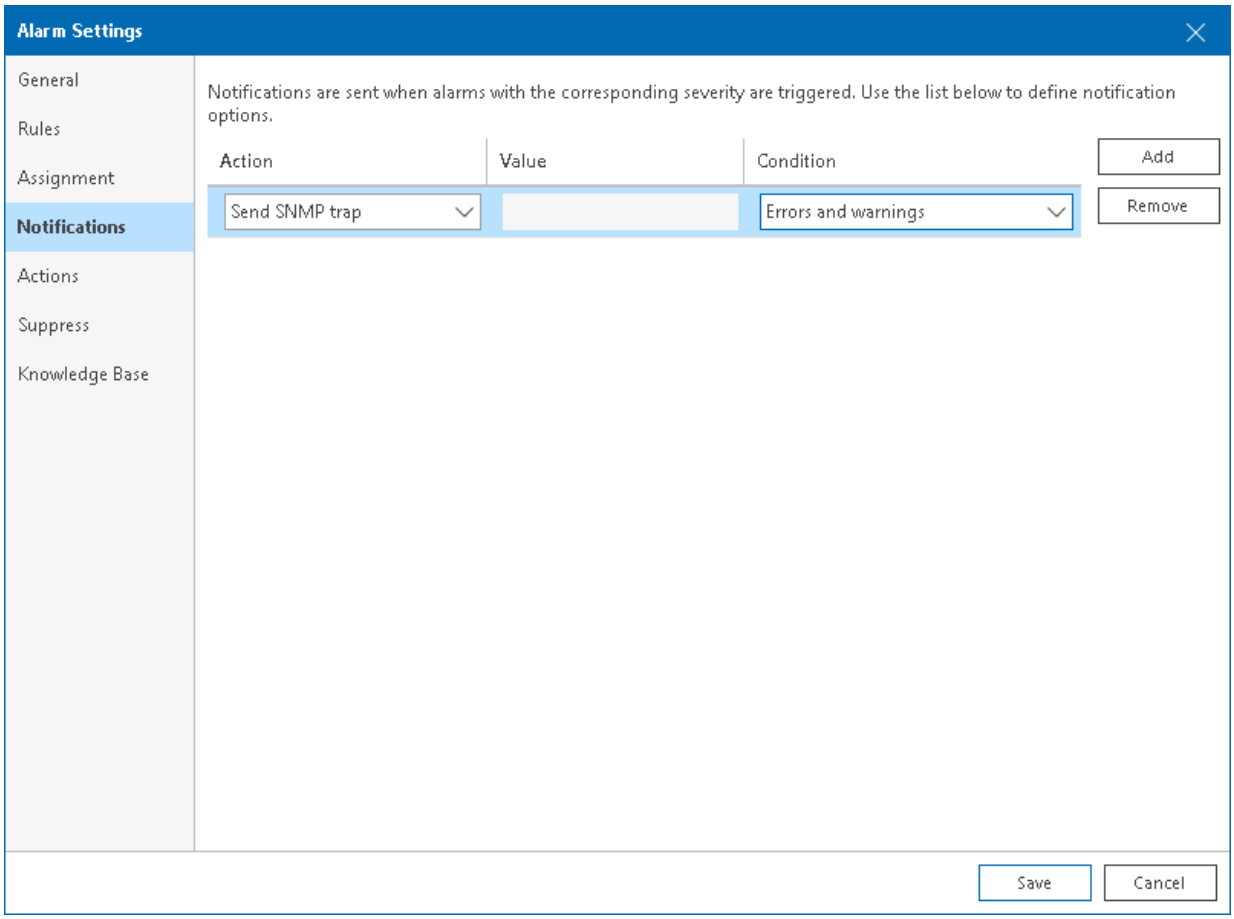
To configure SNMP traps for an alarm:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click **Alarm Management**.
3. To open the **Alarm Settings** window for the necessary alarm, do either of the following:
   - Double click the necessary alarm in the list.
   - Right-click the alarm and choose **Edit** from the shortcut menu.
   - Select the alarm in the list and click **Edit** in the **Actions** pane on the right.
4. In the **Alarm Settings** window, open the **Notifications** tab.
5. On the **Notifications** tab, click **Add**.
6. From the **Action** list, select **Send SNMP trap**.
7. From the **Condition** list, choose the severity of alarms about which recipients must be notified:
   - **Any state** — an SNMP trap will be sent every time when an alarm status changes to *Error*, *Warning*, *Info* or *Resolved*.
   - **Errors and warnings** — an SNMP trap will be sent every time when an alarm status changes to *Error* or *Warning*.
   - **Resolved** — an SNMP trap will be sent every time when an alarm status changes to *Resolved*.
   - **Errors only** — an SNMP trap will be sent every time when an alarm status changes to *Error*.

8. Click **Save**.



Configuring ServiceNow Incidents

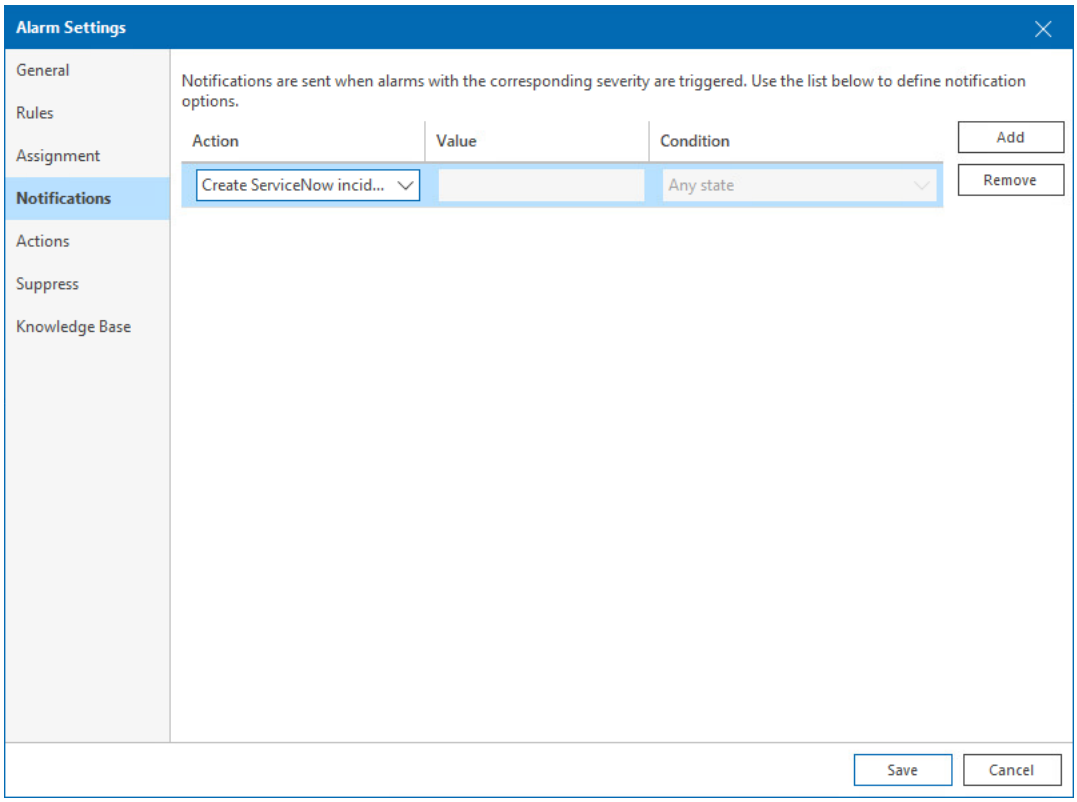
To receive ServiceNow incidents when an alarm is triggered, you must set ServiceNow notifications as a response action for every alarm manually.

To configure ServiceNow alarms:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.
2. At the bottom of the inventory pane, click **Alarm Management**.
3. To open the **Alarm Settings** window for the necessary alarm, do either of the following:
   - Double click the necessary alarm in the list.
   - Right-click the alarm and choose **Edit** from the shortcut menu.
   - Select the alarm in the list and click **Edit** in the **Actions** pane on the right.
4. In the **Alarm Settings** window, open the **Notifications** tab.
5. On the **Notifications** tab, click **Add**.
6. From the **Action** list, select **Create ServiceNow incident**.

7. Click **Save**.



Configuring Syslog Alarms

To receive Syslog alarms when an alarm is triggered, you must set Syslog notification as a response action for every alarm manually.

To configure Syslog alarms:

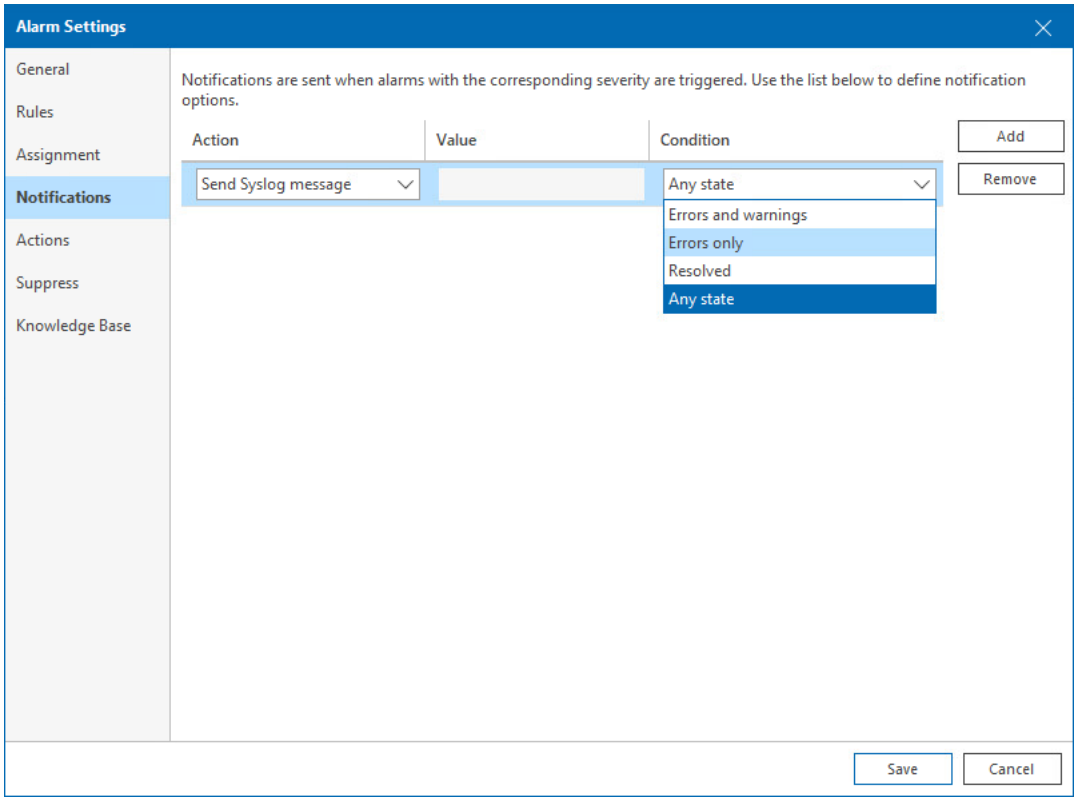
1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click **Alarm Management**.
3. To open the **Alarm Settings** window for the necessary alarm, do either of the following:
   - Double click the necessary alarm in the list.
   - Right-click the alarm and choose **Edit** from the shortcut menu.
   - Select the alarm in the list and click **Edit** in the **Actions** pane on the right.
4. In the **Alarm Settings** window, open the **Notifications** tab.
5. On the **Notifications** tab, click **Add**.
6. From the **Action** list, select **Send Syslog message**.
7. From the **Condition** list, choose the severity of alarms to send Syslog messages:
   - **Any state** — a Syslog message will be sent every time when an alarm status changes to *Error*, *Warning*, *Info* or *Resolved*.

- **Errors and warnings** — A Syslog message will be sent every time when an alarm status changes to *Error* or *Warning*.
- **Resolved** — A Syslog message will be sent every time when an alarm status changes to *Resolved*.
- **Errors only** — A Syslog message will be sent every time when an alarm status changes to *Error*.

8. Click **Save**.



Working with Triggered Alarms

You can perform the following actions with alarms that were triggered by Veeam ONE:

- View triggered alarms
- Resolve alarms
- Acknowledge alarms
- Approve alarm remediation action
- View alarm history
- Export triggered alarms

You can also work with alarms from the Veeam ONE Web Client Alarms Overview section.

Viewing Triggered Alarms

You can view alarms in both Veeam ONE Client and the Veeam ONE Web Client Alarms Overview screen.

Viewing alarms in Veeam ONE Web Client

To view alarms triggered for a specific infrastructure object:

1. Open Veeam ONE Web Client.

   For details, see Accessing Veeam ONE Components.

2. Open the **Alarms Overview** section.

3. At the bottom of the Alarms Overview, click on the necessary alarm in the Alarms list.

   For details on the Alarms Overview alarms list, see Alarms list.

Viewing alarms in Veeam ONE Client

To view alarms triggered for a specific infrastructure object:

1. Open Veeam ONE Client.

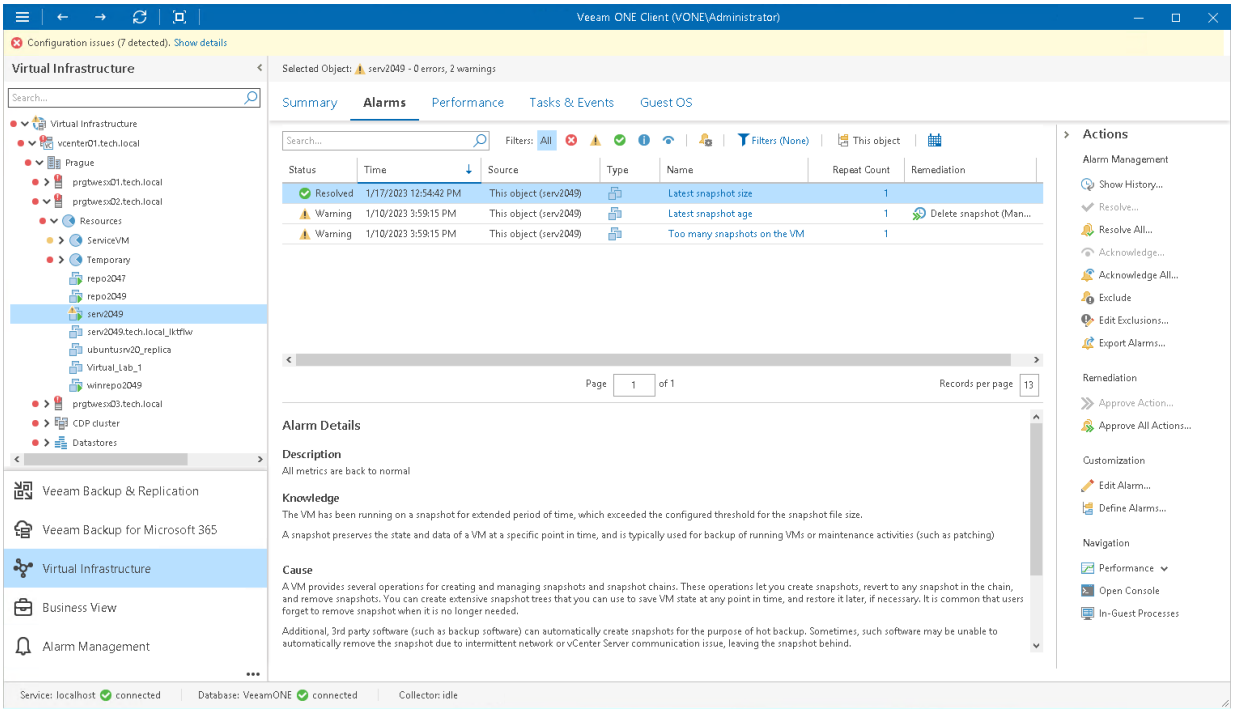
   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click the necessary view (*Veeam Backup & Replication*, *Veeam Backup for Microsoft 365*, *Virtual Infrastructure*, *VMware Cloud Director*, *Business View*).

3. In the inventory pane, select the necessary object.

4. In the information pane, open the **Alarms** tab.

The list of alarms shows alarms triggered for the selected infrastructure object and alarms for child objects.



For every alarm, the following details are available:

- **Status** – current status of the alarm (*Warning*, *Error*, *Resolved*, *Info* or *Acknowledged*). If an alarm was triggered multiple times, its latest state will be displayed in the list.
- **Time** – date and time when the alarm was triggered. If the alarm was triggered multiple times, the latest date time when the alarm was triggered will be displayed in the list.
- **Source** – name of the infrastructure object that caused the alarm. To view all alarms related to the infrastructure object, click the source link.
- **Type** – type of the infrastructure object that caused the alarm.
- **Name** – alarm name. Click the name link to open alarm details in the **Alarm Management** section.

  If the alarm has been already deleted and not available in the **Alarm Management** section, the alarm name is shown as plain text.
- **Repeat count** – the number of times the alarm was triggered or changed its status. Click the repeat count link to view the alarm history.

  For more details, see Viewing Alarm History.
- **Remediation** – remediation action and resolution type configured for an alarm.

  For more information on remediation actions, see Alarm Remediation Actions.

The **Alarm details** section of the information pane displays knowledge base for the selected alarm – description of the problem, possible causes, instructions for resolution, links to external resources, and other details.

The **Actions** pane on the right displays links to actions that you can perform against triggered alarms, as well as navigation links.

Searching for Alarms

To quickly find the necessary alarms, you can use filters and controls at the top of the **Alarms** list.



You can limit the list of alarms by the following criteria:

- To find alarms by alarm name, use the search field.
- To display or hide alarms with a specific severity, click the **Status** icons – *Show alarms with all statuses*, *Show alarms with status "Error"*, *Show alarms with status "Warning"*, *Show alarms with status "Resolved"*, *Show informational alarms,* and *Show alarms with status "Acknowledged"*.
- To display alarms with configured remediation actions, click the **Show alarms with available Remediation Actions** icon.
- To display or hide alarms for a specific type of infrastructure objects, click the object type icons – *Show alarms for all types of objects* or *Show [object type] alarms*.
- To display alarms that are related to the selected infrastructure object, use the **This object** icon. Release the icon to display alarms for the selected infrastructure object and alarms for its child objects. Press the icon to display alarms for the selected object only.
- To set the time interval within which alarms were triggered, use the **Filter alarms by time period** icon and set the necessary time interval. Release the icon to discard the time interval filter.

You can click column names to sort alarms by a specific parameter. For example, to view repetitive alarms, you can sort alarms in the list by **Repeat Count** in the descending order.

Resolving Alarms

Veeam ONE alarms can be resolved automatically or manually.

Alarms are resolved automatically in the following cases:

- When an alarm is disabled or deleted.
- When an object that caused the alarm is deleted or excluded from the alarm assignment scope.
- When conditions that caused the alarm are eliminated, and the alarm is configured to react to this (the alarm resolve action is automatic).

  For example, some alarms are configured to change the alarm severity to **Resolved** in specific cases or during events that occur in the managed infrastructure. Other alarms — such as alarms that are triggered when resource usage is above a certain threshold — are resolved automatically when the resource usage level is back to normal.

You can manually resolve alarms if the state of the monitored object is back to normal, or if the alarm requires no further investigation and no corrective actions should be taken.

Resolving Individual Alarms

You can resolve individual alarms in both Veeam ONE Client and Veeam ONE Web Client.

Resolving alarms in Veeam ONE Web Client

To resolve individual alarms in Veeam ONE Web Client:

1. Open Veeam ONE Web Client.

   For details, see Accessing Veeam ONE Components.
2. Open the **Alarms Overview** section.
3. In the alarm list at the bottom of the screen, click on your desired alarm.
4. On the alarm details window, click **Resolve**.
5. In the **Resolve Alarm** window, specify a reason for changing the alarm status, or provide any other additional information.
6. Click **OK**.

Resolving alarms in Veeam ONE Client

To resolve individual alarms in Veeam ONE Client:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.
2. At the bottom of the inventory pane, click the necessary view (*Veeam Backup & Replication*, *Veeam Backup for Microsoft 365*, *Virtual Infrastructure*, *VMware Cloud Director*, *Business View*).
3. In the inventory pane, select the necessary object.
4. In the information pane, open the **Alarms** tab.

5. In the list of alarms, select one or more alarms and do either of the following:
   - Right-click the selection and choose **Resolve** from the shortcut menu.
   - In the **Actions** pane, click **Resolve**.

   Press and hold the [CRTL] or [SHIFT] key to select multiple alarms.
6. In the **Resolve Alarm** window, specify a reason for changing the alarm status, or provide any other additional information.

   The message you specify will appear in the **Comment** field of the alarm history details, and in the email notification on resolved alarms. For details, see Viewing Alarm History and Notifications on Resolved Alarms.
7. Click **OK**.

Resolving Multiple Alarms

To resolve all displayed alarms at once:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.
2. At the bottom of the inventory pane, click the necessary view (*Veeam Backup & Replication*, *Veeam Backup for Microsoft 365*, *Virtual Infrastructure*, *VMware Cloud Director*, *Business View*).
3. In the inventory pane, select the necessary object.
4. In the information pane, open the **Alarms** tab.
5. Use the filters and the search field at the top of the list to display the alarms that you want to resolve.

   For details on alarm filters, see Searching for Alarms.
6. Do either of the following:
   - Right-click anywhere in the list of alarms and choose **Resolve all alarms** from the shortcut menu.
   - In the **Actions** pane, click **Resolve All**.
7. In the **Resolve All Alarms** window, specify a reason for changing the alarm status, or provide any other additional information.

   The message you specify will appear in the **Comment** field of the alarm history details, and in the email notification on resolved alarms. For details, see Viewing Alarm History and Notifications on Resolved Alarms.
8. Click **OK**.

Notifications on Resolved Alarms

When one or more alarms are resolved, Veeam ONE sends an email notification to users who monitor the affected object. The notification includes information about the number of alarms resolved, resolve action, time and reason, as well as the list of resolved alarms.

To receive notifications about resolved alarms, make sure that:

- You have configured SMTP server settings.

  For details, see Step 1. Configure SMTP Server Settings.

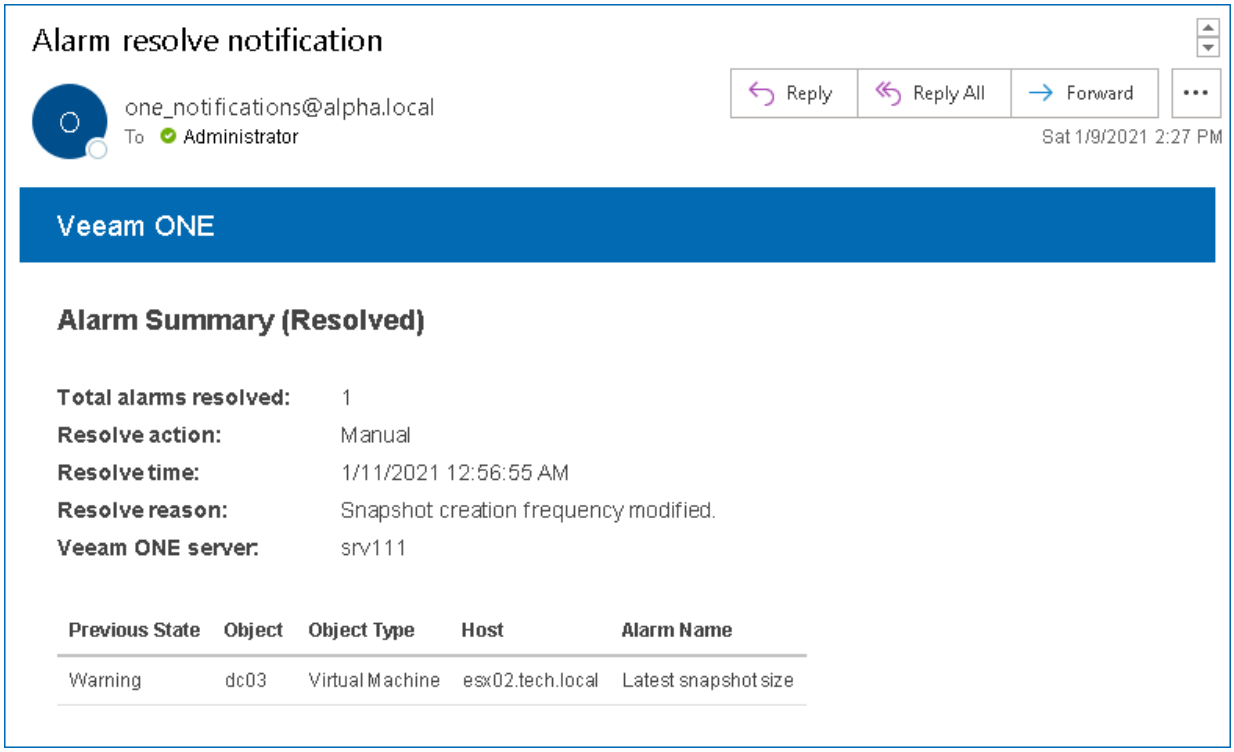
- Your email address is included either in the default notification group, or in the list of notification recipients specified in the alarm action settings, and the notification level is set to *Any state*.

  For details, see Step 4. Configure Email Recipients.

- Notifications about resolved and acknowledged alarms are enabled.

  For details, see Step 5. Configure Notifications About Resolved and Acknowledged Alarms.

The following image shows an example of a notification about a resolved alarm.



Acknowledging Alarms

By acknowledging an alarm you let other administrators know that an issue is being investigated or resolved, so no attention is required from their side.

You can acknowledge alarms that have the *Error* or *Warning* status. When you acknowledge an alarm, its status is changed to *Acknowledged*, and no response actions are performed on it. Additionally, Veeam ONE notifies users who monitor the affected object that the alarm is acknowledged.

Acknowledging Individual Alarms

You can acknowledge individual alarms in both Veeam ONE Client and the Veeam ONE Web Client Alarms Overview screen.

Acknowledging alarms in Veeam ONE Web Client

To acknowledge individual alarms in the Veeam ONE Web Client Alarms Overview:

1. Open Veeam ONE Web Client.

   For details, see Accessing Veeam ONE Components.
2. Open the **Alarms Overview** section.
3. In the alarm list at the bottom of the screen, click on your desired alarm.
4. On the alarm details window, click **Acknowledge**.
5. In the **Acknowledge Alarm** window, specify a comment or a reason for acknowledging the alarm.
6. Click **OK**.

Acknowledging alarms in Veeam ONE Client

To acknowledge individual alarms in Veeam ONE Client:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.
2. At the bottom of the inventory pane, click the necessary view (*Veeam Backup & Replication*, *Veeam Backup for Microsoft 365*, *Virtual Infrastructure*, *VMware Cloud Director*, *Business View*).
3. In the inventory pane, select the necessary object.
4. In the information pane, open the **Alarms** tab.
5. In the list of alarms, select one or more alarms and do either of the following:
   - Right-click the selection and choose **Acknowledge**.
   - In the **Actions** pane, click **Acknowledge**.

   Press and hold the `[CTRL]` or `[SHIFT]` key to select multiple alarms.

6. In the **Acknowledge Alarm** window, specify a comment or a reason for acknowledging the alarms.

   The message you specify will appear in the **Comment** field of the alarm history details, and in the email notification on acknowledged alarms. For details, see Viewing Alarm History and Notifications on Acknowledged Alarms.

7. Click **OK**.

Acknowledging Multiple Alarms

To acknowledge all displayed alarms at once:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click the necessary view (*Veeam Backup & Replication*, *Veeam Backup for Microsoft 365*, *Virtual Infrastructure*, *VMware Cloud Director*, *Business View*).

3. In the inventory pane, select the necessary object.

4. In the information pane, open the **Alarms** tab.

5. Use the filters and the search field at the top of the list to display the alarms that you want to acknowledge.

   For details on alarm filters, see Searching for Alarms.

6. Do either of the following:

   - Right-click anywhere in the list of alarms and choose **Acknowledge all alarms** from the shortcut menu.
   - In the **Actions** pane, click **Acknowledge All**.

7. In the **Acknowledge All Alarms** window, specify a reason for changing the alarm status, or add any other information.

   The message you specify will appear in the **Comment** field of the alarm history details, and in the email notification on acknowledged alarms. For details, see Viewing Alarm History and Notifications on Acknowledged Alarms.

8. Click **OK**.

Notifications on Acknowledged Alarms

When one or more alarms are acknowledged, Veeam ONE sends a notification to users who monitor the affected object. The notification includes information about the number of alarms acknowledged, time when the alarms were acknowledged and reason, as well as the list of acknowledged alarms.

To receive a notification about acknowledged alarms, make sure that:

- You have configured SMTP Server settings.

  For details, see Step 1. Configure SMTP Server Settings.

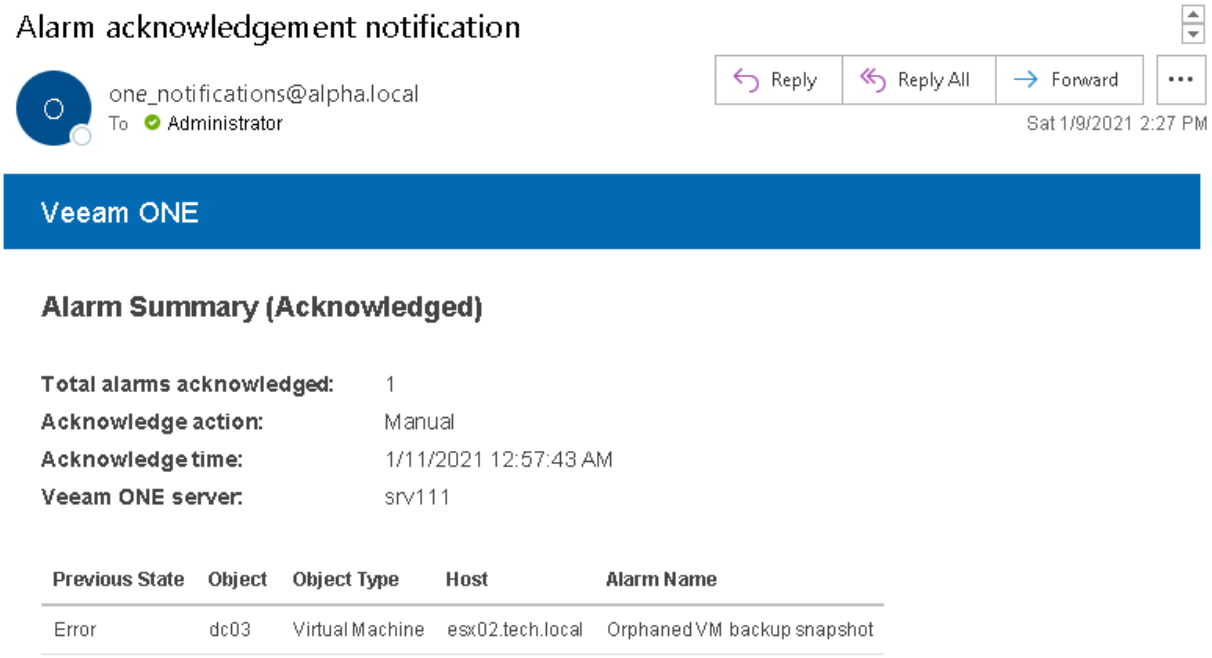
- Your email address is included either in the default notification group, or in the list of notification recipients specified in the alarm action settings, and the notification level is set to *Any state*.

  For details, see Step 4. Configure Email Recipients.

- Notifications about resolved and acknowledged alarms are enabled.

  For details, see Step 5. Configure Notifications About Resolved and Acknowledged Alarms.

The following image shows an example of a notification about acknowledged alarms.



Approving Alarm Remediation Actions

Veeam ONE can run alarm remediation actions automatically or after manual approval.

Veeam ONE runs an alarm action automatically if the resolution type of the alarm remediation action is set to *Automatic*. If the alarm remediation action requires manual approval, you can approve such actions in Veeam ONE Client.

Approving Actions for Individual Alarms

You can approve individual alarms in both Veeam ONE Client and the Veeam ONE Web Client Alarms Overview screen.

Approving actions for alarms in Veeam ONE Web Client

To approve individual alarms in the Veeam ONE Web Client Alarms Overview:

1. Open Veeam ONE Web Client.

   For details, see Accessing Veeam ONE Components.
2. Open the **Alarms Overview** section.
3. Click the Filters button at the top of the screen and click the **Only alarms with remediation** check box.
4. Click **Apply**.
5. In the filtered alarm list at the bottom of the screen, click on your desired alarm.
6. On the alarm details window, click **Approve Action**.
7. In the **Approve Action** window, specify a comment or a reason for approving the alarm.
8. Click **OK**.

Approving actions for alarms in Veeam ONE Client

To approve actions for individual alarms:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.
2. At the bottom of the inventory pane, click the necessary view (*Veeam Backup & Replication*, *Veeam Backup for Microsoft 365*, *Virtual Infrastructure*, *VMware Cloud Director*, *Business View*).
3. In the inventory pane, select the necessary object.
4. In the information pane, open the **Alarms** tab.
5. At the top of the alarms list, click the **Show alarms with available Remediation Actions** icon.
6. In the list of alarms, select one or more alarms and do either of the following:
   - Right-click the selection and choose **Approve action** from the shortcut menu.
   - In the **Actions** pane, click **Approve Action**.

   Press and hold the `[CRTL]` or `[SHIFT]` key to select multiple alarms.

7. In the **Approve Action** window, specify a reason or a comment for approving the alarm actions.

   The message you specify will appear in the **Comment** field of the alarm history details, and in the email notification on acknowledged alarms. For details, see Viewing Alarm History and Notifications on Acknowledged Alarms.

8. Click **OK**.

Approving Actions for Multiple Alarms

To approve actions for all displayed alarms at once:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click the necessary view (*Veeam Backup & Replication*, *Veeam Backup for Microsoft 365*, *Virtual Infrastructure*, *VMware Cloud Director*, *Business View*).

3. In the inventory pane, select the necessary object.

4. In the information pane, open the **Alarms** tab.

5. Use the filters and the search field at the top of the list to display the alarms for which you want to approve actions.

   For details on alarm filters, see Searching for Alarms.

6. Do either of the following:

   - Right-click anywhere in the list of alarms and choose **Approve all actions** from the shortcut menu.
   - In the **Actions** pane, click **Approve All Actions**.

7. In the **Approve All Actions** window, specify a reason or a comment for approving the alarm actions.

   The message you specify will appear in the **Comment** field of the alarm history details, and in the email notification on acknowledged alarms. For details, see Viewing Alarm History and Notifications on Acknowledged Alarms.

8. Click **OK**.

Viewing Alarm History

Veeam ONE keeps the history of alarm status changes for every triggered alarm. You can track the number of times the alarm changed its status and view alarm history details: assigned status, time, rule that triggered the alarm or changed its state, and comments for resolved, remediated, or acknowledged alarms.

To view alarm history:

1. Open Veeam ONE Client.

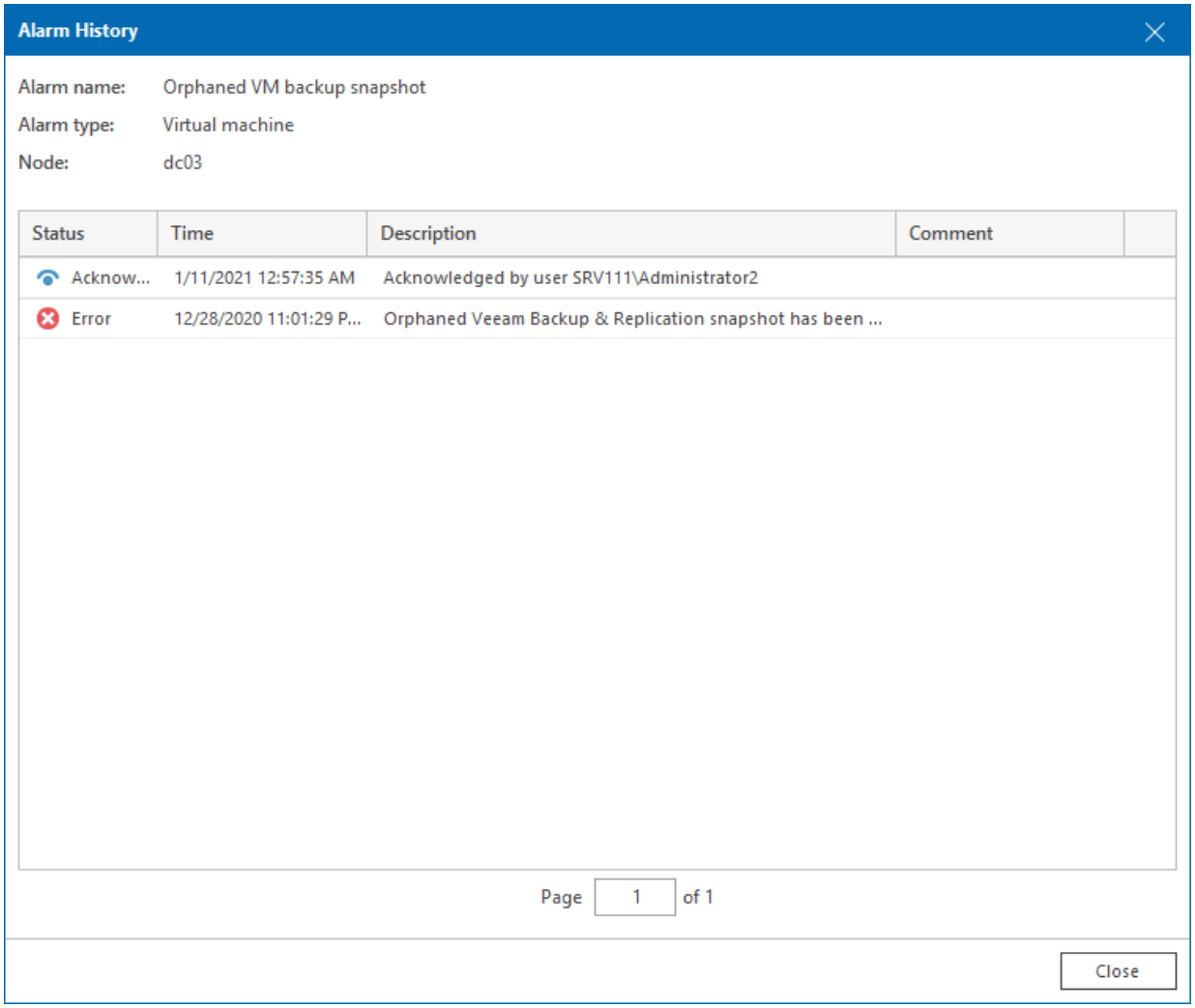
   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click the necessary view (*Veeam Backup & Replication*, *Veeam Backup for Microsoft 365*, *Virtual Infrastructure*, *VMware Cloud Director*, *Business View*).

