Veeam Backup & Replication for Nutanix Mine

Version 12

User Guide

February, 2023

> **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 4

ABOUT THIS DOCUMENT 5

WELCOME TO MINE WITH VEEAM 6

ARCHITECTURE OVERVIEW 7

PLANNING AND PREPARATION 9

- System Requirements 9
- Limitations and Considerations 10
- Ports 11
- Licensing 11

DEPLOYMENT 12

- Accessing Mine Console 12
- Installing Mine with Veeam 14
- Upgrading to Mine with Veeam 3.0 15
  - Installing Veeam Data Mover Service 16
- Expanding Mine with Veeam 17
  - Adding Backup Proxies 17
  - Extending Scale-Out Backup Repository 18
  - Adding Backup Repositories 19
- Updating Backup Server 20

PROTECTING WORKLOADS 21

- Accessing Veeam Backup & Replication Console 21
- Protecting VMware VMs 24
- Protecting Hyper-V VMs 25
- Protecting Nutanix AHV VMs 26
- Protecting Physical Machines 27
- Protecting File Shares 28
- Protecting Microsoft Azure Workloads 29
- Protecting AWS Workloads 30
- Protecting Google Cloud VM Instances 31

REVIEWING MINE WITH VEEAM DASHBOARD 32

- Veeam Backup & Replication Events 34

Contacting Veeam Software

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

Customer Support

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

Company Contacts

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

Online Support

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

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

About This Document

This guide is designed for IT professionals who plan to use Nutanix Mine with Veeam. It is primarily aimed at administrators who want to automate data protection operations in their physical, virtual and cloud environments. The guide includes system requirements, important integration limitations, licensing information and high-level deployment instructions.

Nutanix Mine with Veeam is built on top of Veeam Backup & Replication and Nutanix Mine, and this guide assumes that you have a good understanding of these solutions.

Welcome to Mine with Veeam

Nutanix Mine with Veeam (Mine with Veeam) is a comprehensive scalable backup solution that was designed collaboratively by Nutanix and Veeam for protection and disaster recovery tasks in various environments. The solution integrates the Nutanix Hyperconverged Infrastructure technology and the Veeam Backup & Replication software to simplify the full lifecycle of data protection operations.

Mine with Veeam is deployed as a dedicated cluster on a Mine appliance (Mine with Veeam cluster) with a set of preconfigured backup infrastructure components, which allows you to eliminate error-prone manual steps and reduce time spent while installing and configuring Veeam Backup & Replication. With Mine with Veeam, you can back up and restore the following objects:

- Virtual machines (Nutanix AHV VMs, VMware vSphere VMs, Microsoft Hyper-V VMs)
- Cloud virtual workloads (Amazon EC2, Amazon RDS instances, Amazon EFS file systems and VPC configurations, Microsoft Azure VMs and SQL databases, Google Cloud VM instances)
- Physical machines (Microsoft Windows, macOS, Linux, Unix IBM AIX and Oracle Solaris)
- File shares (Windows-managed or Linux-managed servers, enterprise NAS systems, NFS file shares, SMB file shares)

> NOTE
>
> Mine with Veeam version 3.0 comes with Veeam Backup & Replication version 11a. However, Veeam Backup & Replication version 12 is also fully supported. You can either upgrade to version 12 manually, or use version 11a. In the latter case, see Veeam Backup & Replication 11 for Nutanix Mine Guide.

Architecture Overview

The Mine with Veeam architecture comprises the following set of components:

- Foundation for Mine with Veeam server
- Backup server
- Backup proxies
- Backup repositories

Foundation for Mine with Veeam Server

The Foundation for Mine with Veeam server (foundation server) is the core component of the solution that deploys a backup server, backup proxies and repositories. The foundation server provides the Mine console that allows you to configure Mine with Veeam settings and troubleshoot issues with the Mine with Veeam cluster.

> IMPORTANT
>
> After the foundation server deploys all the components of Mine with Veeam, do not remove the server because it also establishes communication between the backup server and the Mine with Veeam cluster.

Backup Server

The backup server is a Windows-based machine on which Veeam Backup & Replication is installed. The backup server is the configuration, administration and management component of the backup infrastructure. It coordinates backup, replication, recovery verification and restore tasks, controls job scheduling and manages resource allocation. For more information on the backup server, its services and components, see the Veeam Backup & Replication User Guide, section Backup Server.

Mine with Veeam supports 2 deployment scenarios:

- A new backup server is deployed as a part of the Mine with Veeam cluster.
- An existing backup server is connected to the Mine with Veeam cluster — in this case, the backup server is not included in the cluster.

  This scenario is recommended, for example, if you want to deploy Mine with Veeam as a secondary storage solution and to manage all backup jobs from a single Veeam Backup & Replication console.

Backup Proxies

A backup proxy is an architecture component that sits logically between the backup server and other components of the backup infrastructure. While the backup server administers tasks, the proxy processes jobs and delivers backup traffic. For more information on backup proxies, their transport modes, services and components, see the Veeam Backup & Replication User Guide, section Backup Proxy.

The foundation server automatically deploys a number of backup proxies on Windows VMs in your cluster — the number of proxies depends on the size of the Mine with Veeam cluster:

- If the cluster contains less than 8 nodes, 2 backup proxies are deployed.
- If the cluster contains 8 nodes or more, 5 backup proxies are deployed.

Depending on the deployment scenario you choose, the backup server can act as a backup proxy. If the server is deployed as a part of the Mine with Veeam cluster, it is automatically assigned the role of a proxy. If an existing server is connected to the Mine with Veeam cluster, the foundation server deploys an additional standalone proxy because the connected backup server cannot function as a proxy due to technical limitations.

Backup Repositories

A backup repository is an architecture component where backups are stored. Backup repositories can be either configured as dedicated repositories or combined into a single scale-out backup repository — a multi-tier repository system that provides a convenient way of managing and extending the backup storage. For more information on backup repositories and their types, see the Veeam Backup & Replication User Guide, section Backup Repository.

The foundation server automatically deploys a number of backup repositories on Windows VMs in your cluster — the number of repositories depends on the size of the Mine with Veeam cluster:

- If the cluster contains less than 8 nodes, 3 Linux repositories are deployed.
- If the cluster contains 8 nodes or more, 6 Linux repositories are deployed.

The backup repositories in the Mine with Veeam cluster are automatically added as extents of the performance tier to a scale-out backup repository. If the backup repositories run out of free space, you can extend the scale-out backup repository as described in section Expanding Mine with Veeam.

Planning and Preparation

Before you start installing Mine with Veeam, check system requirements, network ports used for data transmission and limitations that must be met to ensure that the solution functions properly.

System Requirements

The Mine appliance where the Mine with Veeam cluster will be deployed must meet the following hardware requirements.

Specification	Requirement
Minimum number of nodes	4
Processor per node	2 x Intel Xeon Silver 4214 (12-core 2.2 GHz) or higher
RAM per node	192 GB or more
SSD per node	2
HDD per node	4

The cluster logical storage capacity is automatically configured depending on the physical capacity of cluster nodes:

Logical Storage Capacity	Node Physical Capacity
1.125 PB	less than 64 TB
2.25 PB	more than 64 TB and less than 120 TB
3.375 PB	120 TB and more

> IMPORTANT
>
> Before deploying Mine with Veeam, you can open a support case to ask for a custom configuration of the cluster logical storage capacity.

The number of nodes defines the number of backup proxies and repositories that the foundation server deploys in the Mine with Veeam cluster. For more information, see Architecture Overview.

