



Veeam Backup & Replication

Version 13

Veeam Kasten Integration 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	5
ABOUT THIS DOCUMENT	6
OVERVIEW	7
BACKUP INFRASTRUCTURE COMPONENTS	8
PLANNING AND PREPARATION	10
System Requirements	11
Limitations and Considerations	12
Used Ports	13
Required Permissions	14
Licensing	15
DEPLOYMENT AND CONFIGURATION	16
Installing Plug-In	18
Adding Kasten Instance	19
Step 1. Launch New Kasten Instance Wizard	20
Step 2. Specify Kasten Instance Name	21
Step 3. Specify Credentials	22
Step 4. Apply Settings	24
Step 5. Finish Working with Wizard	25
Managing Kasten Instance	26
Viewing Snapshots and Backups	27
Editing Instance Settings	28
Opening Instance Web UI	29
Removing Instance	30
Rescanning Instance	31
DATA PROTECTION	32
How Kasten Policy Works	33
Working with Kasten Policies	34
Creating Kasten Policies	35
Managing Kasten Policies	36
Backup Chain and Retention Policy	41
Managing Backed-Up Data	42
Viewing Backup Properties	43
Deleting Backups	44
Exporting Kasten Backups Manually	46
Creating Backup Copy Jobs	47
Copying Data to Cloud Repositories	48
Creating Backups to Tapes	49

Viewing Statistics	50
DATA RECOVERY.....	51
Restoring to Kubernetes	52
Exporting Disks	53
Instant First Class Disk (FCD) Recovery	54
Restoring Guest OS Files	55
Exporting Backup Files.....	56
Viewing Statistics	57
SUPPORT INFORMATION	58

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 document describes the first steps you must perform after setting up an infrastructure for the Veeam Plug-In for Kasten solution.

Intended Audience

This document is intended for administrators who has just set up an infrastructure for the Veeam Plug-In for Kasten solution.

Overview

Veeam Plug-In for Kasten is a solution that allows you to create and manage data protection and disaster recovery tasks for Veeam Kasten environments. Veeam Plug-In for Kasten extends the Veeam Backup & Replication functionality and provides access to Veeam Plug-In for Kasten in Veeam Backup & Replication console.

NOTE

Veeam Plug-In for Kasten is built on top of Veeam Backup & Replication, and this guide assumes that you have a good understanding of the Veeam Backup & Replication solution and Veeam Kasten solutions.

With Veeam Plug-In for Kasten, you can perform the following operations in Veeam Backup & Replication console:

- Add the Veeam Kasten instance to Veeam Backup & Replication infrastructure, manage and remove it.
- Manage Veeam Kasten policies from Veeam Backup & Replication infrastructure.
- View Veeam Kasten backups exported by Veeam Kasten policies.
- Restore from Veeam Kasten backups.
- Restore from Veeam Kasten snapshots.
- Monitor session statistics.

If you export Veeam Kasten backups to the Veeam backup repository, you can also perform the following operations:

- Remove backups exported by Veeam Kasten policies from the Veeam Backup & Replication infrastructure.
- Synthesize an independent full backup file using restore points that are located in your Veeam backup repositories.
- Export disks.
- Perform First Class Disk Recovery.
- Restore guest OS files and folders of backups.
- Export backup files.

NOTE

If you export Veeam Kasten backups to other than the Veeam backup repository, you will be able to view these backups in the Veeam Backup & Replication console. For all other operations you will be navigated to the Veeam Plug-In for Kasten web console.

Backup Infrastructure Components

To export backups created by Veeam Kasten policies using Veeam Plug-In for Kasten, you must configure the infrastructure that will consist of the following components:

1. Kasten application

A platform where you configure and manage Veeam Kasten policies that will export backups of application disks to Veeam backup repositories. For more information on installing a Kasten application, see [Veeam Kasten Docs](#).

2. Veeam Backup & Replication server

A server that manages Veeam Kasten appliance and policies. It allows you to monitor and manage backups exported by Veeam Kasten, perform data protection scenarios, data recovery and restore operations. For more information, see the [Backup Server](#) section in the Veeam Backup & Replication User Guide.

3. Veeam backup repository

This component is obligatory if you use Veeam backup repository to keep exports created by Veeam Kasten policies.

A storage location where Veeam Backup & Replication keeps backups exported by Veeam Kasten policies. You can add multiple repositories to the Veeam Backup & Replication server and set the necessary repository within Veeam Kasten policies settings.

To learn more about Veeam backup repositories and how to manage them, see the [Backup Repositories](#) section in the Veeam Backup & Replication User Guide.

NOTE

We recommend that you use Veeam backup repositories that support the following file systems:

- ReFS for Microsoft Windows and SMB repositories
- XFS for Linux repositories

You can also use backup repositories that utilize deduplication:

- Dell Data Domain with DD Boost
- HPE StoreOnce with Catalyst
- ExaGrid Tiered Backup Storage
- Quantum DXi
- Fujitsu ETERNUS CS800
- Infinidat InfiniGuard

TIP

To prohibit data deletion or data loss due to malware activity, you can make data stored in Veeam backup repositories immutable. Note that this option is available only for hardened repositories. For more information, see the [Hardened Repository](#) section in the Veeam Backup & Replication User Guide. For more information on how to properly configure Veeam Kasten to make backups exported by Veeam Kasten policies immutable, see [Veeam Kasten Docs](#).

4. Additional data protection layers

Veeam Backup & Replication allows you to keep backups exported by Veeam Kasten in the following types of additional repositories:

- Capacity tier: for more information, see the [Capacity Tier](#) section in the Veeam Backup & Replication User Guide.
- Archive tier: for more information, see the [Archive Tier](#) section in the Veeam Backup & Replication User Guide.
- Tape devices: for more information on how to back up to tapes, see the [Backup to Tape](#) section in the Veeam Backup & Replication User Guide.
- Cloud repositories of service providers that keep copies of backups exported by Veeam Kasten policies. For more information, see the [Veeam Cloud Connect Guide](#).
- Secondary Veeam backup repositories that keep backup copies created by backup copy jobs. For more information on backup copy jobs, see the [Backup Copy](#) section in the Veeam Backup & Replication User Guide.

IMPORTANT

Before you deploy the Veeam backup infrastructure, see the following [System Requirements](#).

What You Do Next

[Deployment and Configuration](#)

Planning and Preparation

Before you start using the Veeam Plug-In for Kasten solution, make sure that the backup infrastructure components meet system requirements, all required ports are open, and Veeam backup repositories that you plan to use have the required access permissions.

System Requirements

Before you start using Veeam Plug-In for Kasten, consider the following:

Backup Server

The machine where the Veeam Kasten Plug-in for Veeam Backup & Replication will run must meet the system requirements described in the [System Requirements](#) section in the Veeam Backup & Replication User Guide.

Additionally, the following software must be installed:

- Microsoft .NET Core Runtime 8.0
- Microsoft ASP.NET Core Shared Framework 8.0

IMPORTANT

Microsoft ASP.NET Core Shared Framework and Microsoft .NET Core Runtime must be of the same version (up to the minor version number).

For example, if the version of Microsoft ASP.NET Core Shared Framework is 8.0.8, then the version of Microsoft .NET Core Runtime must also be 8.0.8.

Starting from version 6.5.9, Veeam Plug-In for Kasten no longer supports Veeam Backup & Replication installed on Microsoft Windows Server 2012 and 2012 R2.

Kubernetes Distribution Requirements

Veeam Plug-In for Kasten supports only backup exports of Kubernetes persistent volumes to Veeam backup repositories. For details on which volumes are supported for export to a VBR repository, see [Veeam Kasten Docs](#).

Kasten Application Version

A Veeam Kasten application must be the 5.5.3 version or higher.

Kasten Dashboard Access

An external access to the Kasten dashboard must be set up. For more information, see [Veeam Kasten Docs](#).

Veeam Backup & Replication

Veeam Plug-In for Kasten version 13.2.1.60 supports integration with Veeam Backup & Replication version 13.01.

Veeam Backup Repositories Requirements

Veeam backup repositories, where you want to keep backups exported by Veeam Kasten policies, must meet the system requirements specified in the [Backup Repository Server](#) section in the Veeam Backup & Replication User Guide.

Limitations and Considerations

Consider the following limitations for Veeam Backup & Replication:

- Veeam Plug-In for Kasten does not support Kerberos for Kasten exports to Veeam backup repositories.
- Veeam Plug-In for Kasten does not support IPv6.
- Veeam Plug-In for Kasten does not sync Veeam Kasten retention (retire) sessions.
- A Veeam Kasten instance can operate with only one backup server. If you add it to another backup server, you will not be able to perform any operations with this Veeam Kasten instance on the first backup server.
- Veeam Plug-In for Kasten does not support Kasten exports to direct backup object storage repositories.
- If you delete Veeam Kasten policies created by the Veeam Kasten Multi-Cluster console on Kasten secondary servers, they will be recreated by the Veeam Kasten Multi-Cluster console.
- Veeam Plug-In for Kasten does not support Kasten export from Kasten instance that is not added to the Veeam Backup & Replication infrastructure.
- Veeam Plug-In for Kasten is not supported in the Veeam Backup & Replication web UI.
- If you work with Veeam Backup & Replication on Linux, you cannot use domain user for location profiles in Veeam Kasten.

Used Ports

Veeam Backup & Replication within the Veeam Plug-In for Kasten solution is deployed on a machine that uses the same ports as those listed in the [Ports](#) section of the Veeam Backup & Replication User Guide. Make sure to check that section and add any required ports to achieve the intended Veeam Backup & Replication and Veeam Kasten integration. In addition, Veeam Plug-In for Kasten also uses ports listed in the following table. For more information on Veeam Kasten network ports, see [this Kasten article](#).

NOTE

During installation, Veeam Backup & Replication automatically creates firewall rules for the required ports to allow communication for the application components.

From	To	Protocol	Port	Notes
Veeam Kasten	Veeam Backup & Replication server	TCP	10006	Port used to connect to the Veeam Backup & Replication server.
	VBR RestAPI Service	HTTPS	9419	Port used to validate Veeam Backup & Replication Location Profile.
	Veeam backup repository	TCP	6162 2500 to 3300	Default range of ports used for communication with a backup repository. Note: The port range 2500-3300 is optional. You can use it for failover if port 6162 is unavailable.
Backup server	Backup server	TCP/HTTPS	6172	Used by the Kasten Plug-in for Veeam Backup & Replication to enable communication with the Veeam Backup & Replication database.
	Veeam Kasten	TCP/HTTPS	443	Used by the Kasten Plug-in for Veeam Backup & Replication to connect to Kasten.
Veeam Backup & Replication Remote Console	Veeam Kasten	TCP	443	Needed if you want to open Veeam Kasten instance web UI from Remote Console for restores or dashboard access.

Required Permissions

Make sure the user accounts that you plan to use have permissions described in the following sections.

Veeam Backup & Replication User Account Permissions

The user account you plan to use with Kasten while connecting to Veeam Backup & Replication must have the Veeam Backup Administrator role or must be added to the user group with this role. For more information, see [Managing Users and Roles](#) section in the Veeam Backup & Replication User Guide.

NOTE

If you work with Veeam Backup & Replication on Linux, you cannot use domain user for location profiles in Veeam Kasten.

Veeam Backup Repositories

Make sure that either the **Allow to everyone** or **Allow to the following accounts or groups only** access permissions are granted on Veeam backup repositories where you want to keep backups exported by Veeam Kasten policies. For more information, see the [Access Permissions \(Step 4\)](#) section in the Veeam Backup & Replication User Guide.

IMPORTANT

Do not change access permissions of repositories that already contain backup exported from Veeam Kasten, otherwise the Veeam Kasten policy will fail.

Licensing

If you want to use the Veeam Plug-In for Kasten solution, you must have the following types of product editions installed:

- Veeam Backup & Replication server requires either the Rental license or the Enterprise Plus product edition. For more information, see [Veeam Licensing Policy](#).
- Veeam Kasten requires a valid license to protect Kubernetes applications with Veeam Backup & Replication. For more information, see the [Veeam Kasten product page](#).

NOTE

Veeam licenses Veeam Backup & Replication in two ways: per instance and per socket. However, backups exported by the Veeam Kasten policy do not consume any instances or sockets. For more information on licensing, see the [Licensing](#) section in the Veeam Backup & Replication User Guide.

Deployment and Configuration

To be able to protect data with the Veeam Plug-In for Kasten solution, you must configure the Veeam Kasten instance and Veeam Backup & Replication infrastructure.

