



Veeam Backup & Replication

Version 12

Kasten K10 Integration Guide

December, 2023

© 2023 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	17
Adding K10 Instance	18
Step 1. Launch New Kasten K10 Deployment Wizard	19
Step 2. Specify K10 Cluster Settings	20
Step 3. Specify Credentials	21
Step 4. Apply Settings	22
Step 5. Finish Working with Wizard	23
Managing K10 Instance	24
Viewing Snapshots and Backups	25
Editing Instance Settings	26
Opening Instance Web UI	27
Removing Instance	28
DATA PROTECTION	29
How K10 Policy Works	30
Backup Chain and Retention Policy	31
Creating K10 Policies	32
Managing K10 Policies	33
Starting and Stopping Policies	34
Editing Policies Settings	36
Disabling and Removing Policies	37
Managing Backed-Up Data	39
Viewing Backup Properties	40
Deleting Backups	41
Exporting K10 Backups Manually	43
Creating Backup Copy Jobs	44
Copying Data to Cloud Repositories	45

Creating Backups to Tapes	46
Viewing Statistics	47
DATA RECOVERY.....	48
Restoring to Kasten K10	49
Exporting Disks	50
Instant First Class Disk (FCD) Recovery	51
Restoring Guest OS Files	52
Exporting Backup Files	53
Viewing Statistics	54
SUPPORT INFORMATION	55

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 Backup for Kasten K10 solution.

Intended Audience

This document is intended for administrators who has just set up an infrastructure for the Veeam Backup for Kasten K10 solution.

Overview

Veeam Backup for Kasten K10 is a solution that allows you to create and manage data protection and disaster recovery tasks for K10 environments. Veeam Backup for Kasten K10 extends the Veeam Backup & Replication functionality and provides access to Veeam Backup for Kasten K10 in Veeam Backup & Replication console.

NOTE

Veeam Backup for Kasten K10 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 K10 solutions.

With Veeam Backup for Kasten K10 you can perform the following operations in Veeam Backup & Replication console:

- Add the K10 instance to Veeam Backup & Replication infrastructure, manage and remove it.
- Manage K10 policies from Veeam Backup & Replication infrastructure.
- View backups exported by K10 policies.
- Restore backups exported by K10 policies to Kasten K10 environment.
- Restore snapshots created by K10 policies to Kasten K10 environment.
- Remove backups exported by K10 policies from Veeam Backup & Replication infrastructure.
- Monitor session statistics.
- 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.

Backup Infrastructure Components

To export backups created by K10 policies using Veeam Backup for Kasten K10, you must configure the infrastructure that will consist of the following components:

1. K10 application.

A platform where you configure and manage K10 policies that will export backups of application disks to Veeam backup repositories. For more information on installing a K10 application, see [Kasten Docs](#).

2. Veeam Backup & Replication server.

A server that manages K10 appliance and K10 policies. It allows you to monitor and manage backups, exported by K10, 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 K10 policies.

A storage location where Veeam Backup & Replication keeps backups exported by K10 policies. You can add multiple repositories to the Veeam Backup & Replication server and set the necessary repository within K10 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.

TIP

Starting from K10 4.5.15 and higher to prohibit data deletion or data loss as a result of 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 details on how to properly configure K10 to make backups exported by K10 policies immutable, see [Kasten K10 Docs](#).

4. Additional data protection layers.

Veeam Backup & Replication allows you to keep backups exported by K10 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 [Machines Backup to Tape](#) section in the Veeam Backup & Replication User Guide.
- Cloud repositories of service providers that keep copies of backups exported by K10 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 [Limitations and Considerations](#).

What You Do Next

[Deploy and Configure Infrastructure](#)

Planning and Preparation

Before you start using the Veeam Backup for Kasten K10 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 Backup for Kasten K10, consider the following:

Kubernetes Distribution Requirements

Veeam Backup for Kasten K10 supports only backup exports of Kubernetes persistent volumes to Veeam backup repositories. These persistent volumes must be provisioned with the vSphere CSI driver.

Kasten K10 Application Version

A K10 application must be the 5.5.3 version or later.

Veeam Backup & Replication

Veeam Backup for Kasten K10 supports integration with Veeam Backup & Replication version 12 (build 12.0.0.1420).

Veeam Backup & Replication Hardware and Software Requirements

The machine where you want to deploy the Veeam Backup & Replication server must meet the system requirements specified in the [System Requirements](#) section in the Veeam Backup & Replication User Guide.

Veeam Backup Repositories Requirements

Veeam backup repositories where you want to keep backups exported by K10 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:

- Veeam Backup for Kasten K10 does not support Kerberos for K10 exports to Veeam backup repositories.
- Veeam Backup for Kasten K10 does not support IPv6.
- Veeam Backup for Kasten K10 does not sync K10 restore sessions.
- Veeam Backup for Kasten K10 does not sync K10 retention (retire) sessions.
- You can add only 1 specific K10 instance to Veeam Backup & Replication infrastructure.
- Veeam Backup for Kasten K10 does not support K10 exports to the database-oriented operating system (DBOS) Veeam backup repositories.
- Veeam Backup for Kasten K10 does not provide a granular task progress of sessions.
- If you delete K10 policies created by K10 MultiCluster console on K10 secondary servers, they will be recreated by K10 MultiCluster console.
- Veeam Backup for Kasten K10 does not support K10 export of K10 instance that is not added to Veeam Backup & Replication infrastructure.

Used Ports

Veeam Backup & Replication within the Veeam Backup for Kasten K10 solution is deployed on the machine that uses the same ports as those described in the [Used Ports](#) section in the Veeam Backup & Replication User Guide. In addition, Veeam Backup for Kasten K10 also uses ports listed in the table.

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
Kasten K10 Plug-in for Veeam Backup & Replication	Veeam Backup & Replication server	TCP	6172	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	2500 to 3300	Default range of ports used as data transmission channels. For every TCP connection that a job uses, one port from this range is assigned.
Veeam Backup & Replication console and Veeam Backup & Replication and Veeam One server	Kasten K10 Plug-in for Veeam Backup & Replication	TCP	9404	Port used by Veeam Backup & Replication to connect to Kasten K10 Plug-in for Veeam Backup & Replication.

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 that you plan to use with K10 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 [Roles and Users](#) section in the Veeam Backup & Replication User Guide.

Veeam Backup Repositories

Make sure that either the **Allow to everyone** or **Allow to the following accounts or groups** access permissions are granted on Veeam backup repositories where you want to keep backups exported by K10 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 K10, otherwise the K10 policy will fail.

Licensing

If you want to use the Veeam Backup for Kasten K10 solution, you must have the following types of product editions installed:

- Veeam Backup & Replication server requires either the Rental license or Enterprise Plus product edition. For more information, see [Veeam Licensing Policy](#).
- K10 application requires FREE K10 or Enterprise editions. For more information, see the [Kasten product page](#), section Kasten K10 Editions.

NOTE

Veeam licenses Veeam Backup & Replication in two ways: per instance and per socket. However, backups exported by the K10 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 Backup for Kasten K10 solution, you must configure the K10 instance and Veeam Backup & Replication infrastructure.

Configure K10 Instance Infrastructure

A K10 instance is a source environment that creates snapshots of applications running on Kubernetes persistent volumes. After that, K10 makes exports of snapshot data to the storage locations to keep this data. As a storage location, you can use the Veeam backup repositories. In this case, the exports are stored in a native Veeam format. The K10 instance that you plan to use in the Veeam Backup for Kasten K10 infrastructure must meet the [system requirements](#). For more information on configuring the K10 instance, see [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 Backup for Kasten K10 will be automatically installed along with Veeam Backup & Replication.

3. **Add K10 instance.**

Add the K10 instance to Veeam Backup & Replication infrastructure to be able to create and manage K10 policies. For more information, see [Adding K10 Instance](#).

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

If you want to keep exports created by K10 policies in Veeam backup repositories, you must add the Veeam backup repositories that will store backups exported by K10 policies to Veeam Backup & Replication infrastructure. Make sure that you configured the [required permissions](#). For more information, see the [Backup Repository](#) and [Adding Backup Repositories](#) sections in the Veeam Backup & Replication User Guide.

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

Configure 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 backups exported by K10 policies. 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 backups exported by K10 policies 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.

What You Do Next

After you configure the K10 instance and add it to Veeam Backup & Replication infrastructure, you are ready to [create K10 policies](#) and perform data protection and data recovery options.

Installing Plug-In

Veeam Backup for Kasten K10 is installed automatically while you install or upgrade Veeam Backup & Replication up 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

If you had backups exported by K10 to Veeam Backup & Replication 11 version, these backups will be available in your backup infrastructure after you upgrade to Veeam Backup & Replication version 12. However, you must [add the K10 application](#) to the backup infrastructure, otherwise the Veeam Backup for Kasten K10 data protection and data recovery functionality will not be available.

Adding K10 Instance

Veeam Backup for Kasten K10 allows you to view and manage K10 policies as well as perform data protection and data recovery operations with exports created by K10 from Veeam Backup & Replication console. To do it, you must add the K10 instance to Veeam Backup & Replication infrastructure.

After you add the K10 instance to Veeam Backup & Replication infrastructure, Veeam Backup for Kasten K10 accesses K10 and synchronizes the following information:

- Information on K10 policies.
- Snapshots and exports created by K10 policies.
- Snapshots and exports created manually.
- Statistics for the last 24 hours.

After synchronization is completed, Veeam Backup for Kasten K10 shows this information in Veeam Backup & Replication console and performs incremental syncs every 5 seconds to get updates.