To expand a deployed Mine with Veeam cluster, you can install 2-node blocks. However, this will not change the number of proxies and repositories in the cluster. For more information, see Expanding Mine with Veeam.

Limitations and Considerations

When you plan to deploy and configure Mine with Veeam, consider the following limitations and considerations.

Backup Server

Depending on the deployment scenario you choose, the backup server can be a part of the Mine with Veeam cluster, and then no additional configuration actions are needed. However, if you are willing to connect an existing backup server to Mine with Veeam, consider the following requirements before deploying Mine with Veeam:

- Only the Enterprise and Enterprise Plus Editions of Veeam Backup & Replication are supported.
- Only Veeam Backup & Replication version 12 or later is supported.
- The backup server and the Mine with Veeam cluster must be connected to the same network.
- The Windows Remote Management service must be enabled on the backup server. The foundation server uses this service to establish the connection between the backup server and the Mine with Veeam cluster. To learn how to enable the service, see Microsoft docs.

Backup Repositories

When you deploy Mine with Veeam, the foundation server automatically deploys a number of backup repositories that are added as extents of the performance tier into a single scale-out backup repository. That is why you must take into account the following considerations:

- You must not deploy new VMs in the cluster and assign the role of a repository to them.
- You must not change the configuration settings of VMs deployed with the role of a repository.
- You must not disconnect or reconnect the backup repositories added to the backup infrastructure during cluster deployment.
- You must not edit settings of the backup repositories added to the backup infrastructure during cluster deployment.
- You must not add or remove performance extents included into the scale-out backup repository.

If you need to make any changes to the default backup infrastructure, open a support case.

> **IMPORTANT**
>
> When the amount of free space available on the backup repositories drops below a critical value, Veeam Backup & Replication automatically switches all extents of the performance tier in the scale-out backup repository to the seal mode, which means that no further data is saved to the repositories and only read operations are allowed. For more information on limitations that apply in the seal mode, see the Veeam Backup & Replication User Guide, section Switching to Seal Mode.

Backup Proxies

When you deploy Mine with Veeam, the foundation server automatically deploys a number of backup proxies that are already preconfigured for optimal performance. That is why you must take into account the following considerations:

- You must not deploy new VMs in the cluster and assign the role of a proxy to them.
- You must not change the configuration settings of VMs deployed with the role of a proxy.
- You must not reconfigure, disconnect or reconnect the backup proxies added to the backup infrastructure during cluster deployment.

If you need to make any changes to the default backup infrastructure, open a support case.

Ports

Mine with Veeam uses specific ports to allow communication between the solution components. Depending on the deployment scenario you choose, additional configuration actions may be required. If the backup server is deployed as a part of the Mine with Veeam cluster, the necessary ports are opened automatically. If an existing backup server is connected to the cluster, you must open the following ports manually:

From	To	Protocol	Port	Notes
Backup server	Foundation server	TCP	8743	Used by the backup server to connect to the foundation server.
Foundation server	Backup server	TCP	5985	Used by the foundation server to connect to the backup server.

Licensing

In the Mine with Veeam solution, Veeam Backup & Replication is licensed by the number of instances. Instances are units that you can use to protect any workloads: virtual, physical and cloud-based. For more information on Veeam Backup & Replication licensing, see Veeam Licensing Policy.

Workloads that have been processed during the past 31 days are considered to be protected. Protected workloads consume instances from the license scope that comes with the Mine with Veeam solution. The number of licenses included into the scope depends on the Mine appliance specification. For more information, see Nutanix Mine Software Documentation.

Veeam Backup & Replication keeps track of instances consumed by protected workloads. When the number of consumed instances exceeds the license limit, you get a warning in the Veeam Backup & Replication console. For more information, see Exceeding License Limit.

Deployment

To deploy the Mine with Veeam cluster, perform the following steps:

1. Install a Mine appliance. For more information, see Nutanix Mine Software Documentation.
2. Create an AHV cluster. For more information, see in Nutanix Mine Software Documentation.
3. Install Mine with Veeam.

After you deploy the Mine with Veeam cluster, you will be able to perform the following operations:

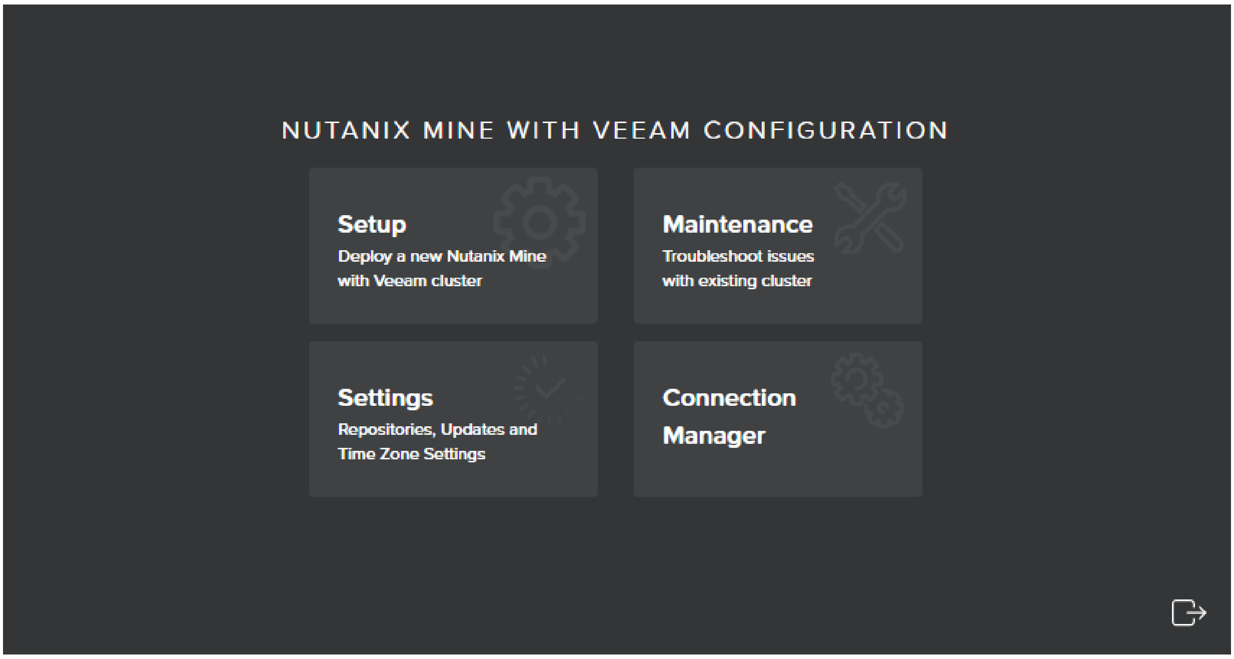
- Manage data protection and disaster recovery tasks. For more information, see Protecting Workloads.
- Monitor backup and restore job statuses, events and alerts. For more information, see Reviewing Mine with Veeam Dashboard.
- Configure, maintain and upgrade the Mine with Veeam cluster. For more information, see Accessing Mine Console.

Accessing Mine Console

The Mine console allows you to configure, maintain and upgrade the Mine with Veeam cluster. To access the Mine console, do the following:

1. In a web browser, navigate to the IP address of the foundation server.
2. In the **username** and **password** fields, enter credentials of a user account with administrative privileges that you specified while deploying the foundation server, and press [Enter] on the keyboard.

To learn how to manage the Mine with Veeam cluster, see Nutanix Mine Software Documentation.


