

Backup Process

Standard Operating Procedures

|  |  |
| --- | --- |
| SOP Title: | Backup Process Standard Operating Procedures |
| SOP #: | Backup and Recovery process for Datacenter Servers |
| SOP Owner: | Vijay Kumar Nuthalpati |
| SOP Approver: | Ramana Vadapalli |
| Version #: | V 1.0 |
| Effective Date: | 1-May-23 |
| Last Reviewed Date: | 1-May-23 |

|  |  |  |
| --- | --- | --- |
| **Index no** | **Annex** | **Page no** |
|  | PSMRI Backup Environment and Standard Operating Procedures |  |
|  |
| 1 | Purpose of the Document | 3 |  |
| 2 | Disclaimer | 3 |  |
| 3 | Scope of the Doc | 4 |  |
| 4 | Policies of Backup process. |  |  |
| 5 | Roles and Responsibilities. |  |  |
| 6 | Backup Solution Installation & Implementation |  |  |
| 7 | Backup Process network Isolation implementation function |  |  |
| 8 | Backup Repository HA implementation and function |  |  |
| 9 | Performing Backup and Adding backup Jobs. |  |  |
| 10 | Verifying Active backup jobs and monitoring. |  |  |
| 11 | Taking Archive backup |  |  |
| 12 | Testing and restoring backups |  |  |
|  | Restoring Local On-prem Server backup to cloud- |  |  |
|  | Restoring Cloud backup to Local On-prem |  |  |
| 13 | Production Server list and owners |  |  |
| 14 | Stake Holders and Big Bets |  |  |
| 15 | Conclusion |  |  |

1 Purpose of the Document

Preparing Backups Process for all Production and Critical Server’s, to address for a data loss disaster before it occurs so that we can speed up the Disaster Recovery process tremendously. The dependency on computers exponentially increases the Data lose risks associated with failure of any component of that system.

This document helps you understand Backup process and Implementing Backup solution in Data Center. (in this document we have used Veeam Backup and Replication Enterprises edition.)

Typically, when a computer crashes catastrophically, the first and foremost task is for  
IT to rebuild and reconfigure the system, restoring mission-critical applications and  
data without excessive downtime.  
Overall disaster risk assessment pertaining to monetary, customer, legal and regulatory  
exposures, as well as interdepartmental dependencies should be considered. Recovery  
and data freshness windows should also be considered when building a disaster  
recovery plan to ensure the recovery time objectives can be attained during a full-scale  
restore operation.

2 Disclaimer

*The information contained in this document reflects the situation in force at the  
Piramal Swasthya at the time of writing and is subject to change.  
The Piramal Swasthya can not be held liable for the consequences of any reliance on  
the information provided or for any inaccuracies in such information and it does not  
commit the Stake holders regarding the future evolution of its data processing  
and network environment.*

3 Scope.

**Main scope of the doc:**

1. Why use backup solution.
2. How to budget backup solution.
3. Who will be responsible for Backup and recovery.
4. How to install Backup Solution.
5. How to Implement Daily, Weekly, Monthly backups.
6. How to restore the backup Image.
7. Frequency of Testing backup restoration process.
8. Archival and storage strategy of Backup Files and repositories.
9. Configuring Backup Repositories in 3-2-1 model.
10. When to decompose backup data of the system.
11. Who will Influence the decisions of Data and Security.
12. Who will be the owners of the Backup of archived data.

*All the above questions will be addressed in this document.*

**3.1 Why use backup solution.**

Backup refers to the copying of physical or virtual files or databases to a secondary location for preservation in case of equipment failure or catastrophe. The process of backing up data is pivotal to a successful disaster recovery plan.

Using Enterprise Backup Solutions to safeguard Organization Important Data and Production Servers.

Enterprises back up data they deem to be vulnerable in the event of buggy software, data corruption, hardware failure, malicious hacking, user error or other unforeseen events. Backups capture and synchronize a point-in-time snapshot that is then used to return data to its previous state.

Backup and recovery testing The goal is to ensure rapid and reliable data retrieval should the need arise. The process of retrieving backed-up data files is known as file restoration.

If this year’s cyberattacks have taught us anything, it’s the importance of server backups and data redundancy.

While part of the problem is vulnerabilities and zero-day threats catching enterprise networks off guard, the sheer amount of data currently collected, stored, and processed is becoming too much to manage.

**3.2 How to budget backup solution.**

Budgeting is the most difficult part of the decision making, as it might appear overspending on Backup would be bad Idea, contrary to that under spending would hurt the Organization when there are many critical Production Server to be handled with different scope of Recovery Time Objective RTO.

**Below Strategy would help us narrow down the decision-making process**

1. **Determine what data has to be backed up**

“Everything” would probably be your answer. However, the level of data protection would vary based on how critical it is to restore that particular dataset. Our Organization’s [Recovery Time Objective (RTO)](https://spanning.com/blog/defining-rto-and-rpo-in-the-age-of-cloud-computing/), which is the maximum acceptable length of time required for an organization to recover lost data and get back up and running, would be a reliable benchmark when forming your backup strategy.

Assess and group your applications and data into the following:

* *Existentially-critical* for the business to survive
* *Mission-critical* for the organization to operate
* *Optimal-for-performance* for the organization to thrive

Once all pertinent data is identified, layer the level of protection accordingly.

**b. Determine how often data has to be backed up**

The frequency with which you back up your data should be aligned with your organization’s Recovery Point Objective (RPO), which is defined as the maximum allowable period between the time of data loss and the last useful backup of a known good state. Thus, the more often your data is backed up, the more likely you are to comply with your stated RPO. As a good rule of thumb, backups should be performed at least once every 24 hours to meet acceptable standards of most organizations.

**c.** **Identify and implement a suitable backup and recovery solution**

Based on your organization’s requirements, you need to identify a suitable backup solution as part of your backup strategy. Some aspects to consider:

* **Types of backup**: full backup, differential backups where only additions/changes are copied, and incremental backups where delta changes since the most recent incremental backup are copied.
* **Where the data is backed up**: Physical/Local backup where the data is backed up on-site using an external hard drive, USB drive or the like. Cloud/Remote backup, where data is backed up off-site in a cloud storage environment.
* **Features your organization requires**: Below are several essential aspects of a comprehensive and dependable backup and restore solution to consider:
  + Ease of Backup: Automated and/or on-demand options
  + Restore Flexibility: Cross-user, search-based, point-in-time
  + Scalability: License and user management
  + Ease of Use: Intuitive user interface and self-service recovery
  + Post-purchase Experience: Free support and unlimited storage
  + Strong Credentials: Superior customer ratings, security & compliance certifications

**d. Test and Monitor your backup system**

Once your backup system is in place, test it, both to check that the backup is successful and that the restore is smooth and accurate. Verify the backup and restore with regards to various types of artifacts – accounts, emails, documents, sites, etc. If the backup solution supports end-user backup – inform and educate your users about using it. Finally, remember to monitor your backup performance and regularly check the logs for data lapses.

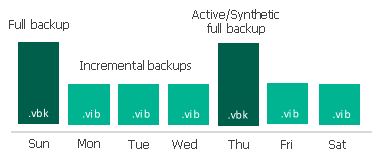
**3.3** How to carry out this procedure.

For each operating system, service and application component we should consider the  
following. These questions should be addressed for each system that is supported by  
IT.

**3.4** When should the Backup be applied?  
Daily, weekly, monthly, and yearly

**3.5** What is the frequency of the Data to be stored?

Weekly for Production and Monthly for Development

  
  
**3.6** What are the possible failure scenarios?  
Server hardware Failure

Disk/Raid Failure  
Data corruption

Ransomware attack

**3.7** Where is the critical data?  
Active Directory  
AMRIT Application

Production Server

Database Servers  
Finance ERP Server  
File Stores  
E-mail  
  
**3.8** How often should backups be performed?  
Full daily backups for all Production servers.  
Friday full backups and weekday differential for Production servers.

**3.9** When should a FULL backup versus an Incremental or Differential Backup  
be performed?  
Differentials would be run to backup files that have been changed since the last  
backup, usually quicker than full backups. We would use differential backups if  
time were at a premium.  
For production servers’ full backups are run on Fridays with Differential backups  
being run in the week, this applies to the majority of systems. Exceptions being  
Active Directory Servers (3), File Store and the Virtual Centre Controller.  
For production servers a full backup is scheduled daily.

**3.10** Should backups be performed on-line while users are working, or off-line?  
All backups are run online.

**3.11** Will backups be done manually or via an automatic scheduling process?  
All backups are performed automatically with staging to Hardened Linux server and other 2 copies to NAS and EHDD/Cloud Storage respectively.

**3.12** How can we verify that a backup was successfully performed?  
Setting Up Monitoring tool to activity monitor All Backup process run in Backup Solution (Zabbix and Veeam Alert management integration) also The backup log files are error checked and “signed” for on a daily basis. The file is held in the IT documentation drive.

**3.13** How will we determine if the backups are useable?  
Restores are carried out through normal helpdesk requests and restoring data to  
an alternative destination periodically checks Storage repositories i.e. Hardened Linux server, NAS, EHDD/Cloud storage.  
Test Restores will be carried out on a quarterly basis by the IT department.  
We periodically perform trial restorations to verify that files are being backed up  
properly. Usually trial restorations will uncover any hidden hardware anomalies.  
These trial restorations will be logged into the evidence file on the IT  
documentation drive.

**3.14** How long will we save backups before reusing the medium?  
We use a grandfather, father, and son schedule on Backup repositories EHDD and we keep monthly  
and annual EHDD to one side, whilst the ‘week’ EHDD rotate on a 4 week cycle.  
Production Backups are sent to disk in the first instance and maintained for 1 years.

**3.15** How much time will it take to restore from the last back up?  
Depends on the amount of data to restore, typically we can restore 100Gb + in  
just over 3 hours if need be. This has been benchmarked. If the amount of data  
is backed up increases, a different set of benchmark tests will be performed.

**3.16** Where will our backup media be stored?  
The backup media is stored in a secure separate vault/building to where the servers  
are located.

**3.17** Do appropriate personnel have access to backup media for restores?  
All IT staff has access to the backup media and can restore data.

**3.18** If the IT System Administrator(s) is (are) not available, is there a source for  
acquiring system passwords and procedures to back ups, and if necessary,  
perform restores?

There will always be a member of the IT department available to enable these  
requests. Any request should be reported to the helpdesk for the IT department.  
Engineers to action. Escalation should be via the IT Support Team Leader then  
the IT Services Manager

**4 Policies**

**4.1 Backup Policy**

A backup policy is a crucial component of an organization’s comprehensive backup strategy. Common backup policies identify critical data and systems to be protected, clarify the frequency of both full and incremental backups, delineate backup administrator responsibilities, and provide details for retention, offsite rotation, restoration procedures, storage of backups, and more.

 There are several benefits to developing a strong backup and recovery policy document:

**Clarity.** A backup policy clarifies specific procedures, policies, and responsibilities, including a well-defined schedule for performing backups, ensuring a more stable process. It also identifies any superseding procedures or policies that already exist, such as contingency plans.

**Control.** A well defined backup policy allows you to control what kind of backups are performed, how often data should be backed up, what software/hardware or cloud service should be used for performing backups, where backups are located, and who can access backups and how to contact them.

**Accountability.** The backup policy identifies primary and secondary contacts who are responsible for performing backups and provides their contact information. This piece of the data backup and recovery policy also identifies who is responsible for confirming that reliable backups are successfully performed, and sets forth how and when they will do this.

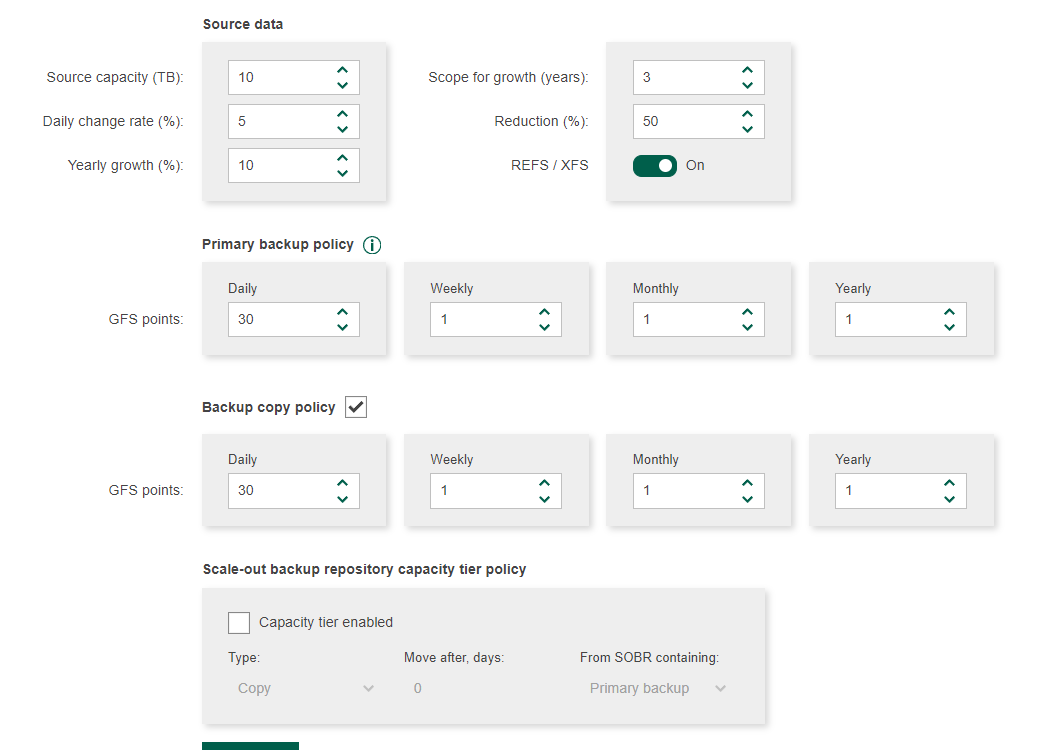
**Reliability.** Stronger backup policies are more likely to result in complete data restoration. They offer details on how to protect data, how to access backups, and how to train those responsible for performing backups. They also ensure multiple copies exist separate from the original data, and also make use of multiple forms of media with complementary strengths. Finally, the policy demands at least partial automation, further increasing reliability.

**4.2 Backup retention policies**

Preserve essential data with a multi-pronged backup policy. **Your backup policy should follow the 3-2-1 rule,** creating at least three backup copies of all data in addition to the original file using two different backup media, with one copy in a remote location. This helps to ensure a full set of accessible backup data no matter what the circumstances leading to the need to recover data.

Storing at least one copy of backup data at a remote location is essential for disaster recovery, especially in the event of site-wide failures or geographical disasters. To protect against malware, remote backup data should be air-gapped (separated) from the original data set. Historically, third party vendors could store backup tapes offsite for a fee, but remote disk and cloud storage can be used as well.

It is important to periodically check the integrity of your backup files. Do this by restoring several files from the backup to confirm that you can, that the backup itself is uncorrupted, and that the media is still accessible.



**4.3 Backup policy best practices**

Follow these best practices to select an ideal backup solution that ensures your data remains recoverable and safe. The best backup policy solutions:

Include remote storage

Take frequent, regular backups.

Use automated backups.

Address retention span. After frequency, how long each backup should be kept is the next important question. Retaining every backup forever is neither desirable nor feasible, so any good data backup and storage policy and solution provides a series of retention schedules.

For example, healthcare organizations will need to craft backup policies that are HIPAA compliant. Businesses that are active in the EU may need a GDPR backup policy.

Encrypt backups. .

Use cloud storage for backup storage.

Find a comprehensive backup solution.

**5 Roles and Responsibilities.**

Once the Backup solution is selected which suits our Organization needs, assigning responsible personals is the immediate task.

We Responsible IT Person of Piramal Swasthya will perform all the Installation and Backup Jobs according to the Organization Architecture which defines Production and Critical Server for the functioning of the Organization. If the project are run on behalf of the Client, respective project MOM has to be meet, Server up time and

**6 Backup Solution Installation and Implementation.**

**System Requirements**

**Make sure that servers that you plan to use as backup infrastructure components meet the system requirements listed below.**

We do not recommend you to install Veeam Backup & Replication and its components on mission-critical machines in the production environment such as Microsoft Hyper-V Server, Domain Controller, Microsoft Exchange Server, Small Business Server/ Windows Server Essentials and so on. If possible, install Veeam Backup & Replication and its components on dedicated machines. Backup infrastructure component roles can be co-installed

**Refer Annex 1 for Server Specification**

**Installation Procedure of Veeam Backup Solution.**

To start the setup wizard:

1. Download the latest version of the Veeam Backup & Replication installation image from the [Download Veeam Products](https://www.veeam.com/downloads.html) page. https://www.veeam.com/downloads.html
2. Mount the installation image to the machine on which you plan to install Veeam Backup & Replication or burn the image file to a flash drive or other removable storage device. If you plan to install Veeam Backup & Replication on a VM, use built-in tools of the virtualization management software to mount the installation image to the VM.

To extract the content of the ISO, you can also use the latest versions of utilities that can properly extract data from ISOs of large size and can properly work with long file paths.

1. After you mount the image or insert the disk, Autorun will open a splash screen. If Autorun is not available or disabled, run the Setup.exe file from the image or disk.
2. In the splash screen, click **Install**.

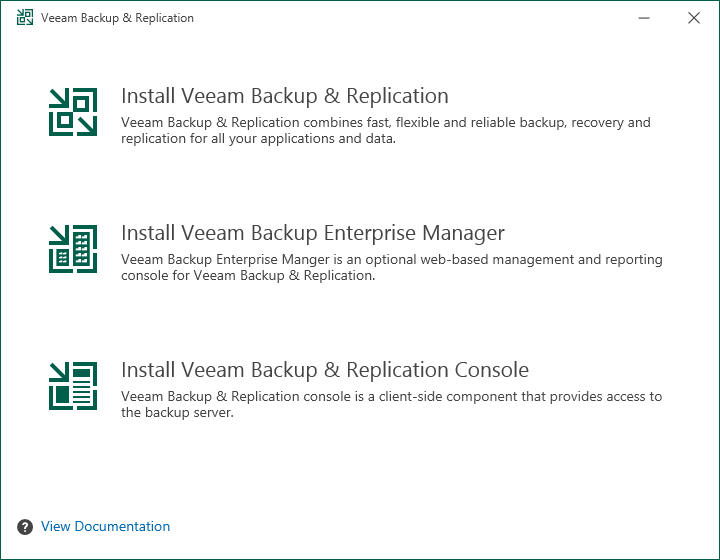
|  |
| --- |
| Important |
| It is strongly recommended that you install Veeam Backup & Replication using Autorun or the Setup.exe file. If you run other installation files from the ISO folders, you may miss some components that need to be installed, and Veeam Backup & Replication may not work as expected. |

[](https://helpcenter.veeam.com/docs/backup/hyperv/images/installation_splash.png)

Step 2. Select Component

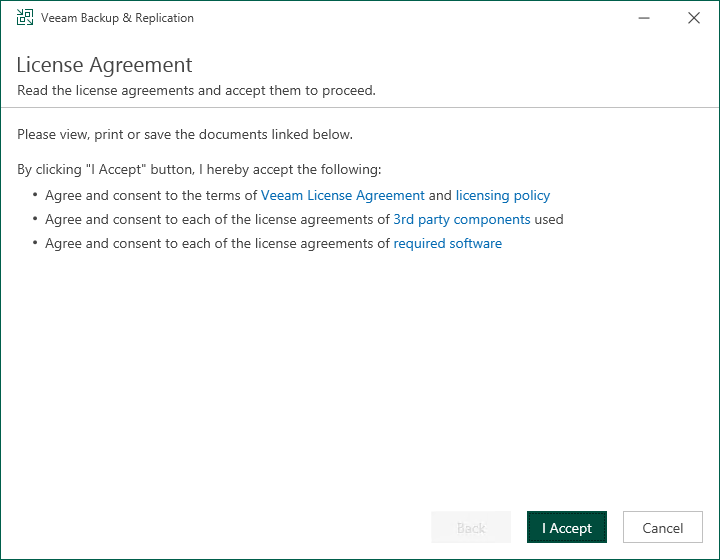
At the Select Veeam Backup & Replication Component step of the wizard, select **Install Veeam Backup & Replication**.

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

[](https://helpcenter.veeam.com/docs/backup/hyperv/images/installation_select_solution.png)

Step 3. Read and Accept License Agreement

At the License Agreement step of the wizard, read Veeam License Agreement and licensing policy as well as license agreements of 3rd party components that Veeam incorporates and license agreements of required software. To accept the license agreements and continue installing Veeam Backup & Replication, click I Accept.

[](https://helpcenter.veeam.com/docs/backup/hyperv/images/installation_accept_la.png)

Step 4. Provide License File

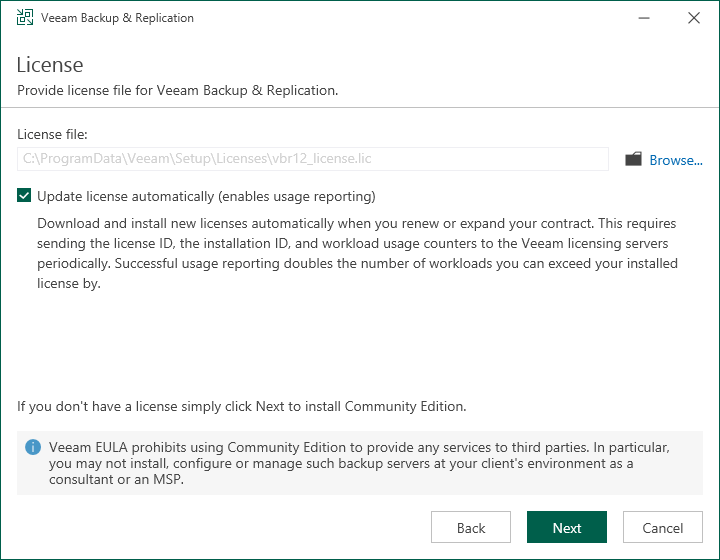
At the Provide License step of the wizard, specify what license you want to install for Veeam Backup & Replication. For more information, see [Licensing](https://helpcenter.veeam.com/docs/backup/hyperv/licensing.html).

If a valid license is already installed on the machine, the setup wizard will inform you about it. In this case, you can skip the Provide License step and move to the next step of the wizard.

If you do not install a license, the product will operate in the Veeam Backup & Replication Community (free) Edition. For more information, see [Veeam Backup & Replication Community Edition](https://www.veeam.com/virtual-machine-backup-solution-free.html).

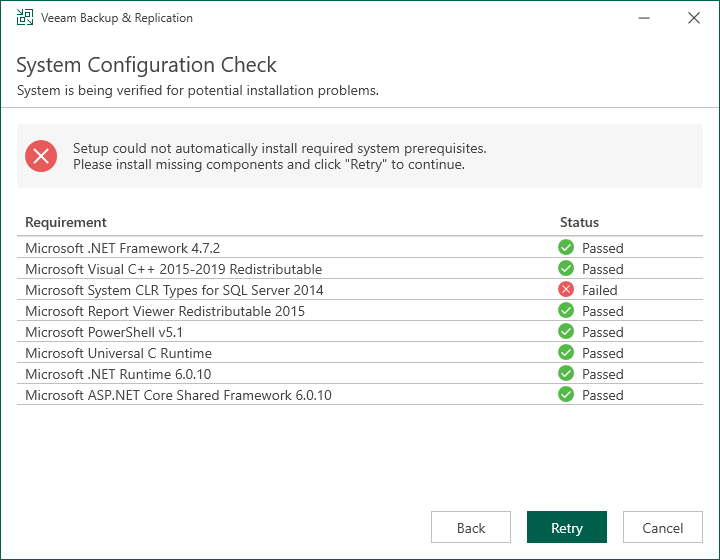
To install a license:

1. Next to the License file field, click Browse.
2. Select a valid license file for Veeam Backup & Replication.
3. To install new licenses automatically when you renew or expand your contract, select the Update license automatically check box. If you enable the automatic license update, and therefore enable usage reporting, you will double the number of workloads by which you can exceed your installed license. For more information, see [Exceeding License Limit](https://helpcenter.veeam.com/docs/backup/hyperv/license_exceeding.html).

[](https://helpcenter.veeam.com/docs/backup/hyperv/images/installation_select_license.png)

Step 5. Install Missing Software

|  |
| --- |
| At the System Configuration Check step of the wizard, the setup wizard checks if the required software is installed on the machine. If some of the required components are missing, the setup will try to install them automatically. After the components are successfully installed, reboot is required. To reboot the machine, click Reboot.  If the setup wizard cannot install some of the required software components automatically, install them manually and click Retry.  Note |
| If all required software is already installed on the machine, the System Configuration Check step will be skipped. For more information on the necessary software, see [System Requirements](https://helpcenter.veeam.com/docs/backup/hyperv/system_requirements.html#backup_server). |

[](https://helpcenter.veeam.com/docs/backup/hyperv/images/installation_missing_components.png)

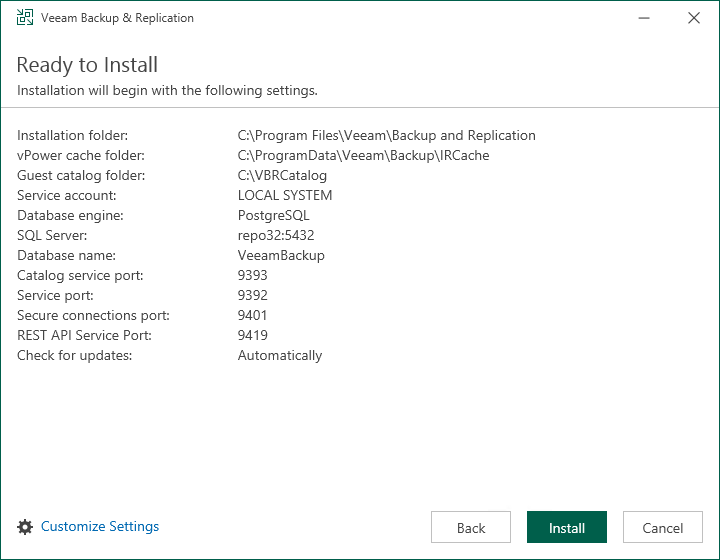
Step 6. Review Default Installation Settings

At the Ready to Install step of the wizard, you can select to install Veeam Backup & Replication with default installation settings or specify custom installation settings.

* To use the default installation settings, click Install.
* To use custom installation settings, click Customize Settings. The setup wizard will include additional steps that will let you configure installation settings.

The table below lists the default installation settings.

|  |  |  |
| --- | --- | --- |
| **Setting** | **Default Value** | **Description** |
| Installation folder | C:\Program Files\Veeam\Backup and Replication | Folder where Veeam Backup & Replication will be installed. |
| Guest catalog folder | C:\VBRCatalog | The VBRCatalog folder on a volume with the maximum amount of free space.  The guest catalog folder stores indexing data for VM guest OS files. Indexing data is required for browsing and searching for VM guest OS files inside backups and performing 1-click restore. |
| Service account | LOCAL SYSTEM | Account under which the Veeam Backup Service runs. |
| Database engine | PostgreSQL | The setup wizard installs PostgreSQL 15.1 as a database engine locally on the Veeam Backup & Replication server. |
| SQL server | <host\_name>:5432 | The local host name and port number to be used by SQL server. |
| Database name | VeeamBackup | The setup deploys the Veeam Backup & Replication configuration database on the locally installed instance of PostgreSQL. |
| Catalog service port | 9393 | The catalog service port is used by the Veeam Guest Catalog Service to replicate catalog data from backup servers to Veeam Backup Enterprise Manager. |
| Service port | 9392 | The service port is used by Veeam Backup Enterprise Manager to collect data from backup servers. In addition to it, the Veeam Backup & Replication console uses this service port to connect to the backup server. |
| Secure connections port | 9401 | The secure connections port is used by the mount server to communicate with the backup server. |
| REST API service port | 9419 | This service port is used to access the Veeam Backup & Replication REST API. |
| Check for updates | Automatically | Veeam Backup & Replication will check for product updates weekly. When a new product build is published on the Veeam update server, a notification is displayed in the Windows Action Center. |

[](https://helpcenter.veeam.com/docs/backup/hyperv/images/installation_ready_to_install.png)

Step 7. Specify Service Account Settings

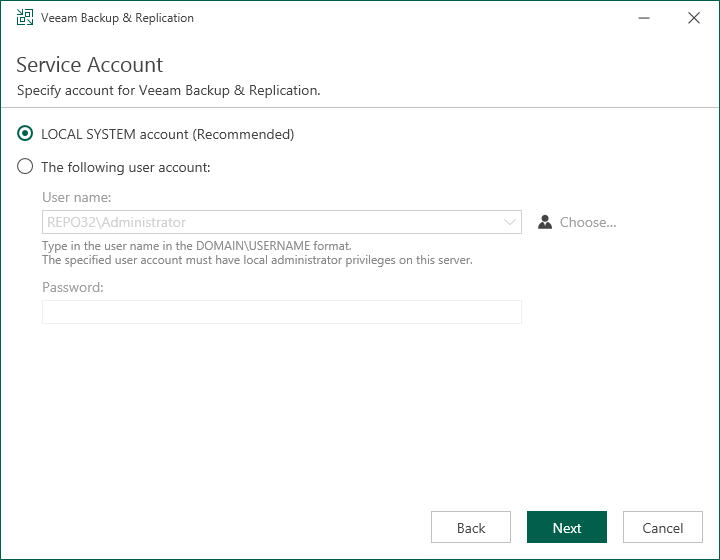
The Service Account step of the wizard is available if you have selected to configure installation settings manually.

You can select an account under which you want to run the Veeam Backup Service:

* LOCAL SYSTEM account (recommended, used by default)
* Another user account

The user name of the custom account must be specified in the DOMAIN\USERNAME format.

|  |
| --- |
| Note |
| The user account must have the following rights and permissions:   * The account must be a member of the Administrators group on the machine where Veeam Backup & Replication is installed. * The account must have db\_owner rights for the configuration database.   Veeam Backup & Replication automatically grants the Log on as service right to the specified user account. |

[](https://helpcenter.veeam.com/docs/backup/hyperv/images/installation_service_account.png)

Step 8. Specify Database Engine and Instance

The Database step of the wizard is available if you have selected to configure installation settings manually.

At this step of the wizard, you can choose a database engine (PostgreSQL or Microsoft SQL Server) for the Veeam Backup & Replication configuration database, specify a new or existing instance where you want to deploy the configuration database, and specify the authentication mode.

|  |
| --- |
| Note |
| Consider limitations and considerations in [Before You Begin](https://helpcenter.veeam.com/docs/backup/hyperv/installation_byb.html). |

1. Select one of the following database engines that you want to use for the configuration database:

* PostgreSQL
* Microsoft SQL Server

1. Specify instance settings:

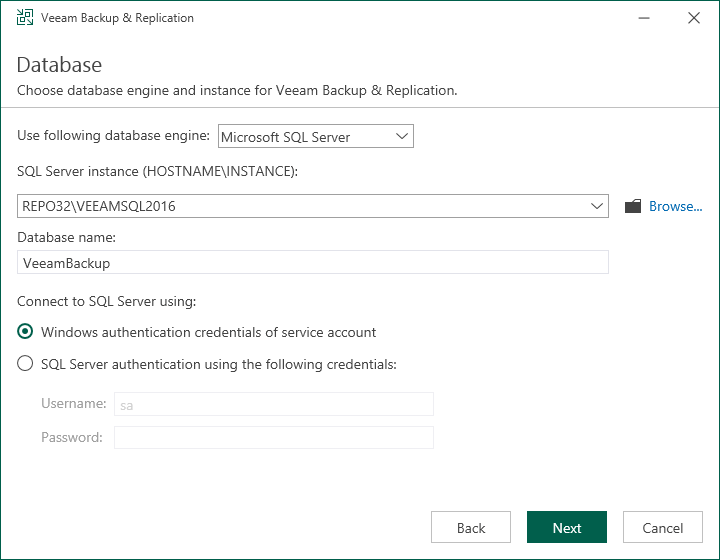
* [For PostgreSQL] You can use an already installed PostgreSQL instance or install a new one.
* To install a new PostgreSQL instance, select the Install a new instance option. The setup will install PostgreSQL 15.1 on the Veeam Backup & Replication server and create a database with the VeeamBackup name.
* To use an already installed PostgreSQL instance, select the Use the existing instance option. Enter the instance name in the HOSTNAME:PORT format. In the Database name field, specify a name for the Veeam Backup & Replication configuration database.

|  |
| --- |
| Important |
| If you use the already installed PostgreSQL instance or make any changes in the machine hardware, perform the additional configuration of the PostgreSQL instance. To do that:   1. Run the [Set-VBRPSQLDatabaseServerLimits](https://helpcenter.veeam.com/docs/backup/powershell/set-vbrpsqldatabaseserverlimits.html?ver=120) cmdlet in the automatic mode. 2. Restart the PostgreSQL service. |

[](https://helpcenter.veeam.com/docs/backup/hyperv/images/installation_database_postgresql.png)

* [For Microsoft SQL Server] You can use an already installed Microsoft SQL Server database only.

1. In the SQL Server instance field, enter the instance name in the HOSTNAME\INSTANCE format or select an instance from the drop-down list. You can also click Browse to choose a Microsoft SQL Server on a remote machine.
2. In the Database name field, specify a name for the Veeam Backup & Replication configuration database.

[](https://helpcenter.veeam.com/docs/backup/hyperv/images/installation_database_mssql.png)

1. Select an authentication mode to connect to the database server instance: Microsoft Windows authentication or native database server authentication. If you select the native authentication, enter credentials of the database account.

If a configuration database with the specified name already exists (for example, it was created by a previous installation of Veeam Backup & Replication), the setup wizard will notify about it. To connect to the detected database, click Yes. If necessary, Veeam Backup Enterprise Manager will automatically upgrade the database to the latest version.

Step 9. Specify Data Locations

The Data Locations step is available if you have selected to configure installation settings manually and to install a new instance of the database server.

At this step of the wizard, you can specify the installation folder and where the write cache and indexing data must be stored.

1. To change the default installation folder, click Browse next to the Installation path field.

By default, the setup wizard uses the following installation folder: C:\Program Files\Veeam\Backup and Replication.

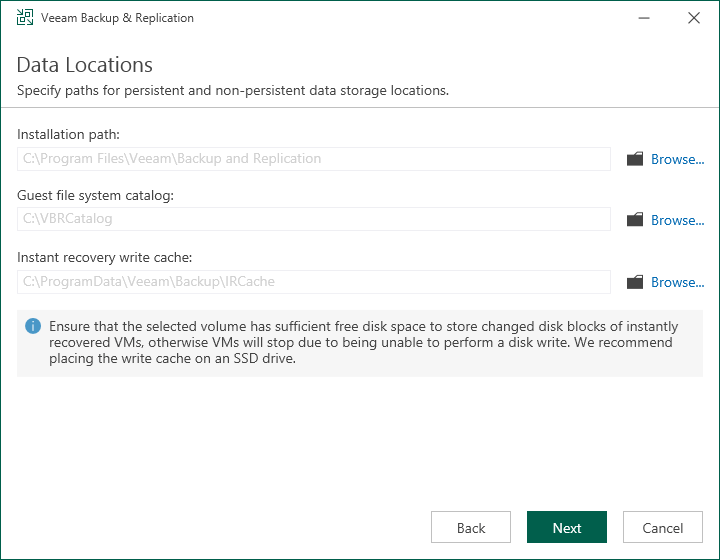
1. To change the path to the folder where index files will be stored, click Browse next to the Guest file system catalog field.

By default, the setup wizard creates the VBRCatalog folder on a volume with the maximum amount of free space, for example: C:\VBRCatalog.

1. [For VMware environments] The instant recovery cache folder stores the write cache for machines that are started from backups during recovery verification or restore operations. To change the path to the IR cache folder, click Browse next to the Instant recovery write cache field. Make sure that you have at least 10 GB of free disk space to store the write cache.

By default, the setup wizard creates the IR cache folder on a volume with the maximum amount of free space, for example: C:\ProgramData\Veeam\Backup\IRCache.

You do not need to configure this data location for Microsoft Hyper-V environments.

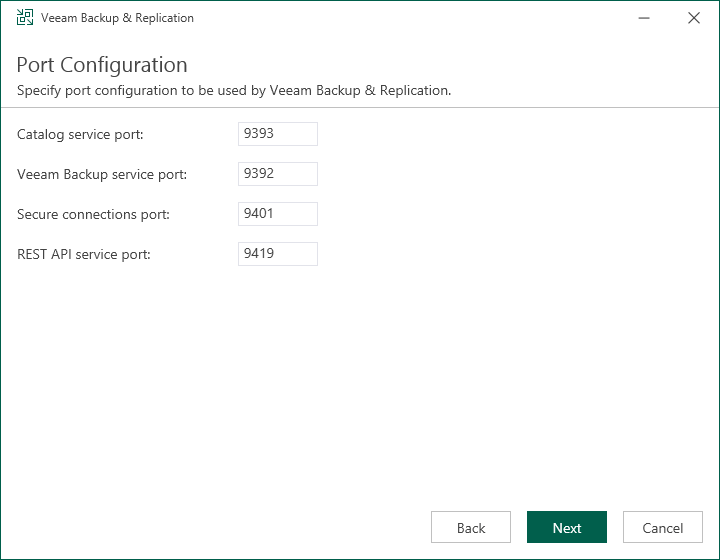
[](https://helpcenter.veeam.com/docs/backup/hyperv/images/installation_data_locations.png)

Step 10. Specify Service Ports

The Port Configuration step of the wizard is available if you have selected to configure installation settings manually.

