Veeam Cloud Connect

Version 12

Administrator Guide

March, 2023

> **NOTE**
>
> Read the End User Software License Agreement before using the accompanying software programs. Using any part of the software indicates that you accept the terms of the End User Software License Agreement.

Contents

Contacting Veeam Software

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

Customer Support

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

Company Contacts

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

Online Support

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

- Full documentation set: veeam.com/documentation-guides-datasheets.html

- Veeam R&D Forums: forums.veeam.com

About This Document

This guide describes how to deploy and configure the Veeam Cloud Connect infrastructure and use cloud repositories and cloud hosts to store data in the cloud. The document applies to version 12 of Veeam Backup & Replication and all subsequent versions until it is replaced by a new document.

Intended Audience

This document is intended for Service Providers who want to use the Veeam Cloud Connect functionality to provide Backup as a Service and/or Disaster Recovery as a Service to their customers, and Service Provider customers who want to store their data in the cloud.

The document provides a general overview of the Veeam Cloud Connect functionality and should be regarded as a supplement to existing technical documentation. The complete set of documentation for Veeam Backup & Replication can be found at https://www.veeam.com/documentation-guides-datasheets.html.

About Veeam Cloud Connect

Service providers (SP) can use Veeam Backup & Replication to offer cloud repository as a service and disaster recovery as a service to their customers (tenants). Veeam Backup & Replication lets SPs set up the cloud infrastructure so that tenants can send their data to the cloud and store it there in an easy and secure way.

Veeam Backup & Replication does not offer its own cloud for storing tenant data. Instead, it uses SP computing, storage and network resources to configure Veeam Cloud Connect Backup and Veeam Cloud Connect Replication infrastructure components:

- Cloud repositories — storage locations in the cloud that store backups of tenant machines. Cloud repositories can be used as primary storage locations and secondary storage locations to meet the 3-2-1 backup best practice.

- Replication resources — dedicated computing, storage and network resources in the SP virtualization environment. To set up replication resources, the SP configures hardware plans and subscribes tenants to one or several hardware plans. For tenants, hardware plans appear as cloud hosts. Tenants can create VM replicas on cloud hosts and fail over to VM replicas in the cloud in case of a disaster on the production site.

Tenants who want to store their data in the cloud can connect to the SP and write their backups to cloud repositories and/or replicate their VMs to cloud hosts.

Veeam Cloud Connect Infrastructure

To expose cloud resources to tenants, the SP must configure the Veeam Cloud Connect infrastructure.

> **NOTE**
>
> Consider the following:
>
> - The SP must not share Veeam Backup & Replication components (backup server, backup proxies, backup repositories, and so on) between the Veeam Cloud Connect infrastructure and regular Veeam backup infrastructure used to protect the SP virtualization environment.
> - If the SP has multiple backup servers deployed in the Veeam Cloud Connect infrastructure, they must not share Veeam Backup & Replication components between these backup servers.

Veeam Cloud Connect Backup
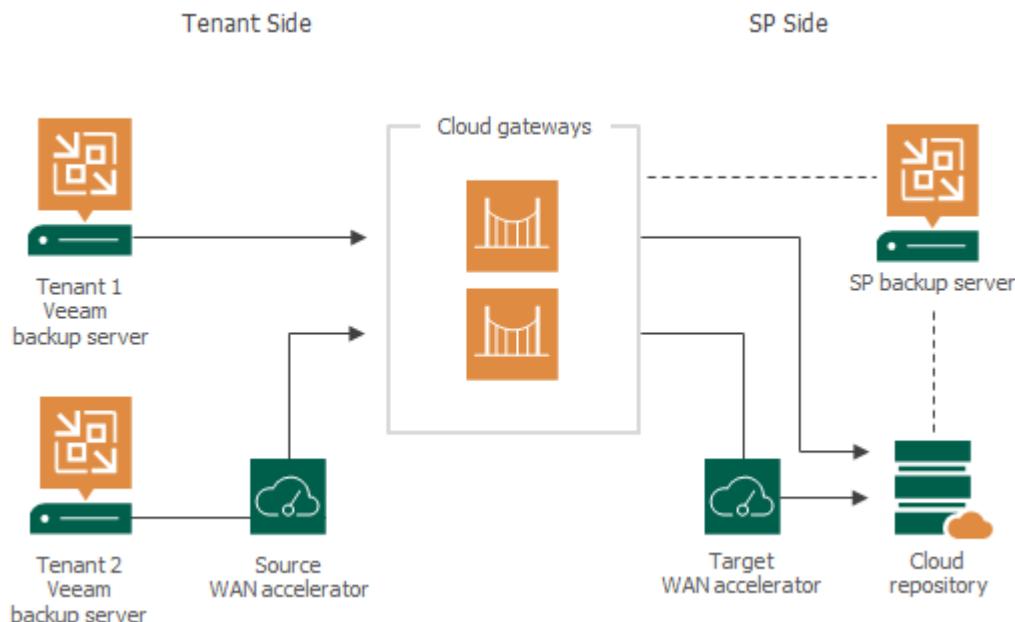
To expose cloud repository resources to tenants, the SP must configure the Veeam Cloud Connect Backup infrastructure. The Veeam Cloud Connect Backup infrastructure comprises the following components:

Components on the SP side

- SP Veeam backup server
- One or several cloud gateways
- One or several cloud repositories
- [Optional] One or several target WAN accelerators

Components on the tenant side

- Tenant Veeam backup server
- [Optional] Source WAN accelerator

Veeam Cloud Connect Replication

To expose cloud host resources to tenants, the SP must configure the Veeam Cloud Connect Replication infrastructure. The Veeam Cloud Connect Replication infrastructure comprises the following components:

Components on the SP side
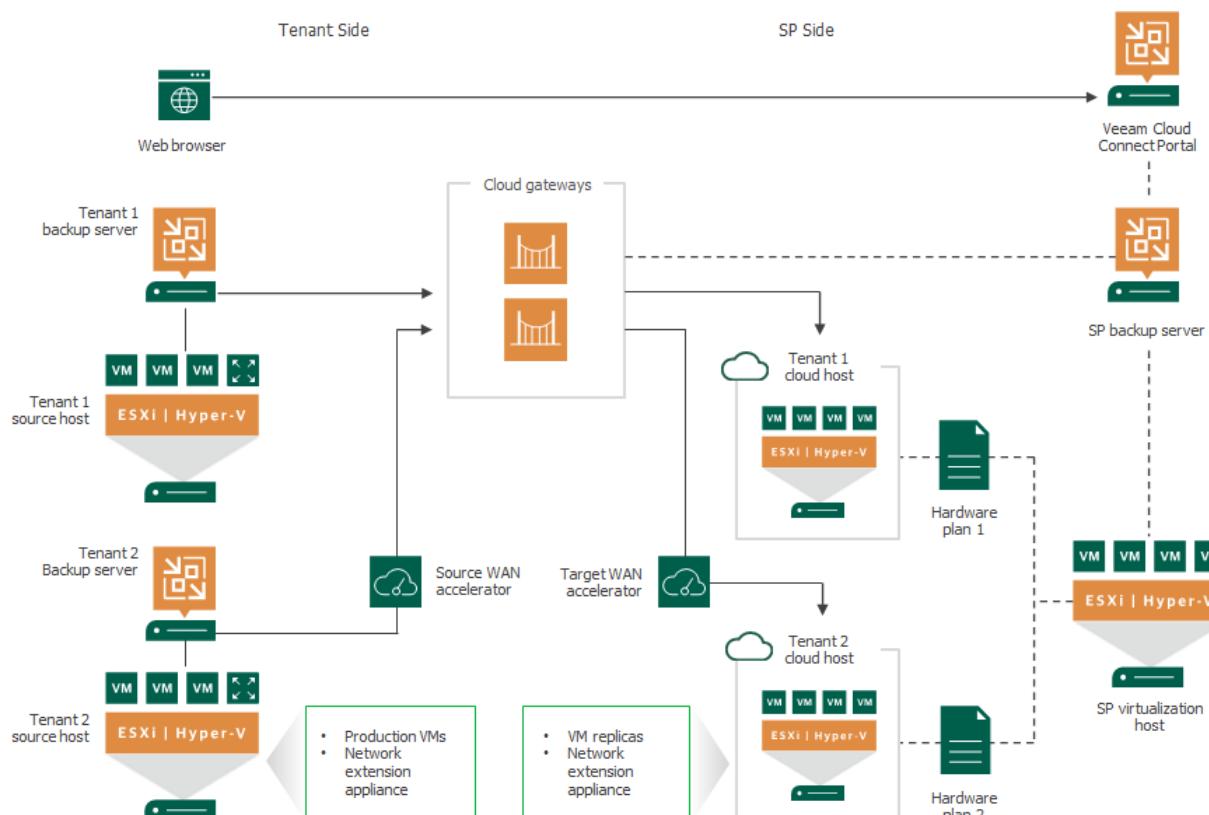
- SP Veeam backup server

- One or several cloud gateways

- One or several hardware plans

- [Optional] One or several network extension appliances

- [Optional] Veeam Cloud Connect Portal

- [Optional] One or several target WAN accelerators

Components on the tenant side

- Tenant Veeam backup server

- One or several network extension appliances

- [Optional] Source WAN accelerator

> **NOTE**
>
> Depending on the replication scenario, the Veeam Cloud Connect Replication infrastructure may require additional components. For example, the SP can use VMware Cloud Director resources instead of hardware plans to provide replication resources to tenants, or offer the CDP functionality to tenants. To learn more, see Continuous Data Protection (CDP) with Veeam Cloud Connect and VMware Cloud Director Support.

SP Veeam Backup Server

The Veeam Cloud Connect infrastructure is organized around the Veeam backup server running on the SP side. The SP Veeam backup server is a configuration and control center of the Veeam Cloud Connect infrastructure. The SP uses the Veeam backup server to set up the Veeam Cloud Connect infrastructure and deliver Backup as a Service and Disaster Recovery as a Service to tenants.

The SP Veeam backup server runs the Veeam Cloud Connect Service — a Microsoft Windows service that is responsible for the following operations:

- Providing tenants with access to cloud repositories and cloud hosts

- Controlling transport services that work with tenant cloud repositories and cloud hosts

- Communicating with the Veeam Backup & Replication database

The Veeam Cloud Connect Service is deployed on every Veeam backup server. However, Veeam Backup & Replication uses this service only for work with Veeam Cloud Connect infrastructure components.

> **IMPORTANT**
>
> The SP must not stop or disable other Veeam Backup & Replication services running on the SP backup server.
>
> For example, in case the SP does not use the Continuous Data Protection (CDP) functionality, the Veeam CDP Coordinator Service must still run on the backup server.

Limitations for SP Veeam Backup Server
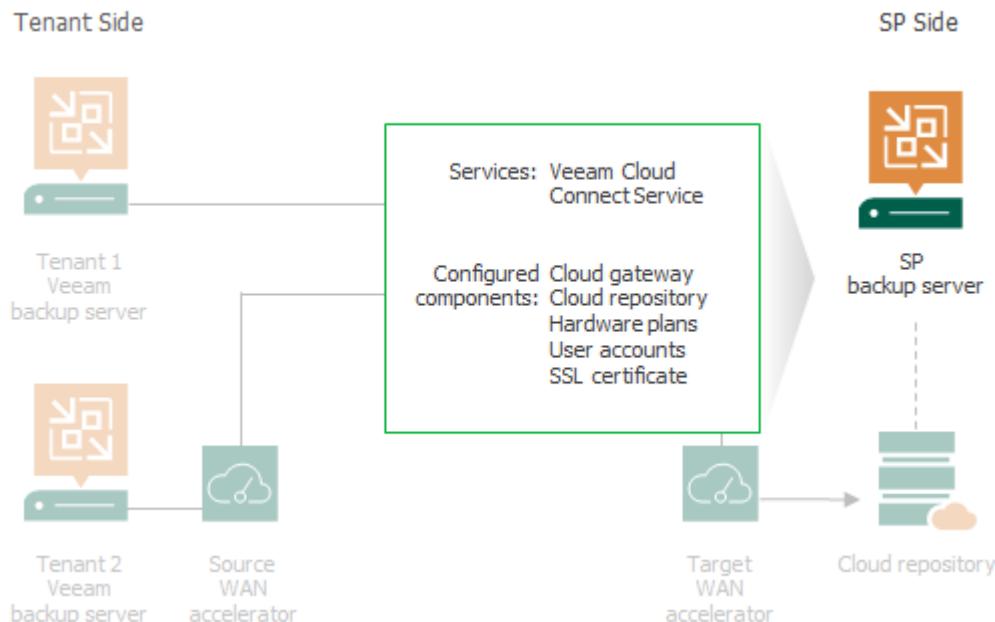
The SP Veeam backup server is intended to be used exclusively for configuring Veeam Cloud Connect infrastructure and providing cloud resources to tenants. The SP cannot perform the following operations on the SP Veeam backup server:

- Perform restore tasks, for example, to restore to the SP virtual environment VM data from tenant backups stored in a cloud repository. To perform data restore tasks, the SP must deploy a separate backup server in its backup infrastructure. The SP can use its existing Veeam Cloud Connect license on this backup server.

- Add itself as an SP in the Veeam Backup & Replication console, for example, to address specific scenarios that were supported in previous versions of Veeam Backup & Replication. For such scenarios, the SP must deploy a separate backup server in its backup infrastructure. The SP can use its existing Veeam Cloud Connect license on this backup server.

- Run backup, backup copy or replication jobs, for example, to back up VMs in the SP virtual environment. To create and run jobs, the SP must deploy a separate backup server (and other Veeam Backup & Replication components) and also obtain a separate license key and install it on this backup server.

    If the SP used such scenario with a previous version of Veeam Backup & Replication, they should follow the SP Veeam backup server split procedure. To learn more, see this Veeam KB article.

> **NOTE**
>
> Usage of the same Veeam backup server to provide Veeam Cloud Connect services and to run backup, backup copy and replication jobs is supported only for *Veeam Cloud Connect for the Enterprise*. For more information, see this Veeam webpage.

Maintenance Mode

In some cases, the SP may need to perform service actions with the SP backup infrastructure, for example, upgrade a server whose resources are consumed by tenant VM backups and replicas. Such operations may require that the SP cloud resources become temporarily unavailable to tenants and tenant activities are temporarily put on hold. To make the SP environment ready for maintenance, the SP can put its backup server to the Maintenance mode.

The Maintenance mode functionality is supported in the following Veeam products:

- Veeam Backup & Replication
- Veeam Agent for Microsoft Windows
- Veeam Agent for Linux
- Veeam Agent for Mac

The Maintenance mode functionality allows the SP to do the following:

1. Gracefully stop currently running tenant jobs targeted at a cloud repository of the SP. The following types of jobs are supported:

   o Veeam Backup & Replication jobs:

     ▪ VMware vSphere, VMware Cloud Director and Microsoft Hyper-V backup jobs

     ▪ Veeam Agent backup jobs configured in Veeam Backup & Replication

     ▪ VMware vSphere, VMware Cloud Director and Microsoft Hyper-V backup copy jobs

     ▪ Backup copy jobs for Veeam Agent backups created in the Veeam backup repository

   o Veeam Agent backup jobs (configured on a Veeam Agent computer)

   After the SP puts the SP backup server to the Maintenance mode, Veeam Backup & Replication checks the status of tenant jobs targeted at the SP cloud infrastructure and does the following:

   o If a Veeam Backup & Replication job is performing, Veeam Backup & Replication allows the currently running task of the job to complete. All subsequent tasks in the job will fail. This helps make sure that backed-up data pertaining to a certain VM or VM disk is successfully transferred to the cloud repository before the SP starts service actions in the Veeam Cloud Connect infrastructure.

   o If a Veeam Agent backup job is performing, Veeam Backup & Replication allows the job to complete. This helps make sure that backed-up data of the Veeam Agent computer is successfully transferred to the cloud repository.

2. Prevent tenant jobs from starting.

   If a tenant starts a new job session at the time when the SP backup server is operating in the Maintenance mode, the job will fail.

3. Notify tenants about maintenance in the cloud infrastructure.

   In the statistics window of a tenant job that completes with the *Failed* status at the time when the SP backup server is operating in the Maintenance mode, an error message will be displayed informing that the SP backup server is under maintenance. By default, an error message contains the following Maintenance mode notification: *Service provider is currently undergoing scheduled maintenance*. The SP can choose to use the default notification or create a custom message. To learn more, see Customizing Maintenance Mode Notification.

> **NOTE**
>
> Consider the following:
>
> - When the SP backup server is operating in the Maintenance mode, the tenant can access backups created in the cloud repository, for example, restore data from such backups. Thus, the SP should not use the Maintenance mode functionality to cease tenant activities before moving tenant backups to another cloud repository. The SP should disable a tenant prior to performing operations with tenant backups.
> - To inform tenants about maintenance on the SP backup server, Veeam Backup & Replication uses the Veeam Cloud Connect Service. As a result, Veeam Backup & Replication does not display the Maintenance mode notification at the time when the Veeam Cloud Connect Service is not running on the SP backup server or when the SP backup server is shut down.

The Maintenance mode does not affect other data protection and recovery tasks available in Veeam Backup & Replication and Veeam Agents.

- In Veeam Backup & Replication, a tenant can successfully perform the following tasks targeted at the SP cloud resources at the time when the SP backup server is operating in the Maintenance mode:

    o Run a replication job targeted at a cloud host provided by the SP.

    o Run a CDP policy targeted at a cloud host provided by the SP.

    o Perform any data restore task with a backup created in a cloud repository provided by the SP (for example, entire VM, VM files, VM disks or file-level restore, and so on).

    o Perform any task with a VM replica on a cloud host provided by the SP (for example, partial or full-site failover, failback to production, and so on).

- In Veeam Agent for Microsoft Windows and Veeam Agent for Linux, a tenant can successfully restore data from backups in the SP cloud repository at the time when the SP backup server is operating in the Maintenance mode.
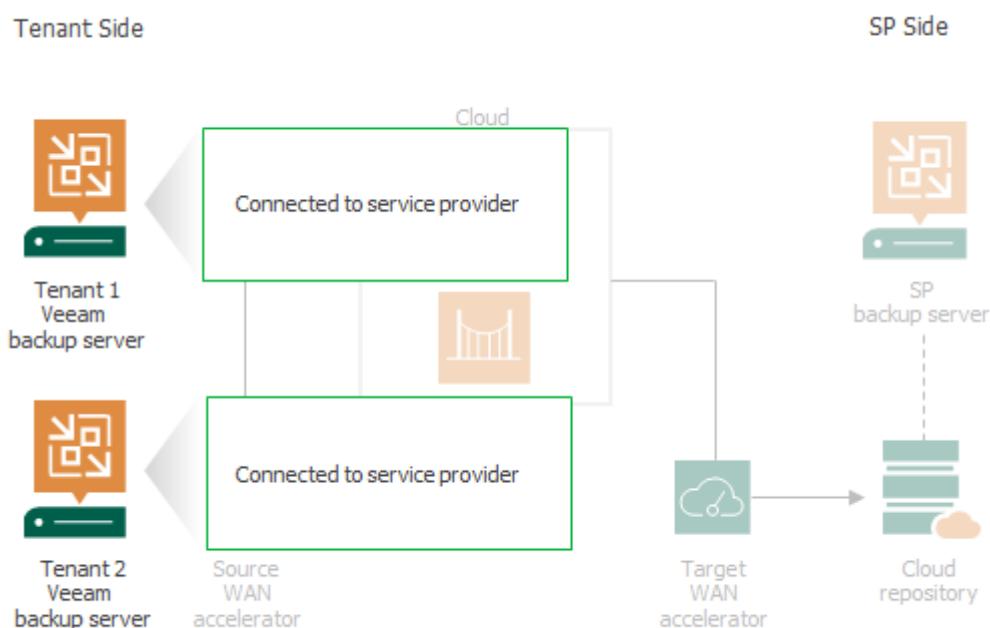
Tenant Veeam Backup Server

To work with Veeam Cloud Connect backup and replication resources, the tenant must deploy the Veeam backup server on the tenant side.

The Veeam backup server on tenant's side is a client machine. The tenant who plans to store VM data in the cloud must connect to the SP using Veeam Backup & Replication. When the tenant connects to the SP, cloud repository and cloud replication resources configured on the SP side become visible in the tenant backup infrastructure. The tenant can create necessary jobs, target them at the cloud repository and/or cloud host and run these jobs to protect tenant VMs.

All data protection and disaster recovery tasks targeted at the cloud repository are performed by tenants themselves. The SP only sets up the Veeam Cloud Connect infrastructure and exposes storage resources on the cloud repository to tenants.

Some disaster recovery tasks with cloud host can be performed not only by tenants but also by the SP. To learn more, see SP and Tenant Roles.

Cloud Gateway

The Veeam Cloud Connect infrastructure configured at the SP side is hidden from tenants. Tenants know only about cloud repositories and/or cloud hosts and can work with them as with locally deployed backup repositories and target hosts. Veeam backup servers on tenants' side do not communicate with cloud repositories and cloud hosts directly. Data communication and transfer in the cloud is carried out through cloud gateways.
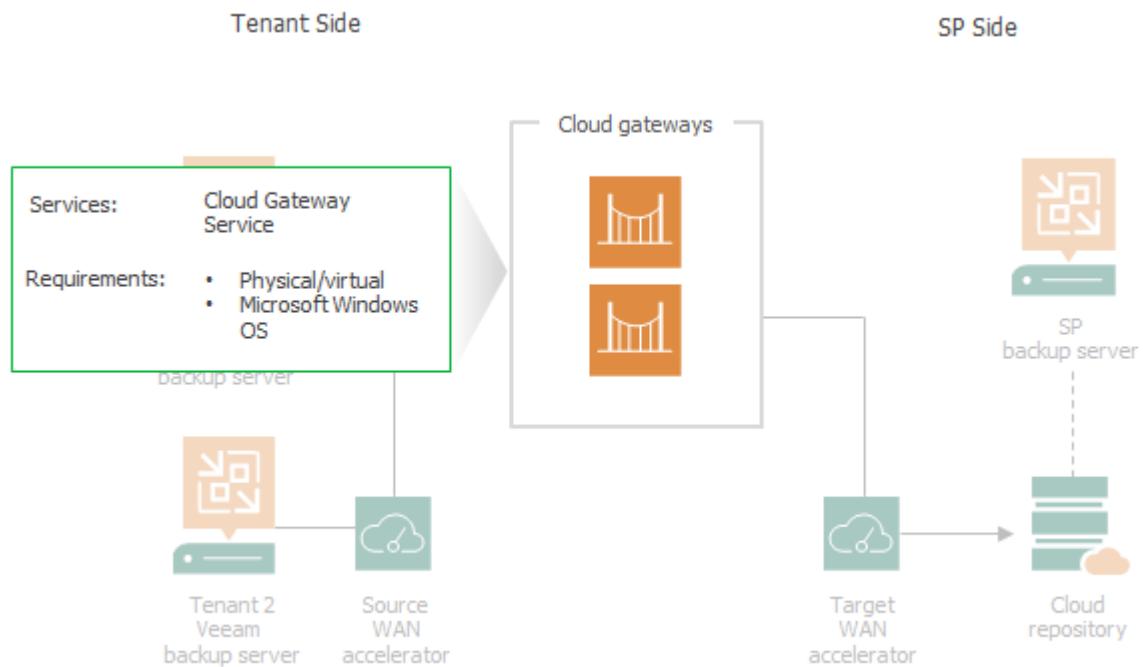
The cloud gateway is a network appliance that resides on the SP side. The cloud gateway acts as communication point in the cloud: it routes commands and traffic between the tenant Veeam backup server, SP Veeam backup server and other Veeam Cloud Connect infrastructure components.

The cloud gateway is a Microsoft Windows server running the Cloud Gateway Service — a Microsoft Windows service responsible for establishing a connection between parties in the Veeam Cloud Connect infrastructure.

To deploy a cloud gateway, the SP must assign the cloud gateway role to a necessary server in the SP backup infrastructure. The SP can configure a dedicated cloud gateway or install this role on the SP Veeam backup server. If traffic between the SP and tenants is significant, it is recommended that the SP deploys a dedicated cloud gateway to reduce the workload on the SP Veeam backup server.

The server performing the role of a cloud gateway must meet the following requirements:

1. The cloud gateway can be a physical or virtual machine.

2. The cloud gateway must run Microsoft Windows OS.

Cloud Gateway Deployment Scenarios

Depending on the size of the Veeam Cloud Connect infrastructure, the SP can deploy one or several cloud gateways. Veeam Backup & Replication supports many-to-one, one-to-many and many-to-many deployment scenarios:

- In the many-to-one deployment scenario, the SP deploys one cloud gateway that works with several tenants. Data flows for different tenants are securely fenced off on the cloud gateway, which eliminates the risk of data interference and interception.

- In the one-to-many and many-to-many scenarios, the SP deploys several cloud gateways that work with one or several tenants. Several cloud gateways can be used for scalability purposes if the amount of traffic going between the SP side and tenants' side is significant.

  Veeam Backup & Replication supports automatic failover between cloud gateways configured in the Veeam Cloud Connect infrastructure. When a tenant connects to the SP using a DNS name or IP address of a cloud gateway, the Veeam backup server on the tenant side obtains a list of all configured cloud gateways. If the primary cloud gateway is unavailable, the Veeam backup server on the tenant side fails over to another cloud gateway from the list.

  The SP can use regular cloud gateways or organize cloud gateways into cloud gateway pools to provide dedicated cloud gateways to the tenant. To learn more, see Cloud Gateway Pool.

  - Regular cloud gateways deployed in the Veeam Cloud Connect infrastructure are intended for use by an unlimited number of tenants. Such cloud gateways are available to tenants to whom the SP does not assign a cloud gateway pool. For a tenant with no cloud gateway pool assigned, communication between the tenant Veeam backup server and the SP Veeam Cloud Connect infrastructure is carried out through cloud gateways that are not added to any cloud gateway pool.

  - Cloud gateways operating as a part of a cloud gateway pool are intended for use by specific tenants. Such cloud gateways are available to tenants to whom the SP assigns the cloud gateway pool. For the tenant with the cloud gateway pool assigned, communication between the tenant Veeam backup server and the SP Veeam Cloud Connect infrastructure is carried out through cloud gateways added to this cloud gateway pool.

Cloud Gateway Pool

In large-scale Veeam Cloud Connect infrastructures with multiple cloud gateways, the SP may want to restrict access to some of the cloud gateways or allocate a dedicated cloud gateway to a specific tenant. For example, this may be required in the following situations:

- To comply with regulations requiring that traffic between the tenant backup server and the SP Veeam Cloud Connect infrastructure components goes only through cloud gateways located in a specific region.

- To provide a tenant with a quicker communication channel to the SP Veeam Cloud Connect infrastructure components.