NUTANIX MINE WITH VEEAM CONFIGURATION
Setup
Deploy a new Nutanix Mine with Veeam cluster
Maintenance
Troubleshoot issues with existing cluster
Settings
Repositories, Updates and Time Zone Settings
Connection Manager

To change the password you use to access the Mine console, do the following:

1. In a web browser, navigate to the virtual IP address of the cluster. You can also use the IP address or the hostname of a Controller VM in the cluster.

2. In the **username** and **password** fields, enter credentials of a user account with Prism Element administrative privileges, and press [Enter] on the keyboard.
3. From the main navigation menu, select **VM**.
4. Click **Table** to see the list of VMs residing on the Mine cluster.
5. Right-click the foundation server VM and select **Launch Console**.
6. In the console window, enter credentials of the user account that you use to access the Mine console.

> TIP
>
> If you cannot remember the password, you can reset it as described in the knowledge base article.

7. Run the following command:

   ```
   sudo passwd <username>
   ```

   where <`username`> is the user name that you use to access the Mine console.
8. Enter the currently used password, specify and confirm a new password.
9. In the Prism Element console, right-click the foundation server VM and select **Power Off Actions**.
10. Select **Guest Reboot** and click **Submit** to reboot the foundation server.

Installing Mine with Veeam

To install Mine with Veeam, do the following:

1. Log in to the Mine console. For more information, see Accessing Mine Web Console.
2. Click **Setup** to launch the Nutanix Mine with Veeam setup wizard.
3. Complete the Nutanix Mine with Veeam cluster setup wizard. For more information, see Nutanix Mine Software Documentation.

As soon as you complete the setup wizard, the foundation server starts deploying the backup infrastructure components. Note that it may take up to 3 hours for the deployment process to complete.

Related Topic

Updating Backup Server

Upgrading to Mine with Veeam 3.0

Upgrade to Mine with Veeam version 3.0 is supported from Mine with Veeam versions 2.0 and 1.0.

To learn how to upgrade Mine with Veeam 1.0 to 3.0, see Nutanix Mine Software Documentation. To upgrade Mine with Veeam 2.0, do the following:

1. Log in to the Mine console. For more information, see Accessing Mine Console.
2. Ensure that credentials used to allow communication between Mine with Veeam components are valid:
   a. Click **Credential manager**.
   b. On the **Credential Manager** page, check the statuses of the credentials of the Mine with Veeam components. If any credentials are invalid, update them as described in Nutanix Mine Software Documentation.
3. Click **Check Updates**.
4. On the **Updates** page, click **Check updates**.

   If Mine with Veeam detects available updates, click **Start update**.

After you upgrade Mine with Veeam to version 3.0, you may need to perform additional configuration actions:

- Install the Veeam Data Mover service on all Mine with Veeam backup repositories to disable SSH access to the repositories.
- Open a support case to increase the total disk capacity of the backup server.

  Starting from version 3.0, Mine with Veeam supports replication operations. Since these operations require replica metadata to be stored on the backup server, the total disk capacity of the backup server must be increased to 400 GB.

Related Topic

Updating Backup Server

Installing Veeam Data Mover Service

The Veeam Data Mover service performs data processing tasks on behalf of Veeam Backup & Replication, such as retrieving source machine data, performing data deduplication and compression, and storing backed-up data on the target storage. Starting from version 3.0, you can install the Veeam Data Mover service on Mine with Veeam repositories to enable certificate-based authentication. This allows Veeam Backup & Replication to disable SSH access to the repositories and, therefore, to improve the security of the solution. For more information, see the Veeam Backup & Replication User Guide, section Veeam Data Movers.

> IMPORTANT
>
> Before you install Veeam Data Mover on a repository, you must stop all running Veeam Backup & Replication jobs to prevent unexpected data loss and backup operation failures.

To install the Veeam Data Mover service on a repository, do the following:

1. Log in to the Mine console. For more information, see Accessing Mine Console.
2. Click **Settings**.
3. On the **Repositories** tab of the **Settings** page, click **Install** next to the necessary repository.

If you install the Veeam Data Mover service on one repository, you must also install it on all other repositories displayed in the **Repositories** list. Otherwise, you may encounter unpredictable data transfer issues.

> TIP
>
> If the Veeam Data Mover service is already installed on a repository, the **Install** button will be replaced with the **Update** button that allows you to check whether any updates with bug fixes and improvements for the service are available. After you click the **Update** button, Veeam Backup & Replication will rescan the repository and update the Veeam Data Mover service if necessary.

After you install the Veeam Data Mover service on a repository, credentials that are used to access the repository may appear in the Veeam Backup & Replication console twice. To remove a duplicate record, do the following:

1. Log in to the Veeam Backup & Replication console. For more information, see Accessing Veeam Backup & Replication Console.
2. Select **Manage Credentials** from the main menu.
3. In the list of the accounts added to Veeam Backup & Replication, find a pair of backup repository accounts with the same **Account**, **Type** and **Description** properties.
4. Select the record with an earlier **Last edited** date and click **Remove**.

Expanding Mine with Veeam

By default, the foundation server deploys a number of backup proxies and repositories that depends on the size of the Mine with Veeam cluster. This defines how many backup jobs can be processed simultaneously and how much space is available for backups. If the default backup infrastructure does not provide enough resources to protect your workloads, you can do the following:

- Add new backup proxies
- Extend the existing scale-out backup repository
- Add new backup repositories

Adding Backup Proxies

Backup proxies perform various backup tasks, such as retrieving data from the production storage, compressing, deduplicating, encrypting, sending data to backup repositories and other backup proxies. In large deployments, the default number of backup proxies deployed in the Mine with Veeam cluster may not be enough to process data of the protected workloads.

To optimize backup performance and to avoid high traffic load on the deployed proxies, you can do the following:

- Deploy an additional Mine with Veeam cluster and connect the existing backup server to the new cluster. Backup proxies deployed in this cluster will be automatically added to the backup infrastructure.
- Deploy a physical server or a virtual machine outside the Mine with Veeam cluster, add it in the Veeam Backup & Replication console and assign the role of a proxy to it. In Veeam Backup & Replication, you can add the following types of proxies:
  - File share backup proxies. For more information, see the Veeam Backup & Replication User Guide, section NAS Backup Support.
  - VMware backup proxies. For more information, see the Veeam Backup & Replication User Guide, section Adding VMware Backup Proxies.
  - VMware CDP backup proxies. For more information, see the Veeam Backup & Replication User Guide, section Adding VMware CDP Proxies.

Related Topics

- Architecture Overview
- System Requirements
- Limitations and Considerations

Extending Scale-Out Backup Repository

All backup repositories deployed in the Mine with Veeam cluster are added as extents of the performance tier to a scale-out backup repository — a multi-tier repository system with horizontal scaling support. If the performance extents of the scale-out backup repository run out of free space, you can do the following:

- Extend the performance tier of the scale-out backup repository
- Add the capacity tier to the scale-out backup repository
- Add the archive tier to the scale-out backup repository

Extending Performance Tier

Performance tier of a scale-out backup repository is used to store backed-up data that you need to access frequently. The performance tier comprises one or more performance extents. In Mine with Veeam, performance extents are backup repositories deployed in the cluster.

To extend the performance tier, add an expansion block to the Mine with Veeam cluster — this will automatically increase the space available on all backup repositories. To learn how to add an expansion block, see Nutanix Mine Software Documentation.