Configure Kasten Instance Infrastructure

A Veeam Kasten instance is a source environment that creates snapshots of applications running on Kubernetes persistent volumes. After that, Veeam Kasten makes exports of snapshot data to storage locations to keep this data. As a storage location, you can use Veeam backup repositories where the application persistent volumes are stored in a native Veeam format. While Veeam Kasten stores the persistent volume's images in the Veeam backup repository, it still requires a primary location to store any file based data and metadata. This location can be any additional storage type supported by Veeam Kasten, such as object storage or NFS.

The Veeam Kasten instance you plan to use in the Veeam Plug-In for Kasten infrastructure must meet the [system requirements](#). For more information on configuring the Veeam Kasten instance, see [Veeam Kasten Docs](#).

Configure Veeam Backup & Replication Infrastructure

To configure Veeam Backup & Replication infrastructure, complete the following steps:

1. **Install or upgrade Veeam Backup & Replication.**

After you install Veeam Backup & Replication, Veeam Plug-In for Kasten will be automatically installed along with Veeam Backup & Replication.

2. **Add Kasten instance.**

Add the Kasten instance to the Veeam Backup & Replication infrastructure to be able to create and manage Kasten policies. For more information, see [Adding Kasten Instance](#).

3. **[Optional] Deploy Veeam backup repositories.**

If you want to keep persistent volumes created by Veeam Kasten policies in Veeam backup repositories, you must add the Veeam backup repositories that will store backups exported by Veeam Kasten policies to Veeam Backup & Replication infrastructure. Make sure that you configured the [required permissions](#). For more information, see the [Backup Repositories](#) and [Adding Microsoft Windows Repositories](#) sections in the Veeam Backup & Replication User Guide.

4. **[Optional] Configure capacity and archive tier.**

Configure the capacity tier and archive tier to set an additional layer of storage. For more information, see [Capacity Tier](#) and [Archive Tier](#) sections in the Veeam Backup & Replication User Guide.

5. **[Optional] Configure Tape infrastructure.**

If you want to use tape devices to store Kubernetes persistent volumes. For more information, see the [Tape Devices Support](#) section in the Veeam Backup & Replication User Guide.

6. **[Optional] Configure Cloud Connect infrastructure.**

If you want to store copies of backed-up Kubernetes persistent volumes in cloud repositories of service providers, configure Cloud Connect infrastructure in a Veeam Backup & Replication console. For more information, see [Veeam Cloud Connect](#) User Guide.

NOTE

The additional level of protection (that is, capacity and archive tier, tape devices and cloud repositories of service providers) is available only if you export Kasten backups to the Veeam backup repository.

What You Do Next

After you configure the Veeam Kasten instance and add it to the Veeam Backup & Replication infrastructure, you are ready to [create Veeam Kasten policies](#) and perform data protection and data recovery options.

Installing Plug-In

Veeam Plug-In for Kasten is automatically installed while you install or upgrade Veeam Backup & Replication to the [required version](#). For more information, see the [Installing Veeam Backup & Replication](#) and [Upgrading Veeam Backup & Replication](#) sections in the Veeam Backup & Replication User Guide.

NOTE

Backups exported by Veeam Kasten to Veeam Backup & Replication 11 version will be available in your backup infrastructure after you upgrade to Veeam Backup & Replication version 12. However, you must [add the Veeam Kasten instance](#) to the backup infrastructure, otherwise the Veeam Plug-In for Kasten data protection and data recovery functionality will not be available.

Adding Kasten Instance

Veeam Plug-In for Kasten allows you to view and manage Kasten policies as well as perform data protection and data recovery operations with exports created by Kasten from the Veeam Backup & Replication console. To do it, you must add the Kasten instance to the Veeam Backup & Replication infrastructure.

After you add the Kasten instance to the Veeam Backup & Replication infrastructure, Veeam Plug-In for Kasten accesses Veeam Kasten and synchronizes the following information:

- Kasten policies.
- Snapshots and exports created by Kasten policies.
- Snapshots and exports created manually.
- Sessions for the last 24 hours.

After synchronization is completed, Veeam Plug-In for Kasten shows this information in the Veeam Backup & Replication console and performs incremental syncs every 5 seconds to get updates.

To add the Kasten instance to Veeam Backup & Replication infrastructure, do the following:

1. [Launch the New Kasten Instance wizard.](#)
2. [Specify the Kasten instance name.](#)
3. [Specify credentials.](#)
4. [Apply Settings.](#)
5. [Finish working with the wizard.](#)

Step 1. Launch New Kasten Instance Wizard

To launch the **New Kasten Instance** wizard, do one of the following:

- Open the **Backup Infrastructure** view. Navigate to **Managed Servers** and click **Add Server** on the ribbon. In the **Add Server** window, select **Veeam Kasten for Kubernetes**.
- Open the **Backup Infrastructure** view. In the inventory pane, right-click the **Managed Servers** node and select **Add Server**. In the **Add Server** window, select **Veeam Kasten for Kubernetes**.

Add Server ✕

Select the type of a server you want to add to your backup infrastructure. All already registered servers can be found under the Managed Servers node on the Backup Infrastructure tab.



Virtualization Platforms

Add supported virtual infrastructures to the inventory.



Veeam Infrastructure Appliance

Add a backup infrastructure host deployed from the Veeam Infrastructure Appliance ISO.



Microsoft Windows

Add a Microsoft Windows server to the inventory.



Linux

Add a Linux server to the inventory.



Veeam cloud-native backup appliance

Add Veeam Backup for AWS, Microsoft Azure and Google Cloud appliance to the inventory.



Veeam Kasten for Kubernetes

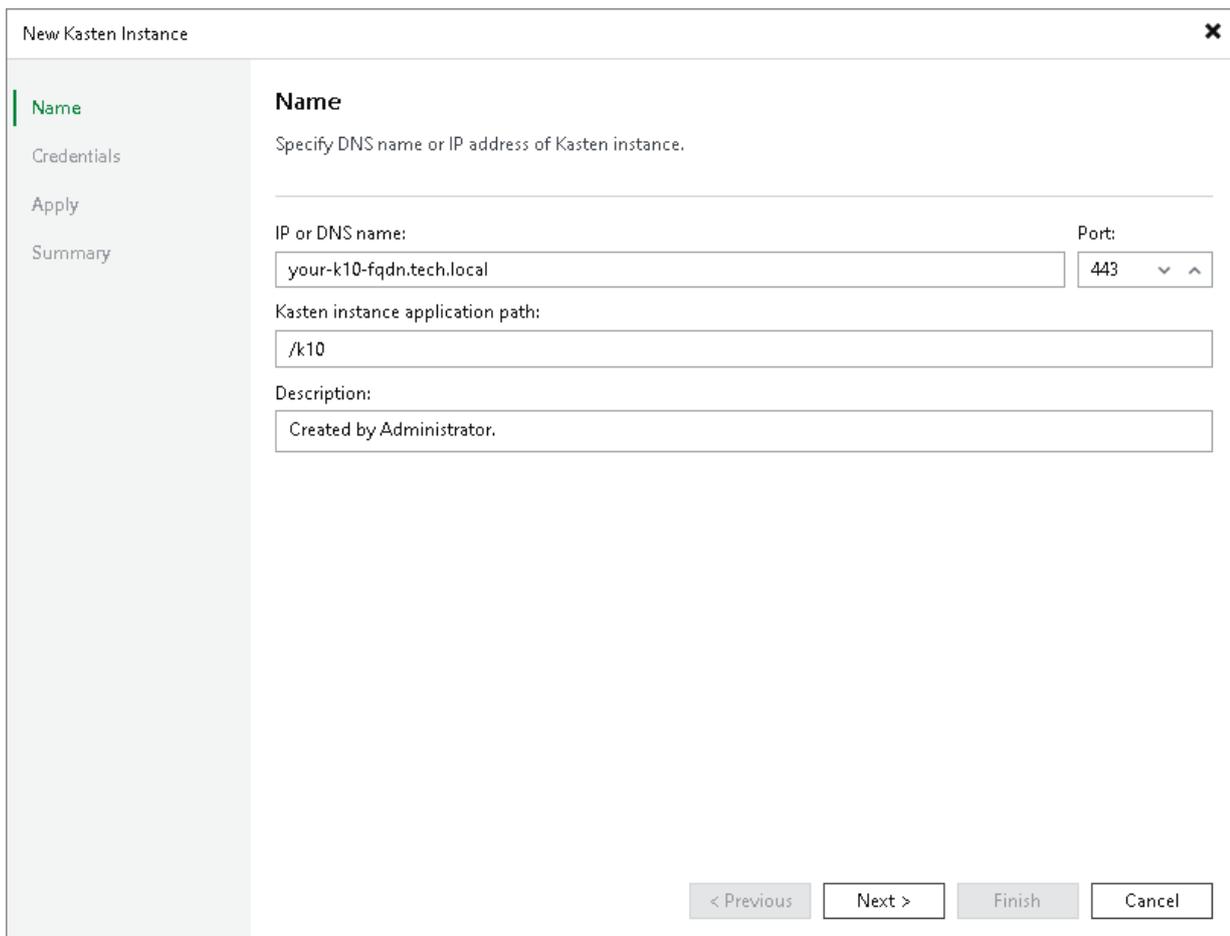
Connect to an existing Kasten instance.

Cancel

Step 2. Specify Kasten Instance Name

At the **Name** step of the **New Kasten Instance** wizard, specify an IP address or DNS name, a URL path and a description of the Veeam Kasten application.

1. In the **IP or DNS name** field, enter an IP address or DNS name. To specify the DNS name, use the following format: *your-k10-fqdn.tech.local*.
2. In the **Kasten instance application path**, provide a URL path to the Veeam Kasten dashboard.
3. In the **Description** field, provide a description of the Veeam Kasten application for future reference. The default description contains information about the user who created the Kasten instance, date and time when the instance was created.



The screenshot shows a window titled "New Kasten Instance" with a close button (X) in the top right corner. On the left side, there is a vertical navigation menu with four items: "Name" (highlighted in green), "Credentials", "Apply", and "Summary". The main content area is titled "Name" and contains the following fields:

- A heading "Name" followed by the instruction "Specify DNS name or IP address of Kasten instance."
- A horizontal line separator.
- A label "IP or DNS name:" followed by a text input field containing "your-k10-fqdn.tech.local".
- A label "Port:" followed by a dropdown menu showing "443" with up and down arrow icons.
- A label "Kasten instance application path:" followed by a text input field containing "/k10".
- A label "Description:" followed by a text input field containing "Created by Administrator."

At the bottom right of the window, there are four buttons: "< Previous" (disabled), "Next >" (active), "Finish" (disabled), and "Cancel" (disabled).

Step 3. Specify Credentials

At the **Credentials** step of the wizard, specify credentials for the Kasten application. If you have not added credentials beforehand, click **Manage accounts** or **Add** to add the necessary credentials and specify the following settings:

1. In the **Service Account** field, specify any symbols that you want to use for a service account.
2. In the **Token** field, specify the bearer token of a cluster service account that has the `k10-admin` ClusterRole. For more information on how to get the bearer token, see section [Obtaining Tokens](#) in Veeam Kasten Docs. For more information on K10 cluster roles, see section [Default Veeam Kasten ClusterRoles](#) in Veeam Kasten Docs.

NOTE

When you add the Veeam Kasten application, Veeam Backup & Replication checks the certificate that is used to access the Kasten dashboard. If the certificate is not trusted, Veeam Backup & Replication will display a certificate warning.

In the warning window, you can do the following:

- Click **View** for the detailed information about the certificate.
- Click **Continue** to trust the certificate.
- Click **Cancel** if you do not trust the certificate. However, in this case, you will not be able to connect to the Kasten instance.

To avoid this warning, you must add the certificate to a list of trusted certificates on a Microsoft Windows machine where Veeam Backup & Replication is installed.

New Kasten Instance ✕

Name

Credentials

Apply

Summary

Credentials

Select Kasten instance administrator credentials.

Select an account with administrative privileges for the Kasten instance being added.

Credentials ✕

Service Account:

Token: 👁

Description:

k10-user

[Manage accounts](#)

Step 4. Apply Settings

At the **Apply** step of the wizard, wait until Veeam Backup & Replication applies the settings. Click **Next** to complete the procedure of adding the Kasten application.

