# Contents

CONTACTING VEEAM SOFTWARE ................................................................. 4
ABOUT THIS DOCUMENT ............................................................................. 5
OVERVIEW ........................................................................................................ 6
BACKUP INFRASTRUCTURE COMPONENTS .................................................. 7
PLANNING AND PREPARATION ..................................................................... 9
  System Requirements .................................................................................. 10
  Used Ports .................................................................................................. 11
  Required Permissions .................................................................................. 12
  Licensing ................................................................................................... 13
DEPLOYMENT AND CONFIGURATION ............................................................. 14
DATA PROTECTION .......................................................................................... 15
  How K10 Policy Works ................................................................................ 16
  Backup Chain and Retention Policy ............................................................. 17
  Creating K10 Policies .................................................................................. 18
  Exporting K10 Backups Manually ................................................................. 19
  Removing K10 Policies ............................................................................... 20
  Managing Backed-Up Data ......................................................................... 21
    Viewing Backup Properties ....................................................................... 22
    Deleting Backups ..................................................................................... 23
  Creating Backup Copy Jobs ......................................................................... 25
  Copying Data to Cloud Repositories ............................................................ 26
  Creating Backups to Tapes .......................................................................... 27
  Viewing Statistics ....................................................................................... 28
DATA RECOVERY .............................................................................................. 29
  Exporting Disks .......................................................................................... 30
  Instant First Class Disk (FCD) Recovery ...................................................... 31
  Restoring Guest OS Files ............................................................................ 32
  Exporting Backup Files .............................................................................. 33
  Viewing Statistics ....................................................................................... 34
SUPPORT INFORMATION .................................................................................. 35
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 Integration with Veeam Backup Repositories for Kasten K10 solution.

Intended Audience

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

Integration with Veeam Backup Repositories for Kasten K10 is a data protection and data recovery solution that allows you to export backups created by K10 policies to Veeam backup repositories directly from the K10 web console. Integration with Veeam Backup Repositories for Kasten K10 is based on the VMB API functionality that allows a K10 cluster to interact with a Veeam Backup & Replication server. After K10 exports backups to Veeam backup repositories, these backups become available in the Veeam Backup & Replication console and you can perform data protection and data recovery operations with them.

IMPORTANT

This guide is intended for users who have already deployed K10 and have a good understanding of the K10 solution.

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

- View backups exported by K10 policies.
- Monitor session statistics.
- Delete policies from the Veeam Backup & Replication infrastructure.
- Remove backups exported by K10 policies from the Veeam Backup & Replication infrastructure.
- 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 Integration with Veeam Backup Repositories for Kasten K10, you must configure the infrastructure that will consist of the following components:

1. **K10 cluster.**
   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 cluster, see Kasten Docs.

2. **Veeam Backup & Replication server.**
   A server that manages Veeam backup repositories and that allows you to perform additional data protection scenarios, different from the K10 policies, perform data recovery and restore operations. For more information, see the Backup Server section in the Veeam Backup & Replication User Guide.

3. **Veeam backup repository.**
   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 Backup Repositories 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.

4. **Additional data protection layers.**
   Veeam Backup & Replication allows you to keep backups exported by K10 policies in the following types of additional repositories:

   - **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
Related Sources

- Planning and Preparation
- Backup Copy in the Veeam Backup & Replication User Guide
- Tape Devices Support in the Veeam Backup & Replication User Guide
- Veeam Cloud Connect Infrastructure in the Veeam Cloud Connect User Guide
Planning and Preparation

Before you start using the Integration with Veeam Backup Repositories 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 Integration with Veeam Backup Repositories for Kasten K10, mind the following:

Kubernetes Distribution Requirements

Integration with Veeam Backup Repositories for Kasten K10 supports only backup exports of Kubernetes persistent volumes provisioned using vSphere CSI driver.

Kasten K10 Cluster Version

A K10 cluster from which you want to export backups to Veeam backup repositories must be the 4.5.6 version or later.

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.
Used Ports

Veeam Backup & Replication within the Integration with Veeam Backup Repositories 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, Integration with Veeam Backup Repositories 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.

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Protocol</th>
<th>Port</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>K10 cluster</td>
<td>Veeam Backup &amp; Replication server</td>
<td>TCP</td>
<td>10006</td>
<td>Port used to connect to the Veeam Backup &amp; Replication server.</td>
</tr>
<tr>
<td>VBR RestAPI Service</td>
<td>TCP</td>
<td>HTTPS</td>
<td>9419</td>
<td>Port used to validate Veeam Backup &amp; Replication Location Profile.</td>
</tr>
<tr>
<td>Veeam backup repository</td>
<td>TCP</td>
<td>2500 to 3300</td>
<td></td>
<td>Default range of ports used as data transmission channels. For every TCP connection that a job uses, one port from this range is assigned.</td>
</tr>
</tbody>
</table>
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 when installing and working with 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 Integration with Veeam Backup Repositories for Kasten K10 solution, you must have the following types of product editions installed:

- Veeam Backup & Replication server requires Enterprise Plus product edition. For more information, see Veeam Licensing Policy.