Adding Capacity Tier

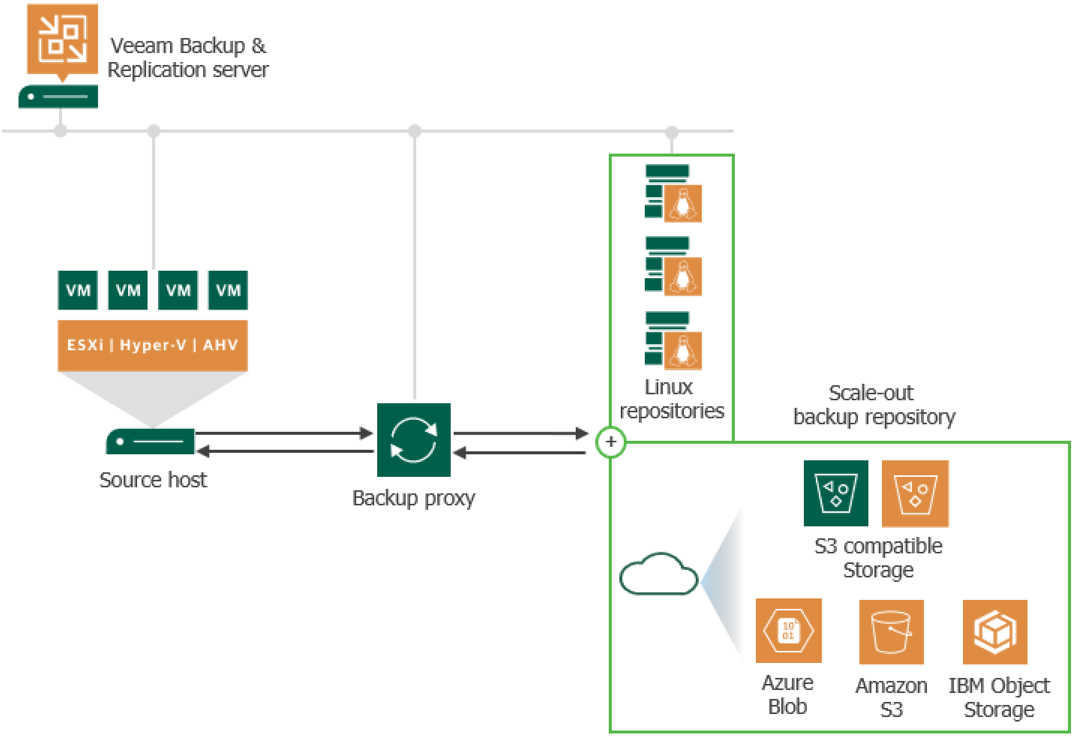
The capacity tier of a scale-out backup repository is used to store backed-up data that you need to access rarely; typically, this is the data from the performance extents that is transported to the capacity tier for long-term storage. The capacity tier consists of a single capacity extent that can be either a cloud-based object storage repository or an on-premises object storage repository (S3-compatible object storage repository, Amazon S3, Microsoft Azure Blob Storage and so on). For more information, see the Veeam Backup & Replication User Guide, section Capacity Tier.

To extend the scale-out backup repository with the capacity tier, add a supported object storage repository to the backup infrastructure and update the scale-out backup repository configuration as described in the Veeam Backup & Replication User Guide, section Adding Scale-Out Backup Repositories.

Adding Archive Tier

The archive tier of a scale-out backup repository is used to store archived data that you need to access infrequently (no more than once a quarter); typically, this is the data from the capacity extent that is transported to the archive tier to optimize the cost of storing backups. The archive tier consists of a single archive extent that is a cloud-based object storage repository (Amazon S3 Glacier or Microsoft Azure Archive Storage). For more information, see the Veeam Backup & Replication User Guide, section Archive Tier.

To extend the scale-out backup repository with the archive tier, add a supported object storage repository to the backup infrastructure and update the scale-out backup repository configuration as described in the Veeam Backup & Replication User Guide, section Adding Scale-Out Backup Repositories.



Adding Backup Repositories

Backup repositories store various types of backup data, such as VM backup files, VM copies, metadata for replicated VMs, configuration backups and so on. In Mine with Veeam, backup repositories are combined into a single scale-out backup repository that has a number of limitations. In large deployments, the default backup repositories deployed in the Mine with Veeam cluster may provide not enough free space to back up all workloads you need to protect. To increase the space available for backup data, you can either extend the existing scale-out backup repository or add more repositories.

To add a repository, you can do the following:

- Deploy a physical server or a virtual machine outside the Mine with Veeam cluster, add it to the backup infrastructure and assign the role of a repository to it. Note that you must not include new repositories into the existing scale-out backup repository.

  To learn how to add repositories to the backup infrastructure, see the Veeam Backup & Replication User Guide, section Adding Backup Repositories.

- Deploy an additional Mine with Veeam cluster and connect the existing backup server to the new cluster. Backup repositories automatically deployed in this cluster will be combined into a new scale-out repository and added to the backup infrastructure.

Related Topics

- Architecture Overview
- System Requirements
- Limitations and Considerations

Updating Backup Server

Veeam Backup & Replication automatically notifies you about updates that can be installed to avoid performance issues while working with the product. When a new Veeam Backup & Replication version is published on the Veeam update server, you will get a notification in the Windows Action Center. To install the update, double-click the notification — Veeam Backup & Replication will open a KB article with the update description and a list of installation links.

> IMPORTANT
>
> After you update the backup server, you must install or update the Veeam Data Mover service on all Mine with Veeam repositories, as described in section Installing Veeam Data Mover Service.

Protecting Workloads

After you deploy Mine with Veeam, you can access the Veeam Backup & Replication console to administer backup, restore and replication operations for the following virtual, physical and cloud workloads:

- VMware VMs
- Hyper-V VMs
- Nutanix AHV VMs
- Physical machines
- File shares
- Microsoft Azure VMs and Azure SQL databases
- Amazon EC2 instances, RDS instances, EFS file systems and VPC configurations
- Google Cloud VM instances

Accessing Veeam Backup & Replication Console

You can access the Veeam Backup & Replication console using one of the following options:

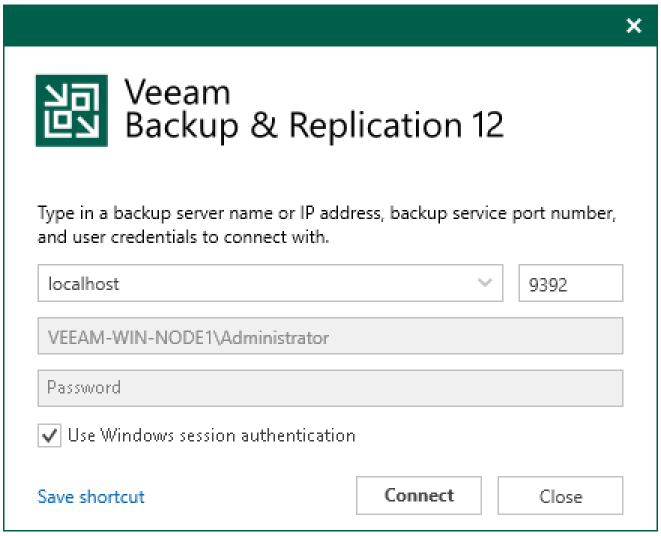
- Connect to the backup server where the console is installed using Prism.
- Connect to the backup server where the console is installed using remote desktop connection.
- Connect to the backup server using a local instance of the console installed on your workstation.