For such scenarios, Veeam Backup & Replication offers the concept of a *cloud gateway pool*. The cloud gateway pool is a logical entity that groups cloud gateways intended for use by a specific tenant. The SP can organize cloud gateways deployed in the Veeam Cloud Connect infrastructure into cloud gateway pools and provide separate cloud gateway pools to different tenants.
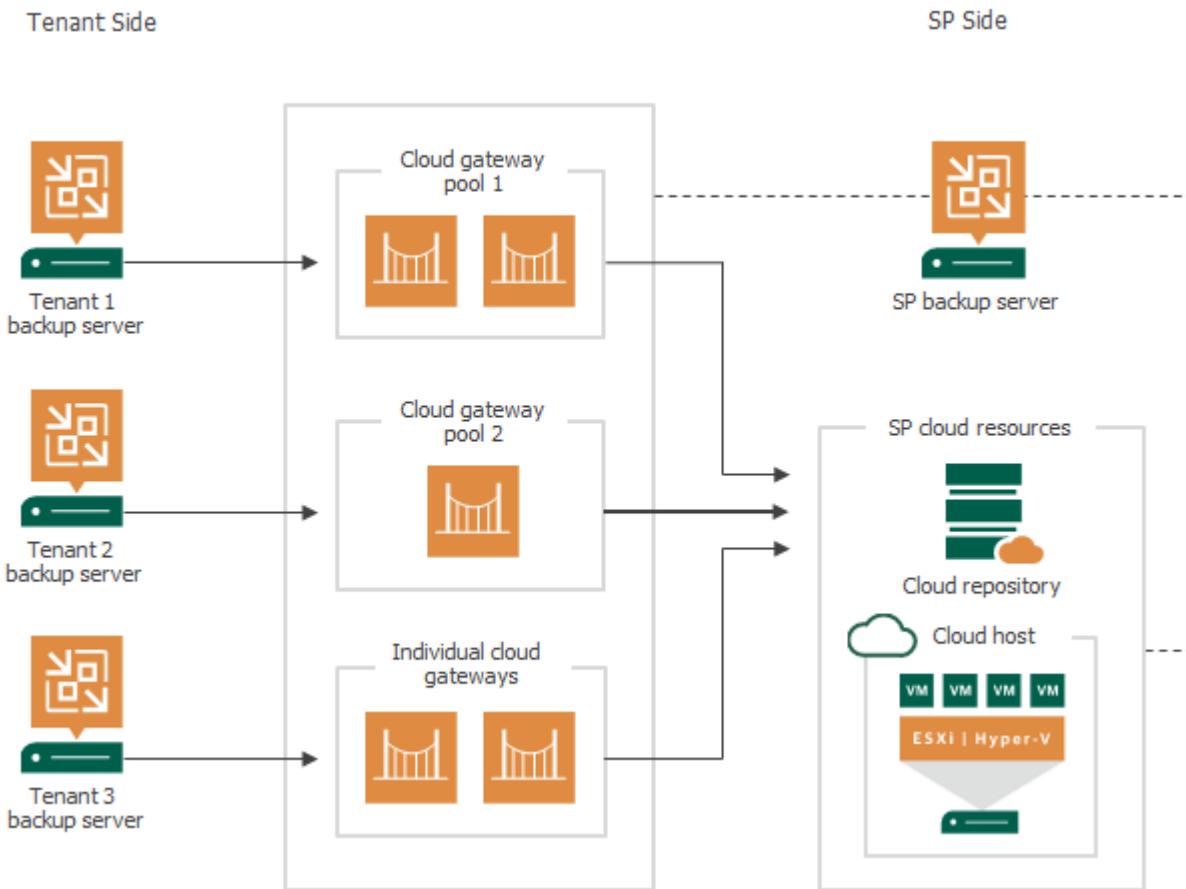
The SP can configure the desired number of cloud gateway pools in the Veeam Cloud Connect infrastructure. Each cloud gateway pool can comprise one or more cloud gateways.

To let the tenant use the cloud gateway pool, the SP must assign the cloud gateway pool to the tenant in the properties of the tenant account. The SP can assign a separate cloud gateway pool to each tenant, assign multiple cloud gateway pools to a single tenant or assign the same cloud gateway pool to multiple tenants.

Tenants to whom the SP does not assign a cloud gateway pool can use only those cloud gateways that are not a part of any cloud gateway pool.

Cloud gateways in a cloud gateway pool operate in the similar way as regular cloud gateways. As well as regular cloud gateways, cloud gateways operating as a part of the pool support automatic failover. If the primary cloud gateway is unavailable, Veeam Backup & Replication fails over to another cloud gateway in the same pool.

By default, in case all cloud gateways in the cloud gateway pool are unavailable for some reason, the tenant Veeam backup server cannot communicate with the Veeam Cloud Connect infrastructure components on the SP side. However, the SP can allow a specific tenant to fail over to cloud gateways that are not a part of a cloud gateway pool.

Cloud Repository

The cloud repository is a storage location in the cloud where tenants can store their VM data. Tenants can utilize the cloud repository as a target for backup and backup copy jobs and restore data from the cloud repository.

The cloud repository is a regular backup repository configured in the SP backup infrastructure. The SP can use the following types of backup repository as a cloud repository:

- Microsoft Windows-based server

- Linux-based server (including hardened backup repository)

- Shared folder

- Deduplicating storage appliance: Dell Data Domain, ExaGrid and Quantum DXi

- Object storage: S3 compatible, Amazon S3, IBM Cloud, Microsoft Azure and Wasabi

  To learn more, see Backup to Object Storage.

> **NOTE**
>
> Hardened (immutable) backup repository is not supported for tenants that run Veeam Backup & Replication versions earlier than version 11.
>
> - If storage quotas are allocated for such tenants on the cloud repository, the SP cannot enable immutability in the backup repository settings.
> - Backup repositories with enabled immutability are not displayed in the Edit Tenant wizard for such tenants.

The SP can expose cloud repository resources to one or several tenants. For each tenant, the SP allocates some storage space on the cloud repository. This storage space is consumed when the tenant runs data protection tasks targeted at the cloud repository.

The amount of space allocated to the tenant on the cloud repository is limited by a storage quota. If tenants must be able to use storage resources on the cloud repository for a limited period of time, the SP can also define a lease period for every tenant.
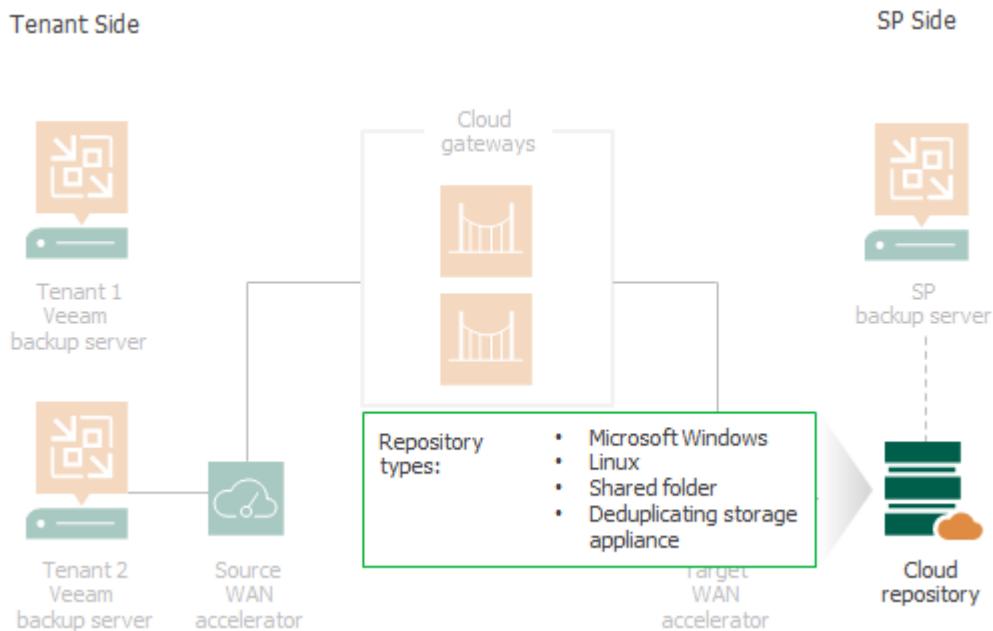
Being a multi-tenant storage resource, the cloud repository still appears as a logically separate backup repository to every tenant. Data in the cloud repository is segregated and isolated. Every tenant has its own folder on the cloud repository where tenant VM data is stored. Tenants do not know about other tenants who work with the cloud repository, and have no access to their data.

The tenant can have quotas on one or several cloud repositories configured by the SP. Several cloud repositories for one SP do not make up a pool of storage resources; they are used as separate backup infrastructure components. For example, if the tenant configures a backup job, the tenant can target it at only one cloud repository. All restore points created by this backup job will be stored on this cloud repository and will not be spread across several cloud repositories, even if the tenant has storage quotas on several cloud repositories.

Support for Scale-Out Backup Repository

Along with a simple backup repository, the SP can use a scale-out backup repository as a cloud repository. In this scenario, the SP can use the Capacity Tier functionality to offload tenant backups to a cloud-based object storage. To learn more, see Support for Capacity Tier.

The SP can also use the archive tier functionality to keep backups of rarely accessed tenant data in an additional tier of storage. To let tenants restore archived data, the SP must retrieve the data from the archive tier. To learn more, see Retrieving Tenant Data from Archive Tier.

Hardware Plan

The hardware plan is a set of resources that the SP allocates in their Veeam Cloud Connect infrastructure to set up a target for tenant VM replicas. For a tenant, a hardware plan appears as a cloud host. A tenant can utilize a cloud host as a regular target host to perform VM replication and failover tasks.

A hardware plan comprises the following resources in the SP virtualization infrastructure:

- **CPU** — limit of CPU that can be used by all replicated VMs of a tenant subscribed to a hardware plan (amount of CPU on the tenant cloud host).

- **Memory** — limit of RAM that can be used by all replicated VMs of a tenant subscribed to a hardware plan (by all tenant VMs on the cloud host).

- **Storage** — a quota on a datastore (for VMware hardware plans) or a volume (for Hyper-V hardware plans) that a tenant can utilize for storing replicated VMs data.

- **Network** — specified number of networks to which tenant VM replicas can connect. When the SP subscribes a tenant to a hardware plan, Veeam Backup & Replication creates the same number of network adapters (vNICs) on the network extension appliance that is deployed on the SP side. To learn more, see Network Extension Appliance.

The SP can configure hardware plans for VMware vSphere and Microsoft Hyper-V platforms. Replication resources that will be provided to tenants through hardware plans can be allocated on standalone hosts and/or clusters.
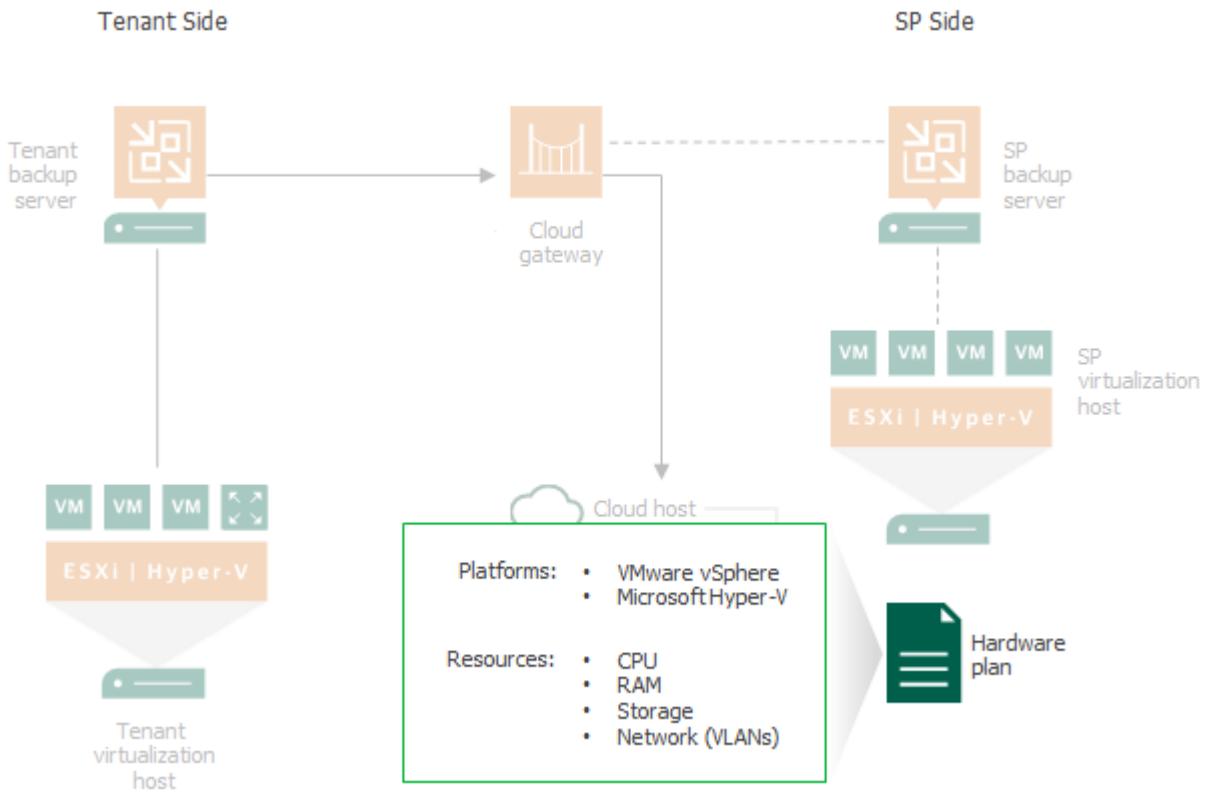
If the SP configures a hardware plan using resources allocated on a cluster, Veeam Backup & Replication automatically distributes the workload between the components of the cluster:

- Selects a host on which to register a VM replica.

- Selects a datastore or volume on which to store VM replica files.

The SP can configure one or several hardware plans. For example, the SP may configure in advance multiple hardware plans for different categories of customers or create custom hardware plans that match production environment of particular tenants.

To let a tenant work with a cloud host based on the hardware plan, the SP must subscribe the tenant to this hardware plan. The SP can subscribe one or several tenants to the same hardware plan. Each tenant subscribed to the hardware plan can use the whole set of resources specified in the hardware plan. Tenants do not know about other tenants who work with cloud hosts, and have no access to their data. As a result, the SP can expose virtualization resources to several tenants and store tenants' data in the cloud in an isolated and segregated way.

The SP can subscribe a tenant to one or several hardware plans that utilize resources on the same SP host or cluster or different hosts or clusters. When the SP subscribes a tenant to a hardware plan, the hardware plan appears in the tenant Veeam Backup & Replication infrastructure as a cloud host.

Cloud Hosts in SP Virtualization Environment

Replication resources allocated for tenant VM replicas appear in the SP virtualization environment differently depending on the virtualization platform: VMware vSphere or Microsoft Hyper-V.

When the SP configures the first VMware hardware plan, Veeam Backup & Replication creates on the host allocated for replication target a parent resource pool for Cloud Connect Replication resources. When the SP subscribes a tenant to a hardware plan, Veeam Backup & Replication creates in this parent resource pool a resource pool that represents a tenant's cloud host. On the datastore that the SP exposes as a storage for tenant VM replicas, Veeam Backup & Replication creates for every tenant a folder in which VM replica files are stored.

For example, when the SP subscribes the tenant *ABC Company* to the hardware plan *VMware Silver*, the resource pool *VMware_Silver_ABC* will be created in the parent *Cloud_Connect_Replication* resource pool on the SP's virtualization host where cloud replication resources are allocated. Tenant VM replicas will be created in the *ABC Company* folder on the selected datastore.

For Microsoft Hyper-V hardware plans, a tenant's cloud host appears in the SP virtualization environment as a dedicated folder on the storage where tenant VM replicas are created.

Network Extension Appliance

To enable communication between production VMs on the tenant side, VM replicas on the cloud host, Veeam Cloud Connect infrastructure components and external network nodes, Veeam Backup & Replication uses network extension appliances. The network extension appliance is a Linux-based auxiliary VM created on virtualization hosts where tenant VMs and their replicas reside.

For every tenant who plans to replicate VMs to the cloud host and use all built-in cloud networking and failover capabilities (perform both full site failover and partial site failover), at least two network extension appliances should be deployed — one on the SP side and the other on the tenant side.

- The network extension appliance on the SP side is deployed on the virtualization host in the SP environment that acts as a replication target. The network extension appliance VM is assigned an IP address from the SP production network and placed to the *Cloud_Connect_Replication* folder and resource pool created on the ESXi host or a dedicated folder on the Hyper-V host.

- The network extension appliance on the tenant side is deployed on the source virtualization host where production VMs reside. The network extension appliance VM is assigned an IP address from a tenant's production network and placed to the selected folder and resource pool created on the ESXi host or a selected folder on the Hyper-V host.
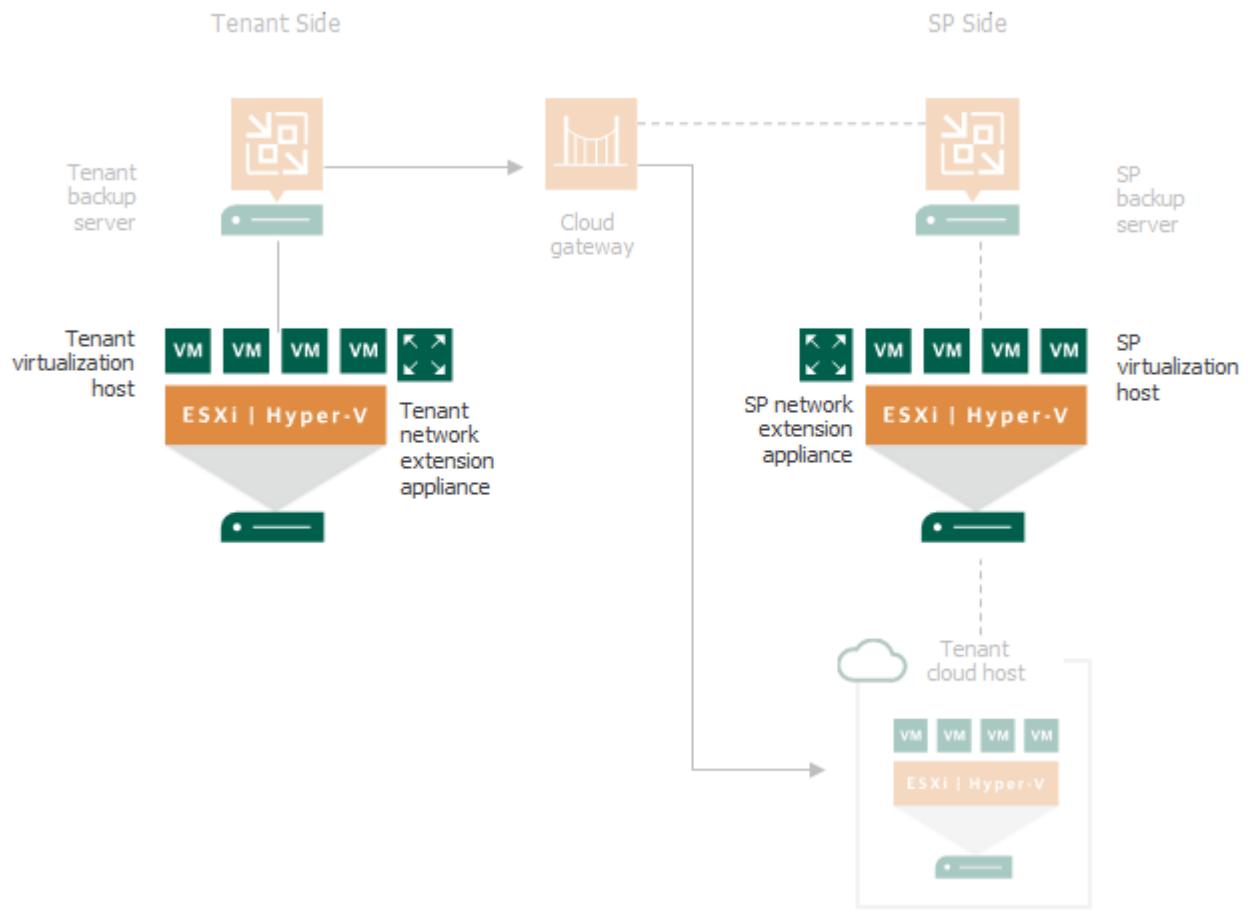
The SP specifies network settings for the provider-side network extension appliance when subscribing a tenant to a hardware plan. To learn more, see Specify Network Extension Settings.

The tenant specifies network settings for the tenant-side network extension appliance when adding the SP or rescanning resources available from the SP in the tenant Veeam backup console. To learn more, see Configure Network Extension Appliances.

Veeam Backup & Replication automatically deploys and configures the network extension appliance VM using the specified settings.

> **NOTE**
>
> The network extension appliance is an obligatory component if you want to use built-in cloud networking and failover capabilities of Veeam Cloud Connect Replication. If the SP or tenant does not specify network extension appliance settings, or if the network extension appliance fails during the failover process, the tenant will not be able to fail over to a VM replica. To learn more about cloud failover, see Cloud Replica Failover and Failback.

Tenant Side   SP Side

Tenant Network Extension Appliance
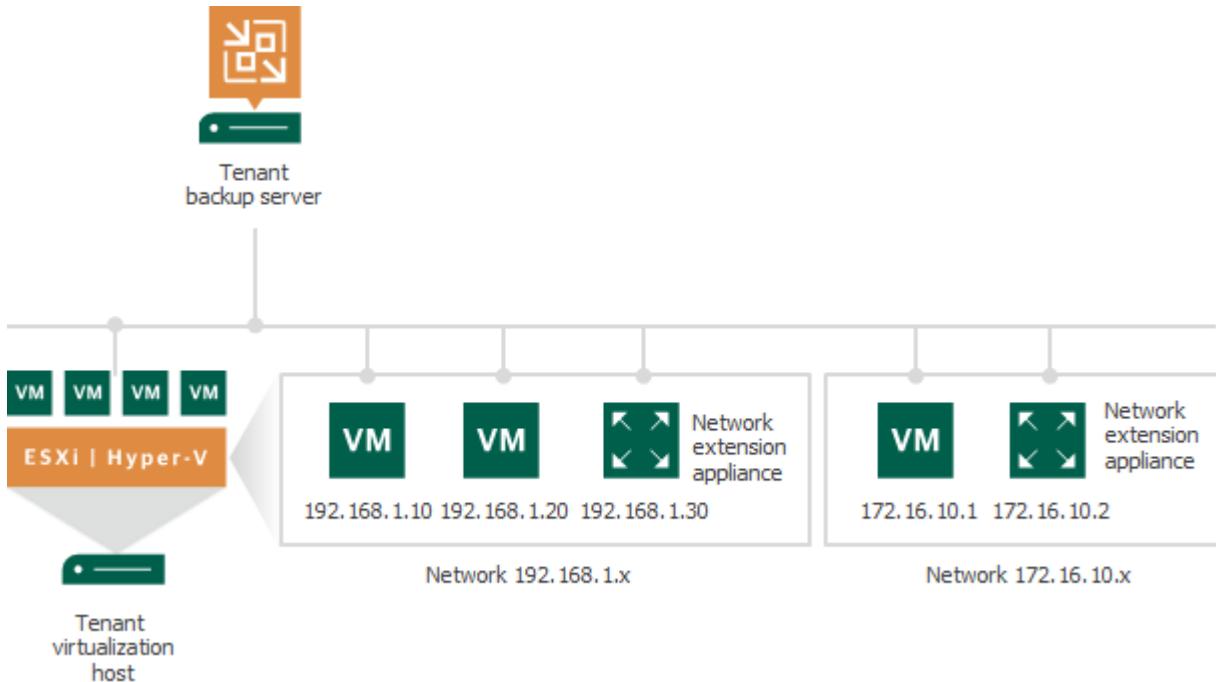
Veeam Backup & Replication uses the network extension appliance on the tenant side to route requests between production VMs on the source host and VM replicas on the cloud host after partial site failover.

The network extension appliance connects to a production network using a network adapter. On the tenant side, a separate network extension appliance must be deployed for every production IP network. For example, if there are 2 networks on the tenant production site, the tenant should configure 2 network extension appliances. The network adapter of each network extension appliance on the tenant side gets an IP address from the production network for which this appliance is configured.

The tenant-side network extension appliance is deployed on the tenant virtualization host when the tenant adds the SP in the tenant Veeam backup console. At the **Network Extension** step of the **Service Provider** wizard, Veeam Backup & Replication offers the tenant to deploy one network extension appliance with default settings. To deploy the default appliance, Veeam Backup & Replication detects the production network, connects the appliance to this network and tries to assign an IP address to the appliance using DHCP.

When adding the SP, the tenant can check and, if necessary, specify custom settings for the network extension appliance instead of the default ones. For example, the tenant can assign a specific IP address to the appliance. If there are multiple production IP networks on the tenant side, the tenant can instruct Veeam Backup & Replication to deploy the required number of network extension appliances with required settings.

If the tenant does not plan to perform partial site failover, they may omit the network extension appliance deployment when adding the SP.

SP Network Extension Appliance

For every tenant subscribed to a hardware plan, Veeam Backup & Replication deploys a dedicated network extension appliance on the SP virtualization host that acts as a replication target. With the network extension appliance, the SP does not need to reconfigure production network in their Veeam Cloud Connect infrastructure. The SP network extension appliance acts as a gateway between the production network and tenant VM replica networks.
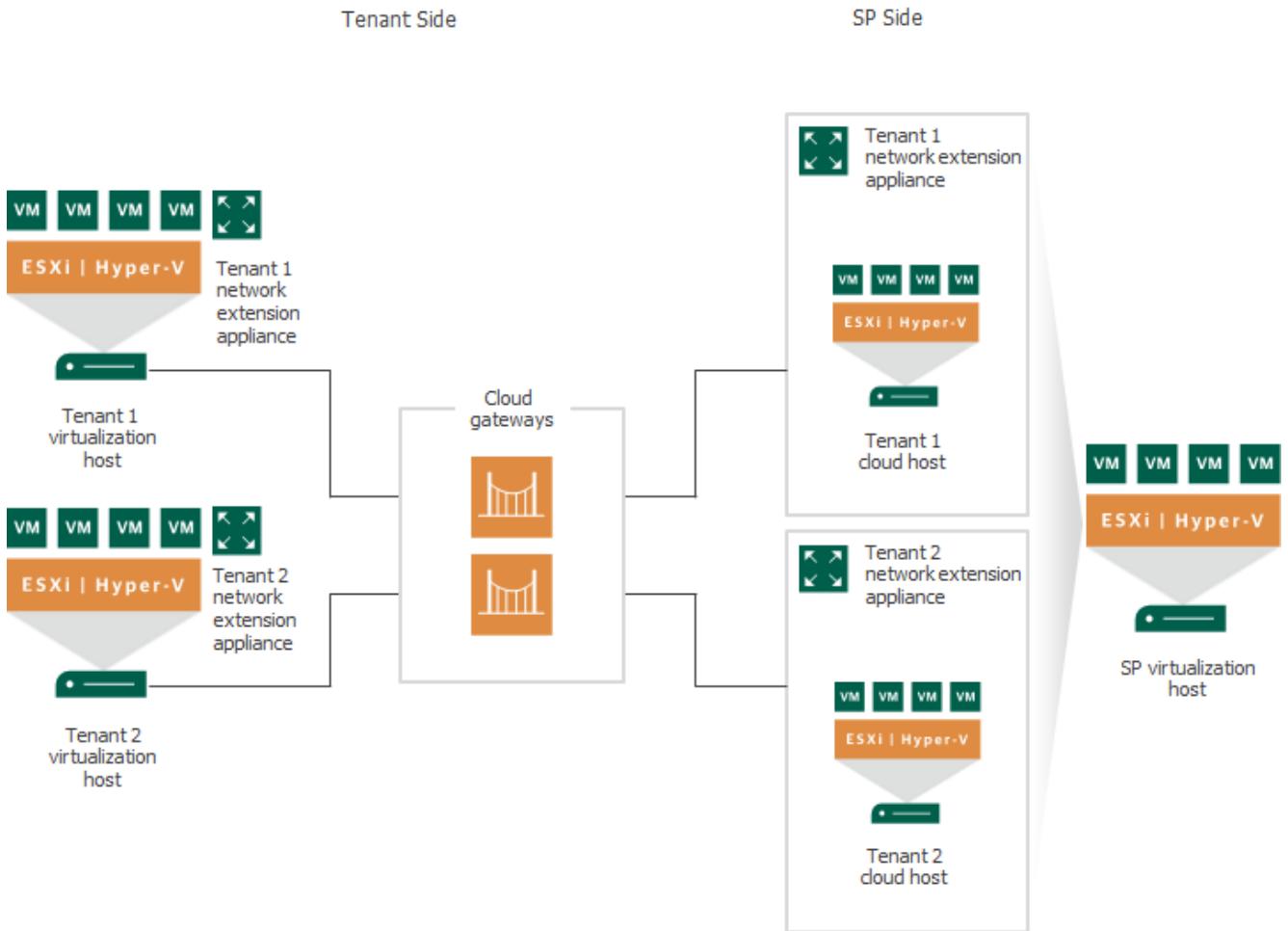
Veeam Backup & Replication uses the network extension appliance on the SP side for the following purposes:

- Routing requests between VM replicas on the cloud host and production VMs on the source host after partial site failover.