3. In the information pane, open the **Alarms** tab.

4. Select the necessary alarm and do either of the following:

   - Click the **Repeat Count** link in the list of alarms.
   - Double-click the alarm in the list.
   - Right-click the alarm and select **Show History** from the shortcut menu.
   - In the **Actions** pane, click **Show History**.



Exporting Triggered Alarms

You can export information about triggered alarms to a CSV file. The file contains the following details for each exported alarm:

- Alarm status
- Alarm name
- Date and time when the alarm was triggered
- Name of the affected object
- Repeat count

To export one or more triggered alarms to a CSV file:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click the necessary view (*Veeam Backup & Replication*, *Veeam Backup for Microsoft 365*, *Virtual Infrastructure*, *VMware Cloud Director*, *Business View*).

3. In the inventory pane, select the necessary object.

4. In the information pane, open the **Alarms** tab.

5. Use the filters and the search field at the top of the list to display the alarms that you want to export.

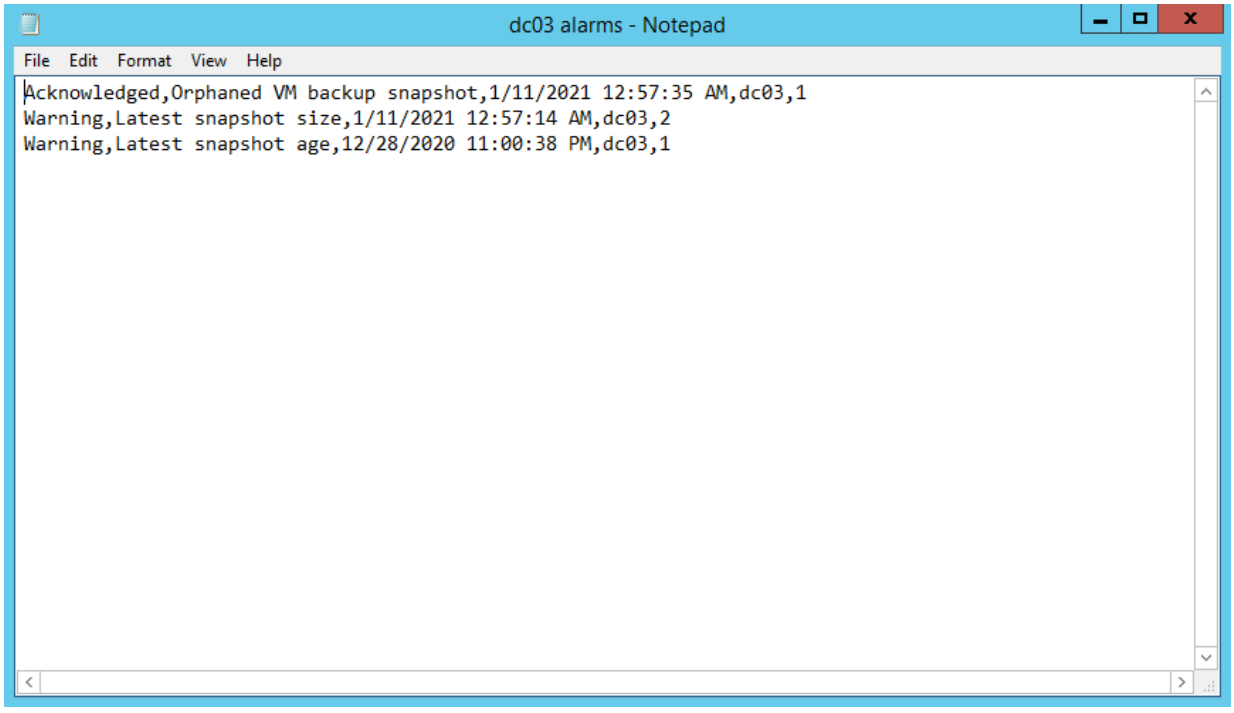
   For details on alarm filters, see Searching for Alarms.

6. In the **Actions** pane on the right, click **Export Alarms**.

7. Save the CSV file with exported data.

8. Click **OK**.

The following image shows an example of alarm details exported to a CSV file.



Working with Internal Alarms

In addition to alarms for monitoring the virtual and backup infrastructure, Veeam ONE includes a set of predefined alarms to monitor internal Veeam ONE problems — such as data collection, connection problems, or license issues. For the list and description of internal alarms, see Internal Alarms.

Viewing Internal Alarms

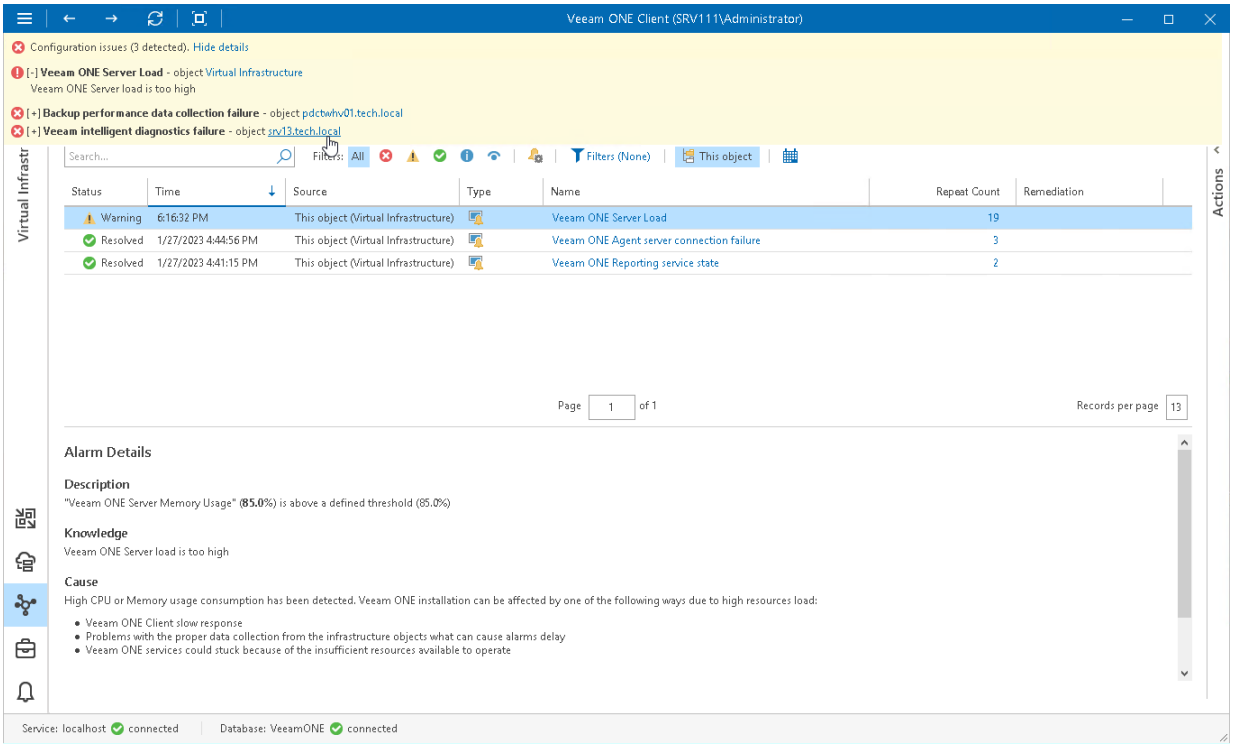
To view Veeam ONE internal alarms:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. In the **Configuration issues** pane, click the **Show details** link.

3. Click the object name to drill down to the list of alarms for the selected object.



Configuring Internal Alarms

You can configure internal alarms similarly to regular alarms:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Components.

2. At the bottom of the inventory pane, click **Alarm Management**.

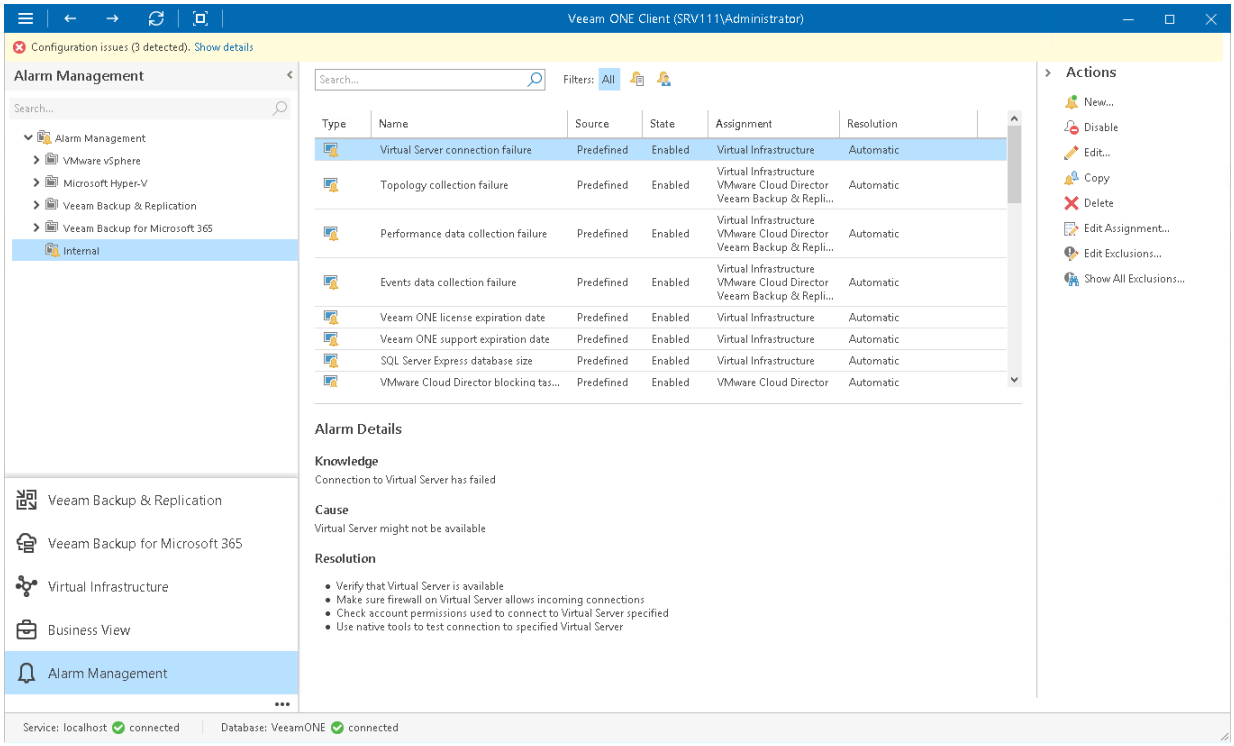
3. In the alarm management three, select the **Internal** node.

4. Select an alarm in the list and do either of the following:

   - Double click the alarm.
   - Right-click the alarm and choose **Edit** from the shortcut menu.
   - In the **Actions** pane, click **Edit**.

5. Change the necessary alarm settings.

   For details on working with alarm settings, see Creating Alarms.



Predefined Alarms

This section lists predefined Veeam ONE alarms.

Veeam Backup & Replication Alarms

This section describes predefined alarms for Veeam Backup & Replication infrastructure components.

Enterprise Manager

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Veeam Backup Enterprise Manager connection failure	State does not equal *Connected*.	Error	Automatic	Veeam ONE failed to connect to Veeam Backup Enterprise Manager.

Veeam Backup & Replication Server

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Agent backup job state	State of an agent backup job equals *Warning*.	Warning	Automatic	One or more computers failed to back up successfully.
	State of an agent backup job equals *Failed*.	Error		
Agent backup policy session state	State of a backup policy session equals *Warning*.	Warning	Automatic	One or more computers failed to back up successfully.
	State of a backup policy session equals *Failed*.	Error		
Application backup policy state	State of a backup policy session equals *Warning*.	Warning	Automatic	One or more application databases failed to back up successfully.
	State of a backup policy session equals *Failed*.	Error		

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Backup Copy Job exceeded data transfer window	Based on event VeeamBpCopyJobNetworkWindowExceededEvent.	Error	Manual	One or more backup copy jobs exceeded defined window, and data transfer between source and target backup repositories has been stopped.
Backup Copy job state	State of an backup copy job equals *Warning*.	Warning	Automatic	One or more objects could not be successfully copied from the backup repository.
	State of an backup copy job equals *Failed*.	Error		
Backup Copy RPO	Restore point copy is missing according to job schedule.	Error	Automatic	One or more backups was not successfully copied to the secondary repository within the defined RPO interval.
Backup Server Failed Logon Attempt	Based on event 44001 Veeam MP	Error	Manual	Authentication of Veeam Backup & Replication service failed during logon.
	Based on event 44002 Veeam MP	Error	Manual	
Backup Server Successful Logon	Based on event 44000 Veeam MP	Information	Automatic	Successful authorization attempt completed on Veeam Backup & Replication.
	44003 Veeam MP	Information	Automatic	

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Backup Server security & compliance state	Backup security & compliance state is not implemented.	Error	Automatic	Security & compliance check finished with warning or error.
	Backup security & compliance state is unable to detect.	Warning		
	Backup security & compliance state is not checked.	Warning		
Cloud instance RPO	No cloud instance protection type was created for more than 24 hours.	Warning	Automatic	No cloud instance protection type was created within the defined RPO interval.
Job disabled	Job is disabled for more than 12 hours.	Warning	Automatic	Job stays in the disabled state for a longer time than configured in the alarm threshold.
Backup job failed to create storage snapshot	Based on event VeeamBpJobFailedToCreateStorageSnapshotEvent.	Warning	Manual	Integrated storage failed to create storage snapshot initiated by Veeam backup job.
Backup job state	State of a backup job equals *Warning*.	Warning	Automatic	Backup job reported either an error or a warning.
	State of a backup job equals *Failed*.	Error		
	State of a Nutanix backup job equals *Warning*.	Warning		
	State of a Nutanix backup job equals *Failed*.	Error		
	SLA decreases to 95% for 5 minutes.	Warning		

Alarm Name	Event/Condition	Severity	Resolve Action	Description
CDP SLA Compliance	SLA decreases to 75% for 5 minutes.	Error	Automatic	SLA % of one or more workloads processed by CDP policy has dropped below threshold.
Cloud backup policy session state	Status of a cloud backup policy session equals *Warning*.	Warning	Automatic	Policy finished with warning or error.
	Status of a cloud backup policy session equals *Error*.	Error		
File backup job state	State of a file backup job equals *Warning.*	Warning	Automatic	File backup job finished with warning or error.
	State of a file backup job equals *Failed.*	Error		
File copy job state	State of a file copy job equals *Warning.*	Warning	Manual	One or more files failed to be transferred to the destination folder.
	State of a file copy job equals *Failed.*	Error		
Job exceeded backup window	Based on event VeeamBpJobWindowExceededEvent.	Error	Manual	One or more jobs exceeded allowed backup window and has been terminated.
License expiration date	Based on event VeeamBackupServerLicenseExpiration.	Warning	Automatic	Veeam Backup & Replication license expired.
	Based on event VeeamBackupServerLicenseChanged.	Resolve		
	Based on event VeeamBackupServerLicenseExpirationResolve.	Resolve		
	Job duration is more than 480 minutes.	Error	Manual	

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Maximum allowed job duration	Job duration is more than 120 minutes.	Warning		Job has exceeded its maximum allowed execution time.
Object storage backup job state	Object storage backup job equals *failed*.	Error	Automatic	One or more unstructured data items in the object storage backup were not successfully backed up.
	Object storage backup job equals *warning*.	Warning		
Potential malware in backups	One or more files detected as infected with malware.	Error	Automatic	One or more files with suspicious or infected malware detection.
	One or more files detected with potential suspicious malware infection.	Warning		
Plug-in backup data collection failure	Plug-in backup data collection failed due to connection loss for more than 5 minutes.	Error	Automatic	Veeam ONE server failed to collect plug-in backup data provided by Veeam Backup & Replication.
Quick Migration job state	Based on event VeeamBpQMigrationSessionWarningEvent.	Warning	Automatic	One or more VMs failed to migrate to another host.
	Based on event VeeamBpQMigrationSessionErrorEvent.	Error		
Replication job state	State of a replication job equals *Warning.*	Warning	Automatic	One or more VMs failed to replicate successfully.
	State of a replication job equals *Failed.*	Error		

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Restore activity	Based on event 290 Veeam MP.	Information	Automatic	Restore session initiated.
	Based on event 40290 Veeam MP.			
Support expiration date	Based on event VeeamBackupServerLicenseSupportExpiration.	Warning	Automatic	Veeam Backup & Replication prepaid support contract expired.
	Based on event VeeamBackupServerLicenseChanged.	Resolve		
	Based on event VeeamBackupServerLicenseSupportExpirationResolved.	Resolve		
SureBackup job state	State of a SureBackup job equals *Warning.*	Warning	Automatic	One or more VMs could not be successfully verified.
	State of a SureBackup job equals *Failed.*	Error		
Suspicious incremental backup size	One of 3 last job increment sizes is above 150% of configured threshold.	Warning	Automatic	The size of the recently created incremental restore point is significantly different from the previously created ones. For Oracle RMAN backup jobs, Veeam ONE analyzes only the differential level 1 backups.
	One of 3 last job increment sizes is above 200% of configured threshold.	Error		
	One of 3 last job increment sizes is below 80% of configured threshold.	Warning		
	One of 3 last job increment sizes is below 70% of configured threshold.	Error		
Tape job state	Status of the file to tape backup job equals *Warning.*	Warning	Manual	One or more VMs, computers or unstructured data items
	Status of the file to tape backup job equals *Failed.*	Error		

Alarm Name	Event/Condition	Severity	Resolve Action	Description
	Status of the backup to tape job equals *Warning.*	Warning		failed to be transferred to the tape device.
	Status of the backup to tape job equals *Failed.*	Error		
Database log backup job state	Microsoft SQL server log backup job completed with warning.	Warning	Automatic	Database transaction logs have not been backed up successfully.
	Microsoft SQL server log backup job failed.	Error		
	Oracle Database log backup job completed with warning.	Warning		
	Oracle Database log backup job failed.	Error		
	PostgreSQL log backup job completed with warning.	Warning		
	PostgreSQL log backup job failed.	Error		
	Enterprise application log backup job completed with warning.	Warning		
	Enterprise application log backup job failed.	Error		
Unusual job duration	Job duration is above 150% of average time interval.	Warning	Automatic	Job duration is above usual values among the set of job sessions.
	Job duration is above 200% of average time interval.	Error		
Veeam Backup & Replication HA cluster created	Based on event 43000 Veeam MP	Information	Automatic	High availability cluster was created.
Veeam Backup & Replication HA cluster disassembled	Based on event 43002 Veeam MP	Information	Automatic	High availability cluster was disassembled.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Veeam Backup & Replication HA cluster primary node state	Based on event VeeamBpHaClusterOfflineEvent	Error	Automatic	Primary node of high availability cluster stopped communicating with Veeam ONE.
	Based on event VeeamBpHaClusterOfflineResolvedEvent	Resolve	Automatic	Communication with primary node of high availability cluster successfully restored.
	Based on event VeeamMonitorServicesStarted	Resolve	Automatic	
Veeam Backup & Replication HA cluster secondary node state	Based on event 43003 Veeam MP	Error	Automatic	Veeam Backup & Replication HA secondary node state is offline.
	Based on event 43003 Veeam MP	Resolve	Automatic	Veeam Backup & Replication HA secondary node state is online.
Veeam Backup & Replication HA cluster failover state	Based on event 43004 Veeam MP	Information	Automatic	High availability cluster failover activity initiated.
Veeam Backup & Replication HA cluster switchover state	Based on event 43006 Veeam MP	Information	Automatic	High availability cluster switchover activity successfully completed.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Veeam Backup & Replication Server connection failure	State does not equal *Connected.*	Error	Automatic	Connection to Veeam Backup & Replication server failed.
Veeam Broker Service state	Based on event VeeamBackupServerBrokerServiceDownEvent.	Warning	Automatic	Veeam Broker Service that interacts with virtual infrastructure to collect and cache its topology is not started and not working properly.
	Based on event VeeamBackupServerBrokerServiceDownEvent.	Resolve		
	Based on event VeeamBackupServerBrokerServiceDownEvent.	Resolve		
Veeam malware detection activity state	Disabled malware detection.	Error	Automatic	This event is triggered when inline entropy or file system activity analysis settings are disabled.
Veeam malware detection exclusions change tracking	Based on event 42260 Veeam MP.	Error	Manual	A workload was added to or removed from the malware detection exclusions list.
	Based on event 42270 Veeam MP.	Error		
Veeam malware detection change tracking	Based on event VeeamMalwareInlineEntropyAnalysisEnabled.	Warning	Manual	Events are triggered when malware scan settings are changed.
	Based on event VeeamMalwareInlineEntropyAnalysisDisabled.	Warning		
	Based on event VeeamMalwareSensitivityDecreased.	Warning		

Alarm Name	Event/Condition	Severity	Resolve Action	Description
	Based on event VeeamMalwareSensitivityIncreased.	Warning		
	Based on event VeeamUpdateMalwareDefinitionsAutomaticallyDisabled.	Warning		
	Based on event VeeamUpdateMalwareDefinitionsAutomaticallyEnabled.	Warning		
	Based on event VeeamMalwareIncludedExtensionsListChanged.	Warning		
	Based on event VeeamMalwareExcludedExtensionsListChanged.	Warning		
	Based on event VeeamMalwareFileSystemActivityAnalysisDisabled.	Warning		
	Based on event VeeamMalwareFileSystemActivityAnalysisEnabled.	Warning		
VM Backup RPO (oVirt KVM, Proxmox VE, Nutanix AHV)	No VM backups were created for more than 24 hours.	Warning	Automatic	This VM has not been backed up within the defined RPO (Recovery Point Objective) interval.

Repository

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Backup repository connection failure	State equals *Not accessible* for more than 5 minutes.	Error	Automatic	Veeam Backup & Replication server

Alarm Name	Event/Condition	Severity	Resolve Action	Description
	State equals *Partially accessible* for more than 5 minutes.	Warning		lost connection to the Microsoft Windows backup repository.
Backup repository free space	Free space is below 5%.	Error	Automatic	Backup repository is low on free space.
	Free space is below 10%.	Warning		
Backup repository version is out-of-date	Component version mismatch.	Warning	Automatic	Veeam backup repository version does not match the version of Veeam Backup & Replication server.
Backup repository ReFS data integrity issue	Based on event 133 ReFS.	Warning	Manual	ReFS-formatted volume of a backup repository experienced a data integrity issue.
	Based on event 135 ReFS.			
	Based on event 136 ReFS.			
Immutability state	Immutability is disabled.	Warning	Automatic	The immutability setting is turned off on one or several backup repositories or scale-out backup repository extents.
Immutability change tracking	Based on event VeeamImmutabilityIntervalDaysDecreased.	Warning	Manual	The configured immutability period has been changed on one or several backup repositories or scale-out backup repository extents.
	Based on event VeeamImmutabilityIntervalDaysIncreased.			
	Based on event VeeamImmutabilityIntervalDaysEnabled.			

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Scale-out backup repository data transfer session state	Scale-out backup repository data transfer session completed with warning.	Warning	Automatic	Scale-out backup repository offload, download, archiving or retrieval data transfer session finished with warning or failed.
	Scale-out backup repository data transfer session failed.	Error		

Proxy

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Backup proxy connection failure	State does not equal *Accessible* for more than 5 minutes.	Error	Automatic	Veeam Backup & Replication server lost connection to the backup proxy server.
Backup proxy version is out-of-date	Component version mismatch.	Warning	Automatic	Veeam backup proxy version does not match the version of Veeam Backup & Replication server.
CDP proxy cache usage	CDP cache usage is above 50%	Warning	Automatic	CDP proxy cache usage has reached the configured threshold.
	CDP cache usage is above 75%	Error		

WAN Accelerator

Alarm Name	Event/Condition	Severity	Resolve Action	Description
WAN accelerator connection state	State does not equal *Accessible* for more than 5 minutes.	Error	Automatic	Veeam Backup & Replication server lost connection to the WAN accelerator

Alarm Name	Event/Condition	Severity	Resolve Action	Description
WAN accelerator version is out-of-date	Component version mismatch.	Warning	Automatic	Veeam WAN accelerator version does not match the version of Veeam Backup & Replication server.

Tape Server

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Tape server connection state	State does not equal *Accessible* for more than 5 minutes.	Error	Automatic	Veeam Backup & Replication server lost connection to the tape server.
Tape server version is out-of-date	Component version mismatch.	Warning	Automatic	Veeam tape server version does not match the version of Veeam Backup & Replication server.

Cloud Repository

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Cloud repository free space	Free space is below 10%.	Warning	Automatic	Cloud repository is low on available free space.
	Free space is below 5%.	Error		
Cloud repository lease expiration date	14 days to lease expiration.	Warning	Automatic	Cloud repository lease time is about to expire.
	0 days to lease expiration.	Error		
VM backups in cloud repository	Number of stored VMs is above the specified threshold.	Warning	Automatic	Number of VMs stored in the cloud repository is above the defined threshold.

Cloud Gateway

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Cloud gateway connection state	State does not equal *Accessible* for more than 5 minutes.	Error	Automatic	Veeam Backup & Replication server lost connection to the cloud gateway.
Cloud gateway version is out-of-date	Component version mismatch.	Warning	Automatic	Veeam cloud gateway version does not match the version of Veeam Backup & Replication server.

Computer

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Computer with no backup	No computer backups were created for more than 24 hours.	Warning	Automatic	This computer has not been backed up within the configured RPO (Recovery Point Objective) period.

Enterprise Application

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Application with no recent data backup sessions	No backup jobs protecting application database finished successfully or with warnings for more than 24 hours.	Warning	Automatic	One or several databases on an application server or application cluster are not protected with a backup job that finished successfully or with warnings within the configured RPO (Recovery Point Objective) period.

Intelligent Diagnostics

List of intelligent diagnostics alarms depends on the set of installed signatures. For details, see Veeam Intelligent Diagnostics.

Veeam Backup for Microsoft 365 Alarms

This section describes predefined alarms for Veeam Backup for Microsoft 365 infrastructure components.

Veeam Backup for Microsoft 365 Server

NOTE:

For the **Restore Activity (Veeam Backup for Microsoft 365)** alarm, Veeam ONE only collects information about restores from Veeam Backup for Microsoft 365 versions 8 and above. Restore data from versions below 8 is not presented in this alarm.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Backup copy job state (Veeam Backup for Microsoft 365)	State of a backup copy job equals *Warning*.	Warning	Automatic	Backup copy job reported either an error or a warning.
	State of a backup copy job equals *Failed*.	Error		
Backup job state (Veeam Backup for Microsoft 365)	State of a backup job equals *Warning*.	Warning	Automatic	Backup job reported either an error or a warning.
	State of a backup job equals *Failed*.	Error		
Job disabled (Veeam Backup for Microsoft 365)	Job is disabled for more than 12 hours.	Warning	Automatic	Job stays in the disabled state for a longer time than configured in the alarm threshold.
License exceeded for Veeam Backup for Microsoft 365	Based on event VeeamVbmServerLicenseCapacityDepleting.	Warning	Automatic	Number of protected user accounts exceeds the
	Based on event VeeamVbmServerLicenseCapacityDepletingResolved.	Resolve		

Alarm Name	Event/Condition	Severity	Resolve Action	Description
	Based on event VeeamMonitorServicesStartedEvent.	Resolve		license limit.
License expiration date (Veeam Backup for Microsoft 365)	Based on event VeeamVbmServerLicenseExpiration.	Warning	Automatic	Veeam Backup for Microsoft 365 license expired.
	Based on event VeeamVbmServerLicenseExpirationResolved.	Resolve		
	Based on event VeeamMonitorServicesStartedEvent.	Resolve		
Restore activity (Veeam Backup for Microsoft 365)	A restore operation of any type has been completed in the organization.	Information	Manual	A restore session has been performed on a Veeam Backup for Microsoft 365 server.
Organization with no backup	Microsoft 365 organization has no restore points created within the last 24 hours.	Warning	Automatic	Microsoft 365 organization was not backed up during the configured RPO period.
Unusual job duration (Veeam Backup for Microsoft 365)	Job duration is above 150% of average time interval.	Warning	Automatic	Job duration is above usual values among the set of job sessions.
	Job duration is above 200% of average time interval.	Error		
Veeam ONE server failed to connect to Microsoft 365 server	State does not equal *Connected* for more than 5 minutes.	Error	Automatic	Connection to Veeam Backup for Microsoft 365 server failed.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Veeam Backup for Microsoft 365 service state	Veeam Backup for Microsoft 365 service status does not equal *Running* for more than 5 minutes.	Error	Automatic	Veeam Backup for Microsoft 365 service is not running on the Veeam Backup for Microsoft 365 server.

Backup Proxy

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Backup proxy connection failure (Veeam Backup for Microsoft 365)	Backup proxy status does not equal *Online* for more than 5 minutes.	Error	Automatic	Veeam Backup for Microsoft 365 server lost connection to the proxy server.
Backup proxy maintenance mode state (Veeam Backup for Microsoft 365)	Backup proxy maintenance mode is enabled.	Warning	Automatic	Backup proxy maintenance mode is enabled.

Backup Repository

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Backup repository free space (Veeam Backup for Microsoft 365)	Free space is below 5%.	Error	Automatic	Backup repository is low on free space.
	Free space is below 10%.	Warning		
Immutability change tracking (Veeam Backup for Microsoft 365)	Based on event VeeamImmutabilityIntervalDaysDecreased.	Warning	Manual	The configured immutability period has been changed on one or several Veeam Backup for
	Based on event VeeamImmutabilityIntervalDaysIncreased.			

Alarm Name	Event/Condition	Severity	Resolve Action	Description
	Based on event VeeamImmutabilityIntervalDaysEnabled.			Microsoft 365 repositories.

VMware vSphere Alarms

This section describes predefined alarms for VMware vSphere infrastructure components.

vCenter Server

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Bad vCenter Server username logon attempt	Based on event BadUsernameSessionEvent.	Error	Manual	This event records a failed user logon. The combination of username, password, and permissions is the mechanism by which vCenter Server authenticate a user for access and authorize the user to perform activities.
Insufficient user access permissions	Based on event NoAccessUserEvent.	Error	Manual	This event records a failed user logon due to insufficient access permission.
Invalid license edition	Based on event InvalidEditionEvent.	Error	Manual	This event records if the license edition is set to an invalid value.
License expired	Based on event LicenseExpiredEvent.	Error	Manual	This event records the expiration of a license.
License file restricted	Based on event LicenseRestrictedEvent.	Error	Manual	This event records if the required licenses could not be reserved because of a restriction in the option file.
License is not compliant	Based on event LicenseNonComplianceEvent.	Error	Manual	This event records that the inventory is not license compliant.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Maximum host connections reached	Based on event HostInventoryFullEvent.	Error	Manual	This event records if the inventory of hosts has reached capacity.
No license reservation	Based on event NoLicenseEvent.	Error	Manual	These are events reported by License Manager. A NoLicenseEvent is reported if the required licenses could not be reserved. Each feature that is not fully licensed is reported.
Non VI workload detected	Based on event NonVIWorkloadDetectedOnDatastoreEvent.	Error	Manual	A potential misconfiguration or I/O performance issue caused by a non-ESX workload has been detected. This alarm is triggered when Storage I/O Control (SIOC) detects that a workload that is not managed by SIOC is contributing to I/O congestion on a datastore that is managed by SIOC.
vCenter Server agent uninstall failure	Based on event VcAgentUninstallFailedEvent.	Error	Manual	This event records when the vCenter Server agent on a host failed to uninstall.
vCenter Server agent upgrade failure	Based on event VcAgentUpgradeFailedEvent.	Error	Manual	This event records when the vCenter Server agent on a host failed to upgrade.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
vCenter Server license expired	Based on event ServerLicenseExpiredEvent.	Error	Manual	This event records an expired vCenter Server license.

Cluster

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Admission control disabled	Based on event DasAdmissionControlDisabledEvent.	Information	Automatic	This event records when admission control checks have been disabled in a HA cluster.
Admission control enabled	Based on event DasAdmissionControlEnabledEvent.	Information	Automatic	This event records when admission control checks have been enabled in a HA cluster.
All hosts in cluster isolated	Based on event DasClusterIsolatedEvent.	Error	Manual	This event records that all hosts have been isolated from the network in a HA cluster.
DRS invocation failure	Based on event DrsInvocationFailedEvent.	Error	Manual	This event records DRS invocation failure. DRS invocation not completed.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
HA disabled for cluster	Based on event DasDisabledEvent.	Information	Automatic	This event records when a cluster has been disabled for HA.
HA enabled for cluster	Based on event DasEnabledEvent.	Information	Automatic	This event records when a cluster has been enabled for HA.
Host cluster capacity overcommitted	Based on event ClusterOvercommittedEvent.	Error	Manual	This event records when a cluster's host capacity cannot satisfy resource configuration constraints.
vSphere cluster warning	Based on event com.vmware.vc.HA.ClusterContainsIncompatibleHosts.	Warning	Manual	One of the hosts in an HA cluster has been isolated.
	Based on event com.vmware.vc.HA.DasFailoverHostIsolatedEvent.			
	Based on event com.vmware.vc.HA.DasFailoverHostPartitionedEvent.			
	Based on event com.vmware.vc.HA.DasFailoverHostUnreachableEvent.			
	Based on event com.vmware.vc.HA.DasHostIsolatedEvent.			

Host

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Bad Host username logon attempt	Based on event BadUsernameSessionEvent.	Warning	Manual	This event records a failed user logon. The combination of username, password, and permissions is the mechanism by which hosts authenticate a user for access and authorize the user to perform activities.
Connection to iSCSI storage target failure	Based on event esx.problem.storage.iscsi.discovery.connect.error.	Error	Manual	The iSCSI initiator is unable to establish a connection to the target.
	Based on event esx.problem.storage.iscsi.discovery.login.error.			
	Based on event esx.problem.storage.iscsi.target.connect.error.			
	Based on event esx.problem.storage.iscsi.target.login.error.			
DPM failed to bring host out of standby mode	Based on event DrsExitStandbyModeFailedEvent.	Error	Automatic	This event records that Distributed Power Management tried to bring a host out of standby mode, but failed. Standby Mode powers off a host and allows it to be powered back on again through the Wake-on-LAN protocol. It can be triggered either manually or automatically by vCenter Server.
	Based on event DrsExitedStandbyMode.	Resolve		
	Based on event ExitedStandbyMode.	Resolve		
DRS host standby mode entrance	Based on event DrsEnteredStandbyModeEvent.	Information	Automatic	This event records that the host has successfully entered standby mode initiated by Distributed Power Management. A host in this mode has no running virtual machines and no provisioning operations are occurring.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
DRS host standby mode exit	Based on event DrsExitedStandbyModeEvent.	Information	Automatic	This event records that Distributed Power Management brings this host out from standby mode.
DRS synchronization failure	Based on event DrsResourceConfigureFailedEvent.	Error	Manual	This event records when resource configuration specification synchronization fails on a host.
DVS host configuration out of sync	Based on event OutOfSyncDvsHost.	Warning	Manual	The list of hosts that have the DVS configuration on the host diverged from that of the vCenter Server.
ESXi host network uplink failure	Based on event esx.problem.net.lacp.uplink.fail.duplex.	Error	Manual	Link Aggregation Control Protocol (LACP) is included in IEEE specification as a method to control the bundling of several physical ports together to form a single logical channel. LACP allows a network device to negotiate an automatic bundling of links by sending LACP packets to the peer (directly connected device that also implements LACP).
	Based on event esx.problem.net.lacp.uplink.fail.speed.			
	Based on event esx.problem.net.lacp.uplink.inactive.			
ESXi host CPU hardware error	Based on event esx.problem.cpu.amd.mce.dram.disabled.	Error	Manual	ESXi host has experienced a CPU hardware error.
	Based on event esx.problem.cpu.intel.ioapic.listing.error.			
	Based on event esx.problem.cpu.mce.invalid.			
	Based on event esx.problem.cpu.smp.ht.invalid.			
	Based on event esx.problem.cpu.smp.ht.numpcpus.max.			