Accessing Veeam Backup & Replication Console Using Prism

To access the Veeam Backup & Replication console using Prism, do the following:

1. Log in to the Prism web console and navigate to the Mine with Veeam dashboard. For more information, see Viewing Mine with Veeam Dashboard.
2. In the **Cluster** widget, click **Launch Console**.
3. Log in to the VM where Veeam Backup & Replication is installed:
    a. In the upper right corner of the welcome screen, click the **Send CtrlAltDel** icon.
    b. In the **password** field, enter the password of the local Windows Administrator that you specified while deploying the Mine with Veeam cluster, and press [Enter] on the keyboard.
4. Open the Veeam Backup & Replication console using one of the following options:
    - Double-click the console icon on the desktop.
    - From the Microsoft Windows **Start** menu, select **All Programs** > **Veeam** > **Veeam Backup & Replication Console**.
    - Use Microsoft Windows Search to find and launch **Veeam Backup & Replication Console**.

5. In the Veeam Backup & Replication console login window, select the **Use Windows session authentication** check box and click **Connect**.



Type in a backup server name or IP address, backup service port number, and user credentials to connect with.

localhost | 9392

VEEAM-WIN-NODE1\Administrator

Password

☑ Use Windows session authentication

Accessing Veeam Backup & Replication Console Using Remote Connection

To access the Veeam Backup & Replication console using remote connection, do the following:

1. Use a remote desktop application to connect to the backup server where the Veeam Backup & Replication console is installed. To do this, enter the IP address of the backup server and credentials of the local Windows Administrator that you specified while deploying the Mine with Veeam cluster.

> **TIP**
>
> You can check the IP address of the Veeam Backup & Replication server on the **Settings** screen in the Mine console.

2. Open the Veeam Backup & Replication console using one of the following options:
   - Double-click the console icon on the desktop.
   - From the Microsoft Windows **Start** menu, select **All Programs** > **Veeam** > **Veeam Backup & Replication Console**.
   - Use Microsoft Windows Search to find and launch **Veeam Backup & Replication Console**.
3. In the Veeam Backup & Replication console login window, select the **Use Windows session authentication** check box and click **Connect**.

Accessing Veeam Backup & Replication Using Remote Console

To access Veeam Backup & Replication using a remote console, first install the Veeam Backup & Replication console version 12 on your workstation as described in the Veeam Backup & Replication User Guide, section Installing Veeam Backup & Replication Console.

To log in to the Veeam Backup & Replication console, do the following:

1. Open the console using one of the following options:
   - Double-click the console icon on the desktop.

- From the Microsoft Windows **Start** menu, select **All Programs** > **Veeam** > **Veeam Backup & Replication Console**.
- Use Microsoft Windows Search to find and launch **Veeam Backup & Replication Console**.

2. In the Veeam Backup & Replication console login window, do the following:

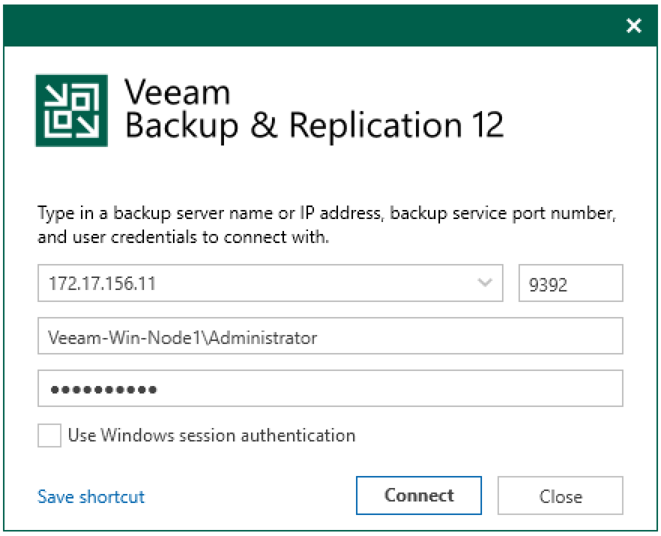
   a. In the **Server** field, enter the IP address of the backup server.

> TIP
>
> You can check the IP address of the backup server on the **Settings** screen in the Mine console.

   b. In the **Port** field, enter the port to connect to the backup server (by default, port **9392)**.

   c. In the **Username** and **Password** fields, enter credentials of the local Windows Administrator that you specified while deploying the Mine with Veeam cluster.

   d. Click **Connect**.



Type in a backup server name or IP address, backup service port number, and user credentials to connect with.

172.17.156.11 | 9392

Veeam-Win-Node1\Administrator

••••••••••

□ Use Windows session authentication

Protecting VMware VMs

To back up a VMware VM using Mine with Veeam, perform the following steps:

1. Add to the backup infrastructure a vCenter Server or an ESXi host that manages the VM. For more information, see the Veeam Backup & Replication User Guide for VMware vSphere, section Adding VMware vSphere Servers.

2. Create a backup job to create restore points for the VM. For more information, see the Veeam Backup & Replication User Guide for VMware vSphere, section Creating Backup Jobs.

   Once the backup job successfully creates a restore point for the VM, you can use the restore the entire VM, its disks, files and application items. For more information, see the Veeam Backup & Replication User Guide for VMware vSphere, section Restore.

After you add a vCenter Server or an ESXi host to the backup infrastructure, you can perform the following operations to protect its workloads:

- Create exact copies of VMware VMs and maintain the copies in sync with the original VMs to be able to switch to the VM replicas in case a disaster strikes. For more information, see the Veeam Backup & Replication User Guide for VMware vSphere, section Replication.

- Test VM backups and replicas to check whether you will be able to use them for recovery operations. For more information, see the Veeam Backup & Replication User Guide for VMware vSphere, section Recovery Verification.

- Configure CDP policies for mission-critical VMs to be able to switch to the VM replicas immediately. For more information, see the Veeam Backup & Replication User Guide for VMware vSphere, section Continuous Data Protection (CDP).

- Copy backup files to secondary repositories to be able to protect your data against disasters and virtual or physical machine failures. For more information, see the Veeam Backup & Replication User Guide for VMware vSphere, section Backup Copy.

- Store copies of backup files on tapes to ensure the data is not accidentally deleted or changed. For more information, see the Veeam Backup & Replication User Guide for VMware vSphere, section Tape Devices Support.

For the complete list of features that Veeam Backup & Replication provides to protect VMware VMs, see the Veeam Backup & Replication User Guide for VMware vSphere.

Protecting Hyper-V VMs

To back up a Hyper-V VM using Mine with Veeam, perform the following steps:

1. Add to the backup infrastructure a Hyper-V host that manages the VM. For more information, see the Quick Start Guide for Microsoft Hyper-V, section Adding Microsoft Hyper-V Servers.
2. Create a backup job to create restore points for the VM. For more information, see the Veeam Backup & Replication User Guide for Microsoft Hyper-V, section Creating Backup Jobs.

   Once the backup job successfully creates a restore point for the VM, you can use the restore point to restore the entire VM, its disks, files and application items. For more information, see the Veeam Backup & Replication User Guide for Microsoft Hyper-V, section Data Recovery.