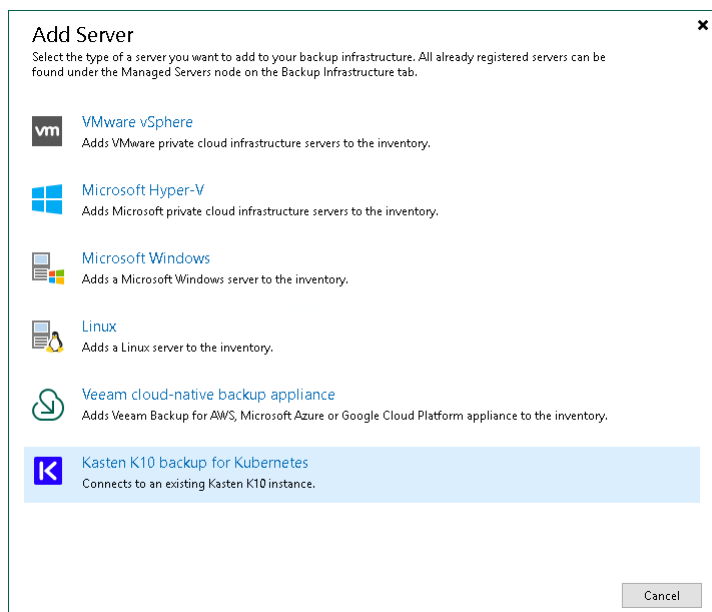
To add the K10 instance to Veeam Backup & Replication infrastructure, do the following:

1. [Launch the New Kasten K10 Instance wizard](#)
2. [Specify the K10 instance name](#)
3. [Specify credentials](#)
4. [Apply Settings](#)
5. [Finish working with the wizard](#)

Step 1. Launch New Kasten K10 Deployment Wizard

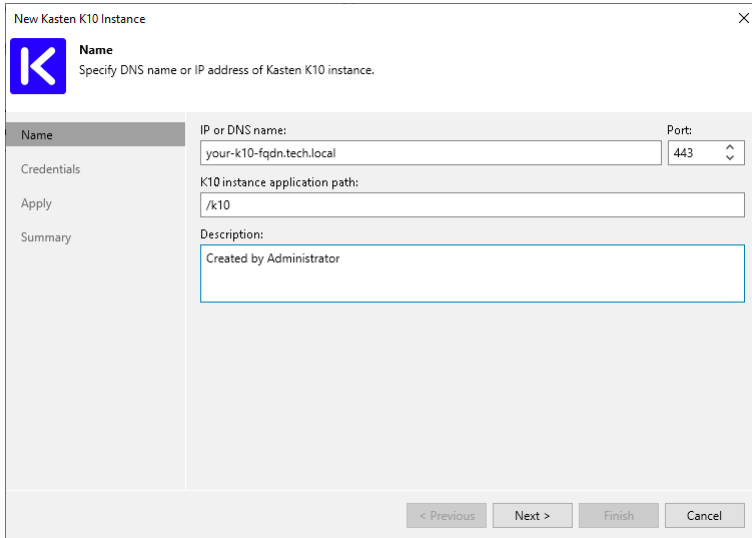
To launch the **New Kasten K10 Instance** wizard, do one of the following:

- Open the **Backup Infrastructure** view. Navigate to **Manage Servers** and click **Add Server** on the ribbon. In the **Add Server** window, select **Kasten K10 backup 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 **Kasten K10 backup for Kubernetes**.



Step 2. Specify K10 Cluster Settings

At the **Name** step of the wizard, specify an IP address or DNS name (to specify the DNS name, use the following format: *your-k10-fqdn.tech.local*), an URL path to the K10 dashboard and a description for the K10 application.



The screenshot shows a wizard window titled "New Kasten K10 Instance" with a close button (X) in the top right corner. The window features a blue "K" logo in the top left. Below the logo, the word "Name" is displayed in bold, followed by the instruction "Specify DNS name or IP address of Kasten K10 instance." A vertical sidebar on the left contains the following items: "Name" (highlighted), "Credentials", "Apply", and "Summary". The main content area is divided into three sections: "IP or DNS name:" with a text input field containing "your-k10-fqdn.tech.local" and a "Port:" dropdown menu set to "443"; "K10 instance application path:" with a text input field containing "/k10"; and "Description:" with a text area containing "Created by Administrator". At the bottom of the window, there are four buttons: "< Previous", "Next >", "Finish", and "Cancel".

Step 3. Specify Credentials

At the **Credentials** step of the wizard, specify credentials for the K10 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 a cluster service account that has the `k10-admin` ClusterRole. For more information on how to get the bearer token, see [Kasten K10 Docs](#). For more information on K10 cluster roles, see [Kasten K10 Docs](#).

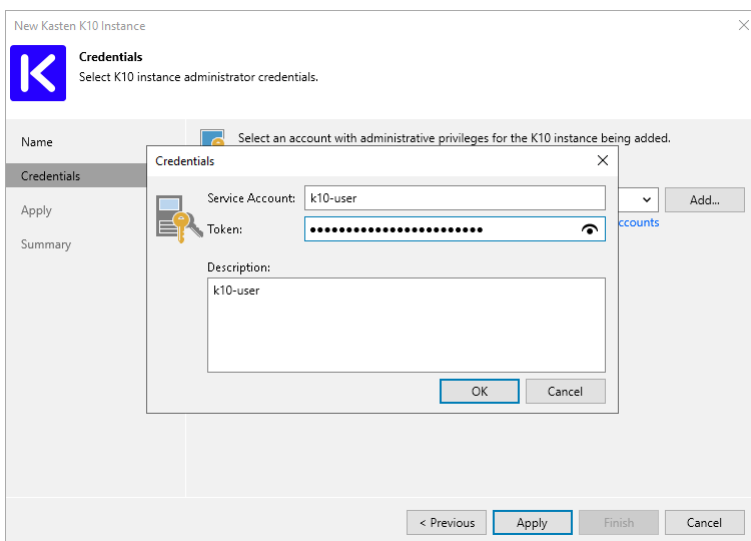
NOTE

When you add the K10 application, Veeam Backup & Replication checks the certificate that is used to access the K10 dashboard. If the certificate is not trusted, Veeam Backup & Replication will display a certificate warning.

In the warning window, you can do the following:

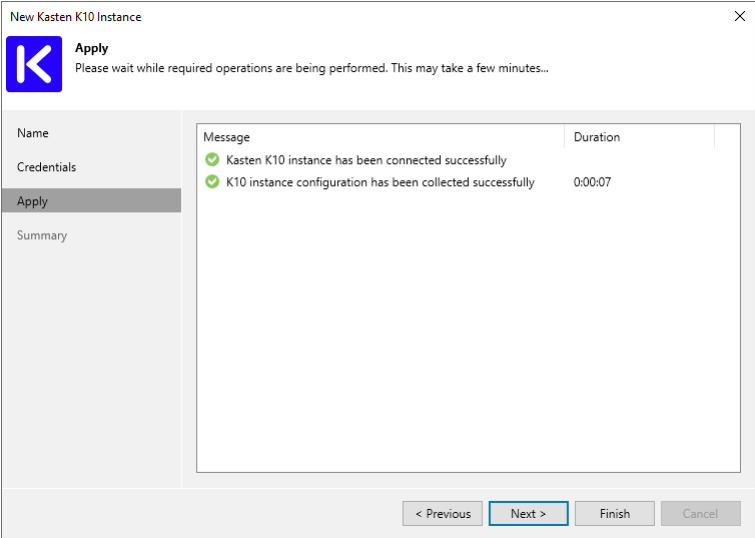
- Click **View** for the detailed information about the certificate.
- Click **Continue** to trust the certificate.
- Click **Cancel** if you do not trust the certificate. However, in this case you will not be able to connect to the K10 application.

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.



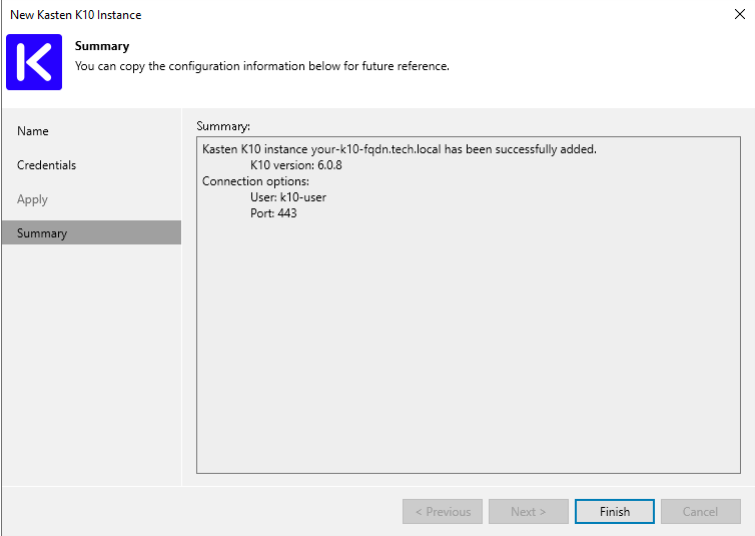
Step 4. Apply Settings

At the **Apply** step of the wizard, wait until Veeam Backup & Replication applies the settings. Click **Next** to complete the procedure of adding the K10 application.



Step 5. Finish Working with Wizard

At the **Summary** step of the wizard, review details of the K10 application and click **Finish**.



Managing K10 Instance

After you add a K10 instance to Veeam Backup & Replication infrastructure, you can edit instance settings, remove it from Veeam Backup & Replication infrastructure, or open the instance Web UI right in Veeam Backup & Replication console.

Viewing Snapshots and Backups

In Veeam Backup & Replication console, you can view information about snapshots and backups exported by K10 policies or manually. Veeam Backup & Replication displays the backups and snapshots located in both Veeam backup repositories and other location profiles, for example, object storage repositories.

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

- The **Backups** node shows exports created by K10 policies.
- The **Snapshots** subnode shows snapshots created by K10 policies.

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

Icon	State
	K10 snapshot or export.
	K10 application.