Alarm Name	Event/Condition	Severity	Resolve Action	Description
ESXi host network error	Based on event esx.problem.dhclient.lease.none.	Error	Manual	DHCP client lease issue has been detected.
ESXi host network uplink problems	Based on event esx.problem.net.lacp.uplink.blocked.	Warning	Manual	Link Aggregation Control Protocol (LACP) is included in IEEE specification as a method to control the bundling of several physical ports together to form a single logical channel. LACP allows a network device to negotiate an automatic bundling of links by sending LACP packets to the peer (directly connected device that also implements LACP).
	Based on event esx.problem.net.lacp.uplink.disconnected.			
ESXi host network warning	Based on event esx.problem.dhclient.lease.offered.error.	Warning	Manual	DHCP client lease issue has been detected.
	Based on event esx.problem.dhclient.lease.persistent.none.			
ESXi host storage error	Based on event esx.problem.scsi.device.state.permanentloss.withreservationheld.	Error	Manual	Storage device becomes permanently lost while SCSI reservation is held by ESXi.
ESXi host storage failure	Based on event esx.problem.visorfs.failure.	Error	Manual	An operation on the root file system has failed.
ESXi host storage warning	Based on event esx.problem.visorfs.inodetable.full.	Warning	Manual	One of the host's ramdisks reached the limit for the number of files it can contain.
	Based on event esx.problem.visorfs.ramdisk.full.	Warning		
	Average memory usage is for 15 minutes is above 80%.	Warning	Automatic	This host is low on available memory.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Host available memory	Average memory usage is for 15 minutes is above 90%.	Error		
Host connection failure	Host state equals *Disconnected* for 5 minutes and more.	Warning	Automatic	This alarm monitors the VMware vCenter Server API for events indicating that a host is disconnected.
	Host state equals *Not responding* for 5 minutes and more.			
Host connectivity failure	Based on event vprob.net.connectivity.lost.	Error	Automatic	This event indicates that one or more portgroups in the host have lost connectivity to the network, resulting in unavailability of all physical connections to the network from this switch.
	Based on event esx.problem.net.connectivity.lost.			
	Based on event esx.clear.net.connectivity.restored.	Resolve		
Host CPU ready	Average CPU Ready for 15 minutes is above 15%.	Warning	Automatic	This Host has exceeded the threshold for CPU Ready Percent.
	Average CPU Ready for 15 minutes is above 25%.	Error		
Host CPU usage	Average CPU usage for 15 minutes is above 75%.	Warning	Automatic	This host has exceeded the threshold for CPU usage.
	Average CPU usage for 15 minutes is above 95%.	Error		
Host disk bus resets	Average datastore bus resets for 15 minutes is above 2.	Warning	Automatic	This host disk (vmhba) has logged one or more SCSI bus resets.
	Average datastore bus resets for 15 minutes is above 4.	Error		
	Average datastore command aborts for 15 minutes is above 2.	Warning	Automatic	This host disk (vmhba) has logged one or more SCSI aborts.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Host disk SCSI aborts	Average datastore command aborts for 15 minutes is above 4.	Error		
Host failed to exit standby mode	Based on event ExitStandbyModeFailedEvent.	Error	Automatic	This event records that the host failed to exit standby mode. Standby Mode powers off a host and allows it to be powered back on again through the Wake-on-LAN protocol. It can be triggered either manually or automatically by vCenter Server.
	Based on event ExitedStandbyMode.	Resolve		
Host HA agent failure	Based on event com.vmware.vc.HA.HostAgentErrorEvent.	Error	Manual	Usually, such triggers indicate that a host has actually failed, but failure reports can sometimes be incorrect. A failed host reduces the available capacity in the cluster and, in the case of an incorrect report, prevents vSphere HA from protecting the virtual machines running on the host.
Host HA disabled	Based on event HostDasDisabledEvent.	Information	Automatic	This event records when HA has been disabled on a host.
Host HA enabled	Based on event HostDasEnabledEvent.	Information	Automatic	This event records when the HA (high-availability) agent has been enabled on a host.
Host hardware status	Hardware sensor equals *Warning.*	Warning	Automatic	One of the hosts' hardware sensors has changed its status.
	Hardware sensor equals *Alert.*	Error		
	Hardware sensor equals *Unknown.*	Warning		
Host IP inconsistent	Based on event HostIpInconsistentEvent.	Warning	Manual	This event records that the IP address resolution returned different addresses on the host.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Host IP to short name failed	Based on event HostIpToShortNameFailedEvent.	Warning	Manual	This event records that the host's IP address could not be resolved to a short name.
Host Isolation IP not available	Based on event HostIsolationIpPingFailedEvent.	Warning	Manual	This event records that the isolation address could not be pinged. The default isolation address is the service console's default gateway.
Host license expired	Based on event HostLicenseExpiredEvent.	Error	Manual	This event records an expired host license.
Host memory pressure	Average memory pressure for 15 minutes is above 150%.	Warning	Automatic	This host has exceeded the threshold for memory pressure.
	Average memory pressure for 15 minutes is above 250%.	Error		
Host NIC link status	Host NIC link status equals *Down.*	Error	Automatic	Physical NIC linkstate is down.
Host not compliant	Based on event HostNonCompliantEvent.	Warning	Manual	This event records that host went out of compliance.
Host operation cancelled	Based on event CanceledHostOperationEvent.	Information	Automatic	An operation performed on the host was canceled.
Host operation timed out	Based on event TimedOutHostOperationEvent.	Warning	Manual	This event indicates that an operation performed on the host timed out.
Host primary agent not in short name	Based on event HostPrimaryAgentNotShortNameEvent.	Warning	Manual	This event records that the primary agent specified is not a short name.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Host reconnection failed	Based on event HostConnectedEvent.	Resolve	Automatic	This event records a failed attempt to re-establish a host connection.
	Based on event HostReconnectionFailedEvent.	Error		
Host redundancy failure	Based on event vprob.net.redundancy.lost.	Warning	Automatic	The event indicates that one or more portgroups in the host has lost a redundant uplink to the physical network. Portgroups are still connected. However this may be the last redundant uplink. Check the event description and context to confirm the status.
	Based on event vprob.net.redundancy.degraded.			
	Based on event esx.problem.net.redundancy.lost.			
	Based on event esx.problem.net.redundancy.degraded.			
	Based on event esx.clear.net.redundancy.restored.	Resolve		
Host short name inconsistent	Based on event HostShortNameInconsistentEvent.	Warning	Manual	This event records that host name resolution returned different names on the host.
Host short name IP resolve failed	Based on event HostShortNameToIpFailedEvent.	Warning	Manual	This event records that the host's short name could not be resolved to an IP address.
Host swap memory	Average memory swap used for 15 minutes is above 64 MB.	Warning	Automatic	This host is swapping too much memory.
	Average memory swap used for 15 minutes is above 128 MB.	Error		

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Host synchronization failed	Based on event HostSyncFailedEvent.	Warning	Manual	This event records a failure to sync up with the vCenter Server agent on the host.
Host upgrade connection failure	Based on event HostUpgradeFailedEvent.	Error	Manual	This event records a failure to connect to a host due to an installation or upgrade issue.
Incorrect host information	Based on event IncorrectHostInformationEvent.	Warning	Manual	This event records if the host did not provide the information needed to acquire the correct set of licenses.
iSCSI target storage connection failure	Based on event esx.problem.storage.iscsi.target.connected.error.	Error	Manual	The iSCSI initiator is unable to establish a connection to the target.
iSCSI targets are permanently removed from ESXi	Based on event esx.problem.storage.iscsi.target.permanently.lost.	Error	Manual	The esx.problem.storage.iscsi.target.permanently.removed message is received when an iSCSI target is no longer presented to ESXi.
Isolation addresses is missing	Based on event com.vmware.vc.HA.HostHasNoIsolationAddrsDefined.	Warning	Manual	ESXi host is missing isolation addresses for isolation detection.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Network rollback detected	Based on event NetworkRollbackEvent.	Error	Manual	In vSphere 5.1, rollback is enabled by default. However, you can enable or disable rollbacks at the vCenter Server level. Several networking events can trigger a rollback. The events are grouped into these categories: • Host networking rollbacks (virtual switches or network system) • Distributed switch rollbacks
No host network for HA available	Based on event HostNoAvailableNetworksEvent.	Warning	Manual	This event records the fact that a host does not have any available networks for HA communication.
Non VI workload detected on host	Based on event EsxProblemIormNonViWorkload.	Error	Manual	A potential misconfiguration or I/O performance issue caused by a non-ESX workload has been detected. This alarm is triggered when Storage I/O Control (SIOC) detects that a workload that is not managed by SIOC is contributing to I/O congestion on a datastore that is managed by SIOC.
SCSI unsupported plugin warning	Based on event esx.problem.scsi.unsupported.plugin.type.	Warning	Manual	An invalid storage module attempted to configure a SCSI device.
Storage connection failure	Based on event vprob.storage.connectivity.lost.	Error	Automatic	The event indicates a loss in connectivity to the specified storage device. The path indicated is the last path that went down.
	Based on event esx.problem.storage.connectivity.lost.			
	Based on event esx.clear.storage.connectivity.restored.	Resolve		

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Storage connection redundancy failure	Based on event vprob.storage.redundancy.lost.	Warning	Automatic	A host has lost a path to access the specified storage and the path to storage is either degraded, or no longer redundant. Check the event description and context to confirm the status.
	Based on event vprob.storage.redundancy.degraded.			
	Based on event esx.problem.storage.redundancy.degraded.			
	Based on event esx.problem.storage.redundancy.lost.			
	Based on event esx.clear.storage.redundancy.restored.	Resolve		
Teaming mismatch error	Based on event TeamingMisMatchEvent.	Error	Manual	The teaming configuration of the uplink ports in the DVS does not match physical switch configuration.
Uplink port MTU error	Based on event UplinkPortMtuNotSupportEvent.	Error	Manual	MTU health check status of an uplink port is changed.
Uplink port VLAN error	Based on event UplinkPortVlanUntrunkedEvent.	Error	Manual	Vlans health check status of an uplink port is changed.
vCenter Server lost connection to host	Based on event HostConnectionLostEvent.	Error	Automatic	vCenter Server has lost connection to this host.
	Based on event HostCnxFailed.			
	Based on event HostConnectedEvent.	Resolve		

Alarm Name	Event/Condition	Severity	Resolve Action	Description
vMotion license expired	Based on event VMotionLicenseExpiredEvent.	Error	Manual	This event records an expired vMotion license.
vSphere Distributed Switch MTU mismatch	Based on event MtuMismatchEvent.	Error	Manual	A larger MTU (maximum transmission unit) bring greater efficiency because each packet carries more user data while protocol overheads; the resulting higher efficiency means a slight improvement in bulk protocol throughput. A larger MTU also means processing of fewer packets for the same amount of data. However, this gain is not without some downside. Large packets can occupy a slow link for some time, causing greater delays to following packets and increasing lag and minimum latency.

Virtual Machine

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Customization unknown failure	Based on event CustomizationUnknownFailure.	Warning	Manual	The customization sequence failed unexpectedly in the guest.
Fault Tolerance VM terminated	Based on event VmFaultToleranceVmTerminatedEvent.	Warning	Manual	This event records a secondary or primary VM is terminated.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
FT VM Failover	Based on event VmPrimaryFailoverEvent.	Error	Manual	This event records a fault tolerance failover.
Guest customization failure	Based on event CustomizationFailed.	Warning	Manual	The customization sequence in the guest failed. Cannot complete customization of VM.
Guest disk space	Guest disk free space space is below 10%.	Warning	Automatic	Guest OS volume is low on available guest disk space.
	Guest disk free space space is below 5%.	Error		
HA agent update failed	Based on event VmDasUpdateErrorEvent.	Error	Manual	The event records an error occurred when updating the HA agents with the current state of the VM.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Heartbeat is missing for VM	Heartbeat not detected for 15 minutes.	Error	Automatic	The heartbeat is the communication to the VMware tools heartbeat running inside the VM. Heartbeat can only be monitored when the VMware tools are installed in a VM. The heartbeat is what vCenter Server uses to determine the general health and availability of a running VM.
High balloon memory utilization	Average memory balloon percent for 15 minutes is above 10%.	Warning	Automatic	There is high utilization of the VMware Tools memory controller, also known as the 'balloon driver', within this VM.
	Average memory balloon percent for 15 minutes is above 50%.	Error		
High memory usage	Average memory usage for 15 minutes is above 90%.	Warning	Automatic	There is high utilization of

Alarm Name	Event/Condition	Severity	Resolve Action	Description
	Average memory usage for 15 minutes is above 95%.	Error		memory within this Virtual Machine. The memory active metric is the current percentage of memory active vs. memory maximum for this VM.
Latest snapshot age	VM snapshot age is 48 hour or more.	Warning	Automatic	The age of the latest snapshot for this VM has exceeded the configured threshold.
Latest snapshot size	VM snapshot size is above 10%.	Warning	Automatic	The size of the latest snapshot file for this VM has exceeded the configured threshold.
	VM snapshot size is above 20%.	Error		
Linux customization identity failure	Based on event CustomizationLinuxIdentityFailed.	Warning	Manual	Failed to set Linux identity.
Potential infrastructure malware activity	Potential malware activity is infected	Error	Automatic	Veeam Backup & Replication server has detected potential malware activity.
	Potential malware activity is suspicious	Warning		

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Network customization setup failure	Based on event CustomizationNetworkSetupFailed.	Warning	Manual	Network setup failed in the guest during customizatio n.
No compatible host for Secondary VM	Based on event VmNoCompatibleHostForSecondaryEvent.	Warning	Manual	This event records that no compatible host was found to place a secondary VM. A default alarm will be triggered upon this event, which by default, triggers a SNMP trap.
No host for a virtual machine available	Based on event VmOrphanedEvent.	Warning	Manual	This event records a VM for which no host is responsible.
No maintenance mode DRS recommendati on for VM	Based on event NoMaintenanceModeDrsRecommendationForVM.	Warning	Manual	This event records that DRS did not recommend a migration for a powered on VM, even though its host is going into maintenance mode.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
No network access for VM migration	Based on event VmNoNetworkAccessEvent.	Warning	Manual	This event records a migration failure when the destination host is not on the same network as the source host.
Not enough resources for failover	Based on event NotEnoughResourcesToStartVmEvent.	Warning	Manual	This event records when the HA does not find sufficient resources to failover a VM.
Orphaned VM backup snapshot	Orphaned VM backup snapshot age is 60 minutes or more.	Error	Automatic	This VM is running on the snapshot left by backup or replication job.
Possible ransomware activity	Average CPU Usage is above 70% and Datastore Write Rate is above 40 MB/s or Network Transmit Rate is above 40 MB/s for 5 minutes.	Warning	Automatic	Veeam ONE detected suspicious activity on this VM.
	Average CPU Usage is above 80% and Datastore Write Rate is above 60 MB/s or Network Transmit Rate is above 60 MB/s for 5 minutes.	Error		

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Secondary VM config update failed	Based on event VmFailedUpdatingSecondaryConfig.	Warning	Manual	This event is recorded after a failover of the new primary VM failed to update the config of the secondary VM.
Secondary VM failed to start	Based on event VmFailedStartingSecondaryEvent.	Warning	Manual	The Secondary VM cannot be powered on as there are no compatible hosts that can accommodate it.
Secondary VM start timeout	Based on event VmTimedoutStartingSecondaryEvent.	Warning	Manual	This event records timeout when starting a secondary VM.
Sysprep customization failure	Based on event CustomizationSysprepFailed.	Warning	Manual	Sysprep failed to run in the guest during customization. This can be caused by the fact that the wrong sysprep was used for the guest or errors in the sysprep file.
	Number of VM snapshots is 3 or more.	Warning		

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Too many snapshots on the VM	Number of VM snapshots is 5 or more.	Error	Automatic	An excessive number of snapshots in a chain has been detected on the VM which may lead to decreased virtual machine and host performance.
Virtual disk creation failed	Based on event VmDiskFailedEvent.	Error	Manual	This event records a failure to create a virtual disk in a VM.
VM clone operation failure	Based on event VmCloneFailedEvent.	Error	Manual	This event records a failure to clone a VM.
VM configuration file missing	Based on event VmConfigMissingEvent.	Warning	Manual	This event records if the configuration file (VMX file) for a VM cannot be found.
VM connection failure	Based on event VmDisconnectedEvent.	Error	Automatic	This VM is 'Disconnected' in vCenter Server.
	Based on event VmConnectedEvent.	Resolve		
VM consolidation needed status	Based on event com.vmware.vc.VmDiskConsolidationNeeded.	Error	Automatic	When initiating Delete or DeleteAll operations on snapshots, the snapshot
	Based on event com.vmware.vc.VmDiskConsolidationNoLongerNeeded.	Resolve		

Alarm Name	Event/Condition	Severity	Resolve Action	Description
	Based on event com.vmware.vc.VmDiskConsolidatedEvent.	Resolve		details are deleted from Snapshot Manager, then the snapshot files are consolidated and merged to another snapshot file or to the virtual machine parent disk. If the consolidation fails, there were no snapshots shown in the Snapshot Manager, but the snapshot files were still being used on the datastore. This can cause the datastore to run out of space.
VM CPU ready	Average CPU ready all cores metric for 15 minutes is above 10%.	Warning	Automatic	This VM has exceeded the threshold for CPU Ready Percent.
	Average CPU ready all cores metric for 15 minutes is above 20%.	Error		
VM CPU usage	Average CPU usage for 15 minutes is above 75%.	Warning	Automatic	This VM has exceeded the threshold for CPU usage.
	Average CPU usage for 15 minutes is above 90%.	Error		
VM disk consolidation failure	Based on event com.vmware.vc.VmDiskFailedToConsolidateEvent.	Error	Automatic	There is an issue with the disk for

Alarm Name	Event/Condition	Severity	Resolve Action	Description
	Based on event com.vmware.vc.VmDiskConsolidatedEvent.	Resolve		this virtual machine.
VM disk SCSI connection failures	Average number of datastore command aborts for 15 minutes is above 2.	Warning	Automatic	This VMGuest disk connection (LUN) has logged one or more SCSI aborts.
	Average number of datastore command aborts for 15 minutes is above 6.	Error		
VM disk SCSI connection resets	Average number of datastore bus resets for 15 minutes is above 2.	Warning	Automatic	This VMGuest disk connection (LUN) has logged one or more SCSI bus resets.
	Average number of datastore bus resets for 15 minutes is above 6.	Error		
VM generic error	Based on event VmMessageErrorEvent.	Error	Manual	This is a generic event for error messages from a VM that do not fit into any other specific vCenter Server event.
VM generic warning	Based on event VmMessageWarningEvent.	Warning	Manual	This is a generic event for warning messages from a VM that did not fit into any other specific vCenter Server event.
VM guest reboot	Based on event VmGuestRebootEvent.	Information	Automatic	This is a VM guest reboot request event.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
VM guest shutdown	Based on event VmGuestShutdownEvent.	Information	Automatic	This is a VM guest shutdown request event.
VM HA error	Based on event com.vmware.vc.HA.FailedRestartAfterIsolationEvent.	Error	Manual	vSphere HA has failed to restart after a host isolation.
VM HA reset	Based on event VmDasBeingResetEvent.	Warning	Manual	This event records when a VM is reset by HA VM Health Monitoring on hosts that do not support the create screenshot APIi or if the create screenshot API fails.
VM HA reset failure	Based on event VmDasResetFailedEvent.	Warning	Manual	This event records when HA VM health monitoring fails to reset a VM after failure.
VM memory swap usage	Average memory swapped for 15 minutes is above 64 MB.	Warning	Automatic	This VM has exceeded the threshold for memory swapping to disk within the host.
	Average memory swapped for 15 minutes is above 128 MB.	Error		

Alarm Name	Event/Condition	Severity	Resolve Action	Description
VM power status	State not equals *Running* for 5 minutes or more.	Error	Automatic	The power state of a VM indicates whether the VM is active and functional.
VM resetting	Based on event VmResettingEvent.	Information	Automatic	This event records a VM resetting.
VM restart on alternate host	Based on event VmRestartedOnAlternateHostEvent.	Information	Automatic	This event records that the VM was restarted on a host, since its original host had failed.
VM Screenshot HA reset	Based on event VmDasBeingResetWithScreenshotEvent.	Warning	Manual	This event records when a VM is reset by HA VM health monitoring on hosts that support the create screenshot API.
VM total disk latency	Average datastore highest latency for 15 minutes is above 50 milliseconds.	Warning	Automatic	Highest latency value across all disks used by the VM.
	Average datastore highest latency for 15 minutes is above 75 milliseconds.	Error		

Alarm Name	Event/Condition	Severity	Resolve Action	Description
VM with no backups	No backup restore points for the past 24 hours.	Warning	Automatic	This VM has not been backed up within the defined RPO (Recovery Point Objective) interval.
VM with no replica	No replica restore points for the past 24 hours.	Warning	Automatic	This VM has not been replicated within the defined RPO (Recovery Point Objective) interval.
VM WWN conflict	Based on event VmWwnConflictEvent.	Error	Manual	This event records a conflict of VM WWNs (World Wide Name).
VMware VM tools state	VMware VM tools state changes equals *Unknown.*	Warning	Automatic	There is a problem with VMware Tools in this Virtual Machine.
	VMware VM tools state changes equals *Out-of-date.*	Warning		
	VMware VM tools state changes equals *Not installed.*	Error		
	VMware VM tools state changes equals *Not running.*	Error		

Datastore

Alarm Name	Event/Condition	Severity	Resolve Action	Description
	Free space is below 10%.	Warning	Automatic	

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Datastore free space	Free space is below 5%.	Error		Datastore is low on available free space.
Datastore is inaccessible	State not equals *Accessible* for 5 minutes or more.	Error	Automatic	The event indicates a loss in connectivity to the specified storage device. The path indicated is the last path that went down.
Datastore over-allocation	Datastore provisioning rate is above 400%.	Warning	Automatic	Datastore is over-allocated.
	Datastore provisioning rate is above 600%.	Error		
Datastore read latency	Maximum datastore read latency for 15 minutes is above 100 milliseconds.	Warning	Automatic	Datastore latency has exceeded the threshold of total read latency.
	Maximum datastore read latency for 15 minutes is above 250 milliseconds.	Error		
Datastore write latency	Maximum datastore write latency for 15 minutes is above 100 milliseconds.	Warning	Automatic	Datastore latency has exceeded the threshold of total write latency.
	Maximum datastore write latency for 15 minutes is above 250 milliseconds.	Error		
Locker misconfiguration	Based on event LockerMisconfiguredEvent.	Warning	Manual	Locker has not been configured properly. Datastore which is configured to back the locker does not exist.

Any Object

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Duplicate IP address detected	Based on event DuplicateIpDetectedEvent.	Warning	Manual	This event records that a duplicate IP address has been observed, with conflict between VM, and the vMotion or IP storage interface configured on the host.
Host cluster destroyed	Based on event ClusterDestroyedEvent.	Information	Automatic	This event records when a cluster is destroyed.
Host failure detected	Based on event DasHostFailedEvent.	Error	Manual	This event records when a host failure has been detected by HA.
Host isolation in HA cluster	Based on event DasHostIsolatedEvent.	Warning	Manual	This event records that a host has been isolated from the network in a HA cluster. Since an isolated host cannot be distinguished from a failed host except by the isolated host itself, this event is logged when the isolated host regains network connectivity.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
No host redundant management network available	Based on event HostNoRedundantManagementNetworkEvent.	Warning	Manual	This event records the fact that a host does not have a redundant management network. It is recommended that host management networks be configured with redundancy.
Primary host connection re-established	Based on event DasAgentFoundEvent.	Information	Automatic	This event records that vCenter Server has re-established contact with a primary host in this HA cluster.
Primary host unavailable	Based on event DasAgentUnavailableEvent.	Error	Automatic	This event records that vCenter Server cannot contact to any primary host in this HA cluster. vCenter Server has lost contact with all primary nodes with a connected state. Attempts to configure HA on a host in this cluster will fail until a DasAgentFoundEvent is logged or unless this is the first node to be configured. For example, if all the other hosts are disconnected first.
	Based on event DasAgentFoundEvent.	Resolve		

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Resource pool configuration conflict	Based on event ResourceViolatedEvent.	Error	Manual	This event records when a conflict with a resource pool's resource configuration is detected.
Storage ATS support failure	Based on event esx.problem.vmfs.ats.support.lost.	Error	Manual	In a shared storage environment, when multiple hosts access the same VMFS datastore, specific locking mechanisms are used. These locking mechanism prevent multiple hosts from concurrently writing to the metadata and ensure that no data corruption occurs. VMFS supports SCSI reservations and atomic test and set (ATS) locking. For storage devices that support hardware acceleration, VMFS uses the ATS algorithm, also called hardware assisted locking. In contrast with SCSI reservations, ATS supports discrete locking per disk sector.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Task timeout reached	Based on event TaskTimeoutEvent.	Warning	Manual	This event records when a task exceeds defined timeout in vCenter Server.
Template deployment failure	Based on event VmDeployFailedEvent.	Error	Manual	This event records a failure to deploy a VM from a template.
vCenter storage availability error	Based on event vprob.vmfs.error.volume.is.locked.	Error	Manual	The alarm indicates that a VMFS volume on the ESXi host is locked due to an I/O error.
	Based on event esx.problem.vmfs.error.volume.is.locked.	Error		
	Based on event vprob.vmfs.extent.offline.	Warning		
	Based on event esx.problem.vmfs.extent.offline.	Warning		
VM instance UUID conflict	Based on event VmInstanceUuidConflictEvent.	Warning	Automatic	This event records a conflict of VM instance UUIDs.
	Based on event VmInstanceUuidChangedEvent.	Resolve		
VM MAC address conflict	Based on event VmMacConflictEvent.	Error	Automatic	This event records a MAC address conflict for a VM.
	Based on event VmStaticMacConflictEvent.			
	Based on event VmMacChangedEvent.	Resolve		
vSphere cluster HA error	Based on event com.vmware.vc.HA.HostDasErrorEvent.	Error	Manual	There is an issue with VMware high-availability configuration for this host.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
vSphere cluster HA warning	Based on event com.vmware.vc.HA.InvalidMaster.	Warning	Manual	There is an issue with VMware high-availability protection for this cluster.
	Based on event com.vmware.vc.HA.UserHeartbeatDatastoreRemoved.			
	Based on event com.vmware.vc.HA.VcCannotFindMasterEvent.			
	Based on event com.vmware.vc.HA.HostPartitionedFromMasterEvent.			
	Based on event com.vmware.vc.HA.HostUnconfiguredWithProtectedVms.			
	Based on event com.vmware.vc.HA.HostUnconfigureError.			
	Based on event com.vmware.vc.HA.NotAllHostAddrsPingable.			

vCloud Director vApp

Alarm Name	Event/Condition	Severity	Resolve Action	Description
vApp health status	VMware Cloud Director object task status equals *Warning.*	Warning	Automatic	vApp health status has changed.
	VMware Cloud Director object task status equals *Alert.*	Error		
vApp runtime lease timeout	vApp runtime lease timeout is 14 days.	Warning	Automatic	vApp runtime lease has expired. Once a vApp is powered on for

Alarm Name	Event/Condition	Severity	Resolve Action	Description
	vApp runtime lease timeout is 7 days.	Error		the first time, the clock starts for the Maximum Runtime Lease. The Maximum Runtime Lease is how long a vApp can be powered on before its automatically suspended.
vApp storage lease timeout	vApp storage lease timeout is 14 days.	Warning	Automatic	vApp storage lease has expired. A vApp storage lease begins when a user stops the vApp. Storage leases do not affect running vApps.
	vApp storage lease timeout is 7 days.	Error		

vCloud Director Organization

Alarm Name	Rule Event	Severity	Resolve Action	Description
Organization blocking task number	Number of blocking tasks is 1 or more.	Warning	Automatic	Some tasks are in a pending state as a result of blocking.
	Number of blocking tasks is 5 or more.	Error		
Organization blocking task timeout	Blocking tasks timeout is 5 minutes.	Warning	Automatic	One or more organization blocking tasks has expired.
	Blocking tasks timeout is 10 minutes.	Error		

vCloud Director Org VDC

Alarm Name	Rule Event	Severity	Resolve Action	Description
Network pool usage	Network pool usage is above 90%.	Warning	Automatic	Network pool usage has exceeded the configured threshold.
	Network pool usage is above 95%.	Error		

Alarm Name	Rule Event	Severity	Resolve Action	Description
Org VDC CPU usage	Average CPU usage for 15 minutes is above 80%.	Warning	Automatic	Organization VDC has exceeded the CPU usage threshold.
	Average CPU usage for 15 minutes is above 90%.	Error		
Org VDC health status	VMware Cloud Director object task status equals *Warning.*	Warning	Automatic	Organization VDC health status has changed.
	VMware Cloud Director object task status equals *Alert.*	Error		
Org VDC memory usage	Average memory usage for 15 minutes is above 80%.	Warning	Automatic	Organization VDC has exceeded the memory usage threshold.
	Average memory usage for 15 minutes is above 90%.	Error		
Org VDC storage usage	Average storage usage for 15 minutes is above 80%.	Warning	Automatic	Organization VDC has exceeded the storage usage threshold.
	Average storage usage for 15 minutes is above 90%.	Error		

vCloud Director Provider VDC

Alarm Name	Rule Event	Severity	Resolve Action	Description
Provider VDC CPU usage	Average CPU usage for 15 minutes is above 80%.	Warning	Automatic	Provider VDC has exceeded the threshold for CPU Usage
	Average CPU usage for 15 minutes is above 90%.	Error		
Provider VDC health status	VMware Cloud Director object task status equals *Warning.*	Warning	Automatic	Provider VDC health status has changed.

Alarm Name	Rule Event	Severity	Resolve Action	Description
	VMware Cloud Director object task status equals *Alert.*	Error		
Provider VDC memory usage	Average memory usage for 15 minutes is above 80%.	Warning	Automatic	Provider VDC has exceeded the memory usage threshold.
	Average memory usage for 15 minutes is above 90%.	Error		
Provider VDC storage usage	Average storage usage for 15 minutes is above 80%.	Warning	Automatic	Provider VDC has exceeded the storage usage threshold.
	Average storage usage for 15 minutes is above 90%.	Error		

Microsoft Hyper-V Alarms

This section describes predefined alarms for Microsoft Hyper-V infrastructure components.

Host

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Bad Hyper-V username logon attempt	Based on event 4625 Microsoft-Windows-Security-Auditing.	Error	Manual	This event records a failed user logon attempt. The combination of username, password and permissions is the mechanism by which Hyper-V server authenticate a user for access and authorize the user to perform activities.
Cluster communication session failed	Based on event 1570 Microsoft-Windows-FailoverClustering.	Error	Manual	Host mode failed to establish a communication session while joining the cluster.
Cluster host node network connectivity error	Based on event 1554 Microsoft-Windows-FailoverClustering.	Error	Manual	This cluster node has no network connectivity. It cannot participate in the cluster until connectivity is restored.
Cluster hosts update version mismatch	Based on event 1548 Microsoft-Windows-FailoverClustering.	Error	Manual	Host node has established a communication session with another node and detected that it is running a different but compatible version of the cluster service software.
Cluster network failure	Based on event 1127 Microsoft-Windows-FailoverClustering.	Warning	Manual	Cluster network interface for cluster node has failed.
Cluster witness resource failure	Based on event 1558 Microsoft-Windows-FailoverClustering.	Error	Manual	The cluster service detected a problem with the witness resource. The witness resource will be failed over to another node within the cluster in an attempt to reestablish access to cluster configuration data.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Cluster witness resource update failure	Based on event 1557 Microsoft-Windows-FailoverClustering.	Error	Manual	Cluster service failed to update the cluster configuration data on the witness resource.
Host available memory	Average Hyper-V Services memory usage for 15 minutes is above 80%.	Warning	Automatic	This host is low on available memory.
	Average Hyper-V Services memory usage for 15 minutes is above 90%.	Error		
Host average disk queue length	Average disk queue length for 15 minutes is above 1.	Warning	Automatic	Average disk queue length on the host may report on too many I/O requests. This means that not all requests are queued. Some requests are completed and are on their way back to where the performance data is being collected.
	Average disk queue length for 15 minutes is above 2.	Error		
Host average memory pressure	Average pressure for 15 minutes is above 90%.	Warning	Automatic	This host has exceeded the threshold for memory pressure.
	Average pressure for 15 minutes is above 100%.	Error		
Host cluster membership	Based on event 1093 Microsoft-Windows-FailoverClustering.	Error	Manual	The Cluster service cannot identify host node as a member of failover cluster.
Host connection failure	State not equals *Connected* for 5 minutes or more.	Error	Automatic	This alarm monitors Hyper-V host connection state.
Host CPU time per dispatch	Average host CPU wait time for 15 minutes is 60 microseconds.	Warning	Automatic	The counter shows the average time Virtual Machines running on the host spent waiting for a virtual processor to be dispatched onto a logical processor. More vCPUs on host means more things the dispatcher has to schedule thus wait time raises.
	Average host CPU wait time for 15 minutes is 100 microseconds.	Error		

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Host CPU usage	Average Total Run Time value for 15 minutes is above 75%.	Warning	Automatic	This host has exceeded the threshold for CPU usage.
	Average Total Run Time value for 15 minutes is above 85%.	Error		
Host failed to form a cluster	Based on event 1546 Microsoft-Windows-FailoverClustering.	Error	Manual	Host node failed to form a failover cluster.
Host Image Management service is not running	*Hyper-V Image Management* service is not running for 5 minutes or more.	Error	Automatic	The service required to manage virtual storage is not running. No virtual storage management operations can be performed.
Host Memory Pages Usage	Average pages/sec value for 15 minutes is above 500.	Warning	Automatic	The counter shows the rate at which pages are read from or written to disk to resolve hard page faults. This counter is a primary indicator of the types of faults that cause system-wide delays.
	Average pages/sec value for 15 minutes is above 1500.	Error		
Host network average output queue length	Average network output queue length for 15 minutes is above 1.	Warning	Automatic	This host has exceeded the threshold for the length of the queue in packets. This counter should be 0 at all times.
	Average network output queue length for 15 minutes is above 2.	Error		
Host network outbound errors number	Average network outbound errors number for 15 minutes is above 1.	Warning	Automatic	This host has exceeded the threshold for the outbound packets that couldn't be transmitted because of errors.
	Average network outbound errors number for 15 minutes is above 2.	Error		

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Host Networking Management service is not running	*Hyper-V Networking Management* service is not running for 5 minutes or more.	Error	Automatic	The Hyper-V Networking Management Service is not configured to start automatically. Virtual networks cannot be managed until the service is started.
Host node failed to form a cluster	Based on event 1573 Microsoft-Windows-FailoverClustering.	Error	Manual	Host node failed to form a cluster.
Host node failed to join cluster	Based on event 1572 Microsoft-Windows-FailoverClustering.	Error	Manual	Host node failed to join the cluster because it could not send and receive failure detection network messages with other cluster nodes.
Host node was evicted from cluster	Based on event 1011 Microsoft-Windows-FailoverClustering.	Warning	Manual	Cluster host node has been evicted from the failover cluster.
Host node was removed from cluster	Based on event 1135 Microsoft-Windows-FailoverClustering.	Error	Manual	Cluster node was removed from the active failover cluster membership. If the Cluster service fails to start on a failover cluster node, the node cannot function as part of the cluster.
Host restart	Based on event 1074 User32.	Information	Automatic	Host operation system has been restarted or shut down.
Missing latest cluster configuration data	Based on event 1561 Microsoft-Windows-FailoverClustering.	Error	Manual	The cluster service has determined that this node does not have the latest copy of cluster configuration data. Therefore, the cluster service has prevented itself from starting on this node.
Network communication failure	Based on event 1592 Microsoft-Windows-FailoverClustering.	Warning	Manual	Cluster node lost communication with another cluster node. Network communication was reestablished.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Unreachable cluster network interface	Based on event 1126 Microsoft-Windows-FailoverClustering.	Warning	Manual	Cluster network interface for cluster node is unreachable by at least one other cluster node attached to the network.
Virtual Machine Management service is not running	*Hyper-V Virtual Machine Management* service is not running.	Error	Automatic	The service required to manage virtual machines is not running. No virtual machine management operations can be performed.