After you add a Hyper-V host to the backup infrastructure, you can perform the following operations to protect its workloads:

- Create exact copies of Hyper-V VMs and maintain the copies in sync with the original VMs to be able to switch to the VM replicas in case a disaster strikes. For more information, see the Veeam Backup & Replication User Guide for Microsoft Hyper-V, section Replication.
- Test VM backups and replicas to check whether you will be able to use them for recovery operations. For more information, see the Veeam Backup & Replication User Guide for Microsoft Hyper-V, section Recovery Verification.
- Copy backup files to secondary repositories to be able to protect your data against disasters and virtual or physical machine failures. For more information, see the Veeam Backup & Replication User Guide for Microsoft Hyper-V, section Backup Copy.
- Store copies of backup files on tapes to ensure the data is not accidentally deleted or changed. For more information, see the Veeam Backup & Replication User Guide for Microsoft Hyper-V, section Tape Devices Support.
- Restore items of applications such as Microsoft Active Directory, Microsoft Exchange, Microsoft SharePoint, Microsoft SQL Server and Oracle Database. For more information, see the Veeam Backup & Replication User Guide for Microsoft Hyper-V, section Application Item Restore.

For the complete list of features that Veeam Backup & Replication provides to protect Hyper-V VMs, see the Veeam Backup & Replication User Guide for Microsoft Hyper-V.

Protecting Nutanix AHV VMs

To back up a Nutanix AHV VM using Mine with Veeam, perform the following steps:

1. [This step applies only if you have connected an existing backup server while deploying Mine with Veeam]

   Install Nutanix AHV Plug-in. For more information, see the Veeam Backup for Nutanix AHV User Guide, section Installing Nutanix AHV Plug-In.

2. Add to the backup infrastructure the Nutanix AHV cluster where the VM is deployed. For more information, see the Veeam Backup for Nutanix AHV User Guide, section Adding Nutanix AHV Cluster.

3. Deploy an AHV backup proxy in the Nutanix AHV cluster and add it to the backup infrastructure. For more information, see the Veeam Backup for Nutanix AHV User Guide, section Deploying New Backup Appliance.

4. Create a backup job to create restore points for the VM. For more information, see the Veeam Backup for Nutanix AHV User Guide, section Creating Backup Jobs.

Once the backup job successfully creates a restore point for the VM, you can perform the following operations to restore the VM:

- Restore the entire VM to an AHV cluster. For more information, see the Veeam Backup for Nutanix AHV User Guide, section Performing VM Restore.

- Immediately restore the VM directly from compressed and deduplicated backup files to Nutanix AHV, VMware vSphere and Hyper-V environments. For more information, see the Veeam Backup for Nutanix AHV User Guide, section Instant Recovery.

- Restore the VM to Microsoft Azure. For more information, see Veeam Backup for Nutanix AHV User Guide, section Restore to Microsoft Azure.

- Restore the VM to Amazon EC2. For more information, see the Veeam Backup for Nutanix AHV User Guide, section Restore to Amazon EC2.

- Restore the VM to Google Cloud. For more information, see the Veeam Backup for Nutanix AHV User Guide, section Restore to Google CE.

- Restore items of applications such as Microsoft Active Directory, Microsoft Exchange, Microsoft SharePoint, Microsoft SQL Server and Oracle Database. For more information, see the Veeam Backup for Nutanix AHV User Guide, section Performing Application Items Restore.

For the complete list of features that Veeam Backup & Replication provides to protect Nutanix AHV VMs, see the Veeam Backup for Nutanix AHV User Guide.

Protecting Physical Machines

To back up a physical Microsoft Windows, Linux, Unix (IBM AIX, Oracle Solaris) or macOS machine using Mine with Veeam, perform the following steps:

1. Add the machine to the backup inventory. To do this, create a protection group of the *Computers with pre-installed agents* type. For more information, see the Veeam Agent Management Guide, section Creating Protection Groups.

2. Install Veeam Agent on the machine you want to protect. For more information, see the Veeam Agent Management Guide, section Deploying Veeam Agents Using Generated Setup Files.

3. Create a backup policy that will process the machine and create restore points for it. For more information, see the Veeam Agent Management Guide, section Creating Veeam Agent Backup Policies.

Once the backup policy successfully creates a restore point for the machine, you can perform the following operations to restore the machine:

- Perform restore to a physical machine, a virtual machine (vSphere VMware, Hyper-V, Nutanix AHV) or a cloud instance (Microsoft Azure, Amazon EC, Google Cloud Platform). For more information, see the Veeam Agent Management Guide, section Restoring Data from Veeam Agent Backups.

- Restore individual files and folders. For more information, see the Veeam Agent Management Guide, section Restoring Files and Folders.

- Restore items of applications such as Microsoft Active Directory, Microsoft Exchange, Microsoft SharePoint, Microsoft SQL Server and Oracle Database. For more information, see the Veeam Agent Management Guide, section Restoring Application Items.

For the complete list of features that Veeam Backup & Replication provides to protect physical machines, see Veeam Agent Management Guide.

Protecting File Shares

To back up a file share using Mine with Veeam, perform the following steps:

1. Add the file share to the backup infrastructure. For more information, see the Veeam Backup & Replication User Guide, section Adding File Share.
2. Add a backup proxy to the backup infrastructure. For more information, see the Veeam Backup & Replication User Guide, section Adding Backup Proxy.

> NOTE
>
> You can assign the role of a backup proxy to any existing VMware backup proxy deployed in the Mine with Veeam cluster.

3. Create a file share backup job to protect the file share. For more information, see the Veeam Backup & Replication User Guide, section Creating File Share Backup Jobs.

After the file share backup job has successfully created restore points for the file share, you can perform the following operations to restore the file share:

- Test the created restore points to check whether you will be able to use them for recovery operations. For more information, see Veeam Backup & Replication User Guide, section Performing Health Check and Repair for File Share Backup Files.
- Restore the entire file share. For more information, see Veeam Backup & Replication User Guide, section Restoring Entire File Share.
- Restore specific files and folders. For more information, see Veeam Backup & Replication User Guide, section Restoring Specific Files and Folders.

For the complete list of features that Veeam Backup & Replication provides to protect file shares, see the Veeam Backup & Replication User Guide, section NAS Backup.

Protecting Microsoft Azure Workloads

To protect an Azure VM using Mine with Veeam, perform the following steps:

1. Add to the backup infrastructure a Veeam Backup for Microsoft Azure appliance that will manage backup and restore operations for Azure workloads. For more information, see the Integration with Veeam Backup for Microsoft Azure Guide, section Adding Veeam Backup for Microsoft Azure Appliances.

2. Add a blob storage backup repository that will be used to store backups created for the Azure VM. For more information, see the Integration with Veeam Backup for Microsoft Azure Guide, section Adding Blob Storage Backup Repositories.

3. Configure a backup policy that will create backups for the Azure VM. For more information, see the Integration with Veeam Backup for Microsoft Azure Guide, section Creating Azure VM Backup Policies.

4. Configure a backup copy job that will transfer the created backups to a Mine with Veeam repository. For more information, see the Integration with Veeam Backup for Microsoft Azure Guide, section Creating Backup Copy Jobs.

Once the backup policy successfully creates a restore point (either a snapshot or a backup) for the Azure VM, you can perform the following operations to restore the VM:

- Restore the entire Azure VM to Microsoft Azure. For more information, see the Integration with Veeam Backup for Microsoft Azure Guide, section Restoring to Microsoft Azure.

- Immediately restore the Azure VM to VMware vSphere or Hyper-V environment. For more information, see the Integration with Veeam Backup for Microsoft Azure Guide, section Performing Instant Recovery.

- Restore the Azure VM to a Nutanix AHV cluster. For more information, see the Integration with Veeam Backup for Microsoft Azure Guide, section Restoring to Nutanix AHV.

- Restore the Azure VM to Amazon EC 2. For more information, see the Integration with Veeam Backup for Microsoft Azure Guide, section Restoring to Amazon EC2.