At this step of the wizard, you can customize port number values that will be used for communication between backup infrastructure components. For more information about Veeam Backup & Replication ports, see [Ports](https://helpcenter.veeam.com/docs/backup/hyperv/used_ports.html).

* Catalog service port. This port is used by the Veeam Guest Catalog Service to replicate catalog data from backup servers to Veeam Backup Enterprise Manager. By default, port 9393 is used.
* Veeam Backup service port. This port is used by Veeam Backup Enterprise Manager to collect data from backup servers. In addition to it, the Veeam Backup & Replication console uses this service port to connect to the backup server. By default, port 9392 is used.
* Secure connections port. This port is used by the mount server to communicate with the backup server. By default, port 9401 is used.
* REST API service port. This port is used to communicate with the Veeam Backup & Replication REST API. By default, port 9419 is used.

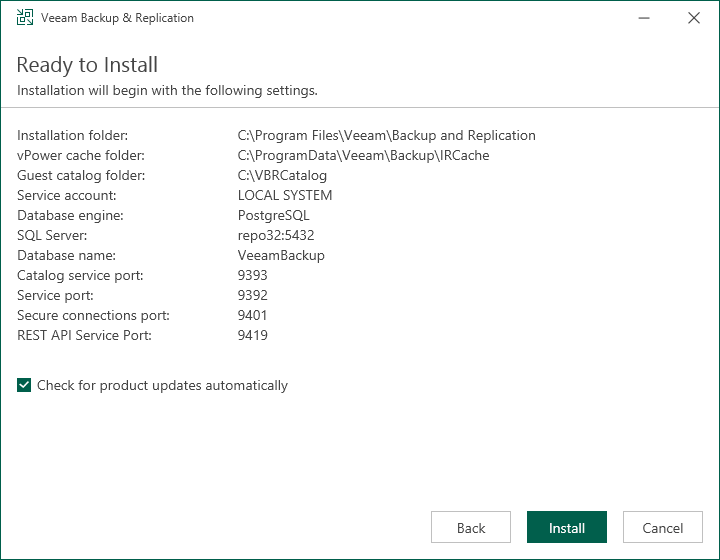
[](https://helpcenter.veeam.com/docs/backup/hyperv/images/installation_port_configuration.png)

Step 11. Begin Installation

The Ready to Install step of the wizard is available if you have selected to configure installation settings manually.

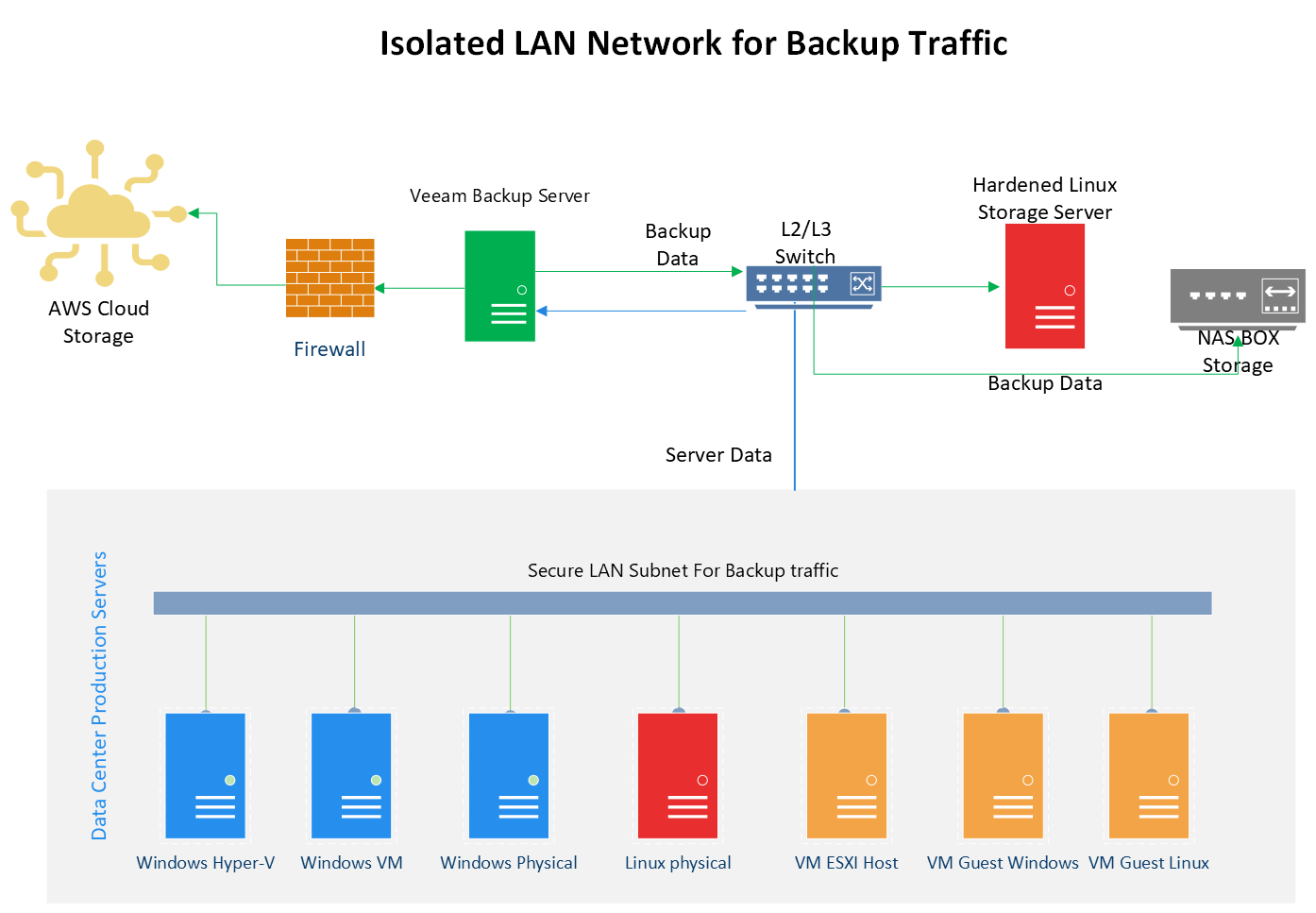
At this step of the wizard, you can review the Veeam Backup & Replication installation settings and start the installation process:

1. If you want Veeam Backup & Replication to check for product updates weekly, select the Check for product updates automatically check box. When a new product build is published on the Veeam update server, a notification will be displayed in the Windows Action Center.
2. Click Install to begin the installation.
3. Wait for the installation process to complete and click Finish to exit the setup wizard.

[](https://helpcenter.veeam.com/docs/backup/hyperv/images/installation_final.png)

**8 Backup Process network Isolation implementation.**

Isolated network for Backup traffic movement for better performance and Security, also so that it will not affect Production traffic and performance.

****

**9 Backup Repository HA implementation and function.**

**Step 4. Configuring Backup Repository**

On This Page

* [Before You Begin](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/setup_repository.html?ver=120#before-you-begin)
* [Adding a Server](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/setup_repository.html?ver=120#adding-a-server)
* [Assigning Backup Repository Role to Added Server](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/setup_repository.html?ver=120#assigning-backup-repository-role-to-added-server)
* [Reference](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/setup_repository.html?ver=120#reference)

The backup repository is a storage where Veeam Backup & Replication keeps backup files and, in case of replication, metadata for replicated VMs. You can use different types of storage as the backup repository. The full list of storage types is available in the [Backup Repository](https://helpcenter.veeam.com/docs/backup/vsphere/backup_repository.html?ver=120) section in the Veeam Backup & Replication User Guide.

In this section, you will learn how to use a Microsoft Windows server as the backup repository. To configure the backup repository, you must add the server to the backup infrastructure and assign the role of the backup repository to it.

**Before You Begin**

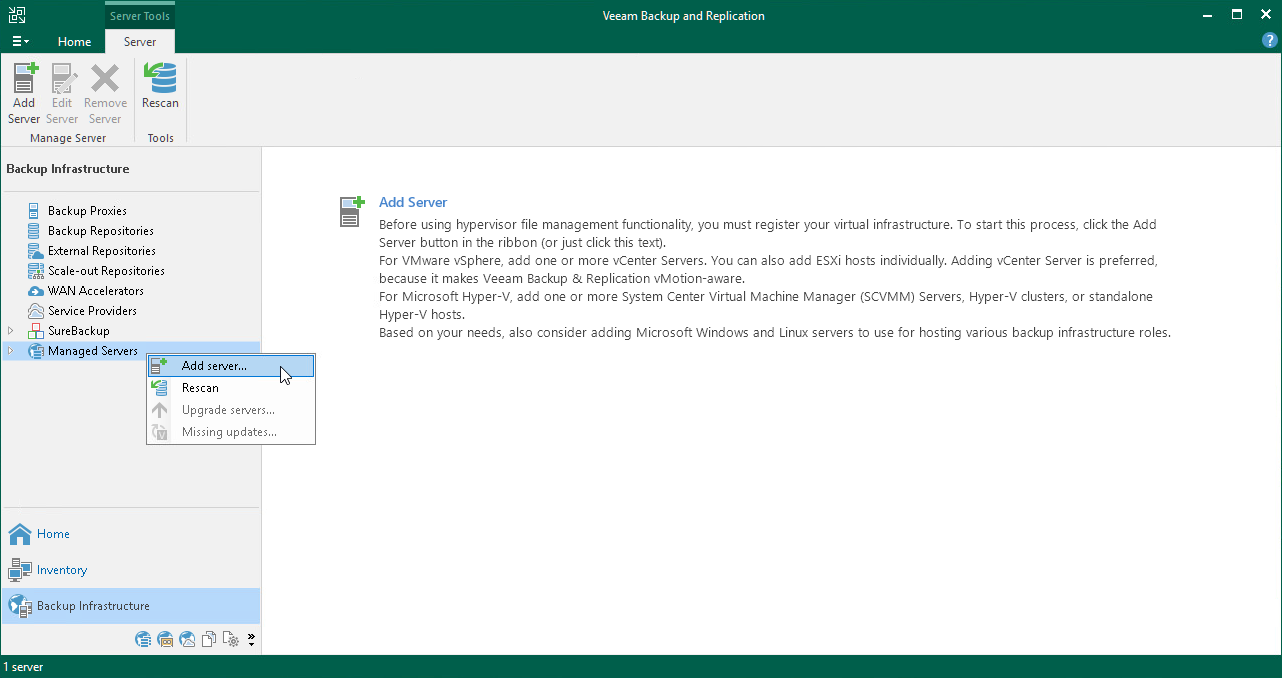
Check the following prerequisites:

* The Microsoft Windows machine that you plan to use as a backup repository must meet system requirements. For details, see [System Requirements](https://helpcenter.veeam.com/docs/backup/vsphere/system_requirements.html?ver=120) in the Veeam Backup & Replication User Guide.
* File and printer sharing must be enabled in network connection settings of the added Microsoft Windows machine. On this machine, Veeam Backup & Replication deploys the required components. Without sharing enabled, Veeam Backup & Replication fails to deploy these components.

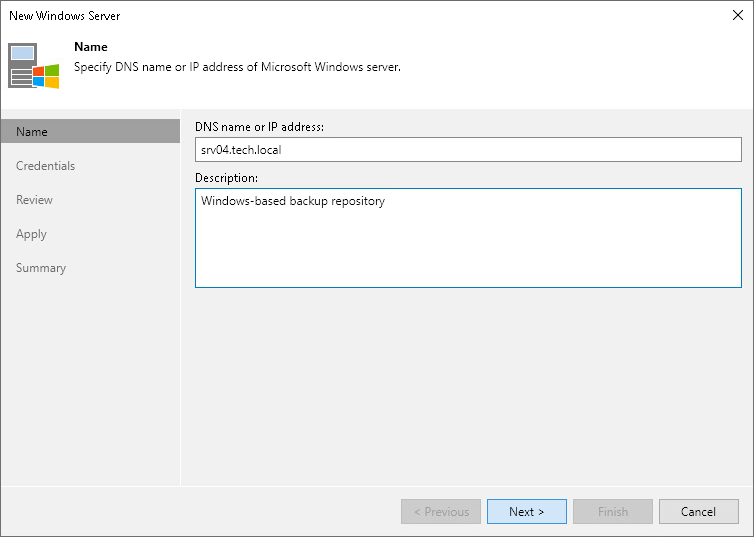
**Adding a Server**

To add a server to the Veeam Backup & Replication infrastructure, do the following.

1. In the inventory pane of the **Backup Infrastructure** view, right-click the **Managed Servers** node and select **Add Server**.

[](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/images/add_host_launch.png)

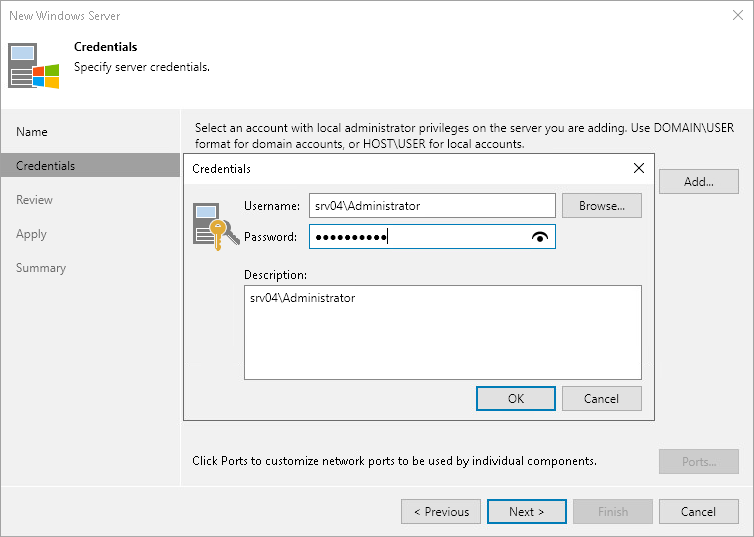
1. In the **Add Server** window, select **Microsoft Windows** to launch the **New Windows Server** wizard.
2. At the **Name** step of the wizard, specify the DNS name or IP address of the server that will perform the role of the backup repository.



1. At the **Credentials** step of the wizard, enter credentials for the user account with local Administrator permissions to the added server.

To add the account, do the following:

1. Click **Add**.
2. Specify the username and password used to connect to the added server.
3. Click **OK**.

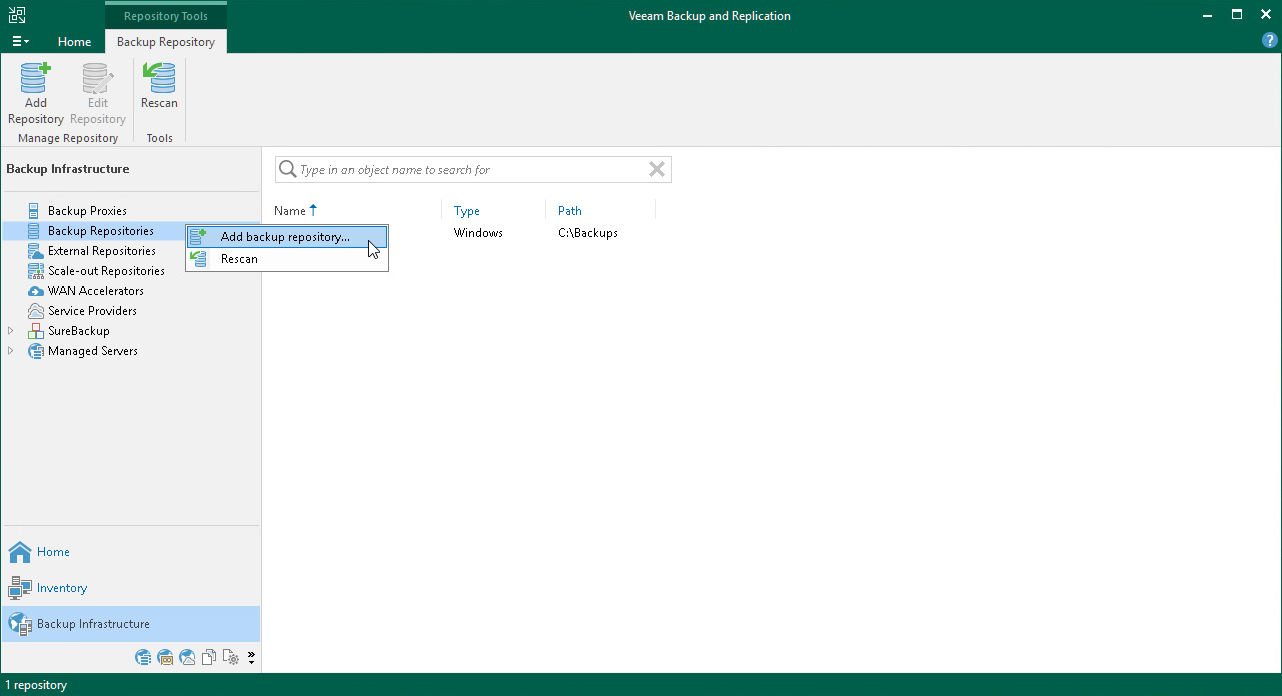


1. Follow the next steps of the wizard. At the last step of the wizard, click **Finish** to add the server.
2. Open the **Backup Infrastructure** view and click the **Managed Servers** node. The added server must be available in the working area.

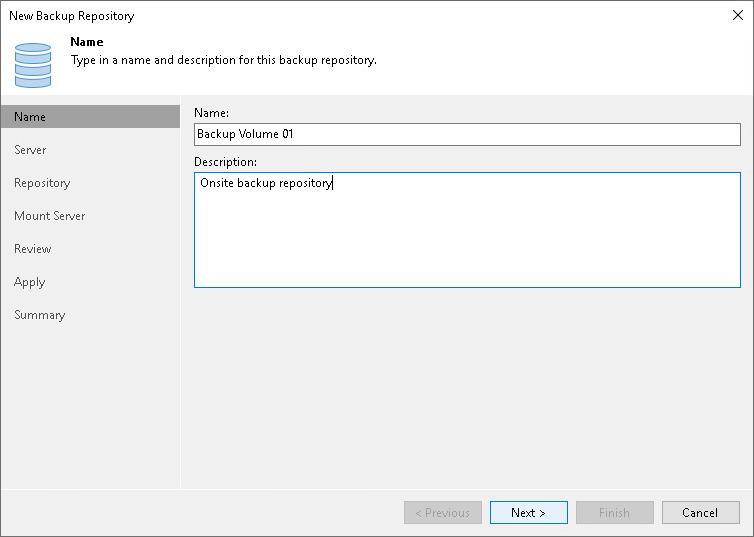
**Assigning Backup Repository Role to Added Server**

To assign the role of the backup repository:

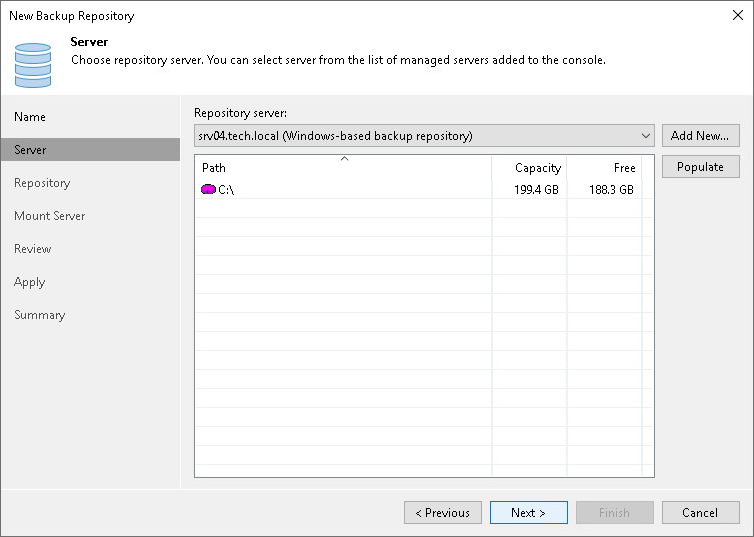
1. In the inventory pane, right-click the **Backup Repositories** node and select **Add Backup Repository** to launch the **New Backup Repository** wizard.

[](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/images/add_repo_launch.png)

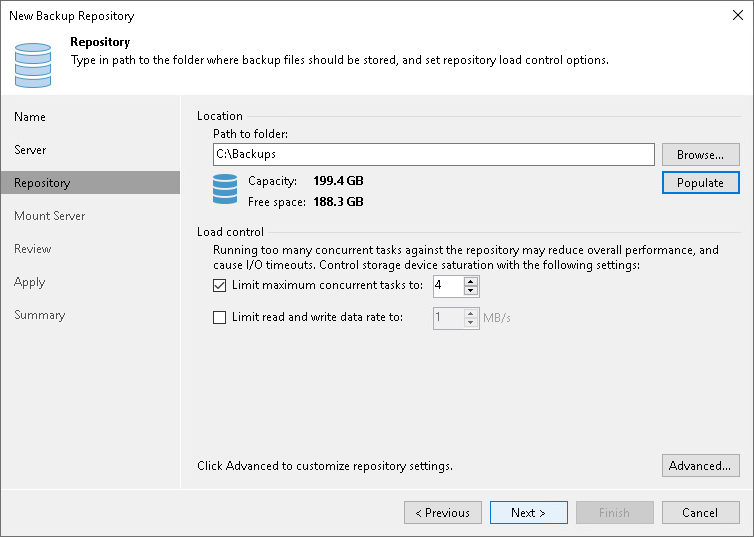
1. In the **Add Backup Repository** window, click **Direct attached storage**>**Microsoft Windows**.
2. At the **Name** step of the wizard, specify the name for the added backup repository.



1. At the **Server** step of the wizard, select the machine that you have added.



1. At the **Repository** step of the wizard, specify a path to the folder where backup files will be stored. In addition to them, auxiliary replica files will be placed in this folder.



1. At the **Mount Server** step of the wizard, keep the default settings.
2. Follow the next steps of the wizard. At the **Summary** step, click **Finish**.
3. Open the **Backup Infrastructure** view and click the **Backup Repositories** node. The added backup repository must be available in the working area.

# **Step 5. Configuring Object Storage Repositories**

On This Page

* [Before You Begin](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/setup_object_storage.html?ver=120#before-you-begin)
* [Configuring Object Storage Repository](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/setup_object_storage.html?ver=120#configuring-object-storage-repository)
* [Reference](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/setup_object_storage.html?ver=120#reference)

An object storage repository is a repository intended for long-term data storage. It can be based on either a cloud solution or an S3 compatible storage solution. Configuring an object storage repositories is an optional step.

Veeam Backup & Replication supports the following types of object storage repositories:

* S3 compatible
* Amazon S3, Amazon S3 Glacier and Amazon Snowball Edge
* Google Cloud
* IBM Cloud
* Microsoft Azure Blob, Azure Archive Storage and Azure Data Box

In this section, you will learn how to configure Amazon S3 storage system as a backup repository.

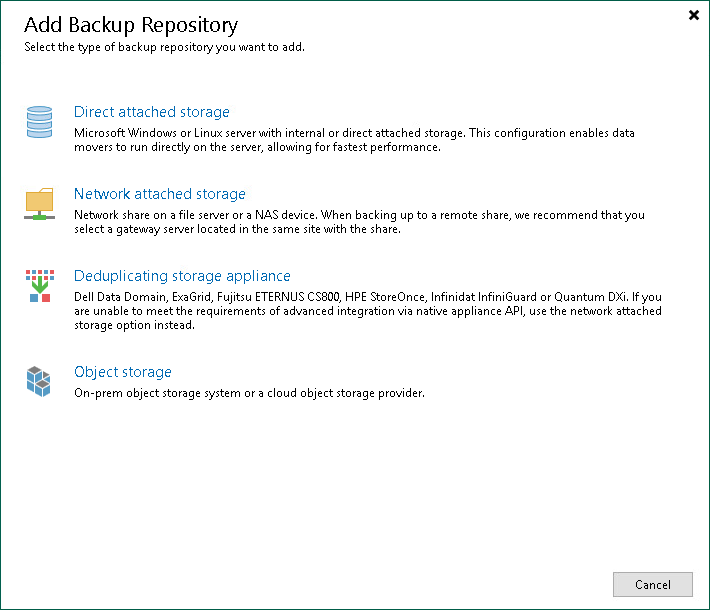
**Before You Begin**

Before you add an object storage repository, check limitations. To learn about limitations for different storage repositories, see [Considerations and Limitations](https://helpcenter.veeam.com/docs/backup/vsphere/object_storage_repository_cal.html?ver=120) in the Veeam Backup & Replication User Guide.

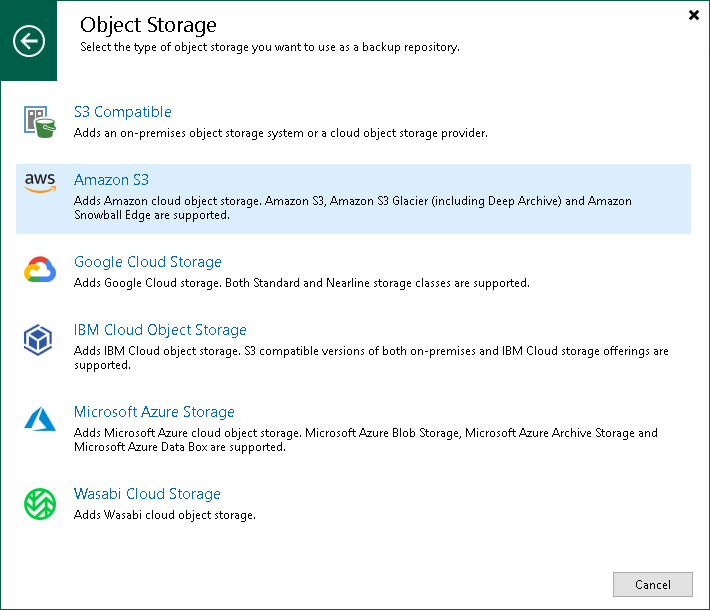
**Configuring Object Storage Repository**

To add an object storage repository to the  Veeam Backup & Replication infrastructure, do the following:

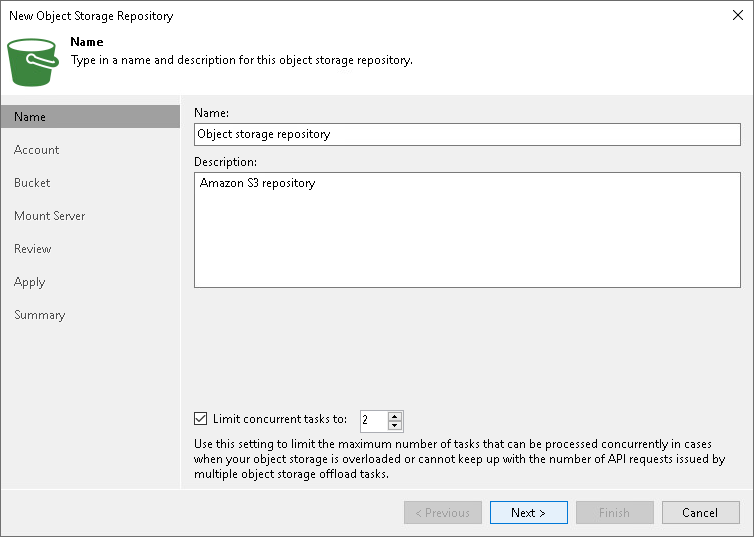
1. Open the **Backup Infrastructure** view. In the inventory pane, right-click the **Backup Repositories** node and select **Add Backup Repository**. In the **Add Backup Repository** dialog, select **Object Storage**.

[](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/images/add_backup_repository.png)

1. In the **Object Storage** dialog, select **Amazon S3**.

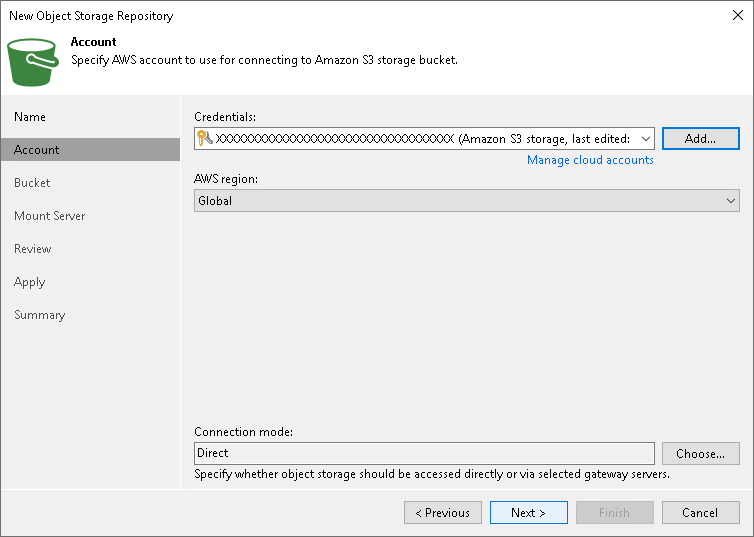
[](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/images/new_amazon_s3_storage_splash.png)

1. At the **Name** step of the wizard, specify the name and description for the object storage repository.

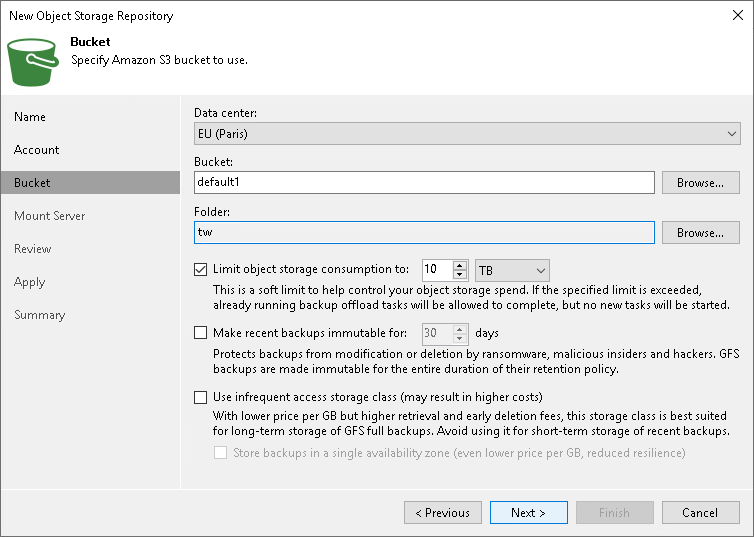


1. At the **Account** step of the wizard, specify the connection settings:
2. From the **Credentials** drop-down list, select user credentials to access your object storage. If you already have a credentials record that was configured in advance, select such a record from the drop-down list. Otherwise, click**Add** and provide your access and secret keys. For more information, see [Cloud Credentials Manager](https://helpcenter.veeam.com/docs/backup/vsphere/cloud_credentials.html?ver=120) in the Veeam Backup & Replication User Guide.
3. In the **AWS region** drop-down list, select a region type.

If your organization has NAT or different types of firewalls and your access to the internet is limited, you may want to use a gateway server. To do so, click **Choose**, select the **Through a gateway server** check box and choose a server from the list.



1. At the **Bucket** step of the wizard, specify how your data will be stored.
2. From the **Data center** drop-down list, select a region.
3. From the **Bucket** drop-down list, select a bucket. Make sure that the bucket you want to use to store your backup data was created in advance.
4. In the **Folder** field, select a cloud folder to which you want to map your object storage repository. To do it, click **Browse** and either select an existing folder or create a new one by clicking **New Folder**.
5. To define a soft limit for your object storage consumption that can be exceeded temporarily, select the **Limit object storage consumption to** check box and provide the value in TB or PB.



1. Follow the next steps of the wizard and leave the default settings. At the **Summary** step of the wizard, review the settings and click **Finish**.
2. Open the **Backup Infrastructure** view and click the **Backup Repositories** node. The added object storage repository must be available in the working area.

# **Step 6. Configuring Scale-Out Backup Repositories**

On This Page

* [Before You Begin](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/setup_sobr.html?ver=120#before-you-begin)
* [Configuring Scale-Out Backup Repository](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/setup_sobr.html?ver=120#configuring-scale-out-backup-repository)
* [Reference](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/setup_sobr.html?ver=120#reference)

A scale-out backup repository is a repository system for multi-tier storage of data, where the capacities of all the added storage devices and systems are summarized. A scale-out backup repository consists of one or more backup repositories called performance extents, and can be expanded with an object repository called capacity extent.

Configuring a scale-out backup repository is an optional step. For more information on scale-out backup repositories, see the [Scale-Out Backup Repository](https://helpcenter.veeam.com/docs/backup/vsphere/backup_repository_sobr.html?ver=120) section in the Veeam Backup & Replication User Guide.

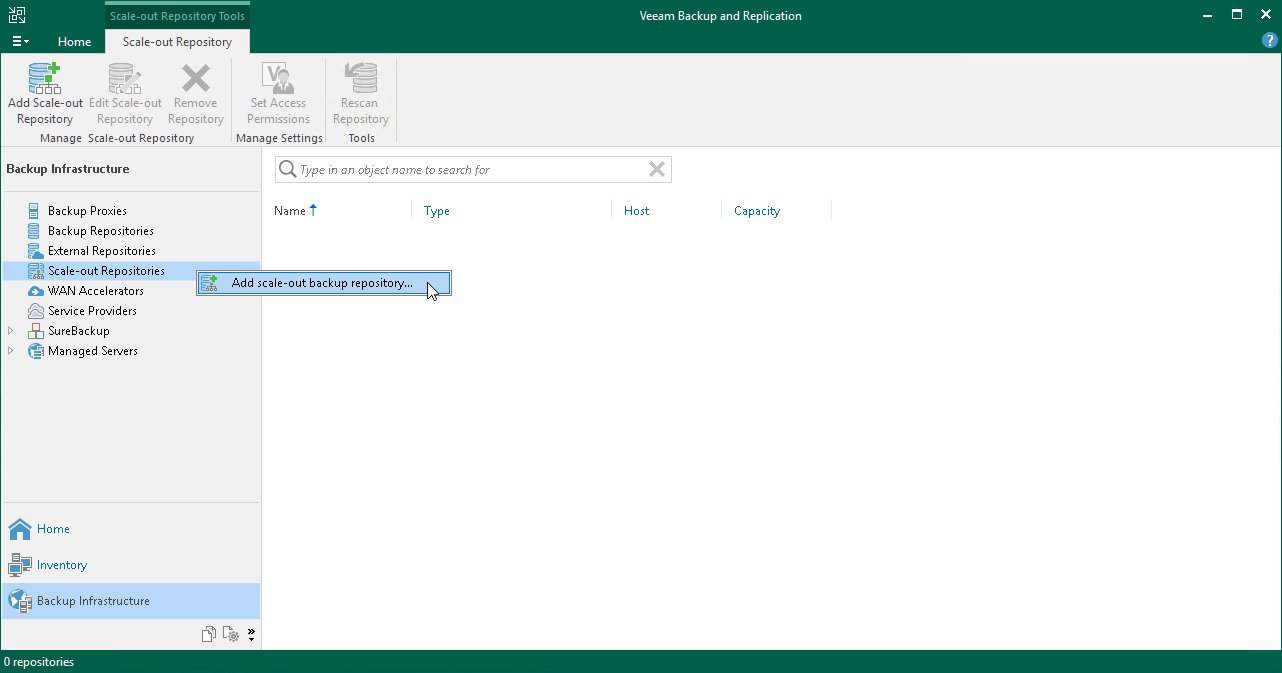
**Before You Begin**

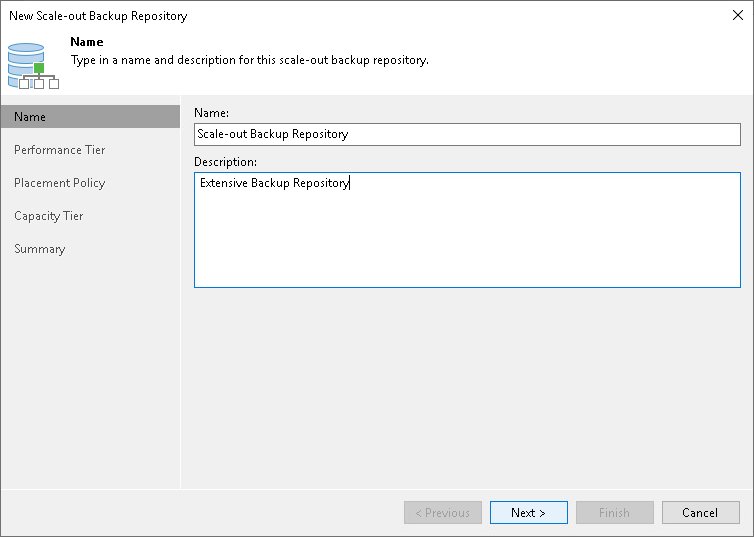
Before you add a scale-out backup repository to the backup infrastructure, check the following prerequisites:

* Backup repositories that you plan to add as performance extents to the scale-out backup repository must be added to the backup infrastructure. For more information, see [Configuring Backup Repository](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/setup_repository.html).
* If you wish to use the capacity tier option of the scale-out backup repository, an object storage repository that you plan to add as a capacity extent to the scale-out backup repository must be added to the backup infrastructure. For more information, see [Configuring Object Storage Repository](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/setup_object_storage.html).
* Check limitations for scale-out backup repositories. For more information, see [Limitations for Scale-Out Backup Repositories](https://helpcenter.veeam.com/docs/backup/vsphere/limitations-for-sobr.html?ver=120) in the Veeam Backup & Replication User Guide.