Virtual Machine

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Background disk merge failed	Based on event 19100 Microsoft-Windows-Hyper-V-VMMS.	Warning	Manual	The parent virtual hard disks associated with this virtual machine may be in an inconsistent state.
Background disk merge interruption	Based on event 19090 Microsoft-Windows-Hyper-V-VMMS.	Warning	Manual	The snapshot merge operation was interrupted.
Checkpoint configuration is not accessible	Based on event 16420 Microsoft-Windows-Hyper-V-VMMS.	Error	Manual	The configuration of checkpoint is no longer accessible.
Current memory pressure	Average memory pressure for 15 minutes is above 110%.	Warning	Automatic	This VM has exceeded the threshold for memory pressure.
	Average memory pressure for 15 minutes is above 125%.	Error		
Failed to assign dynamic MAC address	Based on event 12572 Microsoft-Windows-Hyper-V-SynthNic.	Error	Manual	Dynamic MAC address for VM network adapter was not assigned.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Failed to create memory contents file	Based on event 3320 Microsoft-Windows-Hyper-V-Worker.	Error	Manual	Failed to create memory contents file.
Failed to create VM saved state file	Based on event 3080 Microsoft-Windows-Hyper-V-Worker.	Error	Manual	Failed to create or access VM saved state file.
Failed to delete VM directory	Based on event 16150 Microsoft-Windows-Hyper-V-VMMS.	Warning	Manual	Cannot delete VM directory.
Failed to initialize VM memory	Based on event 3050 Microsoft-Windows-Hyper-V-Worker.	Error	Manual	Failed to initialize VM memory.
Failed to merge virtual disk	Based on event 16210 Microsoft-Windows-Hyper-V-VMMS.	Warning	Manual	Cannot merge disk file on deletion. As a result, this disk may be in an inconsistent state.
Failed to power on VM	Based on event 12010 Microsoft-Windows-Hyper-V-Worker.	Error	Manual	Failed to power on VM.
	Based on event 12030 Microsoft-Windows-Hyper-V-Worker.			
	Based on event 12040 Microsoft-Windows-Hyper-V-Worker.			
	Based on event 12050 Microsoft-Windows-Hyper-V-Worker.			
Failed to restore VM	Based on event 12080 Microsoft-Windows-Hyper-V-Worker.	Error	Manual	Failed to restore a VM.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Failed to save VM	Based on event 12054 Microsoft-Windows-Hyper-V-Worker.	Error	Manual	Failed to save state for a VM.
Guest disk space	Guest disk free space is below 10%.	Warning	Automatic	Guest OS volume is low on available guest disk space.
	Guest disk free space is below 5%.	Error		
Incompatible version of integration services	Based on event 4010 Microsoft-Windows-Hyper-V-Integration.	Warning	Manual	The version of a component of integration services is incompatible with another version.
Insufficient disk space	Based on event 16050 Microsoft-Windows-Hyper-V-VMMS.	Warning	Manual	Hyper-V disk space is low on available free space.
Invalid static MAC address	Based on event 12560 Microsoft-Windows-Hyper-V-SynthNic.	Error	Manual	By default, new virtual machines in Hyper-V are created with NICs that are assigned dynamic MAC addresses.
	Based on event 12560 Microsoft-Windows-Hyper-V-Worker.			
	Based on event 12560 Microsoft-Windows-Hyper-V-VMMS.			
Latest checkpoint age	VM checkpoint age is 48 hours or more.	Warning	Automatic	The age of the latest checkpoint for this VM has exceeded the configured threshold.
Latest checkpoint size	Hyper-V VM checkpoint size is above 10% of the VM size.	Warning	Automatic	The size of the latest checkpoint file for this VM has

Alarm Name	Event/Condition	Severity	Resolve Action	Description
	Hyper-V VM checkpoint size is above 20% of the VM size.	Error		exceeded the configured threshold.
Machine remoting system failure	Based on event 12480 Microsoft-Windows-Hyper-V-Worker.	Warning	Manual	Failure in machine remoting system has been detected.
No disk space to run this VM	Based on event 16060 Microsoft-Windows-Hyper-V-VMMS.	Error	Manual	VM has been paused because it has run out of disk space.
Not enough memory to start a VM	Based on event 3122 Microsoft-Windows-Hyper-V-Worker.	Error	Manual	Hyper-V was unable to allocate RAM resources to start this VM.
	Based on event 3030 Microsoft-Windows-Hyper-V-Worker.			
Possible ransomware activity	Total Run Time is above 70% and Virtual Storage Write is above 40 MB/s or Virtual Network Bytes Sent/sec is above 40 MB/s for 5 minutes.	Warning	Automatic	Veeam ONE detected suspicious activity on this VM.
	Total Run Time is above 80% and Virtual Storage Write is above 60 MB/s or Virtual Network Bytes Sent/sec is above 60 MB/s for 5 minutes.	Error		
Static MAC address conflict	Based on event 12562 Microsoft-Windows-Hyper-V-SynthNic.	Warning	Manual	By default, new virtual machines in Hyper-V are created with NICs that are

Alarm Name	Event/Condition	Severity	Resolve Action	Description
	Based on event 12562 Microsoft-Windows-Hyper-V-Worker.			assigned dynamic MAC addresses.
Unexpected VM error	Based on event 16020 Microsoft-Windows-Hyper-V-VMMS.	Error	Manual	This VM has encountered an unexpected error.
VM configuration is not accessible	Based on event 16410 Microsoft-Windows-Hyper-V-VMMS.	Error	Manual	The configuration of virtual machine is no longer accessible.
	Based on event 16400 Microsoft-Windows-Hyper-V-VMMS.			
VM configuration module error	Based on event 4096 Microsoft-Windows-Hyper-V-Config.	Error	Manual	The VM configuration is no longer accessible.
VM CPU usage	Average guest run time for 15 minutes is above 75%.	Warning	Automatic	This VM has exceeded the threshold for CPU usage.
	Average guest run time for 15 minutes is above 85%.	Error		
VM disk errors	Average number of errors/min for 15 minutes is above 4.	Warning	Automatic	This VM has logged one or more errors that have occurred on its virtual device.
	Average number of errors/min for 15 minutes is above 8.	Error		
VM guest OS reboot	Based on event 18514 Microsoft-Windows-Hyper-V-Worker.	Information	Warning	Virtual Machine was rebooted. This warning is applied only to Windows Server 2012 and Windows Server 2012 R2.
VM initialization error	Based on event 3040 Microsoft-Windows-Hyper-V-Worker.	Error	Manual	VM initialization has failed.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
VM power status	State not equals *Running* for 5 minutes or more.	Error	Automatic	VM power state has been changed.
VM invalid switch port reference	Based on event 12570 Microsoft-Windows-Hyper-V-SynthNic.	Error	Manual	The virtual machine cannot be started.
VM restart	Based on event 18512 Microsoft-Windows-Hyper-V-Worker.	Information	Automatic	Virtual Machine was rebooted. This warning is applied only to Windows Server 2012 and Windows Server 2012 R2.
VM shutdown by guest	Based on event 18508 Microsoft-Windows-Hyper-V-Worker.	Information	Automatic	Virtual Machine was shut down. This warning is applied only to Windows Server 2012 and newer Windows server versions.
VM shutdown by host	Based on event 18504 Microsoft-Windows-Hyper-V-Worker.	Information	Automatic	Virtual Machine was shut down. This warning is applied only to Windows Server 2012 and newer Windows server versions.
VM vCPU time per dispatch	Average CPU wait time for 15 minutes is above 60 microseconds.	Warning	Automatic	The counter shows the average time spent waiting for a virtual processor to be dispatched onto a logical processor.
	Average CPU wait time for 15 minutes is above 100 microseconds.	Error		
VM with no backups	No backup restore points for the past 24 hours.	Warning	Automatic	This VM has not been backed up within the defined RPO (Recovery Point Objective) interval.
VM with no replica	No replica restore points for the past 24 hours.	Warning	Automatic	This VM has not been replicated within the defined RPO (Recovery Point Objective) interval.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
VSS checkpoint failure	Based on event 10102 Microsoft-Windows-Hyper-V-VMMS.	Error	Manual	Failed to create the backup of virtual machine.
	Based on event 15252 Microsoft-Windows-Hyper-V-VMMS.	Error		

Cluster

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Cluster configuration data is missing or corrupt	Based on event 1575 Microsoft-Windows-FailoverClustering.	Error	Manual	An attempt to forcibly start the cluster service has failed because the cluster configuration data on host node is either missing or corrupt.
Cluster configuration database cannot be unloaded	Based on event 1593 Microsoft-Windows-FailoverClustering.	Error	Manual	The failover cluster database could not be unloaded and any potentially incorrect changes in memory could not be discarded. The cluster service will attempt to repair the database by retrieving it from another cluster node.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Cluster database could not be loaded	Based on event 1057 Microsoft-Windows-FailoverClustering.	Error	Manual	The cluster database could not be loaded. Ensure that a good copy of the cluster configuration is available to the node.
Cluster memory overcommitment	Based on event VeeamHvClusterReserveStateOkEvent.	Resolve	Automatic	When placing a virtual machine in a failover cluster, the placement process calculates whether the new virtual machine will over-commit the cluster. If the action will over-commit the cluster, the alarm will trigger.
	Based on event VeeamHvClusterReserveStateErrorEvent.	Error		
Cluster network is down	Based on event 1130 Microsoft-Windows-FailoverClustering.	Warning	Manual	Cluster network is down.
Cluster resource cannot be brought online	Based on event 1207 Microsoft-Windows-FailoverClustering.	Error	Manual	Cluster network name resource cannot be brought online. The computer object associated with the resource could not be updated in domain.
Cluster resource failure	Based on event 1069 Microsoft-Windows-FailoverClustering.	Error	Manual	Cluster resource in clustered service or application has failed.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Cluster service cannot be started	Based on event 1090 Microsoft-Windows-FailoverClustering.	Error	Manual	Cluster service cannot be started. An attempt to read configuration data from the Windows registry failed.
Cluster service failed to start	Based on event 1105 Microsoft-Windows-FailoverClustering.	Error	Manual	Cluster service failed to start because it was unable to register interfaces with the RPC service.
Cluster service failed to write data to a file	Based on event 1080 Microsoft-Windows-FailoverClustering.	Warning	Manual	Cluster service could not write to a file. In a failover cluster, most clustered services or applications use at least one disk, also called a disk resource, that you assign when you configure the clustered service or application. Clients can use the clustered service or application only when the disk is functioning correctly.
Cluster service fatal error	Based on event 1000 Microsoft-Windows-FailoverClustering.	Error	Manual	Cluster service suffered an unexpected fatal error.
Cluster service interruption	Based on event 1006 Microsoft-Windows-FailoverClustering.	Error	Manual	Cluster service was halted due to incomplete connectivity with other cluster nodes.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Cluster service shut down	Based on event 1177 Microsoft-Windows-FailoverClustering.	Error	Manual	The Cluster service is shutting down because quorum was lost.
Cluster Shared Volume is not available	Based on event 5120 Microsoft-Windows-FailoverClustering.	Warning	Automatic	Cluster Shared Volume is no longer available on this node. All I/O will temporarily be queued until a path to the volume is reestablished.
	Based on event 5122 Microsoft-Windows-FailoverClustering.	Resolve		
Cluster Shared Volume is not directly accessible	Based on event 5121 Microsoft-Windows-FailoverClustering.	Warning	Automatic	Cluster Shared Volume is no longer directly accessible from this cluster node. I/O access will be redirected to the storage device over the network through the node that owns the volume. This may result in degraded performance.
	Based on event 5122 Microsoft-Windows-FailoverClustering.	Resolve		
Failed to bring cluster resource online	Based on event 1049 Microsoft-Windows-FailoverClustering.	Error	Manual	Cluster IP address resource cannot be brought online.
Failed to copy cluster configuration data file	Based on event 1581 Microsoft-Windows-FailoverClustering.	Warning	Manual	The restore request for the cluster configuration data failed to make a copy of the existing cluster configuration data file (ClusDB).

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Failed to create cluster resource name in domain	Based on event 1193 Microsoft-Windows-FailoverClustering.	Error	Manual	Cluster network name resource failed to create its associated computer object in domain.
Failed to migrate virtual machine	Based on event 22506 Microsoft-Windows-Hyper-V-High-Availability.	Error	Manual	Live migration for this VM did not succeed.
	Based on event 22505 Microsoft-Windows-Hyper-V-High-Availability.			
	Based on event 21100 Microsoft-Windows-Hyper-V-High-Availability.			
Failed to unload failover cluster database	Based on event 1574 Microsoft-Windows-FailoverClustering.	Error	Manual	The failover cluster database could not be unloaded.
Inconsistency within the failover cluster	Based on event 1073 Microsoft-Windows-FailoverClustering.	Error	Manual	The Cluster service was halted to prevent an inconsistency within the failover cluster.
Invalid IP address detected	Based on event 1047 Microsoft-Windows-FailoverClustering.	Error	Manual	Cluster IP address resource cannot be brought online because the address value is invalid.
Invalid IP address for cluster resource	Based on event 1360 Microsoft-Windows-FailoverClustering.	Error	Manual	Cluster IP address resource failed to come online.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Invalid subnet mask detected	Based on event 1046 Microsoft-Windows-FailoverClustering.	Error	Manual	Cluster IP address resource cannot be brought online because the subnet mask value is invalid.
Unexpected cluster service problem	Based on event 1556 Microsoft-Windows-FailoverClustering.	Error	Manual	The cluster service encountered an unexpected problem and will be shut down.

Cluster Shared Volume

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Active filter drivers detected	Based on event 5125 Microsoft-Windows-FailoverClustering.	Warning	Manual	Cluster Shared Volume has identified one or more active filter drivers on this device stack that could interfere with CSV operations. I/O access will be redirected to the storage device over the network through another Cluster node. This may result in degraded performance.
	Based on event 5126 Microsoft-Windows-FailoverClustering.			
Cluster Shared Volume read latency	Average read latency for 15 minutes is above 40 milliseconds.	Warning	Automatic	Cluster Shared Volume has exceeded the configured threshold of total read latency.
	Average read latency for 15 minutes is above 80 milliseconds.	Error		
Cluster Shared Volume write latency	Average write latency for 15 minutes is above 40 milliseconds.	Warning	Automatic	Cluster Shared Volume has exceeded the configured threshold of total write latency.
	Average write latency for 15 minutes is above 80 milliseconds.	Error		

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Cluster Shared Volume free space	Free space is below 10%.	Warning	Automatic	Cluster Shared Volume is low on available free space.
	Free space is below 5%.	Error		
Redirected access was turned on	Based on event 5136 Microsoft-Windows-FailoverClustering.	Warning	Manual	Cluster Shared Volume redirected access was turned on. Access to the storage device will be redirected over the network from all cluster nodes that are accessing this volume. This may result in degraded performance.
Volume snapshot preparation error	Based on event 1584 Microsoft-Windows-FailoverClustering.	Error	Manual	A backup application initiated a VSS snapshot on Cluster Shared Volume without properly preparing the volume for snapshot. This snapshot may be invalid and the backup may not be usable for restore operations.

Local Storage

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Datastore read latency	Avg Disk sec/Read value for 15 minutes is 40 milliseconds.	Warning	Automatic	This host local disk has exceeded the threshold for total read latency. This performance monitor counter measures the amount of time that read operations take to respond to the operating system.
	Avg Disk sec/Read value for 15 minutes is 80 milliseconds.	Error		
Datastore write latency	Avg Disk sec/Write value for 15 minutes is 40 milliseconds.	Warning	Automatic	This host disk has exceeded the threshold for total write latency. This performance monitor counter measures the amount of time that write operations take to respond to the operating system.
	Avg Disk sec/Write value for 15 minutes is 80 milliseconds.	Error		

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Local volume free space	Free space is below 10%.	Warning	Automatic	Local volume is low on available free space.
	Free space is below 5%.	Error		

Any Hyper-V Object

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Cluster Shared Volume is no longer accessible	Based on event 5142 Microsoft-Windows-FailoverClustering.	Error	Manual	Cluster Shared Volume is no longer accessible from this cluster node because of error.
Failed to load VM configuration	Based on event 16300 Microsoft-Windows-Hyper-V-VMMS.	Error	Manual	Cannot load a virtual machine configuration
Failed to open VM attachment	Based on event 12290 Microsoft-Windows-Hyper-V-Worker.	Error	Manual	Cannot open VM attachment.
	Based on event 12290 Microsoft-Windows-Hyper-V-SynthStor.			
	Based on event 12290 Microsoft-Windows-Hyper-V-VMMS.			
	Based on event 12140 Microsoft-Windows-Hyper-V-VMMS.			
	Based on event 12140 Microsoft-Windows-Hyper-V-Worker.			
	Based on event 12140 Microsoft-Windows-Hyper-V-SynthStor.			

Alarm Name	Event/Condition	Severity	Resolve Action	Description
	Based on event 12240 Microsoft-Windows-Hyper-V-VMMS.			
	Based on event 12240 Microsoft-Windows-Hyper-V-Worker.			
	Based on event 12240 Microsoft-Windows-Hyper-V-SynthStor.			
Failed to register VM configuration file	Based on event 20100 Microsoft-Windows-Hyper-V-VMMS.	Warning	Manual	The Hyper-V Virtual Machine Management service failed to register the configuration for the virtual machine.
Failed to revert to VSS snapshot	Based on event 10104 Microsoft-Windows-Hyper-V-VMMS.	Error	Manual	Failed to revert to VSS snapshot on one or more virtual hard disks of the virtual machine.
Failed to unregister VM configuration file	Based on event 20102 Microsoft-Windows-Hyper-V-VMMS.	Warning	Manual	The Hyper-V Virtual Machine Management service failed to unregister the configuration for the virtual machine.
Failed to verify VM configuration file	Based on event 20104 Microsoft-Windows-Hyper-V-VMMS.	Warning	Manual	The Hyper-V Virtual Machine Management service failed to verify that the configuration is registered for the virtual machine.
VM configuration file is corrupt	Based on event 16310 Microsoft-Windows-Hyper-V-VMMS.	Error	Manual	Cannot load the virtual machine because the configuration is corrupt.

Internal Alarms

The following table describes internal Veeam ONE alarms.

Alarm Name	Event/Condition	Severity	Description
Audit log failure	Based on event VeeamAuditLogFailureEvent.	Error	Veeam ONE failed to add a new record to the audit log.
	Based on event VeeamAuditLogFailureResolvedEvent.	Resolve	
Audit log free space	Amount of free space is below 25%.	Warning	Size of the audit log is reaching the maximum allocated space limit.
	Amount of free space is below 5%.	Error	
Backup performance data collection failure	Based on event VeeamBpPerfCollectionFailedEvent.	Error	Veeam ONE failed to collect performance data from the specified backup server.
	Based on event VeeamMonitorServicesStartedEvent.	Resolve	
	Based on event VeeamBpPerfCollectionFailedResolvedEvent.	Resolve	
Backup data collection failure	Based on event VeeamNoHostConnectionEvent.	Error	Veeam ONE failed to collect data from a Veeam Backup & Replication and Veeam Backup for Microsoft 365 server.
	Based on event VeeamNoHostConnectionResolvedEvent.	Resolve	
	Based on event VeeamMonitorServicesStartedEvent.	Resolve	
Disk cache error	Based on event VeeamDPCacheEvent.	Warning	Veeam ONE failed to write performance data to the
	Based on event VeeamDPCacheResolvedEvent.	Resolve	

Alarm Name	Event/Condition	Severity	Description
	Based on event VeeamMonitorServicesStartedEvent.	Resolve	disk cache folder.
Events data collection failure	Based on event VeeamEventCollectionFailedEvent.	Error	Veeam ONE failed to collect events data from the objects specified.
	Based on event VeeamEventCollectionFailedResolvedEvent.	Resolve	
	Based on event VeeamMonitorServicesStartedEvent.	Resolve	
Guest services collection failure	Based on event VeeamCollectionServiceFailedEvent.	Error	Veeam ONE failed to collect guest services state information.
	Based on event VeeamCollectionServiceFailedResolvedEvent.	Resolve	
Guest processes collection failure	Based on event VeeamCollectionProcessFailedEvent.	Error	Veeam ONE failed to collect guest processes state information.
	Based on event VeeamCollectionProcessFailedResolvedEvent.	Resolve	
Hardware sensors collection failure	Based on event VeeamHardwareSensorsCollectionEvent.	Error	Veeam ONE failed to collect host hardware information.
	Based on event VeeamHardwareSensorsCollectionResolvedEvent.	Resolve	
	Based on event VeeamMonitorServicesStartedEvent.	Resolve	
Performance data collection failure	Based on event VeeamPerfCollectionFailedEvent.	Error	Veeam ONE failed to collect performance data from the objects specified.
	Based on event VeeamPerfCollectionFailedResolvedEvent.	Resolve	
	Based on event VeeamMonitorServicesStartedEvent.	Resolve	

Alarm Name	Event/Condition	Severity	Description
Recon Scanner threat state	Status of threat detection equals *Information*.	Information	Recon Scanner raised the alert based on one or more suspicious behaviors.
	Status of threat detection equals *Warning*.	Warning	
	Status of threat detection equals *Error*.	Error	
Reporting data scheduling issue	Status of a report scheduling task equals *Warning*.	Warning	Veeam ONE failed to deliver a scheduled report, report folder or dashboard.
	Status of a report scheduling task equals *Failed*.	Error	
	Status of a report folder scheduling task equals *Warning*.	Warning	
	Status of a report folder scheduling task equals *Failed*.	Error	
	Status of a dashboard scheduling task equals *Warning*.	Warning	
	Status of dashboard scheduling task equals *Failed*.	Error	
SQL Server Express database size	Based on event VeeamSqlLowDbFreeSpaceEvent.	Warning	Veeam ONE database size is close to maximum database size supported by SQL Server Express Edition.
	Based on event VeeamSqlLowDbFreeSpaceResolvedEvent.	Resolve	
	Based on event VeeamMonitorServicesStartedEvent.	Resolve	
Staging data processing issue	Age of the oldest file that contains staging data equals 1 day.	Error	Age of the oldest file that contains staging data of Veeam ONE databases has reached the configured threshold.

Alarm Name	Event/Condition	Severity	Description
Topology collection failure	Based on event VeeamInfCollectionFailedEvent.	Error	Veeam ONE failed to collect infrastructure topology.
	Based on event VeeamInfCollectionFailedResolvedEvent.	Resolve	
	Based on event VeeamMonitorServicesStartedEvent.	Resolve	
VMware Cloud Director blocking tasks update failure	Based on event VeeamVcdBlockingTaskUpdateFailedEvent.	Error	Veeam ONE failed to update VMware Cloud Director blocking tasks list.
	Based on event VeeamVcdBlockingTaskUpdateFailedResolvedEvent.	Resolve	
VMware Cloud Director connection failure	Based on event VeeamNoVcdHostConnectionEvent.	Error	Veeam ONE failed to collect performance and configuration data from VMware Cloud Director.
	Based on event VeeamNoVcdHostConnectionResolvedEvent.	Resolve	
	Based on event VeeamMonitorServicesStartedEvent.	Resolve	
VMware Cloud Director stranded items update failure	Based on event VeeamVcdStrandedItemUpdateFailedEvent.	Error	Veeam ONE failed to update VMware Cloud Director stranded items list.
	Based on event VeeamVcdStrandedItemUpdateFailedResolvedEvent.	Resolve	
Veeam Backup & Replication license compatibility	Based on event VeeamBackupServerLicenseCompatibility.	Error	License installed on the backup server is not compatible with the license installed on Veeam ONE server.
	Based on event VeeamBackupServerLicenseCompatibilityResolved.	Resolve	

Alarm Name	Event/Condition	Severity	Description
Veeam Analytics service on the Veeam ONE server is not running	Based on event VeeamOneAgentServerNoConnectionEvent.	Error	Veeam Analytics service on the Veeam ONE server is not running.
	Based on event VeeamOneAgentServerNoConnectionResolvedEvent.	Resolve	
	Based on event VeeamMonitorServicesStartedEvent.	Resolve	
Veeam Analytics service on the remote server is not running	Based on event VeeamOneAgentClientNoConnectionEvent.	Error	Veeam Analytics service on the remote server is not running.
	Based on event VeeamOneAgentClientNoConnectionResolvedEvent.	Resolve	
Veeam intelligent diagnostics failure	Based on event VeeamIntelligenceDiagnosisFailedEvent.	Error	Veeam ONE failed to analyze Veeam Backup & Replication server logs.
Veeam ONE agent server connection failure	Based on event VeeamOneAgentServerNoConnectionEvent.	Error	Veeam ONE server failed to connect to Veeam ONE agent server.
	Based on event VeeamOneAgentServerNoConnectionResolvedEvent.	Resolve	
Veeam ONE agent client connection failure	Based on event VeeamOneAgentClientNoConnectionEvent.	Error	Veeam ONE server failed to connect to Veeam ONE agent client.
	Based on event VeeamOneAgentClientNoConnectionResolvedEvent.	Resolve	
Veeam ONE database cleanup task status	Database object removal queue constantly grew for defined time period (default 1 day).	Error	Veeam ONE server processing speed is slower than the deletion of object information.

Alarm Name	Event/Condition	Severity	Description
Veeam ONE email notification delivery failure	Based on event VeeamEmailNotificationFailed.	Error	Veeam ONE server failed to deliver an email notification.
	Based on event VeeamEmailNotificationResolved.	Resolve	
	Based on event VeeamMonitorServicesStartedEvent.	Resolve	
Veeam ONE license expiration date	Based on event VeeamLicenseExpirationWarningEvent.	Warning	Veeam ONE license is going to expire soon.
	Based on event VeeamLicenseExpirationErrorEvent.	Error	
	Based on event VeeamLicenseChangedEvent.	Resolve	
	Based on event VeeamLicenseExpirationResolvedEvent.	Resolve	
	Based on event VeeamMonitorServicesStartedEvent.	Resolve	
Veeam ONE license update failure	Based on event VeeamLicenseUpdateErrorEvent.	Warning	License update failure can take place for a number of reasons such as connection failure, invalid identifier, expired contract, and so on. In case of a connection problem and licensing server key generation error, Veeam ONE will retry to update the license key.
	Based on event VeeamLicenseUpdateResolvedEvent.	Resolve	
	Based on event VeeamMonitorServicesStartedEvent.	Resolve	

Alarm Name	Event/Condition	Severity	Description
Veeam ONE license exceeded	Based on event VeeamVMsExceedErrorEvent.	Error	Veeam ONE license limit has been exceeded.
	Based on event VeeamVMsExceedWarningEvent.	Warning	
	Based on event VeeamSocketExceedEvent.	Error	
	Based on event VeeamBpExceedErrorEvent.	Error	
	Based on event VeeamBpExceedWarningEvent.	Warning	
	Based on event VeeamLicenseGraceOverEvent.	Error	
	Based on event VeeamVMsExceedResolvedEvent.	Resolve	
	Based on event VeeamSocketExceedResolvedEvent.	Resolve	
	Based on event VeeamLicenseChangedEvent.	Resolve	
	Based on event VeeamVbmExceedWarningEvent.	Warning	
	Based on event VeeamVbmExceedResolvedEvent.	Resolve	
Object properties data collection failure	Job state equals *Failed*.	Error	Veeam ONE Object properties data collection job did not finish successfully.
	Job state equals *Warning*.	Warning	

Alarm Name	Event/Condition	Severity	Description
Veeam ONE Reporting service state	Veeam ONE Reporting service is not running.	Error	Veeam ONE Reporting service has failed.
Veeam ONE Server Load	Veeam ONE Server CPU Usage is above 90% or Veeam ONE Server Memory Usage is above 95%.	Error	Veeam ONE Server load is too high.
	Veeam ONE Server CPU Usage is above 75% or Veeam ONE Server Memory Usage is above 85%.	Warning	
Veeam ONE support expiration date	Based on event VeeamLicenseSupportExpirationWarningEvent.	Warning	Veeam ONE support period is going to expire soon.
	Based on event VeeamLicenseSupportExpirationErrorEvent.	Error	
	Based on event VeeamLicenseChangedEvent.	Resolve	
	Based on event VeeamLicenseSupportExpirationResolvedEvent.	Resolve	
	Based on event VeeamMonitorServicesStartedEvent.	Resolve	
Virtual Server connection failure	Based on event VeeamNoHostConnectionEvent.	Error	Connection to virtual server has failed.
	Based on event VeeamNoHostConnectionResolvedEvent.	Resolve	
	Based on event VeeamMonitorServicesStartedEvent.	Resolve	
ServiceNow instance connection state	Based on event VeeamServiceNowNoConnectionEvent	Error	Connection to ServiceNow instance has failed.
	Based on event VeeamServiceNowNoConnectionResolvedEvent	Resolve	

Alarm Name	Event/Condition	Severity	Description
	Based on event VeeamMonitorServicesStartedEvent	Resolve	
Syslog server connection state	Based on event VeeamSyslogServerFailureEvent	Error	The Syslog server is unavailable.
	Based on event VeeamSyslogServerFailureResolvedEvent	Resolve	
	Based on event VeeamMonitorServicesStartedEvent	Resolve	

Alarm Rules Reference

This section describes rules that can be used to create alarms for virtual and backup infrastructures.

Alarm Rules for VMware vSphere

Veeam ONE offers the following types of alarm rules for VMware vSphere infrastructure objects.

vCenter Server

Rule Type	Description
Event-based rule	An alarm is triggered if some vCenter-related event is generated.
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.
Power or connection state changes	An alarm is triggered if the vCenter Server state reports to be equal or not equal to a specific state value (for example, if vCenter Server is not responding).

Cluster

Rule Type	Description
Event-based rule	An alarm is triggered if some cluster-related event is generated.
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.
Resource usage	An alarm is triggered if the specified counter is above or below the specified threshold value (for example, if the memory usage exceeds 80%).

Host

Rule Type	Description
Event-based rule	An alarm is triggered if some host-related event is generated.
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.

Rule Type	Description
Hardware sensor state changes	An alarm is triggered if the sensor state reports to be equal or not equal to a specific state value (*Normal*, *Warning*, *Alert*, *Unknown*).
Number of VMs is out of allowed range	An alarm is triggered if the number of running, powered off or suspended VMs on the ESXi host is above or below the specified threshold value. This type of alarm can be configured if it is necessary to limit the number of VMs running on the ESXi host at the same time to avoid the host overload.
Power or connection state changes	An alarm is triggered if the host state reports to be equal or not equal to a specific state value (for example, if the ESXi host is not responding).
Resource usage	An alarm is triggered if the specified counter is above or below the specified threshold value (for example, if the CPU usage exceeds 75%).

Resource Pool

Rule Type	Description
Event-based rule	An alarm is triggered if some event is generated on a resource pool.
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.
Resource usage	An alarm is triggered if the specified counter is above or below the specified value (for example, if the CPU usage exceeds 80%).

Virtual Machine

Rule Type	Description
Event-based rule	An alarm is triggered if some VM-related event is generated (for example, if the MAC address of the VM conflicts with the MAC address of another VM existing in the virtual infrastructure).

Rule Type	Description
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.
Guest disk space	An alarm is triggered if available disk space on guest volumes is above or below the specified threshold value. You can choose to specify the amount of due free space as an absolute value or a relative value. For example, an alarm is triggered if free disk space falls below 1 GB or 10% of total space.
Heartbeat is missing	An alarm is triggered if a monitored virtual machine is not available or overloaded for a specific period of time (for example, if heartbeat is missing for 5 minutes).
Number of running services	[For Windows-based machines] An alarm is triggered if the number of services running on a VM is greater than the specified threshold.
Orphaned Veeam Backup & Replication snapshot	An alarm is triggered if a VM has a snapshot that Veeam Backup & Replication created (to back up, replicate or perform another data protection operation for the VM) but was unable to remove when the operation was over.
Power or connection state changes	An alarm is triggered if the state of the VM reports to be equal or not equal to the specified state value (for example, if the VM is suspended).
Process performance	[For Windows-based machines] An alarm is triggered if the specified counter for a VM process is above or below the specified value (for example, if the CPU usage by a process exceeds 15%).
Process state	[For Windows-based machines] An alarm is triggered if VM process state is equal or not equal to a specific state value (*Terminated*, *Running*).
Resource usage	An alarm is triggered if the specified counter is above or below the specified value (for example, if the CPU ready level exceeds 5%).
Service state	[For Windows-based machines] An alarm is triggered if service state is equal or not equal to a specific state value (*Running*, *Paused*, *Stopped*).

Rule Type	Description
Snapshot age for VM	An alarm is triggered if the current snapshot is older than a specified number of hours. This rule helps monitor forgotten snapshots that are consuming valuable storage space and degrading performance of virtual machines.
Snapshot size for VM	An alarm is triggered if the size of the VM snapshot is above or below the specified threshold value. You can choose to specify the size of the snapshot as an absolute value or a relative value. For example, an alarm is triggered if the snapshot size exceeds 5 GB or 10% of total available disk space.
VM snapshots number has exceeded the configured threshold	An alarm is triggered if the number of snapshots created for the VM is greater than the specified threshold.
VMware VM tools state changes	An alarm is triggered if the state of the VMware Tools reports to be equal or not equal to the specified state value (for example, if the VMware Tools is out of date).
VMs with no restore points	An alarm is triggered if the age of the latest backup or replica restore point for the VM has exceeded the threshold (that is, if there are no restore points for the specified RPO period).

Datastore

Rule Type	Description
Datastore is running out of free space	An alarm is triggered if free space on the datastore is above or below the specified threshold value. You can choose to specify the free space threshold as an absolute value or a relative value. For example, an alarm is triggered if the datastore space falls below 10 GB or 15% of total space.
Datastore performance	An alarm is triggered if a performance counter of a datastore is above or below the specified threshold value.
Datastore provisioned space	An alarm is triggered if the provisioned disk space is above or below the specified threshold value. You can select to specify the threshold as an absolute value or a relative value. For example, an alarms is triggered if the provisioned disk space exceeds 500 GB or 400% compared to the datastore capacity.

Rule Type	Description
Event-based rule	An alarm is triggered if some datastore-related event is generated.
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.
Power or connection state changes	An alarm is triggered if the state of the datastore reports to be equal or not equal to the specified state value (for example, if the datastore is not accessible).
Resource usage	An alarm is triggered if the specified counter is above or below the specified threshold value (for example, if the datastore I\O threshold is violated).

Any Object

Rule Type	Description
Event-based rule	An alarm is triggered if some event is generated on any object in the infrastructure.
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.

vCloud Director vApp

Rule Type	Description
Event-based rule	An alarm is triggered if some vApp-related event in generated.
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.
Resource usage	An alarm is triggered if the specified counter is above or below the specified value (for example, if the storage usage exceeds 80%).
System health status change	An alarm is triggered if the object health state changes.

Rule Type	Description
vApp runtime lease timeout	An alarm is triggered in N days after the vApp runtime lease has expired.
vApp storage lease timeout	An alarm is triggered in N days after the vApp storage lease has expired.
vCloud Director object task status	An alarm is triggered if the vApp state reports to be equal or not equal to a specific state value (for example, if warnings are registered for the vApp).

vCloud Director Organization

Rule Type	Description
Event-based rule	An alarm is triggered if some event is generated on the organization.
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.
Organization VDC blocking task number	An alarm is triggered if the number of pending blocking tasks has exceeded the specified threshold.
Organization VDC blocking task timeout	An alarm is triggered in N minutes after the blocking tasks has expired.
System health state change	An alarm is triggered if the object health state changes.
vCloud Director object task status	An alarm is triggered if the organization state reports to be equal or not equal to a specific state value (for example, if warnings are registered for the organization).

vCloud Director Org VDC

Rule Type	Description
Event-based rule	An alarm is triggered if some event is generated on the organization VDC.

Rule Type	Description
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.
Network pool is running out of available IP addresses	An alarm is triggered if the number of remaining IP addresses is above or below the specified threshold value. You can select to specify the threshold as an absolute value or a relative value. For example, if the number of remaining IP addresses is lower than 5 or 10% of the total number for the organization VDC network.
Resource usage	An alarm is triggered if the specified counter is above or below the specified value (for example, if the CPU ready level exceeds 5%).
System health status change	An alarm is triggered if the object health state changes.
vCloud Director object task status	An alarm is triggered if the organization VDC state reports to be equal or not equal to a specific state value (for example, if warnings are registered for the organization VDC).

vCloud Director Provider VDC

Rule Type	Description
Event-based rule	An alarm is triggered if some event is generated on the provider VDC.
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.
Resource usage	An alarm is triggered if the specified counter is above or below the specified value (for example, if the storage usage exceeds 80%).
System health status change	An alarm is triggered if the object health state changes.
vCloud Director object task status	An alarm is triggered if the provider VDC state reports to be equal or not equal to a specific state value (for example, if warnings are registered for the provider VDC).