New Kasten Instance ✕

Name

Credentials

Apply

Summary

Apply

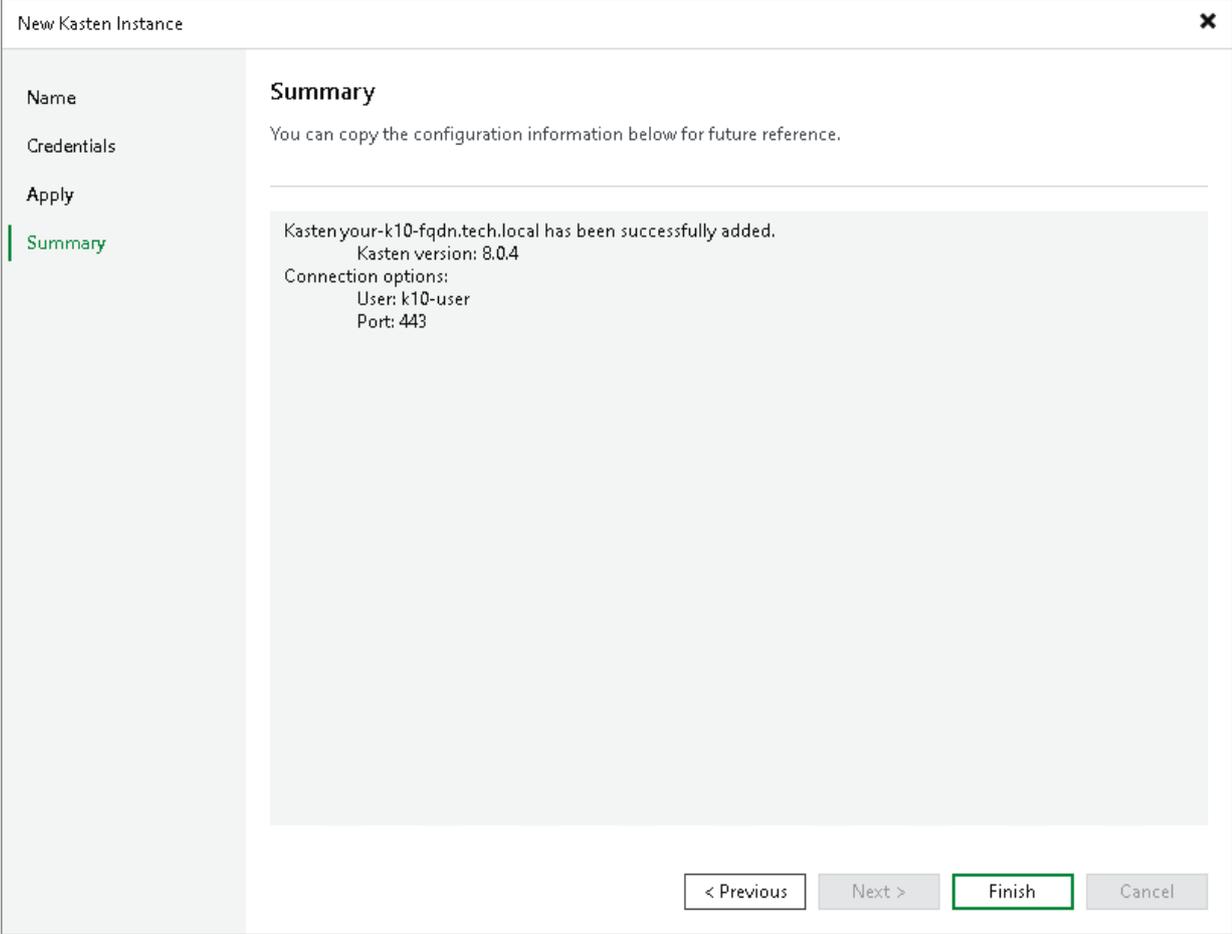
Please wait while required operations are being performed. This may take a few minutes...

Message	Duration
✓ Kasten instance has been connected successfully	
✓ Kasten instance configuration has been collected successfully	0:00:40

< Previous Next > Finish Cancel

Step 5. Finish Working with Wizard

At the **Summary** step of the wizard, review details of the Kasten application and click **Finish**.



Managing Kasten Instance

After you add a Kasten instance to the Veeam Backup & Replication infrastructure, you can edit instance settings, remove it from the Veeam Backup & Replication infrastructure, or open the instance Web UI right in the Veeam Backup & Replication console.

Viewing Snapshots and Backups

In the Veeam Backup & Replication console, you can view information about snapshots and backups exported by Veeam Kasten policies or manually. Veeam Backup & Replication displays the backups and snapshots located in both Veeam backup repositories and other location profiles, such as object storage repositories.

Available backups and snapshots are displayed in the **Home** view:

- The **Backups** node shows exports created by Veeam Kasten policies.
- The **Snapshots** subnode shows snapshots created by Veeam Kasten policies.

When you expand a node in the working area, you can see the following icons:

Icon	State
	Kasten snapshot or export
	Kasten application

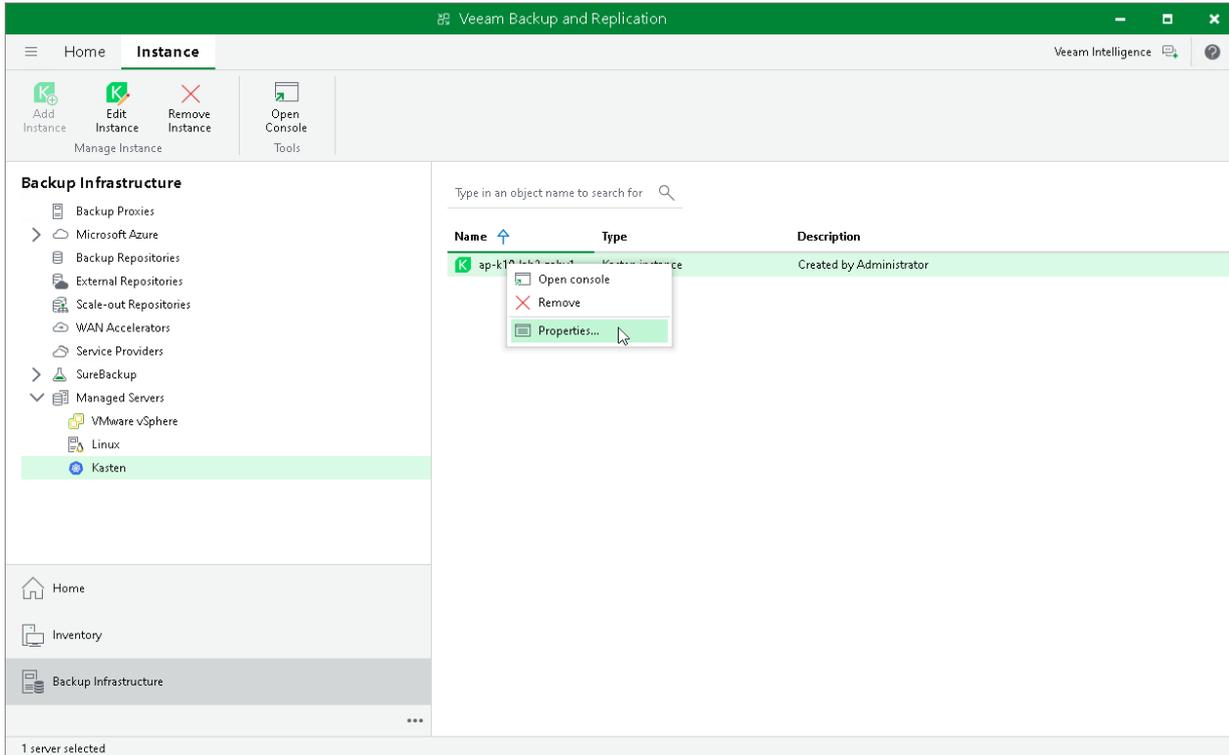
This information in the working area provides the following data:

- Veeam backup repository and folder on this repository where the backup is stored.
- Available restore points.
- Date of restore points creation.
- Data size and backup file size.
- A type of platform service where backups are created.

Editing Instance Settings

To edit the settings of a Kasten instance, do the following:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select **Managed Servers**.
3. In the working area, select the Kasten instance and click **Edit Instance** on the ribbon. Alternatively, right-click the appliance and select **Properties**.
4. Complete the wizard as described in the [Adding Kasten Instance](#) section.



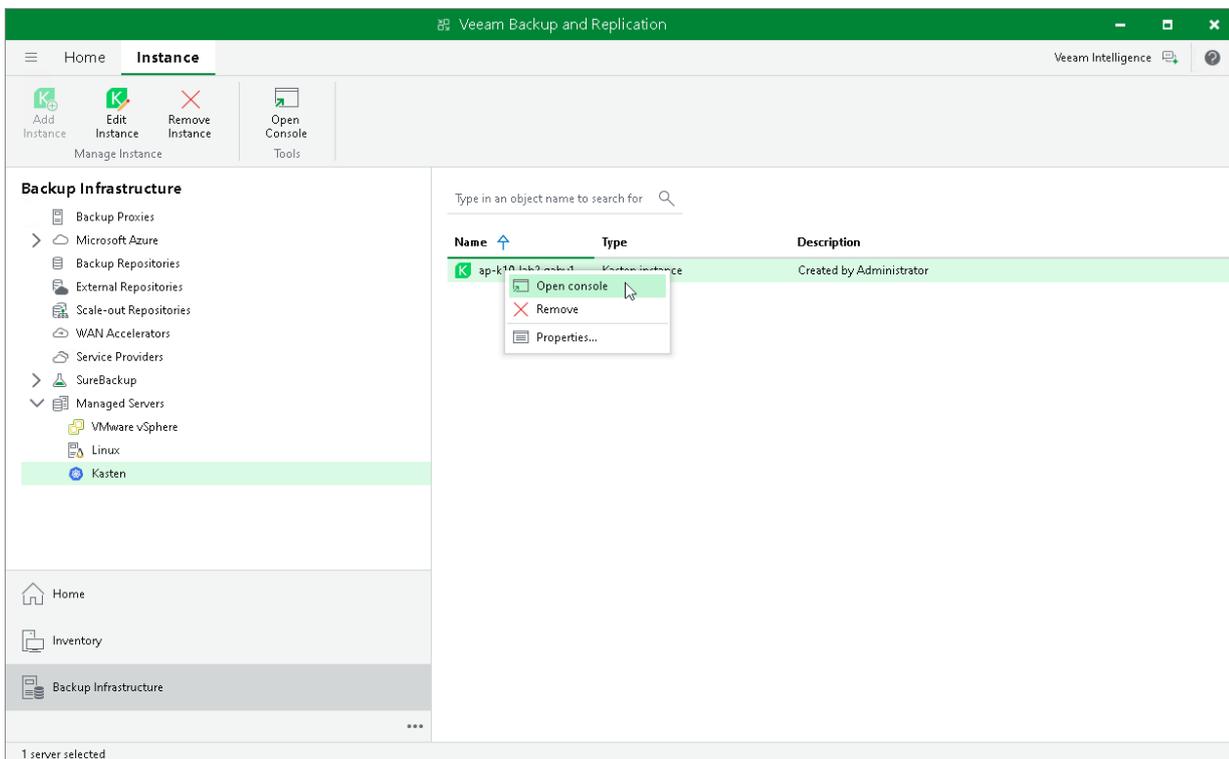
Opening Instance Web UI

If you want to access Veeam Kasten and configure options not available in the Veeam Backup & Replication console, you can perform the necessary actions using the Veeam Kasten Web UI.

To open the Veeam Kasten Web UI, do the following:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select **Managed Servers**.
3. In the working area, select the Kasten instance and click **Open Console** on the ribbon. Alternatively, right-click the instance and select **Open console**.

Veeam Backup & Replication will open a web browser and navigate you to the Veeam Kasten URL. For more information on what you can do in the Web UI, see the [Veeam Kasten Docs](#).