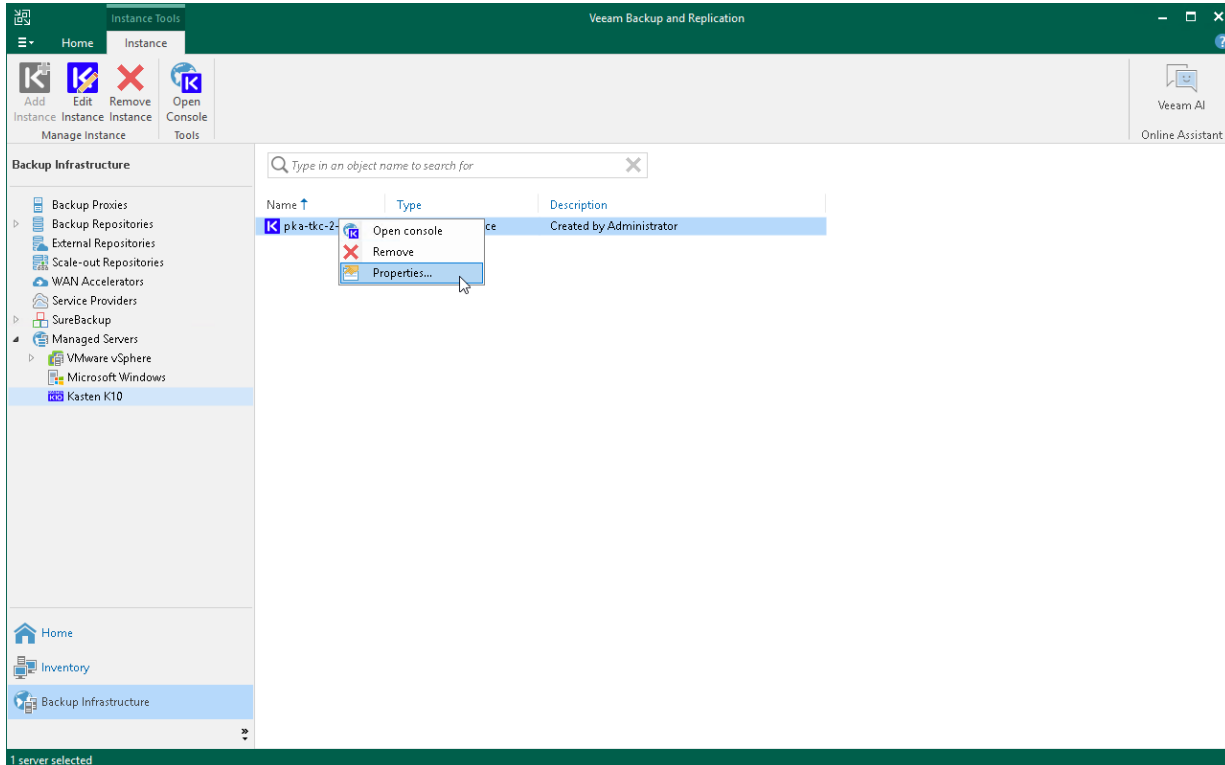
This information in the working area provides the following data:

- 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 a platform service where backups are created

Editing Instance Settings

To edit settings of a K10 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 K10 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 K10 Instance](#) section.



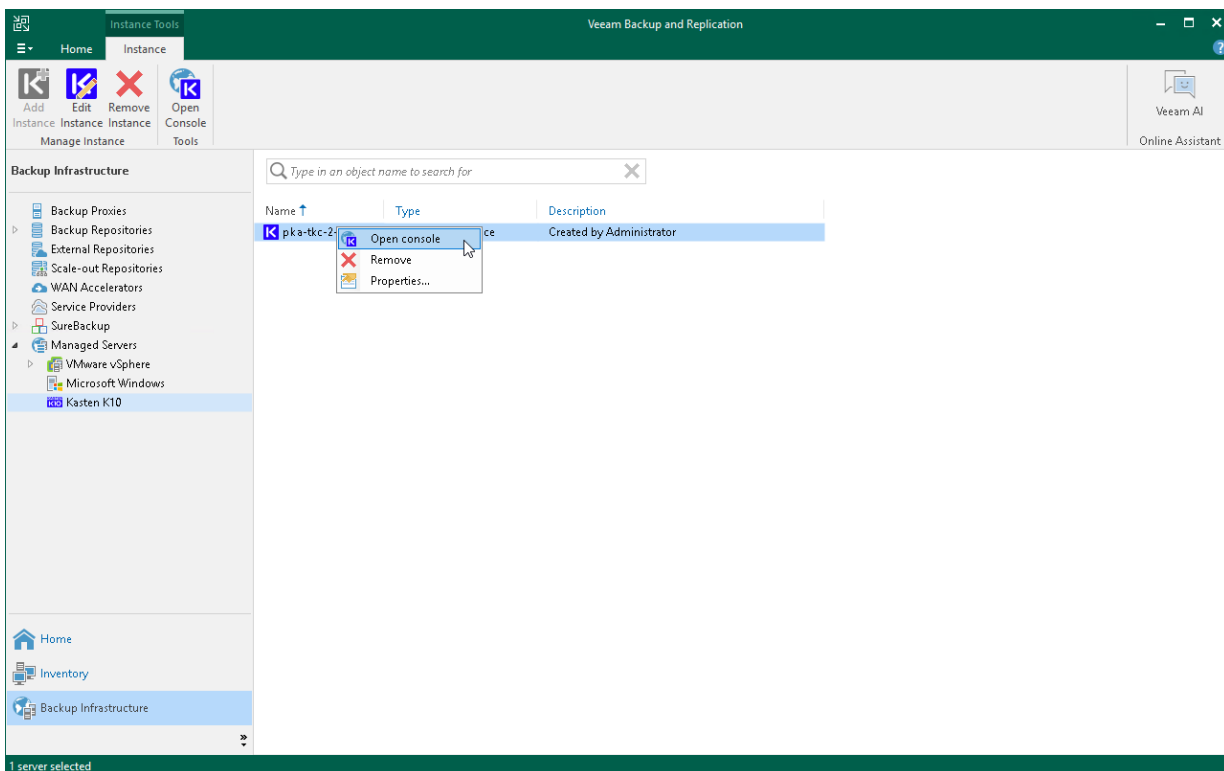
Opening Instance Web UI

If you want to access Kasten K10 and configure options not available in Veeam Backup & Replication console, you can perform the necessary actions using the Kasten K10 Web UI.

To open the Kasten K10 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 K10 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 will navigate you to the Kasten K10 URL. For more information on what you can do in the Web UI, see the [Kasten Docs](#).



Removing Instance

If you do not plan to manage a K10 instance from Veeam Backup & Replication console, you can remove it from Veeam Backup & Replication infrastructure.

NOTE

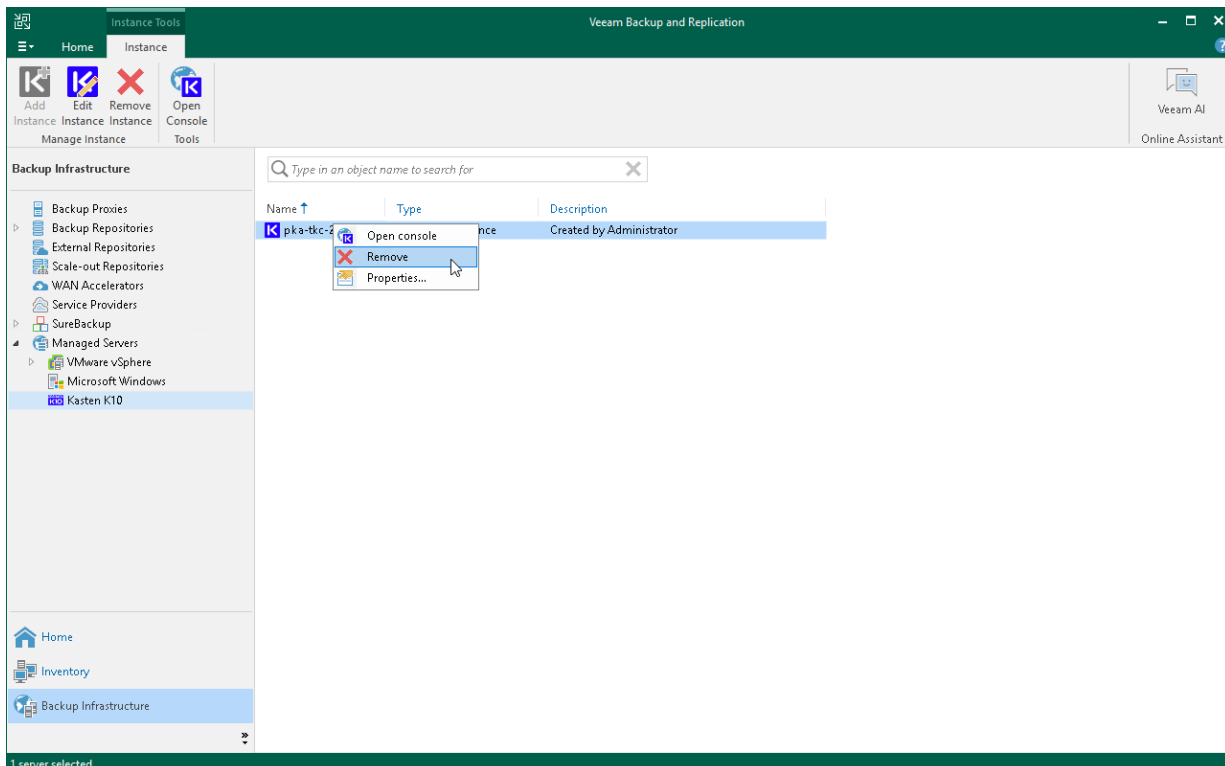
After you remove the K10 instance, the changes will take place on the Veeam Backup & Replication side and it will result in the following limitations:

- K10 policies belonging to the instance will not be available in the Veeam Backup & Replication console.
- All snapshots are no longer available in the **Snapshot** node.
- You will not be able to restore to Kubernetes snapshots and K10 exports belonging to the instance to Kubernetes.

Removing Instance

To remove an 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 appliance that you want to remove, and click **Remove Instance** on the ribbon. Alternatively, right-click the instance and select **Remove**.
4. In the Veeam Backup & Replication window, click **Yes**.



Data Protection

To protect applications running in your K10 environment, you must create K10 policies. For more information, see [Kasten Docs](#). After policies are created and backups of application are exported to Veeam backup repositories and other location profiles, you can view the backed-up applications, check statistics on K10 policies and remove these policies from Veeam Backup & Replication infrastructure.

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 not available. For more information, see [Creating Backup Copy Jobs for K10 Backups](#).

- **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 K10 Backups to Cloud Repositories](#).

- **Backup to tape jobs**

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

How K10 Policy Works

To move backups exported by K10 policies to Veeam backup repositories, a K10 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 K10 cluster to backup repositories. When you start a K10 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 K10 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 K10 policy is completed, Veeam Data Movers are removed from both the K10 and Veeam Backup & Replication infrastructure. For more information, see the [Veeam Data Mover](#) section in the Veeam Backup & Replication User Guide.

When you launch a K10 policy, the following happens:

1. K10 takes a snapshot of applications and uses these snapshots to make exports.
2. K10 copies configuration files of applications to 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.