  All traffic that comes from tenant VM networks to cloud hosts on the SP side is encapsulated in individual VPN tunnels opened between a pair of network extension appliances.

- Separating traffic of the SP production network(s) and tenant VM networks (by connecting to different VLANs in the SP network infrastructure).

- Providing VM replicas with public IP addresses after full site failover.

- Routing requests between VM replicas on the cloud host and network hosts in the internet after full site failover.

The network extension appliance connects to the SP production network and to virtual networks (VLANs) provided to a tenant through a hardware plan using vNIC adapters. Veeam Backup & Replication does not deploy a separate network extension appliance on the SP side for every IP network in a hardware plan. Instead, it adds to the appliance one vNIC adapter per each VLAN in all hardware plans to which the SP subscribes the tenant.

For example, the SP can configure on the same host one hardware plan with 2 networks and another hardware plan with 3 networks. When the SP assigns both hardware plans to the same tenant, Veeam Backup & Replication will add 6 vNIC adapters to the network extension appliance — 1 vNIC adapter for the SP production network and 5 vNIC adapters for all networks (VLANs) provided to a tenant through hardware plans configured on the SP host.

If the SP assigns to a tenant several hardware plans that utilize resources on different hosts, Veeam Backup & Replication will deploy network extension appliances for this tenant on every host that acts as a replication target.

Network Extension Appliances Interaction

The SP and tenant network extension appliances use a set of networking technologies to automatically establish and maintain a secure connection between a VM network on the tenant side and VM replica network on the SP side. A pair of network extension appliances acts as gateways between the two networks, routing requests from the tenant's production site to VM replicas on the cloud host and in the opposite direction.

When a tenant performs the partial site failover operation, a production VM and a failed-over VM replica on the cloud host begin to communicate to each other using network extension appliances in the following way:

1. Veeam Backup & Replication powers on a VM replica on the cloud host.

2. Veeam Backup & Replication powers on a network extension appliance VM on the SP host where the replication target is configured and starts a VPN server on the appliance.

3. On the tenant side, Veeam Backup & Replication powers on a network extension appliance VM, starts a VPN client on the appliance and connects to the VPN server on the SP network extension appliance to establish a secure VPN tunnel between two appliances through the cloud gateway.

4. The network extension appliance on the tenant side receives requests from a production VM that are addressed to a failed-over VM and transmits them to the appliance on the SP side through the VPN tunnel.

5. The network extension appliance on the SP side accepts requests from the tenant appliance and transmits them to the VM replica.

6. VM replica receives a request from the SP network extension appliance.

7. VM replica sends a request to the production VM in the similar order.

8. Production VM and VM replica continue communication through a secure VPN tunnel.

Limitations for Network Extension Appliance

The network extension appliance deployed on the SP side has the following limitations:

- The network extension appliance supports one failover operation type at a time. A tenant cannot perform partial site failover and full site failover simultaneously.

- The network extension appliance does not support usage of port 22 as a port for a public IP address in public IP addressing rules. Veeam Backup & Replication uses this port for communication with the network extension appliance. To learn more about public IP addressing settings, see Specify Public IP Addressing Rules.

- You cannot deploy a network extension appliance on the following types of storage:

  o VMware Virtual Volumes (VVol)

  o Datastore Cluster

Veeam Cloud Connect Portal

Veeam Cloud Connect Portal is a web tool for performing full site failover. With Veeam Cloud Connect Portal, tenants can run cloud failover plans to switch to snapshot-based VM replicas in the cloud DR site in an easy and secure way.

> **NOTE**
>
> The tenant cannot use Veeam Cloud Connect Portal to perform full site failover to CDP replicas.

Veeam Cloud Connect Portal is deployed by the SP in the SP backup infrastructure as part of the Veeam Backup Enterprise Manager installation process. To learn more about Veeam Backup Enterprise Manager deployment, see the Installing Veeam Backup Enterprise Manager section in the Veeam Backup Enterprise Manager User Guide.

Veeam Cloud Connect Portal is available to every tenant for whom the SP has registered a tenant account. To provide tenants with access to Veeam Cloud Connect Portal, the SP must add to Veeam Backup Enterprise Manager all Veeam backup servers on which tenant accounts are registered.

A tenant can access Veeam Cloud Connect Portal with a web-browser using URL address and credentials of the tenant account provided by the SP. With Veeam Cloud Connect Portal, a tenant can perform the following operations:

- Start a full site failover by a cloud failover plan

- Retry a full site failover by a cloud failover plan

- Undo a full site failover by a cloud failover plan

- Monitor full site failover process and view historical data on cloud failover plan sessions

WAN Accelerators

WAN accelerators are optional components in the Veeam Cloud Connect infrastructure. Tenants may use WAN accelerators:
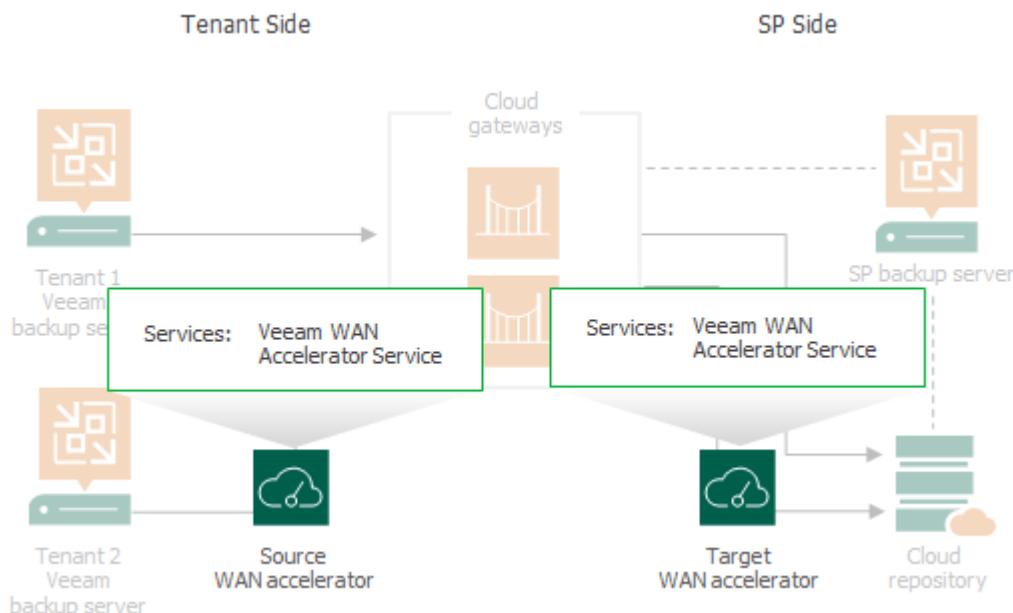
- For backup copy jobs targeted at the cloud repository

- For replication jobs targeted at cloud hosts

WAN accelerators in the Veeam Cloud Connect infrastructure run the same services and perform the same role as WAN accelerators in a regular backup infrastructure. When configuring backup copy or replication jobs, tenants can choose to exchange data over a direct channel or communicate with the cloud repository or cloud host through WAN accelerators. To pass VM data through WAN accelerators, the SP and tenants must configure WAN accelerators in the following way:

- The source WAN accelerator is configured on the tenant side.

- The target WAN accelerator is configured on the SP side.

The SP can configure several target WAN accelerators and assign them to different tenants. Each target WAN accelerator is strictly associated with tenant's quota on the cloud repository and the hardware plan to which the tenant is subscribed (cloud host). This way, tenant's data always go through the assigned target WAN accelerator and Veeam Backup & Replication can use the global cache on the target WAN accelerator more efficiently.

Tenants do not know about target WAN accelerators on the SP side: they can only see whether Veeam Cloud Connect resources can use WAN acceleration or not. When tenants create backup copy or replication jobs that transfer data through WAN accelerators, they define only the source WAN accelerator in the job properties. The target WAN accelerator is not selected. During the backup copy or replication job, the Veeam Cloud Connect Service on the SP Veeam backup server automatically assigns the necessary target WAN accelerator on the SP side for the job.

Limitations for WAN Accelerators in Veeam Cloud Connect Infrastructure

Veeam Backup & Replication does not use tenant backups to populate global cache on the service provider side. For more information about global cache population, see Population of Global Cache.

SP and Tenant Roles

Communication in the cloud is carried out between two parties: SP on one side and tenants on the other side.

- The SP is an organization that provides cloud services to tenants:
    - Backup as a Service (Veeam Cloud Connect Backup)
    - Disaster Recovery as a Service (Veeam Cloud Connect Replication)
- The tenant is an SP customer who wants to copy data offsite, store backups in a cloud repository or create VM replicas on a cloud host on the SP side.

SP Tasks

In the cloud, the SP is responsible for performing the following tasks:

Veeam Cloud Connect Backup Tasks

- Configuring the Veeam Cloud Connect Backup infrastructure — environment needed to expose cloud repository resources to tenants. As part of this process, the SP takes the following steps:
    - Decides what backup repositories must be used as cloud repositories.
    - Sets up TLS certificates to enable secure communication in the Veeam Cloud Connect infrastructure.
    - Configures cloud gateways.
    - Registers tenant accounts.
- Managing tenant accounts and tenant data to ensure flawless work of the Veeam Cloud Connect infrastructure.
- Performing instant recovery from tenant backups.

Veeam Cloud Connect Replication Tasks

- Configuring the Veeam Cloud Connect Replication infrastructure — environment needed to expose SP's virtualization resources as cloud hosts to tenants. As part of this process, the SP takes the following steps:
    - Sets up TLS certificates to enable secure communication in the Veeam Cloud Connect infrastructure.
    - Configures cloud gateways.
    - Allocates VLANs for cloud networking.
    - Allocates public IP addresses for tenant VM replicas.
    - Configures hardware plans or VMware Cloud Director resources to provide tenants with computing, storage and network resources to create VM replicas in the cloud and perform failover tasks with VM replicas on the cloud host.
    - Registers tenant accounts.

- Managing tenant accounts and tenant data to ensure flawless work of the Veeam Cloud Connect infrastructure.

- Running tenant cloud failover plans to perform full site failover and managing tenant VM replicas upon tenant requests.

Tenant Tasks

Tenants, on their hand, are responsible for performing the following tasks:

- Connecting to the SP to be able to use Veeam Cloud Connect resources (cloud repository and cloud host).

- Configuring and running backup and backup copy jobs targeted at cloud repositories.

- Configuring and running replication jobs and CDP policies targeted at cloud hosts.

- Performing restore tasks with VM backups created by backup jobs.

- Configuring cloud failover plans to perform full site failover for VM replicas.

- Performing failover tasks with VM replicas created by replication jobs.

- Configuring subtenant accounts to allow tenant-side users to create Veeam Agent backups in a cloud repository. To learn more, see Subtenants.

- Performing restore tasks with Veeam Agent backups created by subtenants in a cloud repository.

> **NOTE**
>
> Consider the following:
>
> - A set of tasks available to the tenant depends on the type of the tenant account. To learn more, see Tenant Account Types.
> - It is recommended that the tenant enables the encryption option for backup jobs targeted at the cloud repository. Data encryption helps tenants protect sensitive VM data from unauthorized access while this data is stored in the cloud repository.
>
> On the SP side, the SP should ensure integrity of tenant backups. It is not recommended that the SP uses tenant backups to perform operations that go beyond the scope of regular Veeam Cloud Connect tasks. For example, importing a tenant backup in the Veeam Backup & Replication console on the SP backup server and performing recovery verification of this backup with a SureBackup job may result in failure of the tenant backup job and corruption of the configuration database on the SP backup server.

SP and Tenant Roles in Managed Service Scenario

In addition to Backup as a Service (Veeam Cloud Connect Backup) and Disaster Recovery as a Service (Veeam Cloud Connect Replication), the SP can use Veeam Backup & Replication to offer the Managed Service (MSP Backup and Disaster Recovery as a Service) to tenants. In this scenario, the tenant may not take part in deploying and managing backup infrastructure. The SP takes responsibility for configuring backup infrastructure on the tenant side and performing all data protection and disaster recovery tasks. To learn more, see Managed Service.

Tenant Account Types

To work with the cloud resources provided by the SP, the tenant uses a tenant account. Veeam Backup & Replication offers the following types of tenant accounts:

- *Standalone tenant account* — a regular tenant account for Veeam Cloud Connect Backup and Veeam Cloud Connect Replication scenarios. When the SP creates an account of this type, the SP specifies a name and password for the account, assigns a quota on the cloud repository to the tenant and subscribes the tenant to a hardware plan. To learn more, see Veeam Cloud Connect Backup and Veeam Cloud Connect Replication.

- *Active Directory tenant account* — a tenant account for Microsoft Active Directory (AD) users. Tenants with accounts of this type can connect to the SP using their AD credentials and use Veeam Agent operating in the standalone mode to back up data to a cloud repository. To learn more, see Active Directory Tenant Account.

- *VMware Cloud Director tenant account* — a tenant account used to provide Veeam Cloud Connect backup and replication resources to VMware Cloud Director organizations. When the SP creates an account of this type, the SP specifies an organization, assigns a quota on the cloud repository to the tenant and specifies an organization VDC that will be used as a cloud host for tenant VM replicas. To learn more, see VMware Cloud Director Tenant Account.

Active Directory Tenant Account

Veeam Backup & Replication lets the SP provide Active Directory users with access to a cloud repository. This functionality can be useful for large organizations that have Microsoft Active Directory and Veeam Cloud Connect infrastructure deployed and want to allow their users to create off-site backups with Veeam Agent.

Using the Active Directory tenant account functionality, a backup administrator of the organization can allocate quotas on a cloud repository directly for AD users without the need to configure subtenant accounts. For Veeam Agent users, the functionality helps to avoid maintaining additional set of tenant account credentials. Instead, users can connect to the SP using credentials of their user account in AD.

Active Directory tenant accounts utilize the secondary password functionality. To learn more, see Secondary Password for Tenant Account.

How It Works

Data backup to a cloud repository using an Active Directory tenant account works in the following way:

1. The SP creates an Active Directory tenant account. In the properties of the tenant account, the SP specifies settings to connect to the AD domain controller, selects an AD user account and assigns backup resources to the tenant account. To learn more, see Configuring Active Directory Tenant Account.

2. A Veeam Agent user creates a backup job targeted to a cloud repository. In the properties of the Veeam Agent backup job, the user specifies credentials of their user account in Active Directory.

3. Veeam Agent connects to the SP backup server. Veeam Backup & Replication on the SP backup server authenticates the user in Active Directory.

4. Veeam Backup & Replication creates a secondary password for the tenant account and passes this password to Veeam Agent. Veeam Agent saves the secondary password to its database.

5. During subsequent backup job sessions, Veeam Agent uses the secondary password to connect to the SP.

Considerations and Limitations

Consider the following:

- You can create an Active Directory tenant account for a user account registered in any domain to which you have access.

- You cannot assign replication resources to an Active Directory tenant account.

- You cannot configure subtenant accounts for an Active Directory tenant account.

- To connect to the SP using an Active Directory tenant account, you must use Veeam Agent for Microsoft Windows version 5.0 or later.

- The Active Directory tenant account functionality is intended for Veeam Agent backup only. You cannot use an Active Directory tenant account to connect to the SP in the Veeam backup console.

Tenant Account Credentials

To connect to the SP, the tenant uses credentials of the tenant account provided by the SP. Credentials of the tenant account depend on the account type. The following table contains information about credentials for different tenant account types.

Account Type	Account Name	Password[1]
Standalone tenant account	Name specified by the SP in the properties of the tenant account.	Password specified by the SP in the properties of the tenant account.
VMware Cloud Director tenant account	Name of the organization to which the tenant is granted access in VMware Cloud Director. To connect to the SP, the tenant specifies the user name of the VMware Cloud Director organization administrator account. To learn more, see Connecting to Service Providers.	Password of the VMware Cloud Director organization administrator account.
Active Directory tenant account	Name of the user account in Microsoft Active Directory. To connect to the SP, the tenant specifies credentials of their AD user account in the *Domain|Username* format.	Password of the user account in Microsoft Active Directory.

[1] Primary password for the tenant account. Veeam Backup & Replication can also use secondary passwords generated automatically by the product. To learn more, see Secondary Password for Tenant Account.

Secondary Password for Tenant Account

In addition to a primary password of the tenant account used to connect the tenant to the SP, Veeam Backup & Replication can use secondary passwords for backup operations. A secondary password is an additional password automatically generated by Veeam Backup & Replication for the tenant account. Veeam Backup & Replication uses secondary passwords for Veeam Agent backup.

Veeam Backup & Replication uses secondary passwords in the following scenarios:

- Scenario 1. The SP backup server is managed by Veeam Service Provider Console version 5.0 or later. The SP creates Veeam Agent backup jobs and/or backup policies in Veeam Service Provider Console. To learn more, see How It Works.

- Scenario 2. The SP provides users with access to a cloud repository through Active Directory tenant accounts. A user connects to the SP in Veeam Agent using an Active Directory tenant account. To learn more, see Active Directory Tenant Account.

The secondary password functionality helps to provide an individual unique password for each Veeam Agent connected to the SP. It also helps to avoid passing the primary password outside of Veeam Backup & Replication and saving tenant password to the Veeam Service Provider Console or Veeam Agent configuration database.

Secondary passwords are used by the product in the background and are not displayed to users.

How It Works
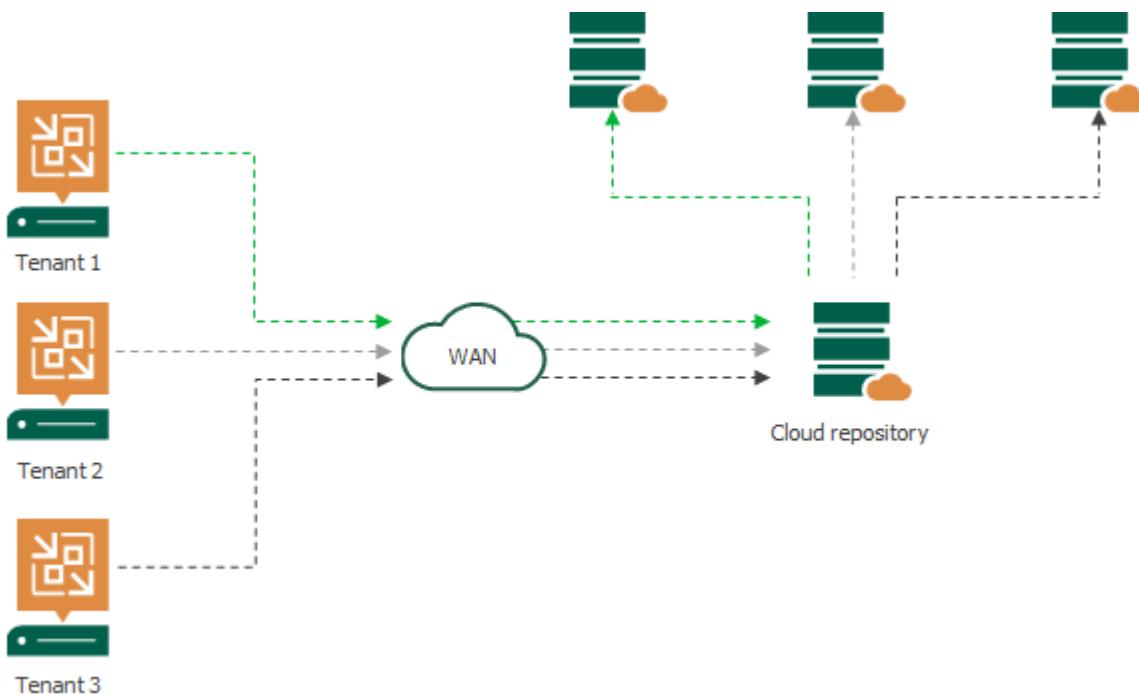
In the scenario where the SP backup server is managed by Veeam Service Provider Console, Veeam products work with secondary passwords in the following way:

1. A backup administrator on the SP side configures a backup job or backup policy in Veeam Service Provider Console. Once a backup job or backup policy is added, Veeam Service Provider Console requests a secondary password in Veeam Backup & Replication.

2. Veeam Backup & Replication generates a secondary password for Veeam Agent added to the backup job. For a backup policy, Veeam Backup & Replication generates an individual secondary password for each Veeam Agent added to the backup policy.

3. Veeam Backup & Replication passes secondary passwords to Veeam Service Provider Console.

4. Veeam Service Provider Console applies backup job or backup policy settings to Veeam Agent. These settings include credentials to connect to the SP.

5. When the backup job starts in Veeam Agent, Veeam Agent connects to the SP backup server using the secondary password.

Veeam Cloud Connect Backup

SP can use Veeam Backup & Replication to offer cloud repository as a service to their customers.

Cloud repositories have a multi-tenant architecture. Veeam Backup & Replication creates a storage abstraction layer and virtually partitions storage resources of a cloud repository. As a result, the SP can expose cloud repository resources to several tenants and store tenants' data in the cloud in an isolated and segregated way. Veeam Backup & Replication establishes a secure channel to transfer tenant data to and from the cloud repository and offers data encryption capabilities to protect tenant data at rest.

All data protection and disaster recovery tasks targeted at the cloud repository are performed by tenants on their own. Tenants can set up necessary jobs themselves and perform tasks on Veeam backup servers deployed on their side. Tenants can perform the following operations:

- Back up virtual and physical machines to the cloud repository

- Copy backup files to the cloud repository

- Restore data from the cloud repository

- Perform file copy operations between the tenant side and the cloud repository (Manual operations only. Scheduled file copy jobs are not supported.)

Getting Started with Veeam Cloud Connect Backup

To provide Backup as a Service to tenants, the SP must set up the Veeam Cloud Connect Backup infrastructure.

As part of the configuration process, the SP must perform the following tasks:

1. Deploy the SP Veeam backup server.

2. Set up TLS certificates.

3. Create cloud gateways.

4. Configure cloud repositories.

5. [Optional] Configure target WAN accelerators.

6. Register tenant accounts.

7. Communicate information about the tenant account and gateway to all tenants who plan to connect to the SP.
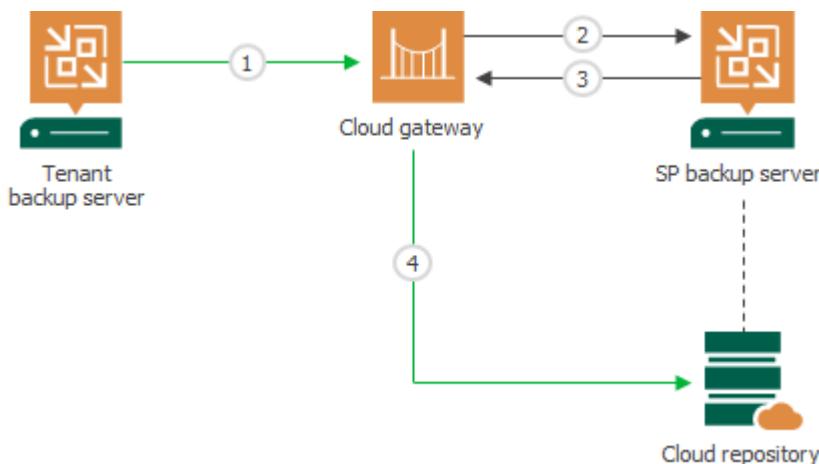
Once the SP has configured necessary components, tenants can add the SP to their Veeam Backup & Replication consoles and use cloud repositories allocated to them in the SP Veeam Cloud Connect infrastructure.

How Veeam Cloud Connect Backup Works

Tenants who plan to store their data in the cloud must configure backup or backup copy jobs on their Veeam backup servers and target them at the cloud repository. When a job starts, Veeam Backup & Replication performs the following actions:

1. The tenant starts a backup or backup copy job. The Veeam backup server on tenant's side sends a request to the cloud gateway to access the cloud repository.

2. The cloud gateway passes this request to the SP Veeam backup server.

3. The SP Veeam backup server provides a TLS certificate and establishes a secure connection between the SP Veeam backup server and tenant Veeam backup server.

4. VM data from tenant's side is transported through the cloud gateway to the cloud repository. If the SP has several cloud gateways, VM data is transported through the least loaded cloud gateway being online.

The restore process from the cloud repository is performed in a similar manner. Tenant's Veeam backup server creates a communication channel with the cloud repository through the cloud gateway and retrieves VM data over this channel.

Tasks with Cloud Repository

Tasks on Tenant Side

Tenants can perform the following data backup and recovery tasks in Veeam Backup & Replication against the cloud repository:

Data Backup

- VM backup

- VMware Cloud Director backup (for VMware vSphere platform)

- Veeam Agent backup

- Backup copy

  Backup copy is supported to a cloud repository only. Backup copy from a cloud repository is not supported.

  For information about types of backups for which backup copy to the cloud repository is supported, see Backup Copy to Cloud Repository.

Data Recovery

Tenants can perform the following operations:

- Data restore

  - Entire VM restore

  - VMware Cloud Director restore (for VMware vSphere platform)

  - VM files restore

  - VM disks restore (for VMware vSphere platform)

  - VM guest OS files restore (Microsoft Windows only. Multi-OS restore is not supported.)

  - Application items restore

  - Volume restore (for backups created with Veeam Agent for Microsoft Windows)

  - Disk export (for backups created with Veeam Agent for Microsoft Windows)

  - Guest OS files restore (for backups created with Veeam Agent for Microsoft Windows)

- Backup export

- File copy (manual operations)

Tasks on SP Side

In addition to data restore operations performed by the tenant, the SP can perform Instant Recovery from tenant backups in the cloud repository.

Insider Protection

In some situations, keeping primary or additional backups in a cloud repository may be not enough to ensure data security for a tenant. The backed-up data may become unavailable because of an insider attack. For example, a hacker can gain access to the tenant Veeam Backup & Replication console and delete all tenant backups, including off-site backups stored in the cloud repository. Or a backup administrator on the tenant side can accidentally or intentionally delete backups from a cloud repository. Veeam Backup & Replication allows the SP to protect tenant data against attacks of this kind.

Veeam Backup & Replication offers the insider protection functionality for the following types of tenant backups:

- VM backups and Veeam Agent backups created by backup jobs configured in Veeam Backup & Replication

- Backups of physical or virtual machines created by Veeam Agent backup jobs configured in Veeam Agent for Microsoft Windows or Veeam Agent for Linux

- Backup copies of VM backups or Veeam Agent backups created by backup copy jobs configured in Veeam Backup & Replication

The SP can enable the insider protection option individually for a specific tenant. To enable the option, the SP must select the **Keep deleted backup files for <N> days** check box in the properties of the tenant account. With this option enabled, when a backup or a specific restore point in the backup chain is deleted from the cloud repository, Veeam Backup & Replication does not immediately delete the actual backup files. Instead, Veeam Backup & Replication moves backup files to the "recycle bin".

Technically, a "recycle bin" is a folder on the backup repository in the SP backup infrastructure whose storage resources are exposed to tenants as cloud repositories. Veeam Backup & Replication automatically creates this folder at the time when a tenant backup file is moved to the "recycle bin" for the first time.

Backup files in the "recycle bin" do not consume the tenant quota. However, these backup files consume disk space on the SP storage where the cloud repository is configured. Thus, if the SP plans to offer insider protection to tenants, they should consider allocating sufficient storage resources in the Veeam Cloud Connect infrastructure.

For the tenant, backup files moved to the "recycle bin" appear as actually deleted. The tenant cannot access backup files in the "recycle bin" and perform operations with them. If a tenant needs to restore data from a deleted backup whose backup files still reside in a "recycle bin", the tenant must contact the SP to obtain the necessary backup file(s). To learn more, see Data Restore from Deleted Backups.