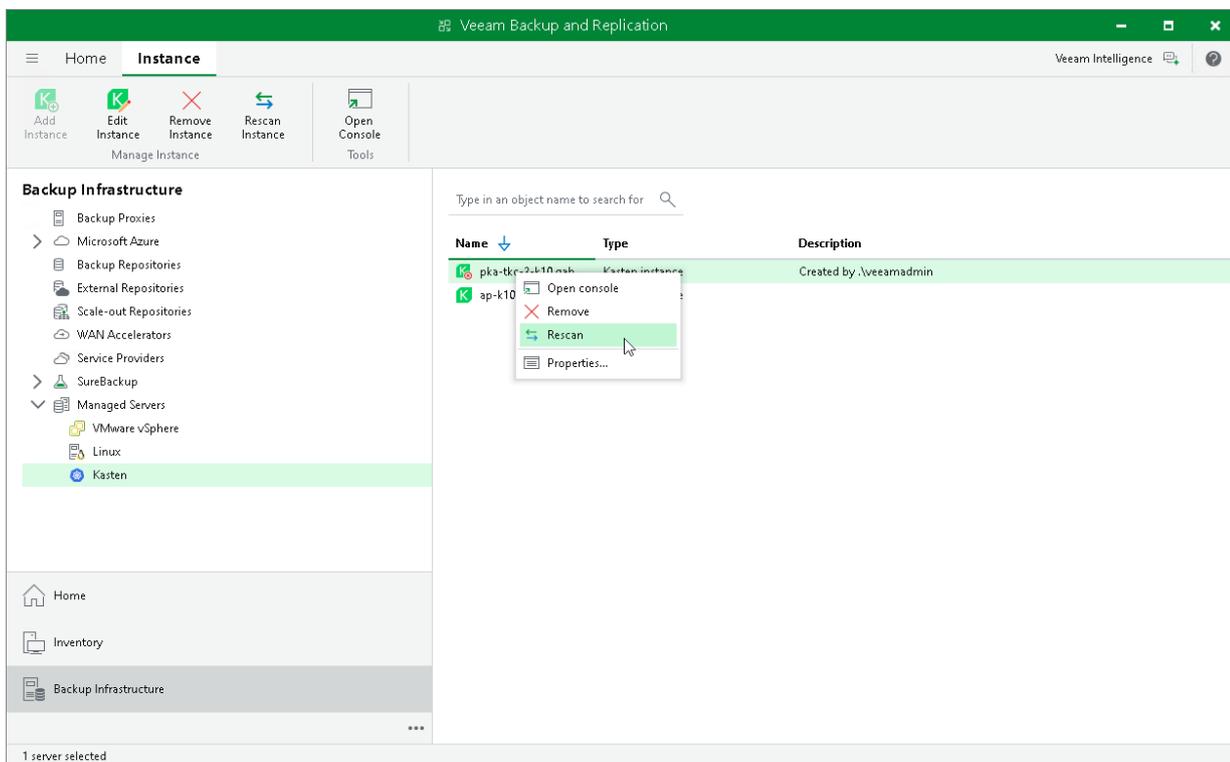


Rescanning Instance

You can rescan the Kasten instance configured in the backup infrastructure. It may be necessary when the Kasten instance becomes unavailable, or there is a mismatch between data in the backup console and on the actual appliance. Veeam Backup & Replication will erase and re-download Kasten instance settings and some statistics during the rescan operation.

To rescan the Kasten instance, do the following:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select **Managed Servers**.
3. In the working area, select the Kasten instance and click **Rescan Instance** on the ribbon. Alternatively, right-click the instance and select **Rescan**.
4. In the Veeam Backup & Replication window, click **Yes**.



Data Protection

This section provides instructions on how to export backups of applications running in your Veeam Kasten environment to Veeam backup repositories. Before you export backups, you need to create Veeam Kasten policies. For more information, see [Veeam Kasten Docs](#). After you create the policies and export backups, you can view the backed-up applications, check statistics on Veeam Kasten policies, and remove these policies from the Veeam Backup & Replication infrastructure. It is also possible to export backups to other location profiles. For more information, see [Veeam Kasten Docs](#).

Additional Data Protection Options

With Veeam Backup & Replication, you can also add an additional layer of protection for your infrastructure by creating the following types of backups to secondary destinations:

- **Backup copy jobs**

Backup copy jobs allow you to create and keep multiple instances of the same backed-up data in different locations. Storing data in different locations increases its availability and ensures that data can be recovered in case a disaster strikes and a primary Veeam backup repository is unavailable. For more information, see [Creating Backup Copy Jobs](#).

- **Backup copy to Cloud Connect**

The backup copy to cloud option allows you to create and keep multiple instances of the same backed-up data in the cloud repositories. For more information, see [Copying Data to Cloud Repositories](#).

- **Backup to tape jobs**

Backup to tape jobs allows you to keep backed-up data on tape devices. For more information, see [Creating Backups to Tapes](#).

NOTE

Consider the following:

- The additional data protection options are available only if you export Kasten backups to the Veeam backup repository.
- Restore points created by backup copy jobs or tape jobs can be recovered only by using operations available in the Veeam Backup & Replication console. You cannot use Veeam Kasten recovery options.

How Kasten Policy Works

To move backups exported by Veeam Kasten policies to Veeam backup repositories, a Veeam Kasten cluster and a Veeam Backup & Replication server use Veeam Data Movers. Veeam Data Mover is a non-persistent runtime component that allows you to export application disks from the Veeam Kasten cluster to backup repositories. When you start a Veeam Kasten policy, the following Veeam Data Movers are created:

- Source Veeam Data Mover – the Veeam Data Mover that runs in the Kanister Pod added to the Veeam Kasten cluster.
- Target Veeam Data Mover – the Veeam Data Mover that runs in the Veeam backup repository added to the Veeam Backup & Replication server.

After the Veeam Kasten policy is completed, Veeam Data Movers are removed from both the Veeam Kasten and Veeam Backup & Replication infrastructure. For more information, see the [Veeam Data Mover Service](#) section in the Veeam Backup & Replication User Guide.

When you launch a Veeam Kasten policy, the following happens:

1. Veeam Kasten takes a snapshot of applications and uses these snapshots to make exports.
2. Veeam Kasten copies configuration files of applications to the cloud storage of a public or private cloud provider.
3. Source Veeam Data Mover retrieves application data, compresses and deduplicates it.
4. Source Veeam Data Mover exports application data to the target Veeam Data Mover.
5. Target Veeam Data Mover forwards exported application data to the Veeam backup repository in the Veeam proprietary format.

Working with Kasten Policies

This section explains how to create Veeam Kasten policies and manage them using the Veeam Backup & Replication console.

Creating Kasten Policies

To export backups of applications to Veeam backup repositories, you must create Veeam Kasten policies and define the necessary settings in the Veeam Kasten dashboard associated with your Veeam Kasten cluster.

To create a Veeam Kasten policy, open the Veeam Kasten dashboard and perform the following steps:

- 1. Configure Veeam Backup repository location.**

At the location profile settings, specify the Veeam Backup & Replication server and the Veeam backup repository that will keep backups exported by Veeam Kasten policies. For more information, see [Veeam Kasten Docs](#).

- 2. Configure Kasten policy.**

In the Veeam Kasten dashboard, configure a policy and select the necessary Veeam backup location profile. Veeam Kasten will export backups of applications from the Veeam Kasten cluster to the Veeam backup repository according to these settings. For more information, see [Kasten Docs](#).

After you configure the Veeam Kasten policy, it appears in the Veeam Backup & Replication infrastructure.

Managing Kasten Policies

After you install Veeam Plug-In for Kasten, you can use the Veeam Backup & Replication console to manage Veeam Kasten policies. You can start, stop, edit, disable and delete backup policies directly in Veeam Backup & Replication console.

Starting and Stopping Policies

Veeam Plug-In for Kasten allows you to start a Veeam Kasten policy manually from the Veeam Backup & Replication console. It can be helpful if you want to create an additional snapshot or export without modifying the configured backup policy schedule. Additionally, you can stop a Veeam Kasten backup policy if the processing of applications is about to take too long and you do not want the policy to produce a heavy load on the production environment during business hours.

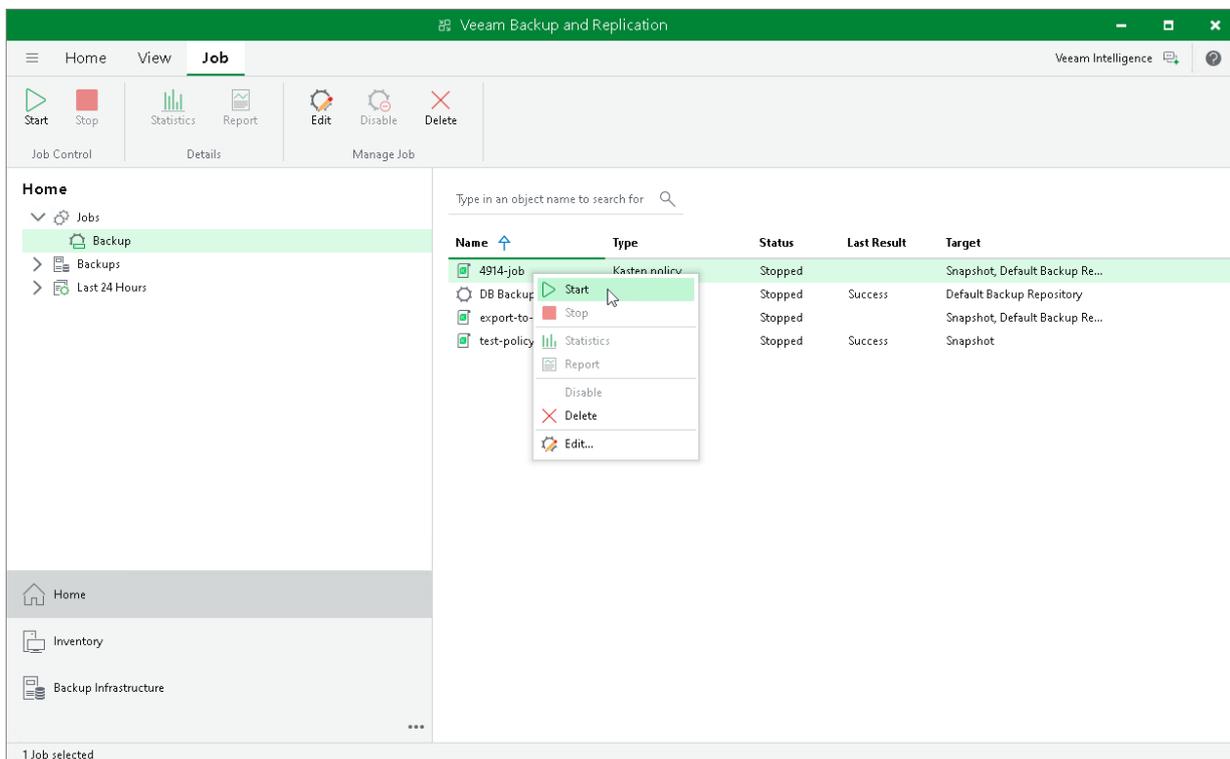
Starting Kasten Policies

To start a Kasten policy:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the necessary Veeam Kasten policy and click **Start** on the ribbon. Alternatively, right-click the selected policy and click **Start**.

TIP

To select several Kasten policies, click the first policy, press and hold the [SHIFT] key and select the other policies.



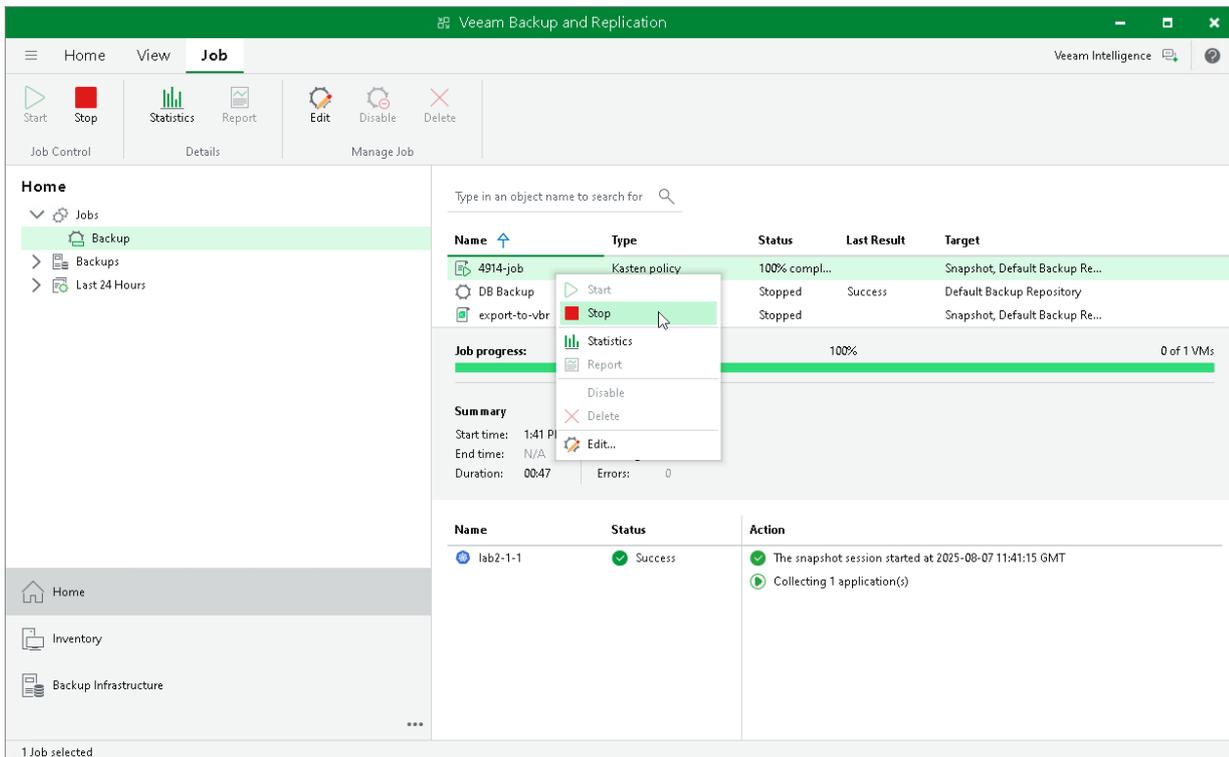
Stopping Kasten Policies

To stop a Veeam Kasten policy:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the necessary Veeam Kasten policy and click **Stop** on the ribbon. Alternatively, right-click the selected policy and click **Stop**. In the displayed window, click **Yes**.