Alarm Rules for Microsoft Hyper-V

Veeam ONE offers the following types of alarm rules for Microsoft Hyper-V infrastructure objects.

Host

Rule Type	Description
Event-based rule	An alarm is triggered if some host-related event is generated.
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.
Power or connection state changes	An alarm is triggered if the host state reports to be equal or not equal to a specific state value (for example, if the Hyper-V host is not responding).
Service state	An alarm is triggered if host service state is equal or not equal to a specified state value (*Running*, *Paused*, *Stopped*).
Resource usage	An alarm is triggered if the specified counter is above or below the specified threshold value (for example, if the Total Run Time exceeds 75%).
Service state	An alarm is triggered if service state is equal or not equal to a specific state value (*Running*, *Paused*, *Stopped*).

Virtual Machine

Rule Type	Description
Checkpoint age for Hyper-V VM has exceeded the configured threshold	An alarm is triggered if the current checkpoint is older than a specified number of hours. This rule helps monitor forgotten checkpoints that are consuming valuable storage space and degrading performance of virtual machines.

Rule Type	Description
Checkpoint size for Hyper-V VM is out of allowed range	An alarm is triggered if the size of the VM checkpoint is above or below the specified threshold value. You can choose to specify the size of the checkpoint as an absolute value or a relative value (for example, if the checkpoint size exceeds 10% of total available disk space). For example, if the checkpoint size exceeds 5 GB or 10% of total disk space.
Event-based rule	An alarm is triggered if some VM-related event is generated (for example, if the MAC address of the VM conflicts with the MAC address of another VM existing in the virtual infrastructure).
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.
Guest volumes are running out of free disk space	An alarm is triggered if available disk space on guest volumes is below the specified threshold value. You can choose to specify the amount of due free space as an absolute value or a relative value. For example, alarm triggers if free disk space falls below 1 GB or 10% of total space.
Number of running services	[For Windows-based machines] An alarm is triggered if the number of services running on a VM is greater than the specified threshold.
Process performance	[For Windows-based machines] An alarm is triggered if the specified counter for a VM process is above or below the specified value (for example, if the CPU usage by a process exceeds 15%).
Process state	[For Windows-based machines] An alarm is triggered if VM process state is equal or not equal to a specific state value (*Terminated*, *Running*).
Resource usage	An alarm is triggered if the specified counter is above or below the specified threshold value (for example, if the Guest Run Time level exceeds 5%).
Service state	[For Windows-based machines] An alarm is triggered if service state is equal or not equal to a specific state value (*Running*, *Paused*, *Stopped*).

Rule Type	Description
VMs with no restore points	An alarm is triggered if the age of the latest backup or replica restore point for the VM has exceeded the threshold (that is, if there are no restore points for the specified RPO period).
Power or connection state changes	An alarm is triggered if the VM state reports to be equal or not equal to a specific state value (for example, if the VM is not responding).

Cluster

Rule Type	Description
Event-based rule	An alarm will be triggered if some cluster-related event is generated.
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.

Cluster Shared Volumes (CSV)

Rule Type	Description
CSV is running out of free space	An alarm is triggered if free space on the CSV is above or below the specified threshold value. You can choose to specify the free space threshold as an absolute value or a relative value. For example, an alarm is triggered if the CSV space is below 10 GB or 15% of total space.
Event-based rule	An alarm is triggered if some event occurs on Cluster Shared Volumes level.
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.
Resource usage	An alarm is triggered if the specified counter is above or below the specified threshold value (for example, if read latency exceeds 40 milliseconds).

Local Storage

Rule Type	Description
Event-based rule	An alarm is triggered if some storage-related event is generated.
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.
Hyper-V Datastore is running out of free space	An alarm is triggered if free space on the datastore is above or below the specified threshold value. You can choose to specify the free space threshold as an absolute value or a relative value. For example, an alarm is triggered if the datastore space is below 10 GB or 15% of total space.
Resource usage	An alarm will be triggered if the specified counter is above or below the specified threshold value (for example, the average time of disk read exceeds 40 milliseconds).

Any Object

Rule Type	Description
Event-based rule	An alarm is triggered if some event is generated on any object.
Existing alarm	An alarm is triggered if the status of another alarm specified in the settings is changed.
Process state	An alarm is triggered if the state of the specified process reports to be equal or not equal to a specific state value (*Terminated*, *Running*).
Service state	An alarm is triggered if the state of the specified service reports to be equal or not equal to a specific state value for a specified time (for example, if a service is paused for 10 minutes).

Alarm Rules for Veeam Backup & Replication

Veeam ONE offers the following types of alarm rules for Veeam Backup & Replication infrastructure objects.

Enterprise Manager

Rule Type	Description
Event-based rule	An alarm is triggered if some Veeam Backup & Replication event is generated for the Veeam Backup Enterprise Manager.
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.
Power or connection state changes	An alarm is triggered if the state of Veeam Backup Enterprise Manager is equal or not equal to the specified value (for example, if connection to the Enterprise Manager is lost).

Backup Server

Rule Type	Description
CDP VM SLA %	An alarm is triggered if CDP policy SLA is below the specified threshold.
Backup Copy RPO	An alarm is triggered if no backup copy VM restore points were created during the specified period.
Cloud instance RPO	An alarm is triggered if no cloud instance restore points were created during the specified period.
Incremental backup size	An alarm is triggered if size of one or more increments has exceeded the specified threshold.
Disabled job	An alarm is triggered if the time during which a job was disabled has exceeded the specified threshold.
Job/Policy status	An alarm is triggered if the job or policy status is equal or not equal to the specified value.

Rule Type	Description
Plug-in backup data collection failure	An alarm is triggered if the Veeam ONE server fails to collect plug-in backup data.
Event-based rule	An alarm is triggered if some Veeam Backup & Replication event is generated for the backup server.
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.
Job duration exceeded the allowed time period	An alarm is triggered if duration of a job exceeds the threshold specified in minutes.
Power or connection state changes	An alarm is triggered if the state of Veeam Backup & Replication server is equal or not equal to the specified value (for example, if connection to the backup server is lost).
Unusual job duration	An alarm is triggered if duration of a job session is above specified percentage based on the set of latest job sessions.
Backup security and compliance	An alarm is triggered if the defined best practices statuses are detected.
Disabled malware detection	An alarm is triggered if disabled malware is detected.
Potential malware activity	An alarm is triggered if suspicious or infected malware is detected on your data.
VM Backup RPO (oVirt KVM, Proxmox, AHV)	An alarm is triggered if no VM (oVirt KVM, Proxmox, AHV) restore points were created during the specified period.

Repository

Rule Type	Description
Event-based rule	An alarm is triggered if some Veeam Backup & Replication event is generated for the repository.
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.

Rule Type	Description
Immutability state	An alarm is triggered if immutability is disabled for repositories or repository extents.
Out-of-date state	An alarm is triggered if Veeam Backup & Replication software components installed on the repository server are out of date.
Power or connection state changes	An alarm is triggered if the state of the backup repository is equal or not equal to the specified value (for example, if connection to the repository is lost).
Repository server is running out of free space	An alarm is triggered if free space on the repository is above or below the specified threshold value. You can select to specify the free space threshold as an absolute value or a relative value. For example, an alarm is triggered if the storage space is below 10 GB or 15% of total space.

Proxy

Rule Type	Description
CDP Proxy Cache Usage	An alarm is triggered if the CDP cache usage is above the specified threshold.
Event-based rule	An alarm is triggered if some Veeam Backup & Replication event is generated for the proxy server.
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.
Out-of-date state	An alarm is triggered if Veeam Backup & Replication software components installed on the proxy server are out of date.
Power or connection state changes	An alarm is triggered if the state of proxy server is equal or not equal to the specified value (for example, if connection to the proxy server is lost).

WAN Accelerator

Rule Type	Description
Event-based rule	An alarm is triggered if some Veeam Backup & Replication event is generated for the WAN accelerator.
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.
Out-of-date state	An alarm is triggered if Veeam Backup & Replication software components installed on the WAN accelerator server are out of date.
Power or connection state changes	An alarm is triggered if the state of the WAN accelerator is equal or not equal to the specified value (for example, if connection to the WAN accelerator is lost).

Tape Server

Rule Type	Description
Event-based rule	An alarm is triggered if some Veeam Backup & Replication event is generated for the tape server.
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.
Out-of-date state	An alarm is triggered if Veeam Backup & Replication software components installed on the tape server are out of date.
Power or connection state changes	An alarm is triggered if the state of the backup repository is equal or not equal to the specified value (for example, if connection to the server is lost).

Cloud Repository

Rule Type	Description
Cloud repository lease expiration	An alarm is triggered if cloud repository lease time will expire in the specified number of days.

Rule Type	Description
Event-based rule	An alarm is triggered if some Veeam Backup & Replication event is generated for the cloud repository.
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.
Number of VMs stored in repository	An alarm is triggered if the number of VMs stored in the backup repository has exceeded the specified threshold.
Repository server is running out of free space	An alarm is triggered if free space on the repository is above or below the specified threshold value. You can select to specify the free space threshold as an absolute value (for example, if the storage space should not fall below 10 GB) or a relative value (for example, if the free space should not fall below 15% of total space).

Cloud Gateway

Rule Type	Description
Event-based rule	An alarm is triggered if some Veeam Backup & Replication event is generated for the cloud gateway.
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.
Out-of-date state	An alarm is triggered if Veeam Backup & Replication software components installed on the cloud gateway server are out of date.
Power or connection state changes	An alarm is triggered if the state of the backup repository is equal or not equal to the specified value (for example, if connection to the cloud gateway is lost).

Enterprise Application

Rule Type	Description
Event-based rule	An alarm is triggered if some Veeam Backup & Replication event is generated for the application.

Rule Type	Description
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.
Application backup RPO	An alarm is triggered if no application database backups were created during the specified period.

Alarm Rules for Veeam Backup for Microsoft 365

Veeam ONE offers the following types of alarm rules for Veeam Backup for Microsoft 365 infrastructure objects.

Veeam Backup for Microsoft 365 Server

Rule Type	Description
Job disabled	An alarm is triggered if the time during which a job was disabled has exceeded the specified threshold.
Job status	An alarm is triggered if the job status is equal or not equal to the specified value.
Event-based rule	An alarm is triggered if some Veeam Backup for Microsoft 365 event is generated for the backup server.
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.
Organization without backups	An alarm is triggered if no backups were created for a Microsoft 365 organization during the specified RPO interval.
Power or connection state changes	An alarm is triggered if the state of Veeam Backup for Microsoft 365 server is equal or not equal to the specified value (for example, if connection to the server is lost).
Restore activity	An alarm is triggered if Veeam Backup for Microsoft 365 restore session is initiated for the defined object type.
Unusual job duration	An alarm is triggered if duration of a job session is above specified percentage based on the set of latest job sessions.
Veeam Backup for Microsoft 365 Service state	An alarm is triggered if the Veeam Backup for Microsoft 365 Service state is equal or not equal to the specified value.

Backup Proxy

Rule Type	Description
Event-based rule	An alarm is triggered if some Veeam Backup for Microsoft 365 event is generated for the proxy server.
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.
Power or connection state changes	An alarm is triggered if the state of proxy server is equal or not equal to the specified value (for example, if connection to the proxy server is lost).
Maintenance mode	An alarm is triggered if backup proxy maintenance mode is enabled.

Backup Repository

Rule Type	Description
Event-based rule	An alarm is triggered if some Veeam Backup & Replication event is generated for the repository.
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.
Backup repository is running out of free space	An alarm is triggered if free space on the repository is above or below the specified threshold value. You can select to specify the free space threshold as an absolute value or a relative value. For example, an alarm is triggered if the storage space is below 10 GB or 15% of total space.

Rules for Internal Alarms

Veeam ONE offers the following types of rules for internal alarms:

Rule Type	Description
Audit log free space	An alarm is triggered if free disk space allocated to an audit log is below or beyond a specific value (for example, if free space is below 15%).
Database cleanup queue growth	An alarm is triggered when object information is deleted faster than the Veeam ONE server can process.
Event-based rule	An alarm is triggered if some Veeam Backup & Replication event is generated for the Veeam Backup Enterprise Manager.
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.
Resource usage	An alarm is triggered if the specified counter is above or below the specified threshold value (for example, if CPU usage exceeds 90%).
Staging data processing state	An alarm is triggered if the age of the oldest staging data file reaches the specified value.
Recon Scanner threat detection	An alarm is triggered if Recon Scanner raises an alert based on one or more suspicious behaviors.
Veeam ONE Web Client task state	An alarm is triggered if Veeam ONE Web Client task state is equal or not equal to a specific state value (*Failed*, *Warning*, *Success*).

Remediation Actions

This section lists alarms with predefined remediation actions.

Alarm Name	Infrastructure	Resolve Actions	Action Type	Description
Job disabled	Veeam Backup & Replication	Enable backup job	Default action for warning severity	Veeam ONE runs the script that enables the disabled job.
Suspicious incremental backup size	Veeam Backup & Replication	Add job to SureBackup job and start verification	Extra action	Veeam ONE runs the script that starts a SureBackup job to check the restore point containing the suspicious increment.
Veeam Backup & Replication HA cluster primary node state	Veeam Backup & Replication	Perform failover	Default action for error severity	Veeam ONE initiates failover on the high availablity cluster.
Latest snapshot age	VMware vSphere	Delete snapshot	Default action for warning severity	Veeam ONE runs the script that deletes the latest snapshot.
		Delete all snapshots	Extra action	Veeam ONE runs the script that deletes all snapshots in the current snapshot branch.
Latest snapshot size	VMware vSphere	Delete snapshot	Default action for error severity	Veeam ONE runs the script that deletes the latest snapshot.
		Delete all snapshots	Extra action	Veeam ONE runs the script that deletes all snapshots in the current snapshot branch.
Too many snapshots on the VM	VMware vSphere	Delete snapshot	Default action for error severity	Veeam ONE runs the script that deletes the latest snapshot.
		Delete all snapshots	Extra action	Veeam ONE runs the script that deletes all snapshots in the current snapshot branch.

Alarm Name	Infrastructure	Resolve Actions	Action Type	Description
Orphaned VM backup snapshot	VMware vSphere	Delete orphaned snapshot	Default action for error severity	Veeam ONE runs the script that deletes the snapshot left by backup or replication job.
Potential infrastructure malware activity	VMware vSphere	Disable VM Network	Default action for error severity	Veeam ONE runs the script that disables the VM network.
		Switch VM Network	Additional configuration option	Veeam ONE runs the script that switches the VM network.
VM power status	VMware vSphere	Power on VM	Default action for error severity	Veeam ONE runs the script that powers on the VM.
VM with no backups	VMware vSphere	Add VM to backup job	Default action for warning severity	Veeam ONE runs the script that adds the VM to an existing backup job. For this action you must specify a backup server and a job to which the VM must be added. You can suppress this action if the VM and a target repository do not share location. To do that, select the Suppress if original VM location does not match target repository location check box.
		Add VM to backup job and run	Extra action	Veeam ONE runs the script that adds the VM to an existing backup job and starts that job. For this action you must specify a backup server and a job to which the VM must be added. You can suppress this action if the VM and a target repository do not share location. To do that, select the Suppress if original VM location does not match target repository location check box.

Alarm Name	Infrastructure	Resolve Actions	Action Type	Description
		Run parent backup job	Extra action	Veeam ONE runs the script that starts an existing backup job into which the VM is included. The latest session of the job must have the *Success* status.
		Start Quick backup	Extra action	Veeam ONE runs the script that starts a quick backup job for the VM. For this action you must specify backup server. For details on quick backup, see Quick Backup.
		Start VeeamZIP	Extra action	Veeam ONE runs the script that creates an independent full backup file. For this action you must specify a backup server and a backup repository. You can suppress this action if the VM and a target repository do not share location. To do that, select the Suppress if original VM location does not match target repository location check box. For details on VeeamZIP, see VeeamZIP.
VM with no replica	VMware vSphere	Add VM to replication job	Default action for warning severity	Veeam ONE runs the script that adds the VM to an existing replication job. For this action you must specify a backup server and a job to which the VM must be added. You can suppress this action if the VM and a target repository do not share location. To do that, select the Suppress if original VM location does not match target repository location check box.

Alarm Name	Infrastructure	Resolve Actions	Action Type	Description
		Add VM to replication job and run	Extra action	Veeam ONE runs the script that adds the VM to an existing replication job and starts that job. For this action you must specify a backup server and a job to which the VM must be added. You can suppress this action if the VM and a target repository do not share location. To do that, select the Suppress if original VM location does not match target repository location check box.
		Run parent replication job	Extra action	Veeam ONE runs the script that starts an existing replication job into which the VM is included. The latest session of the job must have the *Success* status.
		Start Quick backup	Extra action	Veeam ONE runs the script that starts a quick backup job for the VM. For this action you must specify backup server. For details on quick backup, see Quick Backup.
		Start VeeamZIP	Extra action	Veeam ONE runs the script that creates an independent full backup file. For this action you must specify a backup server and a backup repository. You can suppress this action if the VM and a target repository do not share location. To do that, select the Suppress if original VM location does not match target repository location check box. For details on VeeamZIP, see VeeamZIP.

Alarm Name	Infrastructure	Resolve Actions	Action Type	Description
Latest checkpoint age	Microsoft Hyper-V	Delete checkpoint	Default action for warning severity	Veeam ONE runs the script that deletes the latest checkpoint.
		Delete checkpoint subtree	Extra action	Veeam ONE runs the script that deletes all checkpoints in the current subtree.
Latest checkpoint size	Microsoft Hyper-V	Delete checkpoint	Default action for error severity	Veeam ONE runs the script that deletes the latest checkpoint.
		Delete checkpoint subtree	Extra action	Veeam ONE runs the script that deletes all checkpoints in the current subtree.
VM power status	Microsoft Hyper-V	Power on VM	Default action for error severity	Veeam ONE runs the script that powers on the VM.
VM with no backup	Microsoft Hyper-V	Add VM to backup job	Default action for warning severity	Veeam ONE runs the script that adds the VM to an existing backup job. For this action you must specify a backup server and a job to which the VM must be added. You can suppress this action if the VM and a target repository do not share location. To do that, select the Suppress if original VM location does not match target repository location check box.

Alarm Name	Infrastructure	Resolve Actions	Action Type	Description
		Add VM to backup job and run	Extra action	Veeam ONE runs the script that adds the VM to an existing backup job and starts that job. For this action you must specify a backup server and a job to which the VM must be added. You can suppress this action if the VM and a target repository do not share location. To do that, select the Suppress if original VM location does not match target repository location check box.
		Run parent backup job	Extra action	Veeam ONE runs the script that starts an existing backup job into which the VM is included. The latest session of the job must have the *Success* status.
		Start Quick backup	Extra action	Veeam ONE runs the script that starts a quick backup job for the VM. For this action you must specify backup server. For details on quick backup, see Quick Backup.
		Run VeeamZIP	Extra action	Veeam ONE runs the script that creates an independent full backup file. For this action you must specify a backup server and a job to which the VM must be added. You can suppress this action if the VM and a target repository do not share location. To do that, select the Suppress if original VM location does not match target repository location check box. For details on VeeamZIP, see VeeamZIP.

Alarm Name	Infrastructure	Resolve Actions	Action Type	Description
VM with no replica	Microsoft Hyper-V	Add VM to replication job	Default action for warning severity	Veeam ONE runs the script that adds the VM to an existing replication job. For this action you must specify a backup server and a job to which the VM must be added. You can suppress this action if the VM and a target repository do not share location. To do that, select the Suppress if original VM location does not match target repository location check box.
		Add VM to replication job and run	Extra action	Veeam ONE runs the script that adds the VM to a existing replication job and starts that job. For this action you must specify a backup server and a job to which the VM must be added. You can suppress this action if the VM and a target repository do not share location. To do that, select the Suppress if original VM location does not match target repository location check box.
		Run parent replication job	Extra action	Veeam ONE runs the script that starts an existing replication job into which the VM is included. The latest session of the job must have the *Success* status.
		Start Quick backup	Extra action	Veeam ONE runs the script that starts a quick backup job for the VM. For this action you must specify backup server. For details on quick backup, see Quick Backup.

Alarm Name	Infrastructure	Resolve Actions	Action Type	Description
		Run VeeamZIP	Extra action	Veeam ONE runs the script that creates an independent full backup file. For this action you must specify a backup server and a job to which the VM must be added. You can suppress this action if the VM and a target repository do not share location. To do that, select the Suppress if original VM location does not match target repository location check box. For details on VeeamZIP, see VeeamZIP.

Appendices

This section provides advanced configuration options for Veeam ONE. It includes guidance on database creation, data collection, certificate usage, scheduling scripts, settings utility, and grouping expressions.

Creating Veeam ONE Database with SQL Script

In some circumstances, it might be undesired to create the Veeam ONE database automatically, using the **Veeam ONE Setup** wizard. For example, Veeam ONE components and the Microsoft SQL Server can be hosted on different systems, and you do not have sufficient permissions on the Microsoft SQL Server to create the database. In this case, you can use a SQL script to create the Veeam ONE database on a Microsoft SQL Server. The script is included with the Veeam ONE installation image.

To create the Veeam ONE database with the SQL script, perform the steps described below. Note that the database must be created before you start installation of Veeam ONE components.

Step 1. Locate the SQL Script

Download the Veeam ONE installation image and burn it to a blank CD/DVD or mount the image using disk image emulation software. If you are working with a virtual machine, use built-in tools of the virtualization management software to mount the installation image to the virtual machine.

In Windows Explorer, right-click the drive with the image, select **Open** and go to the `<CD Drive>\Addins\SQLScript` directory. Copy the `VeeamONE.sql` file to the location from which it can be accessed or run.

Step 2. Create the Veeam ONE Database

Connect to the necessary Microsoft SQL Server with Microsoft SQL Server Management Studio and create a new database (for example, *VeeamOne*).

Step 3. Run the SQL Script Against the Veeam ONE Database

Execute the `VeeamONE.sql` script against the Veeam ONE database in Microsoft SQL Server Management Studio.

Alternatively, you can execute the script using the **sqlcmd** utility. In the command prompt, run the command of the following form:

```
sqlcmd -S localhost\VEEAMSQL2017 -d VeeamOne -E -i "E:\Addins\SQLScript\VeeamONE.sql"
```

The following command-line options are used to run the script:

Option	Description
-S	Specifies the SQL Server instance to which **sqlcmd** connects.
-d	Specifies the name of the database against which the script is executed.

Option	Description
-E	Instructs **sqlcmd** to connect to the SQL Server Database Engine using Windows Integrated Security.
-i	Specifies the full path to the script file for execution.

Step 4. Grant Database Permissions

Create a Microsoft SQL Server account with required permissions. For details, see Connection to Microsoft SQL Server.

Data Collection Modes

Data collection mode determines what metrics Veeam ONE will collect, and specifies the product configuration in a number of areas. Choosing an appropriate data collection mode allows you to optimize monitoring and reporting performance and improve user experience in Veeam ONE.

The Data Collection Mode is configured during deployment and can be modified after deployment using the Veeam ONE Settings Utility.

Settings

Changing between data collection modes affects the following Veeam ONE settings.

Configuration Option	Description	Veeam backup data and virtual infrastructure	Veeam backup data and large-scale virtual infrastructure	Veeam Backup Data Only
VMware real-time performance	Timeout for collecting VMware vSphere real-time performance data.	30 minutes	30 minutes	N/A
	Sampling renewal interval for real-time counters.	20 seconds	300 seconds (5 minutes)	N/A
VMware historical performance	Sampling renewal interval for historical counters (older than one hour).	5 minutes	30 minutes	5 minutes
	Sampling renewal interval for historical counters (older than one week).	2 hours	2 hours	2 hours
Min tree check interval	Updating the object inventory tree in Veeam ONE Client.	10 seconds	1 minute	10 seconds
Page update delay	Loading data after choosing an object in the object inventory tree in Veeam ONE Client.	0.5 second	1.5 second	0.5 second
Get VM snapshot timeout	Timeout for collecting data about VM snapshot files from datastores.	900 seconds (15 minutes)	3600 seconds (1 hour)	900 seconds (15 minutes)

Configuration Option	Description	Veeam backup data and virtual infrastructure	Veeam backup data and large-scale virtual infrastructure	Veeam Backup Data Only
Virtual machines files data collection	Collecting information about VM files (for the *Active Snapshots* and *Garbage Files* reports).	Yes	No	No
Hyper-V real-time performance	Timeout for collecting Microsoft Hyper-V real-time performance data.	30 minutes	30 minutes	N/A
	Sampling renewal interval for real-time counters.	60 seconds	300 seconds (5 minutes)	N/A

Collected Performance Metrics

Data collection mode defines what performance metrics must be collected.

Performance Metric	Object Type	Veeam backup data and virtual infrastructure	Veeam backup data and large-scale virtual infrastructure	Veeam Backup Data Only
Available Memory	Backup Enterprise Manager	Yes	Yes	Yes
CPU Usage	Backup Enterprise Manager	Yes	Yes	Yes
Disk Bytes/sec	Backup Enterprise Manager	Yes	Yes	Yes
Memory Usage	Backup Enterprise Manager	Yes	Yes	Yes
Network Bytes Sent/sec	Backup Enterprise Manager	Yes	Yes	Yes
Available Memory	Backup Server	Yes	Yes	Yes
CPU Usage	Backup Server	Yes	Yes	Yes
Disk Bytes/sec	Backup Server	Yes	Yes	Yes

Performance Metric	Object Type	Veeam backup data and virtual infrastructure	Veeam backup data and large-scale virtual infrastructure	Veeam Backup Data Only
Memory Usage	Backup Server	Yes	Yes	Yes
Network Bytes Sent/sec	Backup Server	Yes	Yes	Yes
Available Memory	Backup Repository	Yes	Yes	Yes
Backup Repository Capacity	Backup Repository	Yes	Yes	Yes
CPU Usage	Backup Repository	Yes	Yes	Yes
Disk Bytes/sec	Backup Repository	Yes	Yes	Yes
Memory Usage	Backup Repository	Yes	Yes	Yes
Network Bytes Sent/sec	Backup Repository	Yes	Yes	Yes
Repository File Backups Size	Backup Repository	Yes	Yes	Yes
Repository Image Backups Size	Backup Repository	Yes	Yes	Yes
Repository Used Space	Backup Repository	Yes	Yes	Yes
Slot Capacity	Backup Repository	Yes	Yes	Yes
Used Slots	Backup Repository	Yes	Yes	Yes
Available Memory	Backup Proxy	Yes	Yes	Yes
CPU Usage	Backup Proxy	Yes	Yes	Yes
CDP Proxy Cache Size	Backup Proxy	Yes	Yes	Yes

Performance Metric	Object Type	Veeam backup data and virtual infrastructure	Veeam backup data and large-scale virtual infrastructure	Veeam Backup Data Only
CDP Proxy Cache Usage	Backup Proxy	Yes	Yes	Yes
CDP Proxy Cache Usage %	Backup Proxy	Yes	Yes	Yes
Disk Bytes/sec	Backup Proxy	Yes	Yes	Yes
Memory Usage	Backup Proxy	Yes	Yes	Yes
Network Bytes Sent/sec	Backup Proxy	Yes	Yes	Yes
Slot Capacity	Backup Proxy	Yes	Yes	Yes
Used Slots	Backup Proxy	Yes	Yes	Yes
Available Memory	WAN Accelerator	Yes	Yes	Yes
CPU Usage	WAN Accelerator	Yes	Yes	Yes
Disk Bytes/sec	WAN Accelerator	Yes	Yes	Yes
Memory Usage	WAN Accelerator	Yes	Yes	Yes
Network Bytes Sent/sec	WAN Accelerator	Yes	Yes	Yes
Available Memory	Tape Server	Yes	Yes	Yes
CPU Usage	Tape Server	Yes	Yes	Yes
Disk Bytes/sec	Tape Server	Yes	Yes	Yes
Memory Usage	Tape Server	Yes	Yes	Yes
Network Bytes Sent/sec	Tape Server	Yes	Yes	Yes

Performance Metric	Object Type	Veeam backup data and virtual infrastructure	Veeam backup data and large-scale virtual infrastructure	Veeam Backup Data Only
External Repository Used Space	External Repository Used Space	Yes	Yes	Yes
Object Storage Repository Used Space	Object Storage Repository Used Space	Yes	Yes	Yes
Storage Usage	VMware Cloud Director Organization VDC	Yes	Yes	No
CPU Usage	VMware Cloud Director Provider VDC	Yes	Yes	No
Memory Usage	VMware Cloud Director Provider VDC	Yes	Yes	No
Storage Space Usage	VMware Cloud Director Provider VDC	Yes	No	No
Storage Space Usage Pct	VMware Cloud Director Provider VDC	Yes	Yes	No
Backup Job Memory Usage	Veeam Backup & Replication Objects	Yes	Yes	Yes
Backup Job Processor Usage	Veeam Backup & Replication Objects	Yes	Yes	Yes
Adapter I/O	ESXi Host	Yes	No	No
Adapter Read I/O	ESXi Host	Yes	No	No
Adapter Read Latency	ESXi Host	Yes	No	No
Adapter Read Rate	ESXi Host	Yes	No	No

Performance Metric	Object Type	Veeam backup data and virtual infrastructure	Veeam backup data and large-scale virtual infrastructure	Veeam Backup Data Only
Adapter Write I/O	ESXi Host	Yes	No	No
Adapter Write Latency	ESXi Host	Yes	No	No
Adapter Write Rate	ESXi Host	Yes	No	No
Average CPU Ready	ESXi Host	Yes	Yes	No
CPU Usage	ESXi Host	Yes	Yes	No
CPU Usage MHz	ESXi Host	Yes	Yes	No
Disk/ESXi: Datastore Bus Resets	ESXi Host	Yes	Yes	No
Disk/ESXi: Datastore Command Aborts	ESXi Host	Yes	Yes	No
Disk/ESXi: Datastore Highest Latency	ESXi Host	Yes	Yes	No
Disk/ESXi: Datastore I/O	ESXi Host	Yes	Yes	No
Disk/ESXi: Datastore Latency Observed by VMs	ESXi Host	Yes	No	No
Disk/ESXi: Datastore Maximum Queue Depth	ESXi Host	Yes	No	No
Disk/ESXi: Datastore Read I/O	ESXi Host	Yes	Yes	No
Disk/ESXi: Datastore Read Latency	ESXi Host	Yes	Yes	No
Disk/ESXi: Datastore Read Rate	ESXi Host	Yes	Yes	No

Performance Metric	Object Type	Veeam backup data and virtual infrastructure	Veeam backup data and large-scale virtual infrastructure	Veeam Backup Data Only
Disk/ESXi: Datastore Usage	ESXi Host	Yes	Yes	No
Disk/ESXi: Datastore Write I/O	ESXi Host	Yes	Yes	No
Disk/ESXi: Datastore Write Latency	ESXi Host	Yes	Yes	No
Disk/ESXi: Datastore Write Rate	ESXi Host	Yes	Yes	No
Memory Active	ESXi Host	Yes	Yes	No
Memory Baloon	ESXi Host	Yes	Yes	No
Memory Compressed	ESXi Host	Yes	No	No
Memory Consumed	ESXi Host	Yes	Yes	No
Memory Latency	ESXi Host	Yes	No	No
Memory Overhead	ESXi Host	Yes	No	No
Memory Pressure	ESXi Host	Yes	Yes	No
Memory Shared	ESXi Host	Yes	No	No
Memory Shared Common	ESXi Host	Yes	No	No
Memory Swap Used	ESXi Host	Yes	Yes	No
Memory Usage	ESXi Host	Yes	Yes	No
Network Receive Rate	ESXi Host	Yes	Yes	No

Performance Metric	Object Type	Veeam backup data and virtual infrastructure	Veeam backup data and large-scale virtual infrastructure	Veeam Backup Data Only
Network Transmit Rate	ESXi Host	Yes	Yes	No
Network Usage	ESXi Host	Yes	Yes	No
Packet Receive Errors	ESXi Host	Yes	No	No
Packet Transmit Errors	ESXi Host	Yes	No	No
Path I/O	ESXi Host	Yes	No	No
Path Read I/O	ESXi Host	Yes	No	No
Path Read Latency	ESXi Host	Yes	No	No
Path Read Rate	ESXi Host	Yes	No	No
Path Write I/O	ESXi Host	Yes	No	No
Path Write Latency	ESXi Host	Yes	No	No
Path Write Rate	ESXi Host	Yes	No	No
Power Usage	ESXi Host	Yes	No	No
Receive Packets Dropped	ESXi Host	Yes	No	No
Received Packets per Second	ESXi Host	Yes	No	No
Swap In Rate	ESXi Host	Yes	No	No
Swap Out Rate	ESXi Host	Yes	No	No
Total Errors	ESXi Host	Yes	No	No
Total Packets Dropped	ESXi Host	Yes	No	No

Performance Metric	Object Type	Veeam backup data and virtual infrastructure	Veeam backup data and large-scale virtual infrastructure	Veeam Backup Data Only
Transmit Packets Dropped	ESXi Host	Yes	No	No
Transmitted Packets per Second	ESXi Host	Yes	No	No
VM Heartbeat	ESXi Host	Yes	Yes	No
Average CPU Idle All Cores	vSphere Virtual Machine	Yes	No	No
Average CPU Ready All Cores	vSphere Virtual Machine	Yes	Yes	No
Average CPU Standstill All Cores	vSphere Virtual Machine	Yes	No	No
Average CPU Wait All Cores	vSphere Virtual Machine	Yes	No	No
CPU Co-Stop All Cores	vSphere Virtual Machine	Yes	No	No
CPU Usage	vSphere Virtual Machine	Yes	Yes	No
CPU Usage MHz	vSphere Virtual Machine	Yes	Yes	No
Datastore Bus Resets	vSphere Virtual Machine	Yes	Yes	No
Datastore Command Aborts	vSphere Virtual Machine	Yes	Yes	No
Datastore Highest Latency	vSphere Virtual Machine	Yes	Yes	No
Datastore I/O	vSphere Virtual Machine	Yes	Yes	No

Performance Metric	Object Type	Veeam backup data and virtual infrastructure	Veeam backup data and large-scale virtual infrastructure	Veeam Backup Data Only
Datastore Read I/O	vSphere Virtual Machine	Yes	Yes	No
Datastore Read Latency	vSphere Virtual Machine	Yes	Yes	No
Datastore Read Rate	vSphere Virtual Machine	Yes	Yes	No
Datastore Usage	vSphere Virtual Machine	Yes	Yes	No
Datastore Write I/O	vSphere Virtual Machine	Yes	Yes	No
Datastore Write Latency	vSphere Virtual Machine	Yes	Yes	No
Datastore Write Rate	vSphere Virtual Machine	Yes	Yes	No
Disk/vSAN: Recovery Write I/O	vSphere Virtual Machine	Yes	No	No
Disk/vSAN: Recovery Write Latency	vSphere Virtual Machine	Yes	No	No
Disk/vSAN: Recovery Write Rate	vSphere Virtual Machine	Yes	No	No
Guest Disk Free Space	vSphere Virtual Machine	Yes	No	No
Guest Disk Usage	vSphere Virtual Machine	Yes	Yes	No
Memory Active	vSphere Virtual Machine	Yes	Yes	No
Memory Baloon	vSphere Virtual Machine	Yes	Yes	No

Performance Metric	Object Type	Veeam backup data and virtual infrastructure	Veeam backup data and large-scale virtual infrastructure	Veeam Backup Data Only
Memory Baloon Percent	vSphere Virtual Machine	Yes	Yes	No
Memory Compressed	vSphere Virtual Machine	Yes	No	No
Memory Consumed	vSphere Virtual Machine	Yes	Yes	No
Memory Entitlement	vSphere Virtual Machine	Yes	No	No
Memory Latency	vSphere Virtual Machine	Yes	No	No
Memory Overhead	vSphere Virtual Machine	Yes	No	No
Memory Saved by Zipping	vSphere Virtual Machine	Yes	No	No
Memory Shared	vSphere Virtual Machine	Yes	No	No
Memory Swapped	vSphere Virtual Machine	Yes	Yes	No
Memory Usage	vSphere Virtual Machine	Yes	Yes	No
Network Receive Rate	vSphere Virtual Machine	Yes	Yes	No
Network Transmit Rate	vSphere Virtual Machine	Yes	Yes	No
Network Usage	vSphere Virtual Machine	Yes	Yes	No
Power Usage	vSphere Virtual Machine	Yes	No	No