> **NOTE**
>
> Consider the following:
>
> - If a tenant renames a job targeted at the cloud repository, and then deletes a backup, Veeam Backup & Replication will move the backup file(s) to a folder with the initial name of the job. As a result, it may become difficult for the SP to find the necessary backup files in case the tenant needs to restore data from backup files in the "recycle bin". To overcome such situations, the SP should recommend tenants who use the insider protection functionality to avoid renaming jobs targeted at the cloud repository of the SP.
> - After the SP enables insider protection for the tenant account, the tenant can use the **Files** view in the Veeam Backup & Replication console only to delete backup files from the cloud repository. Other operations with backup files in the **Files** node are unavailable.
> - The insider protection functionality is not supported for backups that reside in an object storage repository used as a cloud repository.

Veeam Backup & Replication keeps tenant backup files in the "recycle bin" for a specific number of days defined by the SP. After this period expires, Veeam Backup & Replication completely deletes tenant backup files from the "recycle bin".

How Insider Protection Works

Veeam Backup & Replication performs protection of tenant backup files against accidental or intentional deletion in the following way:

1. The SP enables the **Keep deleted backup files for <N> days** option in the properties of the tenant account.

2. The tenant creates a backup in the cloud repository in one of the following ways:

   o In Veeam Backup & Replication, runs a VM backup job, Veeam Agent backup job or backup copy job targeted at the cloud repository.

   o In Veeam Agent for Microsoft Windows or Veeam Agent for Linux, runs a Veeam Agent backup job targeted at the cloud repository.

3. When a backup or restore point is deleted from the cloud repository, Veeam Backup & Replication moves the backup file(s) to the _RecycleBin_ folder on the SP backup repository whose storage resources are exposed to tenants as cloud repositories. Veeam Backup & Replication performs this operation in the following cases:

   o When the tenant performs the _Delete from disk_ operation with a backup on a cloud repository.

      In this case, Veeam Backup & Replication performs the following operations:

      i. On the tenant side, Veeam Backup & Replication removes the backup from the tenant Veeam Backup & Replication console and database.

      ii. On the SP side, Veeam Backup & Replication moves backup files pertaining to the deleted backup to the "recycle bin".

   o When the tenant performs the _Delete_ operation with a backup file on a cloud repository in the **Files** node of the Veeam Backup & Replication console.

   o When one or more backup files are automatically deleted from the backup chain in a cloud repository according to the retention policy defined in the job settings. This includes deletion of obsolete backup files within a backup or backup copy job session, or by a background retention job. This does not include incremental backup files of forever forward incremental backup chains that are merged to a full backup file during backup chain transform.

   Veeam Backup & Replication moves to the "recycle bin" only backup files of the VBK, VIB and VRB types. VBM backup files are deleted from disk immediately.

> **NOTE**
>
> Consider the following:
>
> - If the tenant plans to create off-site backups with a backup copy job, they should enable GFS retention settings in the job properties. This way, Veeam Backup & Replication will be able to protect backups created with the job against an attack when a hacker reduces the job's retention policy and creates a few incremental backups to remove backed-up data from the backup chain.
>
>   With GFS retention settings enabled, the backup chain will contain a sequence of full backups that will not merge according to a retention policy. After such a backup is moved to the "recycle bin", the tenant will be able to use it for data restore.
>
>   If the tenant does not enable GFS retention settings for the backup copy job, the job will complete with a warning. In the job statistics window, Veeam Backup & Replication will display a notification advising to use the GFS retention scheme for the job.
>
> - If the SP uses the capacity tier or archive tier functionality, insider protection processes backup files differently depending on the way the backup files were offloaded to object storage. For more information, see Insider Protection and Capacity Tier.

4. Veeam Cloud Connect Service running on the SP backup server checks the configuration database to get the date when the backup file was moved to the "recycle bin" and compares it to the current date. This operation is performed regularly with an interval of 20 minutes.

5. When the time interval between the date when the backup file was moved to the "recycle bin" and the current date exceeds the number of days specified in the **Keep deleted backup files for <N> days** setting, Veeam Backup & Replication deletes the backup file from the _RecycleBin_ folder.

Insider Protection and Capacity Tier

The SP can use insider protection along with the capacity tier functionality. In this scenario, when a tenant backup whose data was offloaded to capacity tier is deleted from the cloud repository, Veeam Backup & Replication processes backup files in one of the following ways:

- If the tenant data was *copied* to capacity tier, Veeam Backup & Replication moves backup files that reside in performance tier to the "recycle bin". After that, Veeam Backup & Replication deletes backup files that reside in capacity tier from the object storage.

  Backup files are kept in the "recycle bin" for the number of days specified in the properties of the tenant account. After that, Veeam Backup & Replication removes backup files from the "recycle bin".

- If the tenant data was *moved* to capacity tier, Veeam Backup & Replication does not move the actual backup files to the "recycle bin". Instead, Veeam Backup & Replication marks the backup files as moved to the "recycle bin". This information is saved in the configuration database on the SP backup server.

  Information about backups in insider protection is kept in the database for the number of days specified in the properties of the tenant account. After that, Veeam Backup & Replication removes backup files from capacity tier.

In case the tenant needs to restore data from deleted backups whose files reside in capacity tier (that is, backups whose data was *moved* to capacity tier), the SP must download the necessary backup files from capacity tier. This operation is performed using Windows PowerShell scripts. For details, contact Veeam Customer Support.

When the SP downloads deleted backups from capacity tier, Veeam Backup & Replication performs the following operations:

1. Downloads backup files from capacity tier and saves them to the "recycle bin" in performance tier.

2. Removes backup files from capacity tier.

The same mechanism applies to tenant backups that were offloaded to archive tier in the scenario where the SP uses insider protection along with the archive tier functionality.

> **NOTE**
>
> If the tenant uses data deduplication, backup files in object storage that are marked as moved to the "recycle bin" share data blocks with other backup files in object storage.

Data Restore from Deleted Backups

In contrast to backups that reside on the cloud repository, backup files in the "recycle bin" are not intended for regular data restore. However, in a situation where an attacker manages to delete tenant backup(s) from a cloud repository, or if the tenant deletes a backup from a cloud repository by mistake, the tenant may need to restore data from a backup file that was moved to the "recycle bin". Data restore directly from a backup file in the "recycle bin" is not supported in Veeam Backup & Replication. To restore data from such a backup, the tenant needs to obtain backup file(s) from the "recycle bin" first.

Veeam Backup & Replication moves to the "recycle bin" only backup files of the VBK and VIB type. VBM files are deleted from disk immediately when a tenant deletes a backup or a backup file is automatically deleted from the backup chain according to the retention policy. As a result, the SP cannot simply move a backup file back to the folder with tenant backups on the cloud repository. Instead, the SP and tenant need to complete the following steps:

1. The tenant contacts the SP informing that they want to restore data from a deleted backup.

   > **IMPORTANT**
   >
   > Before restoring data from a deleted backup, the tenant must make sure that a VBM file with metadata of this backup does not remain on the cloud repository. If a tenant needs to restore data from a deleted backup file pertaining to a backup that still exists on the cloud repository, the tenant must delete this backup prior to importing a VBK file in the tenant backup console.
   >
   > For assistance with data restore from a deleted backup, consider submitting a support case to the Veeam Support Team.

2. The SP finds one or more backup files required for data restore in the "recycle bin" and passes them to the tenant, for example, over the network or on a portable drive.

   Alternatively, if the SP uses a simple backup repository as a cloud repository, the SP can copy backup files from the "recycle bin" to the folder with tenant backups in the cloud repository. The tenant can then copy the backup files from the cloud repository using the **Files** view in the tenant Veeam Backup & Replication console.

   > **NOTE**
   >
   > If the SP uses the capacity tier functionality, and deleted backups reside in capacity tier, the SP must locate the necessary backup files and download them from capacity tier using Windows PowerShell scripts. For details, contact Veeam Customer Support.

3. The tenant imports the VBK files in the Veeam Backup & Replication console on the tenant backup server.

4. After successful import of a backup, the tenant can restore data from the backup in a regular way.

5. [Optional] The tenant may want to continue the backup chain started with the obtained backup file(s). This operation can be available depending on multiple conditions. For details, consider submitting a support case to the Veeam Support Team.

Support for Capacity Tier

SPs who use a scale-out backup repository as a cloud repository can use the *Capacity Tier* functionality. This functionality allows the SP to offload backup chains created by tenant jobs from an on-premises extent of a scale-out backup repository to a cloud-based object storage. This helps the SP free up disk space on the on-premises extent and make this space available for new backup files created by tenants. Whereas offloaded tenant data is kept in a less expensive object storage.

For more information, see the Capacity Tier section in the Veeam Backup & Replication User Guide.

Veeam Backup & Replication supports offload to capacity tier for backups created by tenant VM backup jobs, Veeam Agent backup jobs and backup copy jobs.

For the tenant, backups in capacity tier are displayed in the Veeam backup console in the same way as regular cloud backups. The tenant is unaware of where their actual backup files reside — in performance tier or capacity tier — and cannot copy backup data between the capacity tier and performance tier. The tenant can perform the same data restore operations with backups in capacity tier as with backups in performance tier.

The SP can download tenant data that was offloaded to the capacity tier back to the performance tier. To learn more, see Downloading Tenant Data from Capacity Tier.

Backup to Object Storage

The SP can allocate object storage resources as cloud repository resources to tenants. To do this, the SP must add an object storage repository in the Veeam Backup & Replication infrastructure and assign this backup repository as a cloud repository in the properties of a tenant account. Once the tenant connects to the SP, they can create backup jobs targeted at the cloud repository that uses object storage as a back end.

This functionality allows the SP to use object storage as a target location for tenant backups without the need to configure scale-out backup repositories extended with capacity tier object storage. It may be helpful, for example, if the SP wants to keep the entire tenant data in object storage instead of offloading backup chains from on-premises extents of a scale-out backup repository to a cloud-based object storage.

The SP can use the following types of object storage as a cloud repository:

- S3 compatible

- Amazon S3, Amazon S3 Glacier and AWS Snowball Edge

- Google Cloud

- IBM Cloud

- Microsoft Azure Blob, Azure Archive Storage and Azure Data Box

- Wasabi Cloud Storage

The SP can add use object storage as a simple backup repository or as an extent of a scale-out backup repository — both as a performance tier extent or capacity tier extent.

Veeam products on the tenant side communicate with the object storage using one of the following connection modes:

- *Connection through a gateway server*. In this mode, the tenant accesses object storage through a proxy component — a gateway server assigned in the SP Veeam Backup & Replication console. Backup data is sent from Veeam Backup & Replication or Veeam Agent on the tenant side to the gateway server on the SP side, and then it is sent from the gateway server to the object storage used as a cloud repository.

- *Direct connection*. In this mode, the tenant accesses object storage directly. Backup data is sent from Veeam Backup & Replication or Veeam Agent on the tenant side to the object storage on the SP side.

  To access object storage repository in the direct connection mode, Veeam products on the tenant side use temporary credentials issued by Veeam Backup & Replication running on the SP side. Veeam Backup & Replication on the SP backup server obtains these credentials for each tenant or subtenant through object storage APIs and saves them to its configuration database. Veeam Backup & Replication passes these credentials to the tenant side only for backup, restore and other necessary operations. On the tenant side, the credentials are kept encrypted in the runtime process and are not saved in the configuration database.

  Temporary credentials provide tenants and subtenants with the following permissions:

  o *Read* access to the backup repository configuration

  o *Full* access to the folder in object storage where cloud repository quota for the tenant or subtenant is allocated

Getting Started with Backup to Object Storage

To assign a quota in object storage to the tenant, the SP must complete the following steps:

1. Add an object storage repository in the SP Veeam backup infrastructure. For details, see the Adding Object Storage Repositories section in the Veeam Backup & Replication User Guide.

2. [For S3 compatible object storage] Set up access permissions for the added S3 compatible object storage repository. For details, see the Managing Permissions for S3 Compatible Object Storage section in the Veeam Backup & Replication User Guide.

3. Assign the added object storage repository as a cloud repository to the tenant account. For details, see Registering Tenant Accounts.

Once the tenant connects to the SP, they can create VM backup jobs and Veeam Agent backup jobs targeted at the cloud repository that uses object storage as a back end.

Considerations and Limitations

Backup to object storage in the Veeam Cloud Connect Backup scenario has the following requirements and limitations.

- To be able to back up data to object storage, the tenant must run one of the following Veeam products:

  o Veeam Backup & Replication 12

  o Veeam Agent for Microsoft Windows 6.0

  o Veeam Agent for Linux 6.0

  o Veeam Agent for Mac 2.0

  In earlier product versions, object storage repositories used as cloud repositories are not displayed on the tenant side.

- The Insider Protection functionality is not available to tenant accounts that have at least one object storage repository assigned as a cloud repository.

- Although in the direct connection mode tenant backup data is sent from the tenant side to the object storage on the SP side directly, connection from the tenant Veeam backup server to a cloud gateway is required.

- Object storage repositories used as a cloud repository are not supported by transaction log backup copy jobs.

- The tenant can enable configuration backup in Veeam Backup & Replication and target it at object storage repository used as a cloud repository. I this case, the configuration backup data will be transferred to the object storage through a gateway server regardless of the connection mode specified by the SP in the object storage repository settings.

- Helper appliance used to perform health check for backups that reside in object storage is not supported in Veeam Cloud Connect. If the tenant enables health check in the properties of a backup job targeted at an object storage repository used as a cloud repository, Veeam Backup & Replication will display a message notifying that this operation may require additional costs.

- Data transfer through WAN accelerators is supported only for S3 Compatible object storage repositories in the *Connection through a gateway server* mode.

- Azure Immutability is not supported for object storage repositories in the *Direct connection* mode used as cloud repositories.

- For the Google Cloud storage used as a cloud repository, consider the following:

  o The *Connection through a gateway server* mode is supported without prerequisites and limitations.

  o To use Google Cloud storage as a cloud repository in the *Direct connection* mode, you must configure the helper appliance when adding the object storage repository in Veeam Backup & Replication. Although the helper appliance is not supported for health check with object storage repositories, it is required for issuing temporary credentials to enable direct to access the object storage.

Backup Copy to Cloud Repository

To follow the 3-2-1 backup best practice, you can configure a backup copy job and target it at the cloud repository. Backup copy jobs allow you to create several instances of the same backup file in different locations, onsite or offsite. For example, you can configure a backup job to create a VM backup on the local backup repository, and use the backup copy job to copy the created VM backup from the local backup repository to the cloud repository. Copied backup files have the same format as those created by backup jobs, and you can use any data recovery option for them.

During the backup copying process, Veeam Backup & Replication does not simply copy a backup file from one backup repository to another. Instead, Veeam Backup & Replication retrieves data blocks necessary to create a restore point as of the latest point in time and copies this data to the cloud repository. The backup chain produced on the target backup repository is forever-incremental: the first file in the chain is a full backup while all subsequent restore points are incremental.

The backup copy process is job-driven. When you create a backup copy job, you define what backup file you want to copy, the target repository for storing the copy, retention policy and other settings for the copying process. The backup copy job supports the GFS retention scheme, allowing you to design a long-term archiving plan.

The backup copy process differs depending on the backup copy mode: immediate copy or periodic copy.

- In the immediate copy mode, once a new restore point has been added to the primary backup chain, the backup copy job immediately copies it to the target backup repository. After that, the backup copy job stops until a new restore point appears on the source backup repository. You can specify the backup copy window to allow the job to copy restore points during specific time periods only.

- In the periodic copy mode, the backup copy job runs according to the schedule that you specify in the backup copy job settings. You can set up the job to run daily, monthly or periodically at the specified time, specify automatic job retry settings and specify the backup copy window to allow the job to copy restore points during specific time periods only. When the backup copy job starts, Veeam Backup & Replication checks the source backup repository: if a new restore point has been added to the primary backup chain, Veeam Backup & Replication automatically copies it to the target backup repository.

Supported Backup Types

Veeam Backup & Replication supports backup copy to the cloud repository for the following types of backups:

- Backups of VMware vSphere VMs created by Veeam Backup & Replication

- Backups of VMware Cloud Director VMs created by Veeam Backup & Replication

- Backups of Microsoft Hyper-V VMs created by Veeam Backup & Replication

- Backups of Microsoft Windows machines created by Veeam Agent for Microsoft Windows

- Backups of Linux machines created by Veeam Agent for Linux

- Backups of Mac machines created by Veeam Agent for Mac

- Backups of IBM AIX machines created by Veeam Agent for IBM AIX

- Backups of Oracle Solaris machines (based on the x86 or SPARC architecture) created by Veeam Agent for Oracle Solaris

- Backups of Nutanix AHV virtual machines created by Veeam Backup for Nutanix AHV
- Backups of Amazon EC2 instances created by Veeam Backup for AWS
- Backups of Microsoft Azure virtual machines created by Veeam Backup for Microsoft Azure
- Backups of Google Compute Engine VM instances created by Veeam Backup for Google Cloud

Background Retention for Tenant Backups

In addition to applying a retention policy within a job session, Veeam Backup & Replication performs background retention for backups.

In the Veeam Cloud Connect infrastructure, background retention is applied to tenant backups on the SP side. The background retention job runs automatically in Veeam Backup & Replication on the SP backup server according to the same rules as in the regular Veeam backup infrastructure. The SP can also launch background retention manually. For details, see the Background Retention section in the Veeam Backup & Replication User Guide.

For background retention of tenant backups in the cloud repository, in addition to considerations for the regular background retention, consider the following:

- To all types of tenant accounts, the same background retention rules are applied.

- Background retention is applied to backups created by tenants and their subtenants.

- The background retention job removes tenant backups regardless of whether the tenant is in the *Enabled* or *Disabled* state.

- Insider protection is supported. If the insider protection functionality is enabled for the tenant account, backups removed by the background retention job are moved to the "recycle bin".

- If the SP removes the tenant account and does not delete tenant backup files from the cloud repository, the background retention job will remove the backup files in the same way as a regular orphaned backup chain.

Instant Recovery from Tenant Backups

The SP can perform Instant Recovery for tenant workloads, that is, recover workloads from tenant backups in the cloud repository and register them as VMs on a VMware vSphere host on the SP side. This may be helpful in case a machine on the tenant side becomes unavailable, and the tenant cannot fail over to a VM replica on the cloud host. Instead, the tenant can request the SP to recover the necessary VM from the backup.

To use this functionality, the SP and tenant must make sure that the following conditions are met:

- To allow the SP to view tenant backups in the SP backup console, the tenant must select the **Allow this Veeam Backup & Replication installation to be managed by the service provider** check box when connecting to the SP. For details, see Connecting to Service Providers.

  > **NOTE**
  >
  > For Active Directory tenant account, tenant backups are displayed in the SP backup console regardless of whether the **Allow this Veeam Backup & Replication installation to be managed by the service provider** option is enabled on the tenant side.

- The target VMware vSphere host where the SP plans to register the recovered VMs must be added to the Veeam Backup & Replication infrastructure on the SP backup server.

- Veeam Cloud Connect supports Instant Recovery from unencrypted backups only.

Instant Recovery from tenant backups works in the similar way as the regular one. For more information, see the Instant Recovery to VMware vSphere section in the Veeam Backup & Replication User Guide.

For Instant Recovery from tenant backups, consider the following:

- Veeam Cloud Connect supports Instant Recovery from any type of tenant backups for which recovery to VMware vSphere is supported. This includes VM backups, Veeam Agent backups and backups created by backup copy jobs in the cloud repository.

- Veeam Cloud Connect supports Instant Recovery from backups that reside in performance tier, capacity tier or archive tier.

- During Instant Recovery, the tenant account will be in the disabled state.

- Migration of a recovered VM back to the tenant production site is unavailable. The SP can finalize the Instant Recovery process by migrating the VM to the SP virtual environment.

- Separate prerequisites and limitations apply to Instant Recovery from VM backups and Instant Recovery from Veeam Agent backups. For details, see the following sections in the Veeam Backup & Replication documentation:

  o For Instant Recovery from VM backups, see the Before You Begin section in the Veeam Backup & Replication User Guide.

  o For Instant Recovery from Veeam Agent backups, see the Restoring Veeam Agent Backup to vSphere VM section in the Veeam Agent Management Guide.

Tenant backups become available in the Veeam backup console on the SP side. The SP can view backups in the **Home** view, under the **Backups** node. To identify the owner of the backup, the SP can use the **Tenant Name** column in the working area:

- For VM backups and Veeam Agent backups created under the tenant account, Veeam Backup & Replication displays the tenant name in the **Tenant Name** column.

- For Veeam Agent backups created under the subtenant account, Veeam Backup & Replication displays the subtenant name in the **Tenant Name** column.

Veeam Cloud Connect Replication

With Veeam Backup & Replication, SPs can offer Disaster Recovery as a Service (DRaaS) to their customers.

Veeam Backup & Replication provides disaster recovery through image-based VM replication. The SP can expose resources of their virtualization environment to tenants as cloud hosts.

Tenants can utilize cloud hosts provided by the SP to create VM replicas offsite. In case of a disaster on the production site, tenants can quickly and easily switch to VM replicas in the cloud and use the SP infrastructure as a remote disaster recovery site.

The SP can provide Veeam Cloud Connect Replication resources for the following virtualization platforms:

- VMware vSphere

- Microsoft Hyper-V

As well as the Veeam Cloud Connect Backup infrastructure, the Veeam Cloud Connect Replication infrastructure has a multi-tenant architecture. The SP allocates computing, storage and network resources for a replication target and provides them to tenants through hardware plans. For the SP, a hardware plan is an abstraction layer that lets the SP virtually partition a virtualization host or cluster into multiple replication targets. As a result, the SP can expose replication resources to several tenants and store tenants' data in the cloud in an isolated and segregated way.
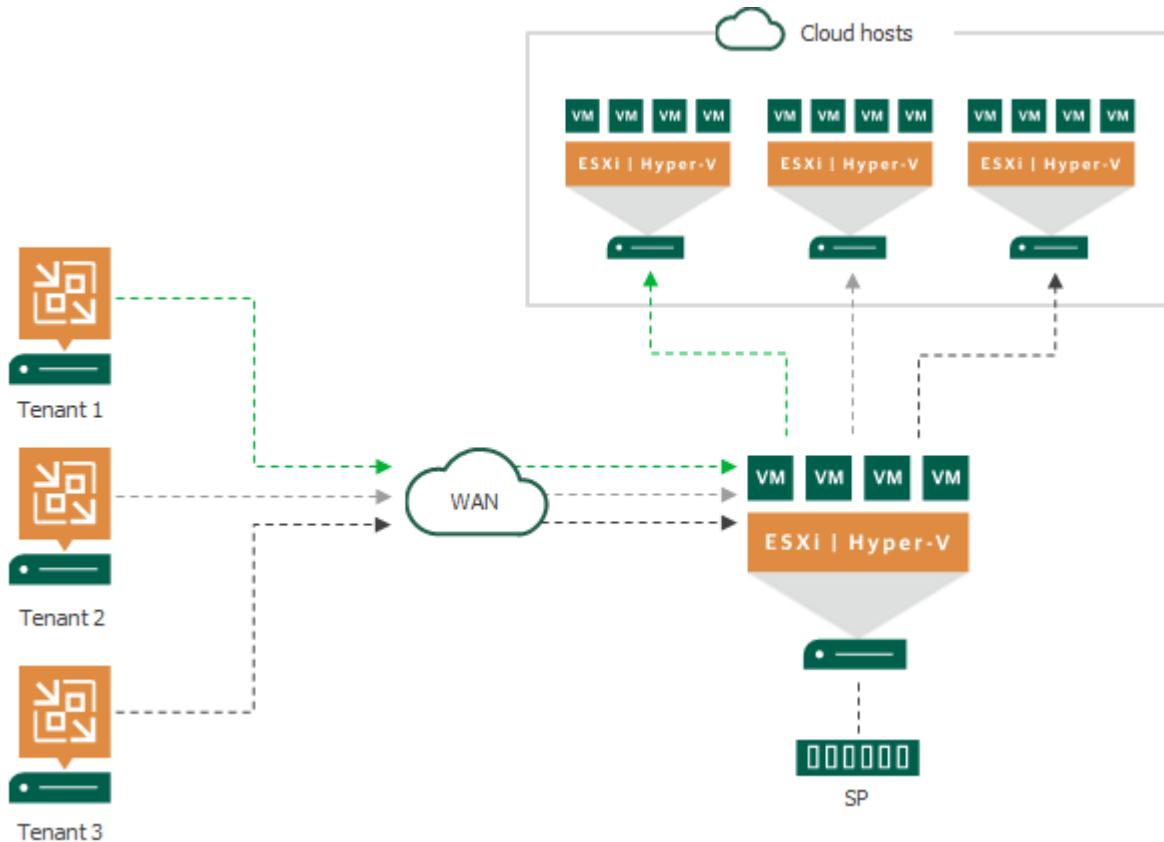
For a tenant, a hardware plan appears as a cloud host that can be used as a regular target host for off-site replication.

To make VM replicas on the cloud host accessible over the network after failover, Veeam Backup & Replication provides each tenant with network resources — network extension appliances and dedicated VLANs. The tenant can fail over a group of production VMs (full site failover) or individual VMs (partial site failover) to VM replicas on the cloud host. Veeam Backup & Replication establishes a secure channel between VM replicas in the cloud and VMs on the production site and offers traffic encryption capabilities.

> **NOTE**
>
> Consider the following:
>
> - The SP can also use VMware Cloud Director to allocate replication resources for tenant VMware vSphere VMs. To learn more, see VMware Cloud Director Support.
> - Apart from snapshot-based replication, the SP can provide the Continuous Data Protection (CDP) functionality to tenants. To learn more, see Continuous Data Protection (CDP) with Veeam Cloud Connect.

Data protection and disaster recovery tasks targeted at the cloud host are performed by tenants. Tenants can set up necessary replication jobs and perform failover operations on Veeam backup servers deployed on their side. Tenants can perform the following operations:

- Replicate VMs to the cloud host.

- Perform failover tasks with VM replicas on the cloud host:

  - Full site failover, when all critical production VMs fail over to their replicas on the cloud host in case the whole production site becomes unavailable.

  - Partial site failover, when one or several VMs become corrupted and fail over to their replicas on the cloud host.

- Perform failback tasks with VM replicas on the cloud host.

Tasks associated with full site failover can be performed either by a tenant or by the SP. This lets the SP test the full site failover process and switch tenant's production site to the cloud host upon tenant's request if the tenant has no access to the backup infrastructure after a disaster.

Getting Started with Veeam Cloud Connect Replication

To provide Disaster Recovery as a Service through image-based VM replication to tenants, the SP must set up the Veeam Cloud Connect Replication infrastructure.

Before the SP starts configuring the Veeam Cloud Connect Replication infrastructure, they must consider limitations for hardware plans. Limitations apply to virtualization hosts whose resources the SP plans to expose as a replication target to tenants. To learn more, see Adding Hardware Plans: Before You Begin.

As part of the configuration process, the SP must perform the following tasks:

1. Deploy the SP Veeam backup server.

2. Set up TLS certificates.

3. Create cloud gateways.

4. Allocate VLANs for cloud networking.

5. Allocate a pool of public IP addresses for full site failover.

6. Configure hardware plans.

7. Specify credentials for network extension appliances.

8. [Optional] Deploy Veeam Cloud Connect Portal.

9. [Optional] Configure target WAN accelerators.