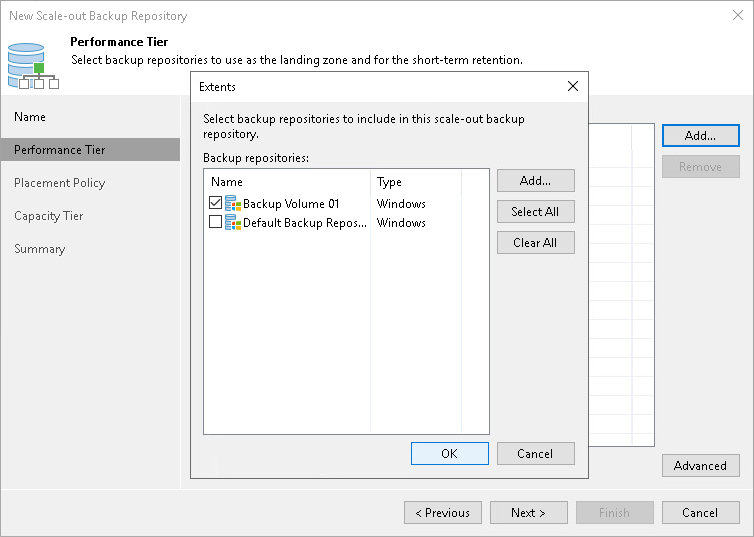
**Configuring Scale-Out Backup Repository**

To add a scale-out backup repository to the Veeam Backup & Replication infrastructure, do the following:

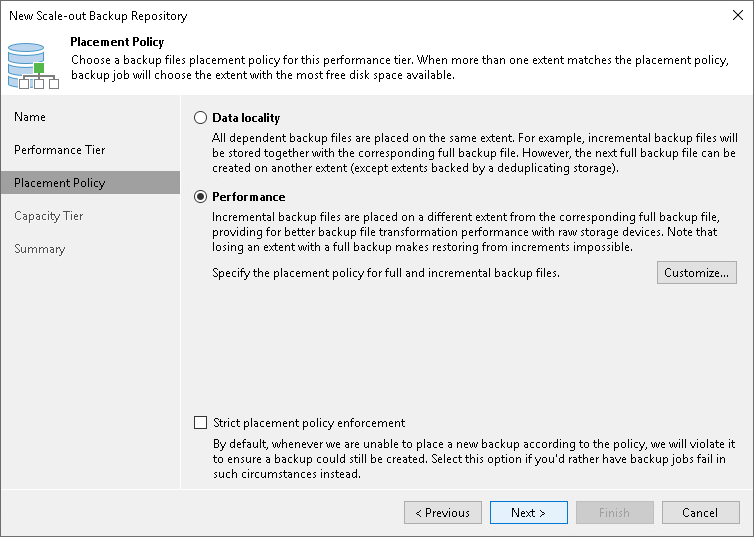
1. In the inventory pane, right-click **Scale-out Repositories** and select **Add Scale-out Backup Repository.** [](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/images/scaleout_repo_add_launch.png)
2. At the **Name** step of the wizard, specify a name and an optional description for the scale-out backup repository.



1. At the**Performance Tier** step of the wizard, specify which backup repositories you want to add as performance extents, and configure options for the scale-out backup repository. To do it, on the right side of the **Extents** list, click **Add**. In the **Extents** window, select check boxes next to backup repositories that you want to add as performance extents. Afterwards, click **OK**.



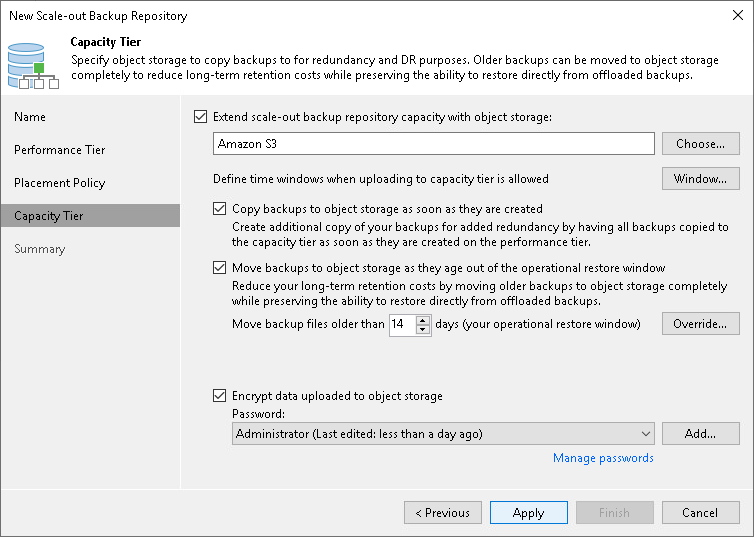
1. At the **Placement Policy** step of the wizard, select **Performance** to store full and incremental backup files at different performance extents of the scale-out backup repository.



1. At the **Capacity Tier** step of the wizard, select an object storage repository that you want to add as a capacity extent and specify when to move or copy data. This is an optional step.

To configure the capacity tier, do the following:

1. Select the **Extend scale-out backup repository capacity with object storage** check box.
2. From the drop-down list, select an object storage repository to which you want to offload your data.
3. Click **Window** and specify when it is allowed or prohibited to move or copy data to object storage.
4. Select the **Copy backups to object storage as soon as they are created** check box to copy new backups as soon as they are created.
5. Select the **Move backups to object storage as they age out of the operational restores window** check box to move inactive backup chains to the capacity extent.
6. To offload data encrypted, select the **Encrypt data uploaded to object storage** check box and provide a strong password. If you have not created the password beforehand, click **Add** or use the **Manage passwords** link to specify a new password.



1. At the **Summary** step of the wizard, review the settings and click **Finish**.
2. Open the **Backup Infrastructure** view and click the **Scale-Out Repositories** node. The added scale-out backup repository must be available in the working area.

**10 Performing Backup and Adding backup Jobs.**

# **Backup Methods**

On This Page

* [Forever Forward Incremental Backup Method](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/backup_methods.html?ver=120#forever-forward-incremental-backup-method)
* [Forward Incremental Backup Method](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/backup_methods.html?ver=120#forward-incremental-backup-method)
* [Reverse Incremental Backup Method](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/backup_methods.html?ver=120#reverse-incremental-backup-method)
* [Reference](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/backup_methods.html?ver=120#reference)

Veeam Backup & Replication provides three methods for creating backup chains:

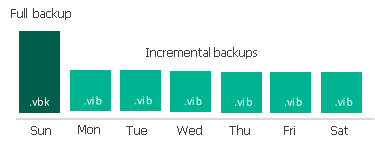
* Forever forward incremental backup
* Forward incremental backup
* Reverse incremental backup

**Forever Forward Incremental Backup Method**

The forever forward incremental backup method produces a backup chain that consists of the first full backup file (.VBK) and a set of forward incremental backup files (.VIB) following it.

During the first session of a backup job, Veeam Backup & Replication creates a full backup file on the backup repository. During subsequent backup job sessions, Veeam Backup & Replication copies only VM data blocks that have changed since the last backup job session and saves these blocks as an incremental backup file in the backup chain.

After adding a new restore point to the backup chain, Veeam Backup & Replication checks the retention policy for the job and deletes outdated restore points. For details, see [Forever Forward Incremental Backup Retention Policy](https://helpcenter.veeam.com/docs/backup/vsphere/retention_forever_incremental.html?ver=120) in the Veeam Backup & Replication User Guide.



**Forward Incremental Backup Method**

The forward incremental backup method produces a backup chain that consists of the first full backup file (.VBK) and a set of forward incremental backup files (.VIB) following it.

Additionally, the forward incremental backup chain contains full backup files that “split” the backup chain into shorter series. The subsequent full backup files can be the following:

* **Active**

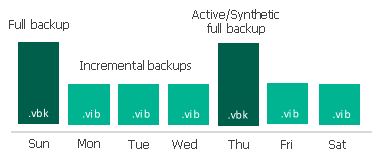
The active full backup contains the copy of a VM. This backup is similar to the full backup created when you run a job for the first time. Veeam Backup & Replication retrieves data for the whole VM from the source, compresses and deduplicates it and stores it to the active full backup file.

* **Synthetic**

The synthetic full backup also contains the copy of a VM. However, this copy is created from the backup files that you already have on the backup repository. Veeam Backup & Replication does not retrieve VM data from the source datastore.

During the first backup job session, Veeam Backup & Replication creates a full backup file. During subsequent backup job sessions, Veeam Backup & Replication copies only VM data blocks that have changed since the last backup job session and saves these blocks as an incremental backup file in the backup chain. On a day when the synthetic or active full backup is scheduled, Veeam Backup & Replication creates a full backup file and adds it to the backup chain.

After adding a new restore point to the backup chain, Veeam Backup & Replication checks the retention policy and deletes outdated restore points. For details, see [Forward Incremental Backup Retention Policy](https://helpcenter.veeam.com/docs/backup/vsphere/retention_incremental.html?ver=120) in the Veeam Backup & Replication User Guide.

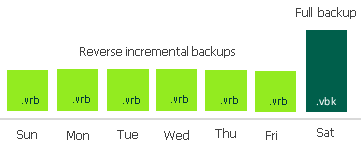


**Reverse Incremental Backup Method**

The reverse incremental backup method produces a backup chain that consists of the last full backup file (.VBK) and a set of reverse incremental backup files (.VRB) preceding it.

During the first backup job session, Veeam Backup & Replication creates a full backup file on the backup repository. During subsequent backup job sessions, Veeam Backup & Replication copies only VM data blocks that have changed since the last backup job session. Veeam Backup & Replication “injects” copied data blocks into the full backup file to rebuild it to the most recent state of the VM. Additionally, Veeam Backup & Replication saves the changed block in the reverse incremental backup file and places this file before the full backup file.

After adding a new restore point to the backup chain, Veeam Backup & Replication checks the retention policy and deletes outdated restore points. For details, see [Reverse Incremental Backup Retention Policy](https://helpcenter.veeam.com/docs/backup/vsphere/retention_reversed.html?ver=120) in the Veeam Backup & Replication User Guide.



# **Creating Backup Job**

On This Page

* [Before You Begin](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/backup_job.html?ver=120#before-you-begin)
* [Creating Backup Job](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/backup_job.html?ver=120#creating-backup-job)
* [Reference](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/backup_job.html?ver=120#reference)

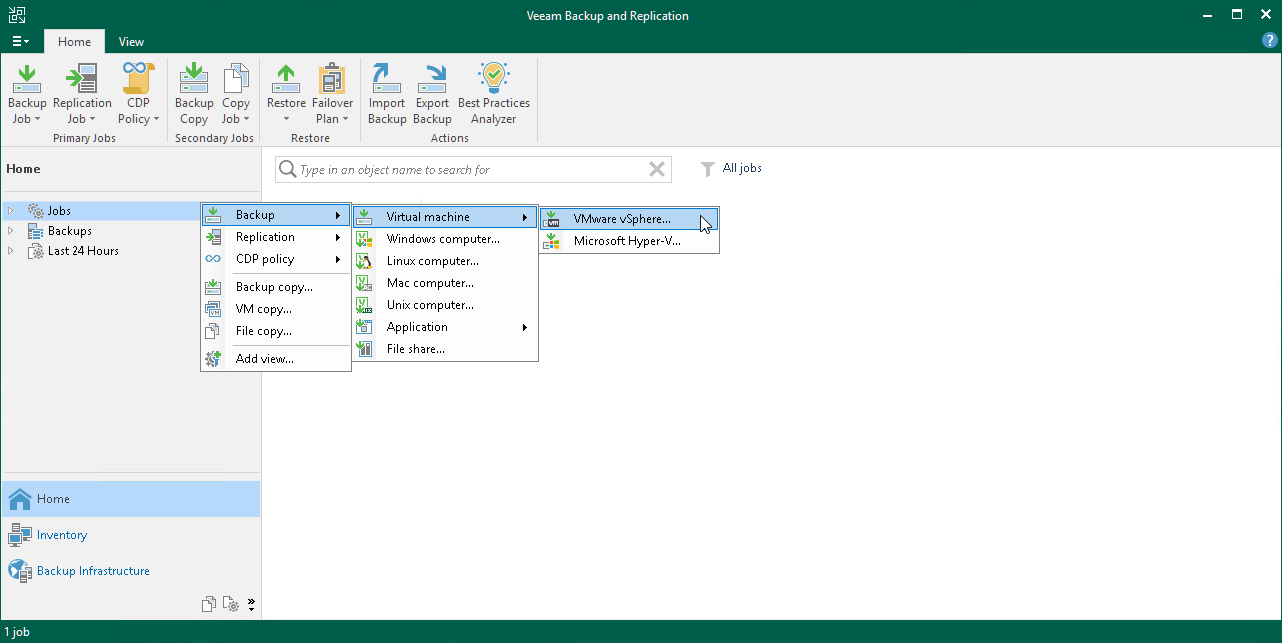
**Before You Begin**

Make sure that all backup infrastructure components that take part in the backup process are added to the backup infrastructure. These components include ESXi hosts on which VMs are registered, VMware backup proxy and backup repository.

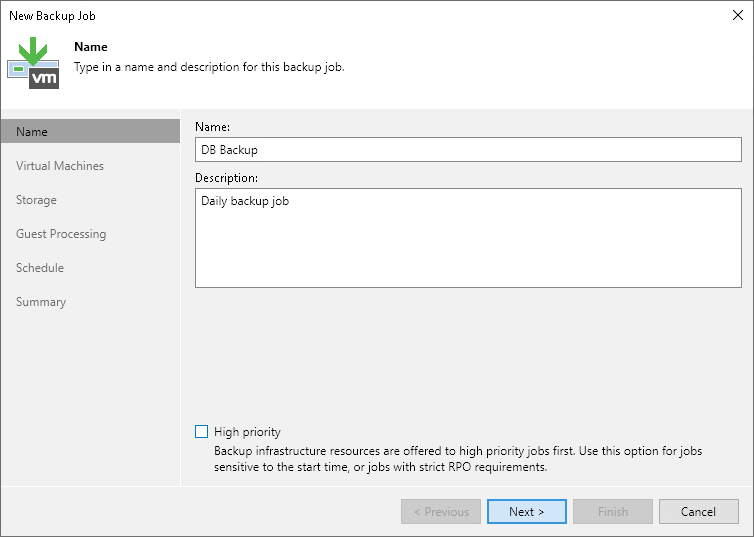
**Creating Backup Job**

To back up VMs, do the following:

1. In the inventory pane of the **Home**view, right-click **Jobs** and select **Backup**>**Virtual Machine**>**VMware vSphere** to launch the **New Backup Job** wizard.

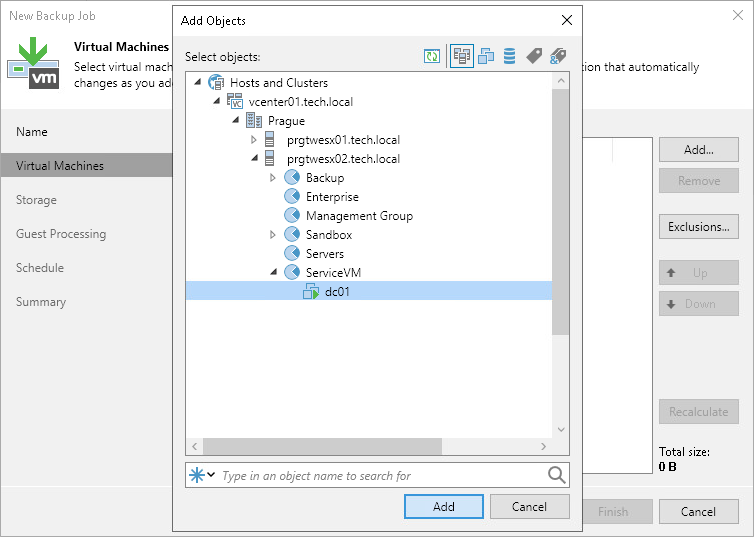
[](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/images/vm_backup_job_create.png)

1. At the **Name** step of the wizard, specify a name and description for the backup job.



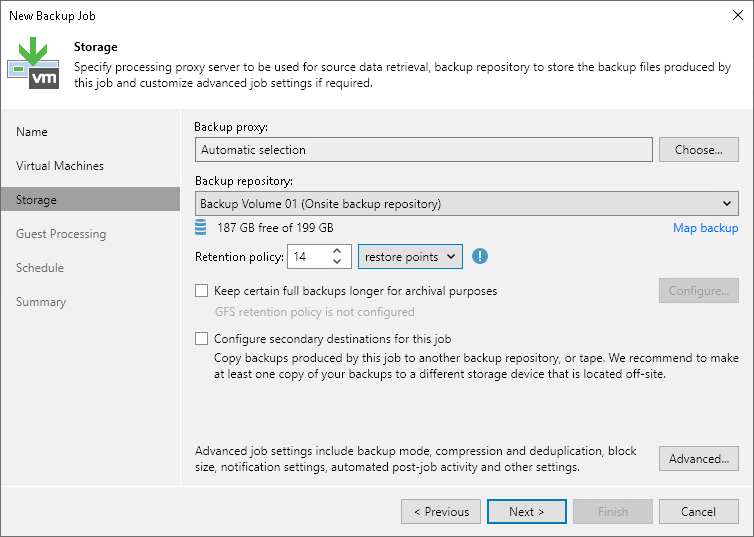
1. At the **Virtual Machines** step of the wizard, click **Add**. From the list, select VMs that you want to back up.

You can also back up VM containers: folders, resource pools, clusters, vApps, datastores and so on. If you add a new VM to the container after the backup job is created, Veeam Backup & Replication automatically updates the job to include the new VM.

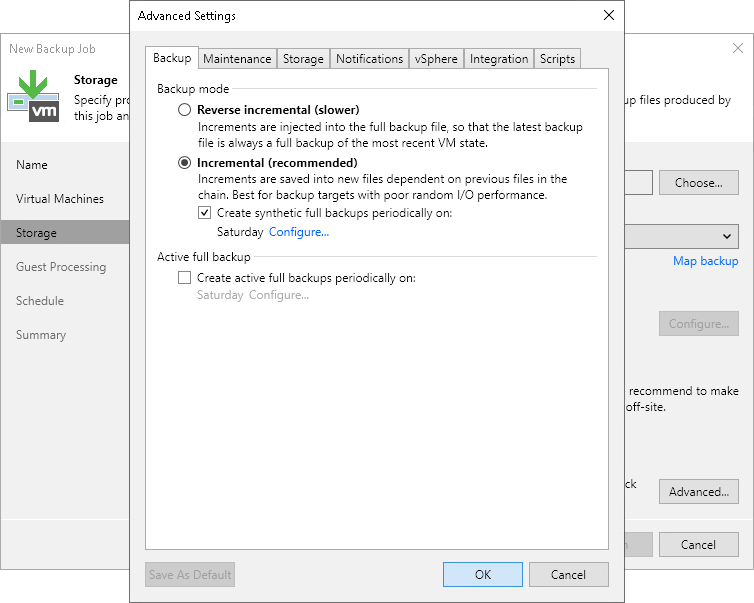


1. At the **Storage** step of the wizard, do the following:
2. From the **Backup repository** list, select the backup repository that you configured in the [Configure Backup Repository](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/setup_repository.html) section.
3. In the **Retention policy**field, define the number of restore points to keep.

When the number of restore points exceeds the allowed value, Veeam Backup & Replication automatically removes the earliest restore point from the backup chain. For more information, see [Retention Policy](https://helpcenter.veeam.com/docs/backup/vsphere/retention_policy.html?ver=120) in the Veeam Backup & Replication User Guide.



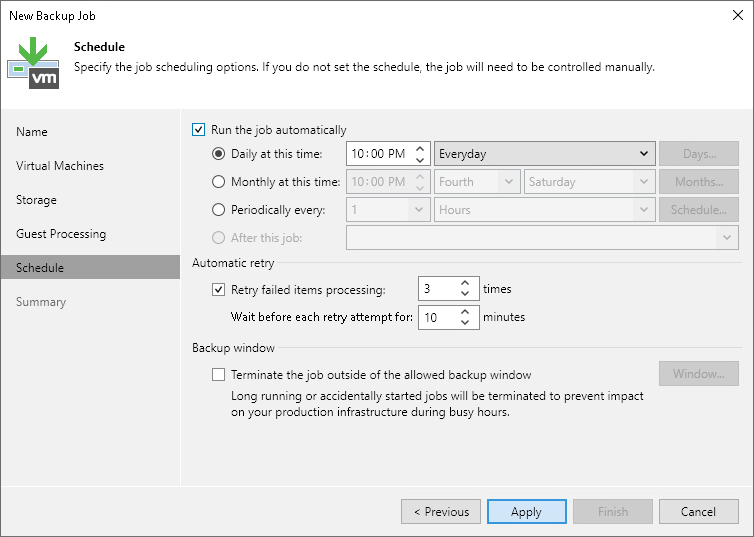
1. Click the **Advanced** button and, in the **Backup** tab, specify the backup method or leave the default settings. For details, see [Backup Methods](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/backup_methods.html).



1. At the **Guest Processing** step of the wizard, leave the default settings.

The settings of this step are detailed in the [Creating Application-Aware Backup Job](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/ms_sql_backup_job.html) section.

1. At the **Schedule** step of the wizard, do the following:
2. Select the **Run the job automatically** check box. If you do not select this check box, you will have to launch the job manually. For details, see [Start Backup Job Manually](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/backup_job_incremental.html).
3. Select the schedule type: daily, monthly or periodically.
4. Make sure the **Retry failed VM processing** check box is selected.
5. Click **Apply**.

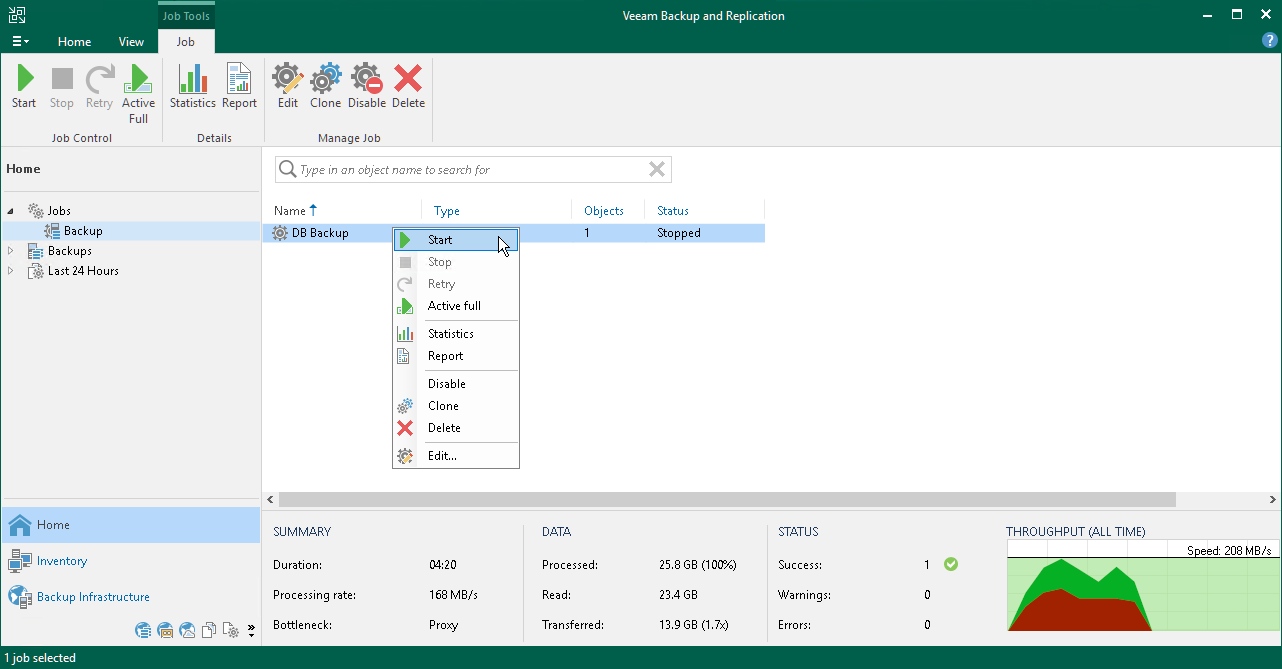


1. At the **Summary** step of the wizard, select the **Run the job when I click Finish** check box and click the **Finish** button.
2. In the inventory pane of the**Home** view, expand the **Last 24 Hours** node to see the created job.

# **Start Backup Job Manually**

If you do not schedule a backup job, you must start it manually. To start the job, do the following:

1. Open the **Home** view.
2. In the inventory pane, select the **Jobs** node.
3. In the working area, right-click the job and select **Start**. Wait for the job to complete. Note that the job must complete with the *Success* or *Warning* status.

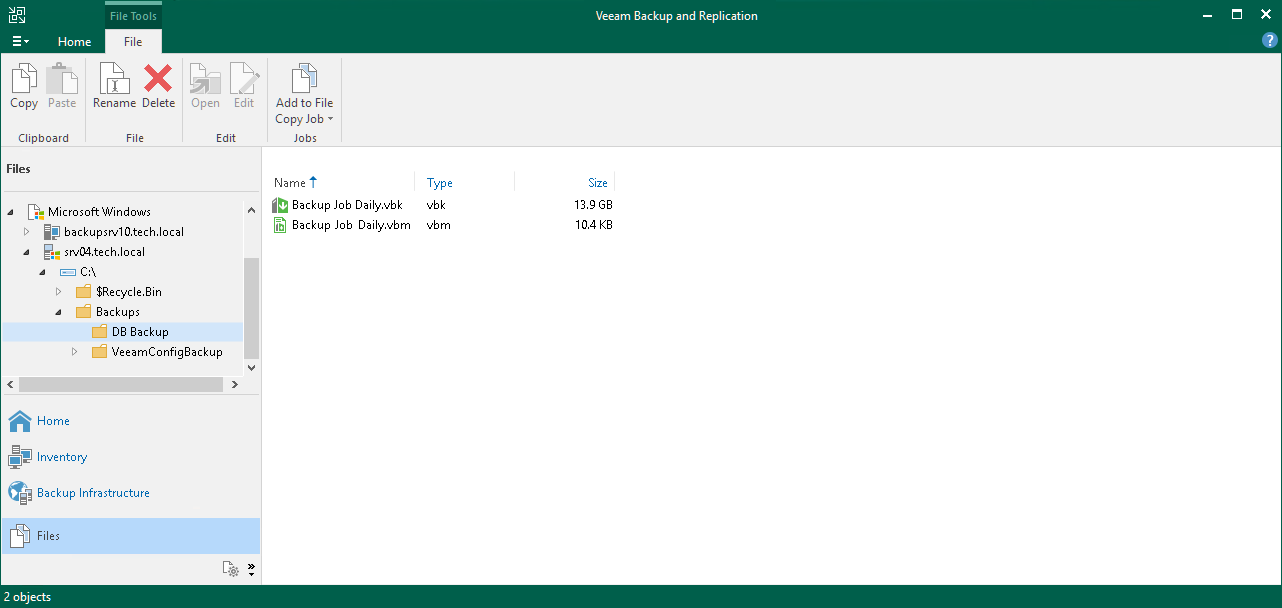
[](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/images/backup_job_incremental.png)

# **Locating Backup Files**

When a backup job finishes, Veeam Backup & Replication saves backup files in the backup repository that you specified as a backup target.

To locate backup files using the Veeam Backup & Replication console, do the following:

1. Open the **Files** view.
2. In the inventory pane, expand the backup repository file tree and open the **Backup** folder.
3. In the **Backup** folder, find the subfolder with the backup job name and open it. It must contain a .VBK and .VBM files. If the job was run several times, the subfolder also contains .VIB or .VRB files.

[](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/images/backup_job_validate.png)

# **Creating Application-Aware Backup Job**

On This Page

* [Before You Begin](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/ms_sql_backup_job.html?ver=120#before-you-begin)
* [Creating Application-Aware Backup](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/ms_sql_backup_job.html?ver=120#creating-application-aware-backup)
* [Reference](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/ms_sql_backup_job.html?ver=120#reference)

Application-aware processing allows you to create transactionally consistent backups. These backups allow you to further restore application items: emails for mail agents, tables for DB servers, accounts for domain controllers.

Veeam Backup & Replication can create transactionally consistent backups of VMs that run the following applications:

* Microsoft Exchange
* Active Directory
* SharePoint
* SQL Server
* Oracle Database

In this section, you will learn how to create the application-aware backup job for a Microsoft SQL Server.

|  |
| --- |
| **IMPORTANT!** |
| Application-aware processing is supported only for the applications listed above and VSS-aware applications. If an application that you want to back up is not supported, you can use VMware Tools quiescence with pre-freeze and post-thaw scripts. For more information, see [VMware Tools Quiescence](https://helpcenter.veeam.com/docs/backup/vsphere/tools_quiescence.html?ver=120) and [Pre-Freeze and Post-Thaw Scripts](https://helpcenter.veeam.com/docs/backup/vsphere/pre_post_scripts.html?ver=120) in the Veeam Backup & Replication User Guide. |

**Before You Begin**

Make sure that the version of your Microsoft SQL Server is supported. For details, see the [System Requirements](https://helpcenter.veeam.com/docs/backup/vsphere/system_requirements.html?ver=120) section in the Veeam Backup & Replication User Guide.

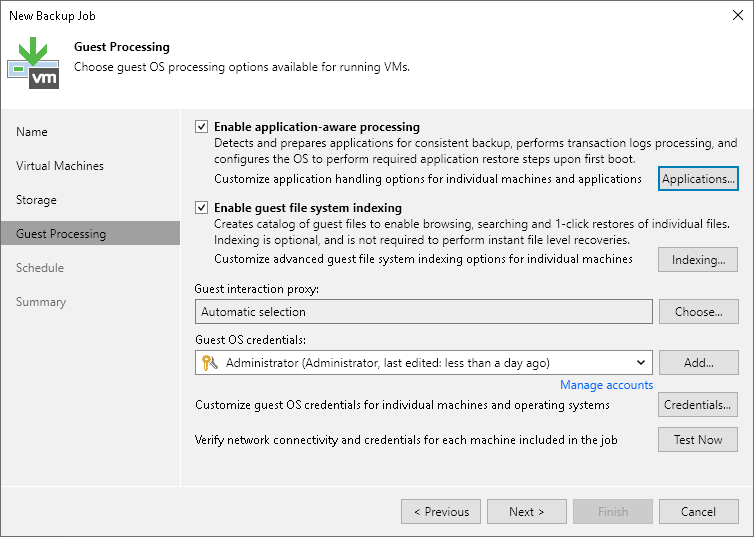
**Creating Application-Aware Backup**

To create the application-aware backup job for the Microsoft SQL Server, do the following:

1. In the inventory pane of the **Home**view, right-click **Jobs** and select **Backup**> **Virtual Machine**>**VMware vSphere** to launch the **New Backup Job** wizard.
2. At the **Name** step of the wizard, specify a name and description for the backup job.
3. At the **Virtual Machines** step of the wizard, select the VM.
4. At the **Storage** step of the wizard, select a backup repository or keep the default settings.
5. At the**Guest Processing** step of the wizard, do the following:
6. Select the**Enable application-aware processing** check box.
7. Select the **Enable guest file system indexing** check box.

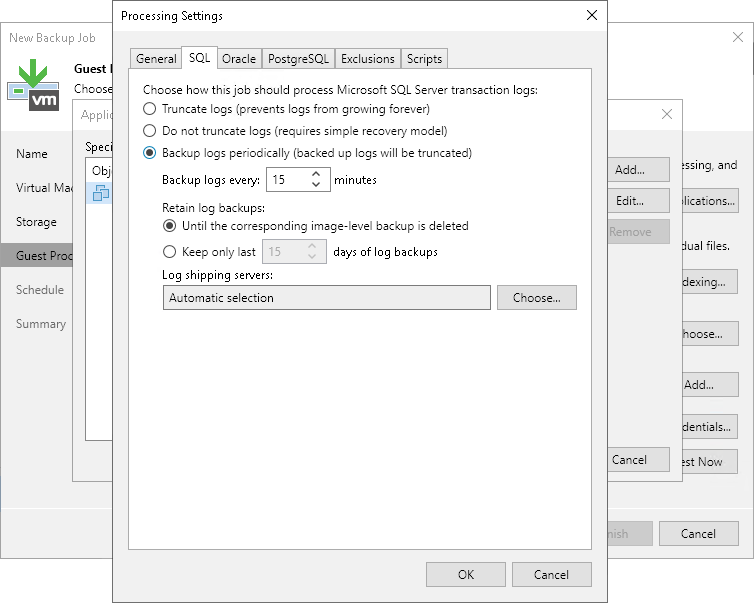
VM guest OS file indexing allows you to search for VM guest OS files inside VM backups and perform 1-click restore in Veeam Backup Enterprise Manager. For details, see [VM Guest OS File Indexing](https://helpcenter.veeam.com/docs/backup/vsphere/backup_job_vss_indexing_vm.html?ver=120) in the Veeam Backup & Replication User Guide.

1. In the **Guest OS credentials** section, specify credentials of a user account to connect to the VM guest OS. The user account must have Administrator permissions on the Microsoft SQL Server.
2. Click the **Applications** button at the top of the window.

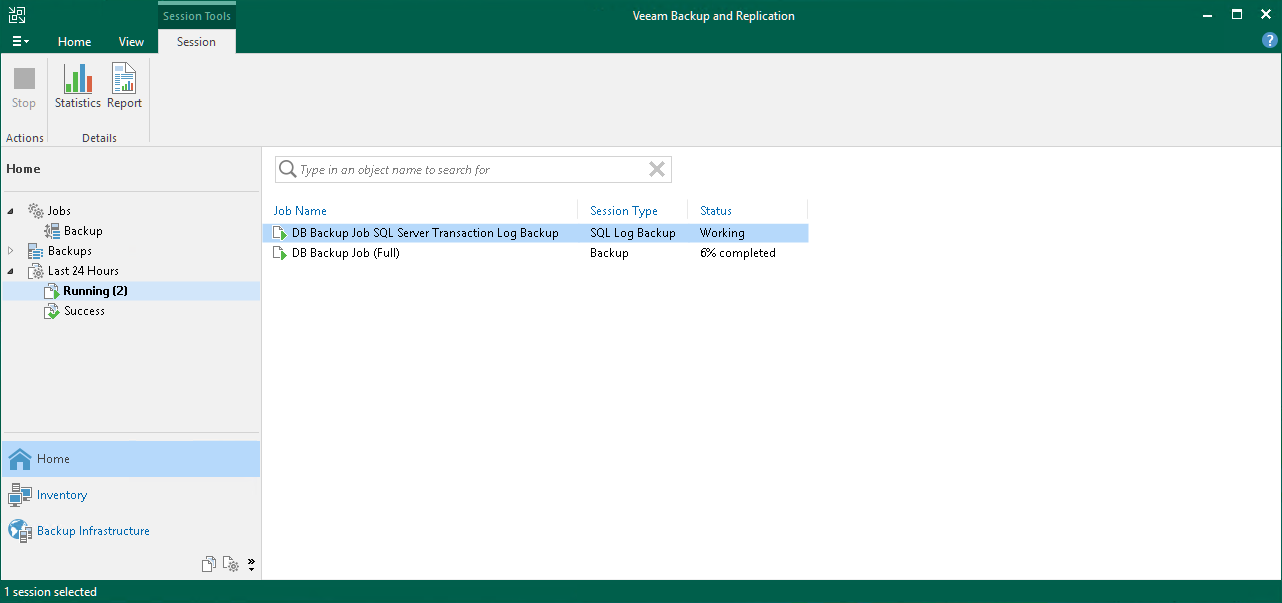


1. In the opened window, select the Microsoft SQL Server from the list and click **Edit**.
2. In the **Processing Settings** windows, do the following:
3. In the **VSS Settings** section of the **General** tab, check that the **Process transaction logs with this job** option is selected.
4. On the **SQL** tab, select **Backup logs periodically** option.

Veeam Backup & Replication will create an auxiliary job that runs continuously and ships database transaction logs. Transaction logs are shipped to the backup repository and saved in .VLB files next to other backup job files. Thus, you have a chain of restore points and a set of transaction logs that cover intervals between these restore points.



1. At the **Schedule** step of the wizard, define scheduling settings for the job.
2. At the **Summary** step of the wizard, select the **Run the job when I click Finish** check box and click the **Finish** button.
3. In the inventory pane of the**Home** view, expand the **Last 24 Hours** node to see the created jobs. You must see two jobs: one that processes the Microsoft SQL Server and the other one that ships transaction logs.

[](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/images/sql_backup_stats.png)

# **Backup Copy**

On This Page

* [Before You Begin](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/backup_copy.html?ver=120#before-you-begin)
* [Creating Backup Copy Job](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/backup_copy.html?ver=120#creating-backup-copy-job)
* [Reference](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/backup_copy.html?ver=120#reference)

Backup copy allows you to create several instances of the same backup data in different locations. This is the mechanism that Veeam Backup & Replication provides to help you follow the the 3-2-1 rule:

* 3: You must have at least three copies of your data: the original production data and two backups.
* 2: You must use at least two different types of media to store copies of your data, for example, local disk and cloud.
* 1: You must keep at least one backup offsite (for example, in the cloud or in a remote site).

In Veeam Backup & Replication, backup copy is a job-driven process. When the backup copying job starts, Veeam Backup & Replication accesses backup files on the source backup repository, retrieves data blocks for a specific machine from the backup file, copies them to the target backup repository, and composes copied blocks into a backup file on the target backup repository. This backup file has the same format as the primary backup file.