TIP

To select several Kasten policies, click the first policy, press and hold the [SHIFT] key and select the other policies.



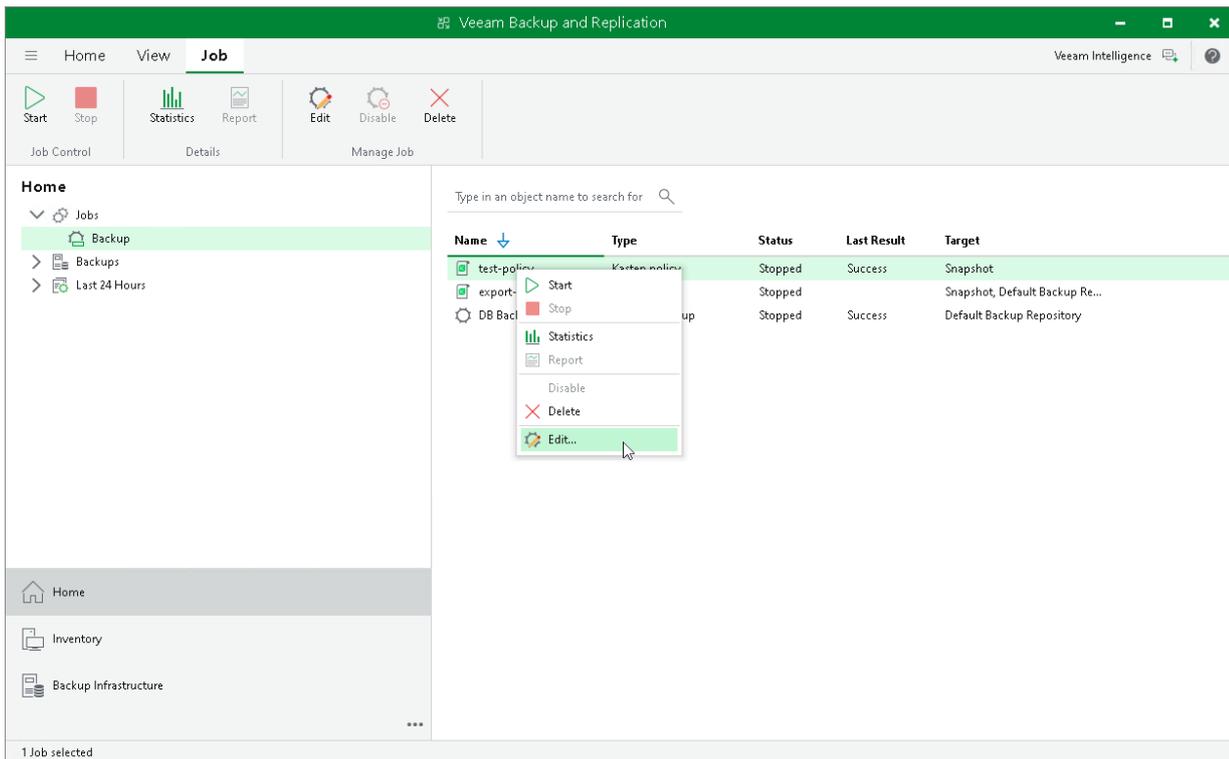
Editing Policies Settings

Veeam Plug-In for Kasten allows you to edit the settings of Veeam Kasten policies from the Veeam Backup & Replication console using redirection to the Veeam Kasten web UI. For example, you can add more applications to the Veeam Kasten policy or change the Veeam Kasten policy description.

To edit a backup policy:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.

3. In the working area, select the necessary backup policy and click **Edit** on the ribbon. Alternatively, right-click the policy and select **Edit**. The **Edit Policy** wizard will open in your browser.



Disabling and Removing Policies

Veeam Plug-In for Kasten allows you to temporarily disable or permanently delete Veeam Kasten policies from both Veeam Backup & Replication and Veeam Kasten infrastructures. When you disable a backup policy, Veeam Plug-In for Kasten disables the schedule configured for the backup policy. It means that the Veeam Kasten policy will no longer start automatically. You can enable and start the disabled policy manually any time you need.

Disabling Kasten Policies

You can disable a Veeam Kasten policy only if it has a schedule configured beforehand. For more information on configuring a Veeam Kasten policy schedule, see [Veeam Kasten Docs](#).

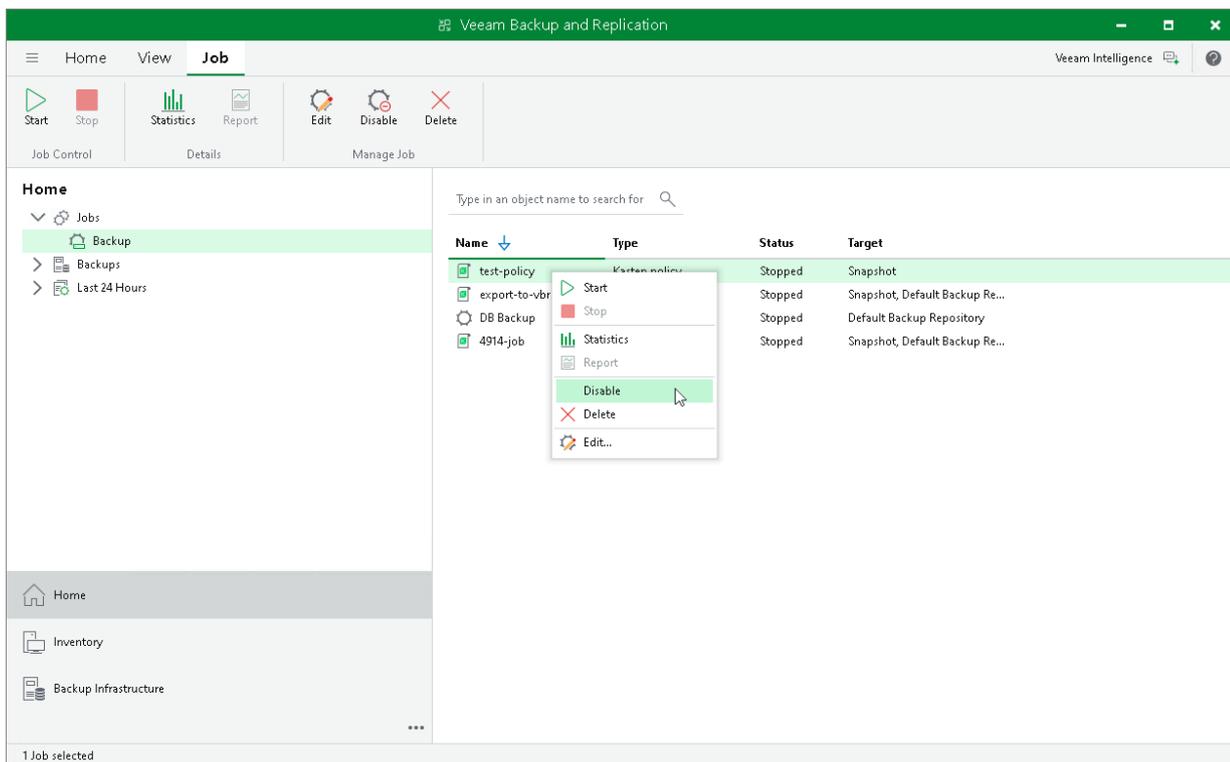
To disable a Veeam Kasten policy:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the necessary backup policy and click **Disable** on the ribbon. Alternatively, right-click the necessary backup policy and select **Disable**.

TIP

Consider the following:

- To select several Kasten policies, click the first policy, press and hold the [SHIFT] key and select the other policies.
- To enable a disabled policy, select it and click **Disable** once again.



Removing Kasten Policies

To delete a Veeam Kasten policy from the Veeam Backup & Replication infrastructure:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the necessary Veeam Kasten policy and click **Delete** on the ribbon. Alternatively, right-click the necessary backup policy and select **Delete**.

TIP

To select several Kasten policies, click the first policy, press and hold the [SHIFT] key and select the other policies.

After the policy is deleted, the backups exported by this policy are displayed under the **Backups > Disk (Orphaned)** node. If the backups exported by the policy were also stored in the capacity tier, they will also be displayed under the **Backups > Capacity Tier (Orphaned)** node.

IMPORTANT

Veeam Plug-In for Kasten deletes a Veeam Kasten policy from both Veeam Backup & Replication infrastructure and the Kasten instance.

Veeam Backup and Replication

Home View Job Veeam Intelligence

Start Stop Statistics Report Edit Disable Delete

Job Control Details Manage Job

Home

- Jobs
 - Backup
 - Backups
 - Last 24 Hours

Type in an object name to search for

Name	Type	Status	Target
test-...	Snapshot	Stopped	Snapshot
expc...	Backup Policy	Stopped	Snapshot, Default Backup Re...
DB E...	Backup Policy	Stopped	Default Backup Repository
4914	Backup Policy	Stopped	Snapshot, Default Backup Re...

Context menu options: Start, Stop, Statistics, Report, Disable, Delete, Edit...

Home Inventory Backup Infrastructure

1 Job selected

Backup Chain and Retention Policy

This section covers information on how Veeam Backup & Replication stores backups exported by Veeam Kasten policies and how Veeam Backup & Replication applies a backup retention policy to these backups.

Backup Chain

Veeam Backup & Replication keeps backups exported by Veeam Kasten policies in Veeam backup repositories in the following backup files.

- VBK – full backup files that store copies of full VM images.
- VBM – backup metadata files that store information about the policy, applications processed by this policy, a number and a structure of backup files, restore points, and so on.

Backup files reside in a dedicated job folder in the backup repository. A set of backup files form a backup chain. For more information, see the [Backup Chain](#) section in the Veeam Backup & Replication User Guide.

To create and keep backup chains in backup repositories, Veeam Backup & Replication uses different backup methods. To keep data exported from Veeam Kasten, Veeam Backup & Replication uses the synthetic full backup method and implements it the following way.

When Veeam Kasten exports application disks to backup repositories for the first time, a Veeam Data Mover creates a VBK file. When a Veeam Kasten policy starts again, the Veeam Data Mover creates a temporary incremental backup file (VIB). This temporary VIB keeps incremental changes of Veeam Kasten backup exports and Veeam Data Mover uses this VIB to create a new VBK file. Once a new full backup file is created and the Veeam Kasten policy session finishes, the temporary incremental backup is removed from the Veeam backup repository. Therefore, a backup chain of data exported from Veeam Kasten consists of VBK and VBM backup files.

Retention Policy

To store and manage backups exported by a Veeam Kasten policy, Veeam Backup & Replication applies the retention policy that you have specified in the Veeam Kasten policy settings. For more information, see [Veeam Kasten Docs](#).

Managing Backed-Up Data

Veeam Plug-In for Kasten allows you to perform the following operations from the Veeam Backup & Replication console with backups exported by Veeam Kasten policies or manually.

Viewing Backup Properties

In the Veeam Backup & Replication console, you can view information about backups exported by Veeam Kasten policies or manually to Veeam backup repositories. This information provides the following data:

- Veeam backup repository and folder on this repository where the backup is stored
- Available restore points
- Date of restore points creation
- Data size and backup file size

In the **Backup Properties** window, you can see the following icons:

Icon	State
	Full restore point
	Missing full restore point

To view summary information for backup files:

1. In the Veeam Backup & Replication console, open the **Home** view.
2. In the inventory pane, select **Backups > Disk**.
3. In the working area, right-click the backup and select **Properties**.
4. To see the list of available restore points, select the necessary application from the **Objects** list.