10. Register tenant accounts.

11. Communicate information about the tenant account and gateway to all tenants who plan to connect to the SP.

> **NOTE**
>
> The SP can also allocate VMware Cloud Director resources as replication resources to the tenant. To learn more, see Veeam Cloud Connect Replication to VMware Cloud Director.
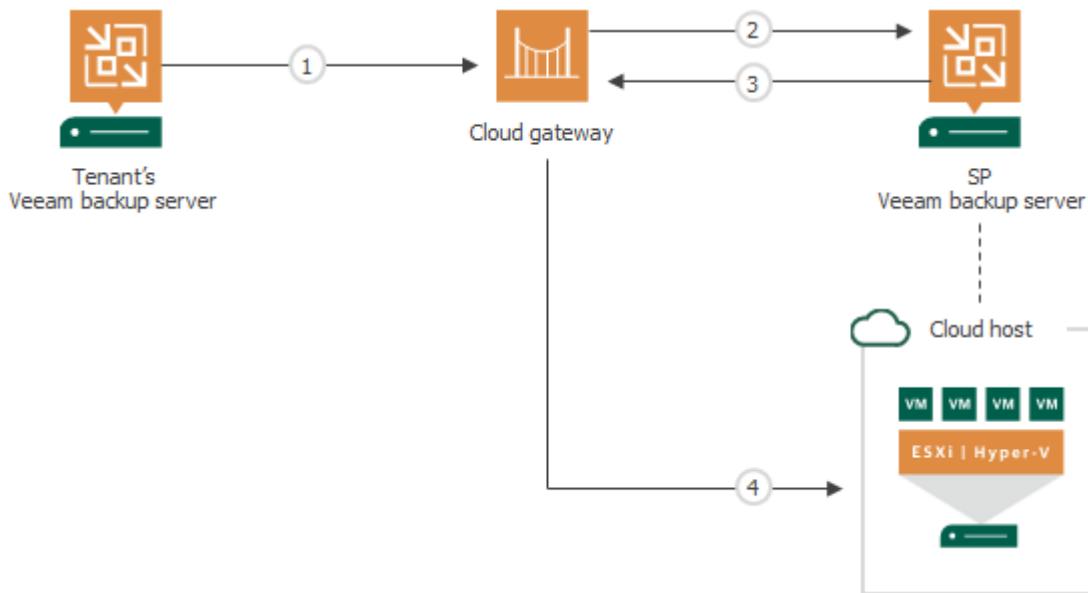
Once the SP has configured necessary components, tenants can add the SP to their Veeam Backup & Replication consoles and use cloud hosts allocated to them in the SP Veeam Cloud Connect infrastructure.

How Veeam Cloud Connect Replication Works

Tenants who plan to replicate their VMs to the cloud must configure replication jobs on their Veeam backup servers and target them at the cloud host. When a job starts, Veeam Backup & Replication performs the following actions:

1. The tenant starts a replication job. The Veeam backup server on tenant's side sends a request to the cloud gateway to access the cloud host.

2. The cloud gateway passes this request to the SP Veeam backup server.

3. The SP Veeam backup server provides a TLS certificate and establishes a secure connection between the SP Veeam backup server and tenant Veeam backup server.

4. VM data from tenant's side is transported through the cloud gateway to the cloud host. If the SP has several cloud gateways, VM data is transported through the least loaded cloud gateway being online.

In case of a disaster on the tenant production site, when one or several VMs become corrupted, a tenant can fail over to VM replicas on the cloud host. To learn more, see Cloud Replica Failover And Failback.

Tasks with Cloud Host

Tenants can perform the following VM replication and data recovery tasks against the cloud host:

- Replication

- Failover:

    o Full site failover (failover by cloud failover plan)

    o Partial site failover

- Failback

- Restore from replica

    o VM guest OS files restore (Microsoft Windows FS only. Multi-OS restore is not supported.)

    o Application items restore

As well as snapshot-based replicas, the tenant can create CDP replicas on the cloud host. To learn more, see Continuous Data Protection (CDP) with Veeam Cloud Connect.

Cloud Replica Failover and Failback

In case of software or hardware malfunction on the production site, a tenant can quickly recover a corrupted VM by failing over to its replica in the cloud. When you perform cloud failover, a replicated VM on the cloud host takes over the role of the original VM. A tenant can fail over to the latest state of a replica or to any of its good known restore points.

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

Depending on the scale of the disaster that affects the production site, a tenant can choose one of the following cloud failover scenarios:

- *Full site failover* — the whole production site becomes unavailable and all critical VMs that run interdependent applications fail over to their replicas on the cloud host.

- *Partial site failover* — one or several VMs become corrupted and fail over to their replicas on the cloud host.

In Veeam Backup & Replication, the actual failover is considered a temporary stage that should be further finalized. While the replica is in the *Failover* state, you can undo failover, perform failback or perform permanent failover.

> **NOTE**
>
> This and subsequent sections describe failover and failback aspects that are specific for Veeam Cloud Connect Replication. To get a detailed description of all failover and failback options supported in Veeam Backup & Replication, see the following sections in the Veeam Backup & Replication User Guide:
>
> - [Replica Failover and Failback](#)
> - [Replica Failover and Failback for CDP](#)

Full Site Failover

If the whole tenant production site becomes unavailable because of a software or hardware malfunction, the tenant can perform full site failover. In the full site failover scenario, all critical VMs fail over to their replicas on the cloud host one by one, as a group.

Full site failover is in many regards similar to regular failover by a failover plan. To perform full site failover, Veeam Backup & Replication uses a cloud failover plan that lets Veeam Backup & Replication automatically start VM replicas on the cloud host in the specified order with the specified time delay. To learn more, see [Cloud Failover Plan](#).

Full site failover is performed in the similar way as regular failover with a failover plan. The main difference is that the full site failover process contains additional steps regarding the use of the provider-side network extension appliance.
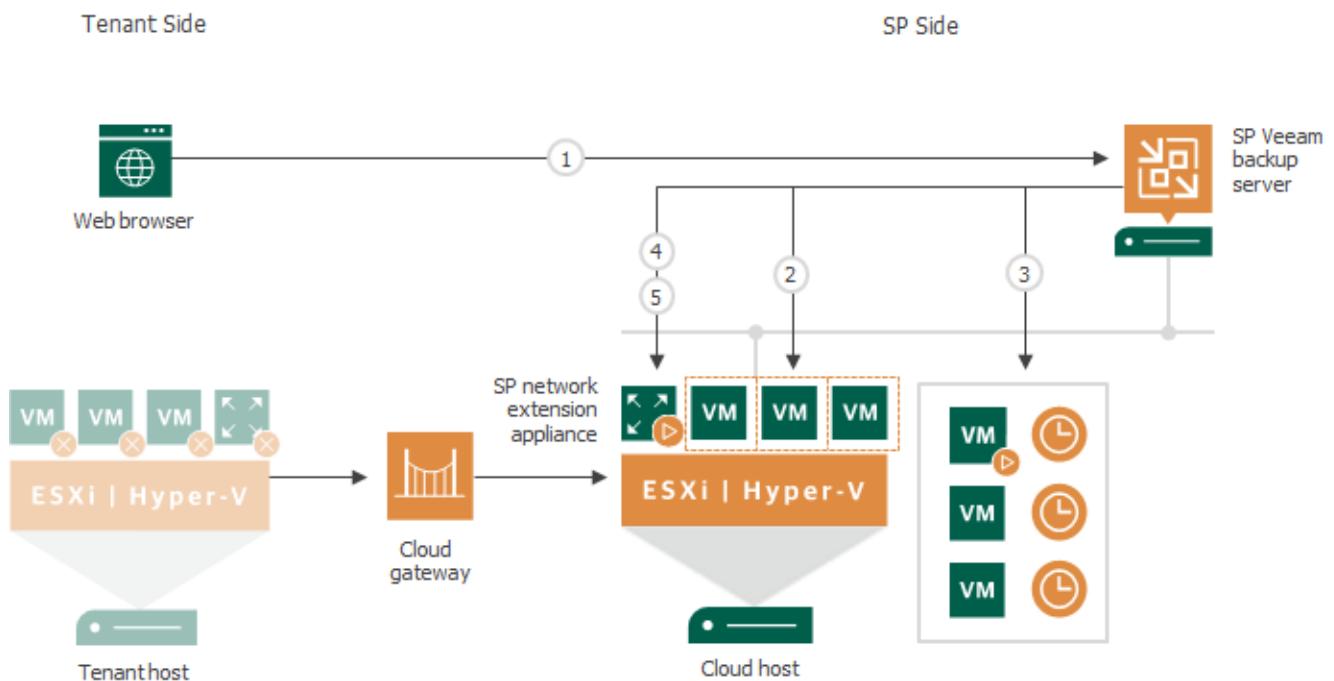
Full site failover is performed in the following way:

1. The tenant starts a cloud failover plan using Veeam Cloud Connect portal (or asks the SP to start full site failover using the SP Veeam Backup & Replication console).

2. For each VM in the cloud failover plan, Veeam Backup & Replication detects its replica. If some VMs in the cloud failover plan have replicas that are already in the *Failover* or *Failback* state, Veeam Backup & Replication suggests that they are processed with the cloud failover plan.

3. The replica VMs are started in the order they appear in the cloud failover plan within the set time intervals.

4. Veeam Backup & Replication starts the network extension appliance on the SP side.

5. Veeam Backup & Replication configures the network extension appliance so that it acts as a gateway between the VM replica network and external networks allowing VM replicas to communicate to the internet.

> **NOTE**
>
> The full site failover process differs for the scenario where tenant VM replicas are created in VMware Cloud Director. To learn more, see Full Site Failover for VMware Cloud Director Replicas.

Cloud Failover Plan

If a tenant production site goes offline after a disaster, a tenant can perform full site failover by running a cloud failover plan.

The cloud failover plan is in many ways similar to the regular failover plan. In the cloud failover plan, you specify VMs that have replicas on the cloud host, set the order in which VMs must be processed and time delays for VMs. The time delay is an interval of time for which Veeam Backup & Replication must wait before starting the failover operation for the next VM in the list. It helps to ensure that some VMs, such as a DNS server, are already running at the time the dependent VMs start. The time delay is set for every VM in the failover plan except the last VM in the list.

The cloud failover plan must be created in advance by a tenant. The created cloud failover plan is stored in the Veeam Backup & Replication database on the SP Veeam backup server. This way, the SP can run a tenant cloud failover plan in case the tenant Veeam backup server is unavailable along with the production site (for example, a tenant Veeam backup server is deployed on a VM that resides on the same host as production VMs).

A tenant can configure one or several cloud failover plans for VMs that have replicas on the same or different cloud hosts. All VMs in the cloud failover plan must have replicas of the same type: either snapshot-based replicas or CDP replicas. Cloud failover plans that contain both VMs with snapshot-based replicas and VMs with CDP replicas are not supported.

In case a group of production VMs goes offline, a tenant can run the cloud failover plan in one of the following ways:

- Start a cloud failover plan using Veeam Cloud Connect Portal.

  This option is available only for cloud failover plans that contain VMs added to replication jobs targeted at the cloud host. It is not available for cloud failover plans created for VMs added to CDP policies.

- Contact the SP so that the SP starts a tenant cloud failover plan using the Veeam Backup & Replication console on the SP Veeam backup server.

- Start a cloud failover plan using the Veeam Backup & Replication console (in case the tenant Veeam backup server is not affected by a disaster).

When the tenant or the SP starts the failover operation, they can choose to fail over to the latest state of a VM replica or to any of its good known restore points.

Limitations for Cloud Failover Plans

- Veeam Backup & Replication supports one failover operation type at a time due to limitations for the network extension appliance:

  o If the tenant or the SP runs a cloud failover plan during partial site failover, Veeam Backup & Replication will prompt to stop the ongoing partial failover operation or wait for the operation to complete before the full site failover operation start.

  o If the tenant or the SP starts partial site failover during full site failover, the partial site failover operation will fail.

- The maximum number of VMs that can be started simultaneously when you run a failover plan is 10. If you have added more VMs to the failover plan and scheduled them to start simultaneously, Veeam Backup & Replication will wait for the first VMs in the list to fail over and then start the failover operation for subsequent VMs. This limitation helps reduce the workload on the production infrastructure and Veeam backup server.

  For example, if you have added 14 VMs to the failover plan and scheduled them to start at the same time, Veeam Backup & Replication will start the failover operation for the first 10 VMs in the list. After the 1st VM is processed, Veeam Backup & Replication will start the failover operation for the 11th VM in the list, then for the 12th VM and so on.

Finalizing Cloud Failover Plans

Failover is a temporary intermediate step that needs to be finalized. The finalizing options for a cloud failover are similar to a regular failover: undoing failover, permanent failover or failback.

> **NOTE**
>
> The failback operation is available on the tenant side only. The SP cannot perform failback for tenant VM replicas in the SP Veeam backup console.

If you decide to perform permanent failover or failback to production, you need to process every VM in the cloud failover plan individually. However, you can undo failover for the whole group of VMs using the undo cloud failover plan option.

Undoing full site failover switches the replica back to the production VM discarding all changes that were made to the replica while it was running. When you undo full site failover, Veeam Backup & Replication detects VMs for which the failover operation was performed during the last cloud failover plan session and switches them back to production VMs. If you perform the failback operation for some of the VMs before undoing the group failover, failed-over VMs are skipped from processing.

Veeam Backup & Replication starts the undo failover operation for a group of 5 VMs at the same time. The time interval between the operation starts is 10 seconds. For example, if you have added 10 VMs to the failover plan, Veeam Backup & Replication will undo failover for the first 5 VMs in the list, then will wait for 10 seconds and undo failover for the remaining 5 VMs in the list. Time intervals between the operation starts help Veeam Backup & Replication reduce the workload on the production environment and Veeam backup server.

Partial Site Failover
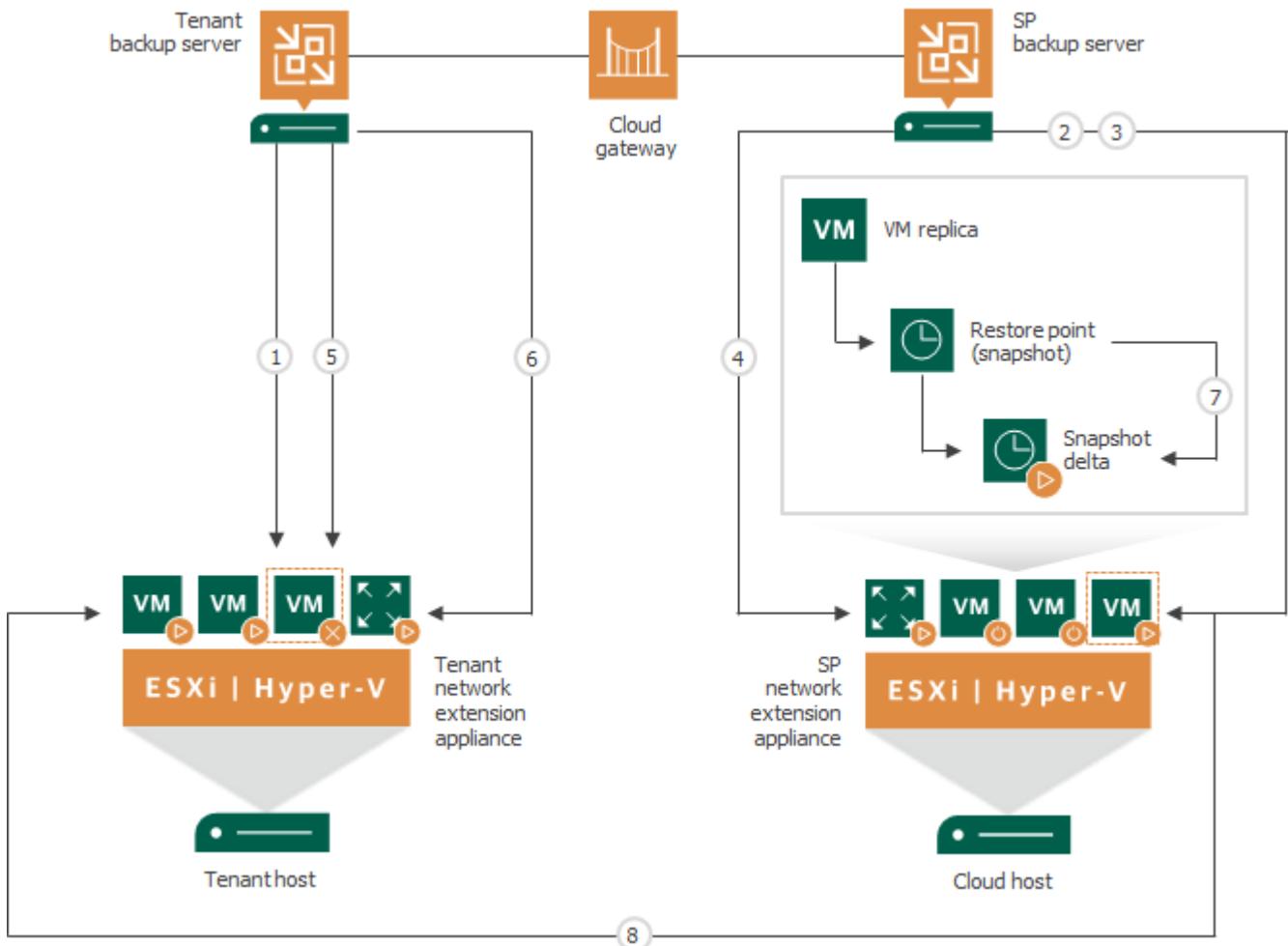
If one or several production VMs become corrupted, but the rest of the production site, including the most critical VMs and Veeam Backup & Replication infrastructure, remain operative, the tenant can perform partial site failover. With partial site failover, the tenant can quickly recover a corrupted VM by failing over to its replica on the cloud host.

To establish a secure connection and enable communication between production VMs and VM replicas on the cloud host after partial site failover, Veeam Backup & Replication uses paired network extension appliances deployed on the tenant side and SP side. To learn more, see Network Extension Appliance.

Partial site failover is performed in the similar way as regular failover. However, the partial site failover process contains several additional steps regarding the use of network extension appliances on the tenant side and SP side:

1. The tenant starts the partial site failover process for a VM in the tenant Veeam Backup & Replication console.

2. Veeam Backup & Replication rolls back the VM replica on the cloud host to the required restore point. To do this, it reverts the VM replica to the necessary snapshot in the replica chain.

3. Veeam Backup & Replication powers on the VM replica. The state of the VM replica is changed from *Normal* to *Failover*. If the original VM still exists and is running, the original VM remains powered on.

4. Veeam Backup & Replication powers on the network extension appliance VM on the cloud host and configures network settings on the appliance:

   o Starts a VPN server on the network extension appliance to establish a secure VPN tunnel through the cloud gateway to the appliance on the tenant side.

   o Configures Proxy ARP daemon on the appliance so that the appliance can receive from the VM replica ARP requests addressed to production VMs on the source host and send them to the tenant's network extension appliance through the VPN tunnel.

5. Veeam Backup & Replication temporarily puts replication activities for the original VM on hold (until the VM replica returns to the *Normal* state).

6. Veeam Backup & Replication powers on the network extension appliance on the tenant side and configures network settings on the appliance:

   o Starts a VPN client on the network extension appliance and connects to the VPN server on the network extension appliance on the SP side to establish a secure VPN tunnel through the cloud gateway.

   o Configures Proxy ARP daemon on the network extension appliance so that it can receive ARP requests from production VMs addressed to the VM replica and send them to the network extension appliance on the SP side through the VPN tunnel.

7. All changes made to the VM replica while it is running in the *Failover* state are written to the delta file of the snapshot, or restore point, to which you have selected to roll back.

8. VMs on the tenant side communicate to the VM replica on the cloud host through the secure VPN tunnel that is set between network extension appliances.

Limitations for Partial Site Failover

Partial site failover has the following limitations:

- Veeam Backup & Replication supports one failover operation type at a time. If a tenant or the SP runs a cloud failover plan during partial site failover, Veeam Backup & Replication will suggest that the VM involved in the partial site failover process is processed with the cloud failover plan.

- The tenant can perform partial site failover only for those VMs that have a static IP address.

Network Mapping for Cloud Replicas

To establish a connection between a production VM and a VM replica on the cloud host after partial site failover, Veeam Backup & Replication maps the production network and the virtual network provided to tenant replicas through the hardware plan. As a part of this process, Veeam Backup & Replication applies network settings of the replicated VM to the dedicated SP network extension appliance.

> **NOTE**
>
> This mechanism applies to both snapshot-based replicas and CDP replicas. Keep in mind that for CDP replicas, automatic network mapping is available only if application-aware processing is enabled for the VM in the CDP policy settings.

For Windows-based VMs, Veeam Backup & Replication detects network settings of replicated VMs automatically during every run of a replication job targeted at the cloud host. Veeam Backup & Replication can detect network settings of replicated VMs in the following ways:

- [For snapshot-based replication and CDP] If application-aware processing is enabled for a replication job targeted at the cloud host, Veeam Backup & Replication collects network settings of a replicated VM with the runtime process deployed on this VM for performing guest processing tasks. The runtime process collects network settings of a VM along with information required for VSS-aware restore. To learn more, see the Application-Aware Processing section in the Veeam Backup & Replication User Guide.

- [For snapshot-based replication only] If application-aware processing is not enabled for a replication job targeted at the cloud host, Veeam Backup & Replication collects network settings of a replicated VM within the additional step in the replication process. To do this, Veeam Backup & Replication mounts the system disk of the replicated VM to the tenant Veeam backup server, collects network settings from the registry of the VM and passes the collected settings to the SP backup server. After that, Veeam Backup & Replication transfers VM data from the source host to the cloud host.

  Keep in mind that application-aware processing is a more consistent and reliable method to collect network settings of replicated VMs.

- [For snapshot-based replication only] For VM replicas created from backup files (remote replica from backup scenario), Veeam Backup & Replication applies to the replica network settings that were collected from a VM during the backup process.

If the tenant creates replicas of Windows-based VMs and the number of production networks equals the number of virtual networks on the cloud host, the tenant does not need to specify network mapping settings. Veeam Backup & Replication maps production and virtual networks automatically. After failover, a VM replica in a cloud virtual network will act as if it is connected to the original production network.

For more advanced scenarios, the tenant can create a network mapping table for the replication job targeted at the cloud host. The tenant can perform this operation when creating a replication job, at the **Network** step of the **New Replication Job** wizard.

> **NOTE**
>
> For CDP replicas, the tenant can specify network mapping rules at the **Network** step of the **New CDP Policy** wizard.

For example, specifying network mapping settings may be required when the cloud host has fewer networks than the number of networks in the production infrastructure. This operation is also obligatory if non-Windows VMs are included in the replication job. Automatic network mapping for non-Windows VMs is not currently supported in Veeam Cloud Connect Replication.

Permanent Failover

To finalize the failover process, a tenant can permanently fail over to the VM replica on the cloud host. A tenant can perform the permanent failover operation if they want to permanently switch from the original VM to a VM replica on the cloud host and use this replica as the original VM. As a result of permanent failover, the VM replica takes on the role of the original VM.

In the cloud replication scenario, you can perform permanent failover after full site failover. The permanent failover operation can be started by a tenant from the tenant Veeam backup console or by the SP from the SP Veeam backup console. To perform permanent failover for all VMs in the cloud failover plan, a tenant or the SP needs to process every VM in the cloud failover plan individually.

Permanent failover in the Veeam Cloud Connect Replication scenario practically does not differ from the regular permanent failover operation.

Permanent Failover for Snapshot-Based Replicas

The permanent failover operation for snapshot-based replicas is performed in the following way:

1. Veeam Backup & Replication removes snapshots (restore points) of the VM replica from the snapshot chain and deletes associated files from the storage (datastore or volume depending on the virtualization platform). Changes that were written to the snapshot delta file or differencing disk are committed to the VM replica disk files to bring the VM replica to the most recent state.

2. Veeam Backup & Replication removes the VM replica from the Veeam Backup & Replication console and database on the tenant side and SP side.

3. To protect the VM replica from corruption after permanent failover is complete, Veeam Backup & Replication reconfigures the replication job by adding the source VM to the list of exclusions. When the replication job starts, the original VM is skipped from processing. As a result, no data is written to the working VM replica. Note that other jobs are not modified automatically. When the replication job starts, the source VM is skipped from processing. As a result, no data is written to the working VM replica.

Permanent Failover for CDP Replicas

The permanent failover operation for CDP replicas is performed in the following way:

1. Veeam Backup & Replication powers off the replica.

2. Veeam Backup & Replication removes short-term and long-term restore points of the replica from the replication chain and deletes associated files from the datastore. Changes that were written to the protective virtual disks (*<disk_name>-interim.vmdk*) are committed to the replica to bring the replica to the most recent state.

3. Veeam Backup & Replication removes the replica from the Veeam Backup & Replication console and database on the tenant side and SP side.

4. To protect the replica from corruption after permanent failover is complete, Veeam Backup & Replication reconfigures the current CDP policy by adding the source VM to the list of exclusions. Note that other policies and jobs are not modified automatically. When the CDP policy starts, the source VM is skipped from processing. As a result, no data is written to the working VM replica.

Failback

If a tenant wants to resume operation of a production VM, they can fail back to it from a VM replica on the cloud host. When you perform failback, you get back from the VM replica to the original VM, shift your I/O and processes from the cloud host to the source production host and return to the normal operation mode.

A tenant can perform failback to a production VM after partial site failover or full site failover. If a tenant performs the failback operation after full site failover, they need to process every VM in the cloud failover plan individually.

If a tenant managed to restore operation of the source host at the production site, a tenant can switch from the VM replica to the original VM on the source host. If the source host is not available, a tenant can restore the original VM to a new location and switch back to it.

- To learn more about failback for snapshot-based replicas, see the Failback section in the Veeam Backup & Replication User Guide.

- To learn more about failback for CDP replicas, see the Failback for CDP section in the Veeam Backup & Replication User Guide.

Failback to production is a temporary stage that should be further finalized. After a tenant tests the recovered original VM and make sure it is working without problems, they should commit failback. A tenant also has an option to undo failback and return the VM replica back to the *Failover* state.

The failback operation is available on the tenant side only. The SP cannot perform failback for tenant VM replicas in the SP Veeam backup console.

Continuous Data Protection (CDP) with Veeam Cloud Connect

SPs can use the continuous data protection (CDP) functionality to offer Disaster Recovery as a Service to tenants. CDP extends Veeam Cloud Connect Replication scenarios with an option to create replicas of VMware vSphere VMs without creating snapshots. This allows the SP to protect mission-critical tenant VMs for which data loss is unacceptable: compared to snapshot-based VM replication, CDP provides near-zero recovery time objective (RTO) because CDP replicas are in a ready-to-start state.

CDP with Veeam Cloud Connect is in many ways similar to both CDP in the regular Veeam Backup & Replication infrastructure and snapshot-based Veeam Cloud Connect Replication.

- CDP in the Veeam Cloud Connect environment uses vSphere APIs for I/O filtering (VAIO) in the same way as regular CDP. The general concept of CDP is similar as well: Veeam Backup & Replication maintains the CDP infrastructure and performs continuous data replication of VMware vSphere VMs. To learn more about CDP mechanisms in Veeam Backup & Replication, see the Continuous Data Protection (CDP) section in the Veeam Backup & Replication User Guide.

- CDP in the Veeam Cloud Connect environment supports data protection and disaster recovery scenarios similar to snapshot-based Veeam Cloud Connect Replication, and offers similar workflow. The SP allocates computing, storage and network resources and provides them to tenants through hardware plans or organization VDCs in VMware Cloud Director. CDP has a multi-tenant architecture; CDP infrastructure components are distributed between the tenant side and SP side, and communicate through the cloud gateway.

To use CDP with Veeam Cloud Connect, the SP and tenants must configure the CDP infrastructure on their sides. After that, tenants can create CDP policies targeted at a cloud host. In case a disaster strikes, the tenant can fail over a group of production VMs or individual VMs to CDP replicas on the cloud host.