**Before You Begin**

Before you create a backup copy job, consider the following:

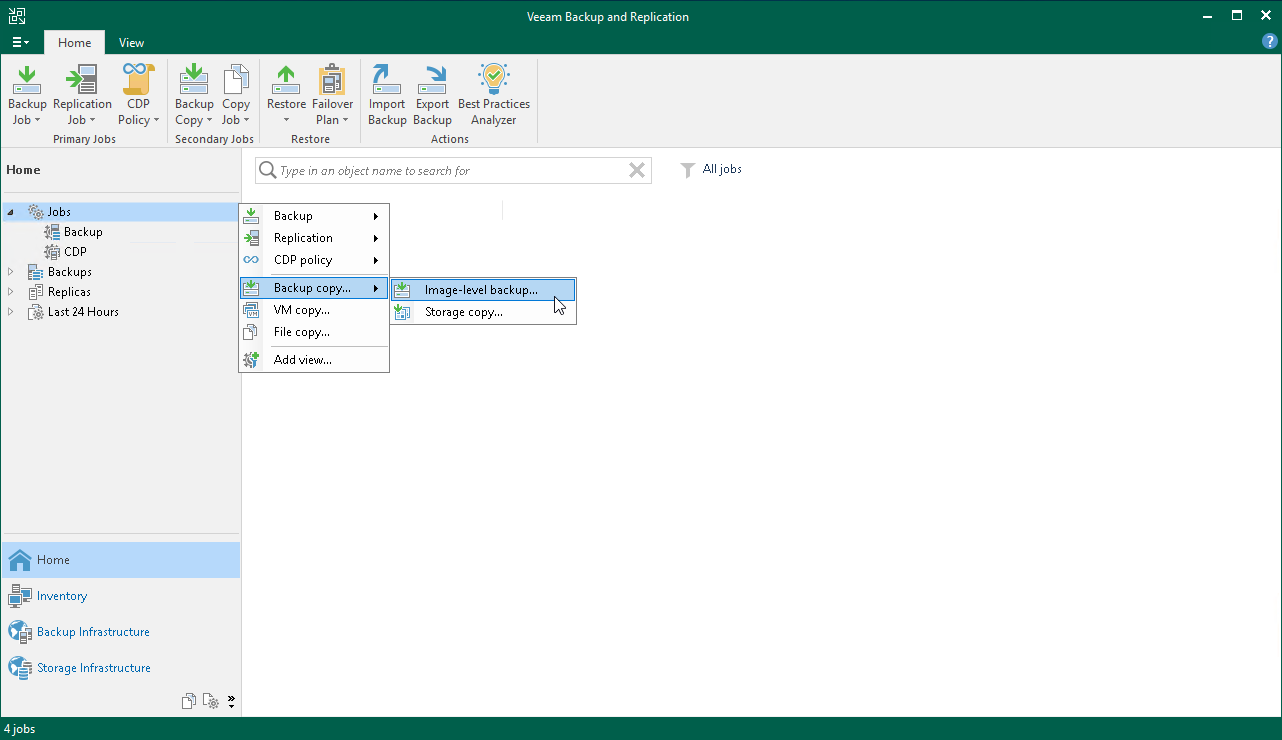
* The source and target backup repositories that take part in the backup copy process must be added to the backup infrastructure.
* You must have a backup that has been successfully run at least once.

To check whether restore points are created, open the inventory pane of the **Home** view and select the **Backups** node. Then, expand the backup job and verify that there is at least one restore point available.

**Creating Backup Copy Job**

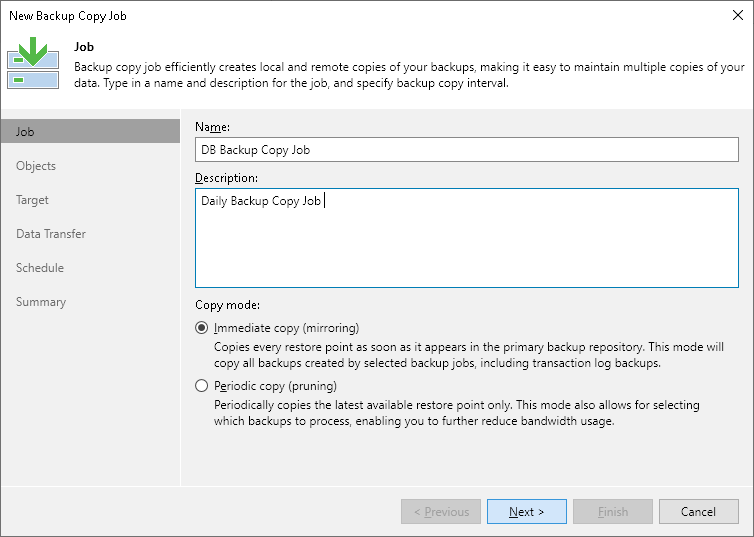
To create a backup copy job, do the following:

1. Open the **Home** view.
2. In the inventory pane, right-click **Jobs** and select **Backup Copy**>**Image-level backup** to launch the **New Backup Copy Job** wizard.

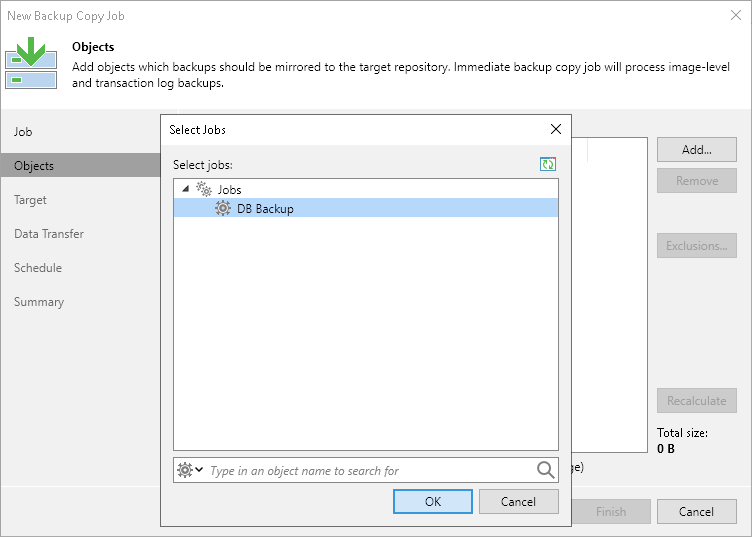
[](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/images/backup_copy_launch.png)

1. At the **Job** step of the wizard, do the following:
2. Specify a name and description for the backup copy job.
3. In the **Copy mode** field, check that the **Immediate copy** is selected.

In the immediate copy mode, Veeam Backup & Replication copies new data as soon as it appears on the source repository. For more information, see [Backup Copy Modes](https://helpcenter.veeam.com/docs/backup/vsphere/backup_copy_modes.html?ver=120) in the Veeam Backup & Replication User Guide.



1. At the **Objects** step of the wizard, click **Add** and select backup jobs that you want to copy.



1. At the **Target** step of the wizard, select the backup repository where you want to store the backup copy. For other settings, keep the default values.



1. At the **Data Transfer** step of the wizard, keep the default settings.
2. At the **Schedule** step of the wizard, define the period of time when the backup copy job is allowed to transport data over the network.
3. At the last step of the wizard, select the **Enable the job when I click Finish** check box and click **Finish**. The job will start running in the continuous mode.

# **Creating Replication Job**

On This Page

* [Before You Begin](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/replication_job.html?ver=120#before-you-begin)
* [Creating Replication Job](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/replication_job.html?ver=120#creating-replication-job)
* [Reference](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/replication_job.html?ver=120#reference)

**Before You Begin**

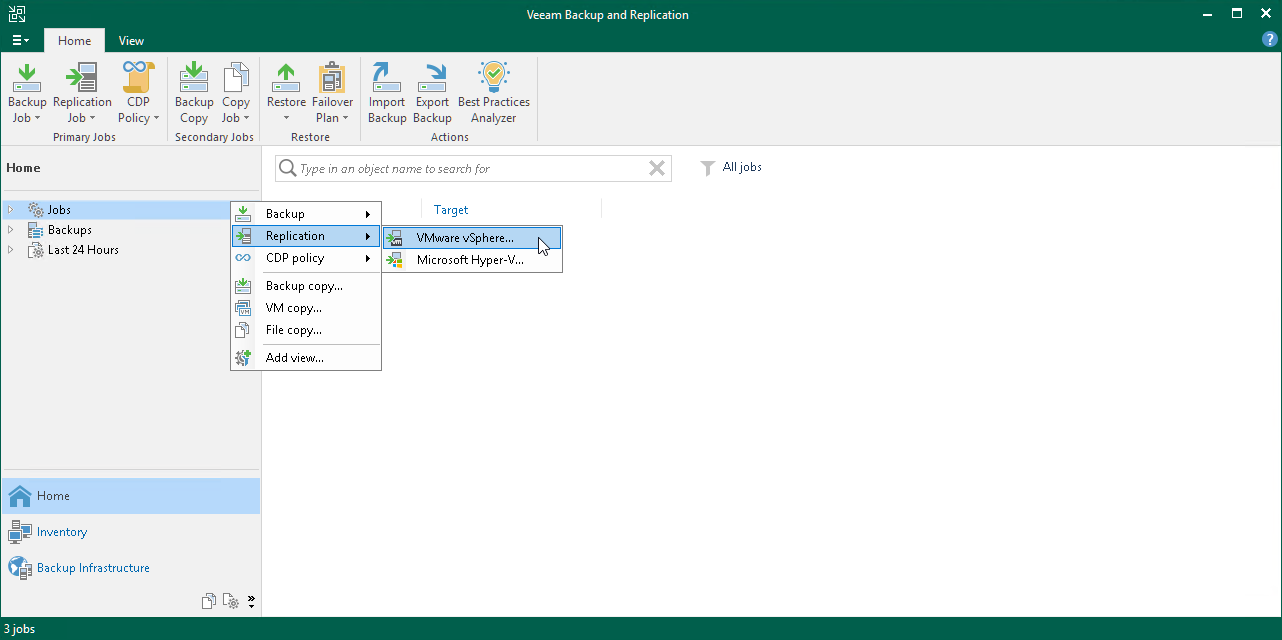
Before you replicate a VM, consider the following:

* You must add all components needed for the replication process to the backup infrastructure. These components are source and target ESXi hosts, VMware backup proxy and backup repository.
* Due to VMware vSphere limitations, if you change the size of VM disks on the source VM, Veeam Backup & Replication deletes all available restore points on the VM replica during the next replication job session. For more information, see [this Veeam KB article](https://kb.vmware.com/s/article/1004047).

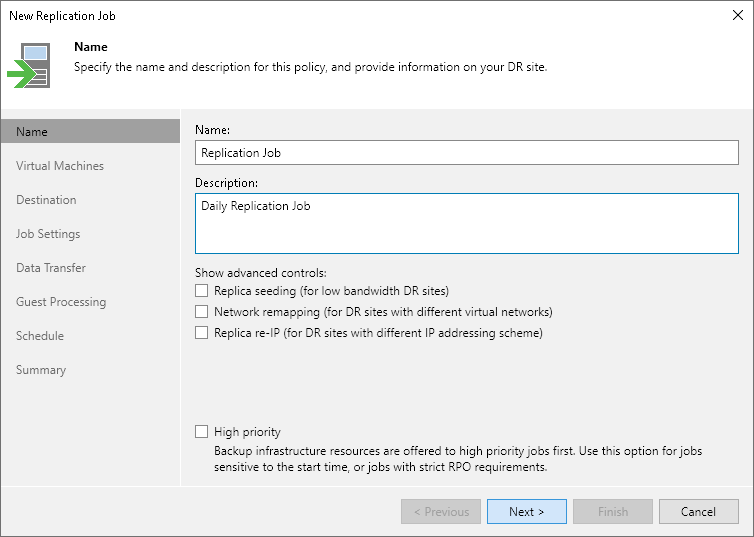
**Creating Replication Job**

To replicate a VM, do the following:

1. Open the **Home** view.
2. In the inventory pane of the **Home** view, right-click the **Jobs** node and select **Replication** > **Virtual machine** > **VMware vSphere** to launch the **New Replication Job** wizard.

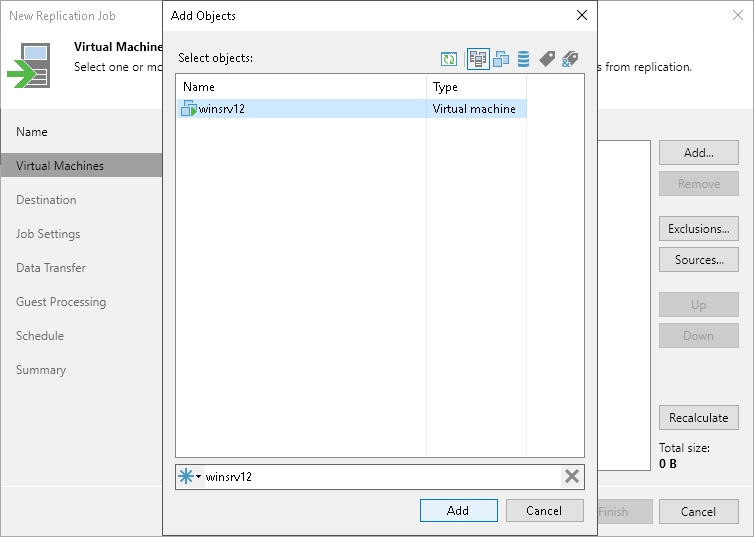
[](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/images/vm_replica_job_launch.png)

1. At the **Name** step of the wizard, specify a name and description for the replication job. For other settings, leave the default values.

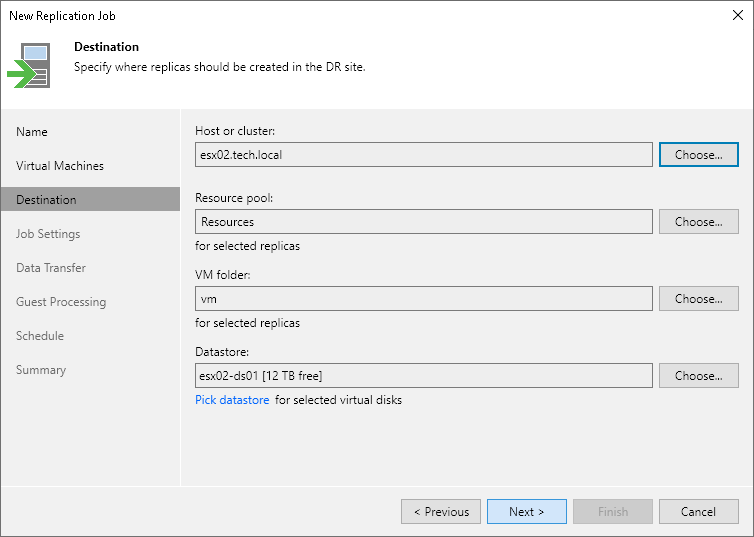


1. At the **Virtual Machines** step of the wizard, click **Add**. From the list, select VMs that you want to replicate.

You can also replicate VM containers: folders, resource pools, clusters, vApps, datastores and so on. If you add a new VM to the container after the replication job is created, Veeam Backup & Replication automatically updates the job to include the new VM.



1. At the **Destination** step of the wizard, do the following:
2. Click **Choose** next to the **Host or cluster** field and select a host on which the VM replica must be registered.
3. Click **Choose** next to the**Resource pool** field and select the target resource pool.
4. Click **Choose** next to the **VM folder** field and select the folder in which the replica must be placed.
5. Click **Choose** next to the **Datastore** field and select a datastore where VM replica files must be stored.



1. At the **Job Settings** step of the wizard, do the following:
2. In the **Repository for replica metadata** list, select the backup repository where you want to store the metadata file.
3. In the **Replica name suffix** field, specify the suffix that will be appended to the name of the original VM.
4. In the **Restore points to keep** field, define the number of restore points to keep.

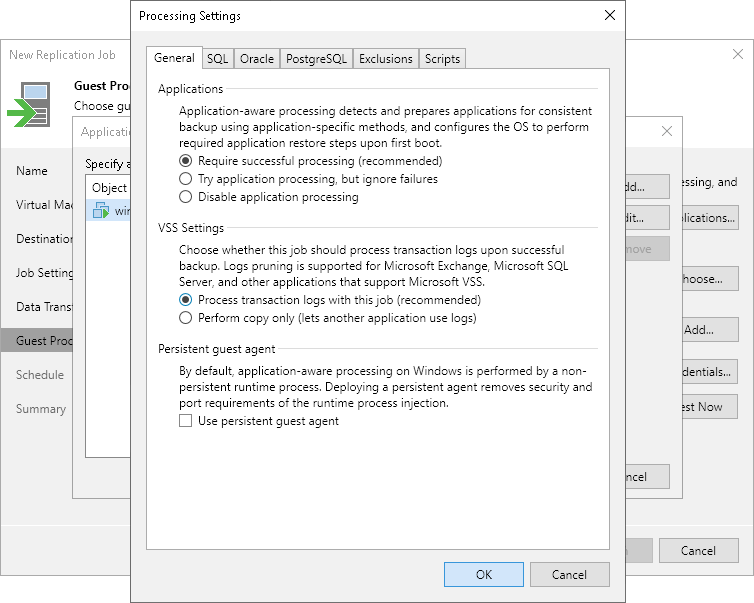
When this number is exceeded, the earliest restore point is removed. Due to VMware restrictions, the maximum number of restore points for VM replicas is limited to 28.



1. At the **Data Transfer** step of the wizard, leave the default settings.
2. At the **Guest Processing** step of the wizard, leave the default settings if you do not need transactionally consistent replicas. Otherwise, select the **Enable application-aware processing** check box and specify credentials of a user account to connect to the VM guest OS. The user account must have Administrator permissions.

To specify advanced options for VSS processing, click **Applications**. Select a VM in the list and click **Edit**. In the opened window on the **General** tab, do the following:

1. In the **Applications** section, select **Try application processing, but ignore failures** to continue the replication job even if VSS errors occur. If VSS processing fails, the created replica will not be transactionally consistent but crash consistent.
2. In the **Transaction logs** section, check that the **Process transaction logs with this job** option is selected.



1. At the **Schedule** step of the wizard, do the following:
2. Select the **Run the job automatically** check box. If you do not select this check box, you will have to launch the job manually. For details, see [Start Replication Job Manually](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/replication_job_incremental.html).
3. Select the schedule type: daily, monthly or periodically.

In the **Periodically every** field, you can select **Continiously** to run the job in a non-stop manner. A new session of the job will start as soon as the previous job session completes.

1. Make sure the**Retry failed VM processing** check box is selected.

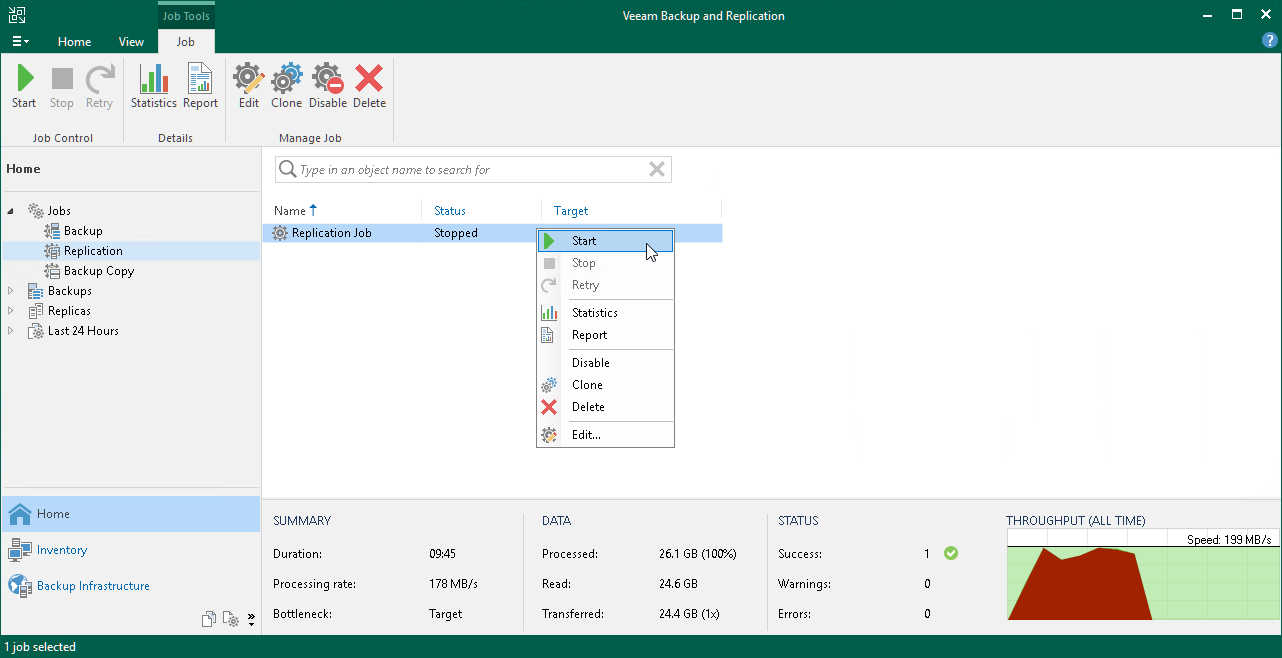


1. At the **Summary** step of the wizard, select the **Run the job when I click Finish** check box and click the **Finish** button.
2. In the inventory pane of the **Home** view, expand the **Last 24 Hours** node to see the created job.
3. Open **vSphere Client** and make sure that the replica appeared on the target host.

# **Start Replication Job Manually**

If you do not schedule a replication job, you must start it manually. To start the job, do the following:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs** > **Replication**.
3. In the working area, right-click the job and select **Start**. Wait for the job to complete. Note that the job must complete with the *Success* or *Warning* status.
4. Open **vSphere Client** and make sure that a VM replica is created.

[](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/images/replication_job_incremental.png)

# **Replica Failover and Failback**

If the original VM in the production site becomes unavailable, you can quickly restore services by failing over to its replica. When you perform failover, the VM replica takes the role of the original VM. All processes shift from the original VM on the production host to the VM replica on the secondary host. You can fail over to the latest state of a replica or to any of its restore points.

When you fail over to the VM replica, Veeam Backup & Replication changes the replica state from *Normal* to *Failover*.

Failover is an intermediate step that needs to be finalized. Depending on a disaster recovery scenario, you can do one of the following:

* **Undo failover**

When you undo failover, you switch back to the original VM and discard all changes made to the VM replica while it was running. The state of the VM replica gets back to *Normal*. You can use the undo failover scenario if you have failed over to the VM replica for testing and troubleshooting purposes and you do not need the changes made to the VM replica.

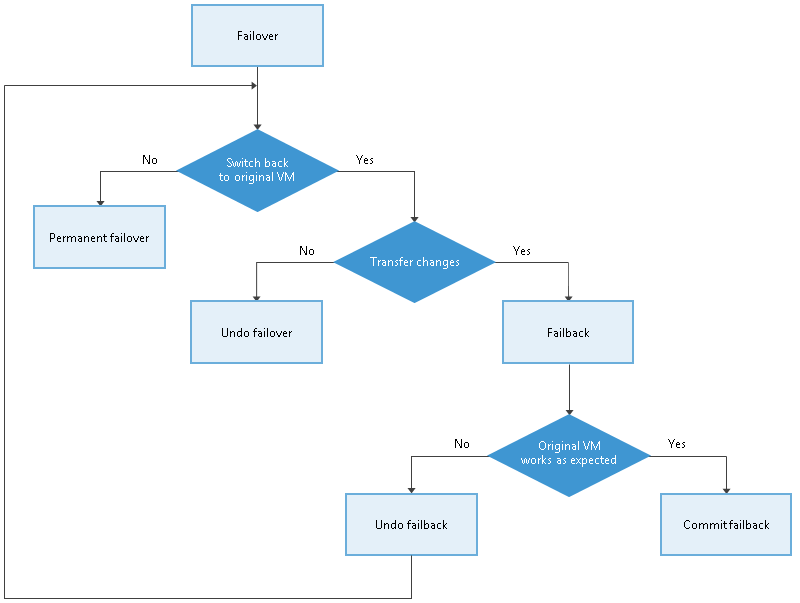
* **Perform failback**

When you perform failback, you switch back to the original VM and transfer all changes that took place while the VM replica was running to the original VM. If the source host is not available, you can restore the original VM to a new location and switch back to it.

When you perform failback, changes are only transferred but not published. You must test whether the original VM works with these changes. Depending on the test results, you can do the following:

* **Commit failback**. When you commit failback, you confirm that the original VM works as expected and you want to get back to it. The state of the VM replica gets back to *Normal*.
* **Undo failback**. If the original VM is not working as expected, you can undo failback and get back to the VM replica. In this case, the state of the VM replica returns to *Failover*.
* **Perform permanent failover**

When you perform failover, you permanently switch from the original VM to a VM replica and use this replica as the original VM. This scenario is acceptable if the original VM and VM replica are located in the same site and are nearly equal in terms of resources.

[](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/images/failover_schema.png)

Veeam Backup & Replication supports failover and failback operations for several VMs simultaneously. In case one or several hosts fail, you can use batch processing to restore operations with minimum downtime.

# **Performing Replica Failover**

On This Page

* [Before You Begin](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/replica_failover.html?ver=120#before-you-begin)
* [Performing Failover](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/replica_failover.html?ver=120#performing-failover)
* [Reference](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/replica_failover.html?ver=120#reference)

**Before You Begin**

Before you perform failover, consider the following:

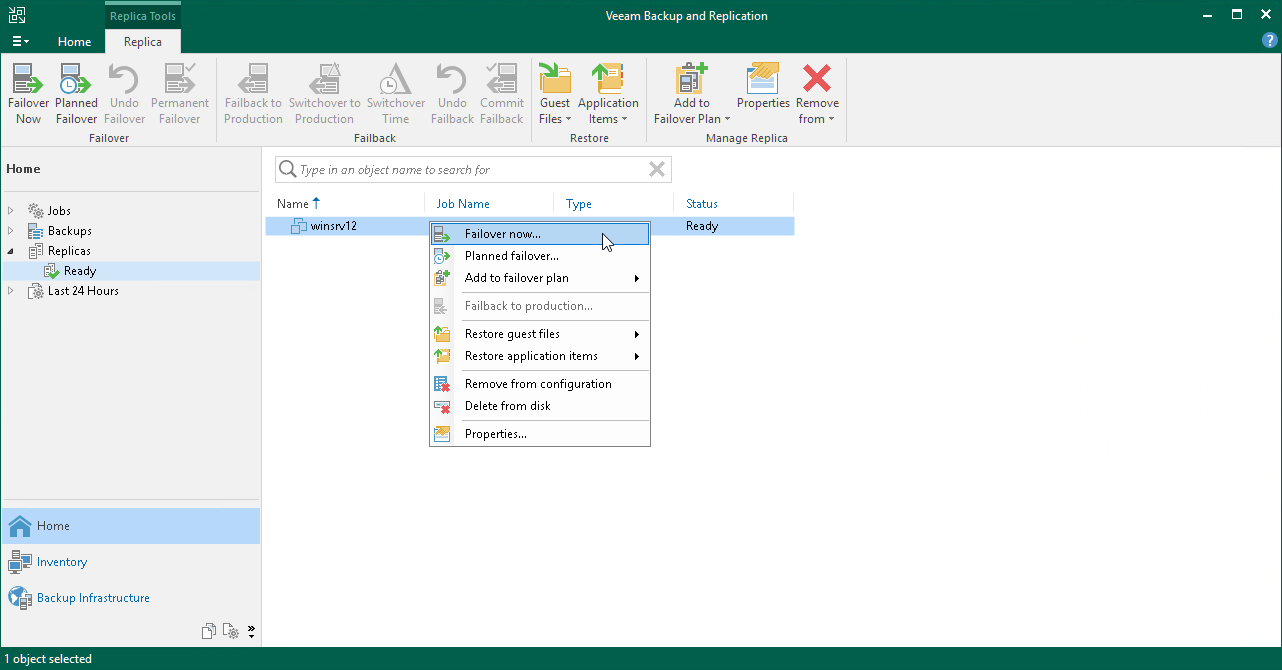
* For original VMs and replica VMs located in the same network. If you plan to perform replica failover while the original VM is running, consider temporarily disconnecting the original VM from the network to avoid IP addresses or machine names conflicts.
* To successfully fail over to a VM replica, make sure that this replica has at least one successfully created restore point.

To check whether restore points are created, open the inventory pane of the **Home** view and select the **Replicas** node. Then, select the VM and verify that there is at least one restore point available for the VM.

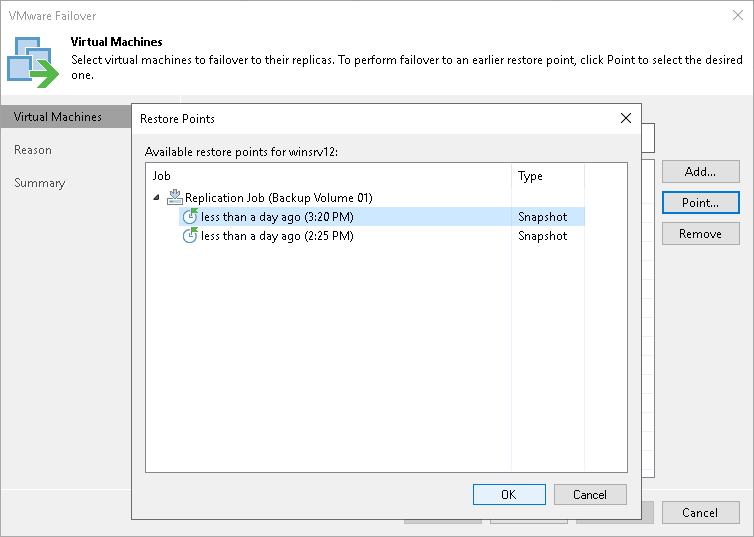
**Performing Failover**

To fail over to a VM replica, do the following.

1. In the inventory pane of the **Home** view, select the **Replicas** node.
2. Right-click the replicated VM and select**Failover Now** to launch the **VMware** **Failover Wizard**.

[](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/images/vm_failover_launch.png)

1. At the **Virtual Machines** step of the wizard, select the VM from the list, click **Point** and choose the restore point to which you want to fail over.



1. At the **Reason** step of the wizard, specify the reason for failover.
2. At the **Summary** step of the wizard, click **Finish** to fail over to the VM replica.

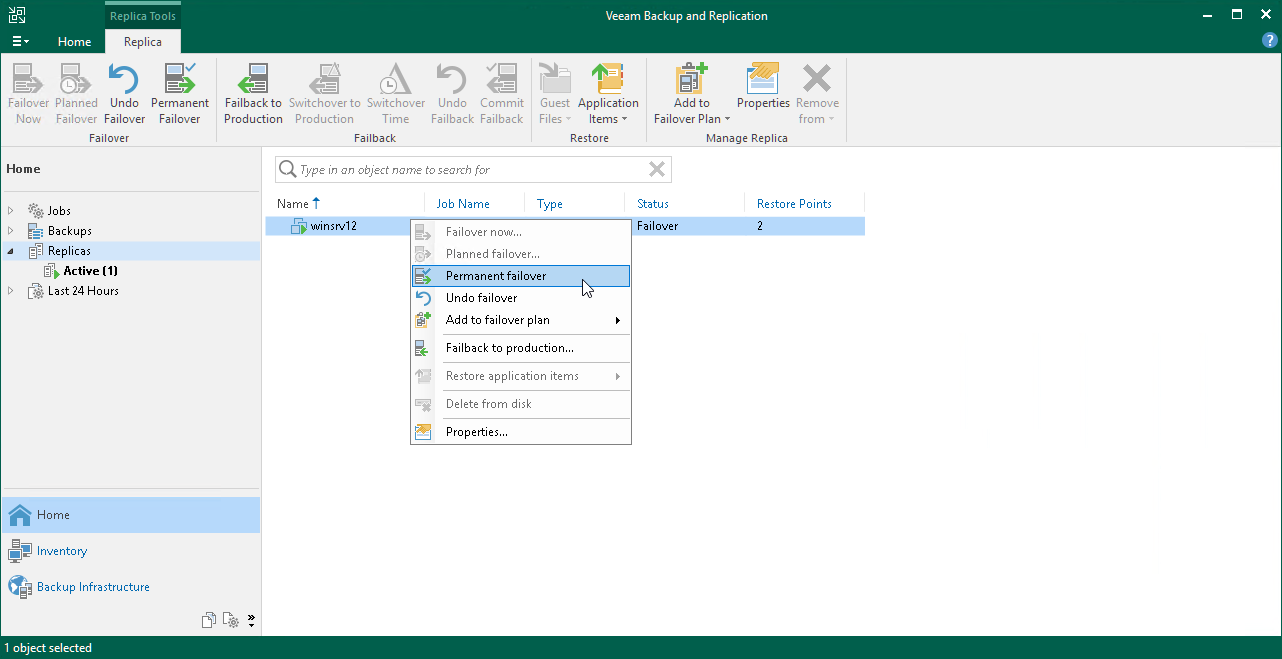
# **Performing Permanent Failover**

On This Page

* [Reference](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/replica_permanent_failover.html?ver=120#reference)

To perform permanent failover, do the following:

1. In the inventory pane of the **Home** view, click the **Replicas** node.
2. In the working area, right-click the VM replica and select **Permanent Failover**.
3. In the opened window, click **Yes** to confirm the operation.

[](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/images/vmware_definite_failover.png)

**Reference**

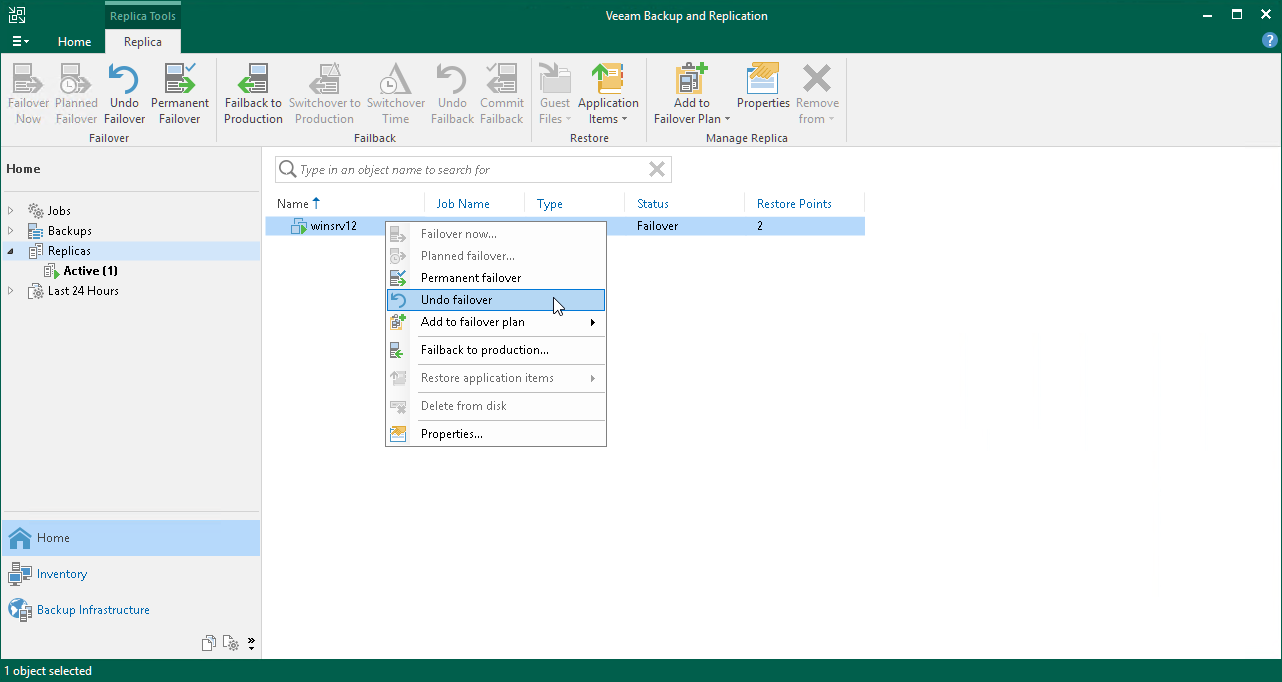
# **Undoing Failover**

On This Page

* [Reference](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/undoing_failover.html?ver=120#reference)

To undo failover, do the following:

1. In the inventory pane of the **Home** view, select the **Replicas** node.
2. In the working area, right-click the VM replica and select **Undo Failover**.
3. In the opened window, click **Yes** to confirm the operation.

[](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/images/vmware_undo_failover.png)

# **Performing Failback**

On This Page

* [Before You Begin](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/replica_failback.html?ver=120#before-you-begin)
* [Performing Failback](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/replica_failback.html?ver=120#performing-failback)
* [Reference](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/replica_failback.html?ver=120#reference)

You can fail back to a VM in the original or new location. In this section, you will learn how to fail back to the original VM on the source host. For more information on how to do this on another host, see the [Performing Failback](https://helpcenter.veeam.com/docs/backup/vsphere/performing_failback.html?ver=120) section in the Veeam Backup & Replication User Guide.