Backup Chain and Retention Policy

This section covers information on how Veeam Backup & Replication stores backups exported by K10 policies and how Veeam Backup & Replication applies backup retention policy to these backups.

Backup Chain

Veeam Backup & Replication keeps backups exported by K10 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 K10, Veeam Backup & Replication uses the synthetic full backup method and implements it the following way.

When K10 exports application disks to backup repositories for the first time, a Veeam Data Mover creates a VBK file. When a K10 policy starts again, the Veeam Data Mover creates a temporary incremental backup file (VIB). This temporary VIB keeps incremental changes of K10 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 K10 policy session finishes, the temporary incremental backup is removed from the Veeam backup repository. Therefore, a backup chain of data exported from K10 consists of VBK and VBM backup files.

Retention Policy

To store and manage backups exported by a K10 policy, Veeam Backup & Replication applies retention policy that you have specified in the K10 policy settings. For more information, see [Kasten Docs](#).

Creating K10 Policies

To export backups of applications to Veeam backup repositories, you must create K10 policies and define the necessary settings in the K10 dashboard associated with your K10 cluster.

To create a K10 policy, open the K10 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 K10 policies. For more information, see [Kasten Docs](#).

2. **Configure K10 policy.**

In the K10 dashboard, configure a policy and select the necessary Veeam backup location profile. K10 will export backups of applications from the K10 cluster to the Veeam backup repository according to these settings. For more information, see [Kasten Docs](#).

After you configured the K10 policy, it appears in Veeam Backup & Replication infrastructure.

Managing K10 Policies

After you install Veeam Backup for Kasten K10, you can use Veeam Backup & Replication console to manage K10 policies. You can start, stop, edit, disable and delete backup policies directly in Veeam Backup & Replication console.

Starting and Stopping Policies

Veeam Backup for Kasten K10 allows you to start a K10 policy manually from Veeam Backup & Replication console. It can be help if you want to create an additional snapshot or export and do not want to modify the configured backup policy schedule. You can also stop a K10 backup policy if processing of applications is about to take too long, and you do not want the policy to produce heavy load on the production environment during business hours.

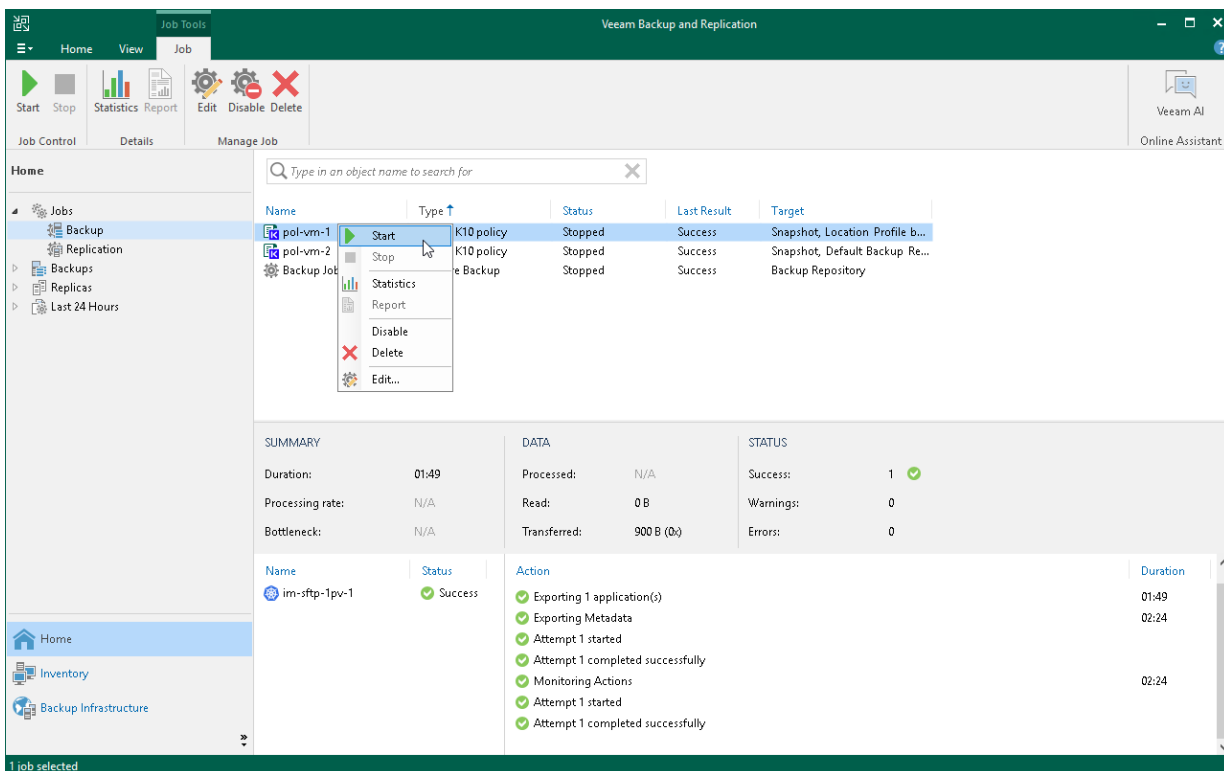
Starting K10 Policies

To start a K10 policy:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the necessary K10 policy and click **Start** on the ribbon. Alternatively, right-click the selected policy and click **Start**.

TIP

To select several K10 policies, click the first policy, press and hold the [SHIFT] key and select the other policies.



Stopping K10 Policies

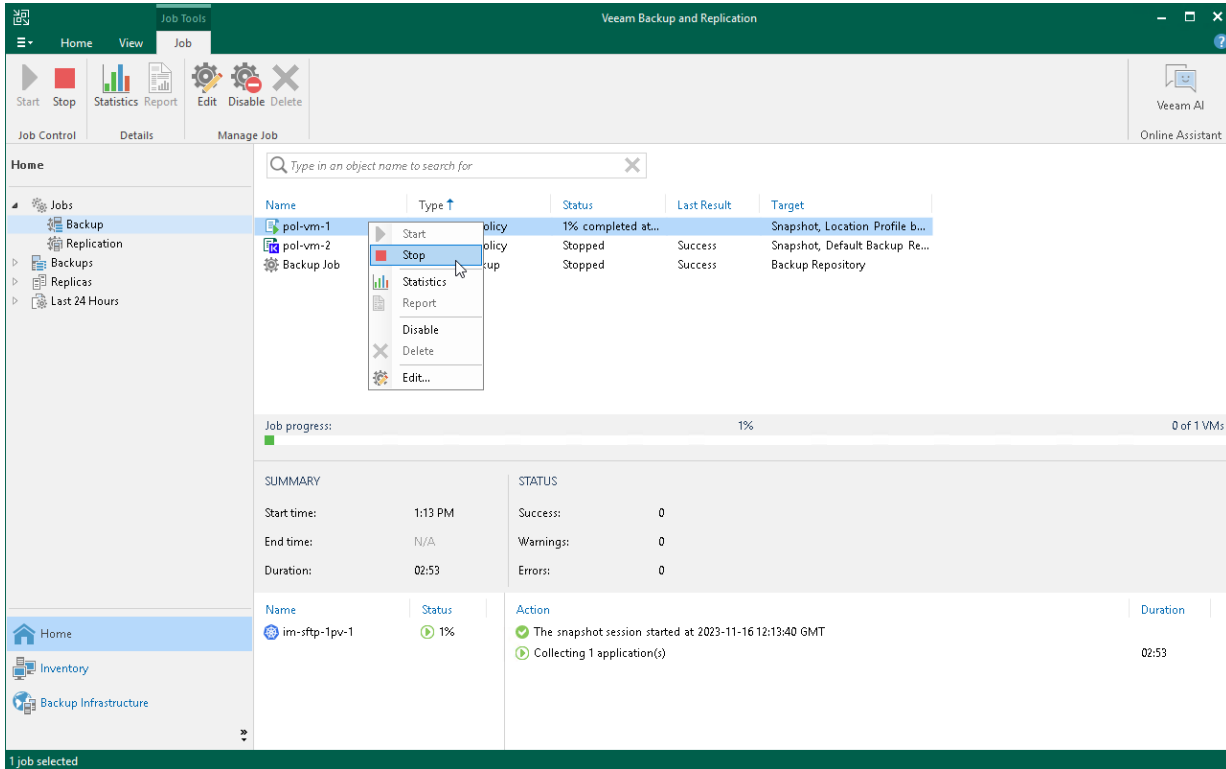
To stop a K10 policy:

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

3. In the working area, select the necessary K10 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 K10 policies, click the first policy, press and hold the [SHIFT] key and select the other policies.