Backup Properties test-policy-ma (Default Backup Repository) ✕

Objects:

Restore points:

 Copy path Show issues only

Name	Original Size	File Name	Data Size	Backup Size	Data Reduction	Immutable Until	Type	Status
 lab2-1-1	5.00 GB	 lab2-1-1...	5.00 GB	414 MB	12.4 x	8/14/2025	Full	OK

Total size: 5.00 GB

Backup size: 414 MB Restore points: 1

Close

Deleting Backups

Veeam Plug-In for Kasten allows you to permanently delete backups exported by Veeam Kasten policies.

If you want to remove records about backups from both Veeam Backup & Replication infrastructure and configuration database, you can use **Delete from disk** operation. When you delete backup files from a disk, Veeam Backup & Replication deletes the whole chain from the Veeam backup repository. Thus, on the next run of the Veeam Kasten policy, Veeam Plug-In for Kasten will create full backups for applications included and added to the job.

IMPORTANT

Do not delete backup files from the Veeam backup repository manually. If you delete backup files manually, subsequent backup or replication job sessions will fail.

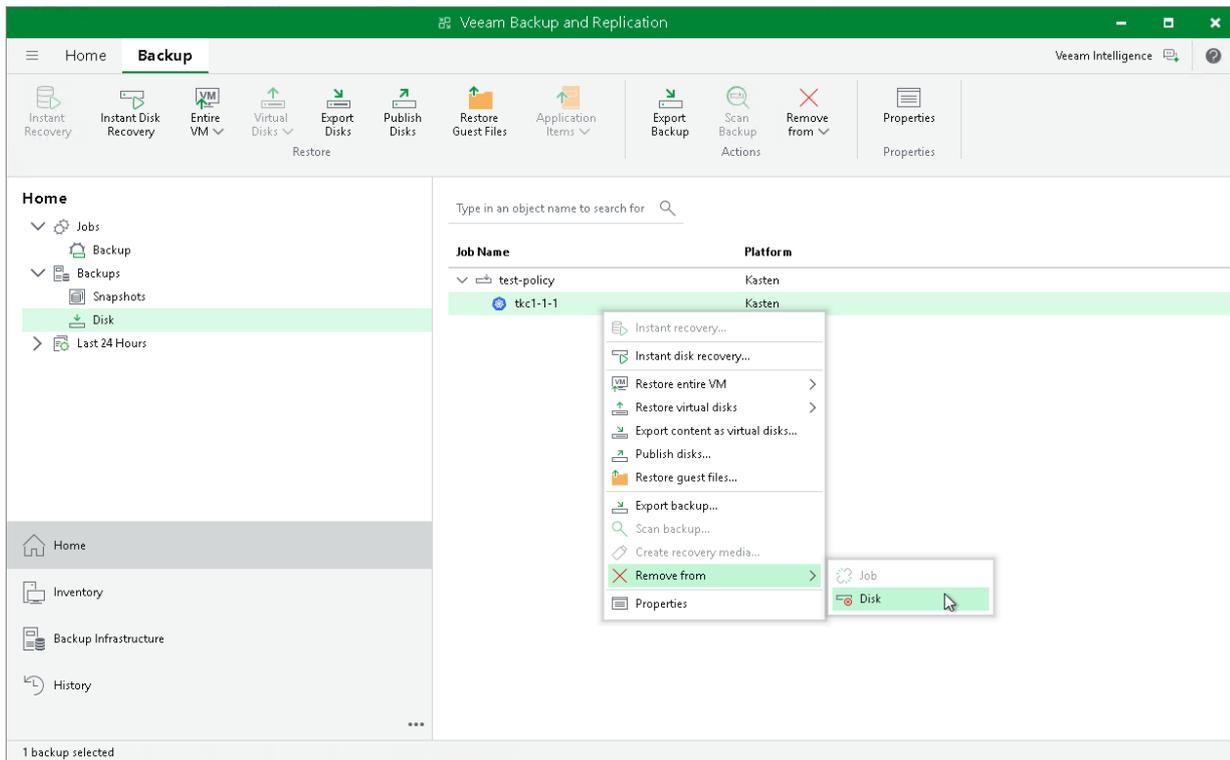
This option allows you to delete the following type of data:

- Backup files from the Veeam backup repository
- Specific applications from backups

To delete backup files or applications from the Veeam backup repository, do the following:

1. In the Veeam Backup & Replication console, open the **Home** view.
2. In the inventory pane, select **Backups > Disk**.
3. In the working area, do one of the following:
 - [To delete a backup] In the working area, select the backup and click **Remove from > Disk** on the ribbon. You can also right-click the backup and select **Remove from > Disk**.

- [To delete an application from a backup] In the working area, expand the necessary backup, select the application you want to delete and click **Remove from > Disk** on the ribbon. You can also right-click the backup and select **Remove from > Disk**.



Exporting Kasten Backups Manually

You can manually export backups of Veeam Kasten applications to Veeam backup repositories.

To export application backups, you must perform the following steps:

1. **Configure Veeam Backup repository location.**

At the location profile settings, specify the Veeam Backup & Replication server and the Veeam backup repository that will keep application backups. For more information, see [Veeam Kasten Docs](#).

2. **Export application restore point.**

In the Veeam Kasten dashboard, select the restore point of an application which backup you want to export and select the necessary Veeam backup location profile. Veeam Kasten will export application backups to the Veeam backup repository according to these settings. For more information on the manual export of application backups, see [Veeam Kasten Docs](#).

After you start the manual export, it appears in the Veeam Backup & Replication infrastructure under the **Backups > Disk (Exported)** node.

Creating Backup Copy Jobs

Backup copy is a technology that helps you create and store backup data in different locations. Storing data in different locations increases its availability and ensures that data can be recovered in case a disaster strikes.

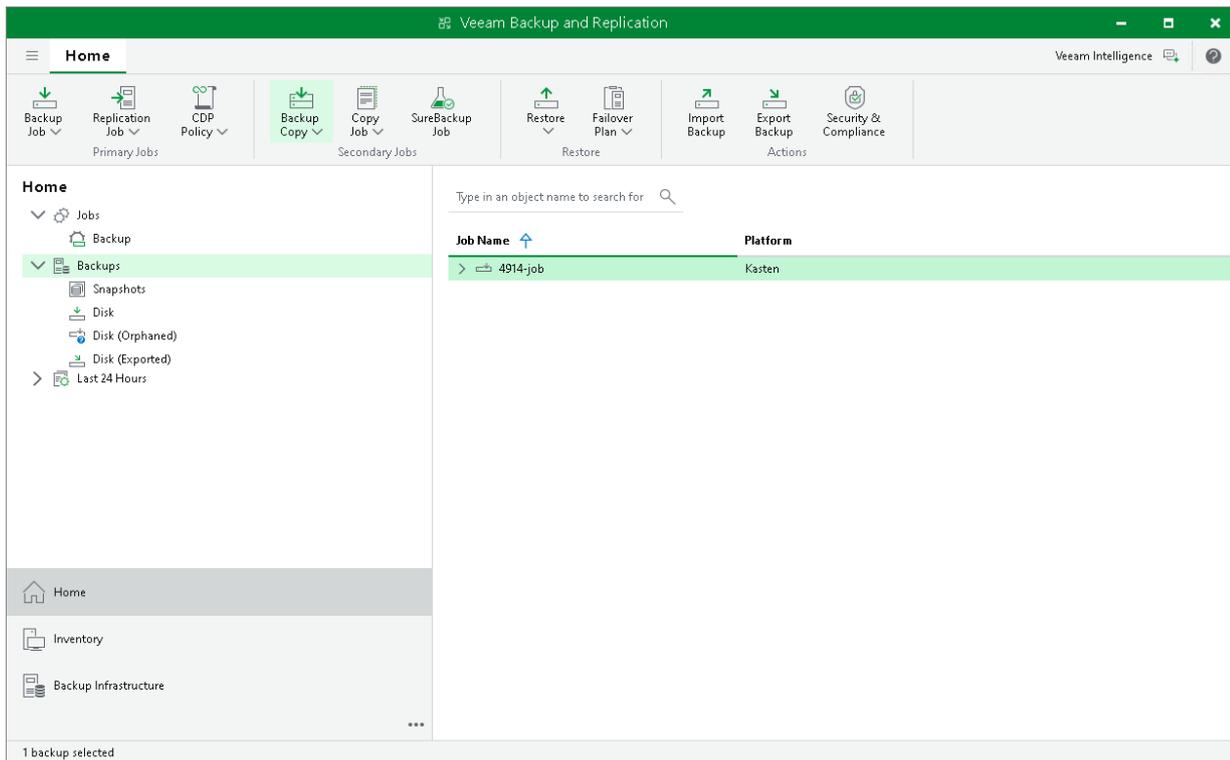
The backup copy is a job-driven process. Veeam Backup & Replication fully automates the backup copy process and lets you specify retention settings to maintain the desired number of restore points, as well as full backups for archival purposes. To create a backup copy job, Veeam Backup & Replication uses the Veeam Kasten policy as a source and copies backed-up data created by this policy. For more information on the backup copy functionality, see the [Backup Copy](#) section in the Veeam Backup & Replication User Guide.

IMPORTANT

As a source, you can use only Veeam Kasten policies that export backups to Veeam backup repositories.

To create a backup copy job, do the following:

1. Check [limitations and prerequisites](#) listed in the Veeam Backup & Replication User Guide.
2. Open the **Home** view, navigate to **Backups** and select the necessary Veeam Kasten policy.
3. Complete the **New Backup Copy Job** wizard as described in the [Creating Backup Copy Jobs for VMs and Physical Machines](#) section in the Veeam Backup & Replication User Guide.



Copying Data to Cloud Repositories

If you want to store copies of backups exported from Veeam Kasten in cloud repositories, you can connect to a service provider (SP) and store copies of these backups in cloud repositories. For more information, see the [Veeam Cloud Connect Guide](#).

To copy backups exported from Veeam Kasten to cloud repositories, do the following:

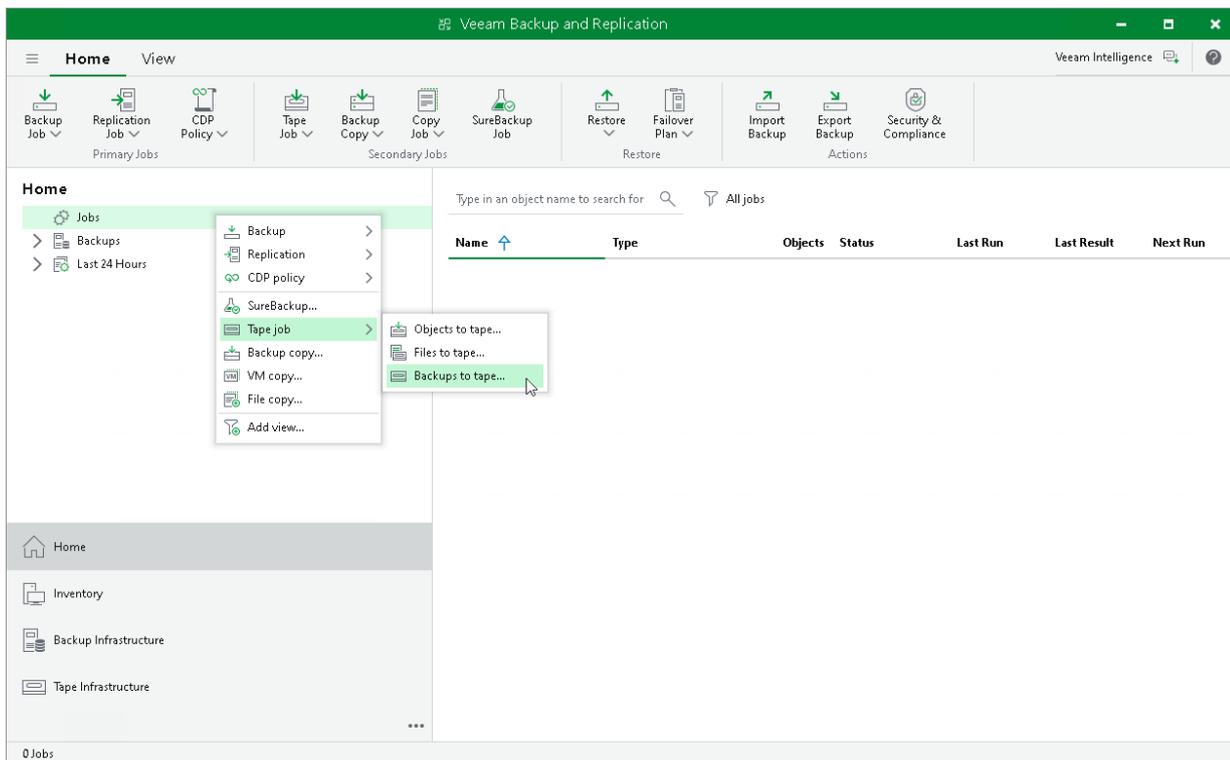
1. Depending on your environment, configure one of the following Cloud Connect Infrastructure types:
 - [For service providers] Follow the steps described in the [Setting Up SP Veeam Cloud Connect Infrastructure](#) section in the Veeam Cloud Connect User Guide.
 - [For tenants] Follow the steps described in the [Setting Up Tenant Veeam Cloud Connect Infrastructure](#) section in the Veeam Cloud Connect User Guide.
2. Run a Veeam Kasten policy.
3. Configure a backup copy job for backups exported from Veeam Kasten. Follow the instructions provided in [Creating Backup Copy Jobs](#).