Veeam Cloud Connect CDP Scenarios
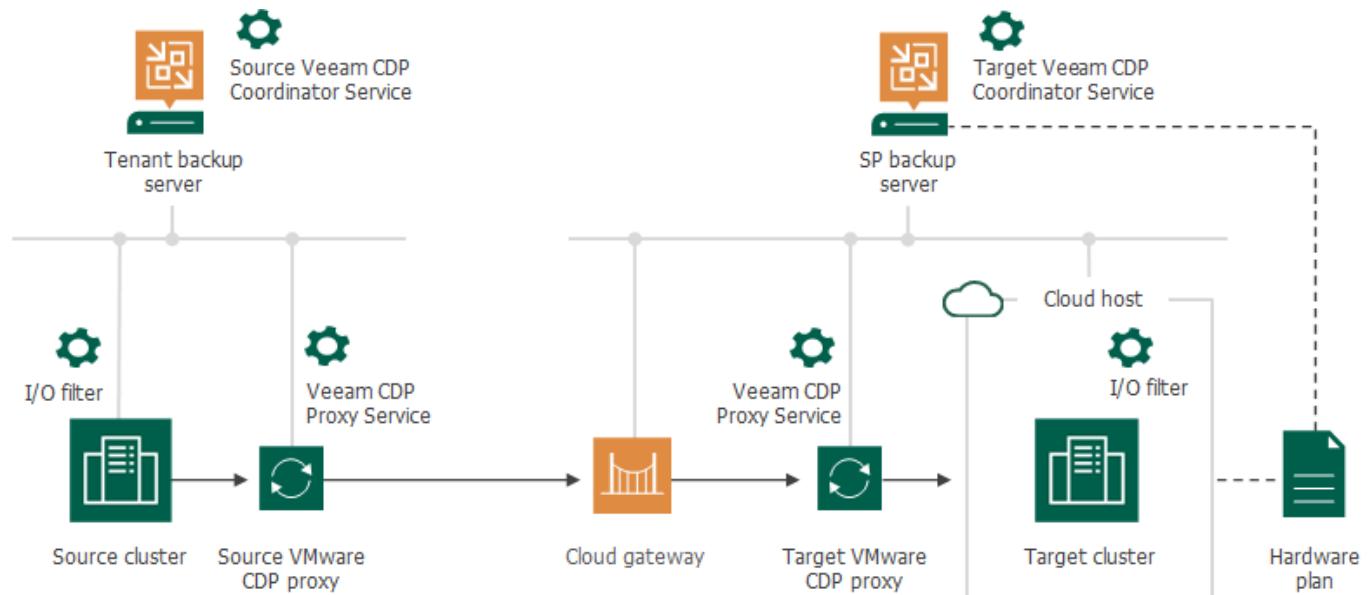
Veeam Cloud Connect offers the following CDP scenarios.

Scenario 1. CDP to VMware vSphere

In this scenario, the SP allocates computing, storage and network resources for tenant CDP replicas on a VMware vSphere cluster and provides them to the tenant through a hardware plan.

The tenant connects to the SP using credentials of the standalone tenant account obtained from the SP. After that, the tenant can create CDP policies targeted at the cloud host. Tenant data will be replicated from the source VMware vSphere host to the cloud host that has VMware vSphere resources as a back end.

This scenario is similar to the regular snapshot-based replication in Veeam Cloud Connect.
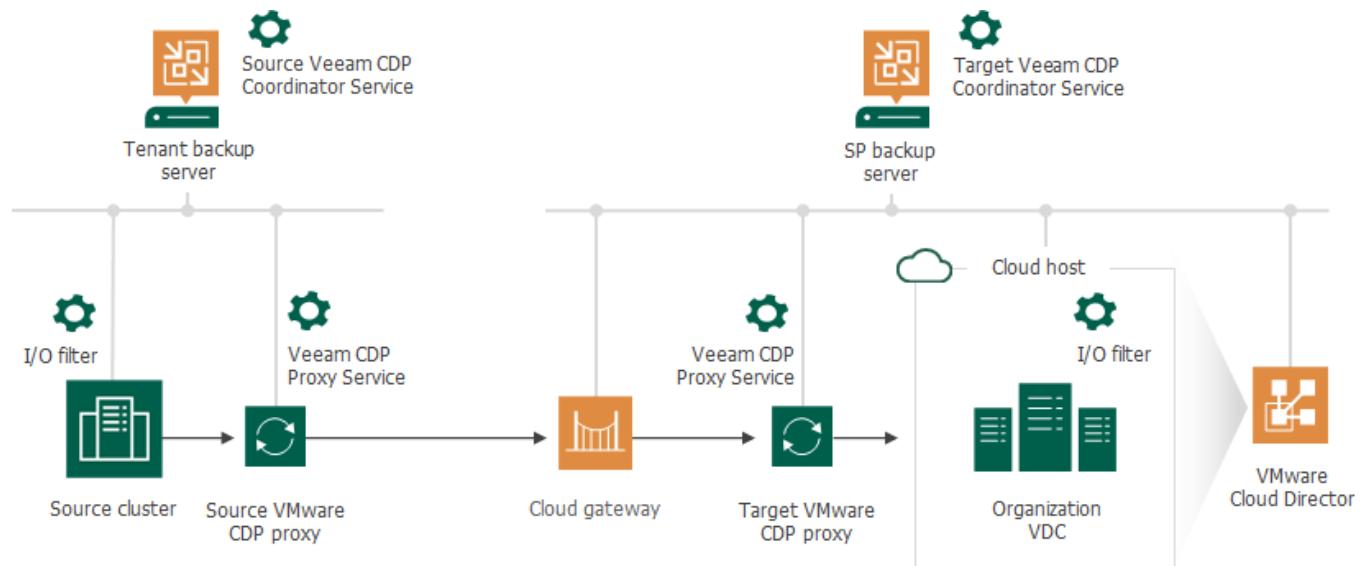
Scenario 2. CDP to VMware Cloud Director

In this scenario, the SP provides replication resources for tenant CDP replicas through organization VDCs configured in VMware Cloud Director.

The tenant connects to the SP using credentials of the VMware Cloud Director tenant account obtained from the SP. After that, the tenant can create CDP policies targeted at the cloud host. Tenant data will be replicated from the source VMware vSphere host to the cloud host that has VMware Cloud Director resources as a back end.

This scenario is similar to Veeam Cloud Connect Replication with VMware Cloud Director.

CDP Infrastructure in Veeam Cloud Connect

The following CDP infrastructure components are required in the Veeam Cloud Connect environment.

Components on the SP side

- SP Veeam backup server

- One or more hardware plans whose resources will be available to tenants as cloud hosts

  Alternatively, if the SP uses VMware Cloud Director in their virtualization environment, they can provide cloud hosts to tenants through organization VDCs.

- One or more target VMware CDP proxies

Components on the tenant side

- Tenant Veeam backup server

- One or more source virtualization hosts

- One or more source VMware CDP proxies

> **NOTE**
>
> This section contains overview of CDP infrastructure components in the Veeam Cloud Connect environment. To get a detailed description of each component, see the Backup Infrastructure for CDP section in the Veeam Backup & Replication User Guide.

SP and Tenant Backup Servers

The backup server is the configuration, administration and management core of the backup infrastructure. The SP and tenant backup servers run the Veeam CDP Coordinator Service:

- The SP backup server runs the source Veeam CDP Coordinator Service.

- The tenant backup server runs the target Veeam CDP Coordinator Service.

The source and target Veeam CDP Coordinator Service communicate with each other through a persistent connection to coordinate replication and data transfer tasks, and control resource allocation.

Source Host

The source host is located on the tenant side and contains production VMs for which the tenant wants to create CDP replicas offsite. The source host must be a part of a VMware vSphere cluster managed by vCenter Server. vCenter Server must be connected to the tenant backup server.

To be able to use the source host for CDP, the tenant must install the I/O filter on the VMware vSphere cluster. To learn more, see I/O Filters.

Tenant VM data from the source host is moved to the cloud host located in the SP Veeam Cloud Connect infrastructure.

Cloud Host

The target host in the Veeam Cloud Connect environment is represented by the cloud host. The cloud host is located on the SP side and contains CDP replicas of tenant VMs. The SP can provide tenants with cloud hosts of the following types:

- Cloud host that uses resources of a VMware vSphere cluster. To provide the tenant with a cloud host of this type, the SP must create a hardware plan. The process of allocating resources for CDP replicas does not differ from the same process for snapshot-based replicas. To learn more, see Hardware Plan.

- Cloud host that uses VMware Cloud Director resources. To provide the tenant with a cloud host of this type, the SP must configure an organization VDC in VMware Cloud Director and grant the tenant access to the VDC through a VMware Cloud Director tenant account. This process does not differ from the same process for snapshot-based replicas. To learn more, see Getting Started with Replication to VMware Cloud Director.

To be able to use the target host for CDP, the SP must install the I/O filter on the VMware vSphere cluster or VMware Cloud Director organization VDC. To learn more, see I/O Filters.

I/O Filters

To be able to use hosts for CDP, the SP and tenant must install I/O filters on the source and target hosts.

- On the SP side, the I/O filter must be installed on the VMware vSphere cluster or VMware Cloud Director organization VDC where replication resources for the tenant are allocated. The installation procedure does not differ from the one in the regular CDP infrastructure. To learn more, see the Installing I/O Filter and Installing I/O Filter on VDCs sections in the Veeam Backup & Replication User Guide.

  After the SP installs the I/O filter on the cluster, Veeam Backup & Replication automatically installs the filter on all hosts added to the cluster. Likewise, after the SP installs the I/O filter on the organization VDC, Veeam Backup & Replication automatically installs the filter on all clusters and hosts that provide resources to this VDC.

- On the tenant side, the I/O filter must be installed on the VMware vSphere cluster where VMs they plan to replicate reside. For details on how to install the filter, see the Installing I/O Filter section in the Veeam Backup & Replication User Guide.

  After the tenant installs the I/O filter on the cluster, Veeam Backup & Replication automatically installs the filter on all hosts added to the cluster.

I/O filters are built on the basis of vSphere API for I/O filtering (VAIO) and perform the following operations:

- Read and process I/O operations in transit between the protected VMs and VM replicas, and their underlining datastores.

- Send and receive data to and from VMware CDP proxies.

- Communicate with the Veeam CDP Coordinator Service on the backup server and notify the service that the backup infrastructure must be reconfigured if any proxy becomes unavailable.

Source and Target VMware CDP Proxies

A VMware CDP proxy is a component that operates as a data mover and transfers data between the source and target hosts. We recommend you to configure at least two VMware CDP proxies: one (source proxy) in the production environment on the tenant side and one (target proxy) in the disaster recovery site on the SP side.

The source and target VMware CDP proxies perform the following tasks:

- The source proxy prepares data for short-term restore points from data received from the source host, compresses and encrypts the data (if encryption is enabled in the network traffic rules). Then sends it to the target proxy.

- The target proxy receives the data, decompresses and decrypts it, and then sends to the target host.

For more information on VMware CDP proxies, their requirements, limitations and deployment, see the VMware CDP Proxy section in the Veeam Backup & Replication User Guide.

Getting Started with CDP

To start using the CDP functionality in the Veeam Cloud Connect environment, the SP and tenant must perform the following tasks.

> **NOTE**
>
> Before you start using the CDP functionality in the Veeam Cloud Connect environment, consider requirements and limitations.

Tasks on SP Side

To let the tenant create CDP replicas on the cloud host, the SP must complete the following steps:

1. Set up the Veeam Cloud Connect infrastructure:

    a. Deploy the SP Veeam backup server.

    b. Set up a TLS certificate.

    c. Deploy one or more cloud gateways or configure a cloud gateway pool.

    d. [For the CDP to VMware vSphere scenario] Allocate VLANs for cloud networking.

    e. [For the CDP to VMware vSphere scenario] Allocate a pool of public IP addresses for full site failover.

    This step is not required if the SP already uses Veeam Backup & Replication to provide cloud services to tenants, and the Veeam Cloud Connect infrastructure is set up on the SP side.

2. Configure replication resources for tenant CDP replicas. This operation differs depending on what resources you want to provide to the tenant as a replication target:

    o [For the CDP to VMware vSphere scenario] If you want to use resources of a VMware vSphere cluster, create a one or more VMware vSphere hardware plans. The process of creating a hardware plan for CDP replicas does not differ from the same process for snapshot-based replicas. For details, see Configuring Hardware Plans.

    o [For the CDP to VMware Cloud Director scenario] If you want to use resources of VMware Cloud Director, create the necessary number of organization VDCs in VMware Cloud Director and add the VMware Cloud Director server to the backup infrastructure on the SP backup server. For details, see Getting Started with Replication to VMware Cloud Director.

3. Deploy the CDP infrastructure components:

    a. Deploy the target VMware CDP proxy. For details, see the see the Adding VMware CDP Proxies section in the Veeam Backup & Replication User Guide.

    b. Install the I/O filter on the VMware vSphere cluster or VMware Cloud Director organization VDC where replication resources are allocated. For details, see the Installing I/O Filter and Installing I/O Filter on VDCs sections in the Veeam Backup & Replication User Guide.

4. Assign replication resources that you configured at the step 2 to a new or existing tenant account.

   o [For the CDP to VMware vSphere scenario] Subscribe as tenant with a standalone tenant account to a hardware plan. For details, see Configuring Standalone Tenant Account.

   o [For the CDP to VMware Cloud Director scenario] In the properties of a VMware Cloud Director tenant account, select an organization VDC that will be used as a cloud host. For details, see Configuring VMware Cloud Director Tenant Account.

   Once the tenant account is created, the SP must pass the account credentials as well as a DNS name or IP address of the cloud gateway to the tenant.

Tasks on Tenant Side

To work with CDP replicas on the cloud host, the tenant must complete the following steps:

1. Set up the Veeam Cloud Connect infrastructure. To learn more, see Deploying Tenant Veeam Backup Server and Connecting Source Virtualization Hosts.

   This step is not required if the Veeam Cloud Connect infrastructure is already configured on the tenant side.

2. Deploy the CDP infrastructure components:

   a. Deploy the source VMware CDP proxy. For details, see the see the Adding VMware CDP Proxies section in the Veeam Backup & Replication User Guide.

   b. Install the I/O filter on the VMware vSphere cluster where source hosts with production VMs reside. For details, see the Installing I/O Filter section in the Veeam Backup & Replication User Guide.

3. Add the SP in the tenant Veeam backup console using credentials of the tenant account obtained from the SP. For details, see Connecting to Service Providers.

   Alternatively, the tenant can rescan the SP. Cloud host provided to the tenant will become available as a cloud host.

   o Cloud hosts that use resources provided to the tenant through a hardware plan are displayed under the **VMware vSphere** > **VMware Cloud Hosts** node of the tenant Veeam backup console.

   o Cloud hosts that use resources provided to the tenant in VMware Cloud Director are displayed under the **VMware Cloud Director** > **VMware Cloud Director Cloud Hosts** node of the tenant Veeam backup console.

4. Create a CDP policy targeted at a cloud host. For details, see Creating CDP Policies.

5. In case one or more VMs in the production site become unavailable, the tenant can perform failover tasks with VM replicas on the cloud host. For details, see Performing Full Site Failover and Performing Partial Site Failover.

Failover and Failback for CDP

In case of software or hardware malfunction on the production site, a tenant can quickly recover a corrupted VM by failing over to its CDP replica in the cloud. When you perform cloud failover, a replicated VM on the cloud host takes over the role of the original VM. A tenant can fail over to the latest state of a replica or to any of its good known restore points.

For CDP replicas, Veeam Cloud Connect offers the same failover scenarios as for regular, snapshot-based replicas:

- *Full site failover* — the whole production site becomes unavailable and all critical VMs that run interdependent applications fail over to their replicas on the cloud host.

- *Partial site failover* — one or several VMs become corrupted and fail over to their replicas on the cloud host.

To learn more, see Cloud Replica Failover and Failback.

VMware Cloud Director Support
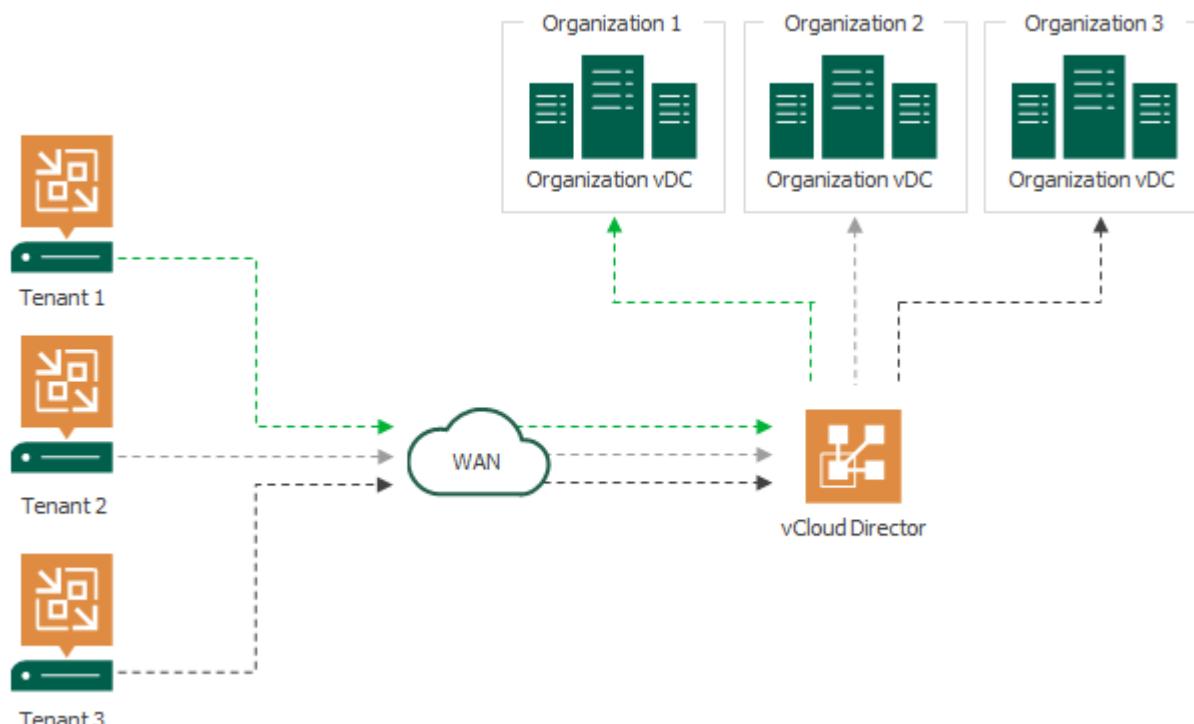
SPs who have VMware Cloud Director deployed in their infrastructure can expose VMware Cloud Director resources as cloud hosts for tenant VM replicas. This allows such SPs to offer Disaster Recovery as a Service (Veeam Cloud Connect Replication) to tenants without the need to deploy additional VMware vSphere hosts in their virtual infrastructure. Whereas SPs who already provide cloud services based on the VMware Cloud Director technology can now offer new data protection and recovery scenario to their tenants.

To support replication of tenant VMs to VMware Cloud Director, Veeam Backup & Replication does not introduce additional Veeam Cloud Connect infrastructure components. The SP does not need to configure cloud replication resources, such as hardware plans, in Veeam Backup & Replication. Instead, the SP configures replication target resources directly in VMware Cloud Director and provides the tenant with access permissions to these resources.

- The SP allocates one or more organization VDCs to an organization in VMware Cloud Director. Each organization VDC provides CPU, RAM, storage and network resources for tenant VM replicas. To grant access to VMware Cloud Director resources to the tenant, the SP creates for this tenant a VMware Cloud Director tenant account. In the properties of this account, the SP selects an organization whose VDC will act as a cloud host for tenant VM replicas. To learn more, see VMware Cloud Director Tenant Account.

- The tenant adds the SP in the Veeam backup console using credentials of the organization administrator account. After the tenant connects to the SP, organization VDCs allocated to the organization appear in the tenant Veeam backup console as cloud hosts. The tenant can configure replication jobs targeted at these cloud hosts and create VM replicas in VMware Cloud Director.

  The tenant can perform the same tasks with VM replicas in VMware Cloud Director as with VM replicas on a regular cloud host provided to the tenant through a hardware plan. To learn more, see Tasks with Cloud Host.

The SP can also use VMware Cloud Director resources as a target location for tenant CDP replicas. To learn more, see Continuous Data Protection (CDP) with Veeam Cloud Connect.

Getting Started with Replication to VMware Cloud Director

The SP and tenant can use VMware Cloud Director resources as a target for snapshot-based replication and CDP. Within the Veeam Cloud Connect Replication to VMware Cloud Director scenario, the SP and tenant perform the following tasks.

Tasks on SP Side

To let the tenant create snapshot-based replicas or CDP replicas on a cloud host that uses VMware Cloud Director resources as a back end, the SP must complete the following steps:

1. Configure replication target resources in VMware Cloud Director:

   a. Create a VMware Cloud Director organization.

   b. Create a user account with administrative rights in the organization. The tenant will use the credentials of this account to connect to the SP. To learn more, see VMware Cloud Director Tenant Account.

   c. Create one or more organization VDCs that will be used as cloud hosts for tenant VM replicas.

   d. Configure an NSX Edge gateway and/or IPsec VPN connection to enable network access to tenant VM replicas.

      An NSX Edge gateway provides network access to VM replicas in VMware Cloud Director after partial site failover and full site failover.

      An IPsec VPN connection may be used to provide network access to tenant VM replicas after partial site failover. Alternatively, the SP can choose to use the network extension appliance for partial site failover.

      To learn more, see Network Resources for VMware Cloud Director Replicas.

   For information about how to perform these tasks, refer to the VMware Cloud Director documentation.

   > **NOTE**
   >
   > The SP must disable VM discovery in VMware Cloud Director that is used to allocate replication resources for tenants.

2. Configure Veeam Cloud Connect infrastructure in Veeam Backup & Replication:

   a. Deploy the SP backup server. For details, see Deploying SP Veeam Backup Server.

   b. Set up a TLS certificate. For details, see Managing TLS Certificates.

   c. Deploy one or more cloud gateways or cloud gateway pools. For details, see Adding Cloud Gateways and Configuring Cloud Gateway Pools.

   d. Add the VMware Cloud Director server to the backup infrastructure on the SP backup server. For details, see the Adding VMware Cloud Director section in the Veeam Backup & Replication User Guide.

   e. Deploy the necessary number of target backup proxies: VMware backup proxies (for snapshot-based replication) or VMware CDP proxies (for CDP). For details, see the Adding VMware Backup Proxies and Adding VMware CDP Proxies sections in the Veeam Backup & Replication User Guide.

f. [For CDP] Install the I/O filter on organization VDCs that will be used as cloud hosts for tenant VM replicas. This operation does not differ from the VMware Cloud Director CDP scenario in the regular Veeam Backup & Replication infrastructure. For details, see the Installing I/O Filter on VDCs section in the Veeam Backup & Replication User Guide.

g. Create VMware Cloud Director tenant account and assign to this tenant account replication resources that use an organization VDC as a back end. For details, see Configuring VMware Cloud Director Tenant Account.

> **NOTE**
>
> Steps a–c are not required if the SP already uses Veeam Backup & Replication to provide cloud services to tenants, and the Veeam Cloud Connect infrastructure is set up on the SP side.

Tasks on Tenant Side

To create snapshot-based replicas or CDP replicas on a cloud host that uses VMware Cloud Director resources as a back end, the tenant must complete the following steps:

1. Set up the Veeam Cloud Connect infrastructure. For details, see Deploying Tenant Veeam Backup Server and Connecting Source Virtualization Hosts.

    This step is not required if the Veeam Cloud Connect infrastructure is already configured on the tenant side.

2. Deploy the necessary number of source backup proxies: VMware backup proxies (for snapshot-based replication) or VMware CDP proxies (for CDP). For details, see the Adding VMware Backup Proxies and Adding VMware CDP Proxies sections in the Veeam Backup & Replication User Guide.

3. [For CDP] Install the I/O filter on the VMware vSphere cluster where tenant VMs reside. This operation does not differ from the CDP scenario in the regular Veeam Backup & Replication infrastructure. For details, see the Installing I/O Filter section in the Veeam Backup & Replication User Guide.

4. Add the SP in the tenant Veeam backup console using credentials of the VMware Cloud Director organization administrator account. For details, see Connecting to Service Providers.

5. Depending on the required RPO, create a replication job or CDP policy targeted at a cloud host that uses an organization VDC as a back end. For details, see Creating Replication Jobs and Creating CDP Policies.

6. In case one or more VMs in the production site become unavailable, the tenant can perform failover tasks with VM replicas on the cloud host. To learn more, see Performing Full Site Failover and Performing Partial Site Failover.

VMware Cloud Director Tenant Account
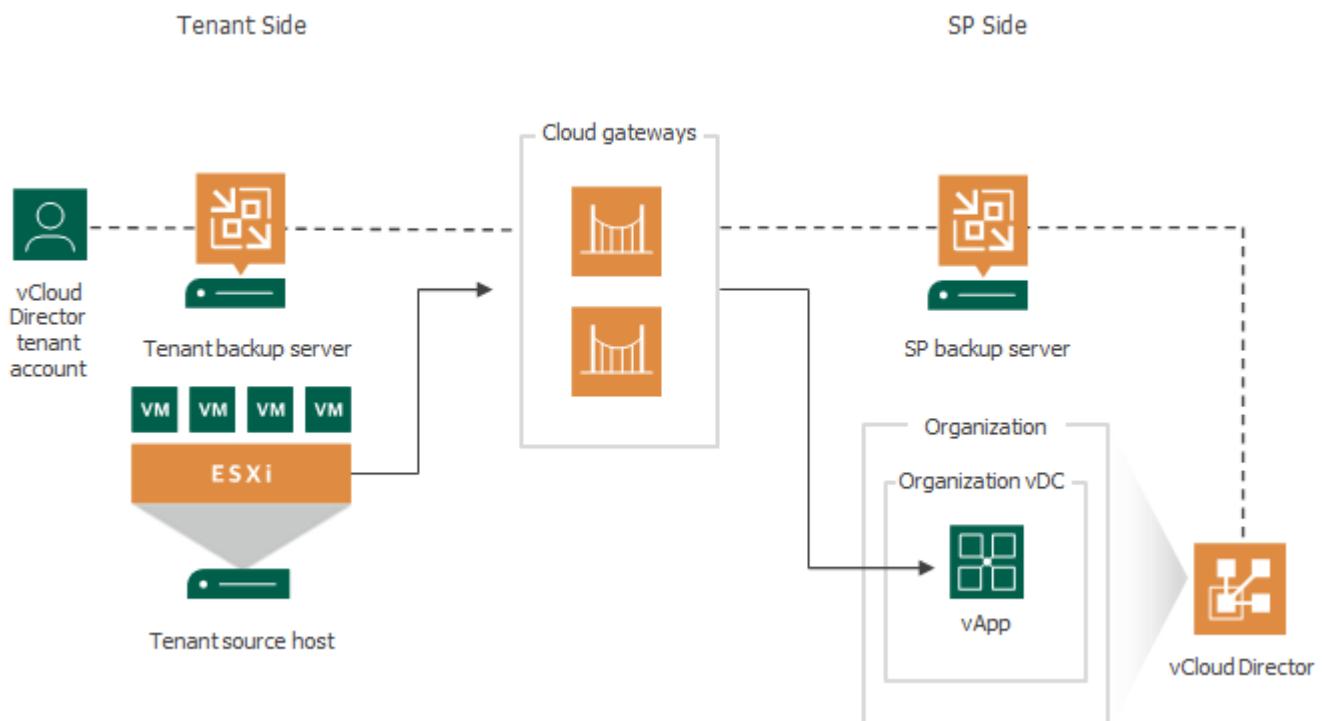
To let the tenant create VM replicas in VMware Cloud Director, the SP must register for this tenant a tenant account of a specific type — a VMware Cloud Director tenant account. When the SP registers a VMware Cloud Director tenant account, the SP permits the tenant to access Cloud Director organization resources from Veeam Backup & Replication. To provide replication resources to an account of this type, in the properties of the account, the SP selects an organization and its organization VDCs that will be available to the tenant as cloud hosts. This contrasts to the similar scenario for a standalone tenant account where replication resources are provided to tenants through hardware plans.