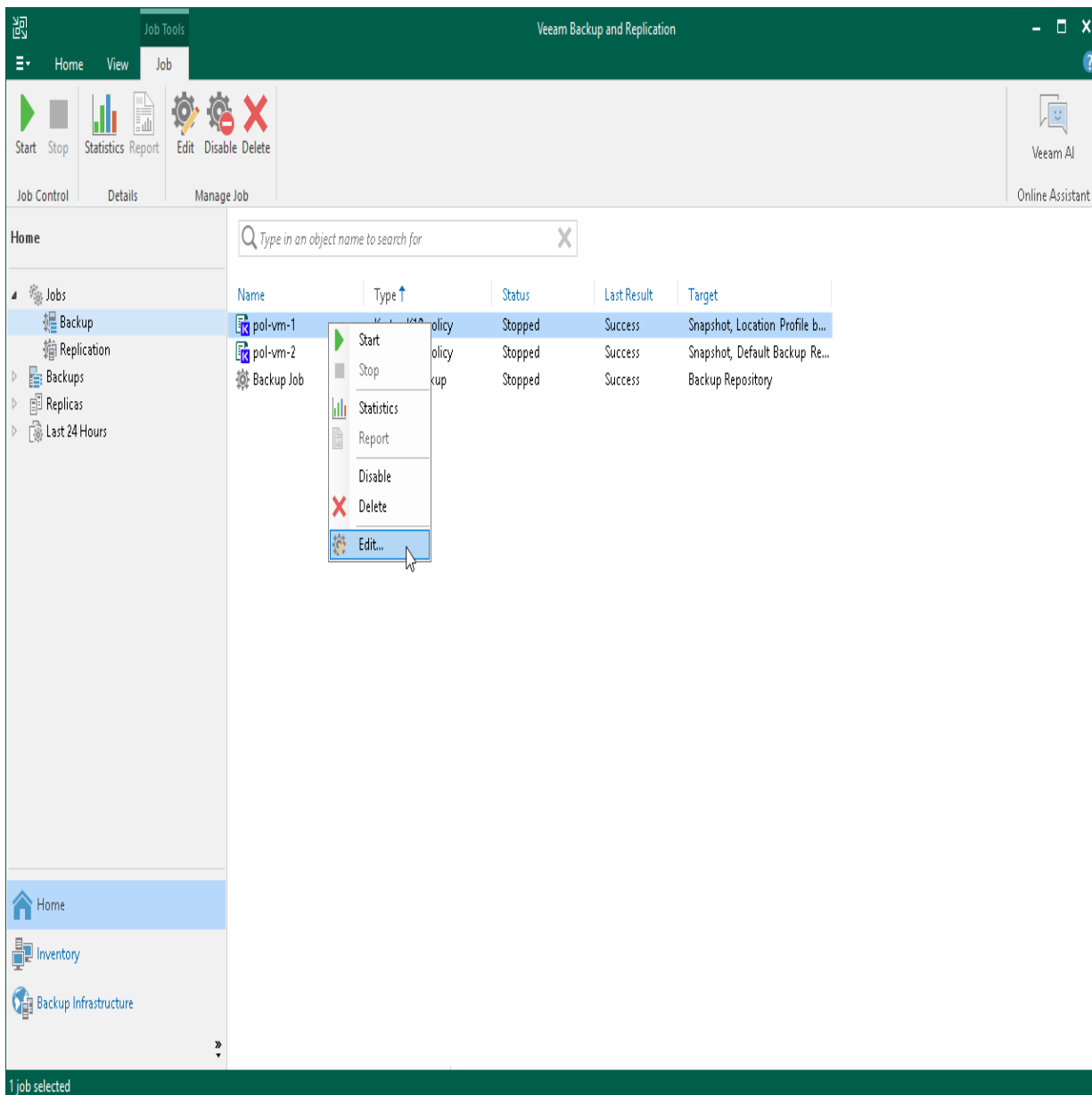


Editing Policies Settings

Veeam Backup for Kasten K10 allows you to edit settings of K10 policies from Veeam Backup & Replication console using redirection to the K10 web UI. For example, you can add more applications to the K10 policy or change the K10 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 Backup for Kasten K10 allows you to temporarily disable or permanently delete K10 policies from both Veeam Backup & Replication and K10 infrastructure. When you disable a backup policy, Veeam Backup for Kasten K10 disables the schedule configured for the backup policy. This means that the K10 policy will no longer start automatically. You can enable and start the disabled policy manually any time you need.

Disabling K10 Policies

You can disable a K10 policy only if it has a schedule configured beforehand. For more information on configuring a K10 policy schedule, see [Kasten Docs](#).

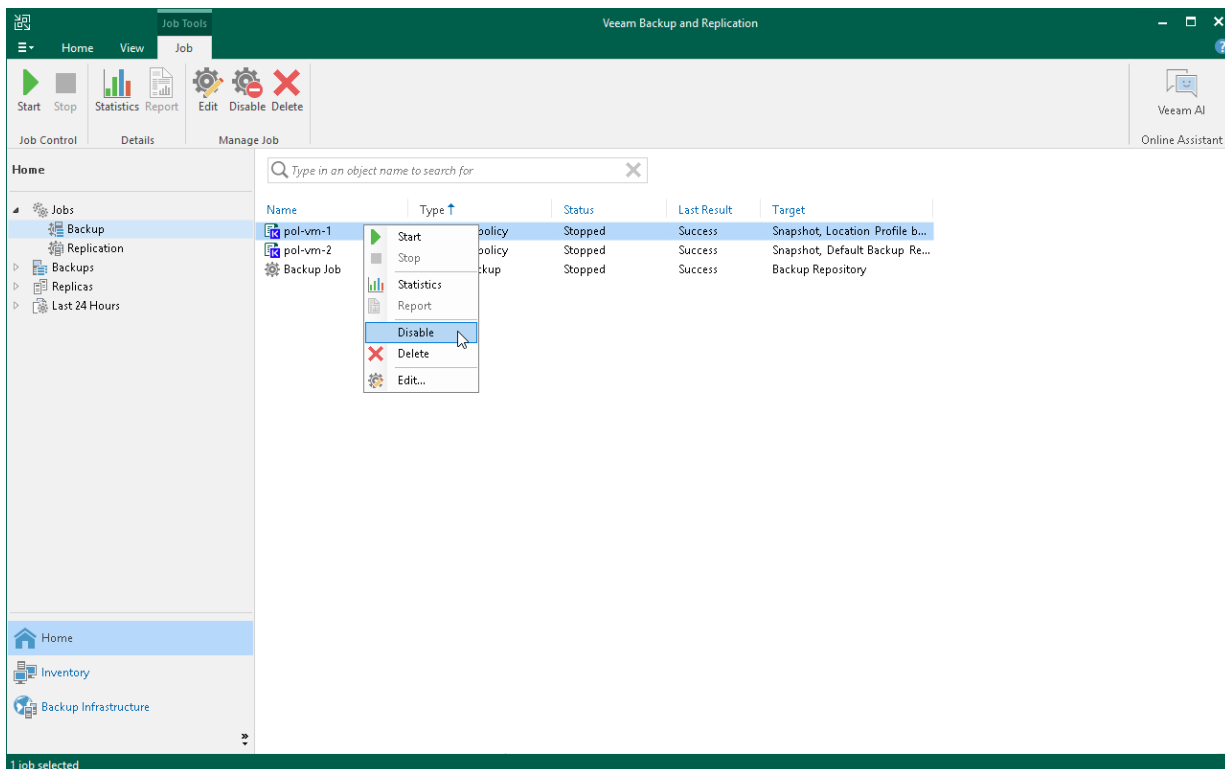
To disable a K10 policy:

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 K10 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.



To delete a K10 policy from Veeam Backup & Replication infrastructure:

1. Open the **Home** view.

2. In the inventory pane, select **Jobs**.
3. In the working area, select the necessary K10 policy and click **Delete** on the ribbon. Alternatively, right-click the necessary backup policy and select **Delete**.

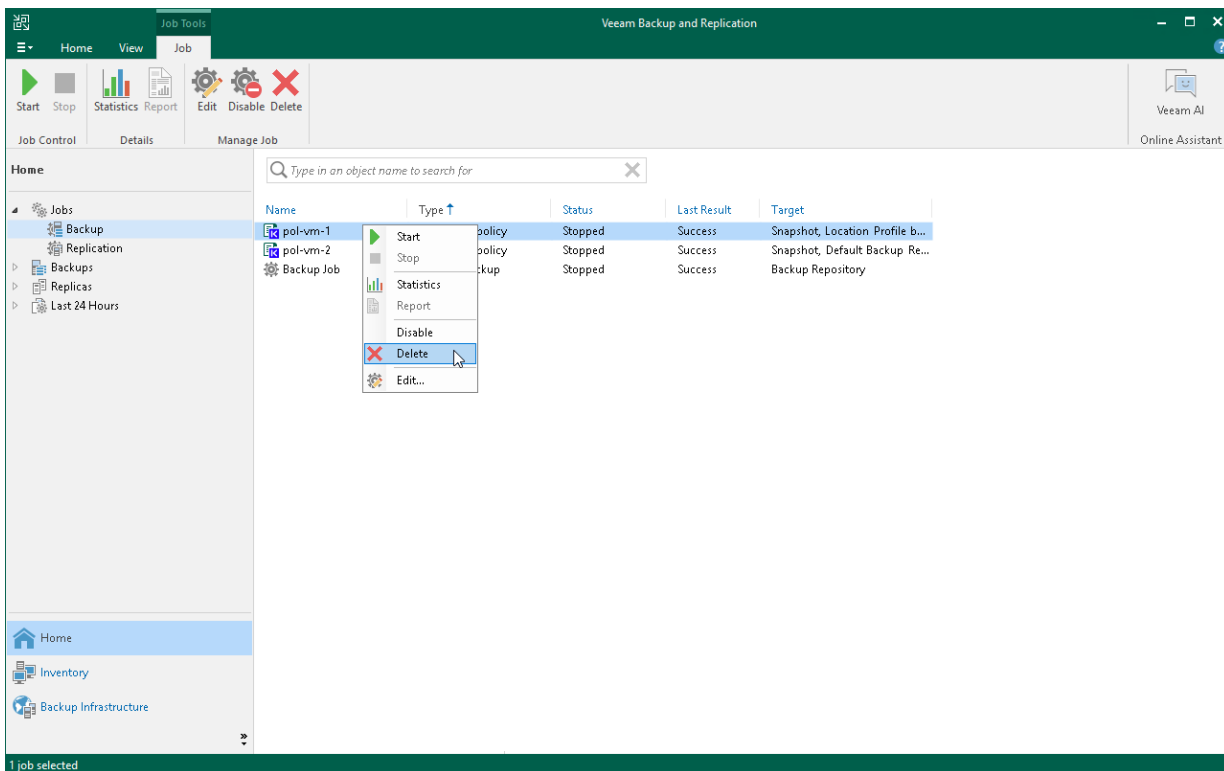
TIP

To select several K10 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 archive tier, they will also be displayed under the **Backups > Archive (Orphaned)** node.

IMPORTANT

Veeam Backup for Kasten K10 deletes a K10 policy from both Veeam Backup & Replication infrastructure and K10 instance.



Managing Backed-Up Data

Veeam Backup for Kasten K10 allows you to perform the following operations from Veeam Backup & Replication console with backups exported by K10 policies or manually.