Creating Backups to Tapes

Storing data on tape devices helps you improve the level of safety and implement the 3-2-1 rule (3 copies, 2 types of media, 1 offsite location). To administer all operations on tapes in your Veeam Backup & Replication console, Veeam Backup & Replication allows you to automate the copying of image-level backups to tape devices. It lets you specify scheduling, archiving and media automation options. For more information on the supported tapes and operations you can perform with tapes, see the [Tape Devices Support](#) section in the Veeam Backup & Replication User Guide.

To copy backups exported by Veeam Kasten policies to tapes, do the following:

1. Configure the tape infrastructure:
 - a. Connect tape devices as described in the [Tape Devices Deployment](#) section in the Veeam Backup & Replication User Guide.
 - b. Perform the initial configuration as described in steps 1-3 of the [Getting Started with Tapes](#) section in the Veeam Backup & Replication User Guide.
2. Create a backup to tape job as described in the [Creating Backup to Tape Jobs](#) section in the Veeam Backup & Replication User Guide.



Viewing Statistics

You can use the Veeam Backup & Replication console to view real-time statistics for any backup policy. For more information on how to review statistics, see [Reporting](#) section in the Veeam Backup & Replication User Guide.

Data Recovery

Veeam Plug-In for Kasten offers the following recovery options for various disaster recovery scenarios:

- [Restoring to Kubernetes](#)
Restores applications to the Kubernetes cluster (using the Veeam Kasten web console).
- [Exporting Disks](#)
Restore persistent disks from backups and convert them to disks in the VMDK, VHD or VHDX format.
- [Instant First Class Disk \(FCD\) Recovery](#)
Recover persistent disks from backup files and register them as First Class Disks (FCDs).
- [Restoring Guest OS Files](#)
Recover individual guest OS files from Linux file systems.
- [Exporting Backup Files](#)
Synthesize an independent full backup file using restore points that are located in your Veeam backup repositories.

IMPORTANT

Consider the following:

- Veeam Plug-In for Kasten does not allow you to restore Kubernetes containers from a Veeam Backup & Replication server to a Veeam Kasten cluster or any other location. To perform the restore operations with Kubernetes containers, use Veeam Kasten recovery options. For more information, see [Veeam Kasten Docs](#).
- You can perform the recovery options (except restore to the Kubernetes cluster) only for restore points exported to the Veeam backup repository.
- Restore points created by backup copy jobs or tape jobs can be recovered only by using operations available in the Veeam Backup & Replication console. You cannot use Veeam Kasten recovery options.

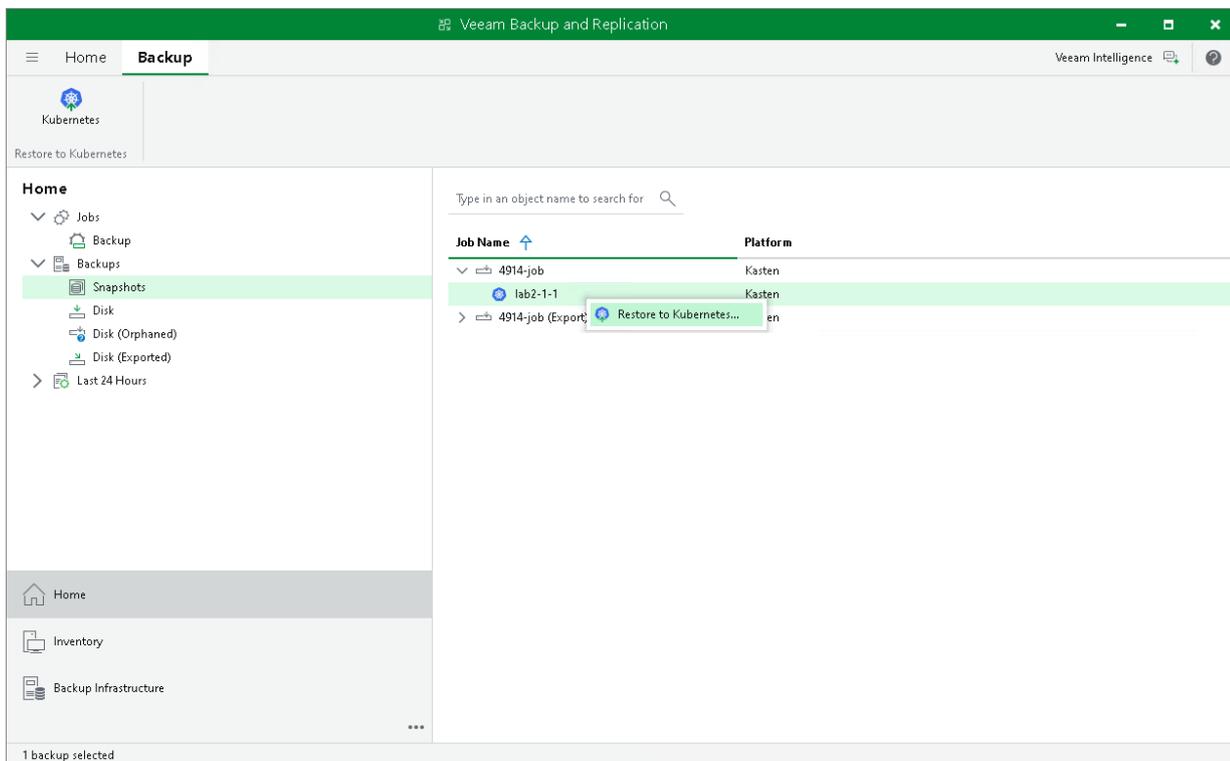
Restoring to Kubernetes

Veeam Backup & Replication allows you to restore applications to the Kubernetes cluster. When you restore applications, Veeam Backup & Replication redirects you to the Veeam Kasten Web UI to proceed with the restore.

To restore applications, do the following:

1. Open the **Home** view. In the inventory pane, navigate to **Backups > Disk** if you want to restore from Kasten exports or to **Backups > Snapshots** if you want to restore from snapshots. In the working area, select an application whose snapshot you want to restore. On the ribbon, click **Kubernetes**. Alternatively, right-click the application and select **Restore to Kubernetes**.
2. Follow the instructions provided in the [Veeam Kasten docs](#).

You can view restore sessions under the **Home > Last 24 Hours** node or under **History > Restore** node.

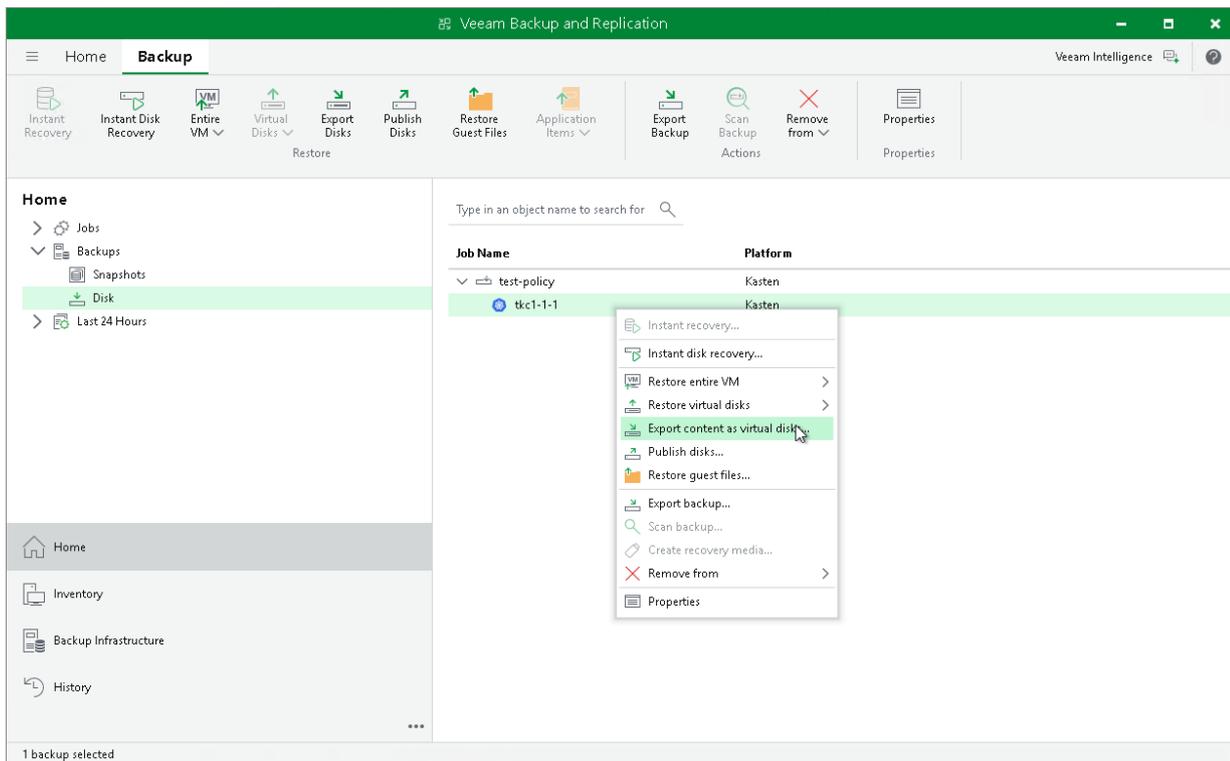


Exporting Disks

Veeam Backup & Replication allows you to restore disks of backups exported from Veeam Kasten. You can restore disks in the VMDK, VHD or VHDX format. For more information on disk export, see the [Disk Export](#) section in the Veeam Backup & Replication User Guide.

To restore disks of backups exported from Veeam Kasten and convert them to the VMDK, VHD or VHDX format:

1. Launch the **Export Disk** wizard. To do that, open the **Home** view. In the inventory pane, navigate to **Backups > Disk**. In the working area, select applications whose disk you want to export. On the ribbon, click **Export Disks**. Alternatively, right-click the application and select **Export content as virtual disks**.
2. Complete the wizard as described in the [Exporting Disks](#) section in the Veeam Backup & Replication User Guide.