Performance Metric	Object Type	Veeam backup data and virtual infrastructure	Veeam backup data and large-scale virtual infrastructure	Veeam Backup Data Only
Process CPU Usage	vSphere Virtual Machine	Yes	Yes	No
Process Memory Usage	vSphere Virtual Machine	Yes	Yes	No
Read I/O	vSphere Virtual Machine	Yes	No	No
Read Latency	vSphere Virtual Machine	Yes	No	No
Read Rate	vSphere Virtual Machine	Yes	No	No
Received Packets per Second	vSphere Virtual Machine	Yes	No	No
Running Services	vSphere Virtual Machine	Yes	Yes	No
Swap In Rate	vSphere Virtual Machine	Yes	No	No
Swap Out Rate	vSphere Virtual Machine	Yes	Yes	No
Transmitted Packets per Second	vSphere Virtual Machine	Yes	No	No
Virtual Disk Provisioned	vSphere Virtual Machine	Yes	Yes	No
Virtual Disk Used	vSphere Virtual Machine	Yes	Yes	No
VM Hearbeat	vSphere Virtual Machine	Yes	Yes	No
Write I/O	vSphere Virtual Machine	Yes	No	No

Performance Metric	Object Type	Veeam backup data and virtual infrastructure	Veeam backup data and large-scale virtual infrastructure	Veeam Backup Data Only
Write Latency	vSphere Virtual Machine	Yes	No	No
Write Rate	vSphere Virtual Machine	Yes	Yes	No
Disk/Datastore: Datastore Bus Resets	vSphere Datastore	Yes	Yes	No
Disk/Datastore: Datastore Command Aborts	vSphere Datastore	Yes	Yes	No
Disk/Datastore: Datastore I/O	vSphere Datastore	Yes	Yes	No
Disk/Datastore: Datastore Provisioned Space	vSphere Datastore	Yes	Yes	No
Disk/Datastore: Datastore Read I/O	vSphere Datastore	Yes	Yes	No
Disk/Datastore: Datastore Read Latency	vSphere Datastore	Yes	Yes	No
Disk/Datastore: Datastore Read Rate	vSphere Datastore	Yes	Yes	No
Disk/Datastore: Datastore Usage	vSphere Datastore	Yes	Yes	No
Disk/Datastore: Datastore Write I/O	vSphere Datastore	Yes	Yes	No
Disk/Datastore: Datastore Write Latency	vSphere Datastore	Yes	Yes	No

Performance Metric	Object Type	Veeam backup data and virtual infrastructure	Veeam backup data and large-scale virtual infrastructure	Veeam Backup Data Only
Disk/Datastore: Datastore Write Rate	vSphere Datastore	Yes	Yes	No
Disk/Datastore: Free Space	vSphere Datastore	Yes	Yes	No
Average Pressure	Hyper-V Host	Yes	Yes	No
Committed Bytes	Hyper-V Host	Yes	No	No
Disk/Host: Avg Disk Queue Length	Hyper-V Host	Yes	Yes	No
Disk/Host: Avg Disk Read Bytes/sec	Hyper-V Host	Yes	Yes	No
Disk/Host: Avg Disk sec/Read	Hyper-V Host	Yes	Yes	No
Disk/Host: Avg Disk sec/Write	Hyper-V Host	Yes	Yes	No
Disk/Host: Avg Disk Usage Bytes/sec	Hyper-V Host	Yes	Yes	No
Disk/Host: Avg Disk Write Bytes/sec	Hyper-V Host	Yes	Yes	No
Guest Run Time	Hyper-V Host	Yes	No	No
Heartbeat	Hyper-V Host	Yes	Yes	No
Heartbeat Status	Hyper-V Host	Yes	Yes	No
Host CPU Wait Time	Hyper-V Host	Yes	Yes	No
Hyper-V Services Memory Consumed	Hyper-V Host	Yes	Yes	No

Performance Metric	Object Type	Veeam backup data and virtual infrastructure	Veeam backup data and large-scale virtual infrastructure	Veeam Backup Data Only
Hyper-V Services Memory Usage	Hyper-V Host	Yes	Yes	No
Hypervisor Run Time	Hyper-V Host	Yes	No	No
Idle Time	Hyper-V Host	Yes	Yes	No
Memory Consumed	Hyper-V Host	Yes	Yes	No
Memory Usage	Hyper-V Host	Yes	Yes	No
Network Bytes Received/sec	Hyper-V Host	Yes	Yes	No
Network Bytes Sent/sec	Hyper-V Host	Yes	Yes	No
Network Bytes Total/sec	Hyper-V Host	Yes	Yes	No
Network Offloaded Connections	Hyper-V Host	Yes	No	No
Network Outbound Errors	Hyper-V Host	Yes	Yes	No
Network Output Queue Length	Hyper-V Host	Yes	Yes	No
Network Packets Received/sec	Hyper-V Host	Yes	No	No
Network Packets Sent/sec	Hyper-V Host	Yes	No	No
Network Packets/sec	Hyper-V Host	Yes	No	No
Network Received Errors	Hyper-V Host	Yes	No	No

Performance Metric	Object Type	Veeam backup data and virtual infrastructure	Veeam backup data and large-scale virtual infrastructure	Veeam Backup Data Only
Page Faults/sec	Hyper-V Host	Yes	No	No
Page Reads/sec	Hyper-V Host	Yes	No	No
Page Writes/sec	Hyper-V Host	Yes	No	No
Pages Input/sec	Hyper-V Host	Yes	No	No
Pages Output/sec	Hyper-V Host	Yes	No	No
Pages/sec	Hyper-V Host	Yes	Yes	No
Total Interrupts/sec	Hyper-V Host	Yes	No	No
Total Run Time	Hyper-V Host	Yes	Yes	No
Total Run Time MHz	Hyper-V Host	Yes	Yes	No
vCPU Total Run Time	Hyper-V Host	Yes	No	No
Virtual Switch Bytes Received/sec	Hyper-V Host	Yes	No	No
Virtual Switch Bytes Sent/sec	Hyper-V Host	Yes	No	No
Virtual Switch Bytes/sec	Hyper-V Host	Yes	No	No
Virtual Switch Packets Received/sec	Hyper-V Host	Yes	No	No
Virtual Switch Packets Sent/sec	Hyper-V Host	Yes	No	No
Virtual Switch Packets/sec	Hyper-V Host	Yes	No	No

Performance Metric	Object Type	Veeam backup data and virtual infrastructure	Veeam backup data and large-scale virtual infrastructure	Veeam Backup Data Only
CPU Wait Time	Hyper-V Virtual Machine	Yes	Yes	No
Current Pressure	Hyper-V Virtual Machine	Yes	Yes	No
Demand	Hyper-V Virtual Machine	Yes	Yes	No
Errors/min	Hyper-V Virtual Machine	Yes	Yes	No
Flushes/min	Hyper-V Virtual Machine	Yes	Yes	No
Guest Disk Free Space	Hyper-V Virtual Machine	Yes	Yes	No
Guest Disk Used Space	Hyper-V Virtual Machine	Yes	Yes	No
Guest Run Time	Hyper-V Virtual Machine	Yes	Yes	No
Guest vCPU Guest Run Time MHz	Hyper-V Virtual Machine	Yes	Yes	No
Guest Visible Physical Memory	Hyper-V Virtual Machine	Yes	Yes	No
Hypervisor Run Time	Hyper-V Virtual Machine	Yes	No	No
IOPS	Hyper-V Virtual Machine	Yes	Yes	No
Legacy Network Bytes /sec	Hyper-V Virtual Machine	Yes	No	No
Legacy Network Bytes Dropped/sec	Hyper-V Virtual Machine	Yes	No	No

Performance Metric	Object Type	Veeam backup data and virtual infrastructure	Veeam backup data and large-scale virtual infrastructure	Veeam Backup Data Only
Legacy Network Bytes Received/sec	Hyper-V Virtual Machine	Yes	No	No
Legacy Network Bytes Sent/sec	Hyper-V Virtual Machine	Yes	No	No
Physical Memory	Hyper-V Virtual Machine	Yes	Yes	No
Process CPU Usage	Hyper-V Virtual Machine	Yes	Yes	No
Process Memory Usage	Hyper-V Virtual Machine	Yes	Yes	No
Reads/sec	Hyper-V Virtual Machine	Yes	Yes	No
Running Services	Hyper-V Virtual Machine	Yes	Yes	No
Total Run Time	Hyper-V Virtual Machine	Yes	Yes	No
vCPU Total Run Time MHz	Hyper-V Virtual Machine	Yes	No	No
Virtual Disk Provisioned	Hyper-V Virtual Machine	Yes	Yes	No
Virtual Disk Used	Hyper-V Virtual Machine	Yes	Yes	No
Virtual Network Bytes /sec	Hyper-V Virtual Machine	Yes	Yes	No
Virtual Network Bytes Received/sec	Hyper-V Virtual Machine	Yes	Yes	No
Virtual Network Bytes Sent/sec	Hyper-V Virtual Machine	Yes	Yes	No

Performance Metric	Object Type	Veeam backup data and virtual infrastructure	Veeam backup data and large-scale virtual infrastructure	Veeam Backup Data Only
Virtual Network Packets Received/sec	Hyper-V Virtual Machine	Yes	No	No
Virtual Network Packets Sent/sec	Hyper-V Virtual Machine	Yes	No	No
Virtual Storage Read Bytes/sec	Hyper-V Virtual Machine	Yes	Yes	No
Virtual Storage Usage Bytes/sec	Hyper-V Virtual Machine	Yes	Yes	No
Virtual Storage Write Bytes/sec	Hyper-V Virtual Machine	Yes	Yes	No
Writes/sec	Hyper-V Virtual Machine	Yes	Yes	No
Disk Free Space	Hyper-V Physical Disk	Yes	Yes	No
Disk Provisioned Space	Hyper-V Physical Disk	Yes	Yes	No
Disk Used Space	Hyper-V Physical Disk	Yes	Yes	No
Disk/Physical Disk: Avg Disk Queue Length	Hyper-V Physical Disk	Yes	No	No
Disk/Physical Disk: Avg Disk sec/Read	Hyper-V Physical Disk	Yes	Yes	No
Disk/Physical Disk: Avg Disk sec/Write	Hyper-V Physical Disk	Yes	Yes	No
Disk/Physical Disk: Disk Bytes/sec	Hyper-V Physical Disk	Yes	Yes	No

Performance Metric	Object Type	Veeam backup data and virtual infrastructure	Veeam backup data and large-scale virtual infrastructure	Veeam Backup Data Only
Disk/Physical Disk: Disk Read Bytes/sec	Hyper-V Physical Disk	Yes	Yes	No
Disk/Physical Disk: Disk Transfers/sec	Hyper-V Physical Disk	Yes	Yes	No
Disk/Physical Disk: Disk Write Bytes/sec	Hyper-V Physical Disk	Yes	Yes	No
Cache IO Read Bytes/sec	Hyper-V CSV 2012	Yes	No	No
Cache Reads/sec	Hyper-V CSV 2012	Yes	No	No
CSV FS Free Space	Hyper-V CSV 2012	Yes	Yes	No
CSV FS Provisioned Space	Hyper-V CSV 2012	Yes	No	No
CSV FS Used Space	Hyper-V CSV 2012	Yes	No	No
Disk/CSV 2012: Direct Bytes/sec	Hyper-V CSV 2012	Yes	Yes	No
Disk/CSV 2012: Direct IOPS	Hyper-V CSV 2012	Yes	Yes	No
Disk/CSV 2012: Direct Latency	Hyper-V CSV 2012	Yes	Yes	No
Disk/CSV 2012: IOPS	Hyper-V CSV 2012	Yes	No	No
Disk/CSV 2012: Latency	Hyper-V CSV 2012	Yes	Yes	No
Disk/CSV 2012: Queue Length	Hyper-V CSV 2012	Yes	No	No
Disk/CSV 2012: Read Bytes/sec	Hyper-V CSV 2012	Yes	Yes	No

Performance Metric	Object Type	Veeam backup data and virtual infrastructure	Veeam backup data and large-scale virtual infrastructure	Veeam Backup Data Only
Disk/CSV 2012: Read Latency	Hyper-V CSV 2012	Yes	Yes	No
Disk/CSV 2012: Read Queue Length	Hyper-V CSV 2012	Yes	No	No
Disk/CSV 2012: Reads/sec	Hyper-V CSV 2012	Yes	No	No
Disk/CSV 2012: Redirected Bytes/sec	Hyper-V CSV 2012	Yes	Yes	No
Disk/CSV 2012: Redirected IOPS	Hyper-V CSV 2012	Yes	Yes	No
Disk/CSV 2012: Redirected Latency	Hyper-V CSV 2012	Yes	Yes	No
Disk/CSV 2012: Total Bytes/sec	Hyper-V CSV 2012	Yes	Yes	No
Disk/CSV 2012: Write Bytes/sec	Hyper-V CSV 2012	Yes	Yes	No
Disk/CSV 2012: Write Latency	Hyper-V CSV 2012	Yes	Yes	No
Disk/CSV 2012: Write Queue Length	Hyper-V CSV 2012	Yes	No	No
Disk/CSV 2012: Writes/sec	Hyper-V CSV 2012	Yes	No	No
SMB Share Free Space	Hyper-V Share	Yes	Yes	No
SMB Share Used Space	Hyper-V Share	Yes	No	No
SMB Share Provisioned Space	Hyper-V Share	Yes	No	No

Performance Metric	Object Type	Veeam backup data and virtual infrastructure	Veeam backup data and large-scale virtual infrastructure	Veeam Backup Data Only
Disk/Share: IOPS	Hyper-V Share	Yes	No	No
Disk/Share: Writes/sec	Hyper-V Share	Yes	No	No
Disk/Share: Reads/sec	Hyper-V Share	Yes	No	No
Disk/Share: Virtual Storage Usage Bytes/sec	Hyper-V Share	Yes	No	No
Disk/Share: Virtual Storage Write Bytes/sec	Hyper-V Share	Yes	Yes	No
Disk/Share: Virtual Storage Read Bytes/sec	Hyper-V Share	Yes	Yes	No
Disk/Share: SMB Share Error Count/min	Hyper-V Share	Yes	No	No
Disk/Share: SMB Share Flush Count/min	Hyper-V Share	Yes	No	No

Scheduling Script Examples

To facilitate the process of dashboards and report creation, you can schedule automatic delivery of dashboards and reports. As one of the delivery options, you can save created dashboards and reports to a disk or network share. To learn about scheduling dashboards and reports, see Scheduling Dashboards and Scheduling Reports.

If you need to perform further manipulations with the saved files, you can configure Veeam ONE Web Client to run a custom script after reports and dashboards are saved to the target folder. Veeam ONE Web Client allows you to use .BAT, .CMD, .VBS, .JS, .WSF, .EXE, .VBE, .JSE, .WSH or .PS1 scripts.

You can pass the following parameters to post-delivery scripts:

Parameter	Description
%ReportName%	Name of the generated report.
%ReportFolder%	Target folder to which created reports are saved (as specified in the **Path** field).
%DashboardName%	Name of the generated dashboard.
%JobName%	Name of the scheduling job that generates reports.
"-hidden"	Defines whether it is necessary to open created .VMR reports with the Veeam Report Viewer. If the parameter is specified, the reports will not be opened.

This section explains how to use post-delivery scripts and contains simple script examples.

- Example A. Copying a Report to Network Shares
- Example B. Sorting Reports by Name

Example A. Copying a Report to Network Shares

Consider the following scenario: your backup administrators want to obtain a weekly report with the list of protected VMs in your virtual environment. To deliver the **Protected VMs** report to backup administrators on a weekly basis, you can take the following steps:

1. Save the Protected VMs report with the necessary parameters.
2. Create a script that will copy the report to network shares of backup administrators.
3. Set the necessary schedule for the report and specify the post-delivery script.

Step 1. Save Protected VMs Report

Save the **Protected VMs** report with the necessary parameters as described in Saving Reports.

Step 2. Create Script

When you schedule a report delivery to a folder or a network share, Veeam ONE Web Client saves the generated report to a target location by the following path:

```
<TargetDirectory>\reporting-task-for-ssrs-report-<ReportName><ID>\
```

The sample script must perform the following operations after the report is created:

1. Access the target report location:

   ```
   C:\reports\reporting-task-for-ssrs-report-<ReportName><ID>\
   ```

2. Copy the report from the target location to network shares:
   - `\\andy\shared\backups\reports\`
   - `\\brian\shared\backups\reports\`
   - `\\chris\shared\backups\reports\`
3. Remove the report from the target location and delete the target directory.

An example of the script is provided below:

```
::Changing directory to the target report location
cd reporting-task-for-ssrs-report*
set RD=%cd%

::Copying the report from the target location to admins' shares
xcopy Protected*.* \\andy\shared\backups\reports\*.* /y
xcopy Protected*.* \\brian\shared\backups\reports\*.* /y
xcopy Protected*.* \\chris\shared\backups\reports\*.* /y

::Removing the target report location
cd ..\
rd %RD% /s/q
```

Save the script as a Windows batch file on the machine where Veeam ONE Server is installed.

To follow this example, save the script with the `postdelivery.bat` name to the `C:\reports\` directory.

Step 3. Configure Scheduling Settings

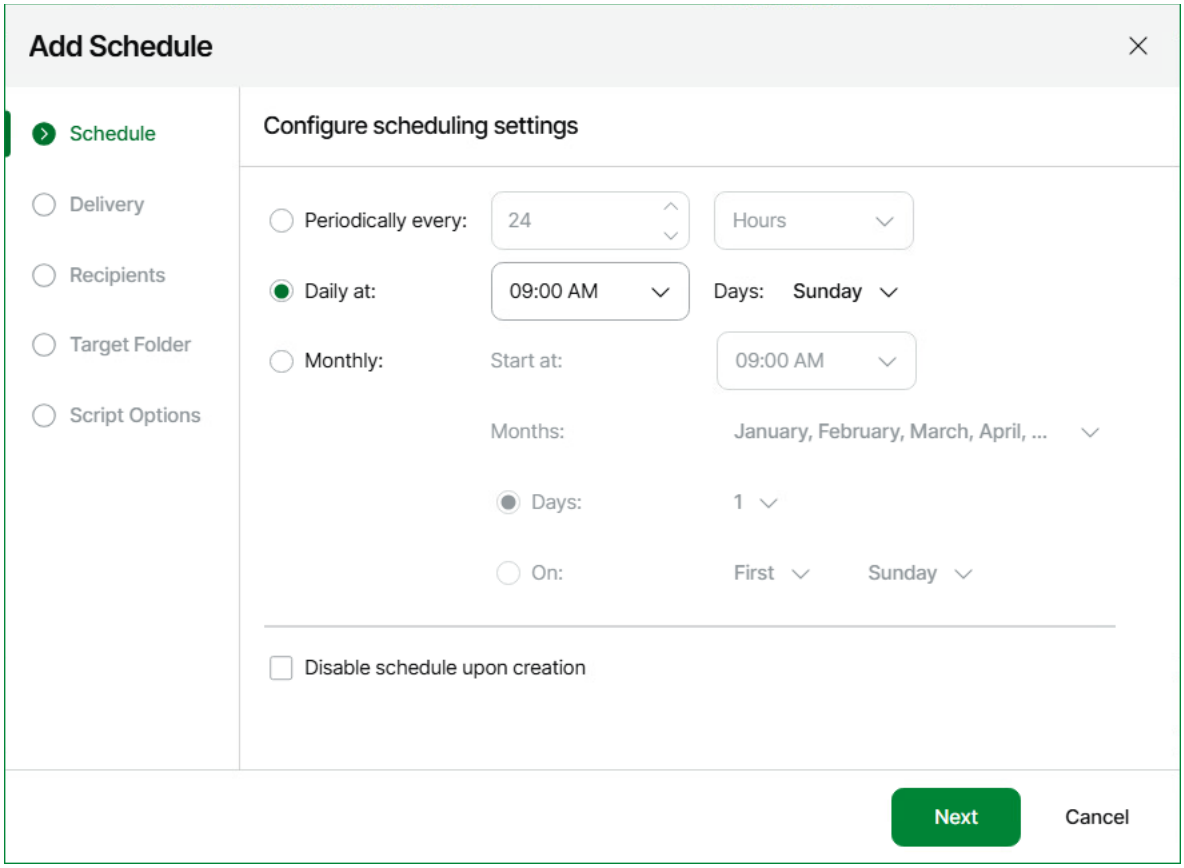
Before scheduling report delivery, make sure that:

- The account under which the *Veeam ONE Reporter Server* service runs has appropriate write permissions on the destination network shares.
- Object properties data collection task that gathers data from virtual infrastructure and Veeam Backup & Replication servers completes before the scheduled report generation time.

Configure scheduling settings for the saved report as follows:

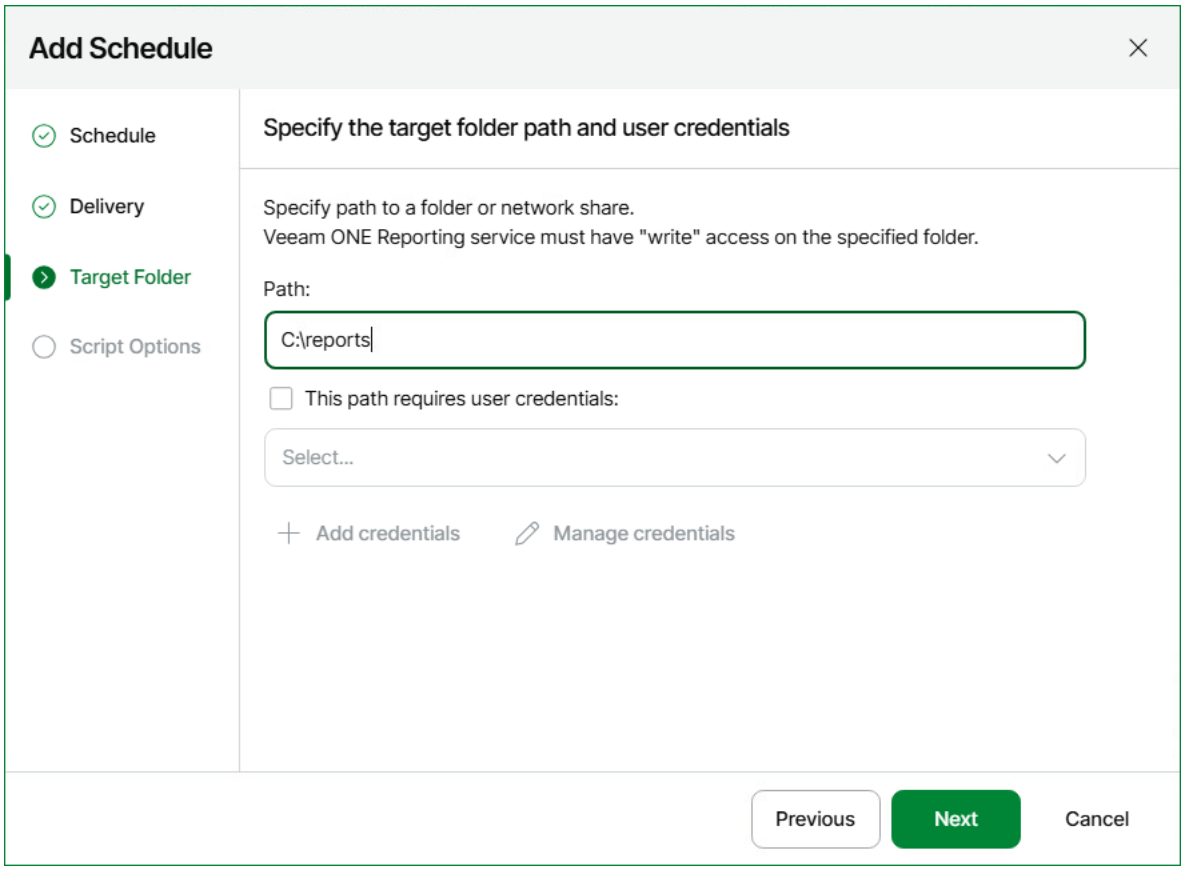
1. Open Veeam ONE Web Client.
2. Open the **Saved Reports** section.
3. On the saved report or report folder, right-click the necessary folder and select **Schedule** in the context menu.
4. In the **Report Scheduling Settings** window, click **Add**.

   Veeam ONE Web Client will launch the **Add Schedule** wizard.
5. In the **Add Schedule** window, configure automatic delivery settings as follows:
   a. At the **Schedule** step of the wizard, create a schedule according to which the report should be generated. To follow this example, schedule the report to run on a weekly basis.



   b. At the **Delivery** step of the wizard, select only the **Save to a folder** check box.
   c. At the **Target Folder** step of the wizard, specify target folder details. In the **Path** field, enter the path to the folder where the generated report will be stored.

d. In the **Script Options** step, specify the location of the script file in the **Path to the script file** field. To follow this example, enter `C:\reports` in the **Path** field and enter `C:\reports\postdelivery.bat` in the **Path to the script file** field.



6. Save the scheduling settings.

Expected Result

The report will be generated and copied in accordance with the specified schedule.

At the specified schedule time, Veeam ONE Web Client will automatically generate the report. After the report is created, Veeam ONE Web Client will trigger the script that will copy the report to network shares.

Example B. Sorting Reports by Name

Consider the following scenario: you want to schedule a weekly delivery for a set of reports. After the reports are created, you want to save each report to a separate folder with the report name.

To sort reports into folders by report name, you can take the following steps:

1. Create a folder that will group a set of necessary reports.
2. Save reports with the necessary parameters into the folder.
3. Create a script that will sort the generated reports.
4. Set the necessary schedule for the folder and specify the post-delivery script.

Step 1. Create Folder

Create a report folder as described in Creating Folders. The folder will be used to group a set of reports that you want to create on a scheduled basis.

Step 2. Save Reports

Save reports with the necessary parameters as described in section Saving Reports.

Step 3. Create Script

When you schedule a report delivery for set of reports in a folder, Veeam ONE Web Client saves the reports to a target location by the following path:

```
<TargetDirectory>\reporting-task-for-folder-<FolderName><ID>\
```

The sample script must perform the following operations:

1. Access the target report location:

   ```
   C:\reports\reporting-task-for-folder-<FolderName><ID>\
   ```

2. For every generated report, retrieve the report name and copy the report to a folder with the report name:

   ```
   C:\share\myreports\%ReportName%\
   ```

   To create a folder with the report name, the script will use the `%ReportName%` parameter.

3. Remove the reports from the target location and delete the target directory.

An example of the script is provided below:

```
::Changing directory to the target report location
cd reporting-task-for-folder*
set RD=%cd%

::Removing extension and date from the report file name
set ReportName=%~n1
set Extension=%~x1
set FolderName=%ReportName:~0,-11%

::Copying the report to a folder with the report name
echo f | xcopy %1 "c:\share\myreports\%FolderName%\%ReportName%%Extension%" /y

::Removing the target report location
cd ..\
rd %RD% /s/q
```

Save the script as a Windows batch file on the machine where Veeam ONE Server is installed.

To follow this example, save the script with the `postdelivery.bat` name to the `C:\reports\` directory.

Step 4. Configure Scheduling Settings

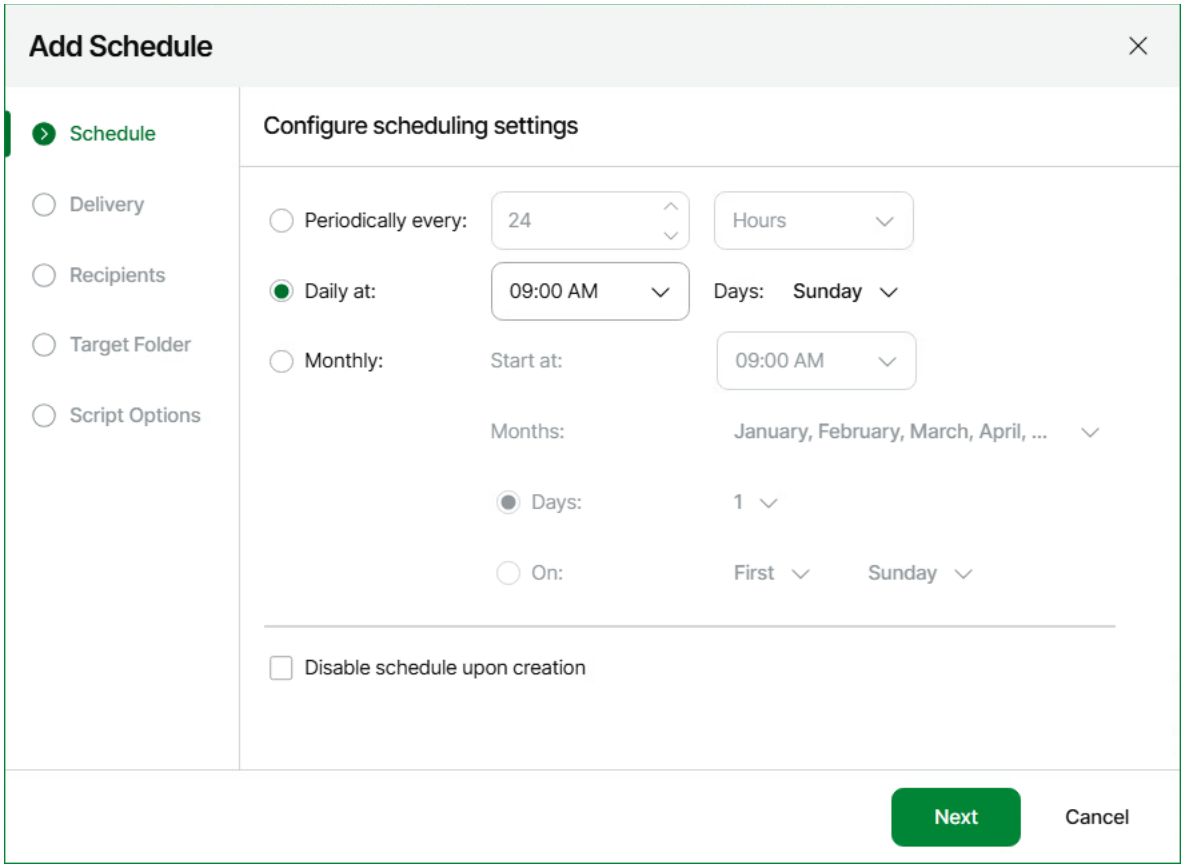
Configure scheduling settings for the saved report as follows:

1. Open Veeam ONE Web Client.
2. Open the **Saved Reports** section.
3. On the saved report or report folder, right-click the necessary folder and select **Schedule** in the context menu.
4. In the **Report Scheduling Settings** window, click **Add**.

   Veeam ONE Web Client will launch the **Add Schedule** wizard.

5. In the **Add Schedule** window, configure automatic delivery settings as follows:

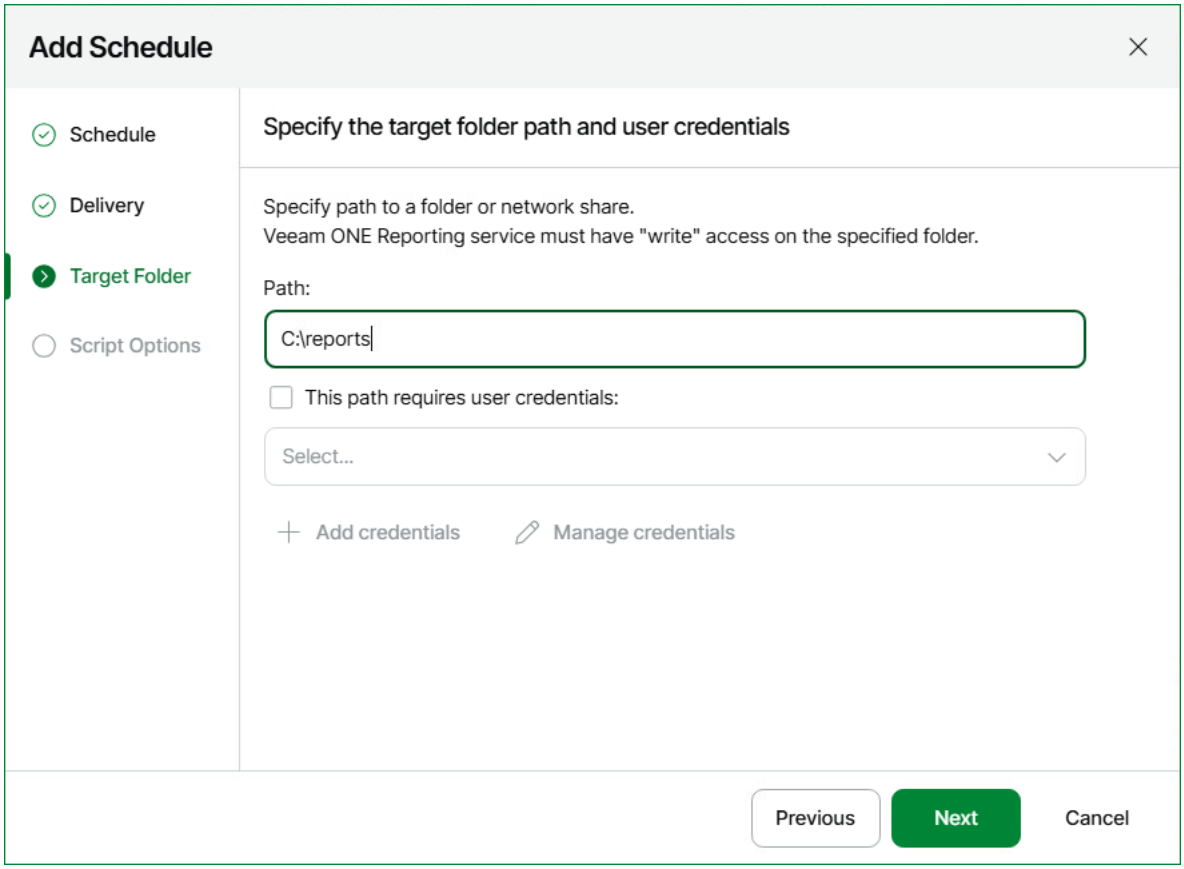
   a. At the **Schedule** step of the wizard, create a schedule according to which the report should be generated. To follow this example, schedule the report to run on a weekly basis.



   b. At the **Delivery** step of the wizard, select only the **Save to a folder** check box.

   c. At the **Target Folder** step of the wizard, specify target folder details. In the **Path** field, enter the path to the folder where the generated report will be stored.

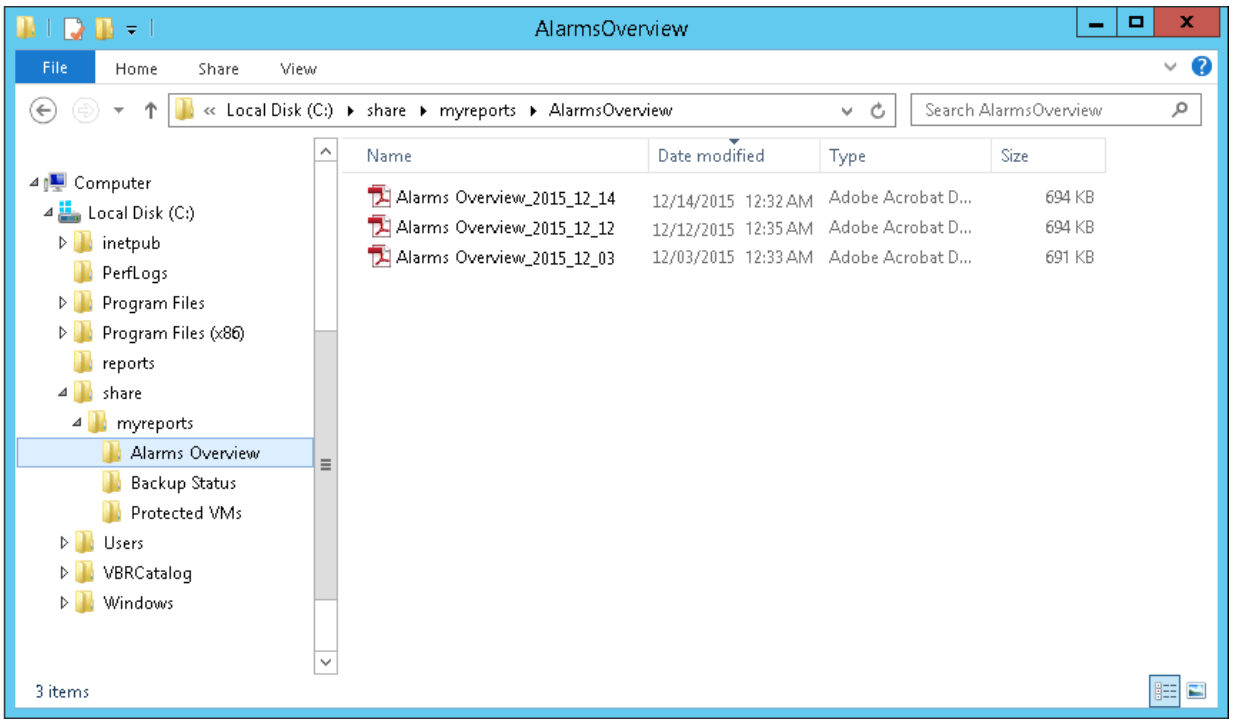
d. In the **Script Options** step, specify the location of the script file in the **Path to the script file** field. To follow this example, enter `C:\reports` in the **Path** field. In the **Path to the script file** field, enter the path to the script and pass the report name parameter to the script:
`C:\reports\postdelivery.bat %ReportName%`



6. Save the scheduling settings.

Expected Result

At the specified schedule time, Veeam ONE Web Client will automatically generate the reports. When a report is created, Veeam ONE Web Client will trigger the script that will copy the report to a separate folder.