- [View Backup Properties](#)
- [Delete Backups](#)

Viewing Backup Properties

In Veeam Backup & Replication console, you can view information about backups exported by K10 policies or manually. This information provides the following data:

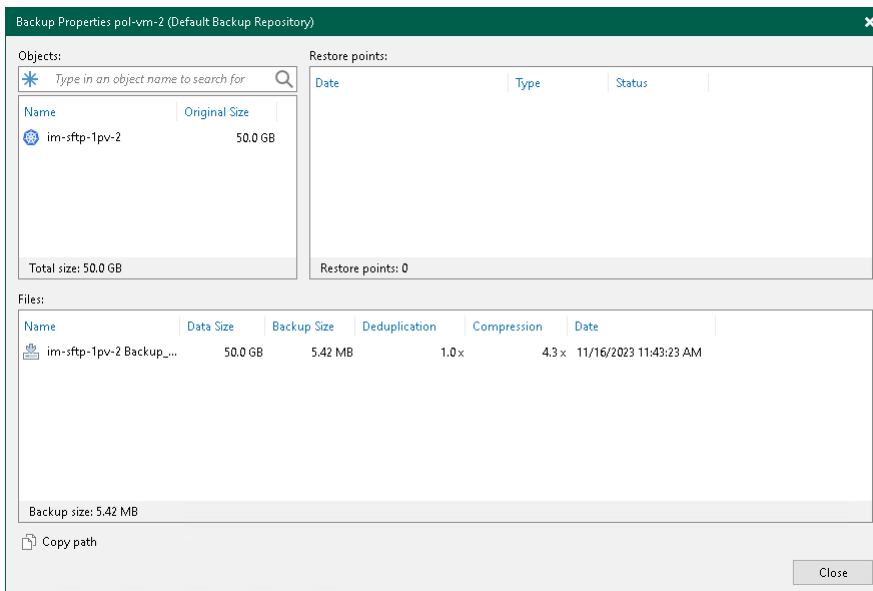
- Veeam backup repository and folder on this repository where the backup is stored
- Available restore points
- Date of restore points creation
- Data size and backup file size

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 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.



Deleting Backups

Veeam Backup for Kasten K10 allows you to permanently delete backups exported by K10 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 K10 policy, Veeam Backup for Kasten K10 will create full backups for applications included 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.

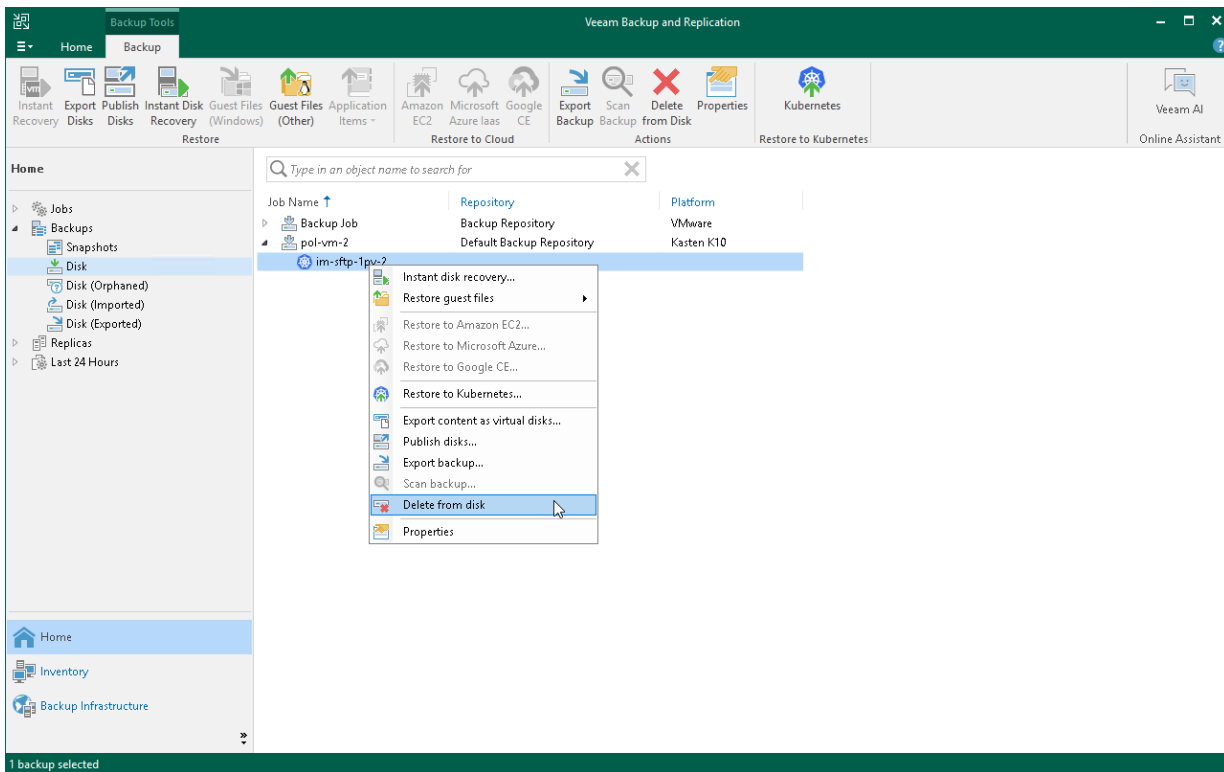
This option allows you to delete the following type of data:

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



Exporting K10 Backups Manually

You can manually export backups of K10 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 [Kasten Docs](#).

2. **Export application restore point.**

In the K10 dashboard, select a restore point of an application which backup you want to export and select the necessary Veeam backup location profile. K10 will export application backups to the Veeam backup repository according to these settings. For more information on the manual export of application backups, see [Kasten Docs](#).

After you started the manual export, it appears in 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.

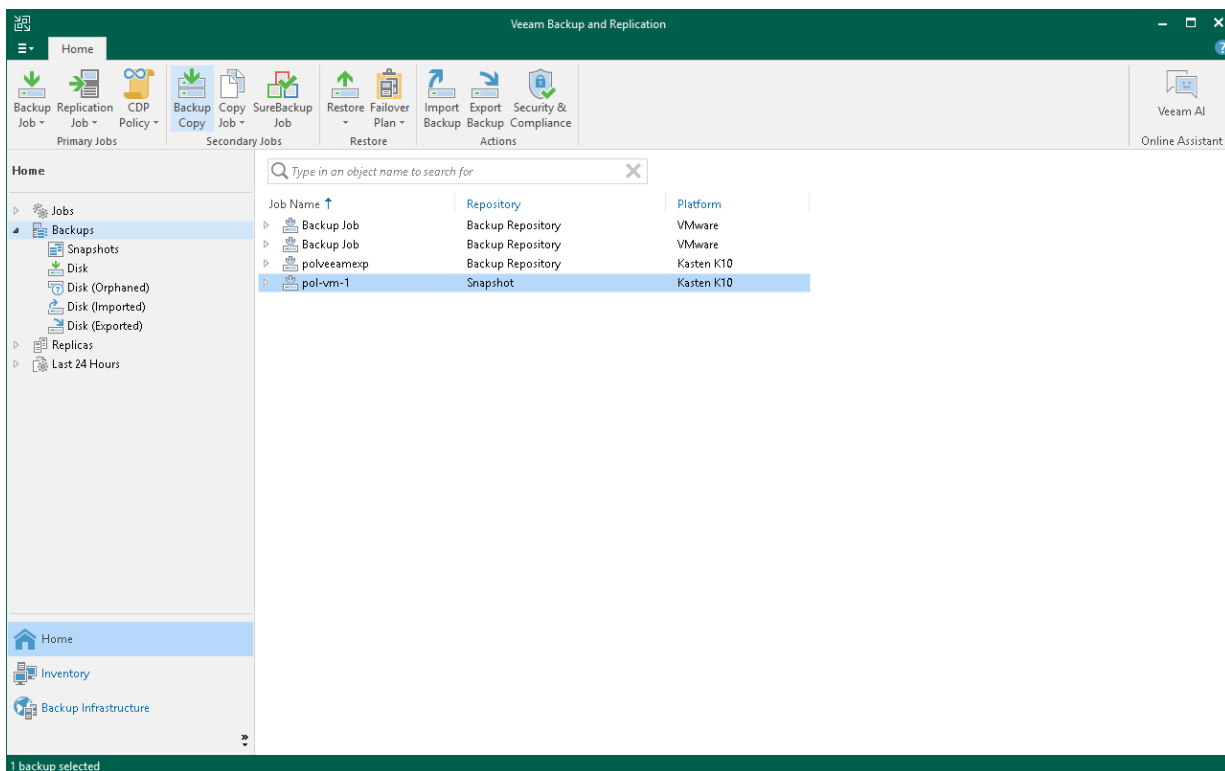
Backup copy is a job-driven process. Veeam Backup & Replication fully automates the backup copy process and lets you specify retention settings to maintain the desired number of restore points, as well as full backups for archival purposes. To create a backup copy job, Veeam Backup & Replication uses K10 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 K10 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 and navigate to **Backups** and select the necessary K10 policy.
3. Complete the **New Backup Copy Job** wizard as described in the [Creating Backup Copy Jobs](#) section in the Veeam Backup & Replication User Guide.



Copying Data to Cloud Repositories

If you want to store copies of backups exported from K10 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 K10 to cloud repositories, do the following:

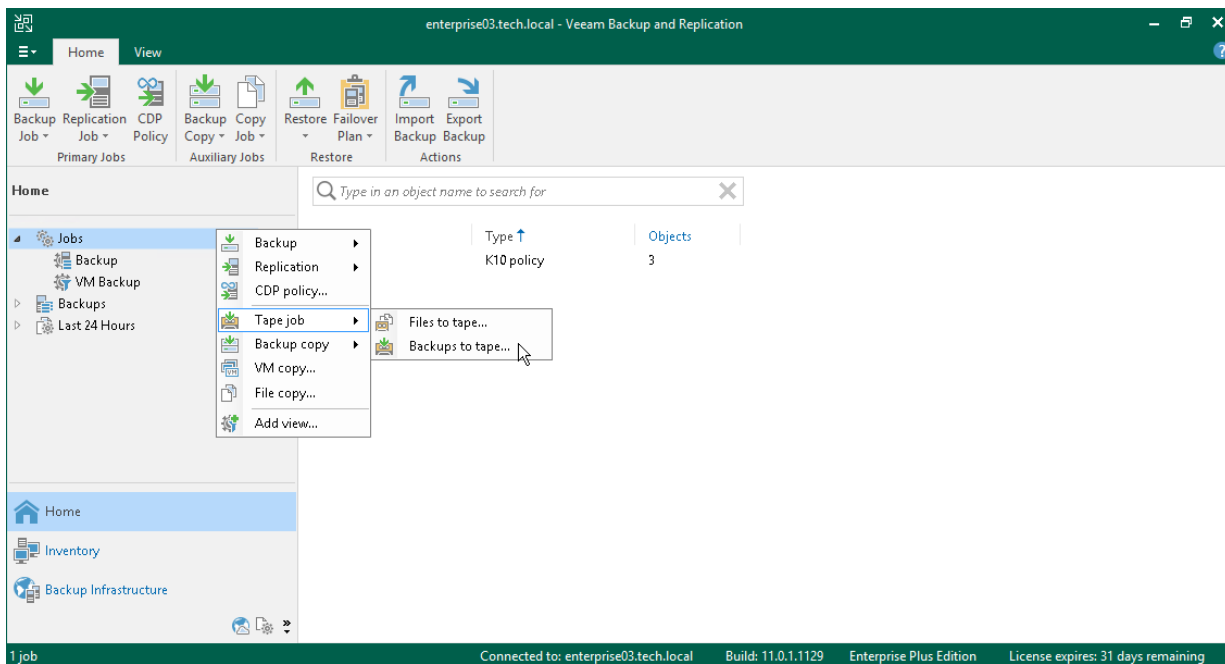
1. Depending on your environment, configure one of the following Cloud Connect Infrastructure types:
 - [For service providers] Follow steps described in the [Setting Up SP Veeam Cloud Connect Infrastructure](#) section in the Veeam Cloud Connect User Guide.
 - [For tenants] Follow steps described in the [Setting Up Tenant Veeam Cloud Connect Infrastructure](#) section in the Veeam Cloud Connect User Guide.
2. Run a K10 policy.
3. Configure a backup copy job for backups exported from K10. Follow the instructions provided in [Creating Backup Copy Jobs for K10 Backup Exports](#).

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 copying of image-level backups to tape devices and lets you specify scheduling, archiving and media automation options. For more information on the supported tapes and operations which you can perform with tapes, see the [Tape Devices Support](#) section in the Veeam Backup & Replication User Guide.

To copy backups exported by K10 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 Veeam Backup & Replication console to view real-time statistics for any backup policy. For more information on how to review statistics, see the [Reporting](#) section in the Veeam Backup & Replication User Guide.

Data Recovery

Veeam Backup for Kasten K10 offers the following recovery options for various disaster recovery scenarios:

- [Restoring to Kasten K10](#)
Restores snapshots to Kasten K10.
- [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 Backups](#)
Synthesize an independent full backup file using restore points that are located in your Veeam backup repositories.

IMPORTANT

Veeam Backup for Kasten K10 does not allow you to restore Kubernetes containers from a Veeam Backup & Replication server to a K10 cluster or any other location. To perform restore operations with Kubernetes containers, use K10 recovery options. For more information, see [Kasten Docs](#).

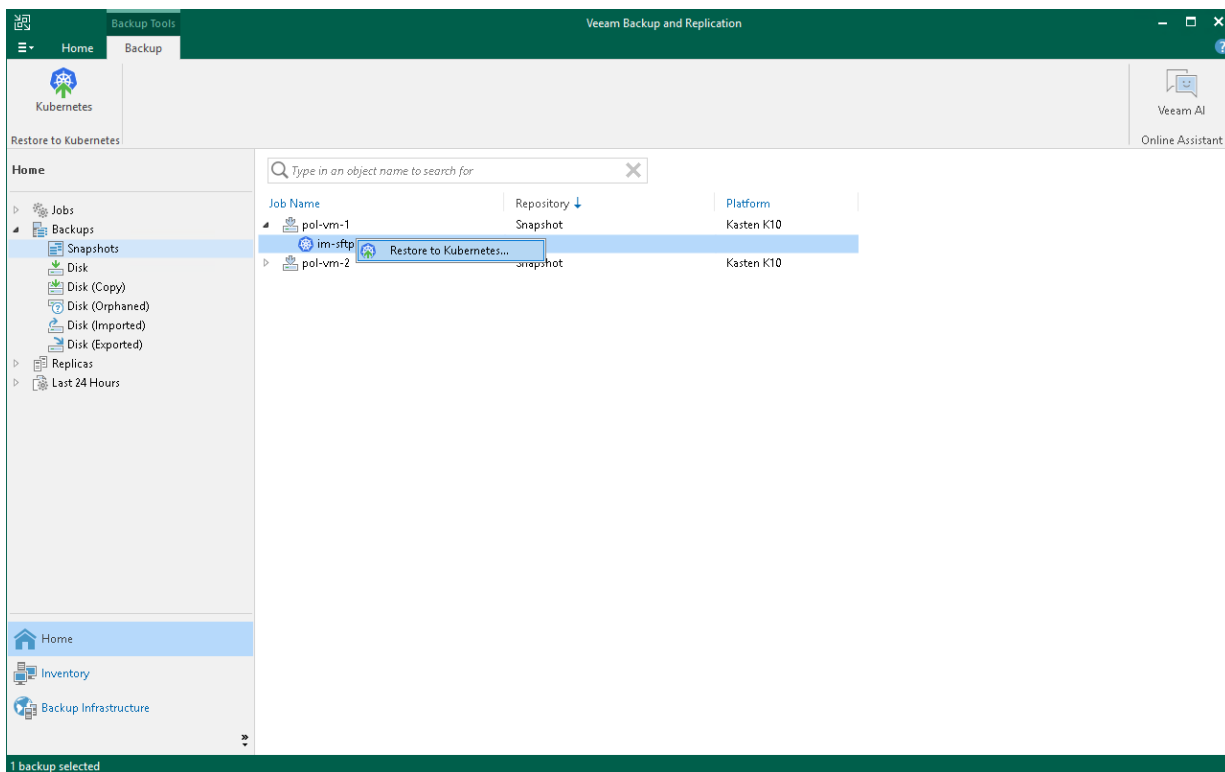
Restoring to Kasten K10

Veeam Backup & Replication allows you to restore backups exported from K10 to Kasten K10 environment. When you restore backups, Veeam Backup & Replication redirects you to the Kasten K10 Web UI to proceed with restore.

To backups exported from K10 to Kasten K10, do the following:

1. Open the **Home** view. In the inventory pane, navigate to **Backups > Disk** if you want to restore from K10 exports, or to **Backups > Snapshots** if you want to restore from snapshots. In the working area, select applications whose snapshots 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 [Kasten docs](#).

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

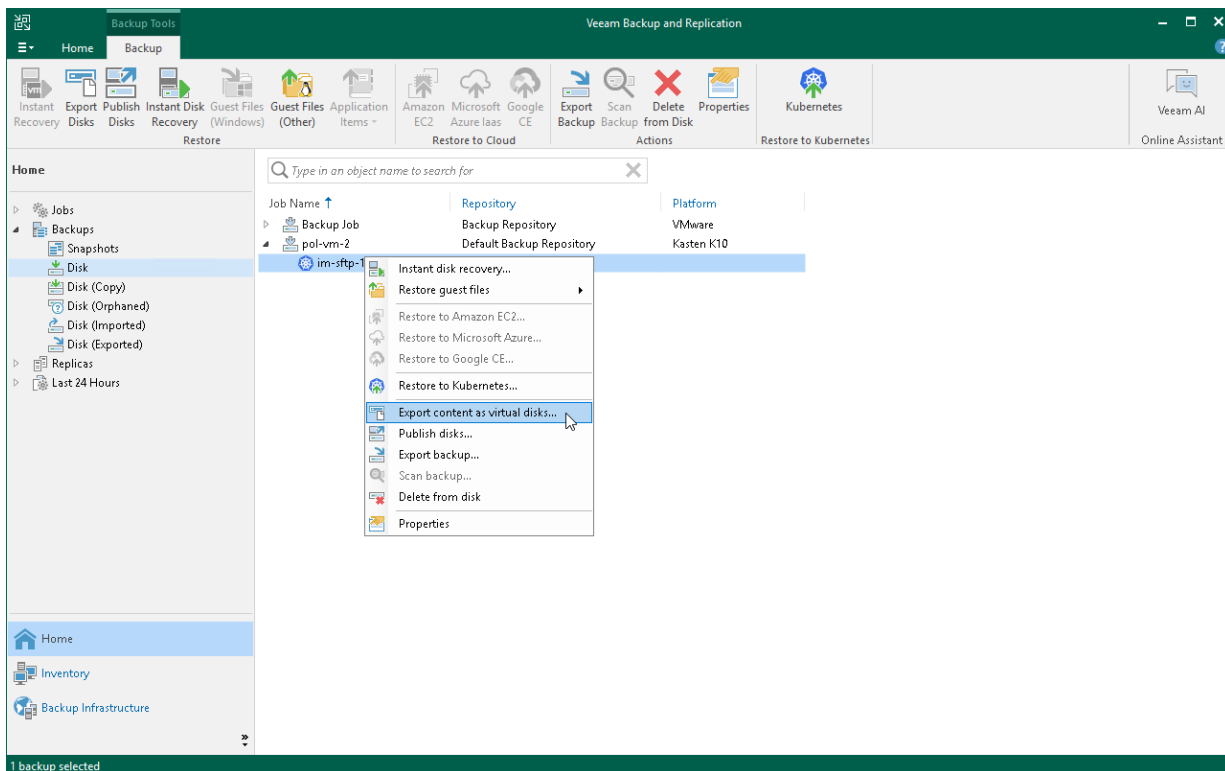


Exporting Disks

Veeam Backup & Replication allows you to restore disks of backups exported from K10. You can restore disks in the VMDK, VHD or VHDX format. For more information on disks export, see the [Disk Export](#) section in the Veeam Backup & Replication User Guide.

To restore disks of backups exported from K10 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 Disk**. 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.