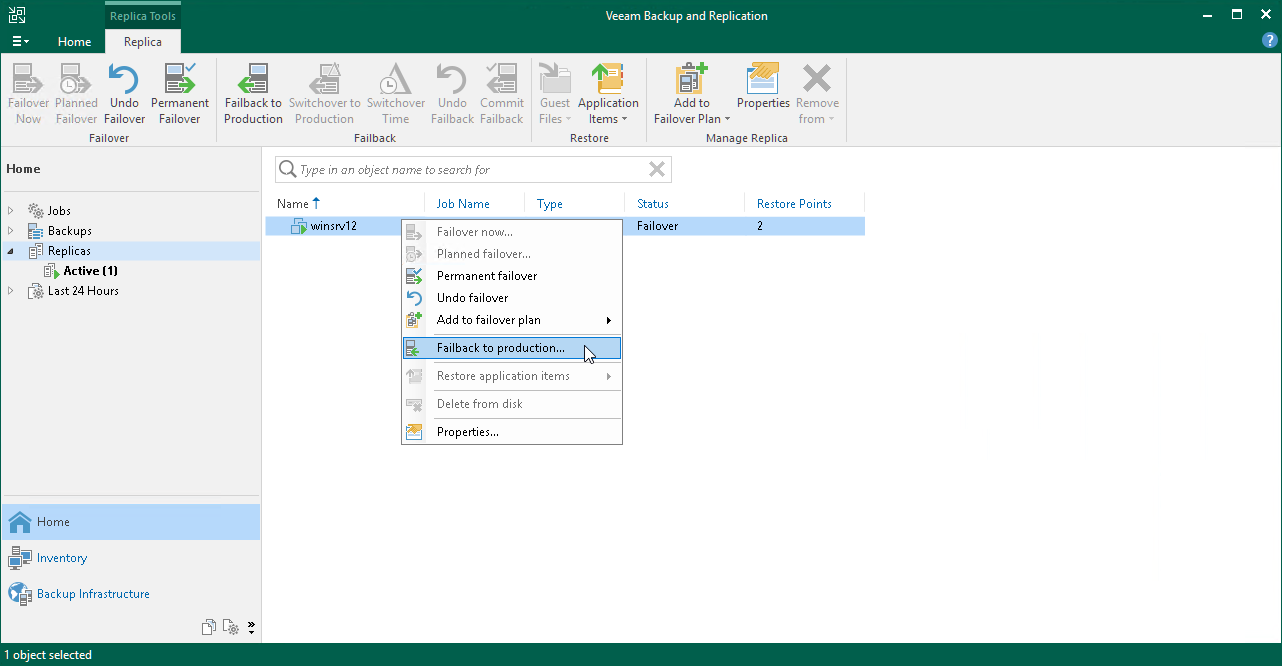
**Before You Begin**

Make sure that the VM replica for which you want to perform failback is in the *Failover* state. The replica gets into this state after you [perform replica failover](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/replica_failover.html).

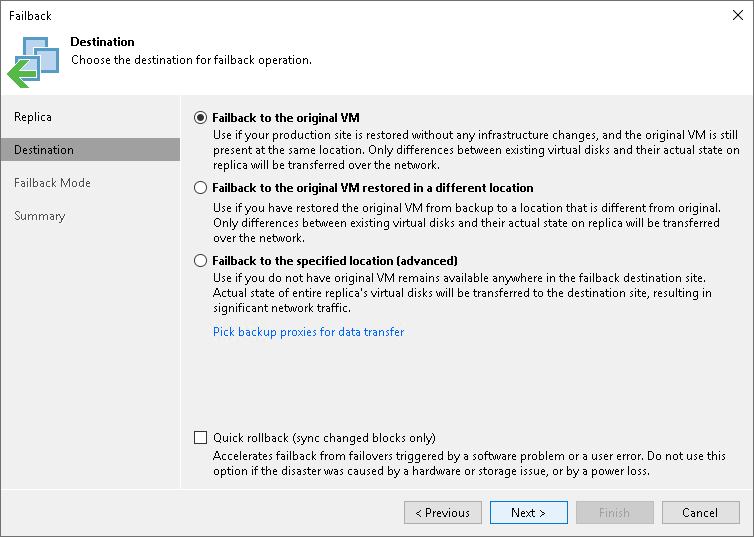
**Performing Failback**

To fail back from VM replica to the original VM on the source host, do the following:

1. In the inventory pane of the **Home** view, select the **Replicas** node.
2. In the working area, right-click the VM replica and select **Failback to production** to launch the **Failback Wizard**.

[](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/images/vm_failback_launch.png)

1. At the **Replica** step of the wizard, click **Next**.
2. At the **Destination** step of the wizard, select **Failback to the original VM**.



1. At the **Failback Mode** step of the wizard, select **Auto**. In this case, failback will be performed as soon as VMs are ready.
2. At the **Summary** step of the wizard, select the **Power on VM after restoring** check box and click **Finish**.

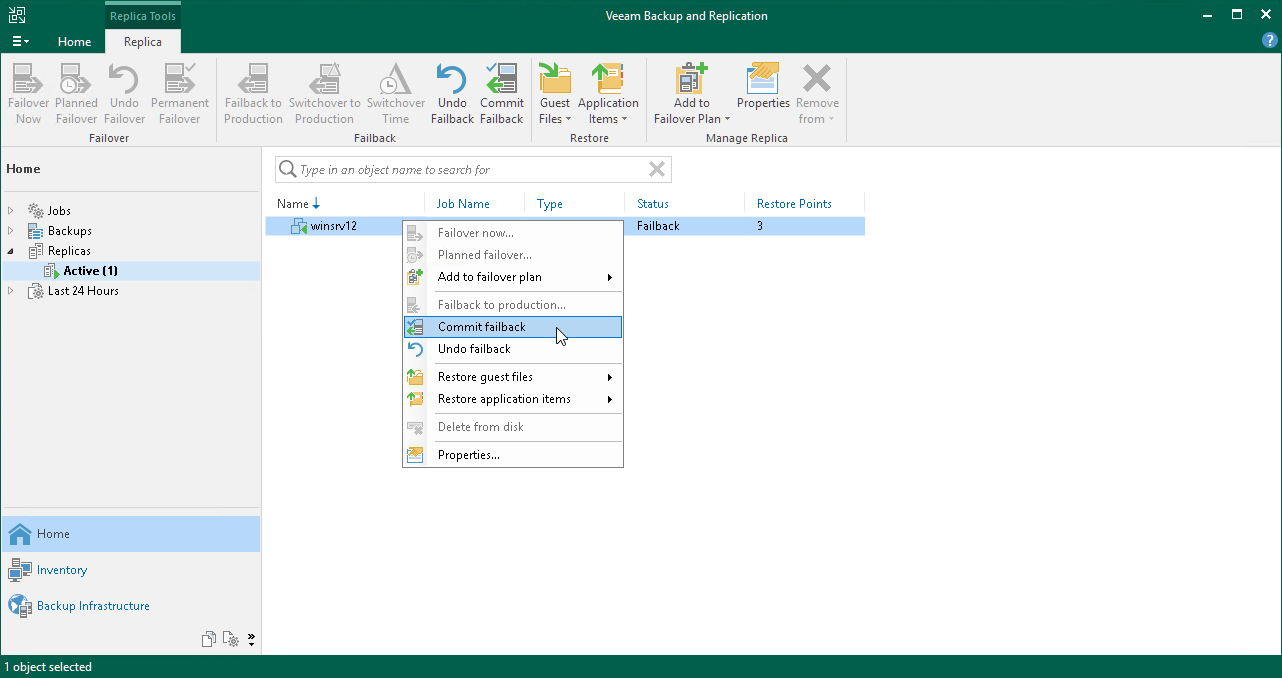
# **Committing Failback**

On This Page

* [Reference](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/committing_failback.html?ver=120#reference)

To commit a failback, do the following:

1. In the inventory pane of the **Home** view, select the **Replicas** node.
2. In the working area, right-click the VM replica and select **Commit Failback**.
3. In the opened window, click **Yes** to confirm the operation.

[](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/images/complete_failback.png)

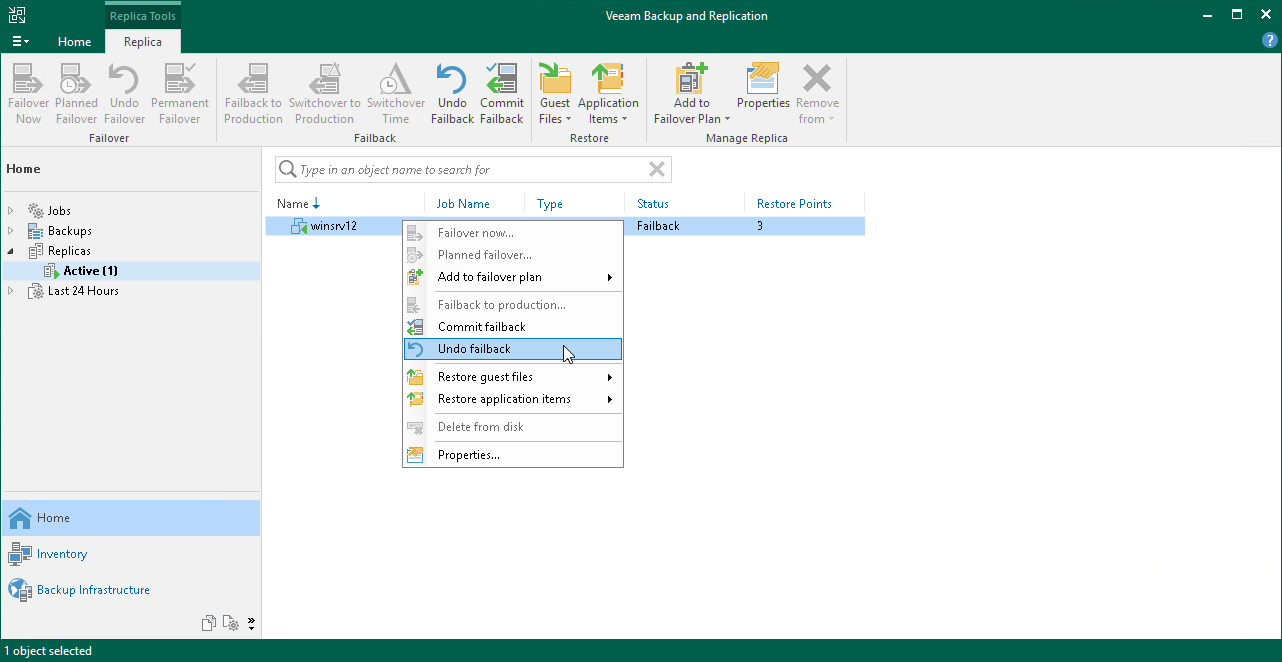
# **Undoing Failback**

On This Page

* [Reference](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/undoing_failback.html?ver=120#reference)

To undo a failback, do the following:

1. In the inventory pane of the **Home** view, select the **Replicas** node.
2. In the working area, right-click the VM replica and select **Undo Failback**.
3. In the opened window, click **Yes** to confirm the operation.

[](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/images/vmware_undo_failback.png)

# **Backing Up Physical Machines**

On This Page

* [How to back up physical machines](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/agent_backup.html?ver=120#how-to-back-up-physical-machines)
* [Reference](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/agent_backup.html?ver=120#reference)

To back up physical machines, Veeam Backup & Replication uses Veeam Agents: Veeam Agent for Microsoft Windows and Veeam Agent for Linux.

You do not need to install, set up and operate Veeam Agent on every machine whose data you want to protect. Instead, you can perform the whole set of deployment, administration, data protection and disaster recovery tasks on computers remotely from the Veeam Backup & Replication console.

**How to back up physical machines**

To back up physical machines using Veeam Backup & Replication, you must do the following:

1. [Create a protection group](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/protection_group_create.html)

When you create a protection group, you add individual machines or Active Directory containers to the protection group. Veeam Backup & Replication automatically installs agents and other required components on the machines included in the protection group.

1. [Create an Agent backup job](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/agent_backup_job_create.html)

In the Veeam Backup & Replication console, create an agent job that will back up machines included in the protection group.

# **Creating Protection Group**

On This Page

* [Before You Begin](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/protection_group_create.html?ver=120#before-you-begin)
* [Creating Protection Group](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/protection_group_create.html?ver=120#creating-protection-group)
* [Reference](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/protection_group_create.html?ver=120#reference)

In Veeam Backup & Replication, protection groups are logical containers that pool protected computers of a specific type into groups. For example, you can create a protection group for computers of the same type (laptops, workstations or servers) or computers running the same OS type to simplify their management.

You can add individual machines or Active Directory objects that include several machines to the protection group. In this section. you will learn how to create the protection group with Active Directory objects.

|  |
| --- |
| **TIP:** |
| If you plan to manage only a small number of computers, you can add the necessary computers directly to a Veeam Agent backup job. Veeam Backup & Replication will automatically add such computers to the **Manually Added** protection group. For details, see [Protection Groups](https://helpcenter.veeam.com/docs/backup/agents/protection_groups.html?ver=120) in the Veeam Agent Management Guide. |

**Before You Begin**

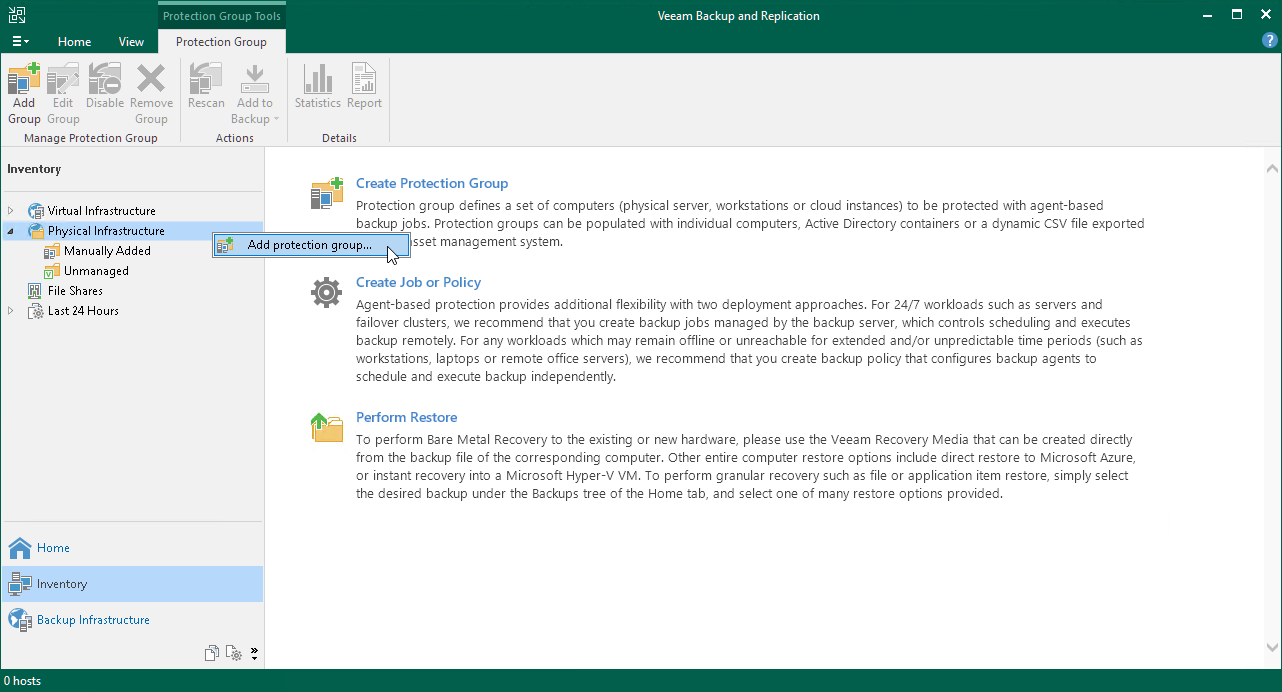
Consider the following:

* Make sure that all computers added to the protection group are powered on and can be accessed over the network.
* If you add an Active Directory container to a protection group, it is not recommended to add a computer that exists in this container to another protection group.

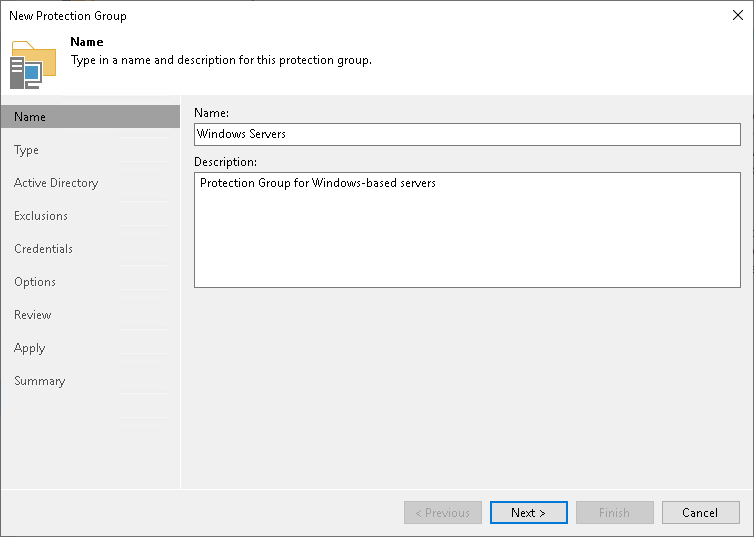
**Creating Protection Group**

To create a protection group, do the following:

1. In the inventory pane of the **Inventory** view, right-click the **Physical & Cloud Infrastructure** node and select **Add protection group** to launch the **New Protection Group** wizard.

[](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/images/protection_group_add.png)

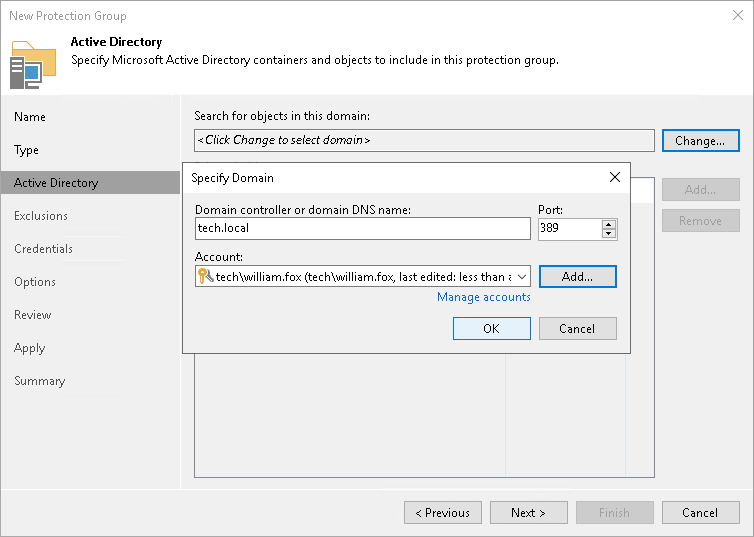
1. At the **Name** step of the wizard, specify a name and description for the protection group.



1. At the **Type** step of the wizard, select **Microsoft Active Directory objects**.

Active Directory objects can be the following: entire domain, container, organization unit, group, computer or cluster. Protection groups that include Active Directory objects are dynamic. Veeam Backup & Replication discovers these computers and deploy Veeam Agent on them during the next rescan session.

1. At the **Active Directory** step of the wizard, click **Change** near the **Search for objects in this domain field**. In the opened window, do the following:
2. In the **Domain controller or domain DNS name** field, type a name of the domain controller or domain whose objects you want to include in the protection group.
3. In the **Port** field, leave the default value.
4. Near the **Account** field, click **Add** and specify user credentials. This user must ba a member of the *DOMAIN\Administrators* group. Click **OK**.
5. Click **OK**.



1. Click **Add** near the **Selected objects** field. In the **Add Objects** window, select the necessary Active Directory object and click **OK**.
2. At the **Exclusions** step of the wizard, leave the default settings.
3. At the **Credentials** step of the wizard, specify credentials to connect to computers included in the protection group.

If you want to use the same credentials for all computers in the protection group, select the necessary user account from the **Master account** list. The account must have administrative permissions on all computers that you have added to the protection group.

You can also specify credentials for individual computes. For details, see [Specify Credentials](https://helpcenter.veeam.com/docs/backup/agents/protection_group_accounts.html?ver=120) in the Veeam Agent Management Guide.



1. At the **Options** step of the wizard, leave the default settings.
2. At the **Review** step of the wizard, review the components that will be installed. Click **Apply**.
3. At the **Apply** step of the wizard, Veeam Backup & Replication creates the configured protection group. Wait for the operation to complete and click **Next**.
4. At the **Summary** step of the wizard, select the **Run discovery when I click Finish** check box and click **Finish**.

# **Creating Veeam Agent Backup Job**

On This Page

* [Before You Begin](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/agent_backup_job_create.html?ver=120#before-you-begin)
* [Creating Veeam Agent Backup Job](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/agent_backup_job_create.html?ver=120#creating-veeam-agent-backup-job)
* [Reference](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/agent_backup_job_create.html?ver=120#reference)

To back up physical machines, you must configure a Veeam Agent backup job in the Veeam Backup & Replication console. In Veeam Backup & Replication, you can create Veeam Agent backup jobs of the following types:

* **Backup job**

The backup job runs on the backup server, like VM backup jobs. The backup job is intended for computers that are connected to the backup server. This connection must not be interrupted.

* **Backup policy**

The backup policy describes configuration of individual Veeam Agent backup jobs that run on protected computers. The backup policy is intended for computers that are connected to the backup server. The connection may be interrupted for short periods of time. For example, when you move your laptop from one location to another. Veeam Backup & Replication uses the backup policy as a template and applies settings from the backup policy to Veeam Agents that run on computers specified in the backup policy.

In this guide, we do not detail backup policy. For more information, see [Creating Veeam Agent Backup Policy](https://helpcenter.veeam.com/docs/backup/agents/agent_policy.html?ver=120).

Veeam Backup & Replication lets you create backup jobs for Microsoft Windows and Linux computers. In this section, you will learn how to create a Veeam Agent backup job for Microsoft Windows computes. For details on how to create back jobs for Linux computes, see [Creating Agent Backup Job for Linux Computers](https://helpcenter.veeam.com/docs/backup/agents/agent_job_create_linux.html?ver=120) in the Veeam Agent Management Guide.

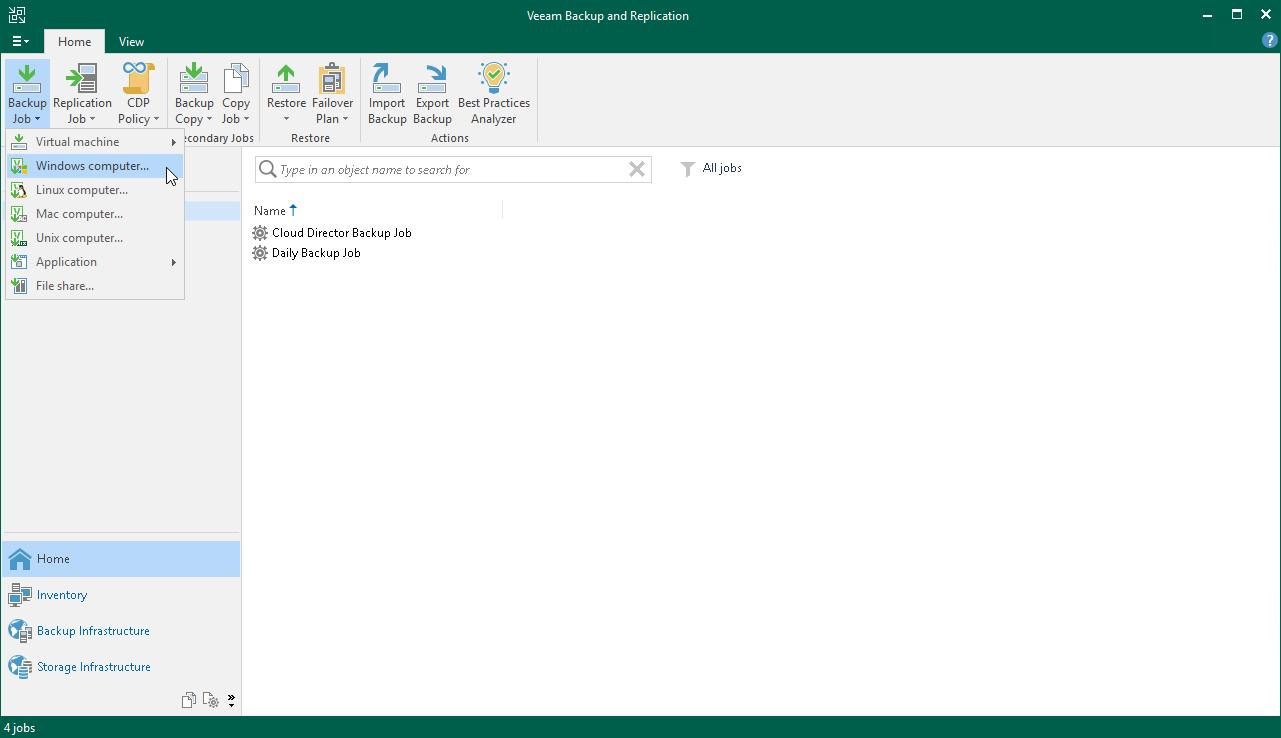
**Before You Begin**

Consider the following:

* You must have at least one protection group. For details, see [Creating Protection Group](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/protection_group_create.html).
* You can create Veeam Agent backups on a Veeam backup repository only. Other types of target locations are not supported.
* Veeam Agent for Microsoft Windows does not back up data to which symbolic links are targeted. It only backs up the path information that the symbolic links contain. After restore, identical symbolic links are created in the restore destination.

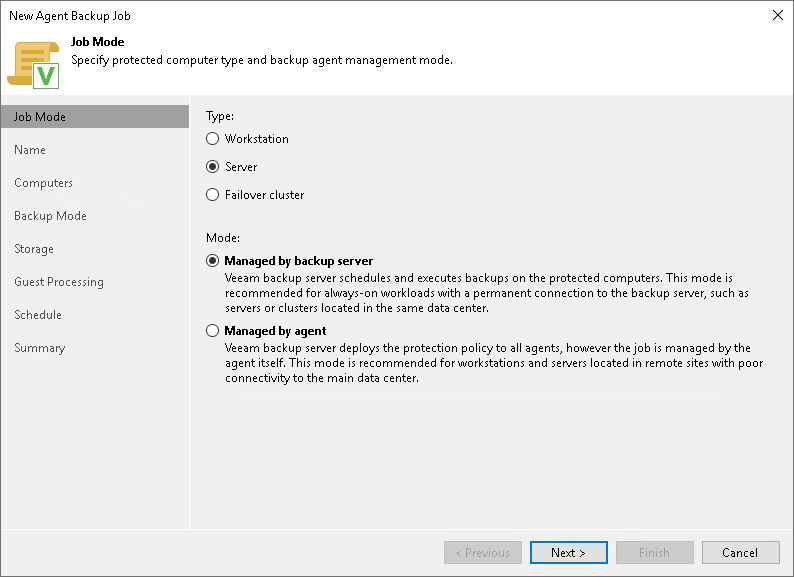
**Creating Veeam Agent Backup Job**

1. On the **Home** tab, click **Backup Job**>**Windows computer** to open the **New Agent Backup Job** wizard.

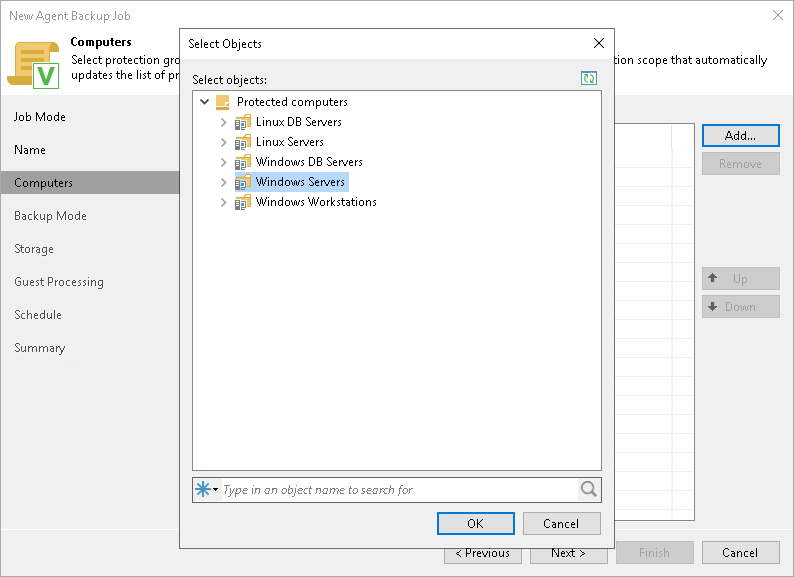
[](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/images/agent_backup_job_launch.png)

1. At the **Job Mode** step of the wizard, specify protection settings for the backup job:
2. In the **Type** list, select **Server** to add to the backup job standalone servers that have permanent connection to the backup server.
3. In the **Mode** list, select **Managed by backup server**.

When you create a Veeam Agent backup job managed by the backup server, Veeam Backup & Replication saves the job settings in its database. Veeam Backup & Replication performs all management tasks for the Veeam Agent backup job: starts a job upon the defined schedule, allocates backup infrastructure resources and so on.

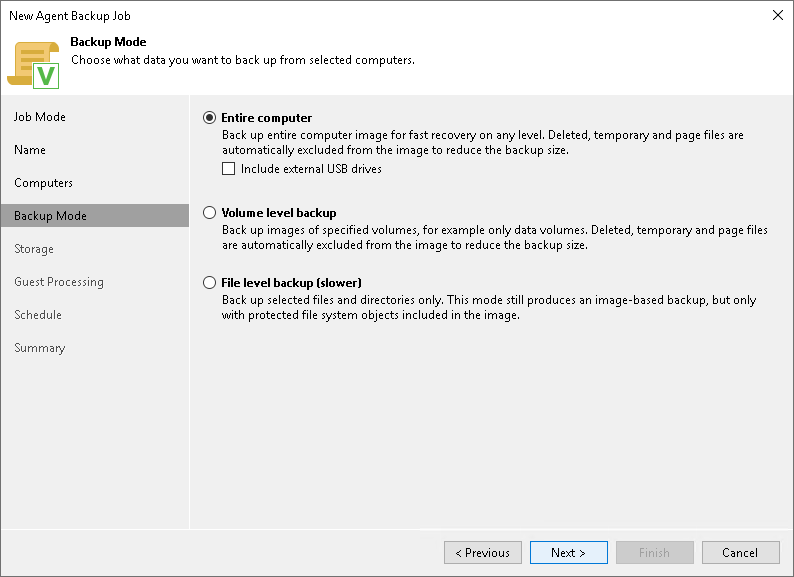


1. At the **Name** step of the wizard, specify a name and description for the backup job.
2. At the **Computers** step of the wizard, click **Add** and select one or several protection groups or computers in the list. Click **OK**.



1. At the **Backup Mode** step of the wizard, select **Entire computer**.

When you restore data from such a backup, you are able to recover the entire computer image as well as data on specific computer volumes: files, folders and application data.



1. At the **Storage** step of the wizard, select the backup repository where you want to store your backups. For other settings, leave the default values.
2. At the **Guest Processing** step of the wizard, leave the default settings.
3. At the **Schedule** step of the wizard, define scheduling settings for the job.
4. At the **Summary** step of the wizard, select the **Run the job when I click Finish** check box and click the **Finish** button.
5. In the inventory pane of the**Home** view, expand the **Last 24 Hours** node to see the created job.

**s**

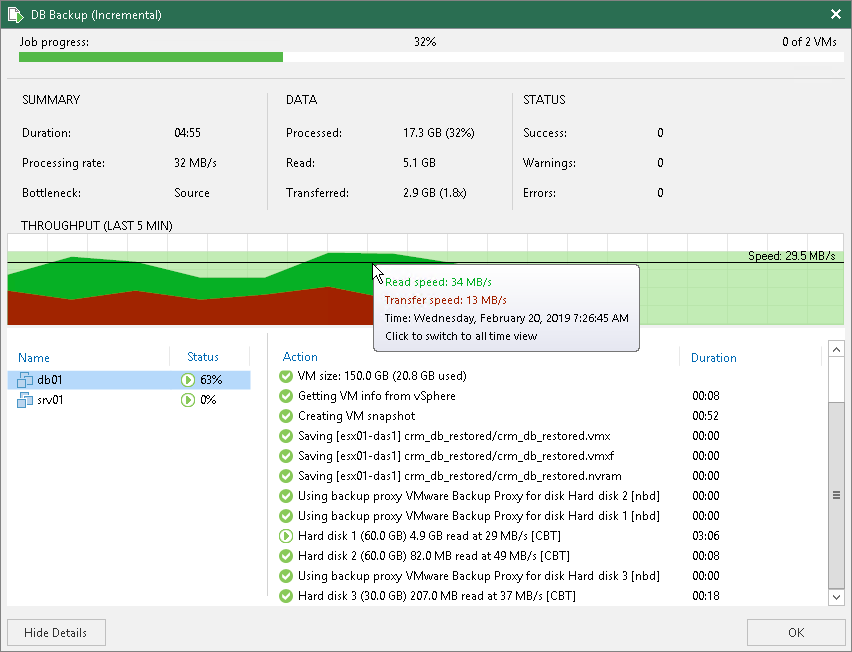
**11 Verifying Active backup jobs and monitoring.**

# **Monitoring Job Performance in Real Time**

When the job is running, you can view job statistics in real time. Statistics include job progress, duration, processing rate, performance bottlenecks, the amount of read and transferred data, and other details of the job performance.

To view the job statistics, do the following:

1. In the inventory pane of the **Home** view, select the **Jobs** node.
2. In the working area, right-click a running job and click **Statistics**.
3. In the opened window, select a VM to view its statistics.

[](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/images/realtime_stats.png)

Note that the job must complete with the *Success* or *Warning* status. If the job completes with the *Failed* status, Veeam Backup & Replication does not create the backup file is not able to perform restore operations.

# **Configuring Global Email Notification Settings**

On This Page

* [Configuring Mail Server](https://helpcenter.veeam.com/docs/backup/vsphere/general_email_notifications.html?ver=120#configuring-mail-server)
* [Customizing Send Settings](https://helpcenter.veeam.com/docs/backup/vsphere/general_email_notifications.html?ver=120#customizing-send-settings)

To configure global email notification settings:

1. From the main menu, select **General Options**.
2. Open the**E-mail Settings** tab and select the **Enable e-mail notifications** check box.
3. [Configure mail server](https://helpcenter.veeam.com/docs/backup/vsphere/general_email_notifications.html?ver=120#configuring_mail_server).
4. [Customize send settings](https://helpcenter.veeam.com/docs/backup/vsphere/general_email_notifications.html?ver=120#customizing_send_settings).

**Configuring Mail Server**

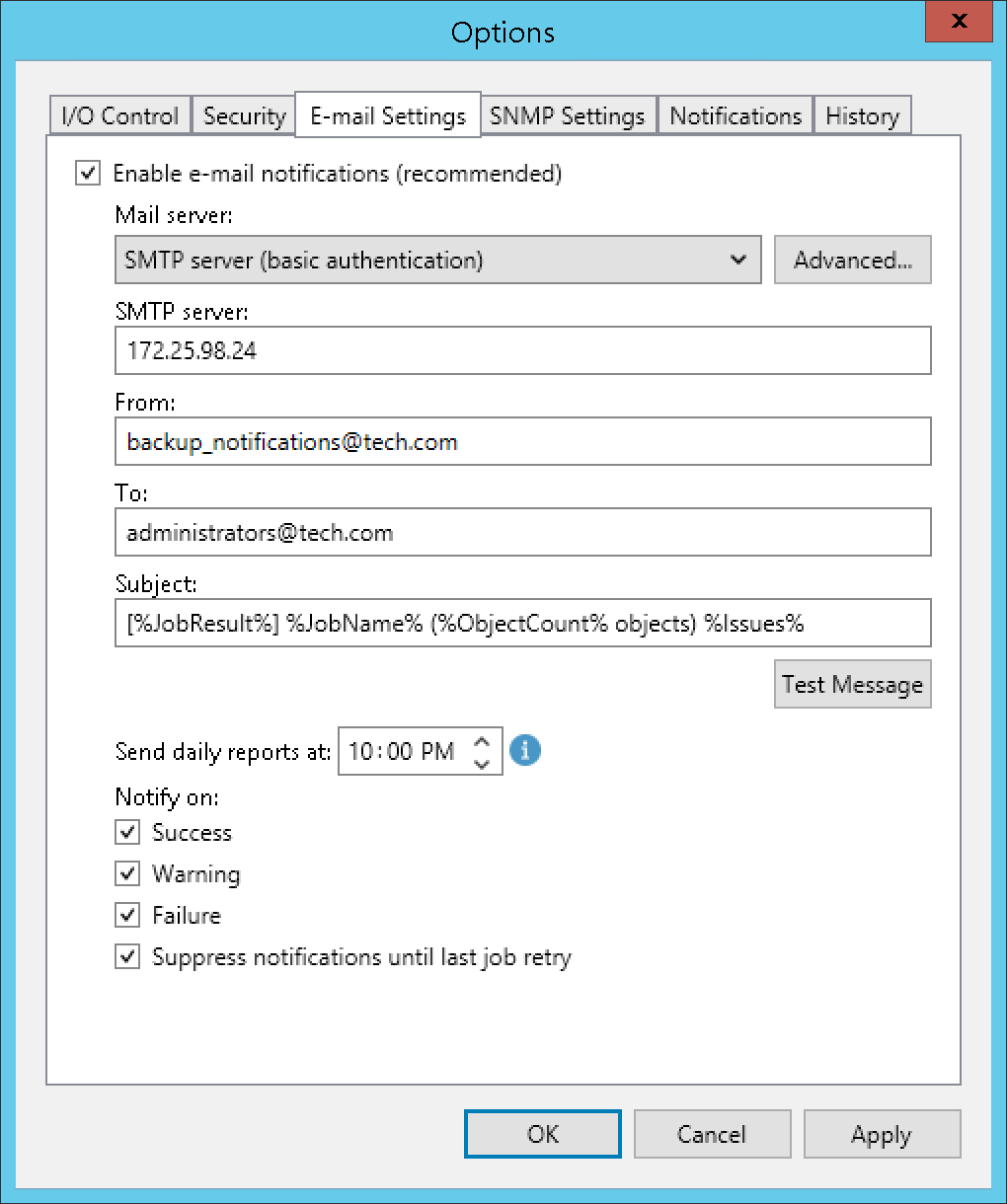
To configure mail server, perform the following steps:

1. In the **Mail Server** field, specify the authentication method you want to use. Veeam Backup & Replication supports the following methods:

* SMTP basic authentication
* Google Gmail OAuth 2.0 authentication
* Microsoft 365 OAuth 2.0 authentication

|  |
| --- |
| **NOTE** |
| For more secure environments, it is recommended to use OAuth 2.0 authentication. Also, note that Microsoft and Google consider SMTP basic authentication as an outdated industry standard and plan to disable it. For more information, see [this Microsoft article](https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/deprecation-of-basic-authentication-exchange-online) and [this Google article](https://support.google.com/accounts/answer/6010255). |

1. If you want to use SMTP basic authentication, perform the following steps:
   1. In the **Mail server** field, select *SMTP* *server* from the list.
   2. In the **SMTP server** field, enter a full DNS name, or IPv4 or IPv6 address of the SMTP server that will be used for sending email notifications. Note that you can use IPv6 addresses only if IPv6 communication is enabled as described in [IPv6 Support](https://helpcenter.veeam.com/docs/backup/vsphere/ipv6.html).