- Restore the Azure VM to Google Cloud. For more information, see the Integration with Veeam Backup for Microsoft Azure Guide, section Restore to Google Compute Engine.

- Restore items of applications such as Microsoft Active Directory, Microsoft Exchange, Microsoft SharePoint, Microsoft SQL Server and Oracle Database. For more information, see the Integration with Veeam Backup for Microsoft Azure Guide, section Restoring Application Items.

With Veeam Backup & Replication, you can also back up Azure SQL databases. For the complete list of features that Veeam Backup & Replication provides to protect Microsoft Azure workloads, see Integration with Veeam Backup for Microsoft Azure Guide.

Protecting AWS Workloads

To protect an Amazon EC2 instance using Mine with Veeam, perform the following steps:

1. Add to the backup infrastructure a Veeam Backup for AWS appliance that will manage backup and restore operations for AWS workloads. For more information, see the Integration with Veeam Backup for AWS Guide, section Adding Veeam Backup for AWS Appliances.

2. Add an S3 backup repository that will be used to store backups created for the Amazon EC2 instance. For more information, see the Integration with Veeam Backup for AWS Guide, section Adding S3 Backup Repositories.

3. Configure a backup policy that will create backups for the Amazon EC2 instance. For more information, see the Integration with Veeam Backup for AWS Guide, section Creating Backup Policies.

4. Configure a backup copy job that will transfer the created backups to a Mine with Veeam repository. For more information, see the Integration with Veeam Backup for AWS Guide, section Creating Backup Copy Jobs for EC2 Instances.

Once the backup policy successfully creates a restore point (either a snapshot or a backup) for the Amazon EC2 instance, you can perform the following operations to restore the instance:

- Restore the entire Amazon EC2 instance to AWS. For more information, see the Integration with Veeam Backup for AWS Guide, section Restoring Amazon EC2 Instances.

- Immediately restore the Amazon EC2 instance to a VMware vSphere or Hyper-V environment. For more information, see the Integration with Veeam Backup for AWS Guide, section Performing Instant Recovery.

- Restore the Amazon EC2 instance to a Nutanix AHV cluster. For more information, see the Integration with Veeam Backup for AWS Guide, section Restoring to Nutanix AHV.

- Restore the Amazon EC2 instance to Microsoft Azure. For more information, see the Integration with Veeam Backup for AWS Guide, section Restoring to Microsoft Azure.

- Restore the Amazon EC2 instance to Google Cloud. For more information, see the Integration with Veeam Backup for AWS Guide, section Restore to Google Compute Engine.

- Restore items of applications such as Microsoft Active Directory, Microsoft Exchange, Microsoft SharePoint, Microsoft SQL Server and Oracle Database. For more information, see the Integration with Veeam Backup for AWS Guide, section Restoring Application Items.

With Veeam Backup & Replication, you can also back up Amazon Relational Database Service resources, Amazon Elastic File Systems and Amazon Virtual Private Cloud configurations. For the complete list of features that Veeam Backup & Replication provides to protect AWS workloads, see Integration with Veeam Backup for AWS Guide.

Protecting Google Cloud VM Instances

To protect a Google Cloud VM instance using Mine with Veeam, perform the following steps:

1. Add to the backup infrastructure a Veeam Backup for Google Cloud appliance that will manage backup and restore operations for Google Cloud workloads. For more information, see the Integration with Veeam Backup for Google Cloud Platform Guide, section Adding Veeam Backup for Google Cloud Appliances.

2. Add a Google Cloud storage bucket that will be used to store backups created for the Google Cloud VM instance. For more information, see the Integration with Veeam Backup for Google Cloud Platform Guide, section Adding Cloud Storage Backup Repositories.

3. Configure a backup policy that will create backups for the Google Cloud VM instance. For more information, see the Integration with Veeam Backup Google Cloud Platform Guide, section Creating Backup Policies.

4. Configure a backup copy job that will transfer the created backups to a Mine with Veeam repository. For more information, see the Integration with Veeam Backup for Google Cloud Platform Guide, section Creating Backup Copy Jobs for VM Instances.

Once the backup policy successfully creates a restore point (either a snapshot or a backup) for the Google Cloud VM instance, you can perform the following operations to restore the instance:

- Restore the VM instance to Google Cloud. For more information, see the Integration with Veeam Backup for Google Cloud Platform Guide, section Restoring to Google Compute Engine.

- Immediately restore the VM instance to VMware vSphere or Hyper-V environment. For more information, see the Integration with Veeam Backup for Google Cloud Platform Guide, section Performing Instant Recovery.

- Restore the VM instance to a Nutanix AHV cluster. For more information, see the Integration with Veeam Backup for Google Cloud Platform Guide, section Restoring to Nutanix AHV.

- Restore the VM instance to Amazon EC2. For more information, see the Integration with Veeam Backup for Google Cloud Platform Guide, section Restoring to Amazon EC2.

- Restore the VM instance to Microsoft Azure. For more information, see the Integration with Veeam Backup for Google Cloud Platform Guide, section Restoring to Microsoft Azure.

- Restore items of applications such as Microsoft Active Directory, Microsoft Exchange, Microsoft SharePoint, Microsoft SQL Server and Oracle Database. For more information, see the Integration with Veeam Backup for Google Cloud Platform Guide, section Restoring Application Items.

With Veeam Backup & Replication, you can also back up Google Cloud SQL instances. For the complete list of features that Veeam Backup & Replication provides to protect Google Cloud workloads, see Integration with Veeam Backup for Google Cloud Platform Guide.

Reviewing Mine with Veeam Dashboard

Mine with Veeam comes with a dashboard that provides at-a-glance real-time overview of protected VMs and allows you to evaluate the performance of backup jobs and the health of the cluster.

To access the Mine with Veeam dashboard, do the following:

1. In a web browser, navigate to the virtual IP address of the cluster. You can also use the IP address or the hostname of a Controller VM in the cluster.

2. In the **username** and **password** fields, enter credentials of a user account with Prism Element administrative privileges, and press [Enter] on the keyboard.

3. From the main navigation menu, select **Mine with Veeam**.

The dashboard includes the following widgets:

- **Cluster** — shows the overall health state of the Mine with Veeam cluster that is affected by the following aspects:

  - Health state of the backup infrastructure components (such as the backup server, backup proxies and backup repositories). If the components are in an unhealthy state, the **Veeam Backup & Replication Alerts and Events** widget can help you identify all possible root causes.

  - Health state of the Mine infrastructure components (such as the foundation server, storage, CPU and memory). If the components are in an unhealthy state, the **Nutanix Alerts** widget can help you identify all possible root causes.

  - Amount of free space left on the Mine with Veeam cluster.

- **Physical Cluster Usage** — shows the amount of space that is currently occupied on the physical storage in the Mine with Veeam cluster. The widget also allows you to track how the space usage has been changing during the past 2 hours.

- **Storage Throughput** — allows you to track how the speed of read and write operations on the physical storage in the Mine with Veeam cluster has been changing during the past 2 hours.

- **Protection** — shows the number of workloads protected by Mine with Veeam.

- **Job Status** — shows the number of running, disabled and idle backup jobs managed by the backup server. Note that this widget does not include information on jobs that protect Nutanix AHV VMs.

- **Capacity Usage** — shows the amount of space that is currently occupied by the backup infrastructure data on the logical storage in the Mine with Veeam cluster. The widget also displays how much space remains before the level of resource utilization breaches the following thresholds:

  - **Low on space** — shows the amount of space remaining on the logical storage before extents of the performance tier in the scale-out backup repository start running out of free space.