The tenant with a registered VMware Cloud Director tenant account has access to organization VDCs allocated to the organization in Cloud Director. The tenant can use these organization VDCs as cloud hosts for VM replicas. Tenants without VMware Cloud Director accounts cannot create VM replicas on cloud hosts that utilize Cloud Director resources of the SP.

One VMware Cloud Director tenant account can use resources of one VMware Cloud Director organization only. The SP can allocate to the tenant one or more organization VDCs of the same organization.

The tenant with a registered VMware Cloud Director tenant account connects to the SP in the Veeam backup console using credentials of the organization user account that has administrative rights in the organization. The SP must create this user account in advance in the properties of the organization in VMware Cloud Director. The account must have the following permissions:

- General: Administrator Control

- General: Administrator View

- Group / User: View

Cloud Repository for VMware Cloud Director Tenant Accounts

As well as replication resources, the SP can allocate backup resources to a VMware Cloud Director tenant account. For accounts of this type, the Veeam Cloud Connect Backup scenario is the same as for standalone tenant accounts. To learn more, see Veeam Cloud Connect Backup.

Tenants with VMware Cloud Director tenant accounts can create the following types of backups in a cloud repository:

- VM backups.

- Machine backups created by Veeam Agent operating in the standalone mode. To learn more, see Subtenant Accounts for VMware Cloud Director Tenant Accounts.

Subtenant Accounts for VMware Cloud Director Tenant Accounts

The SP can allow users on the tenant side to connect to the SP in Veeam Agent for Microsoft Windows or Veeam Agent for Linux and create Veeam Agent backups in a cloud repository. To do this, the SP must create one or more subtenant accounts for the VMware Cloud Director tenant account.

The process of creating a subtenant account for a VMware Cloud Director tenant account is similar to the same process for a standalone tenant account. The only difference is that the SP selects from organization user accounts configured in VMware Cloud Director instead of creating a new account. To create a subtenant account, the SP can use any organization user account that is not granted administrative rights in the organization.

> **NOTE**
>
> Veeam Backup & Replication does not support creating managed subtenant accounts for a VMware Cloud Director tenant account. Thus, a Cloud Director tenant cannot add Veeam Agent machines to backup policies targeted at the cloud repository.

Network Resources for VMware Cloud Director Replicas

To allow tenant VM replicas created in VMware Cloud Director to communicate to each other after partial site failover or full site failover, the SP must configure the necessary number of networks in the properties of the organization VDC that will be used as a target for tenant VM replicas. The tenant will be able to map source and target networks in the properties of the replication job that creates VM replicas in VMware Cloud Director.

In addition, the SP must provide tenant VM replicas in VMware Cloud Director with network resources that enable access to VM replicas over the network:

- From the production environment on the tenant side after partial site failover. To learn more, see Network Resources for Partial Site Failover.

- From the internet after full site failover. To learn more, see Network Resources for Full Site Failover.

> **NOTE**
>
> Consider the following:
>
> - The process of allocating network resources for VM replicas in VMware Cloud Director differs from the same process for VM replicas created on a cloud host provided to a tenant through a hardware plan. In the regular Veeam Cloud Connect Replication scenario, network resources for tenant VM replicas are provided through VLANs and public IP addresses reserved in the Veeam Cloud Connect infrastructure. For more information, see Veeam Cloud Connect Replication.
> - Veeam Backup & Replication does not map source networks to which production VMs are connected to isolated vApp networks in VMware Cloud Director.

Network Resources for Partial Site Failover

There are three scenarios for enabling communication between production VMs on the tenant source host and VM replicas in VMware Cloud Director after partial site failover:

- *Using the NSX Edge gateway*. In this scenario, the SP deploys the NSX Edge gateway on the SP side and tenant side and configures the NSX edge gateway in VMware Cloud Director. This scenario does not require additional actions in Veeam Backup & Replication.

- *Using an IPsec VPN connection*. In this scenario, the SP configures an IPsec VPN connection between the tenant side and SP side. This operation is performed in VMware Cloud Director. This scenario does not require additional actions in Veeam Backup & Replication.

- *Using network extension appliances*. In this scenario, the SP does not use VMware Cloud Director resources to enable network access to tenant VM replicas. Instead, the SP and tenant deploy network extension appliances on their sides in the similar way as in the regular Veeam Cloud Connect Replication scenario:

    o The SP deploys the SP-side network extension appliance at the process of creating a VMware Cloud Director tenant account. To learn more, see Configuring VMware Cloud Director Tenant Account.

    o The tenant deploys the tenant-side network extension appliance at the process of adding the SP in the Veeam backup console. To learn more, see Connecting to Service Providers.

    For the scenario where production VMs and VM replicas in VMware Cloud Director communicate through network extension appliances after partial site failover, consider the following:

    o To provide network resources to tenant VM replicas, the SP should use isolated organization VDC networks.

    o The **Enable DHCP** option must be disabled for organization VDC networks that will be used by tenant VM replicas. This operation can be performed by the SP or tenant in VMware Cloud Director.

    o In case Veeam Backup & Replication fails to detect a static IP address of a tenant VM during the replication process, the SP or tenant must manually specify the IP address for the replica of this VM in VMware Cloud Director. In particular, Veeam Backup & Replication cannot detect an IP address of a Linux VM.

    o During partial-site failover, the SP network extension appliance imports in its vApp all organization VDC networks and connects to these networks. This allows the appliance to provide network connection to VM replicas that reside in other vApps of the organization VDC used as a cloud host, including those replicas for which the failover operation can be started later.

    Keep in mind that if the number of organization VDC networks is greater than 9, the failover operation will fail because the number of virtual network adapters for a VMware vSphere VM cannot exceed 10 (one network adapter is used to connect to the management network).

Network Resources for Full Site Failover

To allow tenant VM replicas in VMware Cloud Director to be accessed over the internet, the SP must configure an NSX Edge gateway in VMware Cloud Director.

To assign public IP addresses to tenant VM replicas after full site failover, the SP can create SNAT and DNAT rules on the NSX Edge gateway. Alternatively, the SP can assign public IP addresses to tenant VM replicas using pre-failover and/or post-failover scripts. To do this, the SP must create the scripts in advance and specify these scripts in the cloud failover plan settings.

> **NOTE**
>
> In contrast to the regular Veeam Cloud Connect Replication scenario, the SP cannot use network extension appliances to enable access to VM replicas in VMware Cloud Director after full site failover.

Partial Site Failover for VMware Cloud Director Replicas

If one or more tenant VMs become corrupted, but the rest of the production site, including the most critical VMs and Veeam Backup & Replication infrastructure, remain operative, the tenant can perform partial site failover. With partial site failover, the tenant can quickly recover a corrupted VM by failing over to its replica on the cloud host.

To establish a secure connection and enable communication between production VMs and VM replicas in VMware Cloud Director after partial site failover, the SP can use capabilities of VMware Cloud Director or Veeam Backup & Replication. To learn more, see Network Resources for VMware Cloud Director Replicas.

Partial site failover for VM replicas created in an organization VDC is performed in the similar way as partial site failover for VM replicas created on a cloud host provided through a hardware plan. The difference is that Veeam Backup & Replication does not start network extension appliances on the SP and tenant sides if network connectivity for tenant VM replicas is provided using an NSX Edge gateway or IPsec VPN connection.

Veeam Backup & Replication performs partial site failover for a VM replica created in VMware Cloud Director in the following way:
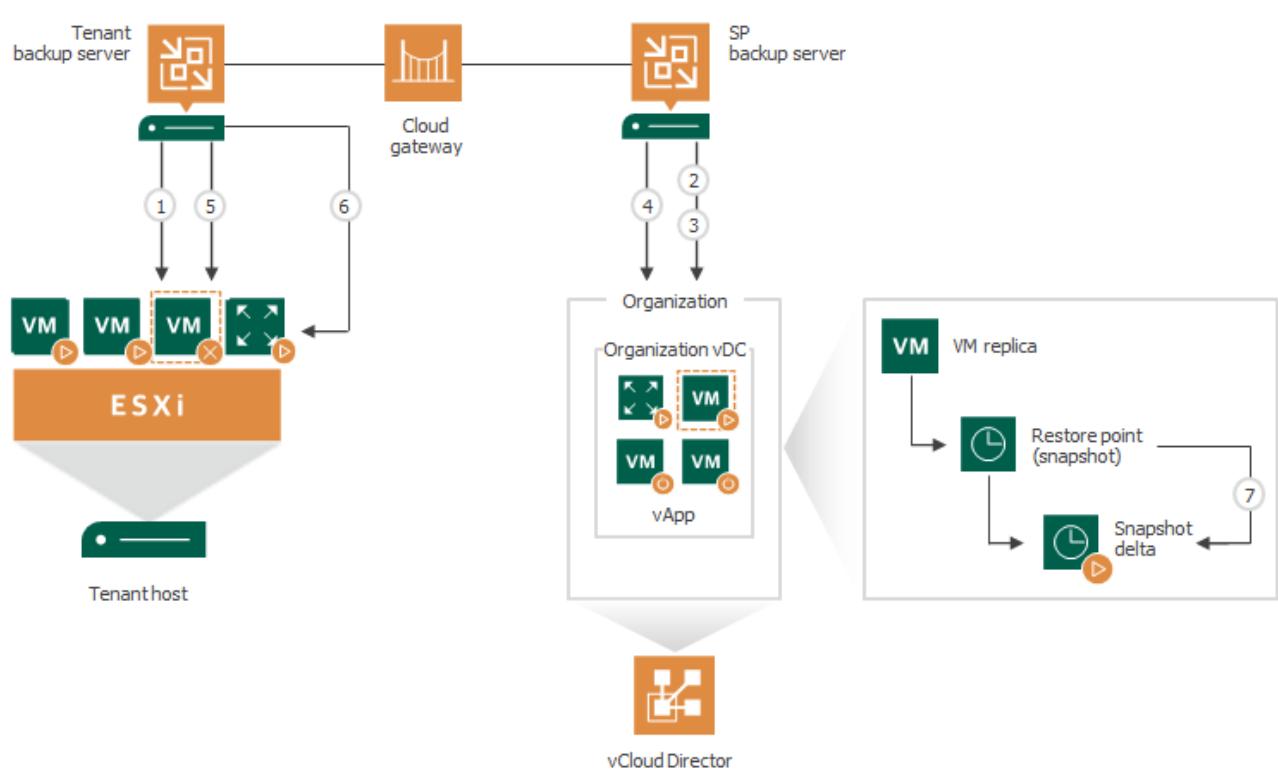
1. The tenant starts the partial site failover process for a VM in the tenant Veeam Backup & Replication console.

2. Veeam Backup & Replication rolls back the VM replica on the cloud host to the required restore point. To do this, it reverts the VM replica to the necessary snapshot in the replica chain.

3. Veeam Backup & Replication powers on the VM replica. The state of the VM replica is changed from *Normal* to *Failover*. If the original VM still exists and is running, the original VM remains powered on.

4. [Optional] If the SP network extension appliance was deployed in the organization VDC that acts as a cloud host, Veeam Backup & Replication powers on the network extension appliance VM in the organization VDC and configures network settings on the appliance:

    o Starts a VPN server on the network extension appliance to establish a secure VPN tunnel through the cloud gateway to the appliance on the tenant side.

    o Configures Proxy ARP daemon on the appliance so that the appliance can receive from the VM replica ARP requests addressed to production VMs on the source host and send them to the tenant's network extension appliance through the VPN tunnel.

    In addition, the SP network extension appliance imports in its vApp all organization VDC networks and connects to these networks. Keep in mind that if the number of organization VDC networks is greater than 9, the failover operation will fail because the number of virtual network adapters for a VMware vSphere VM cannot exceed 10 (one network adapter is used to connect to the management network).

5. Veeam Backup & Replication temporarily puts replication activities for the original VM on hold (until the VM replica returns to the *Normal* state).

6. [Optional] If the tenant network extension appliance was deployed on the source host, Veeam Backup & Replication powers on the network extension appliance on the tenant side and configures network settings on the appliance:

   o Starts a VPN client on the network extension appliance and connects to the VPN server on the network extension appliance on the SP side to establish a secure VPN tunnel through the cloud gateway.

   o Configures Proxy ARP daemon on the network extension appliance so that it can receive ARP requests from production VMs addressed to the VM replica and send them to the network extension appliance on the SP side through the VPN tunnel.

7. All changes made to the VM replica while it is running in the *Failover* state are written to the delta file of the snapshot, or restore point, to which you have selected to roll back.

After the partial site failover operation completes, VMs on the tenant side communicate to the VM replica on the cloud host.

Full Site Failover for VMware Cloud Director Replicas
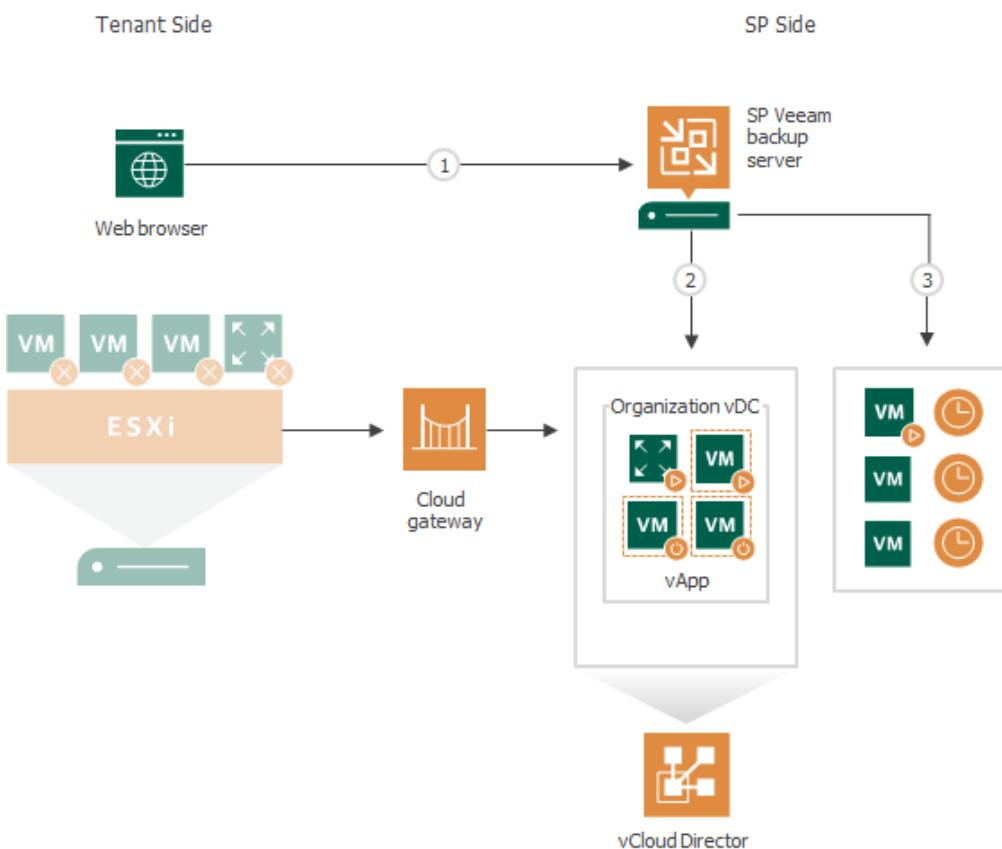
When the whole tenant production site becomes unavailable because of a software or hardware malfunction, the tenant can perform full site failover. In the full site failover scenario, all critical VMs fail over to their replicas on the cloud host one by one, as a group.

Full site failover for tenant VM replicas in VMware Cloud Director is in many regards similar to full site failover for VM replicas created on a cloud host provided through a hardware plan. To perform full site failover to VM replicas in VMware Cloud Director, the tenant must create a cloud failover plan of a specific type — a VMware Cloud Director failover plan. To learn more, see Creating Cloud Failover Plans for VMware Cloud Director Replicas.

In contrast to the regular full site failover process, full site failover to VM replicas in VMware Cloud Director does not involve usage of the SP network extension appliance. To allow tenant VM replicas to be accessed over the internet, the SP must configure an NSX Edge gateway in VMware Cloud Director. This operation must be performed in advance, before the tenant or SP starts the full site failover operation.

Full site failover is performed in the following way:

1. The tenant starts a cloud failover plan using Veeam Cloud Connect portal (or asks the SP to start full site failover using the SP Veeam Backup & Replication console).

2. For each VM in the cloud failover plan, Veeam Backup & Replication detects its replica. If some VMs in the cloud failover plan have replicas that are already in the *Failover* or *Failback* state, Veeam Backup & Replication suggests that they are processed with the cloud failover plan.

3. The replica VMs are started in the order they appear in the cloud failover plan within the set time intervals.

TLS Certificates

Communication between components in the Veeam Cloud Connect infrastructure is carried out over a TLS connection secured with a TLS certificate. The TLS certificate is used for verification of trust. It helps the SP and tenants identify themselves and make sure that parties taking part in data transfer are really the ones that they claim to be.

Veeam Backup & Replication does not use TLS certificates to encrypt data traffic in the Veeam Cloud Connect infrastructure. For data encryption, Veeam Backup & Replication uses the same encryption methods and algorithms as in a regular backup infrastructure.

Types of TLS Certificates

Veeam Backup & Replication can work with the following types of TLS certificates:

- **TLS certificate verified by a Certificate Authority (CA)**. If the SP already has a TLS certificate verified by a CA, the SP can import this TLS certificate and use it to establish a secure connection between Veeam Cloud Connect infrastructure components.

- **Self-signed certificates**. If the SP does not have a TLS certificate verified by a CA, the SP can generate a self-signed TLS certificate with Veeam Backup & Replication. For TLS certificate generation, Veeam Backup & Replication employs the RSA Full cryptographic service provider by Microsoft Windows installed on the Veeam backup server.

  The SP can also generate a self-signed certificate with any third-party solution and import it to Veeam Backup & Replication.

> **NOTE**
>
> Consider the following:
>
> - For communication between the SP and tenants, Veeam Backup & Replication uses a separate TLS certificate from a certificate used for connection between the Veeam backup server and backup infrastructure components. Requirements for the Veeam backup server certificate do not apply to certificates in the Veeam Cloud Connect infrastructure. The SP can use a certificate issued by a third-party CA and intended for usage on a web server.
> - For more information on how to sign a certificate that the SP plans to use in the Veeam Cloud Connect infrastructure, see this web page.
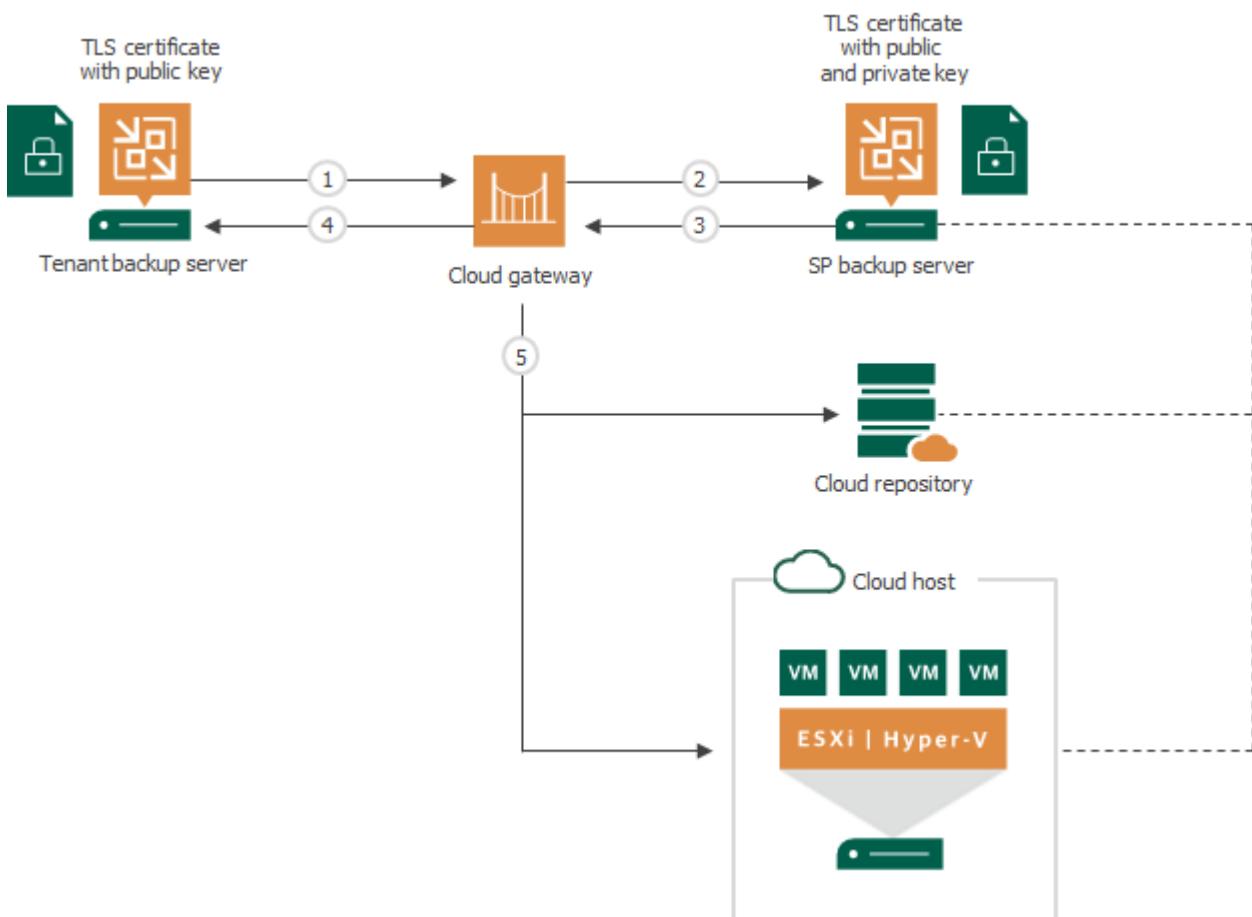
TLS Certificates Handshake

TLS certificates are installed on the following components in the Veeam Cloud Connect infrastructure:

- The TLS certificate with a public key and private key is installed on the SP Veeam backup server. The tenant account under which the Veeam Cloud Connect Service runs must have permissions to access this TLS certificate.

- The TLS certificate with a public key is installed on all tenants' Veeam backup servers (in case of self-signed certificates).

When the tenant starts a job or task targeted at the cloud repository or the cloud host, the parties perform a TLS handshake to authenticate themselves:

1. To connect to Veeam Cloud Connect resources (cloud repository and/or cloud host), the Veeam backup server on the tenant side sends a request to the cloud gateway.

2. The cloud gateway passes this request to the SP Veeam backup server.

3. The SP Veeam backup server exposes a TLS certificate installed on it to tenant Veeam backup server through the cloud gateway.

4. Tenant Veeam backup server checks if the exposed TLS certificate is trusted or matches the TLS certificate saved in the Veeam Backup & Replication database.

5. The SP Veeam backup server establishes a secure communication channel in the Veeam Cloud Connect infrastructure, and VM data from tenant's side is transported to the cloud repository or cloud host.

Veeam Backup & Replication supports both wildcard certificates and certificates that have multiple FQDNs listed in the *Subject* or *Subject Alternative Name* field.

If you use a wildcard certificate (like *.*domain.com*), cloud gateways having DNS names that do not include .*domain.com* will not be trusted, and Veeam Backup & Replication will not use these cloud gateways for communication with the cloud repository.

TLS Certificate Thumbprint Verification

When the tenant adds a SP to the Veeam Backup & Replication console, Veeam Backup & Replication retrieves the TLS certificate with a public key from the SP Veeam backup server and saves it to the database with which tenant Veeam backup server communicates.

To make sure that the obtained TLS certificate is really the TLS certificate used by the SP, tenants can verify the TLS certificate with a thumbprint. Verification with the thumbprint helps tenants protect against the "man-in-the middle" attack when the eavesdropper provides a false TLS certificate to tenants and makes tenants believe that they communicate directly with the SP.

To enable thumbprint verification, the SP must pass the TLS certificate thumbprint to the tenant over a secure channel, for example, by email. When the tenant adds the SP, Veeam Backup & Replication offers the tenant to enter the TLS certificate thumbprint to verify if this TLS certificate is the original SP certificate.

Rights and Permissions to Access TLS Certificates

The Windows account under which the Veeam Cloud Connect Service on the SP Veeam backup server runs must have the following permissions:

1. The Windows account must have access to the private key in the non-interactive mode (without having to enter a password).

2. The Windows account must have access to the TLS certificate store folder where the private key is kept and must have read rights for this folder. To learn more about key directories and files, see Microsoft Docs.

   A self-signed TLS certificate generated with Veeam Backup & Replication is placed to the *Shared* certificate store. The following Windows accounts have access to this certificate:

   o User who created the TLS certificate

   o LocalSystem Windows account

   o Local Administrators group

3. The Windows account must have access to the TLS certificate itself (stored in the registry) and permissions on corresponding registry folders.

   A self-signed TLS certificate generated with Veeam Backup & Replication is placed to *Local Machine|Trusted Root* and *Local Machine|My* registry folders. These folders do not contain any private information and all users have access to these folders by default.

Tenant Lease and Quota

To let the tenant work with the cloud repository and/or the cloud host, the SP must create a tenant account. When the SP configures a tenant account, the SP assigns quota and, optionally, lease settings for the tenant. Lease and quota settings help the SP control how tenants consume storage resources on the cloud repository.

Quota

Veeam Cloud Connect Backup

For Veeam Cloud Connect Backup, quota is the amount of space assigned to one tenant on one cloud repository. It is a chunk of storage resources that the tenant can consume for storing backups on the cloud repository. The SP can assign quotas on different cloud repositories to one tenant.

> **NOTE**
>
> To allow tenants to use all backup scenarios available in Veeam Backup & Replication, the SP should consider assigning the sufficient storage quota to the tenant. For example, for the compact full backup file operation, the storage quota must have enough space to store a file of the full backup size in addition to the existing backup chain. To create active full and synthetic full backups, additional space for creating full backup files on the cloud repository is required as well.

Veeam Backup & Replication tracks quota consumption and updates information about the amount of free and used space within the tenant quota on the cloud repository. This information is updated automatically when the following actions are performed in Veeam Backup & Replication:

- A VM backup job, Veeam Agent backup job or backup copy job targeted at the cloud repository runs on the tenant Veeam backup server.

- The tenant performs a file copy operation with a file stored on the cloud repository using the **Files** view in Veeam Backup & Replication.

- Veeam Agent performs a backup job targeted at the cloud repository.

> **NOTE**
>
> Veeam Backup & Replication does not track operations with files stored on the cloud repository that are performed from outside of the product. Information on quota usage cannot be updated by rescanning the cloud repository after such changes.

A tenant can share their quota with subtenants — tenant-side users who back up data stored on physical devices. To learn more, see Subtenant Quota.

Veeam Cloud Connect Replication

For Veeam Cloud Connect Replication, quota is the amount of CPU, RAM and storage space in the SP virtualization environment provided to one tenant through a hardware plan. It is a chunk of compute and storage resources that the tenant can consume for creating and processing VM replicas on the cloud host. The SP can assign quotas on different cloud hosts to one tenant by subscribing a tenant to several hardware plans.

Storage quota size is specified in GB or TB (GB is considered as 2^30 bytes, and TB is considered as 2^40 bytes). CPU and RAM limits are specified in GHz and GB.

A quota can be valid for indefinite time or can be restricted in time. To limit the quota lifetime, the SP must set a lease for the tenant.

Lease

Lease is a period of time for which the tenant has access to tenant's quotas on the cloud repository and cloud host. The lease settings help the SP restrict for how long tenants should be able to work with cloud resources.

Lease settings apply to all quotas assigned to the tenant. The SP can specify the lease period for the tenant or create a tenant account without a lease.

- If lease settings are specified, the tenant has access to backup and replication resources in the cloud until the lease period expires. When the lease period expires, the tenant cannot perform backup, backup copy and replication tasks, restore and copy VM data from the cloud repository or cloud host.

- If lease settings are not specified, the tenant can work with cloud resources for an indefinite period of time.