[](https://helpcenter.veeam.com/docs/backup/vsphere/images/email_notifications_smtp.png)

1. To specify user credentials and connection options, click the **Advanced** button:

* Specify the port number and connection timeout for the SMTP server.

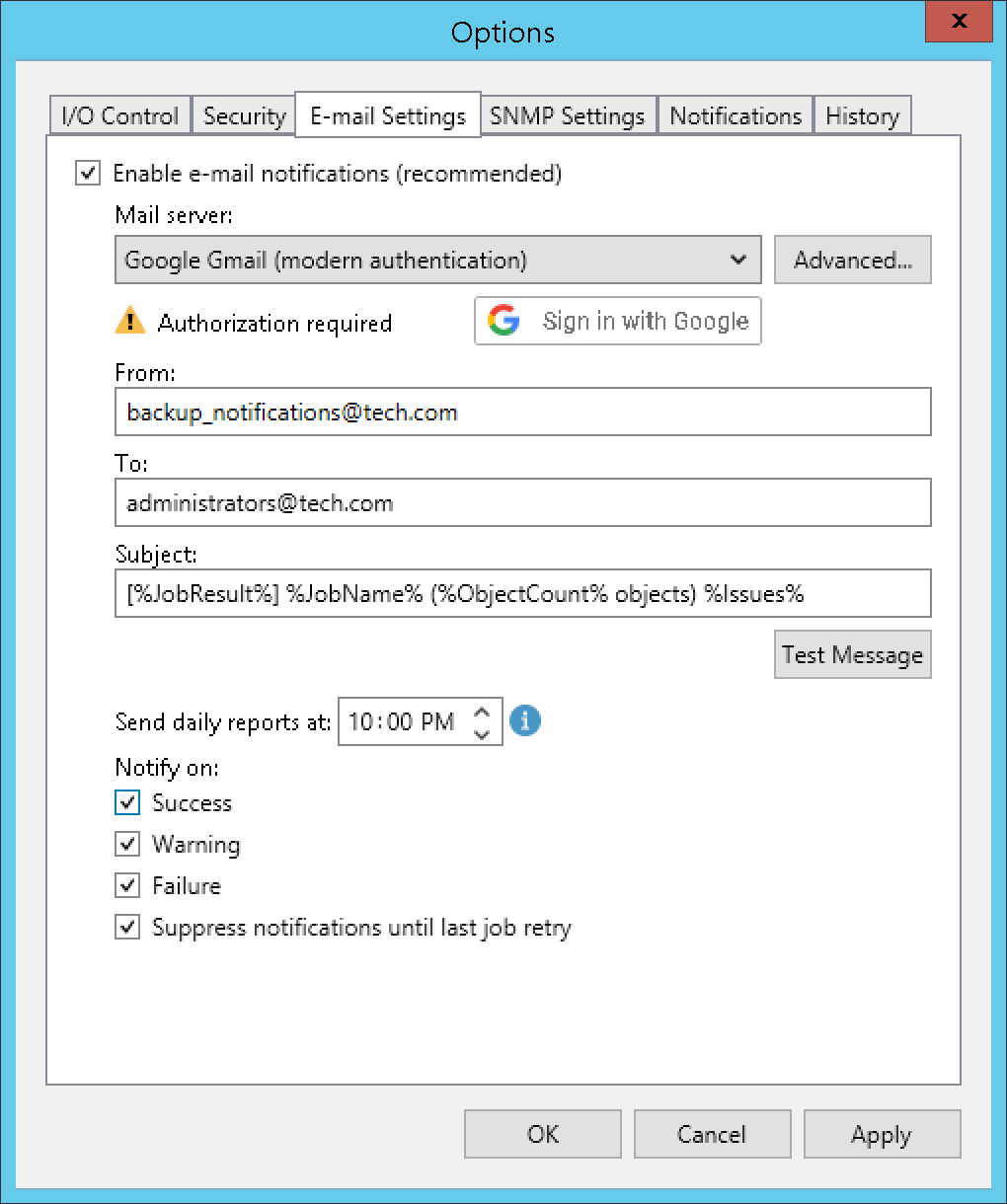
|  |
| --- |
| **NOTE** |
| Sending email notifications using Implicit TLS (over port 465) is not supported. For more information about Implicit TLS, see [this RFC section](https://www.rfc-editor.org/rfc/rfc8314#section-3). |

* To use a secure connection for email operations, select the **Connect using SSL** check box.
* If you need to connect to the SMTP server using a specific account, select the **This SMTP server requires authentication** check box and select the necessary credentials from the **Log on as** list. If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right to add credentials. For more information, see [Managing Credentials](https://helpcenter.veeam.com/docs/backup/vsphere/credentials_manager.html).

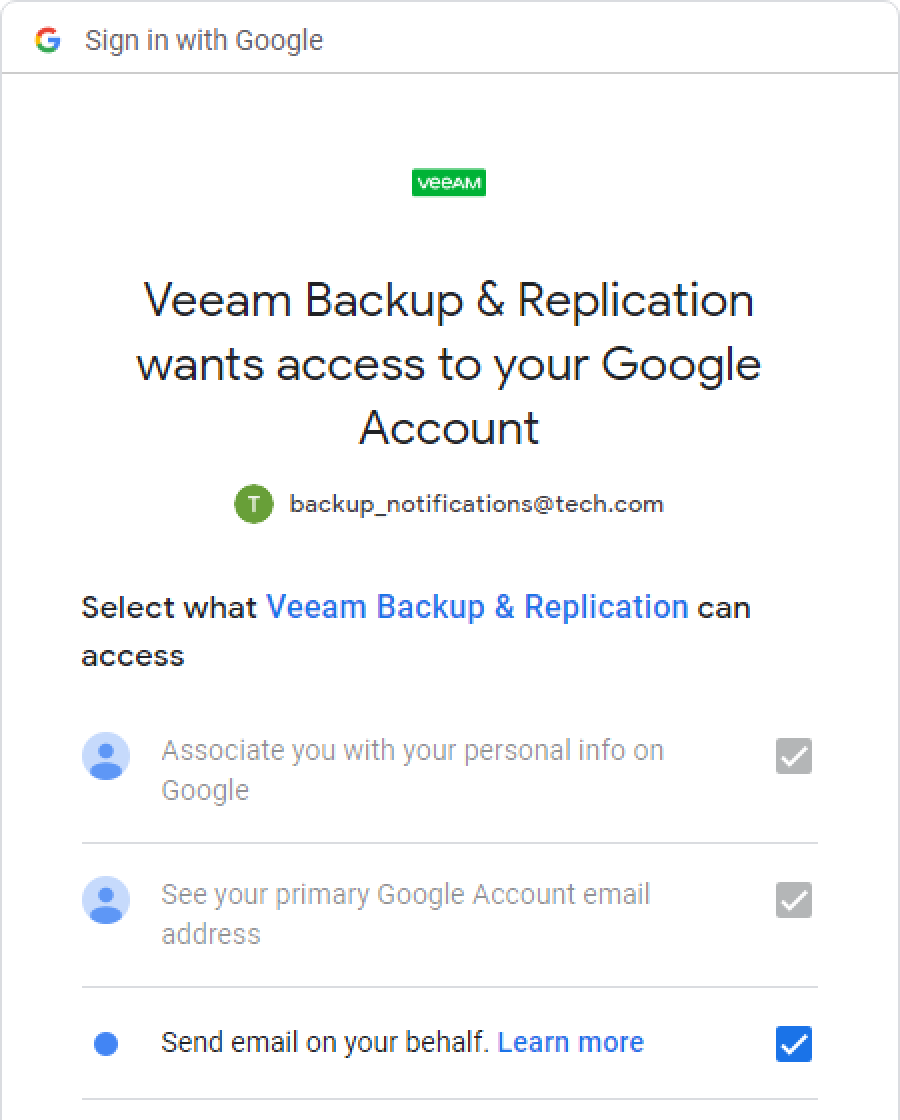
When you add an SMTP server, Veeam Backup & Replication saves to the configuration database a thumbprint of the TLS certificate. If the certificate is not trusted, Veeam Backup & Replication displays a warning. If you trust the certificate, click **Continue**.

[](https://helpcenter.veeam.com/docs/backup/vsphere/images/email_notifications_untrusted_certificate.png)

1. If you want to use Google Gmail OAuth 2.0 authentication, perform the following steps:
   1. In the **Mail server** field, select *Google Gmail* from the list and click the **Sign in with Google** button.

[](https://helpcenter.veeam.com/docs/backup/vsphere/images/email_notifications_google.png)

1. In the opened web browser window, specify the Google account to connect to the Veeam Backup & Replication application. Note that you must select **Send email on your behalf** check box during configuring access options.

[](https://helpcenter.veeam.com/docs/backup/vsphere/images/email_notifications_google_settings.png)

|  |
| --- |
| **NOTE** |
| Consider the following:   * For security reasons, it is recommended to use a dedicated service account with granular SendMail permissions. * To sign in with the Google account, your default web browser must meet Google requirements. For more information, see [this article](https://support.google.com/accounts/answer/7675428?hl=en). |

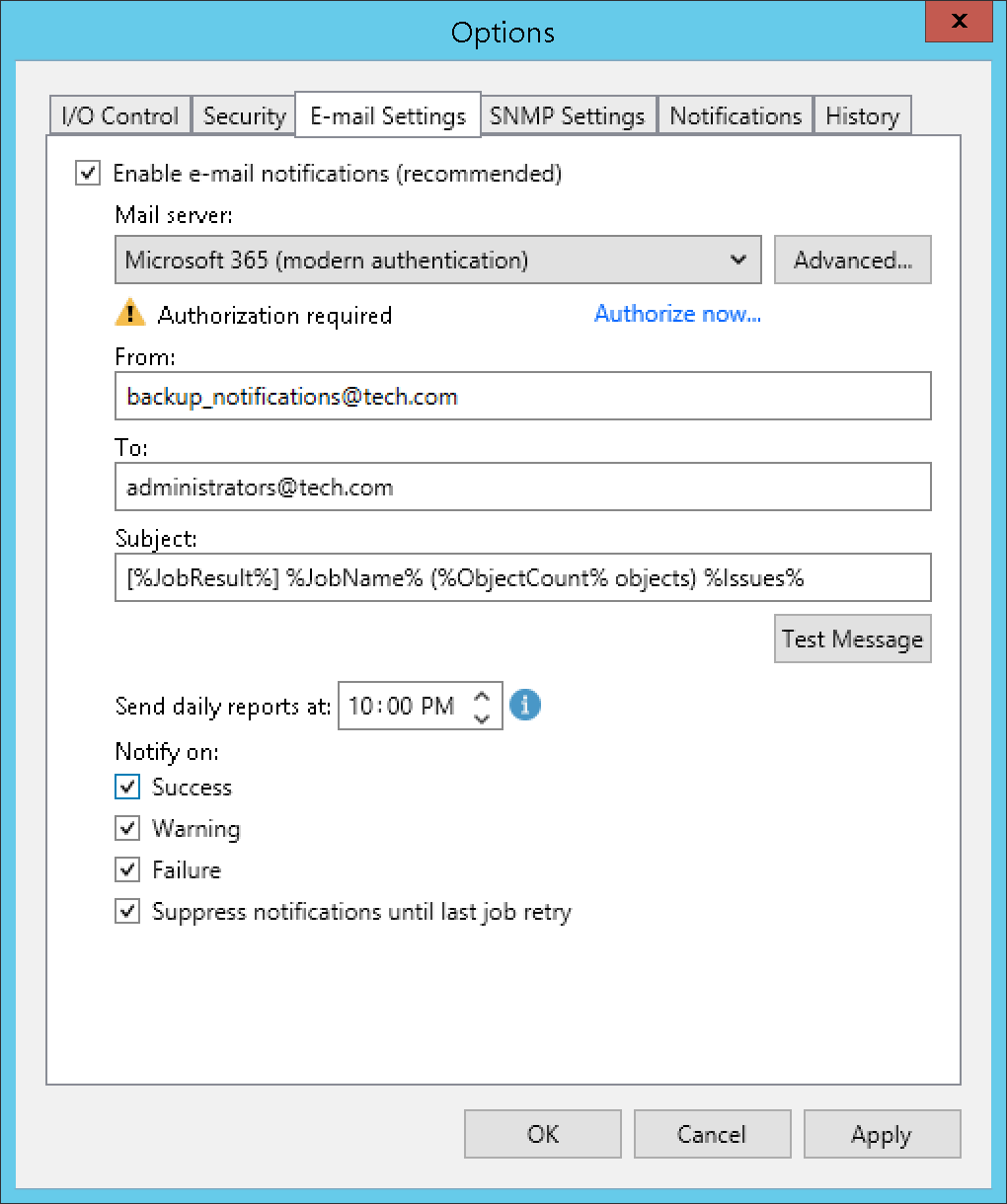
If the authentication is successful, the *Token is valid* notice will appear. The token is refreshed automatically. If it was revoked or the Google account password was changed, click the **Re-authorize** link to update configuration.

To specify custom authentication options, click the **Advanced** button:

* Select the **Use custom application registration settings** check box.
* Specify the application client ID and the client secret.

For more information on how to register your custom application, see [Registering Application in Google Cloud Console](https://helpcenter.veeam.com/docs/backup/vsphere/registering_google_app.html).

1. If you want to use Microsoft 365 OAuth 2.0 authentication, perform the following steps:
   1. In the **Mail server** field, select *Microsoft 365* from the list and click the **Authorize now** link.

[](https://helpcenter.veeam.com/docs/backup/vsphere/images/email_notifications_microsoft.png)

1. In the opened window, specify your Exchange Online credentials to connect to the Veeam Backup & Replication application.

|  |
| --- |
| **NOTE** |
| Consider the following:   * For security reasons, it is recommended to use a dedicated service account with granular SendMail permissions. * To sign in with Exchange Online credentials, turn off the **Internet Explorer Enhanced Security Configuration** option in Server Manager. For more information, see [this article](https://learn.microsoft.com/en-us/troubleshoot/developer/browsers/security-privacy/enhanced-security-configuration-faq#how-to-turn-off-internet-explorer-esc-on-windows-servers). |

If the authentication is successful, the *Token is valid* notice will appear. The token is refreshed automatically. If it was revoked or Exchange Online credentials were changed, click the **Re-authorize** link to update configuration.

To specify custom authentication option, click the **Advanced** button:

* Select the **Use custom application registration settings** check box.
* Specify the application client ID and the tenant ID.

|  |
| --- |
| **NOTE** |
| For custom applications, note that you must select **Consent on behalf of your organization** check box during configuring access options. |

For more information on how to register your custom application, see [Registering Application in Microsoft Azure Portal](https://helpcenter.veeam.com/docs/backup/vsphere/registering_azure_app.html).

**Customizing Send Settings**

To customize send settings, perform the following steps:

1. In the **From** field, specify an email from which email notifications must be sent. Note that for OAuth 2.0 autnentication, it must be the account you use to connect to the Veeam Backup & Replication application.
2. In the **To** field, specify the recipient addresses. Use a semicolon to separate multiple addresses. Recipients specified in this field will receive notification about every job managed by the backup server. You can leave the field empty if required.

For every particular job, you can specify additional recipients. For more information, see [Configuring Job Notification Settings](https://helpcenter.veeam.com/docs/backup/vsphere/job_email_notifications.html).

|  |
| --- |
| **IMPORTANT** |
| If you specify the same email recipient in both job notification and global notification settings, Veeam Backup & Replication will send the job notification only. |

1. In the **Subject** field, specify a subject for the sent message. You can use the following variables in the subject:
2. *%Time%* — completion time
3. *%JobName%*
4. *%JobResult%*
5. *%ObjectCount%* — number of VMs in the job
6. *%Issues%* — number of VMs in the job that have been processed with the *Warning* or *Failed* status
7. In the **Send daily reports at** field, specify at what time Veeam Backup & Replication will send daily email reports. Daily reports are generated for different purposes throughout Veeam Backup & Replication:

* Reports about processing results of scale-out repository data. For more information, see [Receiving Scale-Out Backup Repository Reports](https://helpcenter.veeam.com/docs/backup/vsphere/sobr_reports.html).
* Reports about processing results of backup copy jobs. For more information, see [Notification Settings](https://helpcenter.veeam.com/docs/backup/vsphere/backup_copy_settings_notification.html) in the **Creating Backup Copy Jobs for VMs and Physical Machines** section.
* Reports about processing results of backup copy jobs for transaction log backups. For more information about transaction log backups, see [Microsoft SQL Server Logs Backup](https://helpcenter.veeam.com/docs/backup/vsphere/sql_backup.html).
* Reports about backups of virtual and physical machines created with [Veeam Agent for Microsoft Windows or Veeam Agent for Linux](https://helpcenter.veeam.com/docs/backup/agents/introduction.html?ver=120) in the **Managed by Agent** mode.
* Reports with statistics for rescan job sessions performed for protection groups of virtual and physical machines created with [Veeam Agent for Microsoft Windows or Veeam Agent for Linux](https://helpcenter.veeam.com/docs/backup/agents/introduction.html?ver=120).
* Reports about processing results of backup copy jobs for backups created with [Veeam Plug-ins for Enterprise Applications](https://helpcenter.veeam.com/docs/backup/plugins/overview.html?ver=120).
* Reports about active Instant Recovery sessions, that is, sessions that were not finalized. For more information about Instant Recovery, see [Instant Recovery to VMware vSphere](https://helpcenter.veeam.com/docs/backup/vsphere/instant_recovery.html) and [Instant Recovery to Microsoft Hyper-V](https://helpcenter.veeam.com/docs/backup/vsphere/instant_recovery_to_hv.html).

|  |
| --- |
| **NOTE** |
| Settings configured for a certain report override global notification settings. |

1. In the **Notify on** group, select the **Success**, **Warning** and/or **Failure** check boxes to receive email notification if a job is run successfully, not successfully or with a warning.
2. Select the **Suppress notifications until the last retry** check box to receive a notification about the final job status. If you do not enable this option, Veeam Backup & Replication will send one notification per every job retry.
3. Veeam Backup & Replication allows sending a test email to check if all settings have been configured correctly. To send a test email, click **Test Message**.

**12 Taking Archive backup.**

**14 Testing and restoring backups.**

# **Data Recovery**

Veeam Backup & Replication allows you to perform the following data recovery operations:

* [Restore entire VM](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/vm_restore.html)
* [Restore guest OS files](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/flr.html)
* [Restore VM virtual disks](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/virtual_disk_restore.html)
* [Recover VM files](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/vm_files_restore.html)
* [Recover application items](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/recover_database.html)
* [Export disks](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/exporting_disks.html)

Page updated 5/3/2023

# **Restoring Entire VM**

On This Page

* [Before You Begin](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/vm_restore.html?ver=120#before-you-begin)
* [Restoring Entire VM](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/vm_restore.html?ver=120#restoring-entire-vm)

If a VM fails, you can restore it from a backup file. You can restore a single VM or multiple VMs to the original or new location.

In this section, you will learn how to restore a VM to the original location. For more information on how to restore the VM to another location, see [Restoring Entire VM](https://helpcenter.veeam.com/docs/backup/vsphere/performing_full_recovery.html?ver=120) in the Veeam Backup & Replication User Guide.

**Before You Begin**

Before you restore a VM from a backup, consider the following:

* You can restore the VM from a backup that has at least one successfully created restore point.

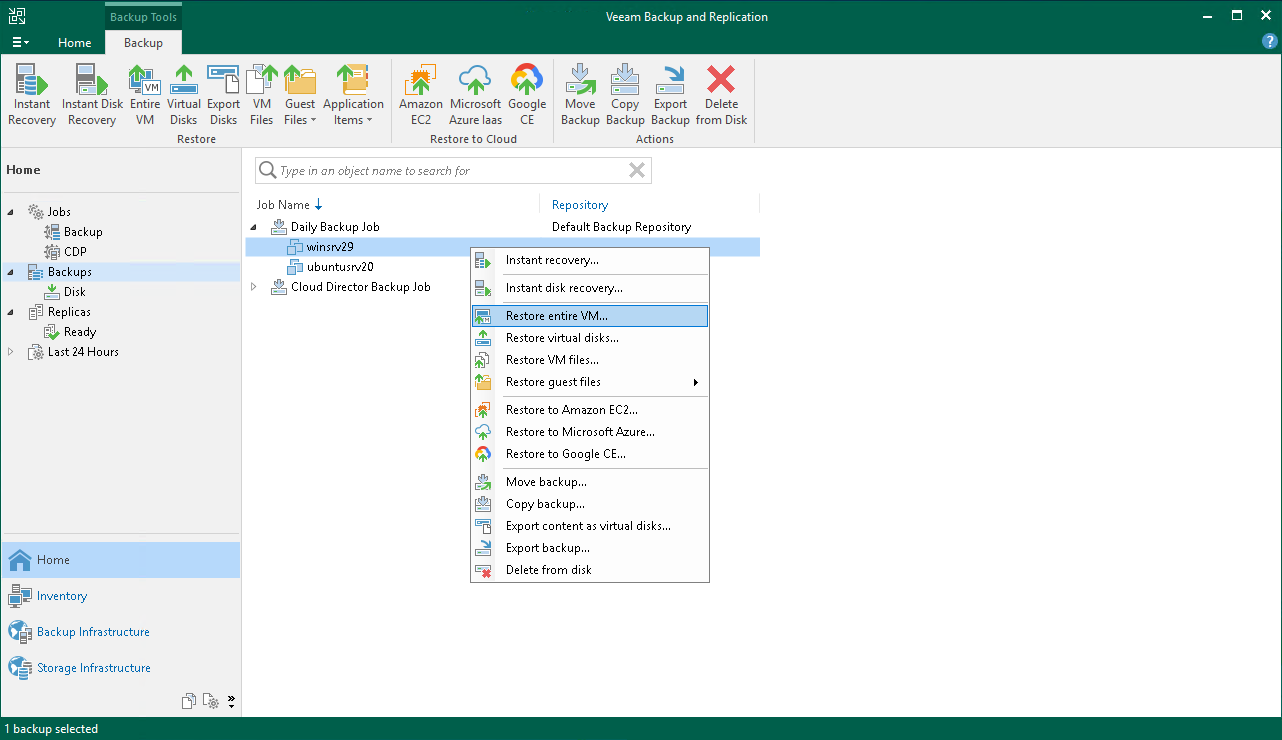
To check whether restore points are created, open the inventory pane of the **Home** view and select the **Backups** node. Then, expand the backup job and verify that there is at least one restore point available for the VM.

* When you restore the VM to its original location, and the original VM is still running, Veeam Backup & Replication powers off the original VM and restores only those disks that are included in the backup. All other disks remain unchanged.

**Restoring Entire VM**

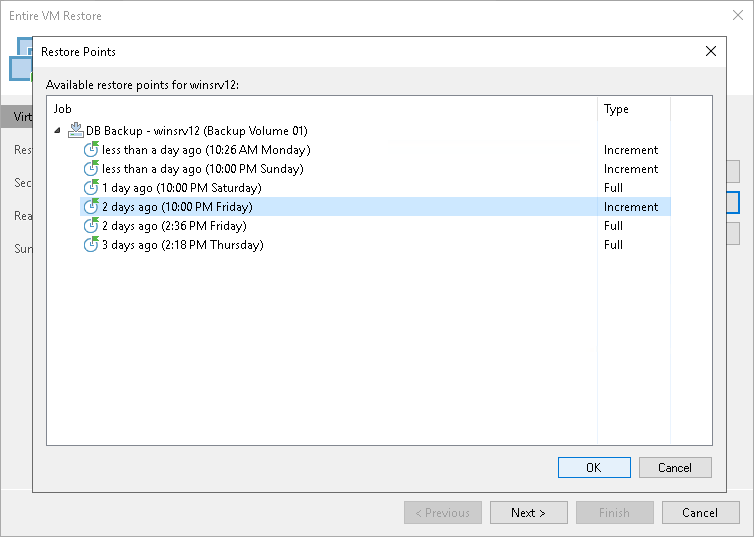
To restore an entire VM to its original location, do the following.

1. Open the **Home** view.
2. In the inventory pane, select the **Backups**>**Disk** node. Expand the backup job in the working area, right-click a VM in a backup job and select **Restore entire VM** to launch the **Entire VM Restore** wizard.

[](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/images/full_vm_restore_launch.png)

1. At the **Virtual Machines** step of the wizard, select the VM from the list, click the **Point** button and choose a restore point.

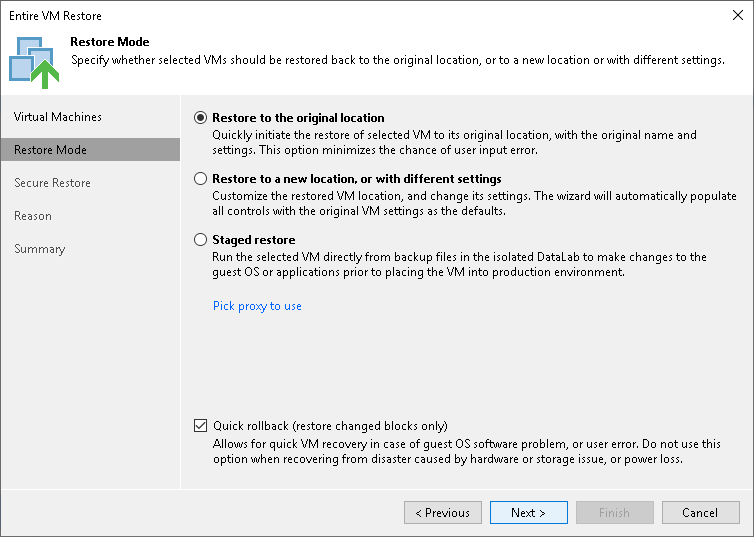
If you select an incremental restore point, Veeam Backup & Replication automatically restores data blocks from the full backup file and the chain of incremental backup files.



1. At the **Restore mode** step of the wizard, do the following:
2. Select the **Restore to the original location** option.
3. Select the **Quick rollback** check box.

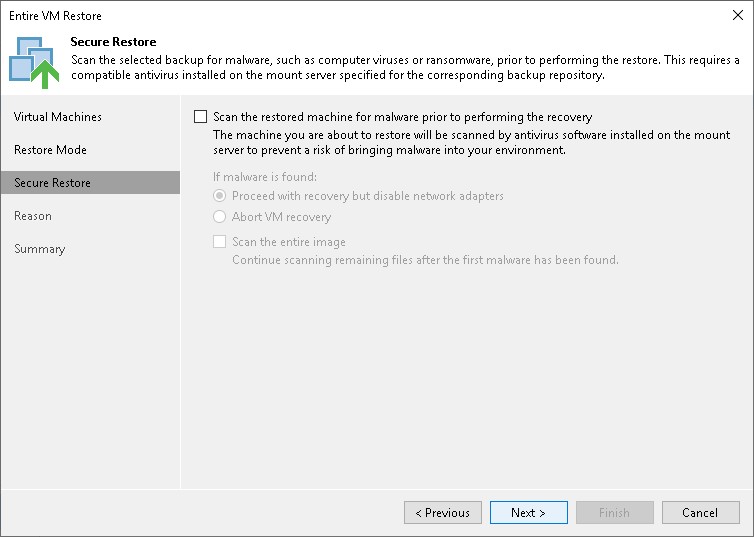
Veeam Backup & Replication will get data blocks that are necessary to revert the VM to an earlier point in time and will restore only these data blocks from the backup. Quick rollback significantly reduces the restore time.

|  |
| --- |
| **IMPORTANT!** |
| Do not enable the **Quick rollback** option if the problem occurred at the VM hardware level, storage level or due to a power loss. |



1. At the **Secure Restore** step of the wizard, enable scanning of the machine or leave the default settings.

If secure restore is enabled, Veeam Backup & Replication uses antivirus software to scan machine data before restoring the machine to the production environment. For details, see [Secure Restore](https://helpcenter.veeam.com/docs/backup/vsphere/av_scan_about.html?ver=120) in the Veeam Backup & Replication User Guide.



1. At the **Reason** step of the wizard, specify the reason for restoring the VM.
2. At the **Summary** step of the wizard, select the **Power on VM after restoring** check box and click **Finish**.

# **Restoring VM Files**

On This Page

* [Before You Begin](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/vm_files_restore.html?ver=120#before-you-begin)
* [Restoring VM Files](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/vm_files_restore.html?ver=120#restoring-vm-files)
* [Reference](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/vm_files_restore.html?ver=120#reference)

Veeam Backup & Replication can help you restore VM files: VMX, VMXF, NVRAM and VMDK including flat files. For example, your VM configuration file is missing and you need to restore it. Instead of restoring the entire VM image, you can restore a single VM file.

You can restore VM files to the latest state or any valid point in time. You can also restore them to the original or new location.

**Before You Begin**

Before you restore VM files from a backup, consider the following:

* You can restore VM files a backup that has at least one successfully created restore point.

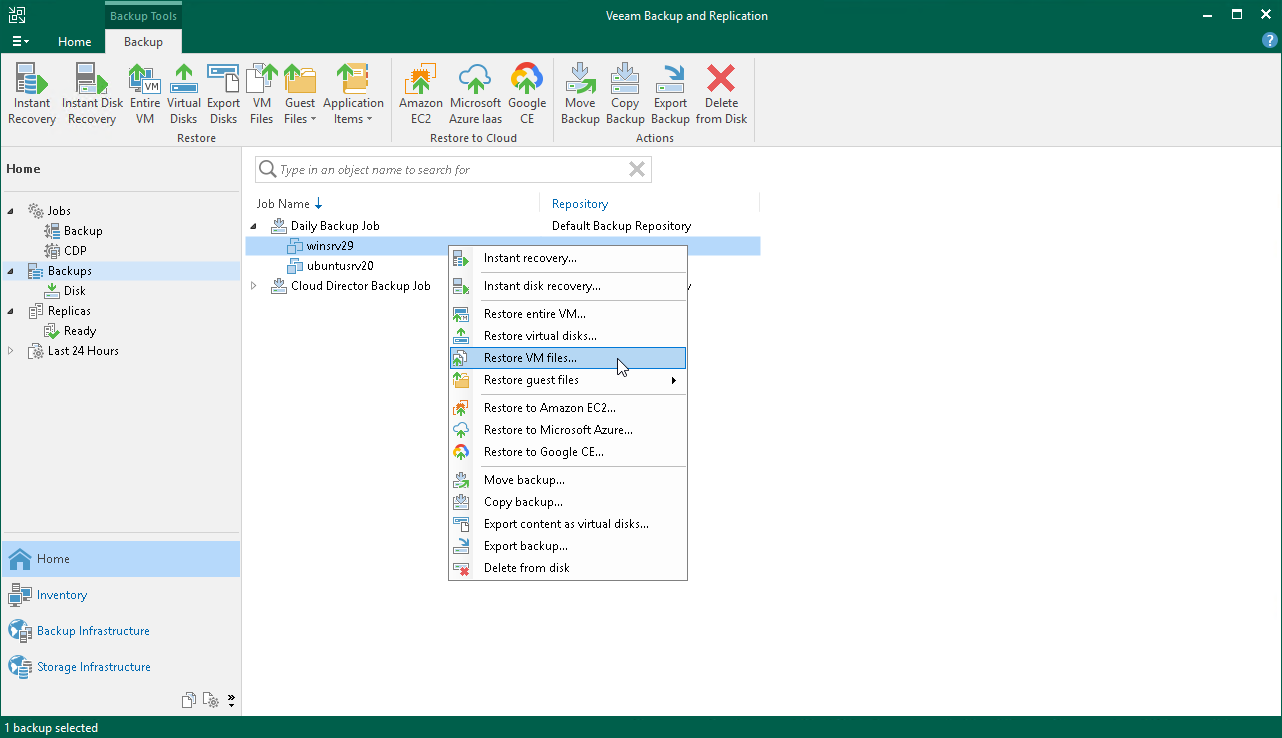
To check whether restore points are created, open the inventory pane of the **Home** view and select the **Backups** node. Then, expand the backup job and verify that there is at least one restore point available for the VM.

* The server on which you plan to save the restored VM files must be added to the backup infrastructure.

**Restoring VM Files**

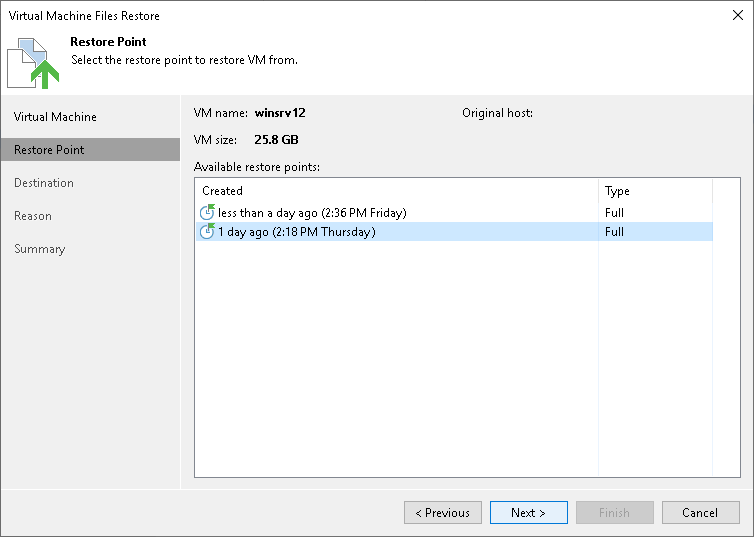
To recover VM files, do the following.

1. Open the **Home** view.
2. In the inventory pane, select the **Backups**>**Disk** node. Expand a backup job in the working area, right-click a VM and choose **Restore VM files** to launch the **Virtual Machine File Restore** wizard.

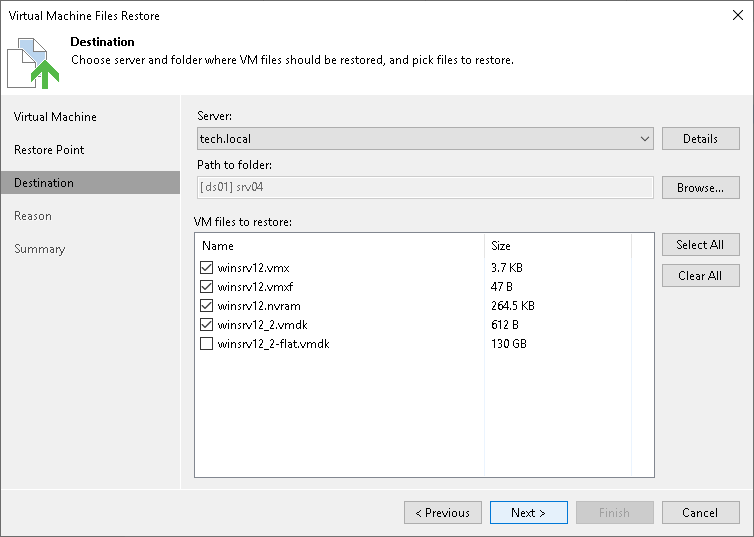
[](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/images/restore_vm_files_launch.png)

1. At the **Restore Point** step of the wizard, select a restore point.

If you select an incremental restore point, Veeam Backup & Replication automatically restores data blocks from the full backup file and the chain of incremental backup files.



1. At the **Destination** step of the wizard, do the following:
2. In the **Server** list, select the server to which you want to restore VM files.
3. In the **Path to folder** field, specify the path to the folder where you want to restore files.
4. In the **VM files to restore** section, select the required files.



1. At the **Reason** step of the wizard, specify the reason for restoring files.
2. At the **Summary** step of the wizard, click **Finish** to restore the VM files.

# **Restoring VM Virtual Disks**

On This Page

* [Before You Begin](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/virtual_disk_restore.html?ver=120#before-you-begin)
* [Restoring Virtual Disks](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/virtual_disk_restore.html?ver=120#restoring-virtual-disks)
* [Reference](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/virtual_disk_restore.html?ver=120#reference)

Veeam Backup & Replication allows you to recover individual virtual disks of a VM. Recovered virtual disks can be attached to the original VM or to any other VM. This recovery option can be helpful if a VM virtual disk becomes corrupted.

You can restore VM virtual disk to the latest state or any valid restore point. You can preserve the format of a recovered virtual disk or convert it to the thin or thick provisioned disk format.