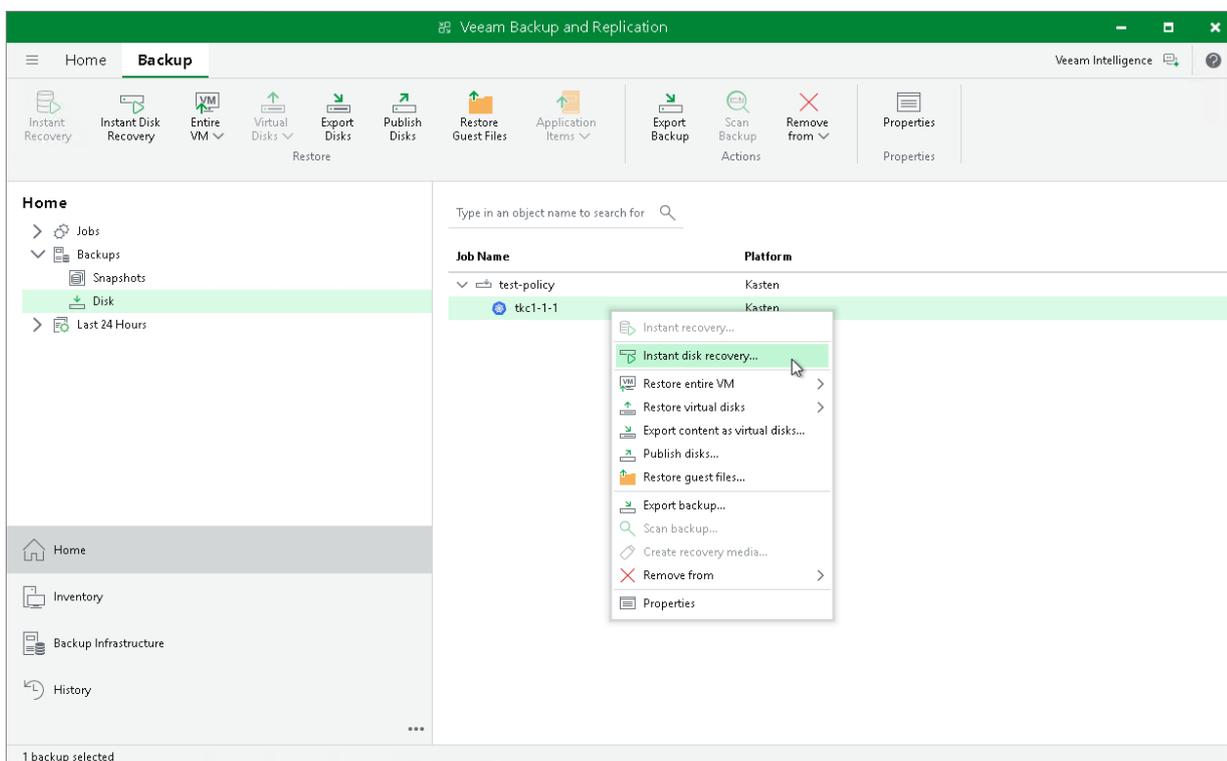


Instant First Class Disk (FCD) Recovery

With Instant First Class Disk (FCD) Recovery, you can immediately restore disks of backups exported from Veeam Kasten and register them as FCDs in a VMware cluster. Instant FCD Recovery allows you to instantly restore FCDs without attaching them to the production environment. For more information on First Class Disk (FCD) Recovery, see the [Instant First Class Disk \(FCD\) Recovery](#) section in the Veeam Backup & Replication User Guide.

To perform FCD recovery of backups exported from Veeam Kasten:

1. Check [limitations and prerequisites](#) listed in the Veeam Backup & Replication User Guide.
2. Launch the **Instant Disk Recovery** wizard. To do that, open the **Home** view. In the inventory pane, navigate to **Backups > Disk**. In the working area, select an application whose disk you want to export. On the ribbon, click **Instant Disk Recovery**. Alternatively, right-click the application and select **Instant disk recovery**.
3. Complete the wizard as described in the [Instant FCD Recovery](#) section in the Veeam Backup & Replication User Guide.



Restoring Guest OS Files

You can restore individual guest OS files and folders from backups exported from Veeam Kasten. You can restore files and folders directly from image-level backups. For more information, see the [Guest OS File Recovery](#) section in the Veeam Backup & Replication User Guide.

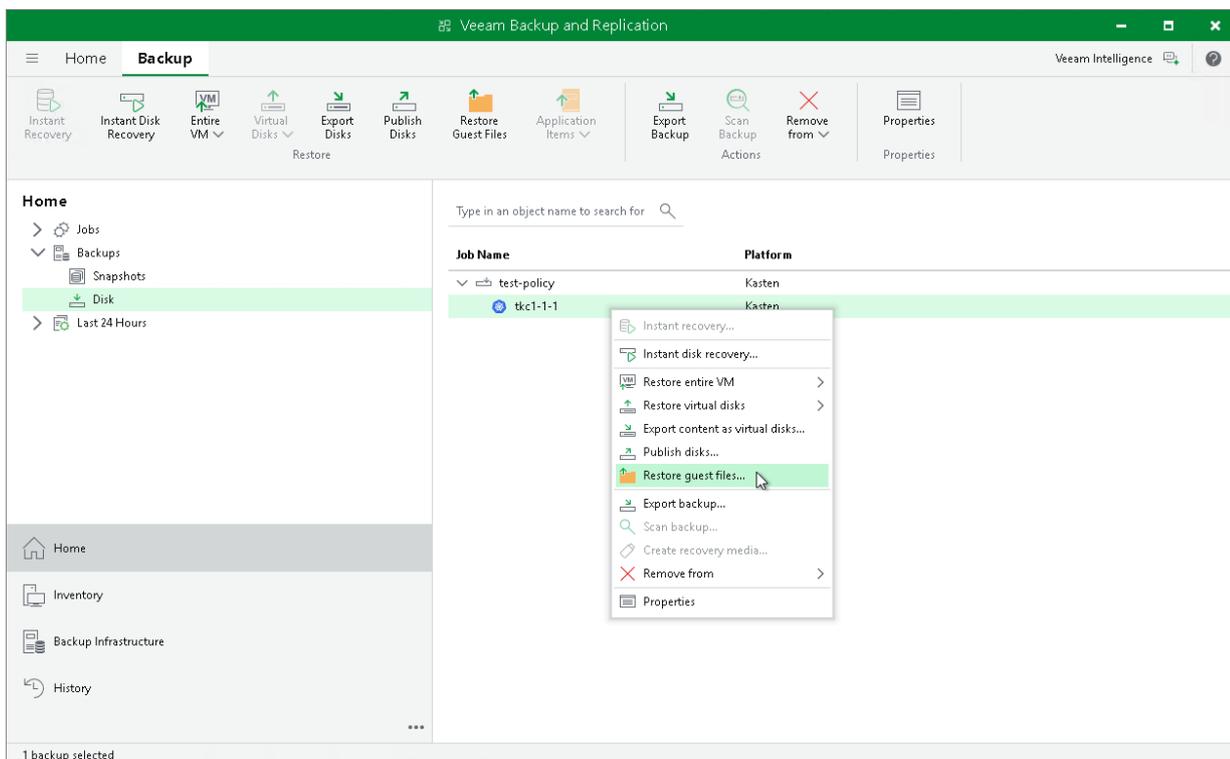
NOTE

Consider the following:

- Veeam Plug-In for Kasten supports only restore from Linux, Unix and other non-Microsoft Windows OSes.
- Veeam Plug-In for Kasten does not support restore of individual guest OS files and folders to the original location (applications added to a Veeam Kasten cluster). You can only save files and folders to a new location. For more information, see the [Saving Files to New Location](#) section in the Veeam Backup & Replication User Guide.

To restore guest OS files from Linux, Unix and other file systems, do the following:

1. Check [considerations and limitations](#) listed in the Veeam Backup & Replication User Guide.
2. Launch and complete the **File Level Restore** wizard. To do that, open the **Home** view and navigate to **Backups > Disk**. In the working area, select an application whose files you want to restore. On the ribbon, click **Restore Guest Files**. Alternatively, right-click the application and select **Restore guest files**.
3. Complete the wizard as described in the [Restoring VM Guest OS Files \(Multi-OS\)](#) section in the Veeam Backup & Replication User Guide.



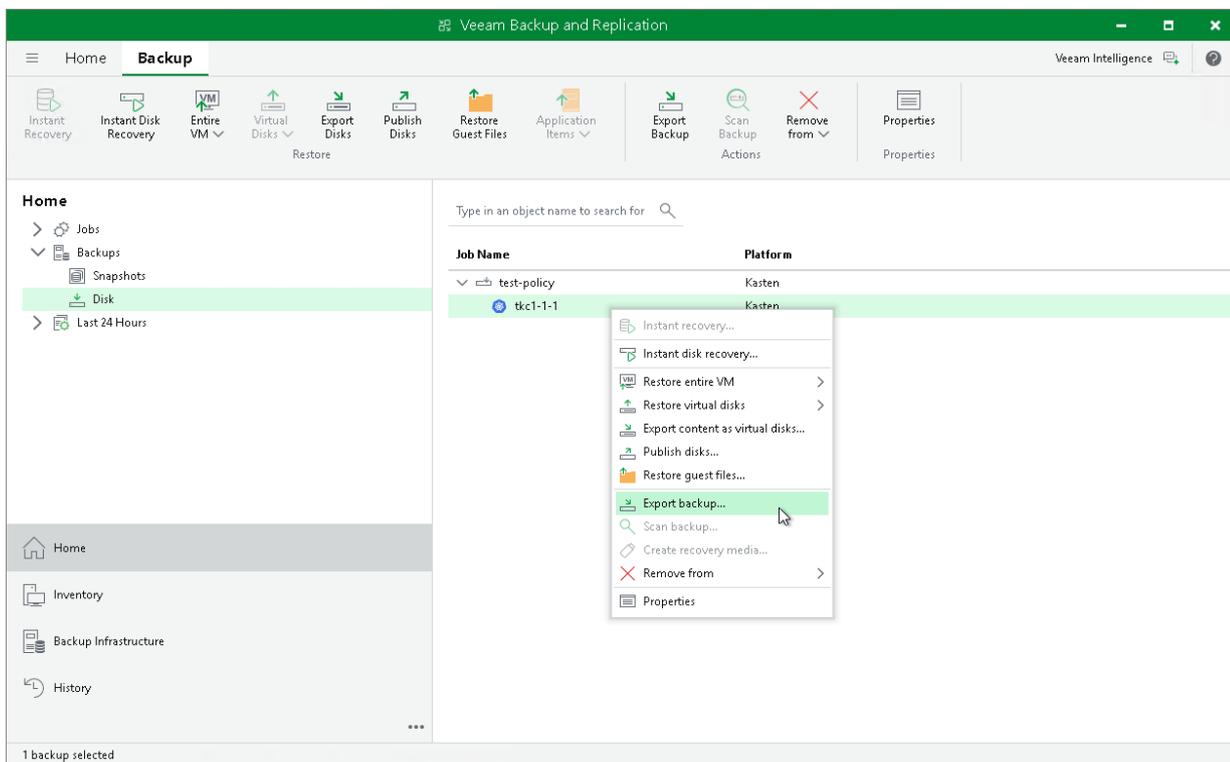
Exporting Backup Files

You can export full backup files of applications backed up by Veeam Kasten policies. Exporting full backup files allows you to produce a full backup file (VBK) that acts as an independent restore point. By default, this backup file is stored in a separate folder in a Veeam backup repository used by the Veeam Kasten policy. You can move this backup file to a different location without affecting a backup chain of backup files exported by the Veeam Kasten policy. For more information on exporting full backups, see the [Exporting Backups](#) section in the Veeam Backup & Replication User Guide.

To export full backup files of applications backed up by Veeam Kasten:

1. Launch the **Export Backup** wizard. To do that, open the **Home** view. In the inventory pane, navigate to **Backups > Disk**. In the working area, select applications whose restore points you want to export. On the ribbon, click **Export Backup**. Alternatively, right-click the application and select **Export backup**.
2. Complete the wizard as described in the [Performing Export](#) section in the Veeam Backup & Replication User Guide.

After backup files are exported, they are displayed under the **Backups > Disk (Exported)** node.



Viewing Statistics

Veeam Plug-In for Kasten allows you to view statistics on data recovery operations. You can view the information on the restore reason, the parameters of the restored instance, the logs of the restore session, and so on. For more information on how to review statistics, see the [Viewing Real-Time Statistics](#) section in the Veeam Backup & Replication User Guide.

Support Information

If you have any questions or issues with Veeam Kasten Plug-in for Veeam Backup & Replication, you can search for a resolution on [Veeam R&D Forums](#) or submit a support case in the [Veeam Customer Support Portal](#).

IMPORTANT

Veeam Customer Support does not assist with issues related to the Veeam Kasten platform, management of Kubernetes containers and Veeam Kasten policies. You have to contact [Veeam Kasten support](#).

When you submit a support case, we recommend you provide information on the installed products to the Veeam Customer Support Team. Product logs contain this information.

To export logs, do the following:

1. From the main menu of the Veeam Backup & Replication console, select **Help > Support Information**.
2. At the **Scope** step of the **Export Logs** wizard, select **Export all logs for selected components**.
3. In the **Managed servers** list, select the Veeam Backup & Replication server and other components for which you want to export logs.
4. Complete the wizard as described in the [Exporting Logs](#) section in the Veeam Backup & Replication User Guide.

IMPORTANT

In the **Export Logs** wizard, you can not export logs for separate Kasten policies and backup files.

Export Logs
✕

Scope

Date Range

Location

Export

Scope

Specify the scope for logs export.

Export logs for this job:
 Choose...

Export logs for these objects:
 Choose...

Export all logs for selected components (may result in a very large log package)

Managed servers:

Server	Components	
✓ vmlinuxma.te...	Dell Data Domain Library, Guest Interactio...	Select All
		Clear All

Collect local PostgreSQL instance logs

< Previous
Next >
Finish
Cancel