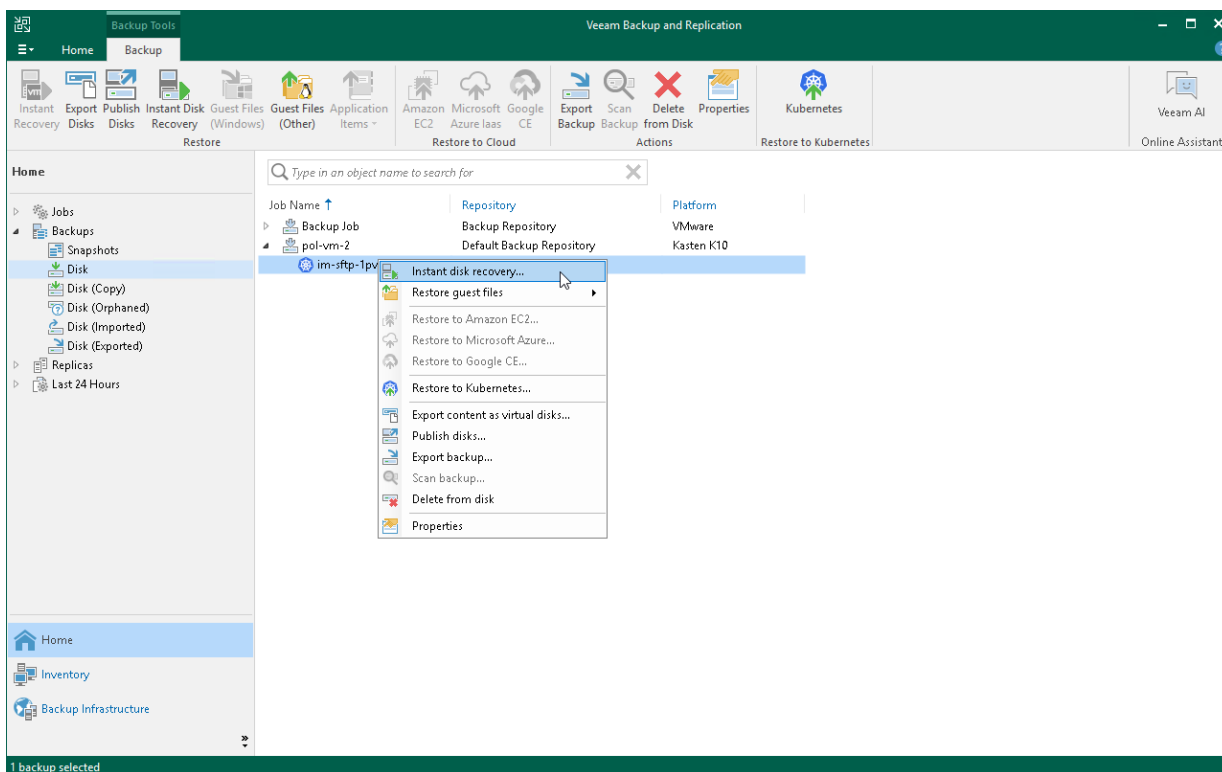


Instant First Class Disk (FCD) Recovery

With Instant First Class Disk (FCD) Recovery, you can immediately restore disks of backups, exported from K10, 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 K10:

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 K10. 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.

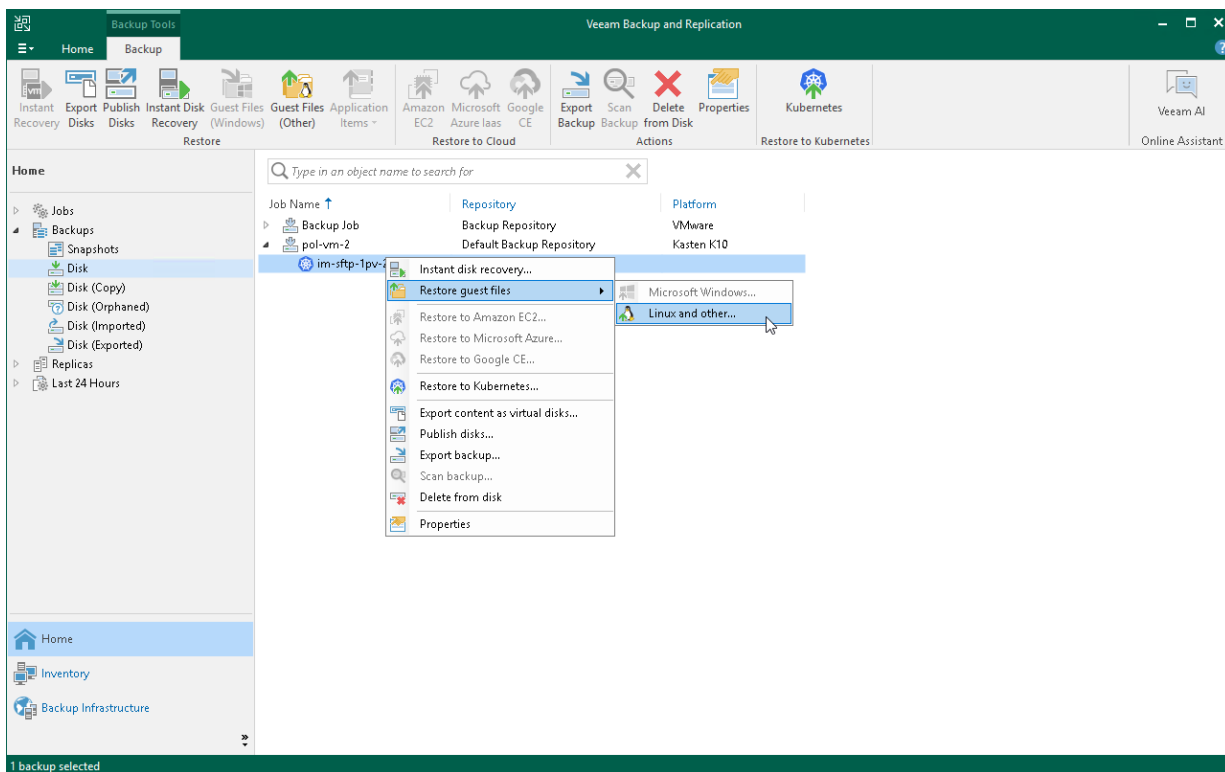
NOTE

Consider the following:

- Veeam Backup for Kasten K10 supports only restore from Linux, Unix and other non-Microsoft Windows OSes.
- Veeam Backup for Kasten K10 does not support restore of individual guest OS files and folders to the original location (applications added to a K10 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 [limitations and prerequisites](#) listed in the Veeam Backup & Replication User Guide.
2. Launch and complete the **Guest File 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 **Guest Files (Other)**. Alternatively, right-click the application and select **Restore guest files > Linux and other**.
3. Complete the wizard as described in the [Restoring VM Guest OS Files \(Multi-OS\)](#) section in the Veeam Backup & Replication User Guide.



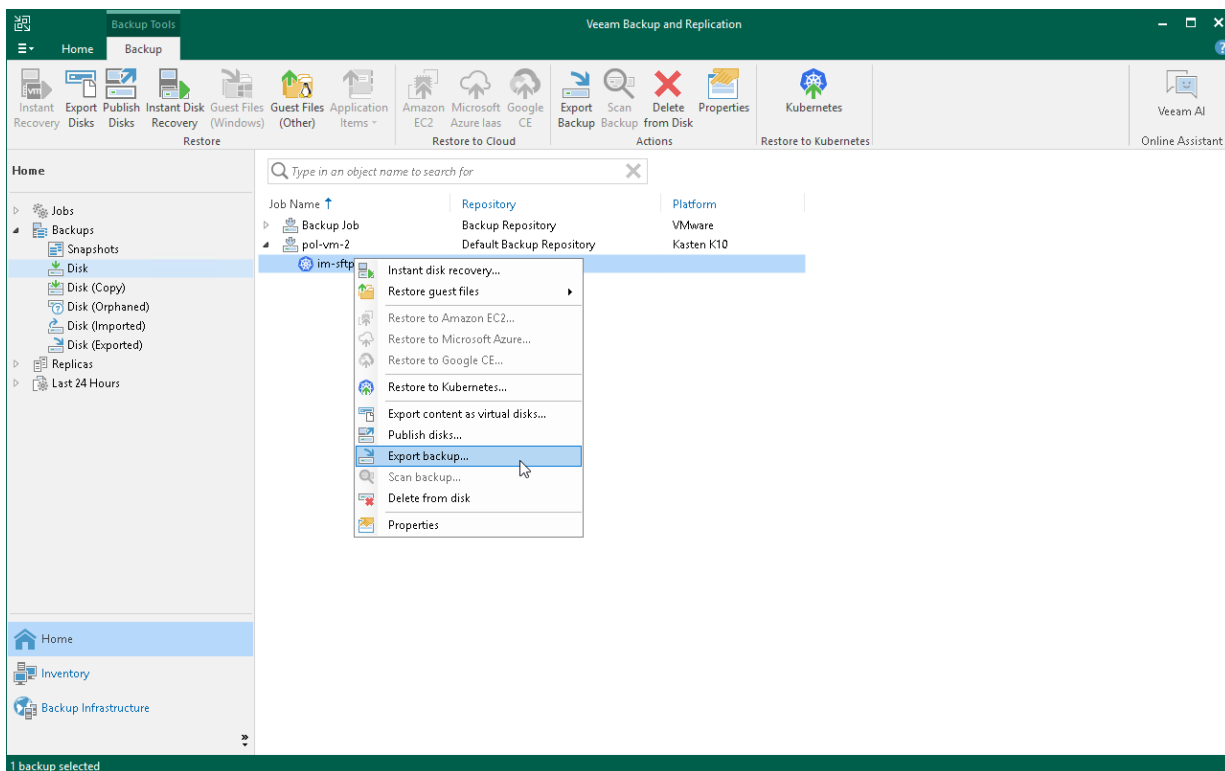
Exporting Backup Files

You can export full backups files of applications backed-up by K10 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 K10 policy. You can move this backup file to a different location without affecting a backup chain of backup files exported by the K10 policy. For more information on exporting full backups, see the [Exporting Backups](#) section in the Veeam Backup & Replication User Guide.

To export full backups files of applications backed-up by K10:

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, it is displayed under the **Backups > Disk (Exported)** node.



Viewing Statistics

Veeam Backup for Kasten K10 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 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 K10 platform, management of Kubernetes containers and K10 policies. You have to contact [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 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 [Export Logs](#) section in the Veeam Backup & Replication User Guide.

IMPORTANT

In the **Export Logs** wizard, you can not export logs for separate K10 policies and backup files.

Export Logs

Scope
Specify the scope for logs export.

Scope

Date Range

Location

Export

Export logs for this job:

Export logs for these objects:

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

Managed servers:

Server	Components
<input checked="" type="checkbox"/> 198.51.100.5	Installer, Mount Server, Transport, Veeam A...

< Previous Finish