**Before You Begin**

Before you restore VM virtual disks from a backup, consider the following:

* You can restore virtual disks from a backup that has at least one successfully created restore point.

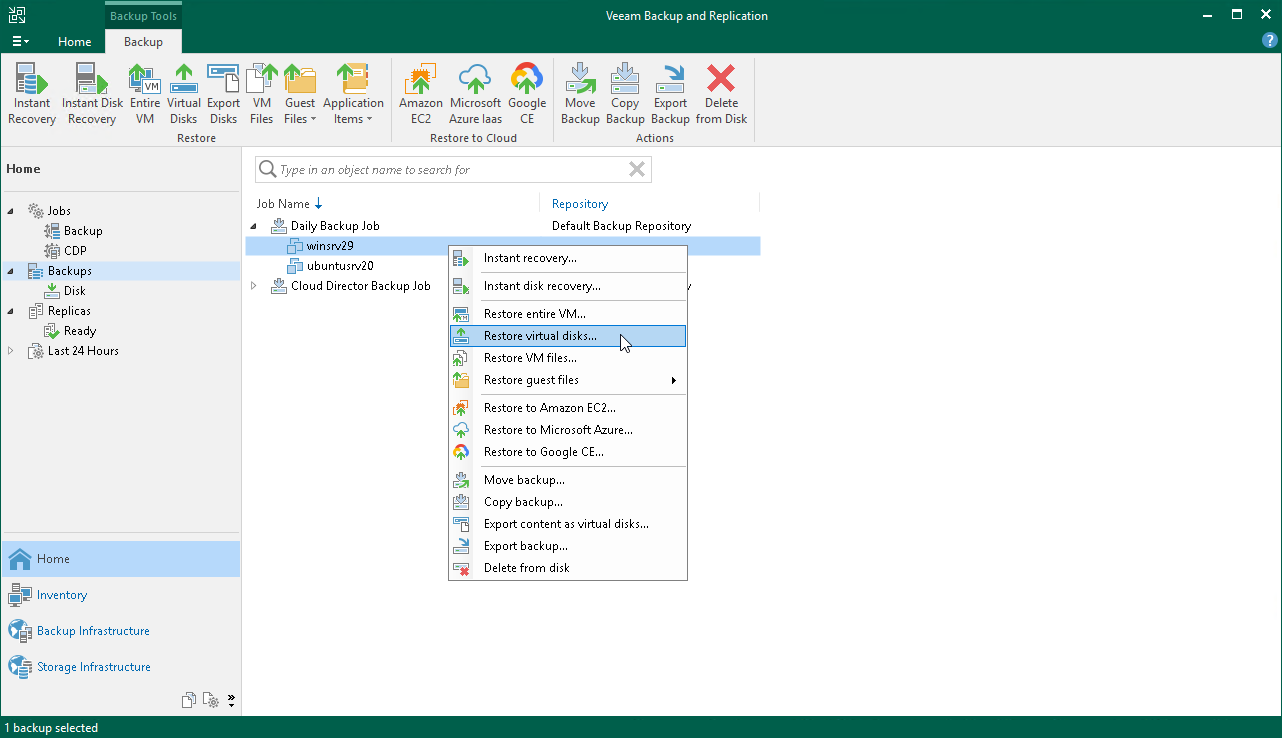
To check whether restore points are created, open the inventory pane of the **Home** view and select the **Backups** node. Then, expand the backup job and verify that there is at least one restore point available for the VM.

* During the virtual disk restore, Veeam Backup & Replication turns off the target VM (the VM to which you plan to attach the restored virtual disk) to reconfigure its settings and connect restored disks. It is recommended that you stop all activities on the target VM for the restore period.

**Restoring Virtual Disks**

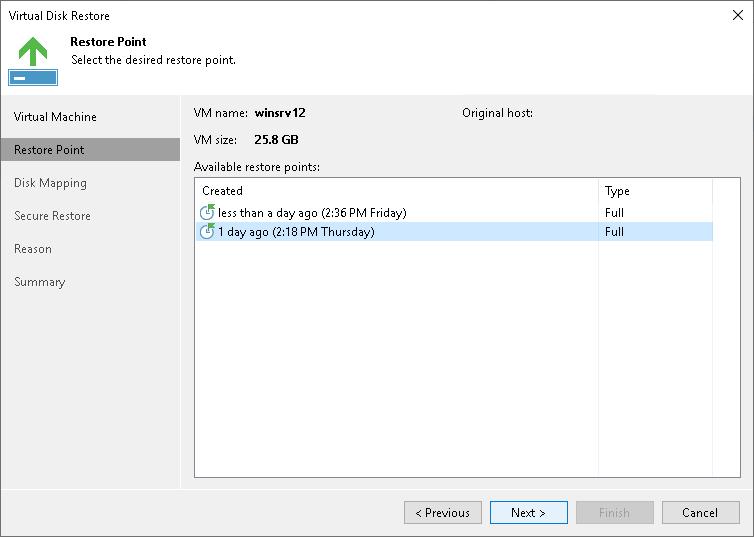
To restore a VM virtual disk and attach it to another VM as a new drive, do the following:

1. Open the **Home** view.
2. In the inventory pane, select the **Backups**>**Disk** node. Expand the backup job in the working area, right-click a VM and select **Restore virtual disks** to launch the **Virtual Disk Restore**wizard.

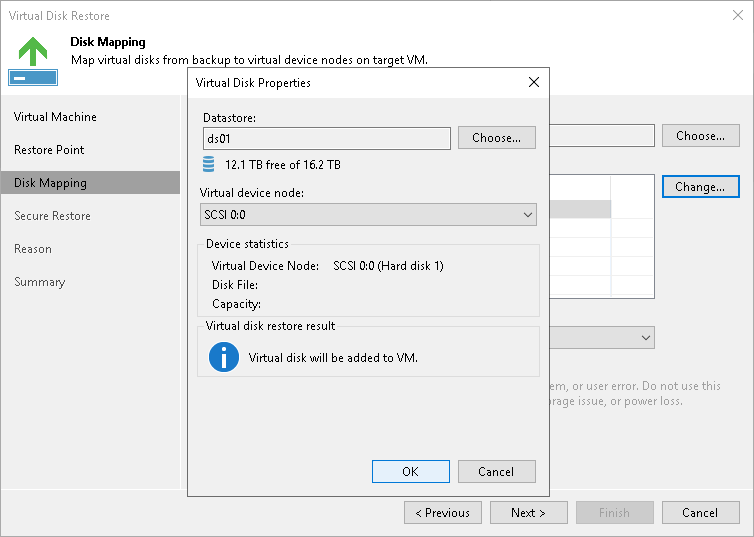
[](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/images/disk_restore_launch.png)

1. At the **Restore Point** step of the wizard, select a restore point.

If you select an incremental restore point, Veeam Backup & Replication automatically restores data blocks from the full backup file and the chain of incremental backup files.



1. At the **Disk Mapping** step of the wizard, do the following:
2. Click **Browse** and select the VM to which the restored hard disk must be attached.
3. Select the virtual hard disk that you want to restore.
4. To change the disk format, select the required option from the **Restored disk type** list: same as the original disk, thin or thick (lazy or eager zeroed).
5. Select the VM disk in the list and click **Change**. From the**Virtual device node** list, select a node that is not occupied yet. Click **OK**.



1. At the **Secure Restore** step of the wizard, enable scanning of the machine or leave the default setting.

If secure restore is enabled, Veeam Backup & Replication uses antivirus software to scan machine data before restoring the machine to the production environment. For details, see [Secure Restore](https://helpcenter.veeam.com/docs/backup/vsphere/av_scan_about.html?ver=120) in the Veeam Backup & Replication User Guide.

1. At the **Reason** step of the wizard, specify the reason for restoring.
2. At the last step of the wizard, select the **Power on VM after restoring** check box and click **Finish**.

# **Restoring VM Guest OS Files (FAT, NTFS, ReFS)**

On This Page

* [Before You Begin](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/flr_windows.html?ver=120#before-you-begin)
* [Restoring Guest OS Files](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/flr_windows.html?ver=120#restoring-guest-os-files)
* [Reference](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/flr_windows.html?ver=120#reference)

You can restore individual files from the backup of a Microsoft Windows VM. For this purpose, Veeam Backup & Replication provides the **File-Level Restore** wizard.

**Before You Begin**

Consider the following:

* You can restore guest OS files from a backup that has at least one successfully created restore point.

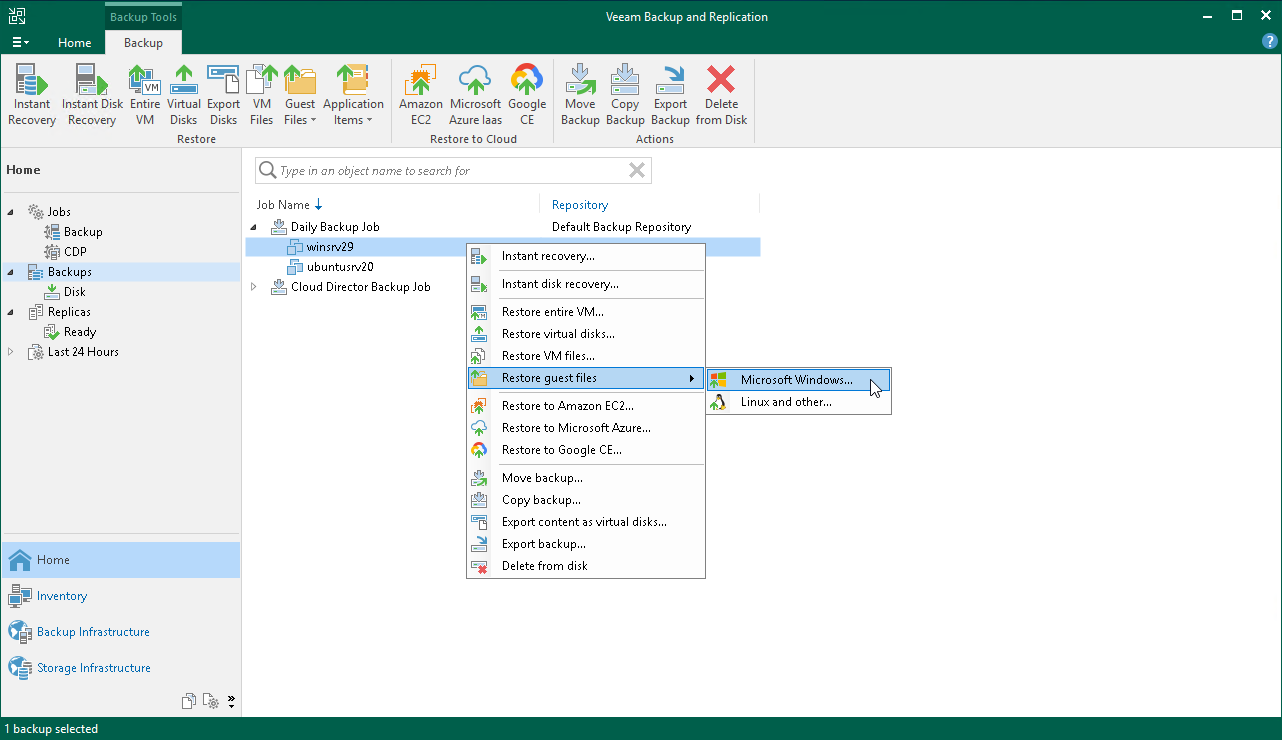
To check whether restore points are created, open the inventory pane of the **Home** view and select the **Backups** node. Then, expand the backup job and verify that there is at least one restore point available for the VM.

* You cannot restore files from a backup created in the reverse incremental mode if the backup job is being performed. If the backup is created in the incremental backup mode and the backup job is being performed, you can restore files from any available restore point.
* You cannot restore VM guest OS files from a running replica or if the replication job with the necessary VM is being performed.

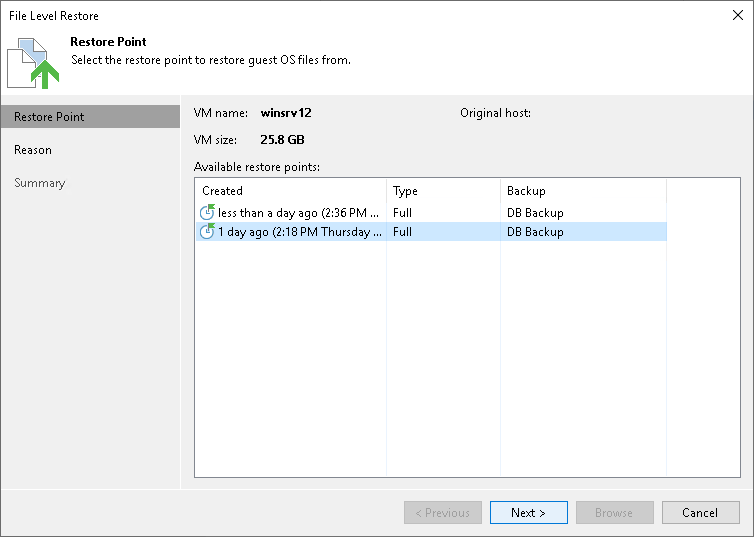
**Restoring Guest OS Files**

To restore guest OS files from a Microsoft Windows VM:

1. Open the **Home** view.
2. In the inventory pane, select the **Backups**>**Disk** node. Expand a backup job in the working area, right-click a VM and choose **Restore guest files**>**Microsoft Windows** to launch the **File Level Restore** wizard.

[](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/images/flr_launch.png)

1. At the **Restore Point** step of the wizard, select the necessary restore point.



1. At the **Reason** step of the wizard, specify the reason for restoring VM guest OS files.
2. At the last step of the wizard, click **Finish**.
3. Veeam Backup & Replication will display the **Backup Browser** window with the file system tree of the VM. Right-click the necessary file or folder, select **Copy To**.
4. In the opened window, specify the location to which you want to restore files or folders. This location is a network shared folder or folder on the backup server.

# **Restoring VM Guest OS Files (Linux, Unix, etc)**

On This Page

* [Before You Begin](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/flr_linux.html?ver=120#before-you-begin)
* [Restoring Guest OS Files](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/flr_linux.html?ver=120#restoring-guest-os-files)
* [Reference](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/flr_linux.html?ver=120#reference)

You can restore individual files and folders from file systems of Linux-based OSes. For this purpose, Veeam Backup & Replication provides the multi-OS **File-Level Restore** wizard. The multi-OS restore wizard allows you to restore guest OS files for such OSes as Linux, Unix, BSD, macOS and others.

To restore files from VM guest OS, Veeam Backup & Replication uses a helper appliance. The helper appliance is a helper VM running a stripped-down Linux kernel that has a minimal set of components. When you perform file-level restore, Veeam Backup & Replication automatically starts the appliance and mounts VM disks to the helper appliance as virtual hard drives. Virtual disks are mounted directly from backup files, without prior extraction of the backup content. This makes the restore process much faster.

**Before You Begin**

Consider the following:

* Check the supported file systems. For details, see the [File-Level Restore](https://helpcenter.veeam.com/docs/backup/vsphere/platform_support.html?ver=120) section in the Veeam Backup & Replication User Guide.
* You can restore guest OS files from a backup that has at least one successfully created restore point.

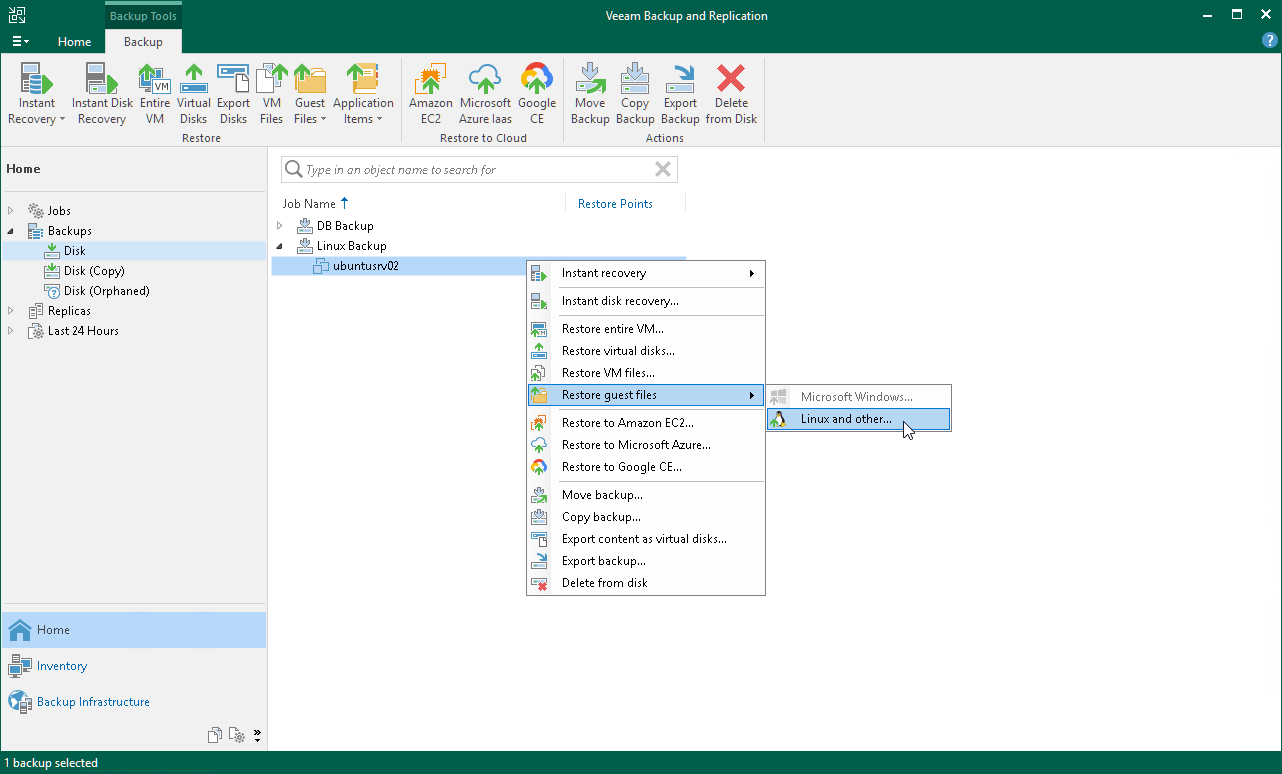
To check whether restore points are created, open the inventory pane of the **Home** view and select the **Backups** node. Then, expand the backup job and verify that there is at least one restore point available for the VM.

* You cannot restore files from reverse incremental backups.
* You cannot restore files from a VM being currently backed up or replicated.

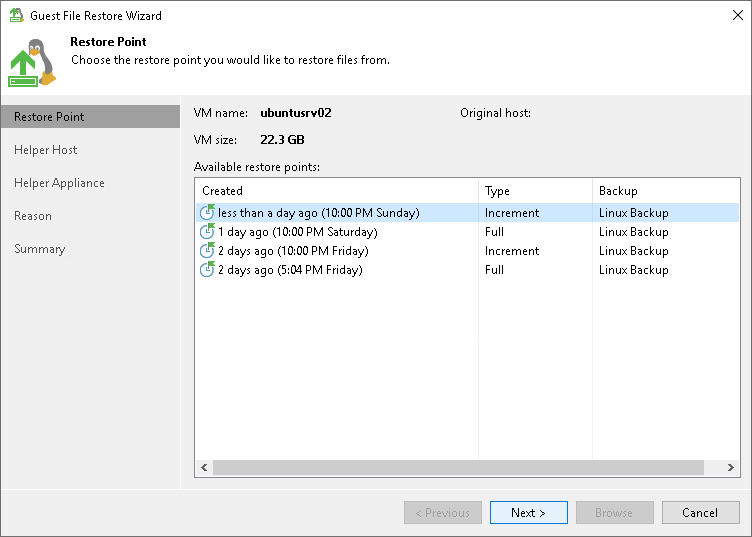
**Restoring Guest OS Files**

To restore guest OS files from a Linux-based VM, do the following.

1. Open the **Home** view.
2. In the inventory pane, select the **Backups**>**Disk** node. Expand a backup job in the working area, right-click a VM and select **Restore guest files**>**Linux and other** to launch the **Guest File Restore** wizard.

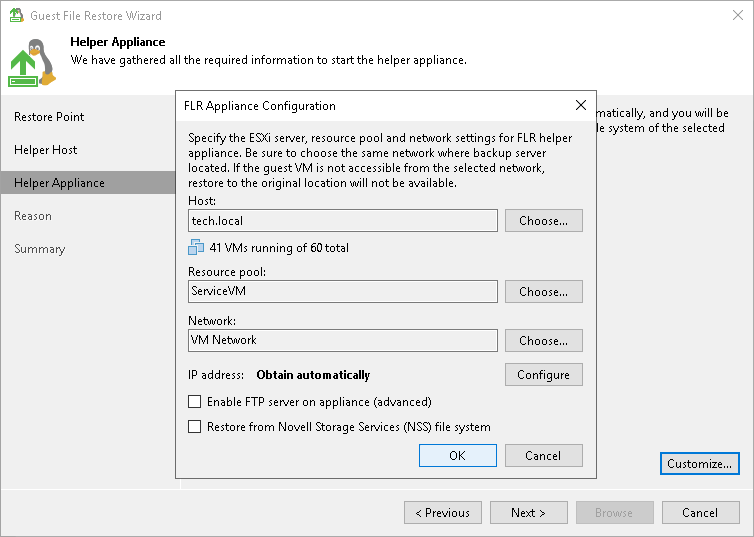
[](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/images/multios_launch.png)

1. At the **Restore Point** step of the wizard, select a restore point.



1. At the **Helper Host** leave the default settings.
2. At the **Helper Appliance** step of the wizard, click **Customize** to specify settings for the helper appliance. Select the ESXi host, resource pool and network on which the helper appliance will run.

If you are restoring files from the NSS file system, select the**Restore from Novell Storage Services (NSS) file system** check box.



1. At the **Reason** step of the wizard, specify the reason for restoring.
2. At the last step of the wizard, click **Finish**. Note that the helper appliance can boot about 20 seconds.
3. Veeam Backup & Replication will display the **Backup Browser** with the file system tree of the VM. Right-click a file or folder, select **Copy To**.
4. In the **Select Destination** window, do the following:
5. In the **Server** field, select the server to which you want to restore files.
6. In the **Path to folder** field, specify a destination folder.
7. Click **Restore**.

# **Restoring Application Items**

On This Page

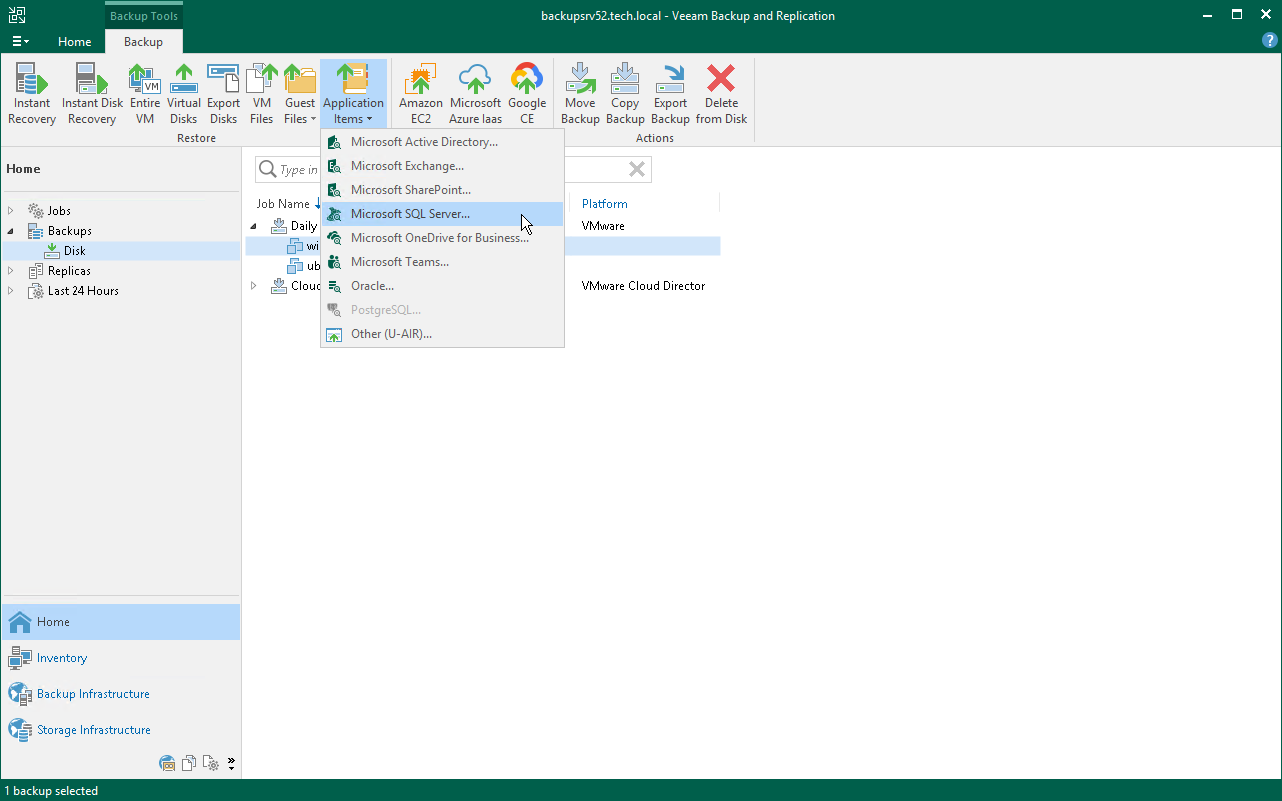
* [Reference](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/recover_database.html?ver=120#reference)

If you have an application-aware backup, you can restore application items for Microsoft SQL Server, Microsoft Active Directory, Microsoft Exchange, Microsoft SharePoint, and Oracle Database. To restore application items, Veeam Backup & Replication uses special built-in tools — Veeam Explorers.

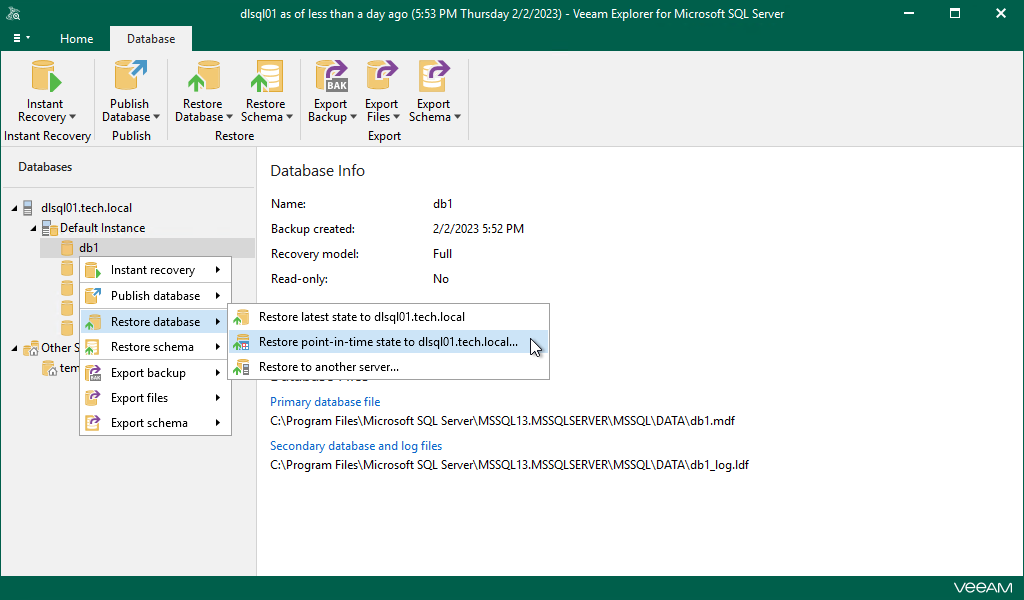
Veeam Explorers mount the file system of the backed up VM, detect available applications and display their content in the convenient interface. You can then browse for necessary application items and restore them to the original or new location. For details, see [Veeam Backup Explorers User Guide](https://helpcenter.veeam.com/docs/backup/explorers/explorers_introduction.html?ver=120).

In this section, you will learn how to restore application items for the Microsoft SQL Server. For this purpose, you will use the backup created in the [Creating Application-Aware Backup Job](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/ms_sql_backup_job.html) section.

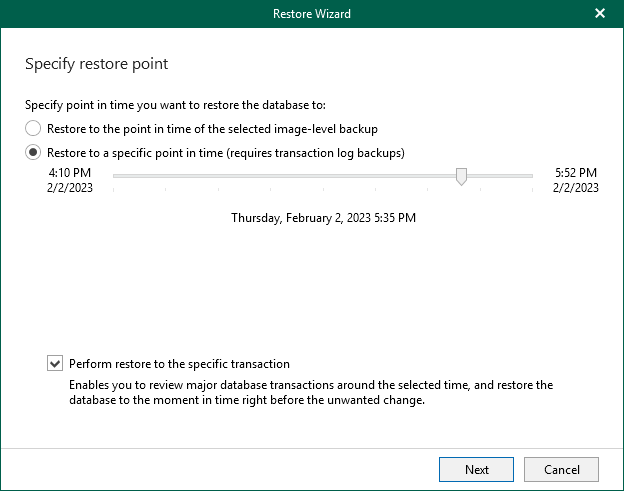
1. In the inventory pane of the **Home** view, click the **Backups** node.
2. In the working area, expand the backup job that processes the VM with Microsoft SQL Server. Select the VM and click **Restore application items** > **Microsoft SQL Server databases** on the ribbon to open the **Microsoft SQL Server Database Restore** wizard.

[](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/images/sql_restore_launch.png)

1. At the **Restore Point** step of the wizard, select the required restore point.
2. At the **Reason** step of the wizard, specify the reason for restoring.
3. At the last step of the wizard, click **Finish** to start the recovery process.
4. Veeam Backup & Replication will display the**Veeam Explorer for Microsoft SQL Server** window with available databases.
5. In the **Databases** pane of the window, right-click a database and select**Restore point-in-time state to <Microsoft SQL Server\Instance Name>**.

[](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/images/sql_restore_db.png)

1. At the **Specify restore point** step of the wizard:
2. Select the **Restore to a specific point in time** option.
3. Use the slider to define the exact point in time to which you want to restore the database.
4. Select the **Perform restore to the specific transaction** check box and click **Next**.



1. At the **Fine-tune the restore point** step of the wizard, select the transaction to which you want to restore the database and click **Restore**.

Veeam Backup & Replication will start restoring the database to the selected transaction. When the restore process is complete, Veeam Explorer for Microsoft SQL Server will display a popup message with the results of the restore operation.

**Reference**

# **Exporting Disks**

On This Page

* [Before You Begin](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/exporting_disks.html?ver=120#before-you-begin)
* [Exporting Disks](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/exporting_disks.html?ver=120#exporting-disks)
* [Reference](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/exporting_disks.html?ver=120#reference)

Veeam Backup & Replication allows you to export disks, that is, convert disks of different workloads (EC2 instances, Microsoft Azure VMs and so on) in the VMDK, VHD or VHDX formats. You can save the exported disks to any server added to the backup infrastructure or place disks on a datastore connected to a host.

**Before You Begin**

Before you export content as virtual disks, consider the following:

* You can export disks from a backup that has at least one successfully created restore point.

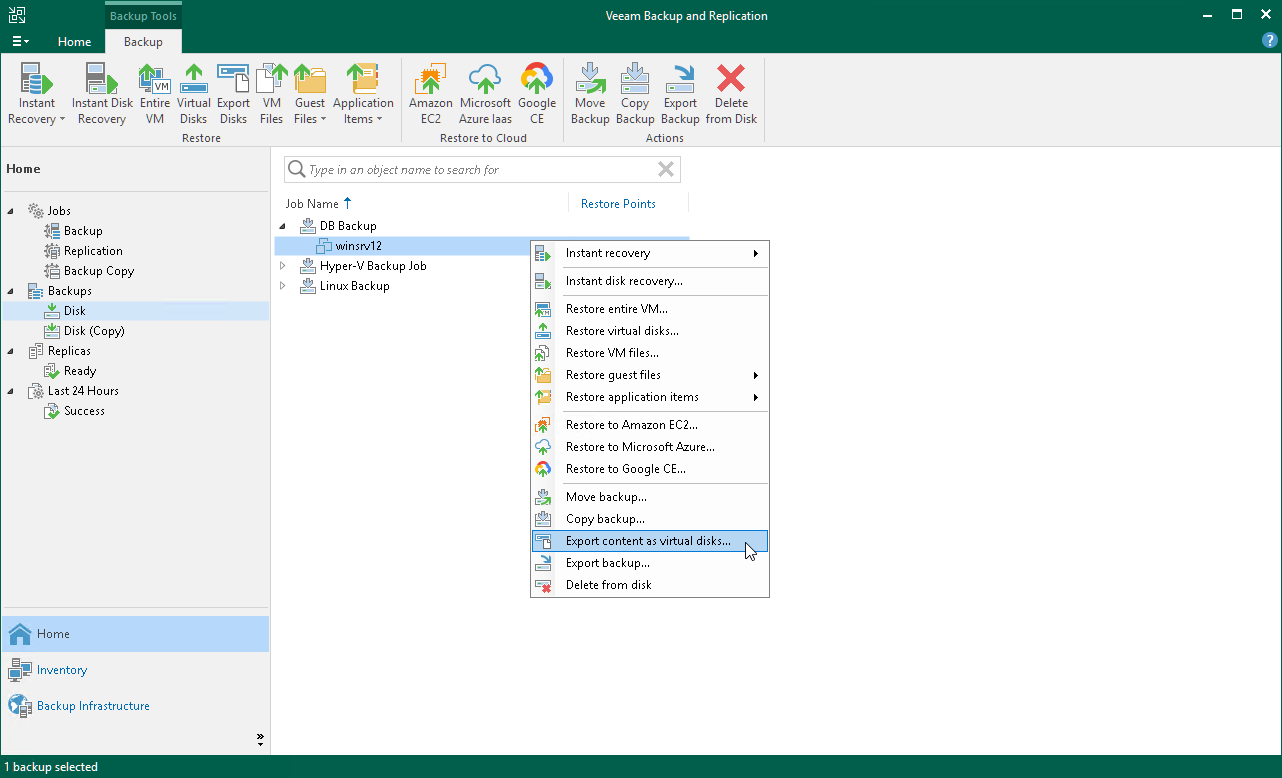
To check whether restore points are created, open the inventory pane of the **Home** view and select the **Backups** node. Then, expand the backup job and verify that there is at least one restore point available for the VM.

* If you export disks to an ESXi datastore, VMDK format is the only available option.

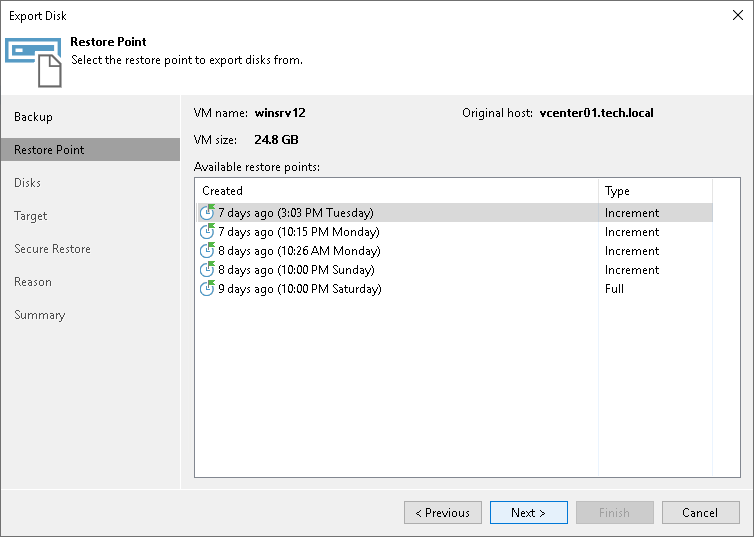
**Exporting Disks**

To export disks from backups and convert them into VHD/VHDX format, do the following:

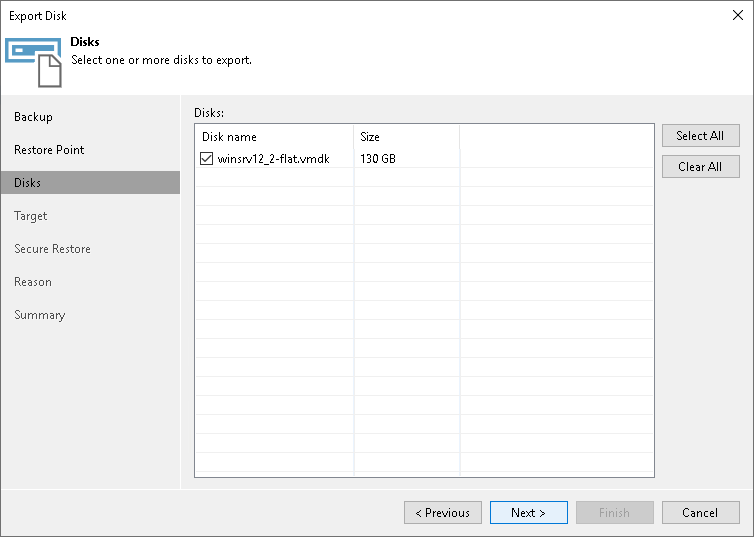
1. Open the **Home** view.
2. In the inventory pane, select the **Backups** > **Disk** node. Expand the backup job in the working area, right-click a VM and select**Export content as virtual disks** to launch the **Export Disk** wizard.