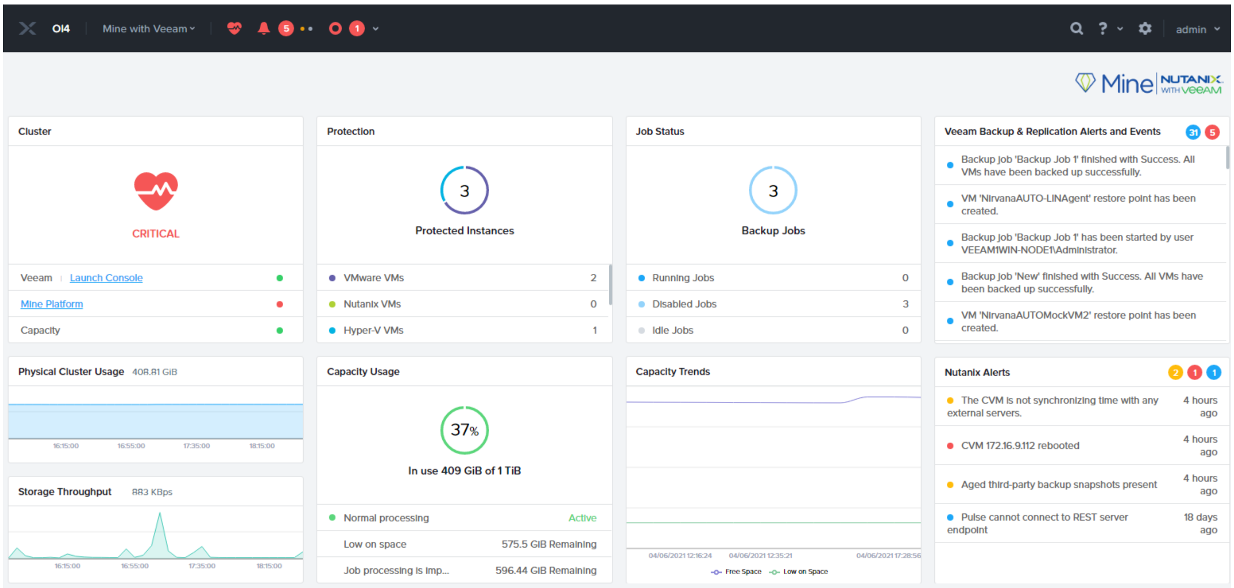
    If the threshold is breached, Veeam Backup & Replication will start uploading backup files to the capacity tier of the scale-out backup repository. To learn how to add the capacity tier to the scale-out backup repository, see Extending Scale-Out Backup Repository.

  - **Job processing is impacted** — shows the amount of space remaining on the logical storage before Veeam Backup & Replication automatically switches all extents of the performance tier in the scale-out backup repository to the seal mode.

    If the threshold is breached, Veeam Backup & Replication will stop jobs that have already started but will suspend all scheduled jobs until more space becomes available. For more information on limitations that apply in the seal mode, see the Veeam Backup & Replication User Guide, section Switching to Seal Mode.

> NOTE
>
> You cannot set threshold values manually — they are both automatically defined taking into account the total amount of space on the physical storage in the Mine with Veeam cluster. If you need to change threshold values, open a support case.

- **Capacity Trends** — shows how the amount of free space on the logical storage in the Mine with Veeam cluster has been changing during the past 2 months.



Veeam | Launch Console	●
Mine Platform	●
Capacity	●

● VMware VMs	2
● Nutanix VMs	0
● Hyper-V VMs	1

● Running Jobs	0
● Disabled Jobs	3
● Idle Jobs	0

● Normal processing	Active
Low on space	575.5 GiB Remaining
Job processing is imp...	596.44 GiB Remaining

- Backup job 'Backup Job 1' finished with Success. All VMs have been backed up successfully.
- VM 'NirvanaAUTO-LINAgent' restore point has been created.
- Backup job 'Backup Job 1' has been started by user VEEAM1WIN-NODE1\Administrator.
- Backup job 'New' finished with Success. All VMs have been backed up successfully.
- VM 'NirvanaAUTOMockVM2' restore point has been created.

● The CVM is not synchronizing time with any external servers.	4 hours ago
● CVM 172.16.9.112 rebooted	4 hours ago
● Aged third-party backup snapshots present	4 hours ago
● Pulse cannot connect to REST server endpoint	18 days ago

Related Topic

Veeam Backup & Replication Events

Veeam Backup & Replication Events

The following tables contain additional information on Veeam Backup & Replication events that can be displayed on the Mine with Veeam dashboard.

General

Event ID	Message Summary	Message Details	Severity
31100	Network traffic rules updated	Network traffic rules have been modified.	Info, Warning, Error

License Events

Event ID	Message Summary	Message Details	Severity
24010	License installed	*<License type>* License key for Veeam Backup & Replication *<Edition>* has been installed.	Info
24020	License expiring	*<License type>* License key for Veeam Backup & Replication *<Edition>* is about to expire in *<Number of days>* Days.	Warning
24022	License evaluation expiring	*<License type>* Evaluation license key for Veeam Backup & Replication *<Edition>* is about to expire in *<Number of days>* Days.	Warning
24030	License expired	*<License type>* License key for Veeam Backup & Replication *<Edition>* has expired.	Error
24040	License support expiring	Support contract for Veeam Backup & Replication is about to expire in *<Number of days>* Days.	Warning
24050	License support expired	Support contract for Veeam Backup & Replication has expired. Contact Veeam sales representative to renew your support contract.	Error
24060	License exceeded	License exceeded.	Error

Event ID	Message Summary	Message Details	Severity
24070	License grace period entered	License grace period entered.	Info

Host Events

Event ID	Message Summary	Message Details	Severity
28300	Host added	Host "<*Host name*>" (<*Host type*>) has been created.	Info, Warning, Error
32900	Component installed or updated	Component "<*Component name*>" on host "<*Host name*>" has been installed or upgraded.	Info, Warning, Error

Proxy Server Events

Event ID	Message Summary	Message Details	Severity
21210	Proxy server established connection	Connection to backup proxy "<*Proxy name*>" has been restored.	Info

Repository Events

Event ID	Message Summary	Message Details	Severity
21220	Repository server established connection	Connection to backup repository "<*Repository name*>" has been restored.	Info
26500	Maintenance mode of scale-out backup repository changed	Extent <*ID*> maintenance mode has been changed. New mode is <*New status*>.	Info

Backup Job Events

Event ID	Message Summary	Message Details	Severity
110	Backup job started	*<Job type>* job "*<Job name>*" has been started.	Info
190	Backup job finished	The *<Job type>* job "*<Job name>*" has finished with *<State name>* state.	Info, Warning, Error
410	Backup copy job started	*<Job type>* job "*<Job name>*" has been started.	Info
490	Backup copy job finished	The *<Job type>* job "*<Job name>*" has finished with *<State name>* state.	Info, Warning, Error
10010	Restore point created	VM "*<Vm name>*" restore point has been created.	Info

Restore Operation Events

Event ID	Message Summary	Message Details	Severity
210	Restore session started	Restore session has been initiated by "*<User name>*".	Info
290	Restore session finished	The restore session has finished with *<State name>* state.	Info, Warning, Error

SureBackup Job Events

Event ID	Message Summary	Message Details	Severity
310	SureBackup job started	*<Job type>* job "*<Job name>*" has been started.	Info
390	SureBackup job finished	The *<Job type>* job "*<Job name>*" has finished with *<State name>* state.	Info, Warning, Error