About This Document

This guide contains detailed description of Veeam ONE Reporter. It has all information you need to access, configure and manage Veeam ONE Reporter. You will find all relevant data on how to customize dashboards and reports according to your requirements and learn how to use preconfigured reports and dashboards.

Intended Audience

The guide is designed for anyone who plans to use the Veeam ONE solution. It is primarily aimed at administrators managing VMware vSphere or Microsoft Hyper-V environments, but can also be helpful for other current and prospective Veeam ONE users.

Veeam ONE Settings Utility

The Veeam ONE Settings utility allows you to change configuration of the Veeam ONE software components.

> **NOTE:**
>
> The Veeam ONE Settings utility must be used only under the guidance of Veeam Support. It is strongly recommended that you obtain detailed instructions from the Veeam Support team before changing any configuration settings in your Veeam ONE deployment.

To run the Veeam ONE Settings utility:

1. Log in to Veeam ONE Client under account with *Local Administrator* permissions on the machine where Veeam ONE Server component is installed.

   For details, see Accessing Veeam ONE Components.

   > **NOTE:**
   >
   > If you use Microsoft Windows authentication to connect to Microsoft SQL Server, make sure that the user under which you launch Veeam ONE Settings utility has sufficient permissions to access Veeam ONE database. Otherwise the **Retention Policy Period** and **Scalability** settings in the utility will be unavailable.

2. In the main menu, click **Settings** > **Server Settings**.

   Alternatively, press `[CTRL + S]` on the keyboard.

3. Open the **Other** tab.

4. In the **Support utility** section, click **Launch**.

This section describes configuration settings that you can change using the Veeam ONE Settings utility.

General Settings

The **General** section groups configuration settings common for all Veeam ONE software components.

This section includes the following tabs:

- Database
- Retention Policy Period

Database

On the **Database** tab, you can modify connection settings for the Veeam ONE database and the Microsoft SQL Server that hosts this database. By default, the fields are populated with the values specified during Veeam ONE installation.

To change database configuration settings:

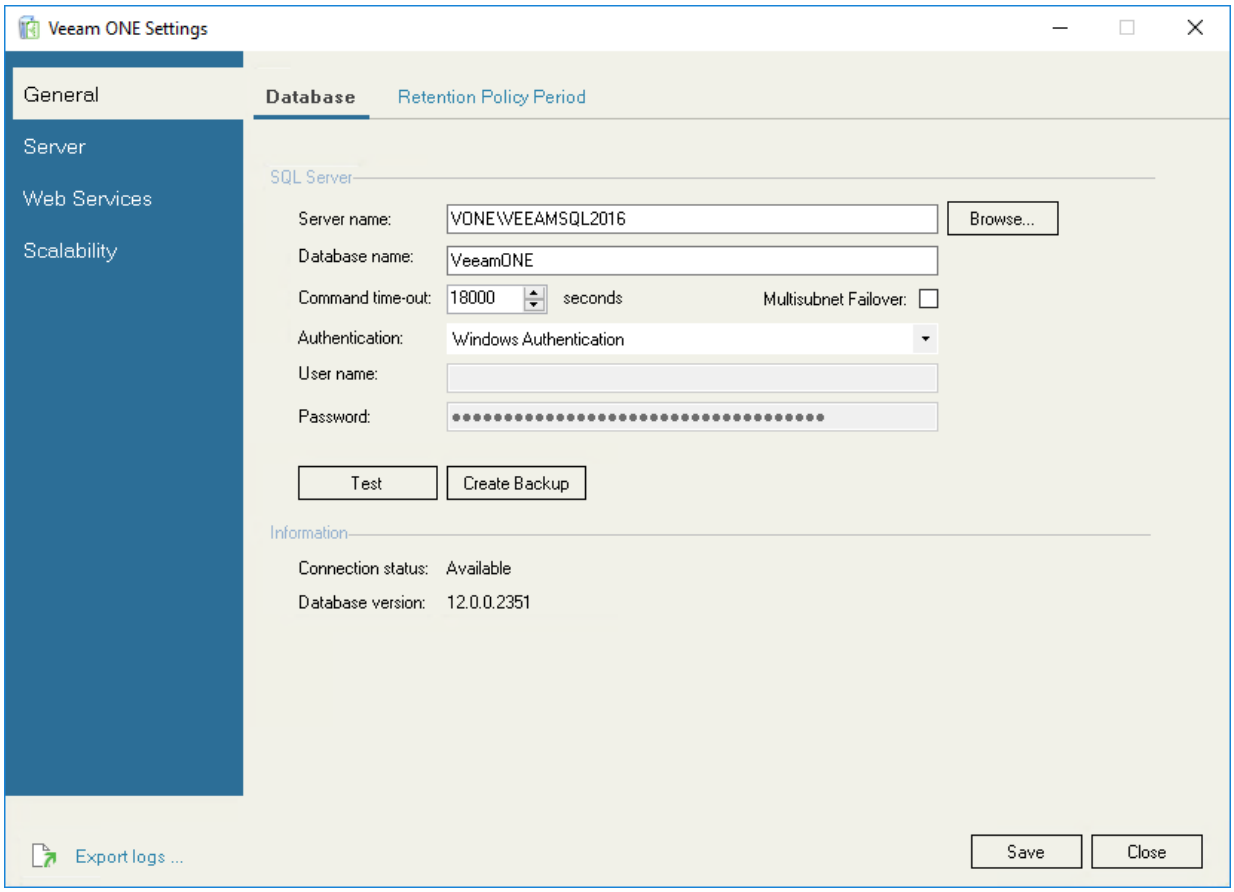
1. In the **Server name** field, specify the name of the SQL Server that hosts the Veeam ONE database.
2. In the **Database name** field, specify the name of the database that stores Veeam ONE data.
3. In the **Command time-out** field, specify the wait time in seconds for a command to execute on the Veeam ONE database.

   By default, the time-out value is set to 18000 seconds (5 hours).

   Select the **Multisubnet Failover** check box, to enable failover in a SQL Server multi-subnet failover cluster.
4. From the **Authentication** list, select the type of authentication that Veeam ONE components must use to connect to the Microsoft SQL Server that hosts the Veeam ONE database:
   - Select **Windows Authentication** to use Windows authentication credentials of the Veeam ONE service account.
   - Select **SQL Server Authentication** to use Microsoft SQL Server account credentials.
5. [For SQL Server Authentication] In the **User name/Password** fields, specify credentials of the SQL account used to connect to the Microsoft SQL Server that hosts the Veeam ONE database.
6. Click **Save** to apply settings.
7. To check if Veeam ONE can connect to the specified database using the specified connection settings, click **Test**.

To back up the Veeam ONE database to a `BAK` file, click **Create Backup** and specify the location where the database backup file must be saved.

In the **Information** section, you can view the Veeam ONE connection status and version number.



Retention Policy Period

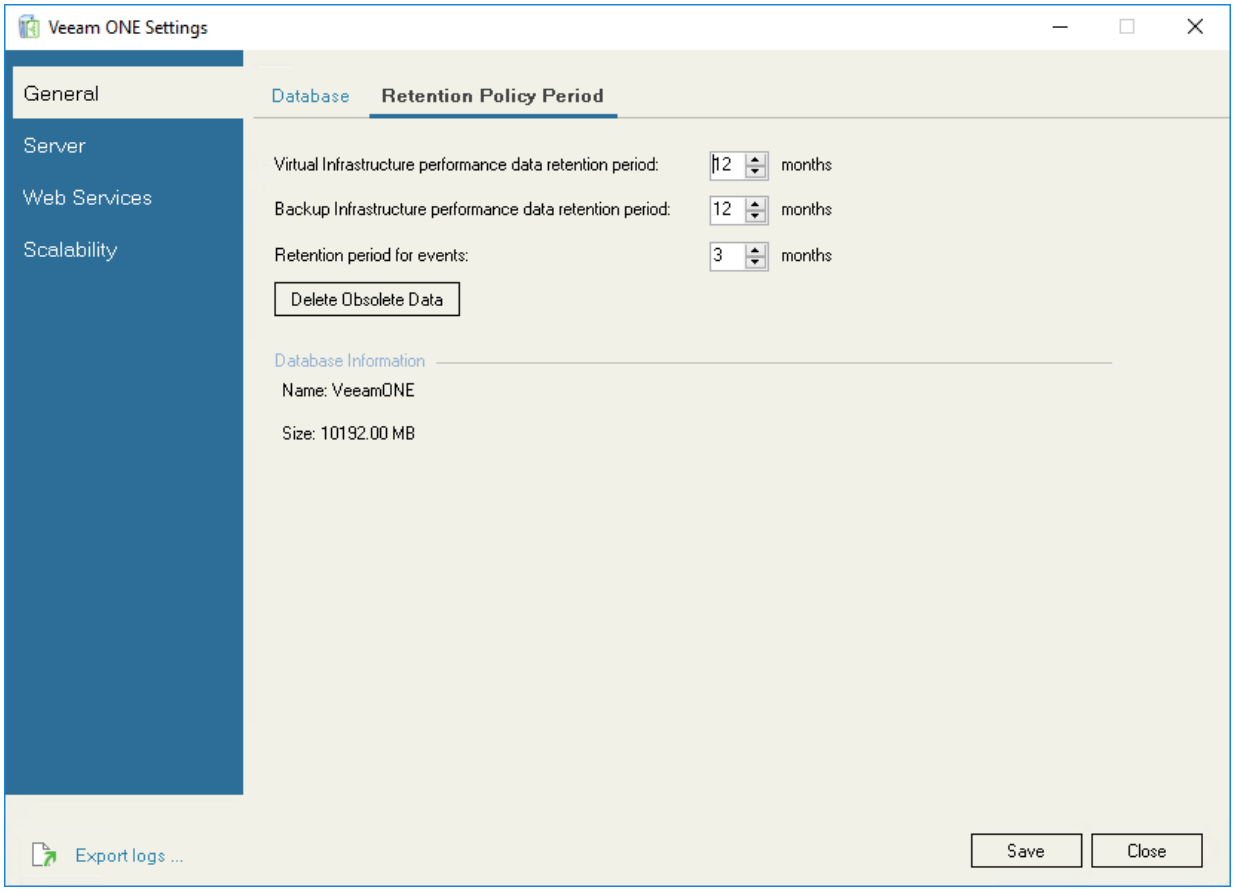
On the **Retention Policy Period** tab, you can modify the time period during which historical data is stored in the Veeam ONE database. By default, virtual and backup infrastructure performance data is retained for 12 months, and event data is stored for 3 months.

To modify the retention period:

- In the **Virtual Infrastructure performance data retention period** field, specify the period for storing virtual infrastructure performance data, in months.
- In the **Backup Infrastructure performance data retention period** field, specify the period for storing backup infrastructure performance data, in months.
- In the **Retention period for events** field, specify the period for storing events data, in months.

  You can specify a value from 1 to 36.

Specified retention values will be applied at the end of the current week. To apply retention settings immediately, click **Delete Obsolete Data**.



Veeam ONE Server Settings

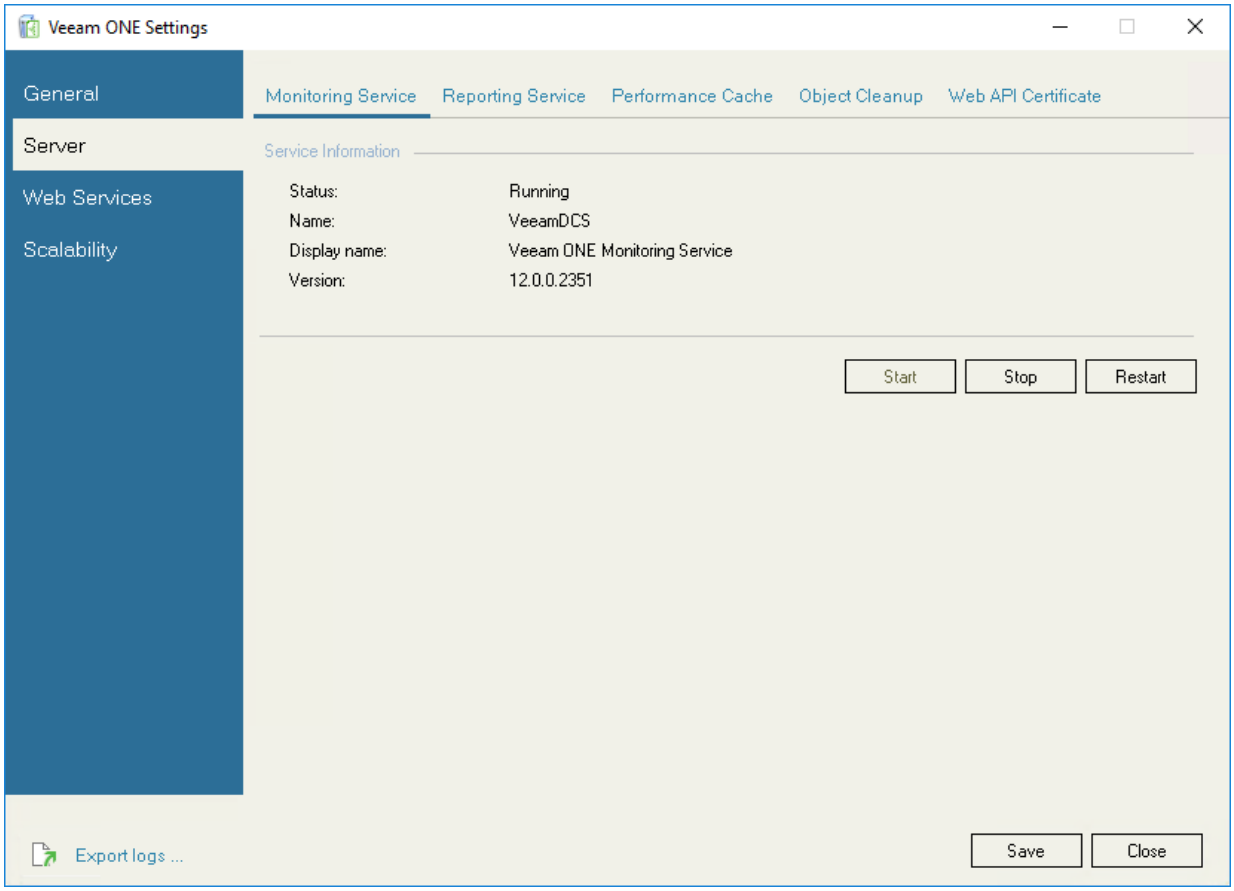
The **Server** section groups configuration settings for the Veeam ONE Server.

This section includes the following tabs:

- Monitoring Service
- Reporting Service
- Performance Cache
- Object Cleanup
- Web API Certificate

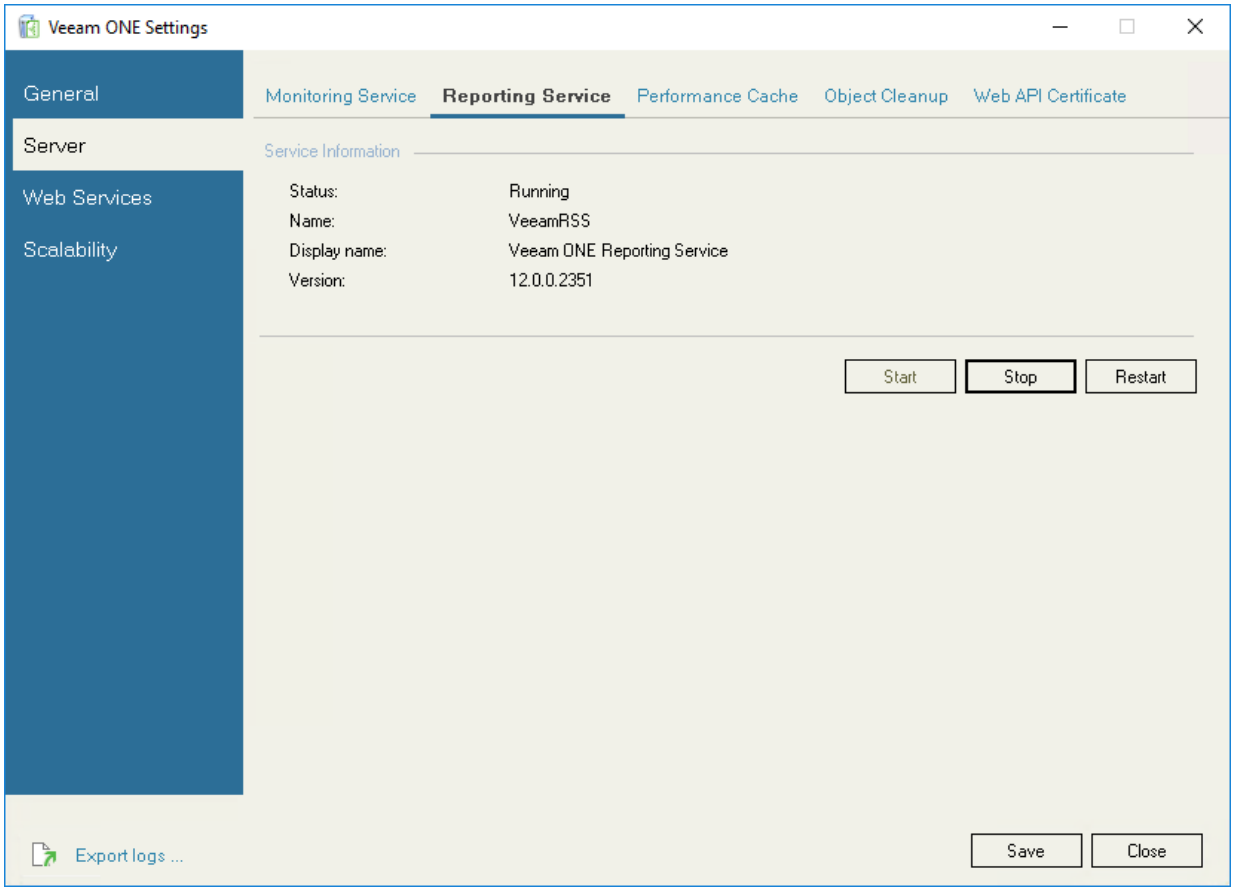
Monitoring Service

On the **Monitoring Service** tab, you can start, stop or restart the Veeam ONE Monitoring service. These operations may be required to complete Veeam ONE configuration updates.



Reporting Service

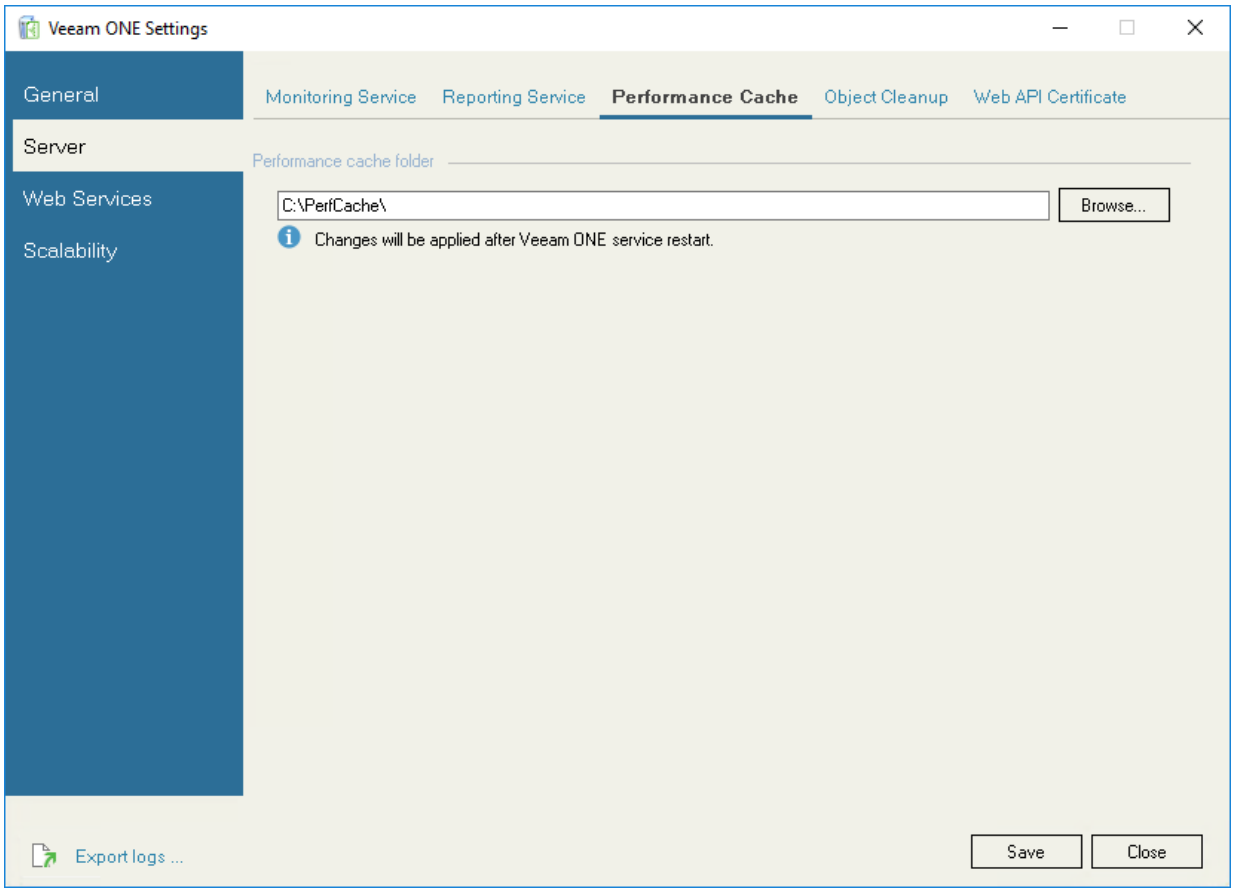
On the **Reporting Service** tab, you can start, stop or restart the Veeam ONE Reporting service. These operations may be required to complete Veeam ONE configuration updates.



Performance Cache

On the **Performance Cache** tab, you can change the path to the directory in which performance cache is stored. After you change the directory, switch to the **Monitoring Service** tab and restart Veeam ONE Monitoring service.

The initial directory to store performance cache is specified during installation.



Object Cleanup

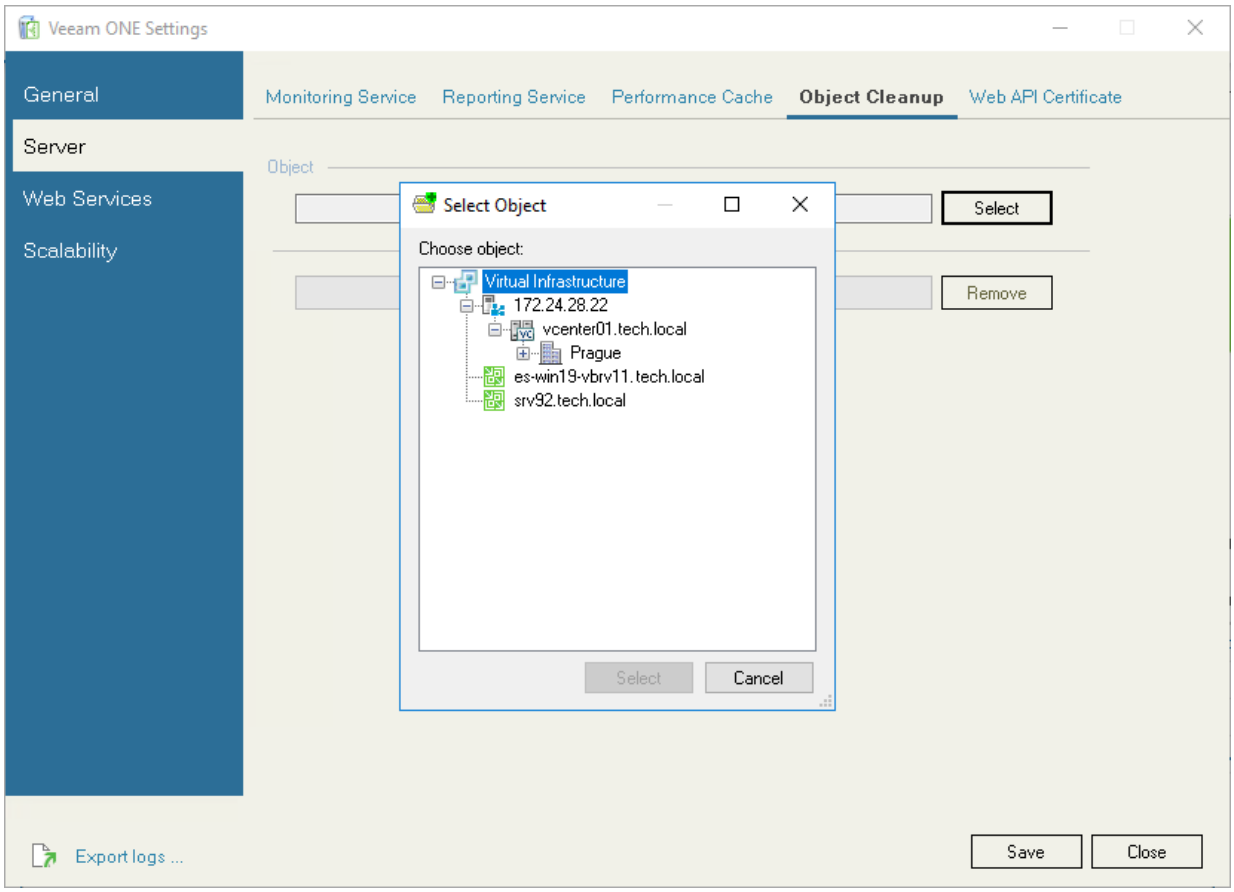
On the **Object Cleanup** tab, you can remove residual data on deleted infrastructure objects from the Veeam ONE database.

In some cases, data collected from infrastructure objects remain in the Veeam ONE database even if connections to these infrastructure objects are removed in the Veeam ONE Client. As a result, residual data may appear in Veeam ONE reports.

To clean data on obsolete infrastructure objects from the Veeam ONE database:

1. Click **Select** and choose an infrastructure object for which data must be removed.

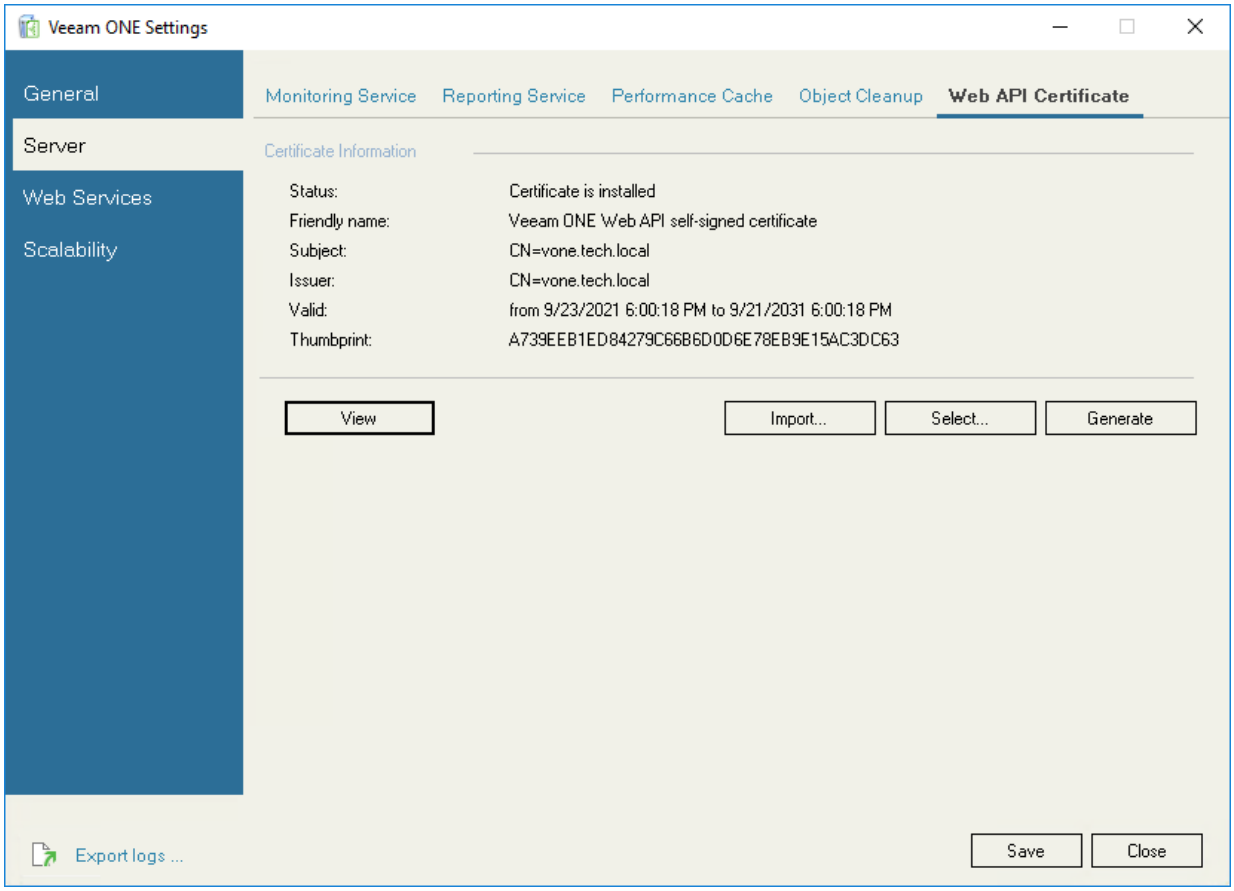
2. Click **Remove** and wait for completion of the object data cleanup.



Web API Certificate

On the **Web API Certificate** tab, you can view and manage a TLS certificate used to establish a secure connection between Veeam ONE components. By default, Veeam ONE uses a self-signed certificate generated during installation or upgrade. For more information on types of certificates supported by Veeam ONE, see Veeam ONE Certificates.

The **Certificate Information** section displays summary details of the currently installed certificate. To see detailed information on the certificate, click **View**.

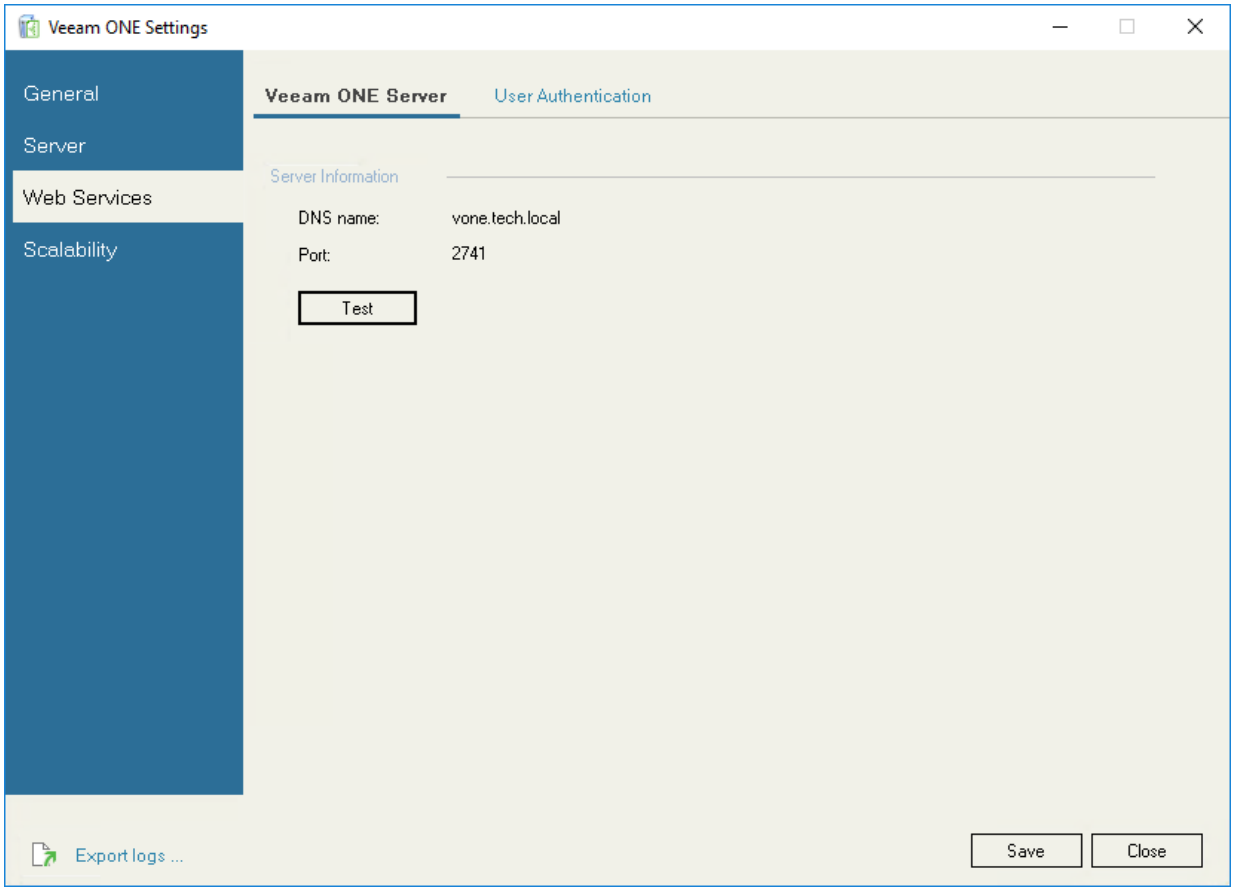


Veeam ONE Web Settings

In the **Web Services** section, you can view Veeam ONE Server connection details and configure.

Veeam ONE Server

On the **Veeam ONE Server** tab, you can review the connection details of the machine where Veeam ONE Server components are installed. This may be required if you installed Veeam ONE using the distributed deployment scenario. Click **Test**, to check connection between Veeam ONE Server and Web Services.



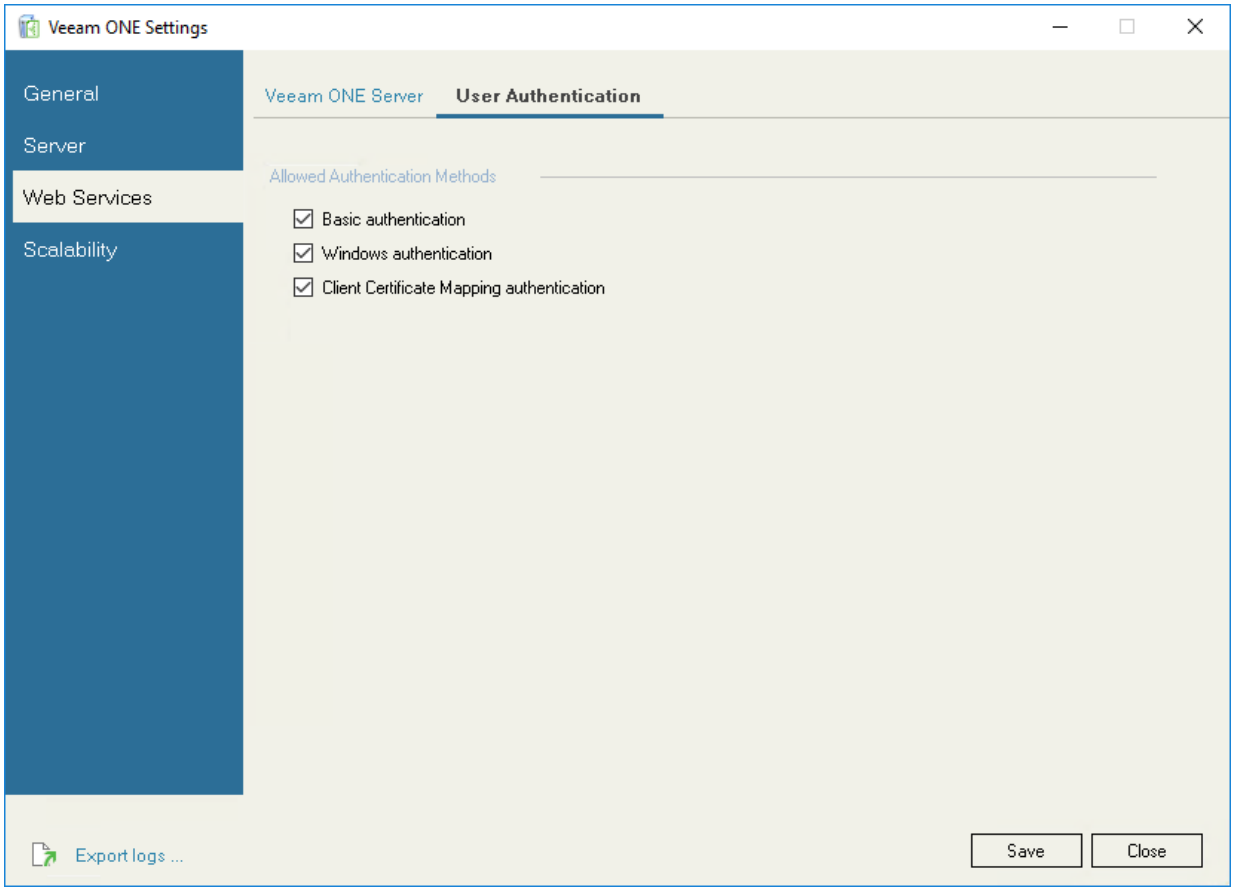
User Authentication

On the **User Authentication** tab, you can select which methods are allowed to authenticate users in Veeam ONE Web Client:

- **Basic authentication** – select this method to allow users to log in with user name and password.
- **Windows authentication** – select this method to allow users to log in with credentials of a Windows user account under which the user is logged on to the machine.