[](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/images/vm_export_disk_launch.png)

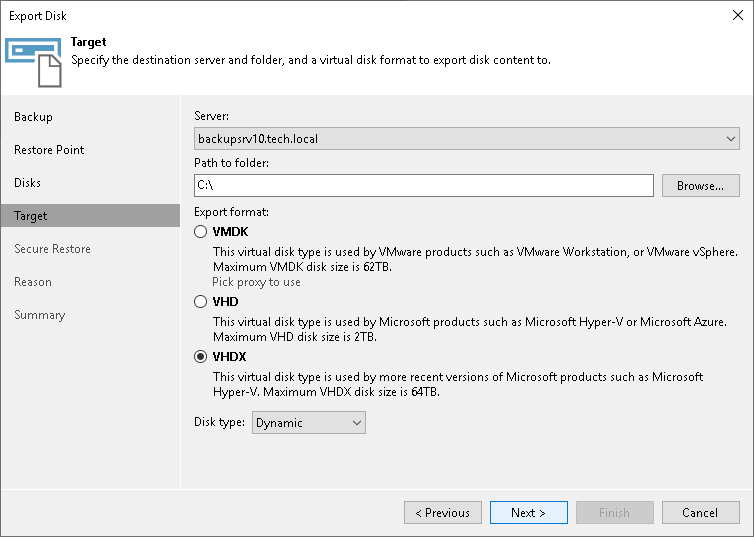
1. At the **Restore Point** step of the wizard, select a restore point.



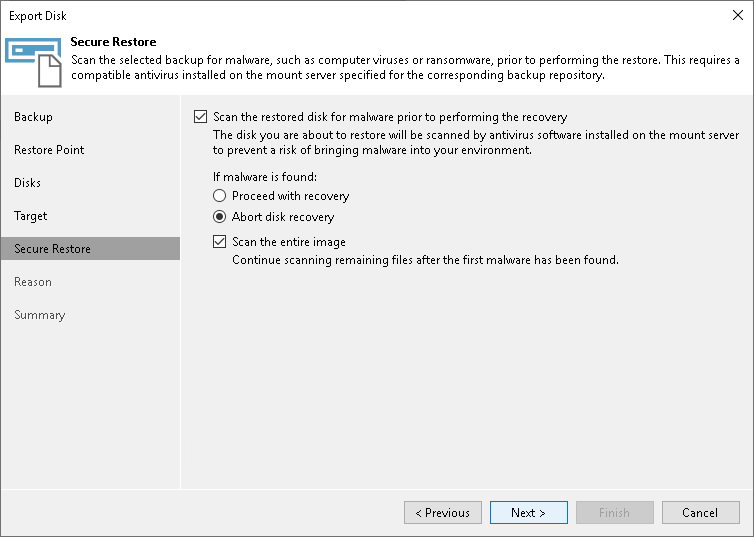
1. At the **Disks** step of the wizard, select which disks you want to export.



1. At the **Target** step of the wizard, select the destination for disk export and format in which you want to save the resulting virtual disks:
2. From the **Server** list, select a server on which the resulting virtual disks must be saved.
3. In the **Path to folder** field, specify a datastore or folder on the server where the virtual disks must be placed.
4. In the**Export format** list, select VHD/VHDX format to save the resulting virtual disk in the Microsoft Hyper-V VHD/VHDX format.
5. From the**Disk Type** drop-down list, select a disk type for the exported disks.



1. At the**Secure Restore** step of the wizard, you can instruct Veeam Backup & Replication to perform secure restore — scan exported disk data with antivirus software before restoring the disk. For more information on secure restore, see [Secure Restore](https://helpcenter.veeam.com/docs/backup/vsphere/av_scan_about.html?ver=120).



1. At the **Reason** step of the wizard, enter a reason for disk export.
2. At the **Summary** step of the wizard, review the configured settings and click **Finish**.

# **Restoring Data of Physical Machines**

On This Page

* [Restoring Files and Folders](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/restoring_from_agent_backups.html?ver=120#restoring-files-and-folders)

Veeam Backup & Replication allows you to restore data of physical machines. You can perform the following data restore tasks with Veeam Agent backups:

* [Restoring Veeam Agent Backup to vSphere VM](https://helpcenter.veeam.com/docs/backup/agents/integration_instant_restore_vsphere.html?ver=120)
* [Restoring Veeam Agent Backup to Hyper-V VM](https://helpcenter.veeam.com/docs/backup/agents/integration_instant_restore_hyperv.html?ver=120)
* [Restoring to Microsoft Azure](https://helpcenter.veeam.com/docs/backup/agents/integration_restore_to_azure.html?ver=120)
* [Restoring to Amazon EC2](https://helpcenter.veeam.com/docs/backup/agents/integration_restore_to_amazon.html?ver=120)
* [Restoring to Google Cloud Platform](https://helpcenter.veeam.com/docs/backup/agents/integration_restore_to_google.html?ver=120)
* [Restoring Volumes](https://helpcenter.veeam.com/docs/backup/agents/integration_volume_restore.html?ver=120)
* [Restoring Files and Folders](https://helpcenter.veeam.com/docs/backup/agents/integration_flr.html?ver=120)
* [Restoring Application Items](https://helpcenter.veeam.com/docs/backup/agents/integration_explorers.html?ver=120)

In this section, you will learn how to restore computer files and folders. For more information on other restore processes, follow the links in the list.

**Restoring Files and Folders**

The procedure of file-level restore from a Veeam Agent backup is similar to the same procedure for a VM backup. The difference is that you select a Veeam Agent backup instead of a VM backup in the **File Level Restore** wizard. To learn more, see [Restoring VM Files](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/vm_files_restore.html).

[](https://helpcenter.veeam.com/docs/backup/qsg_vsphere/images/agent_restore_flr.png)

# **Restoring Veeam Agent Backup to vSphere VM**

You can use the Veeam Backup & Replication console to restore a Veeam Agent computer as a VMware vSphere VM in your virtualization environment. For Instant Recovery to a vSphere VM, you can use backups of Microsoft Windows and Linux computers created on the Veeam backup repository. You cannot perform this operation with Veeam Agent backups created on the Veeam Cloud Connect repository.

A restored VMware vSphere VM has the same settings as a backed-up Veeam Agent computer. During the restore process, Veeam Backup & Replication retrieves settings of the Veeam Agent computer from the backup and applies them to the target VM. These settings include:

* Amount of RAM
* Number of CPU cores
* Number of network adapters
* Network adapter settings
* BIOS UUID

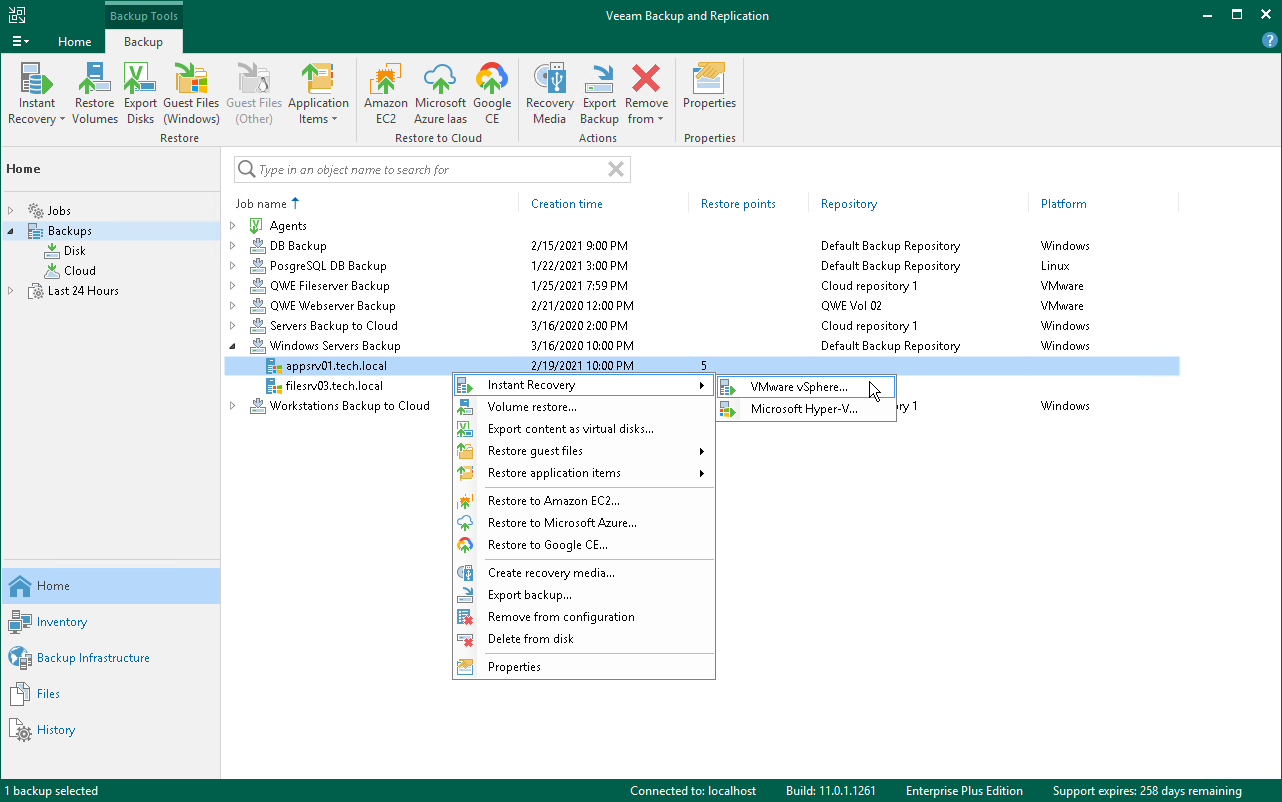
If you do not want to preserve the backed-up machine UUID for a VMware vSphere VM, you can create a new UUID during the Instant Recovery configuration process.

* Number of disks and volumes
* Size of volumes

If you restore a Veeam Agent computer to a VMware vSphere VM, consider the following:

* Make sure that the target host has enough resources for a new VM. Otherwise, your VM will reduce the target host performance.
* If you restore a workload to the production network, make sure that the original workload is powered off.
* [For backups of Linux computers] If the disk you want to restore contains an LVM volume group, Veeam Agent will restore the original disk and the LVM volume group as 2 separate disks. Among other things, this leads to the increase of the required storage space. For example, you restore a machine with 2 disks, and a separate LVM volume group is configured on each of these disks. In this case, Veeam Agent will restore 4 disks. The restored disks will consume storage space equal to the size of 2 original disks and 2 LVM volume groups from these disks.

The procedure of Instant Recovery for a Veeam Agent computer practically does not differ from the same procedure for a VM. The main difference from Instant Recovery is that you do not need to select the recovery mode, because Veeam Agent computers are always restored to a new location. To learn more, see the [Performing Instant Recovery of Workloads to VMware vSphere VMs](https://helpcenter.veeam.com/docs/backup/vsphere/performing_instant_recovery_vm.html?ver=120) section in the Veeam Backup & Replication User Guide.

[](https://helpcenter.veeam.com/docs/backup/agents/images/agent_restore_instant_vmware.png)

# **Restoring Veeam Agent Backup to Hyper-V VM**

You can use the Veeam Backup & Replication console to restore a Veeam Agent computer as a Hyper-V VM in your virtualization environment. For Instant Recovery to a Hyper-V VM, you can use backups of Microsoft Windows and Linux computers created on the Veeam backup repository. You cannot use backups created on the Veeam Cloud Connect repository for this operation.

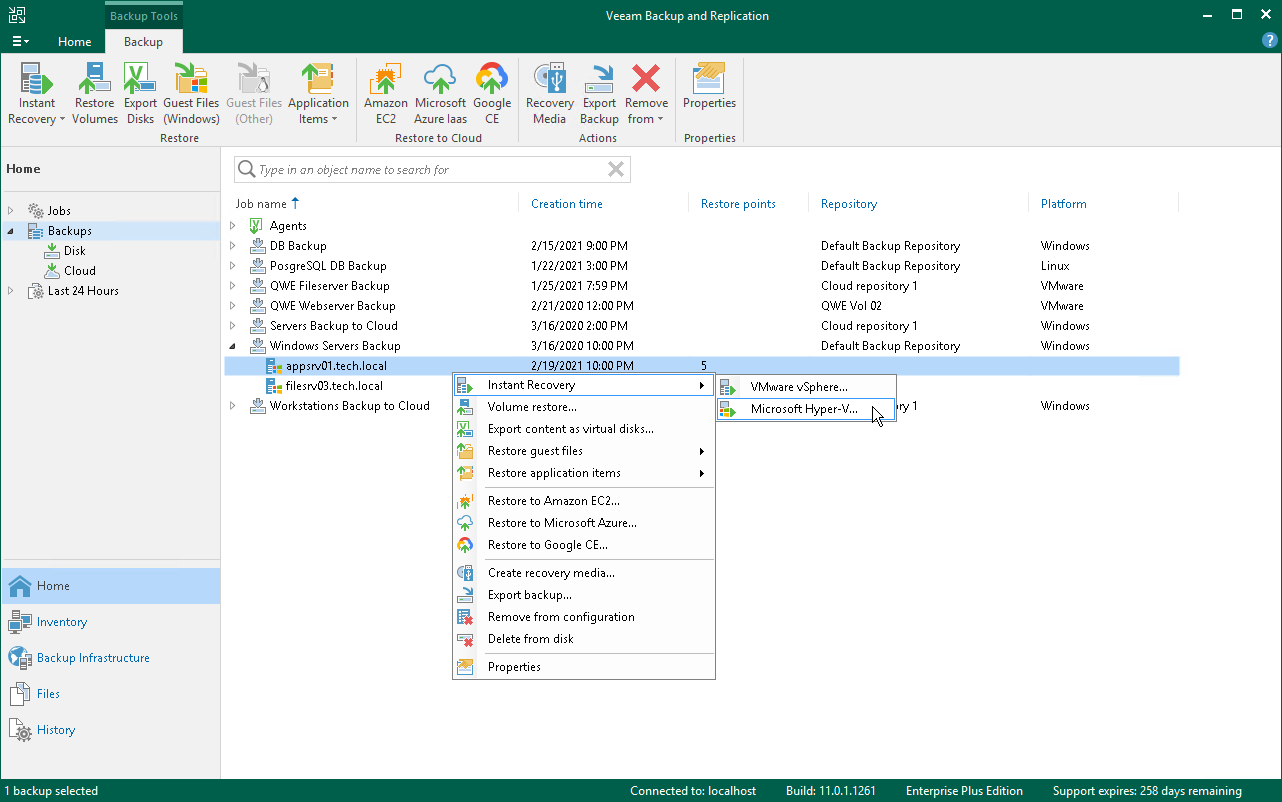
Mind that to restore to a Hyper-V VM using a backup of a Linux computer, you must consider the Hyper-V limitations. To learn more, see [this Microsoft article](https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/supported-linux-and-freebsd-virtual-machines-for-hyper-v-on-windows).

A restored Hyper-V VM has the same settings as a backed-up Veeam Agent computer. During the restore process, Veeam Backup & Replication retrieves settings of the Veeam Agent computer from the backup and applies them to the target VM.

If you restore a Veeam Agent computer to a Hyper-V VM, consider the following:

* [For backups of Microsoft Windows computers] You cannot recover an EFI-based Veeam Agent computer that runs Windows 7, Windows Server 2008 or Windows Server 2008 R2 to a Hyper-V VM. These OSes can be restored only to a Generation 1 VM that does not support EFI. To learn more, see [this Microsoft article](https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/plan/should-i-create-a-generation-1-or-2-virtual-machine-in-hyper-v#BKMK_Windows).
* Make sure that the target host has enough resources for a new VM. Otherwise, your VM will reduce the target host performance.
* Veeam Agent computer disks are recovered as dynamically expanding virtual disks.
* By default, Veeam Backup & Replication automatically powers on a VM after restore. If you do not want to power on a VM after restore, you can change this setting during the Instant Recovery configuration process.
* [For backups of Linux computers] If the disk you want to restore contains an LVM volume group, Veeam Agent will restore the original disk and the LVM volume group as 2 separate disks. Among other things, this leads to the increase of the required storage space. For example, you restore a machine with 2 disks, and a separate LVM volume group is configured on each of these disks. In this case, Veeam Agent will restore 4 disks. The restored disks will consume storage space equal to the size of 2 original disks and 2 LVM volume groups from these disks.

The procedure of Instant Recovery for a Veeam Agent computer practically does not differ from the same procedure for a VM. The main difference from Instant Recovery is that you do not need to select the recovery mode, because Veeam Agent computers are always restored to a new location. To learn more, see the [Performing Instant Recovery of Workloads to Hyper-V VMs](https://helpcenter.veeam.com/docs/backup/vsphere/performing_instant_recovery_hv_vm.html?ver=120) section in the Veeam Backup & Replication User Guide.

[](https://helpcenter.veeam.com/docs/backup/agents/images/agent_restore_instant_hv.png)

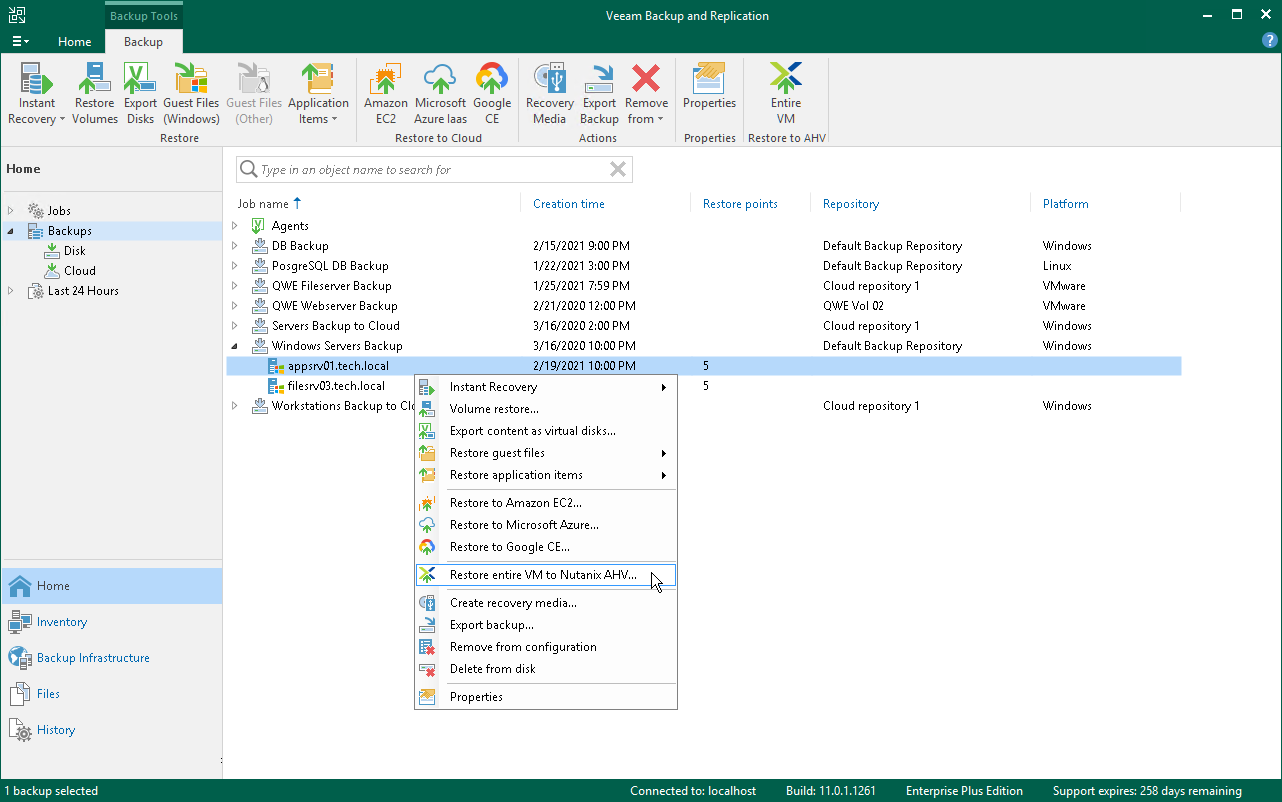
# **Restoring Veeam Agent Backup to Nutanix VM**

You can use the Veeam Backup & Replication console to restore a Veeam Agent computer as a Nutanix AHV VM in your virtualization environment. For restore to Nutanix AHV, you can use backups of Microsoft Windows and Linux computers created on the Veeam backup repository. You cannot perform this operation with Veeam Agent backups created on the Veeam Cloud Connect repository.

Mind that to restore to Nutanix AHV, you must install Nutanix AHV Plug-in on the Veeam Backup & Replication server. To learn more, see the [Installation](https://helpcenter.veeam.com/docs/van/userguide/install_ahv_services.html?ver=40) section in the Veeam Backup for Nutanix AHV User Guide.

|  |
| --- |
| **IMPORTANT** |
| [For backups of Linux computers] If the disk you want to restore contains an LVM volume group, Veeam Agent will restore the original disk and the LVM volume group as 2 separate disks. Among other things, this leads to the increase of the required storage space. For example, you restore a machine with 2 disks, and a separate LVM volume group is configured on each of these disks. In this case, Veeam Agent will restore 4 disks. The restored disks will consume storage space equal to the size of 2 original disks and 2 LVM volume groups from these disks. |

The procedure of restore to Nutanix AHV for a Veeam Agent computer practically does not differ from the same procedure for a VM. To learn more about restore to Nutanix AHV, see the [Restoring VMs Using Veeam Backup & Replication Console](https://helpcenter.veeam.com/docs/van/userguide/restore_vm_ahv.html?ver=40) section in the Veeam Backup for Nutanix AHV User Guide.

[](https://helpcenter.veeam.com/docs/backup/agents/images/agent_restore_nutanix.png)

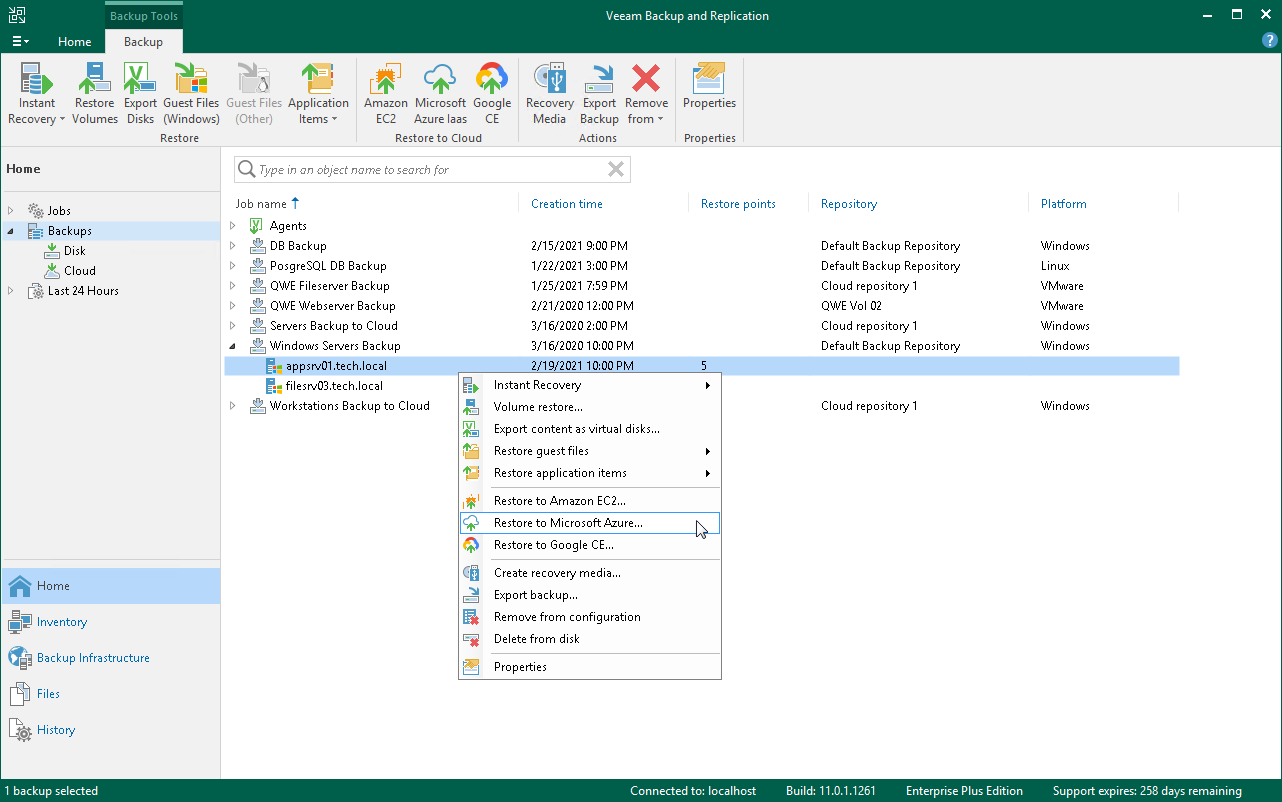
# **Restoring to Microsoft Azure**

You can restore computers from Veeam Agent backups to Microsoft Azure. For restore to Microsoft Azure, you can use backups of Microsoft Windows and Linux computers created on the Veeam backup repository. You cannot perform this operation with Veeam Agent backups created on the Veeam Cloud Connect repository. Backups must be created at the entire machine level or volume level.

If you restore a Veeam Agent machine to Microsoft Azure, consider the following:

* If you recover a EFI-based system to Microsoft Azure, Veeam Agent will restore a BIOS-based Generation 1 VM.
* Veeam Backup & Replication offers experimental support for generation 2 VMs within restore to Microsoft Azure feature. To learn more, see the [Generation 2 VM Support](https://helpcenter.veeam.com/docs/backup/vsphere/generation_2_vm_support.html?ver=120) section in the Veeam Backup & Replication User Guide.
* [For backups of Linux computers] If the disk you want to restore contains an LVM volume group, Veeam Agent will restore the original disk and the LVM volume group as 2 separate disks. Among other things, this leads to the increase of the required storage space. For example, you restore a machine with 2 disks, and a separate LVM volume group is configured on each of these disks. In this case, Veeam Agent will restore 4 disks. The restored disks will consume storage space equal to the size of 2 original disks and 2 LVM volume groups from these disks.

The procedure of restore to Microsoft Azure from a Veeam Agent backup practically does not differ from the same procedure for a VM backup. To learn more about restore to Microsoft Azure, see the [Restore to Microsoft Azure](https://helpcenter.veeam.com/docs/backup/vsphere/restore_azure.html?ver=120) section in the Veeam Backup & Replication User Guide.

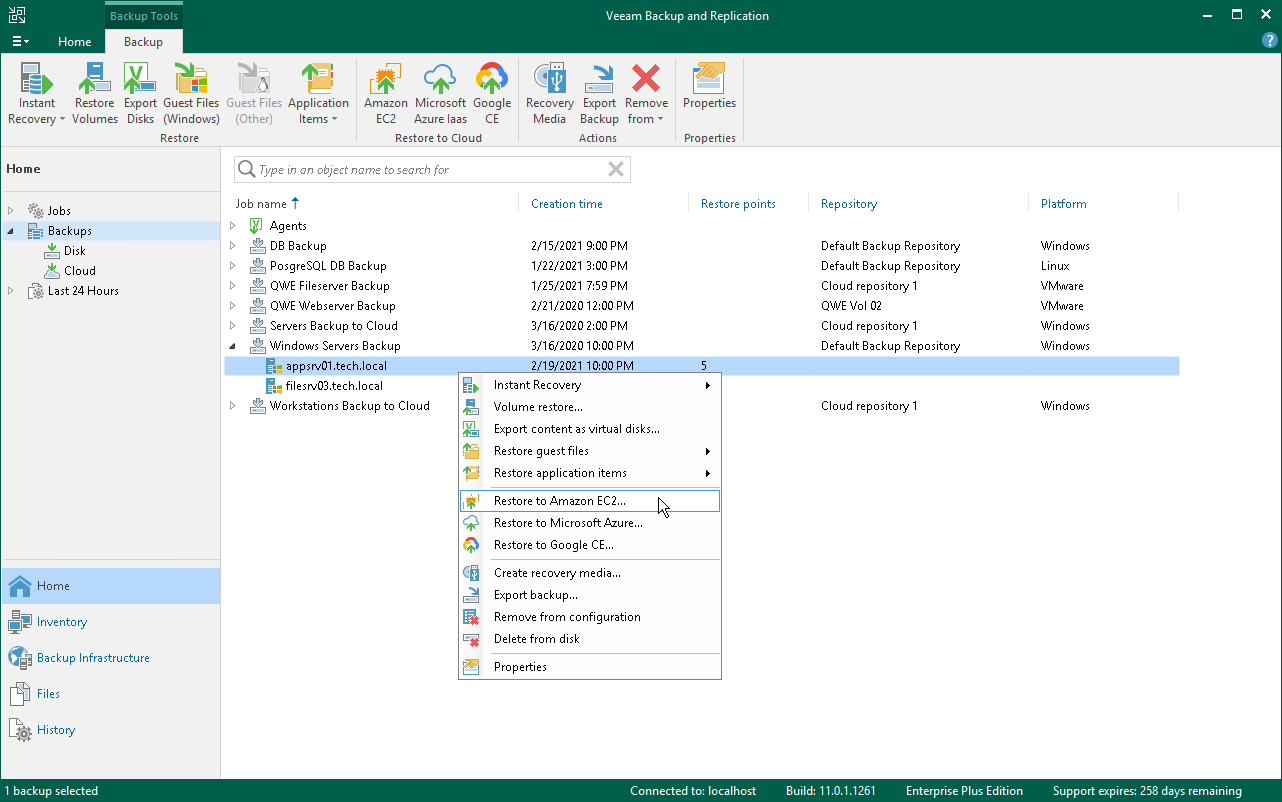
[](https://helpcenter.veeam.com/docs/backup/agents/images/agent_restore_azure.png)

# **Restoring to Amazon EC2**

You can restore computers from Veeam Agent backups to Amazon EC2. For restore to Amazon EC2, you can use backups of Microsoft Windows and Linux computers created on the Veeam backup repository. You cannot perform this operation with Veeam Agent backups created on the Veeam Cloud Connect repository. Backups must be created at the entire machine level or volume level.

|  |
| --- |
| **IMPORTANT** |
| [For backups of Linux computers] If the disk you want to restore contains an LVM volume group, Veeam Agent will restore the original disk and the LVM volume group as 2 separate disks. Among other things, this leads to the increase of the required storage space. For example, you restore a machine with 2 disks, and a separate LVM volume group is configured on each of these disks. In this case, Veeam Agent will restore 4 disks. The restored disks will consume storage space equal to the size of 2 original disks and 2 LVM volume groups from these disks. |

The procedure of restore to Amazon EC2 from a Veeam Agent backup practically does not differ from the same procedure for a VM backup. To learn more about restore to Amazon EC2, see the [Restore to Amazon EC2](https://helpcenter.veeam.com/docs/backup/vsphere/restore_amazon.html?ver=120) section in the Veeam Backup & Replication User Guide.

[](https://helpcenter.veeam.com/docs/backup/agents/images/agent_restore_amazon.png)

# **Restoring Files and Folders**

You can use the Veeam Backup & Replication console to restore individual files and folders from Veeam Agent backups.

For file-level restore, you can use Veeam Agent backups created in the Veeam backup repository or Veeam Cloud Connect repository. For Veeam Agent backups created in the cloud repository, you can perform restore tasks in Veeam Backup & Replication deployed on the tenant backup server. The service provider cannot perform restore tasks with Veeam Agent backups.

Consider the following:

* [For backups of Linux computers] When you perform the file-level restore procedure, Veeam Backup & Replication provides the following options for mounting disks of a Linux computer from the backup or replica:
* Mounting disks to a helper host — a target host where you want to restore files from the backup or any other Linux host.
* Mounting disks to a helper appliance — a helper VM required to mount Linux computer disks from the backup.

If you have selected to mount disks to a helper appliance, it is recommended that you add a vCenter Server and not a standalone ESXi host in the Veeam backup console. If Veeam Backup & Replication is set up to deploy a helper appliance on a standalone ESXi host, after Veeam Backup & Replication removes the helper appliance, the helper VM will be displayed in vCenter as *orphaned*.

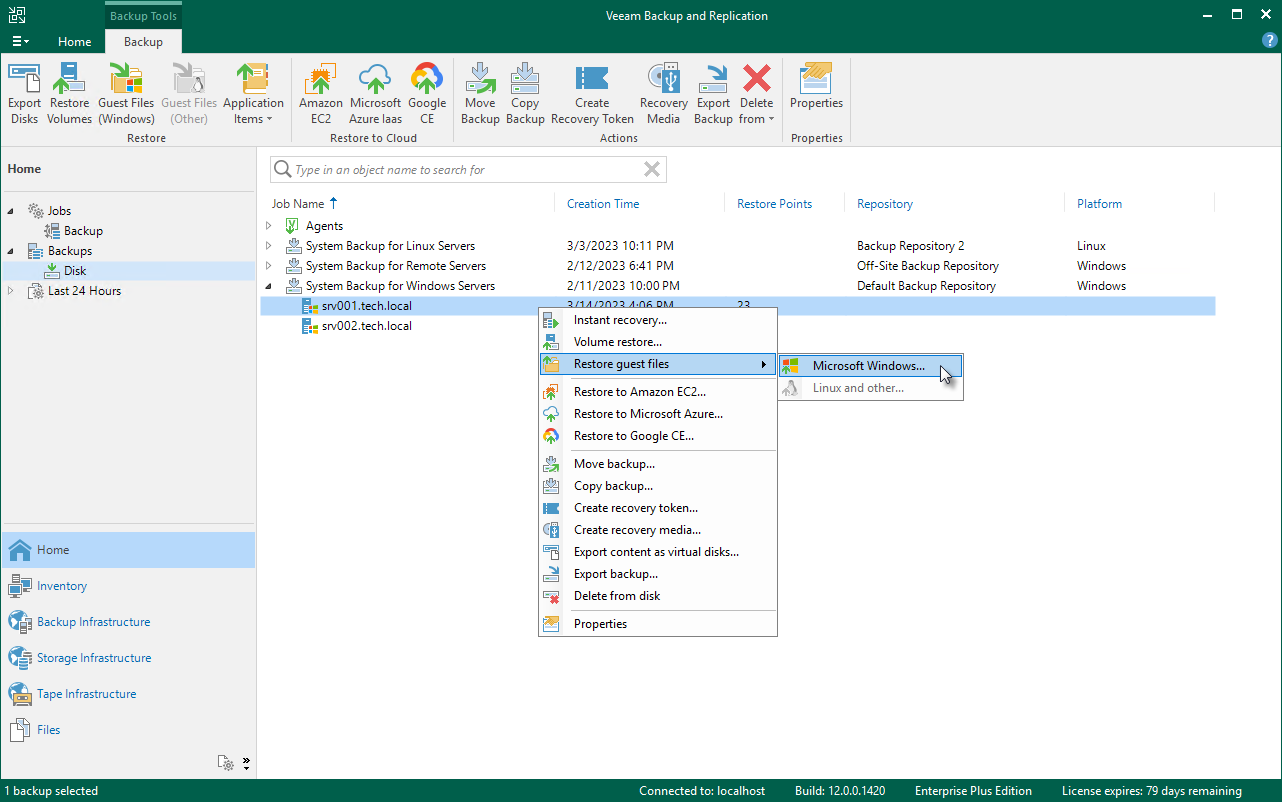
To learn more about these options, see the [Restore from Linux, Unix and Other File Systems](https://helpcenter.veeam.com/docs/backup/vsphere/guest_restore_linux.html?ver=120) section in the Veeam Backup & Replication User Guide.

* [For backups of Microsoft Windows computers] Before you start file-level restore from a backup of a failover cluster, make sure that the cluster is added to a protection group in the Veeam Backup & Replication inventory. The failover cluster may be not present in the inventory, for example, in the following cases:
* The original protection group that contained the cluster was removed from Veeam Backup & Replication.
* You want to restore cluster data from a backup created on another backup server and imported in the Veeam backup console.

In this case, add the failover cluster whose data you want to restore to a protection group.

|  |
| --- |
| **NOTE** |
| When you perform the file-level restore procedure, Veeam Backup & Replication provides the following options for mounting disks of a Linux, Unix or Mac endpoint from the backup or replica:   * Mounting disks to a helper host — a target host where you want to restore files from the backup or any other Linux host. * Mounting disks to a helper appliance — a helper VM required to mount Veeam Agent computer disks from the backup.   If you have selected to mount disks to a helper appliance, it is recommended that you add a vCenter Server and not a standalone ESXi host in the Veeam backup console. If Veeam Backup & Replication is set up to deploy a helper appliance on a standalone ESXi host, after Veeam Backup & Replication removes the helper appliance, the helper VM will be displayed in vCenter as orphaned.  To learn more about these options, see the [Restore from Linux, Unix and Other File Systems](https://helpcenter.veeam.com/docs/backup/vsphere/guest_restore_linux.html?ver=120) section in the Veeam Backup & Replication User Guide. |

The procedure of file-level restore from a Veeam Agent backup practically does not differ from the same procedure for a VM backup. The difference is that you select a Veeam Agent backup instead of a VM backup in the **File Level Restore** wizard. To learn more, see the [Guest OS File Recovery](https://helpcenter.veeam.com/docs/backup/vsphere/guest_file_recovery.html?ver=120) section in the Veeam Backup & Replication User Guide.

[](https://helpcenter.veeam.com/docs/backup/agents/images/am_agent_restore_flr.png)

Backup Calculation

A screenshot of a computer

Description automatically generated with medium confidenceA picture containing text, screenshot, font, number

Description automatically generated