- K10 cluster 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 Integration with Veeam Backup Repositories for Kasten K10 solution, you must configure the K10 cluster and the Veeam Backup & Replication infrastructure.

Configure K10 Cluster Infrastructure

K10 cluster is a source environment that creates snapshots of applications running on Kubernetes persistent volumes. After that, K10 makes exports of snapshot data and moves it to the Veeam backup repositories where this data is stored in a native Veeam format. The K10 cluster that you plan to use in the Integration with Veeam Backup Repositories for Kasten K10 infrastructure must meet the system requirements. For more information on configuring a K10 cluster, see Kasten Docs.

Configure Veeam Backup & Replication Infrastructure

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

1. **Install or upgrade Veeam Backup & Replication.**
   After you install Veeam Backup & Replication, Integration with Veeam Backup Repositories for Kasten K10 component will be automatically installed along with Veeam Backup & Replication. If you are going to upgrade or update your Veeam Backup & Replication version, make sure you install the cumulative patch P20211211. For more information, see the Installing Veeam Backup & Replication, Upgrading to Veeam Backup & Replication 11 or 11a, Updating Veeam Backup & Replication 11 or 11a sections in the Veeam Backup & Replication User Guide.

2. **Deploy Veeam backup repositories.**
   Add the Veeam backup repositories that will store backups exported by K10 policies to the 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.

3. **[Optional] Configure archive tier.**
   Configure archive tier to set an additional layer of storage. For more information, see the Archive Tier section in the Veeam Backup & Replication User Guide.

4. **[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.

5. **[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 cluster and Veeam Backup & Replication infrastructure, K10 will be able to connect to a Veeam backup repository using the VMB API functionality and you are ready to create K10 policies.
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, you can view the backed-up applications, check statistics on K10 policies and remove these policies from the 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 Mover 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 web console associated with your K10 cluster.

To create a K10 policy, open the K10 web console 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 web console, 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 and started the K10 policy, it appears in the Veeam Backup & Replication infrastructure.

**IMPORTANT**

The Veeam Backup & Replication console does not display a number of applications backed-up by K10 policies.
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 web console, 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 the Veeam Backup & Replication infrastructure under the **Backups > Disk (VeeamZip)** node.
Removing K10 Policies

Integration with Veeam Backup Repositories for Kasten K10 allows you to permanently delete K10 policies from the Veeam Backup & Replication infrastructure. Note that this operation does not affect the same policy in K10 web console.

To delete a K10 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 K10 policy and click Delete on the ribbon. Alternatively, right-click the necessary backup policy and select Delete.

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.

TIP

If you delete a K10 policy from the Veeam Backup & Replication infrastructure and then run the same K10 from the K10 web console, this policy will be auto mapped and will appear in the Veeam Backup & Replication console again. Backups associated with this policy will be displayed under the Backups > Disk node.
Managing Backed-Up Data

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

- View Backup Properties
- Delete Backups
Viewing Backup Properties

In the 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

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.
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

Integration with Veeam Backup Repositories for Kasten K10 allows you to permanently delete backups exported by K10 policies or manually from the Veeam Backup & Replication infrastructure in one of the following ways:

- Remove backups from configuration
- Delete backups from disk

Removing from Configuration

If you want to remove records about backups from the Veeam Backup & Replication infrastructure and configuration database, you can use the Remove from configuration operation. When you remove a backup from the configuration, the backup files (VBK and VBM) remain in the Veeam backup repository. You can import the backup later and restore application data and folders from it.

To remove a backup from the configuration:

1. Open the Home view.
2. In the inventory pane, select Backups.
3. In the working area, select the backup and click Remove from > Configuration on the ribbon. Alternatively, right-click the backup and select Remove from configuration.

Deleting Backups from Disk

If you want to remove records about backups from both the 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, Integration with Veeam Backup Repositories 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 the 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.
## 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. For more information on the backup copy functionality, see the [Backup Copy](#) section in the Veeam Backup & Replication User Guide.

To create a backup copy job, do the following:


2. On the **Home** tab, click **Backup Copy** and select K10 backup.

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

After K10 exports application disks to backup repositories, 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 the Reporting section in the Veeam Backup & Replication User Guide.
Data Recovery

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

- **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**
Integration with Veeam Backup Repositories 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 the K10 recovery options. For more information, see Kasten Docs.
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**

Mind the following:

- Integration with Veeam Backup Repositories for Kasten K10 supports only restore from Linux, Unix and other non-Microsoft Windows OSes.
- Integration with Veeam Backup Repositories 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.

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 (VeeamZip) node.
Viewing Statistics

Integration with Veeam Backup Repositories for Kasten K10 allows you to view statistics on data recovery operations that Veeam Backup & Replication performs with backups exported from K10. 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 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 Export Logs section in the Veeam Backup & Replication User Guide.

IMPORTANT
In the Export Logs wizard, you cannot export logs for separate K10 policies and backup files.