- **Client Certificate Mapping authentication** — select this method to allow users to log in with a client certificate.

  For more information, see Configuring Client Certificate Mapping Authentication.



Configuring Client Certificate Mapping Authentication

To allow users to log in to Veeam ONE Web Client with multi-factor authentication (MFA) through client certificate configuration, do the following on the machine that hosts Veeam ONE Web UI component:

- Enable Active Directory Client Certificate Authentication on the IIS.

  For details on Client Certificate Mapping Authentication settings, see this Microsoft article.

- If you have non-self-signed certificates in the Trusted Root Certificate Authorities store, move them to the Intermediate Certification Authorities store.

- If Veeam ONE Web UI component runs on Windows Server 2022, you must disable TLS 1.3 over TCP in the site binding settings.

Scalability

In the **Scalability** section, you can choose Veeam ONE data collection mode and metrics that Veeam ONE must collect.

This section includes the following tabs:

- Data Collection Mode
- Performance Metrics

Data Collection Mode

On the **Data Collection Mode** tab, you can choose Veeam ONE data collection mode. The data collection mode determines what metrics Veeam ONE must collect, and specifies the product configuration.

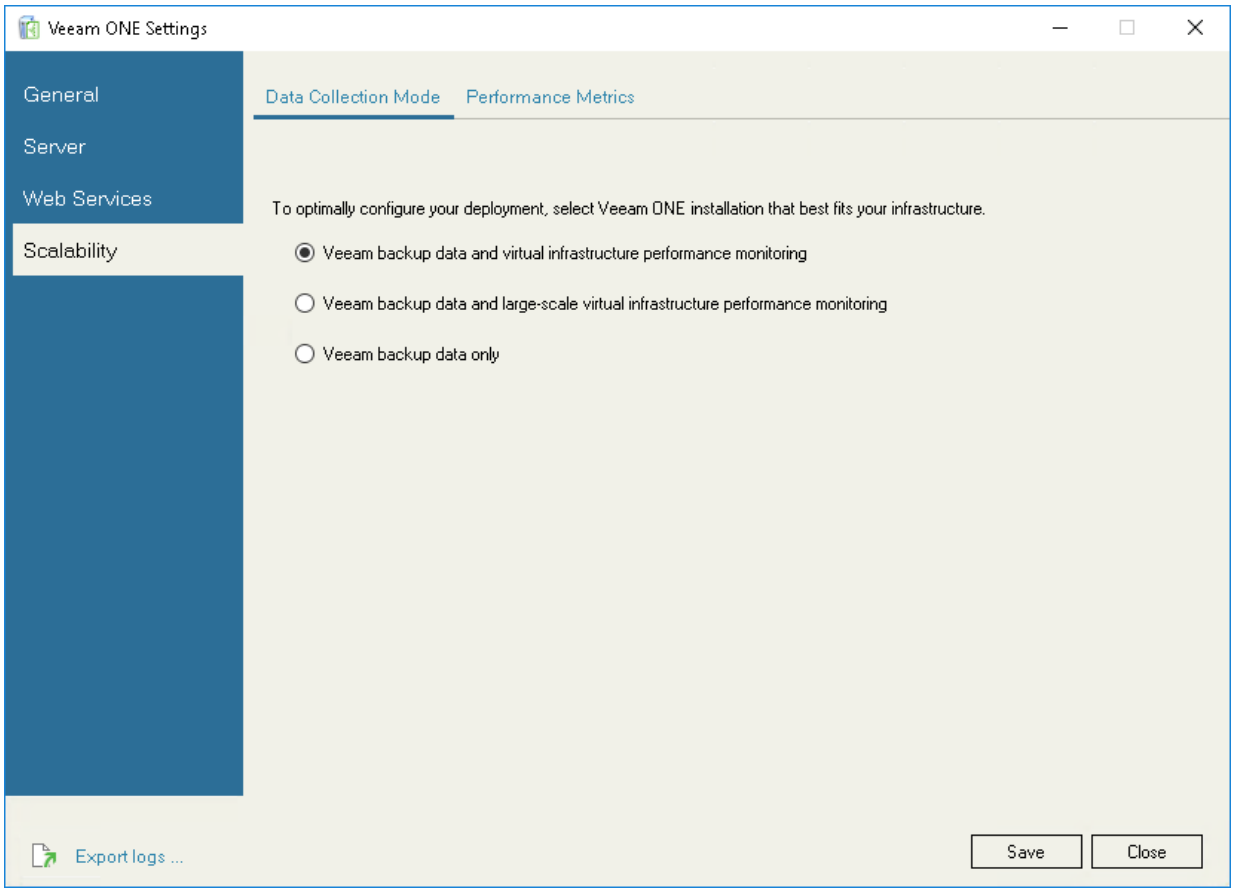
Data collection mode is specified during Veeam ONE installation. In some cases, you may need to change the data collection mode — for example, if you need to change the level of data granularity.

To change the data collection mode:

1. Select the necessary data collection option.

   For details on data collection mode, see Choose Data Collection Mode.

2. Click **Save**.



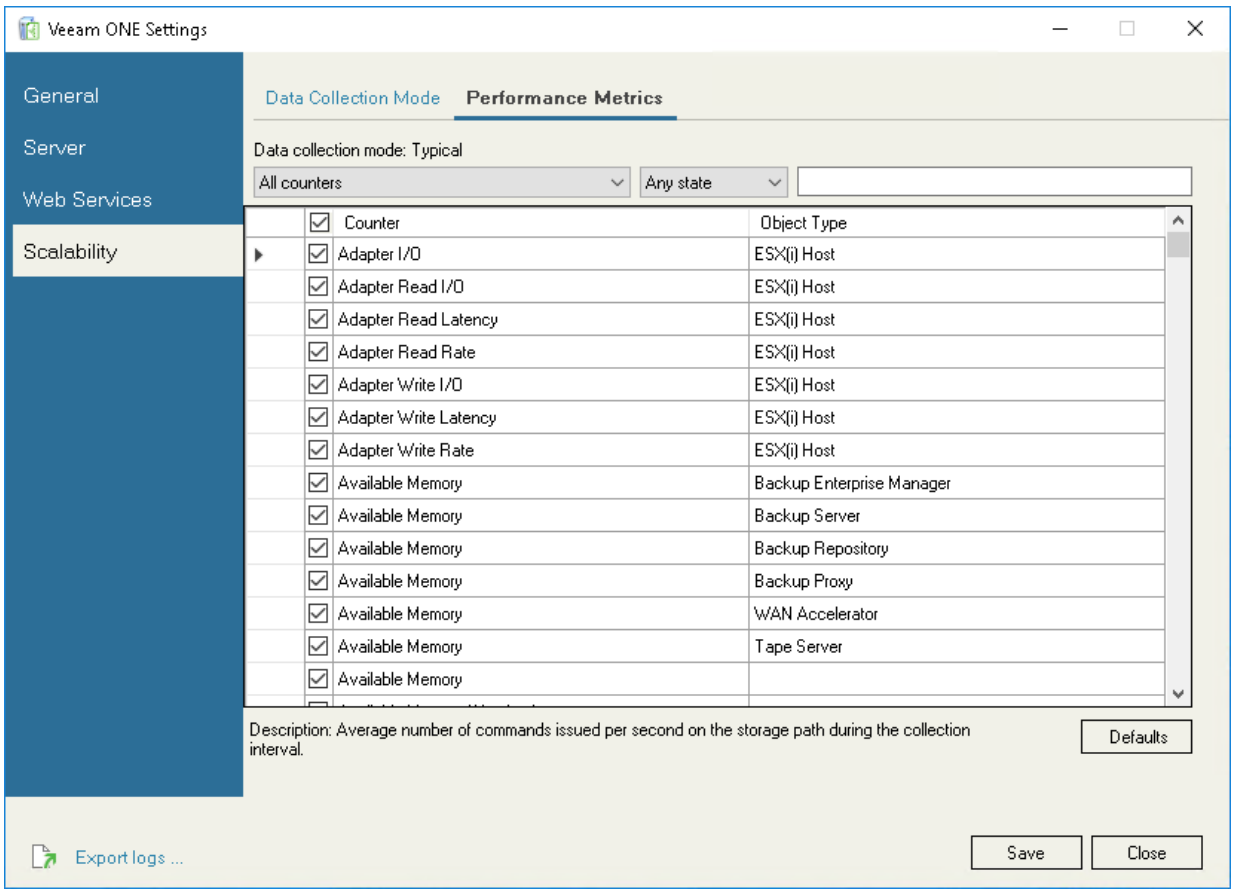
Performance Metrics

On the **Performance metrics** tab, you can explicitly define metrics that Veeam ONE must collect.

The list of metrics that Veeam ONE collects depends on the selected data collection mode. However, you can also manually add a number of performance metrics to that list.

To choose performance metrics that must be collected:

1. In the **Counters** drop-down list, select an infrastructure object to which metrics pertain.
2. In the **State** drop-down list, select the metrics state (*Enabled*, *Disabled*, *Any state*).
3. To quickly find the necessary metric, type the metric name in the search field on the right.
4. Select check boxes next to metrics that Veeam ONE must collect.
5. Click **Save**.



Click **Defaults** to restore Veeam ONE default settings for performance metrics, and select only those metrics that must be collected in accordance with the chosen data collection mode.

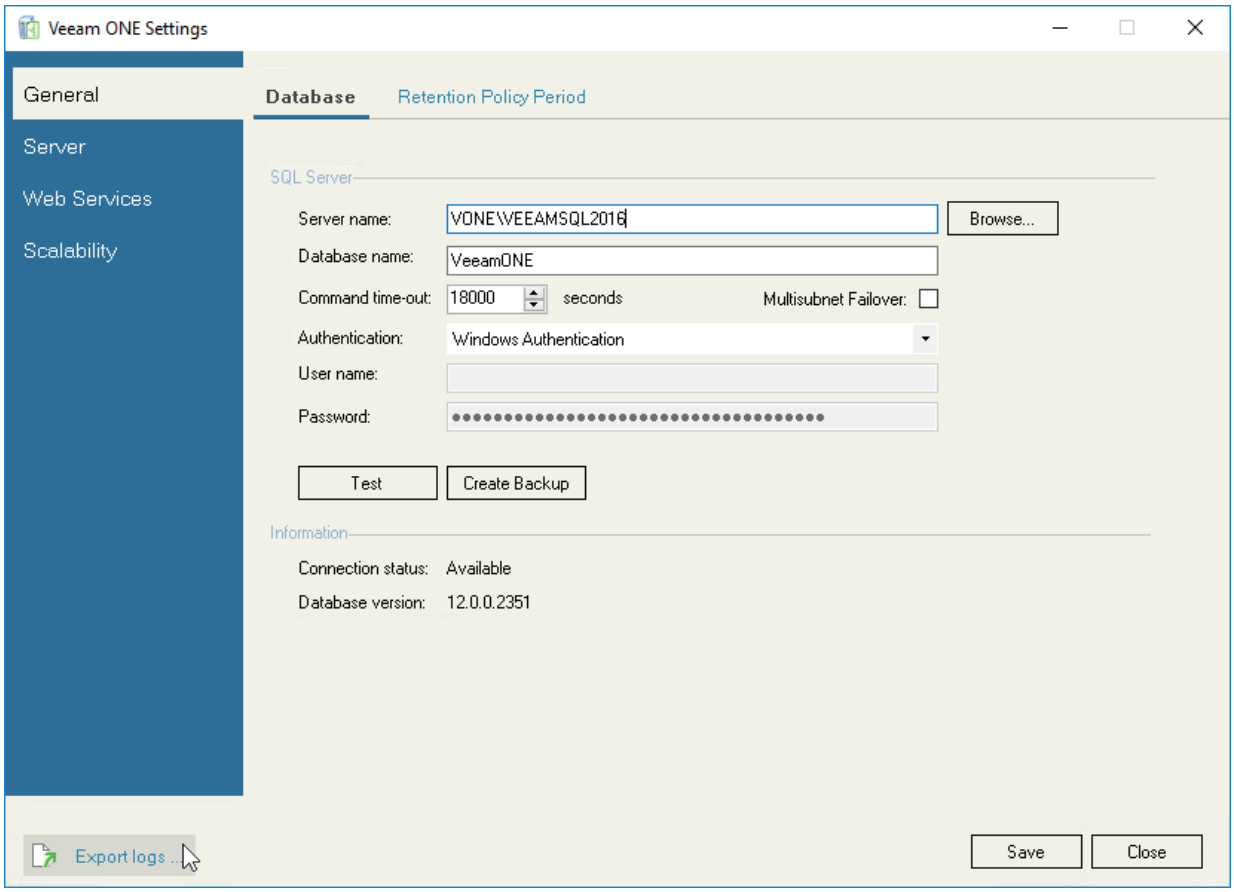
Exporting Logs

Diagnostic logs include information that can be used by the Veeam Support Team to troubleshoot issues that occur in Veeam ONE. In addition, diagnostic logs include information about the managed virtual and backup infrastructures. This type of information is used to speed up the root cause analysis when troubleshooting issues.

Veeam ONE Settings utility allows you to export diagnostic logs for the Monitoring and Reporting services:

1. At the bottom left corner of the Veeam ONE Settings utility, click **Export logs**.
2. Specify a location where the exported logs must be saved.

   The Veeam ONE Settings utility will export logs and save them to a `ZIP` archive in the specified location.



Grouping Expressions Syntax

You can create custom grouping expressions for categories with dynamic groups. In grouping expressions, you can use:

- Object Properties
- Operators
- Functions
- Keywords
- Constants

This section describes components that you can use in grouping expressions.

Object Properties

To create grouping expressions, you can use properties of the following types of objects:

- Host
- Storage
- Cluster
- Virtual Machine
- Computer
- Enterprise Application

Host

The following properties of host systems are supported in grouping expressions.

Property	Return Data Type	Description
CustomAttribute	Text (string)	Returns a value of a custom attribute assigned to a host. Specify the name of a custom attribute in brackets. For example, `CustomAttribute("department")` will return the value of the *'department'* attribute for a host. **Note**: • This property is available for VMware vSphere hosts only. • You cannot use methods to define the custom attribute name. However, the CustomAttribute property can be used to define values in methods.
CustomProperty	Text (string)	Returns a value of a custom property assigned to a host. Specify the name of a custom property in brackets. For example, `CustomProperty("department")` will return the value of the *'department'* property for a host. **Note**: This property is available for Microsoft Hyper-V hosts only.
Tag	Text (string)	Returns a tag assigned to a host. Specify the name of a tag category in brackets. For example, `Tag("department")` will return the tag of the *'department'* category for a host. **Note**: This property is available for VMware vSphere 5.5 or later.
Name	Text (string)	Returns a host name.

Property	Return Data Type	Description
Memory	Numeric (double precision floating-point number)	Returns an amount of host physical memory, in GB.
Location	Text (string)	Returns a location assigned to a host in Veeam Backup & Replication.
ProcessorCores	Numeric (integer)	Returns a number of processor cores for a host.
CPUFrequency	Numeric (double precision floating-point number)	Returns a CPU frequency, in MHz.
VMCount	Numeric (integer)	Returns a number of VMs registered on a host.
Datacenter	Text (string)	Returns a name of a datacenter.
HostModel	Text (string)	Returns a host model. **Note**: This property is available for VMware vSphere hosts only.
CPUSockets	Numeric (integer)	Returns a number of CPU sockets for a host.
InfrastructureLocation	Text (string)	Returns a path to a host in the virtual infrastructure.
Connection_State	Text (string)	Returns a connection state of a host.
PowerState	Text (string)	Returns a power state of a host.

Storage

The following properties of storage systems are supported in grouping expressions.

Property	Return Data Type	Description
CustomAttribute	Text (string)	Returns a value of a custom attribute assigned to a storage. Specify the name of a custom attribute in brackets. For example, `CustomAttribute("department")` will return the value of the *'department'* attribute for a storage. **Notes**: • This property is available for VMware vSphere storage systems only. • You cannot use methods to define the custom attribute name. However, the CustomAttribute property can be used to define values in methods.
Tag	Text (string)	Returns a tag assigned to a storage. Specify the name of a tag category in brackets. For example, `Tag("department")` will return the tag of the *'department'* category for a storage. **Note**: This property is available for VMware vSphere 5.5 or later.
Name	Text (string)	Returns a storage object name.
Capacity	Numeric (double precision floating-point number)	Returns storage capacity, in GB.
FileSystemType	Text (string)	Returns a type of storage file system, such as VMFS or NTFS.
FreeSpace	Numeric (double precision floating-point number)	Returns an amount of free storage space, in GB.
UsedSpace	Numeric (double precision floating-point number)	Returns an amount of used storage space, in GB.

Property	Return Data Type	Description
VMCount	Numeric (integer)	Returns a number of VMs whose files reside on a storage object.
Type	Text (string)	Returns a storage type (*Shared* or *Local*).
InfrastructureLocation	Text (string)	Returns a path to a storage object in the virtual infrastructure.
Datacenter	Text (string)	Returns a name of a datacenter.
DatastoreCluster	Text (string)	Returns a name of a cluster where storage object resides. **Note**: This property is available for VMware vSphere storage objects only.

Cluster

The following properties of clusters are supported in grouping expressions.

Property	Return Data Type	Description
CustomAttribute	Text (string)	Returns a value of a custom attribute assigned to a cluster. Specify the name of a custom attribute in brackets. For example, `CustomAttribute("department")` will return the value of the *'department'* attribute for a cluster. **Notes**: • This property is available for VMware vSphere clusters only. • You cannot use methods to define the custom attribute name. However, the CustomAttribute property can be used to define values in methods.
CustomProperty	Text (string)	Returns a value of a custom property assigned to a cluster. Specify the name of a custom property in brackets. For example, `CustomProperty("department")` will return the value of the *'department'* property for a cluster. **Note**: This property is available for Microsoft Hyper-V clusters only.

Property	Return Data Type	Description
Tag	Text (string)	Returns a tag assigned to a cluster. Specify a name of a tag category in brackets. For example, `Tag("department")` will return the tag of the *'department'* category for a cluster. **Note**: This property is available for VMware vSphere 5.5 or later.
Name	Text (string)	Returns a cluster name.
CPUFrequency	Numeric (integer)	Returns cluster CPU frequency, in MHz.
Connection_State	Text (string)	Returns a connection state of a cluster. **Note**: This property is available for Microsoft Hyper-V clusters only.
Datacenter	Text (string)	Returns a name of a datacenter.
HostCount	Numeric (integer)	Returns a number of hosts in a cluster.
Memory	Numeric (integer)	Returns a memory size of a cluster, in MB.
ProcessorCores	Numeric (integer)	Returns a sum of cores for all hosts in a cluster.
VMCount	Numeric (integer)	Returns a number of VMs whose files reside in a cluster.
InfrastructureLocation	Text (string)	Returns a path to a cluster in the virtual infrastructure.
IsDRSEnabled	Text (string)	Returns a flag that indicates if distributed resource scheduler enabled in a cluster. **Note**: This property is available for VMware vSphere clusters only.
Location	Text (string)	Returns a location assigned to a host in Veeam Backup & Replication.

Virtual Machine

The following properties of VMs are supported in grouping expressions.

Property	Return Data Type	Description
BackupJob	Text (string)	Returns a name of a backup job that protects a VM.
BackupRPO	Numeric (integer)	Returns the number of hours that passed since last backup session completed.
CheckpointCreateTime	Date and time	Returns the date and time when a checkpoint was created, in the `mm/dd/yyyy hh:mm:ss` format. **Notes**: • This property is available for Microsoft Hyper-V VMs only. • If a VM has several checkpoints, the property returns the creation date of the current checkpoint.
ComputerName	Text (string)	Returns a domain name assigned to a VM.
Connection_State	Text (string)	Returns a connection state of a VM.
CustomAttribute	Text (string)	Returns a value of a custom attribute assigned to a VM. Specify the name of a custom attribute in brackets. For example, `CustomAttribute("department")` will return the value of the *'department'* attribute for a VM. **Notes**: • This property is available for VMware vSphere VMs only. • You cannot use methods to define the custom attribute name. However, the CustomAttribute property can be used to define values in methods.
CustomProperty	Text (string)	Returns a value of a custom property assigned to a VM. Specify the name of a custom property in brackets. For example, `CustomProperty("department")` will return the value of the *'department'* property for a VM. **Note**: This property is available for Microsoft Hyper-V VMs only.
CPUFrequency	Numeric (double precision floating-point number)	Returns a frequency of a CPU in MHz. **Note**: This property is available for Microsoft Hyper-V VMs only.

Property	Return Data Type	Description
Datacenter	Text (string)	Returns a name of a datacenter where a VM resides.
Datastore	Text (string)	Returns the name of a storage system (datastore) where VM files reside. **Note**: If VM files reside on several datastores, the property returns the name of a datastore where the VM configuration file is located.
GuestOS	Text (string)	Returns a VM guest OS.
HasBackups	Text (string)	Returns a flag indicating whether a VM has backups or not (*Yes*, *No*).
HasSnapshots	Text (string)	Returns a flag indicating whether a VM has snapshots or not (*Yes*, *No*). **Note**: This property is available for VMware vSphere VMs only.
HasCheckpoints	Text (string)	Returns a flag indicating whether a VM has checkpoints or not (*Yes*, *No*). **Note**: This property is available for Microsoft Hyper-V VMs only.
Host	Text (string)	Returns a name of a host on which a VM resides.
InfrastructureLocation	Text (string)	Returns a path to a VM in the virtual infrastructure.
IpAddress	Text (string)	Returns an IP address assigned to a VM.
IsReplica	Text (string)	Returns a flag indicating whether a VM is a replica of an original VM.
IsShielded	Text (string)	Returns a flag indicating whether a VM is shielded. **Note**: This property is available for Microsoft Hyper-V VMs only.
LastBackupDate	Date and time	Returns the date and time when the latest backup session was performed for a VM in Veeam Backup & Replication, in the `mm/dd/yyyy hh:mm:ss` format. **Note**: The backup session is returned only if a restore point was created as a result of this session.

Property	Return Data Type	Description
Location	Text (string)	Returns a location assigned to a VM in Veeam Backup & Replication.
Memory	Numeric (double precision floating-point number)	Returns the amount of memory allocated to a VM.
Name	Text (string)	Returns a VM name.
Network	Text (string)	Returns the network to which a VM is connected. **Note**: If a VM is connected to several networks, the property will return a random network.
PowerState	Text (string)	Returns a VM power state. • For VMware vSphere: *Powered On*, *Powered Off*, *Suspended* • For Microsoft Hyper-V: *Powered Off*, *Running*, *Saved*
ReplicationJob	Text (string)	Returns a name of a replication job in which a VM is included in Veeam Backup & Replication. **Note**: If a VM is included in several replication jobs, the property will return a random job.
ReplicationRPO	Numeric (integer)	Returns the number of hours that passed since last replication session completed.
SnapshotAge	Numeric (integer)	Returns how many hours ago a snapshot was created. **Note**: This property is available for VMware vSphere VMs only.
SnapshotCreateTime	Date and time	Returns the date and time when a snapshot was created, in the `mm/dd/yyyy hh:mm:ss` format. **Notes**: • This property is available for VMware vSphere VMs only. • If a VM has several snapshots, the property returns the creation date of the latest snapshot.

Property	Return Data Type	Description
Tag	Text (string)	Returns a tag assigned to a VM. Specify the name of a tag category in brackets. For example, `Tag("department")` will return the tag of the *'department'* category for a VM. **Note**: This property is available for VMware vSphere 5.5 or later.
vCPU	Numeric (integer)	Returns the number of vCPUs configured for a VM.
VirtualDiskSize	Numeric (double precision floating-point number)	Returns the amount space occupied by all VM disks.
VMFolder	Text (string)	Returns a name of a folder where VM files reside. **Note**: This property is available for VMware vSphere VMs only.
VMFolderPath	Text (string)	Returns a user path to a VM in the virtual infrastructure. **Note**: This property is available for VMware vSphere VMs only.

Computer

The following properties of protected computers are supported in grouping expressions.

Property	Return Data Type	Description
BackupServer	Text (string)	Returns a name of Veeam Backup & Replication server that manages the backup agent.
LastBackupDate	Date and time	Returns the date and time when the latest backup session was performed for a computer in Veeam Backup & Replication, in the `mm/dd/yyyy hh:mm:ss` format.
BackupRPO	Numeric (integer)	Returns a number of hours that passed since last backup session completed.
BpAgentLicenseType	Text (string)	Returns a type of license installed on a backup agent.

Property	Return Data Type	Description
Location	Text (string)	Returns a location assigned to a computer in Veeam Backup & Replication.
BpAgentManagementType	Text (string)	Returns a management type of a backup agent (*Standalone*, *Managed by VBR*).
Name	Text (string)	Returns a name of a computer that runs a backup agent.
ProtectedComputersGroup	Text (string)	Returns a name of a protection group for a computer.
ClusterName	Text (string)	Returns a name of a failover cluster in which a computer resides.
IpAddress	Text (string)	Returns an IP address assigned to a computer that runs a backup agent.
FQDN	Text (string)	Returns an FQDN assigned to a computer that runs a backup agent.
JobName	Text (string)	Returns a name of a job that runs on a backup agent.
PolicyName	Text (string)	Returns a name of a backup policy assigned to a backup agent.

Enterprise Application

The following properties of protected enterprise applications are supported in grouping expressions.

Property	Return Data Type	Description
ApplicationPolicyName	Text (string)	Returns a name of a backup policy configured for an application.
BackupRPO	Numeric (integer)	Returns a number of hours that passed since last backup session completed.

Property	Return Data Type	Description
BackupServer	Text (string)	Returns a name of Veeam Backup & Replication server that manages the application plug-in.
FQDN	Text (string)	Returns an FQDN assigned to a server that runs a protected application.
HasDataBackupSessions	Text (string)	Returns a flag indicating whether an application has backup policies configured or not (*Yes*, *No*).
IpAddress	Text (string)	Returns an IP address assigned to a server that runs a protected application.
LastBackupDate	Date and time	Returns the date and time when the latest backup session was performed for an application in Veeam Backup & Replication, in the `mm/dd/yyyy hh:mm:ss` format.
Location	Text (string)	Returns a location assigned to an application server in Veeam Backup & Replication.
Name	Text (string)	Returns a name of a server that runs an application.
ProtectionGroup	Text (string)	Returns a name of a protection group for an applications.

Operators

To manipulate values in grouping expressions, you can use the following operators:

Operator	Return Data Type	Description	Example
+	Text (string) Numeric	Joins two string values to one string. Adds two numeric values.	For a VM included in a replication job, expression `"Replication Job: " + ReplicationJob` retuns a string similar to *Replication Job: Webserver Daily Replication*. Expression `2 + 2` returns 4. Expression `2.05 + 1` returns 3.05.
*	Numeric	Multiplies numeric values.	Expression `2 * 2` returns 4. Expression `100 * 0.5` returns 50.
/	Numeric	Divides first numeric value into the second.	Expression `2 / 2` returns 1. Expression `100 / 50` returns 2.
-	Numeric	Subtracts the second numeric value from the first.	Expression `2 - 1` returns 1. Expression `100 - 0.5` returns 99.5.
<	Boolean	Less than. Returns *True* if the value of left operand is less than the value of right operand. Otherwise, returns *False*.	For a VM, expression `Memory < 2048` returns *True* if the amount of memory configured for a VM is less than 2048 MB.
<=	Boolean	Less than or equal to. Returns *True* if the value of left operand is less than or equal to the value of right operand. Otherwise, returns *False*.	For a VM, expression `Memory <= 2048` returns *True* if the amount of memory configured for a VM is less than or equal to 2048 MB.
>	Boolean	Greater than. Returns *True* if the value of left operand is greater than the value of right operand. Otherwise, returns *False*.	For a VM, expression `Memory > 2048` returns *True* if the amount of memory configured for a VM is greater than 2048 MB.

Operator	Return Data Type	Description	Example
>=	Boolean	Greater than or equal to. Returns *True* if the value of left operand is greater than or equal to the value of right operand. Otherwise, returns *False*.	For a VM, expression `Memory >= 2048` returns *True* if the amount of memory configured for a VM is greater than or equal to 2048 MB.
=	Boolean	Equal. Returns *True* if the value of left operand is the same as the value of right operand. Otherwise, returns *False*.	For a VM, expression `Memory = 2048` returns *True* if the amount of memory configured for a VM is equal to 2048 MB. For a VM, expression `Name = "vdi001"` returns *True* if the VM name is *vdi001*.
<>	Boolean	Not equal. Returns *True* if the value of left operand is not the same as the value of right operand. Otherwise, returns *False*.	For a VM, expression `Memory <> 2048` returns *True* if the amount of memory configured for a VM is less or greater than 2048 MB. For a VM, expression `Tag(department) <> "support"` returns *True* if a tag of the *department* category assigned to a VM is other than *support*.
and	Text (string)	Joins conditions with a logical AND operator.	For a VM, expression `Memory = 2048 and Name = "vdi001"` returns *True* if the amount of memory configured for a VM is equal to 2048 MB and the VM name is *vdi001*.
or	Text (string)	Joins conditions with a logical OR operator.	For a VM, expression `Memory = 2048 or Name = "vdi001"` returns *True* if the amount of memory configured for a VM is equal to 2048 MB or the VM name is *vdi001*.

Functions

To manipulate values in grouping expressions, you can use the following functions:

Function	Return Data Type	Description	Example
DateAdd	Date	Returns a date value to which a time interval has been added, or from which a time interval has been subtracted. The function accepts the following arguments: 1. Date and time to which a time interval must be added, in the `YYYY-MM-DD` format. 2. Time interval that must be added to the initial date and time. The interval can be a positive or negative number. 3. Measurement unit of the time interval ("h" - hour, "d" - day, "m" - month, "y" - year).	Expression `DateAdd("2016-10-20", 7, "d")` adds 7 days to the specified date, and returns *2016-10-27*. Nested expression `SnapshotCreateTime < DateAdd (DateAdd(Today, -2, "d"))` returns *True* if the latest VM snapshot was created earlier than 2 days and 12 hour ago.
IndexOf	Numeric (integer)	Returns the position of the first occurrence of a specified value (substring) in a string. Index of the first character in a string is 0. Returns -1 if the value is not found within the string. The function accepts the following arguments: 1. String value. 2. Substring value whose index position must be found within the string value.	Expression `IndexOf("vdi001_mrk", "_")` returns *6*. Expression `IndexOf("vdi001", "_")` returns *-1*.

Function	Return Data Type	Description	Example
Left	Text (string)	Returns a substring that contains a specified number of characters from the left side of a string. The function accepts the following arguments: 1. String value. 2. Number of characters from the left side of a string to return.	Expression `Left("vdi001_mrk", 6)` returns *vdi001*. Nested expression `Left("vdi001_replica", IndexOf("vdi002_replica", "_"))` returns *vdi002*.
Length	Numeric (integer)	Returns the number of characters in a string. The function accepts a string value as an argument.	Expression `Length("123456789")` returns *9*. For a VM, expression `Length("Name")` returns the number of characters in the VM name.
Replace	Text (string)	Returns a string in which a specified substring has been replaced with another substring. The function accepts the following arguments: 1. String value. 2. Substring value that must be replaced. 3. Substring value that must replace the sought substring. **Note**: If the there are two or more equal substrings in a string, all substrings will be replaced.	Expression `Replace("vdi002 mrk", " ", "_")` changes the *vdi002 mrk* value to *vdi002_mrk*. For a VM, expression `Replace(Name, "_replica", "")` removes the *_replica* suffix from the VM name.
Right	Text (string)	Returns a substring that contains a specified number of characters from the right side of a string. The function accepts the following arguments: 1. String value. 2. Number of characters from the right side of a string to return.	Expression `Right("vdi003_mrk", 3)` returns *mrk*. Nested expression `Right("vdi003_replica", (IndexOf("vdi003_replica", "_")) + 1)` returns *replica*.

Function	Return Data Type	Description	Example
Space	Text (string)	Returns a string that consists of the specified number of spaces. The function accepts a positive integer as an argument.	Nested expression `Replace("vdi004_mrk", "_", Space(1))` changes the *vdi004_mrk* value to *vdi004 mrk*.
Substring	Text (string)	Retrieves a substring from a specified string. The substring starts at the specified character position (index) and has the specified length. Index of the first character in a string is 0. The function accepts the following arguments: 1. String value. 2. Start index position of a substring that must be retrieved. 3. Number of characters to retrieve starting with the specified index position.	Expression `Substring("vdi005_mrk", 7, 3)` returns *mrk*.
Trim	Text (string)	Returns a string with no leading or trailing spaces. The function accepts a string value as an argument.	Expression `Trim("  vdi006  ")` returns *vdi006*.
TrimLeft	Text (string)	Returns a string with no leading spaces. The function accepts a string value as an argument.	Expression `Trim("  vdi007")` returns *vdi007*.
TrimRight	Text (string)	Returns a string with no trailing spaces. The function accepts a string value as an argument.	Expression `Trim("vdi008  ")` returns *vdi008*.

Function	Return Data Type	Description	Example
ToDate	Date	Converts a string containing a valid date representation to the DateTime format. **Note**: The function is based on the DateTime.TryParse function and accepts the same input values.	Expression `ToDate("2009/03/12")` returns *2009-03-12*. Expression `ToDate("ToDate("2009/03/01")` returns *2009-03-01*.
ToLowerCase	Text (string)	Converts a string to lower case letters. The function accepts a string value as an argument.	Expression `ToLowerCase("LoWeRCaSe")` returns *lowercase*.
ToUpperCase	Text (string)	Converts a string to upper case letters. The function accepts a string value as an argument.	Expression `ToUpperCase("uppercase")` returns *UPPERCASE*.

Keywords

The logical operator `CASE` represents an *if-else* statement. It is used to evaluate a certain condition and execute an expression if this condition is true. If the condition is false, another expression is executed.

The `CASE` operator has the following syntax:

```
CASE
WHEN "Value" = "1" THEN "Expression 1"
ELSE "Expression 2"
END
```

Here:

- `WHEN` statement represents a condition that must be evaluated.
- `THEN` statement specifies a group to which an object must be placed if the condition is true.
- `ELSE` specifies a group to which an object must be placed if the condition is false.

You can include multiple `WHEN` statements to evaluate multiple conditions:

```
CASE
WHEN "Value" = "1" THEN "Expression 1"
WHEN "Value" = "2" THEN "Expression 2"
WHEN "Value" = "3" THEN "Expression 3"
ELSE "Expression 4"
END
```

Limitations

You cannot nest one CASE expression within another `CASE` expression. However, you can include methods to define values in a `CASE` statement.

Example

Business View includes a number of predefined categories that use `CASE` grouping expressions. You can use these predefined categories to understand how the `CASE` operator works.

For example, the *VMs with Snapshot* category uses the following grouping expression.

```
CASE
WHEN HasSnapshots = "No" THEN "No snapshots"
WHEN SnapshotCreateTime < DateAdd(Today, -30, "d") THEN "Older than 30 days"
WHEN SnapshotCreateTime < DateAdd(Today, -7, "d") THEN "Older than 7 days"
WHEN SnapshotCreateTime < DateAdd(Today, -1, "d") THEN "Older than 1 day"
ELSE "Recent snapshots"
END
```

Here:

- The first `WHEN` statement checks whether a VM has any snapshots. If a VM has no snapshots, this VM is included in the *No snapshots* group.
- The second, third and fourth `WHEN` statements check VM snapshot age. If the age more than 30 days, a VM in included in the *Older than 30 days* group. If the age more than 7 days, a VM in included in the *Older than 7 days* group. If the age more than 1 day, a VM in included in the *Older than 1 day* group.
- The `ELSE` statement includes in the *Recent snapshots* group all VMs with snapshots not older than 1 day.

Constants

To create grouping expressions, you can use the following constants.

Constant	Return Data Type	Description
vCenter	Text (string)	Returns the name of a virtualization server that manages a host, storage or VM.
Today	Date and time	Returns the current date and time in the `YYYY-MM-DDThh:mm:ss` format.