Subtenants

Veeam Backup & Replication supports creating Veeam Agent backups on the cloud repository. Tenants can back up to the cloud not only their VM data but also data stored on physical devices — servers, desktops, laptops, and so on. To let the tenant provide different Veeam Agent users with access to the cloud repository, Veeam Backup & Replication offers the concept of *subtenants*.

In terms of Veeam Backup & Replication, a subtenant is a user on the tenant side who connects to the SP on their own account and uses their own individual quota on the cloud repository. To learn more, see Subtenant Account and Subtenant Quota.

> **NOTE**
>
> Mind the following:
>
> - End users on the tenant side can use subtenant accounts only to connect to the SP in Veeam Agent for Microsoft Windows and Veeam Agent for Linux. The tenant cannot use credentials of a subtenant account to add a SP in the Veeam backup console.
> - Veeam Agent users on the tenant side can connect to the SP and create backups on the cloud repository under the tenant account. However, it is recommended to provide every user with a separate subtenant account. In this case, the tenant or SP can allocate storage resources on the cloud repository individually for every subtenant so that subtenants' data is stored in the cloud in an isolated and segregated way.
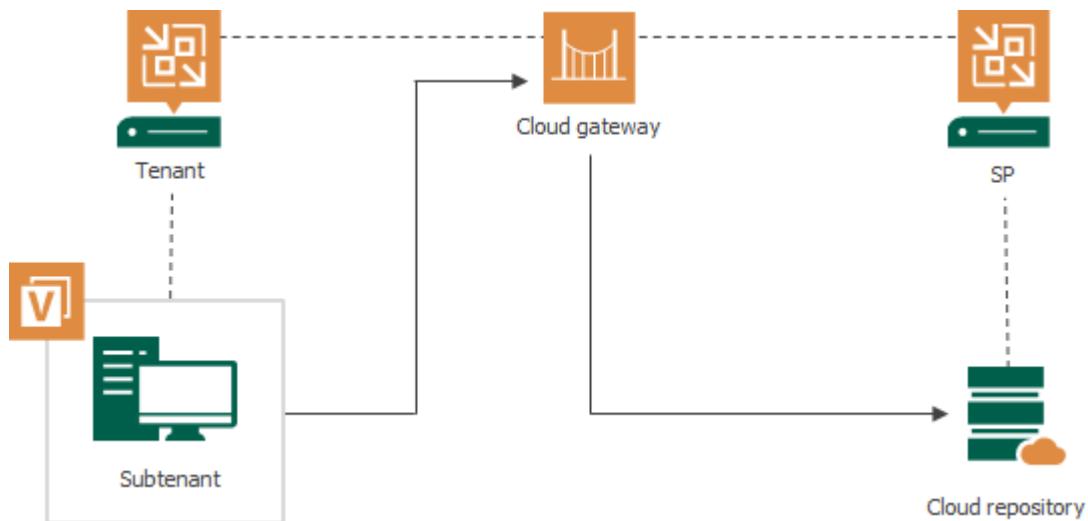
Communication between the subtenant and the SP is carried out in the similar way as between the tenant and the SP. The subtenant connects to the SP, configures a backup job targeted at the cloud repository and transmits backed-up data to the SP side. The difference is that the data is transmitted to the cloud repository from the Veeam Agent computer, and not from a VM on a tenant virtualization host.

The tenant can view properties of Veeam Agent backups created by subtenants on the cloud repository and delete such backups from the cloud repository. To recover data from Veeam Agent backups, the tenant can perform the following operations:

- Export computer disks as virtual disks

- Restore guest OS files

> **TIP**
>
> In the scenario where the SP and tenant have access to the same Microsoft Active Directory infrastructure, the SP can also provide Veeam Agent users with access to a cloud repository through Active Directory tenant accounts. To learn more, see Active Directory Tenant Account.

Subtenant Account

To work with the cloud repository, a subtenant uses the subtenant account. Veeam Backup & Replication offers two types of subtenant accounts:

- Standalone subtenant account — accounts of this type are used to back up data to the cloud repository with Veeam Agent operating in the standalone mode.

- Managed subtenant account — accounts of this type are used in the Veeam Agent management scenario.

> **NOTE**
>
> In the scenario where the SP and tenant belong to the same organization that has Microsoft Active Directory deployed, the SP can allow AD users to create Veeam Agent backups in a cloud repository. To do this, the SP must configure Active Directory tenant accounts instead of subtenant accounts. Veeam Agent users will be able to connect to the SP using credentials of their accounts in AD without the need to remember additional credentials.
>
> To learn more, see Active Directory Tenant Account.

Standalone Subtenant Account

In the scenario where users on the tenant side back up data to the cloud repository with Veeam Agent operating in the standalone mode, the tenant or SP must create subtenant accounts. The number of subtenant accounts created per tenant is not limited in Veeam Backup & Replication.

Typically, the tenant is the party responsible for creating and managing subtenant accounts. However, the SP can perform the same operations with subtenant accounts as the tenant. This allows the SP to create, edit or delete subtenant accounts upon tenant requests, for example, if the tenant has no access to the Veeam Backup & Replication console.

Veeam Backup & Replication saves information about subtenant accounts in the Veeam Backup & Replication database. Every time the tenant or SP performs an operation with the subtenant account, Veeam Backup & Replication updates the subtenant data and replicates this data between the tenant side and SP side.

Managed Subtenant Account

In the Veeam Agent management scenario where Veeam Agent is deployed and managed remotely from Veeam Backup & Replication, the tenant or SP does not need to create subtenant accounts to back up Veeam Agent machines to the cloud repository. In this scenario, Veeam Backup & Replication creates subtenant accounts automatically. Such accounts are considered as managed subtenant accounts.

Veeam Backup & Replication creates a managed subtenant account for each machine added to a backup policy. A machine uses this account to connect to the SP during the backup process.

Veeam Backup & Replication automatically generates names, passwords and descriptions for managed subtenant accounts. In contrast to standalone subtenant accounts, passwords for managed subtenant accounts are saved in the Veeam backup database on the tenant backup server only. Passwords for managed subtenant accounts are not passed to the SP side.

The tenant or SP can manually edit a managed subtenant account, if necessary. The following operations are available:

- Change the password for the subtenant account. This operation is required if you want to perform bare-metal recovery from a Veeam Agent backup created by a backup policy in a cloud repository. Keep in mind that this operation is available only for the tenant in the tenant Veeam backup console. The SP cannot change the password for a managed subtenant account.

- Limit subtenant quota. By default, Veeam Backup & Replication creates managed subtenant accounts with unlimited subtenant quota. The tenant or SP can limit storage quotas individually for each created subtenant account.

- Disable and enable the subtenant account. By default, Veeam Backup & Replication creates managed subtenant accounts in the enabled state. After you disable a managed subtenant account, Veeam Agent managed by Veeam Backup & Replication will not be able to connect to the SP and back up data to the cloud repository.

- Specify a custom description for the managed subtenant account instead of the default description generated by Veeam Backup & Replication.

To learn more about Veeam Cloud Connect support for Veeam Agent managed by Veeam Backup & Replication, see the Backup to Veeam Cloud Connect Repository section in the Veeam Agent Management Guide.

Subtenant Quota

When the tenant or SP creates a subtenant account, they provide to the created account a subtenant quota. A subtenant quota is an amount of storage space within the tenant quota on the cloud repository. The subtenant can consume storage resources provided through the subtenant quota for storing Veeam Agent backups on the cloud repository.
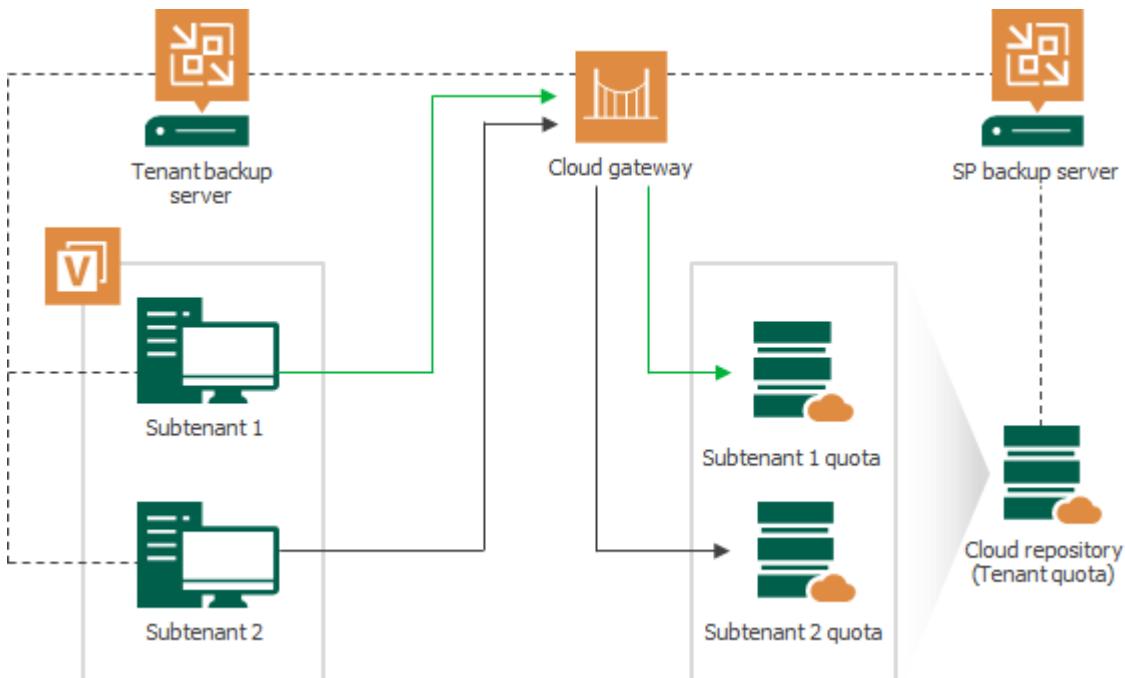
The tenant or SP can allocate only one quota on one cloud repository for each subtenant account. If the tenant or SP wants to provide to a user multiple quotas on the same or different cloud repositories, they must create different subtenant accounts for this user.

The tenant or SP can specify the size of the subtenant quota or create unlimited subtenant quota. With unlimited subtenant quota, subtenant can use all storage space within the tenant quota on the cloud repository. In this case, the tenant should monitor tenant quota consumption to make sure that the amount of free space on the cloud repository is sufficient for storing backups created by this tenant and its subtenants.

> **NOTE**
>
> For managed subtenant accounts, consider the following:
>
> * By default, Veeam Backup & Replication creates managed subtenant accounts with unlimited subtenant quota. The tenant or SP can edit the necessary subtenant account and specify the desired subtenant quota limit for the account.
> * Managed subtenant accounts support multiple subtenant quotas. This allows Veeam Backup & Replication to use the same subtenant account to back up the same machine with multiple Veeam Agent backup jobs targeted at different cloud repositories.

Data Encryption and Throttling

Data Encryption

By default, Veeam Backup & Replication encrypts data traffic going to and from the cloud repository. Additionally, tenants can encrypt backups created with backup jobs and backup copy jobs. To do this, tenants must enable the data encryption option in the job properties.

Network Traffic Throttling

The SP can select to throttle traffic going to and from the SP Veeam Cloud Connect infrastructure. Data throttling rules are specified in the same manner as for regular backup infrastructure components.

By default, the Veeam backup server shares available bandwidth equally between all tenants who work with cloud backup and replication resources simultaneously. The bandwidth available to one tenant is equally split between all tasks performed by this tenant.

For example, the cloud repository is used by two tenants simultaneously:

- *Tenant 1* runs 2 tasks, backup and restore.

- *Tenant 2* runs 1 task.

In this situation, *Tenant 1* will get 50% of bandwidth and this bandwidth will be equally split between 2 tasks: 25% of the initial bandwidth per task. The task performed by *Tenant 2* will get 50% of the initial bandwidth.

To adjust network bandwidth consumption individually for each tenant, the SP can specify the bandwidth limit when assigning cloud backup and replication resources to a tenant. In this case, tenant's backup and replication jobs will split the specified bandwidth regardless bandwidth consumption by other tenants.

Parallel Data Processing

Veeam Cloud Connect supports parallel data processing. The SP can specify the maximum number of concurrent tasks that can be performed within tenant jobs targeted at the cloud repository and cloud host. Task limitation settings are specified individually for each tenant at the process of the tenant account registration. To learn more, see Specify Bandwidth Settings.

When multiple concurrent tasks are allowed for the tenant, the tenant can process in parallel the specified number of VMs and/or VM disks within a single backup or replication job targeted at the cloud repository or cloud host. Parallel data processing also lets the tenant perform multiple jobs targeted at the cloud simultaneously.

> **NOTE**
>
> For backup copy jobs targeted at the cloud repository, Veeam Backup & Replication allows to process multiple jobs or multiple VMs in the job in parallel. VM disks are always processed subsequently, one by one.

The maximum number of concurrent tasks specified for a tenant should not exceed the maximum number of concurrent tasks specified for backup proxies and backup repositories deployed by the SP as a part of the Veeam Cloud Connect infrastructure. Ignoring this rule can lead to overload of backup infrastructure components that take part in processing tenant data.

For example, the tenant has included 1 VM with 4 disks into a backup job targeted at the cloud repository. On the SP side, the following task limitation settings are specified:

- The tenant can process 4 concurrent tasks.

- The cloud repository can process 2 concurrent tasks.

In this situation, Veeam Backup & Replication on the tenant backup server will start 4 concurrent tasks. Limitation for the allowed number of concurrent tasks set for the cloud repository will be ignored.

Resource limitation settings for backup proxies and backup repositories deployed as a part of the Veeam Cloud Connect infrastructure are specified in the same manner as for regular backup infrastructure components. To learn more, refer to the Veeam Backup & Replication User Guide.

> **NOTE**
>
> Veeam Backup & Replication does not apply I/O control settings specified in the general product settings to tenant tasks in the Veeam Cloud Connect scenarios. To control consumption of the SP Veeam Cloud Connect infrastructure resources by tenants, the SP uses parallel data processing and network traffic throttling settings.

Remote Connection to Tenant Backup Server

The SP can use the Veeam Backup & Replication console to connect to the tenant backup server. This may be helpful, for example, if the tenant encounters a problem with managing its backup infrastructure and asks the SP to change settings in Veeam Backup & Replication deployed on the tenant side. The remote connection functionality allows the SP to manage tenant backup servers without the need to configure additional network connections, thus reducing security risks and network management overhead.

The remote connection functionality is available to the SP and tenant if the following conditions are met:

- The tenant connected to the SP using credentials of a standalone tenant account.

  Remote connection to a backup server of a tenant with a VMware Cloud Director tenant account is not supported. To overcome this limitation, the SP can create a separate standalone account for this tenant, and the tenant can connect to the SP using credentials of this account.

  The remote connection functionality is not available to Active Directory tenants as well, because such tenants do not have a tenant backup server and can use their tenant account to connect to the SP in Veeam Agent only.

- The tenant enabled the **Allow this Veeam Backup & Replication installation to be managed by the service provider** option at the process of connecting to the SP. To learn more, see Specify Cloud Gateway Settings.

Veeam Backup & Replication offers two types of connection to the tenant backup server:

- With the Remote Access Console — in this case, the SP can log on to the tenant backup server and perform the required operations in Veeam Backup & Replication. For example, the SP can use the Remote Access Console to change configuration options in Veeam Backup & Replication, run jobs or perform available restore tasks.

- With the Remote Desktop Connection client — in this case, the SP can launch a remote session over the RDP protocol and log on to the Microsoft Windows OS running on the tenant backup server.

To establish and keep remote connections between the tenant backup server and Veeam Cloud Connect infrastructure components on the SP side, Veeam Backup & Replication uses *network redirectors*. Network redirectors communicate through the cloud gateway allowing Veeam Backup & Replication components deployed on the SP side to access the tenant backup server. To learn more, see Network Redirectors.

Network Redirectors

To open and keep a communication channel between the tenant backup server and SP backup infrastructure, Veeam Backup & Replication uses *network redirectors*. Network redirectors route requests between Veeam Backup & Replication components of the two parties allowing Veeam Backup & Replication to pass commands from the SP side to the tenant side. As a result, the SP can remotely access the tenant backup server and perform data protection and disaster recovery tasks in Veeam Backup & Replication deployed on the tenant side.

Technically, a network redirector is an executable file residing in the Veeam Backup & Replication installation folder. A network redirector is deployed on every Veeam backup server or dedicated machine on which you install the Veeam Backup & Replication console. However, Veeam Backup & Replication uses network redirectors only on those machines that take part in establishing a remote connection to the tenant backup server.

Depending on what Veeam Backup & Replication component is deployed on the machine, a network redirector can perform one of the following roles:

- *Cloud network redirector* — a network redirector that runs on the SP backup server (a backup server on which the Veeam Cloud Connect license is installed). Cloud network redirector accepts connections from Tenant network redirectors and Remote Access Console and routes requests between these components.

- *Tenant network redirector* — a network redirector that runs on the tenant backup server. The Veeam Backup Service running on the tenant backup server starts this network redirector when the tenant enables the **Allow this Veeam Backup & Replication installation to be managed by the service provider** option in the **Service Provider** wizard. Tenant network redirector opens a control connection to the cloud network redirector and runs in the background enabling remote access to the tenant backup server from the SP side.

- *Remote network redirector* — a network redirector that runs on the machine where Remote Access Console is installed (the SP backup server of a dedicated machine). Veeam Backup & Replication uses this network redirector only to open a remote desktop session to the tenant backup server. The Remote Access Console starts the Remote network redirector when the SP selects the tenant in the *Open Remote Access Console* window. After the SP closes the Remote Access Console, Veeam Backup & Replication stops the Remote network redirector, too.

Veeam Backup & Replication components involved in remote connection scenarios communicate differently depending on the type of connection to the tenant backup server — with the Remote Access Console or over the Remote Desktop Protocol. To learn more, see How Remote Access Console Works and How Remote Desktop Connection to Tenant Works.

Remote Access Console

The Remote Access Console is a Veeam Cloud Connect infrastructure component that provides access to the tenant backup server. With the Remote Access Console, the SP can connect to the tenant backup server, log on to Veeam Backup & Replication deployed on the tenant side and perform required data protection, disaster recovery or administration tasks.

The Remote Access Console is in many ways similar to the regular Veeam Backup & Replication console: it is a client-side component that communicates to the backup server. However, the Remote Access Console does not connect directly to the tenant backup server. Instead, it communicates to the Veeam Backup Service and Cloud network redirector running on the SP backup server. Veeam Backup & Replication passes commands from the Remote Access Console to the tenant backup server through network redirectors. To learn more, see How Remote Access Console Works.

> **NOTE**
>
> For more information about the regular Veeam backup console, see the Backup & Replication Console section in the Veeam Backup & Replication User Guide.

The Remote Access Console is available on every machine where the regular Veeam backup console is installed. On the SP backup server, Veeam Backup & Replication creates a desktop icon for the Remote Access Console. On other machines where the Veeam backup console is installed, to open the Remote Access Console, use the following command:

```
"%ProgramFiles%\Veeam\Backup and Replication\Console\veeam.backup.shell.exe" -T
enantRemoteAccess
```

To connect to the tenant backup server, the SP needs to specify the following settings:

- The name or IP address of the SP backup server or cloud gateway (depending on the location of the Remote Access Console. To learn more, see Deployment Scenarios for Remote Access Console).
- Credentials to connect to the SP backup server.
- Credentials to connect to the tenant backup server.
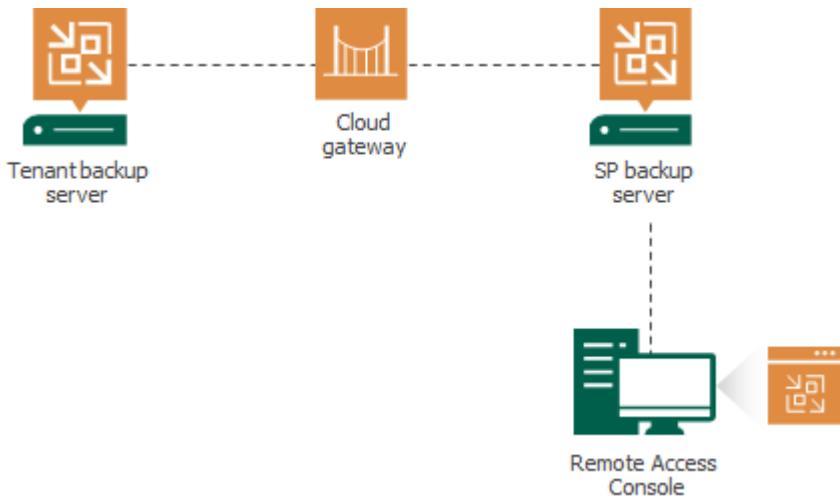
> **NOTE**
>
> The process of establishing a connection to the SP and tenant backup servers with the Remote Access Console may require longer time depending on the distance between these components and quality of the network connection.

The SP can use the same Remote Access Console to connect to different tenant backup servers. For convenience, the SP can save several shortcuts for these connections.

Deployment Scenarios for Remote Access Console
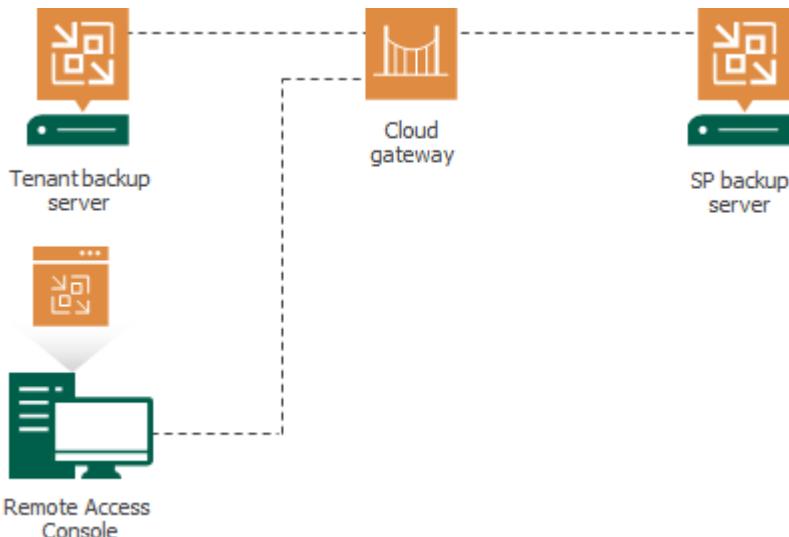
Veeam Backup & Replication offers the following scenarios of the Remote Access Console usage:

- The SP can use the Remote Access Console installed on the SP backup server or dedicated machine that is connected to the SP backup infrastructure network. In this scenario, the Remote Access Console will connect directly to the SP backup server to communicate to the Veeam Backup Service and Cloud network redirector.

- The SP can use the Remote Access Console on any machine that resides outside of the SP backup infrastructure and has access to the cloud gateway. In this case, the Remote Access Console will connect to the SP backup server over the internet through the cloud gateway.

  By default, Veeam Backup & Replication does not accept connections from the Remote Access Console over the internet. The SP can enable this functionality in the in the Veeam Backup & Replication settings if necessary. To learn more, see Enabling Access to Cloud Gateway.
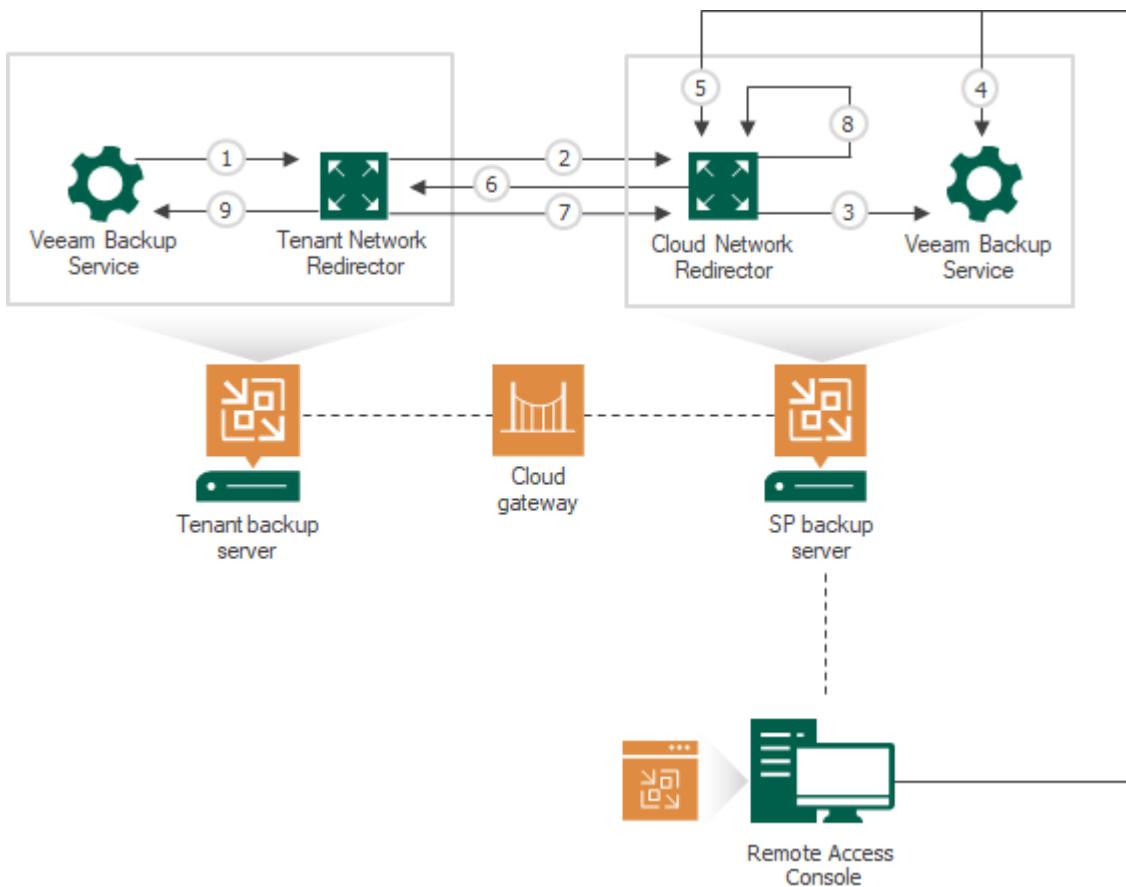
How Remote Access Console Works

To open and keep a remote connection to the tenant backup server with the Remote Access Console, Veeam Backup & Replication components communicate in the following way:

1. After the tenant adds the SP in its Veeam Backup & Replication console, the Veeam Backup Service running on the tenant backup server starts the Tenant network redirector.

2. The Tenant network redirector establishes the control connection to the Cloud network redirector that runs on the SP backup server waiting for connections from tenants.

3. The Cloud network redirector accepts the control connection from the Tenant network redirector and reports information about the connected tenant to the Veeam Backup Service running on the SP backup server. The control connection remains open.

4. The Remote Access Console connects to the Veeam Backup Service running on the SP backup server and retrieves information about tenants who have opened control connections to the SP.

5. When the SP starts using the Remote Access Console to connect to the tenant backup server, the Remote Access Console connects to the Cloud network redirector. The Remote Access Console provides to this network redirector information about the tenant to whose backup server the SP wants to connect.

6. The Cloud network redirector puts on hold the connection from the Remote Access Console and notifies the Tenant network redirector over the control connection that the Remote Access Console has requested to connect to the tenant backup server.

7. After the Tenant network redirector accepts the request over the control connection, the Tenant network redirector opens the new connection to the Cloud network redirector and provides to this network redirector information about the Remote Access Console that has requested to connect to the tenant backup server.

8. The Cloud network redirector accepts the connection from the Tenant network redirector, opens the awaiting connection from the Remote Access Console and starts redirecting requests between these connections.

9. The Tenant network redirector connects to the Veeam Backup Service running on the tenant backup server and starts redirecting requests between opened connections. The Remote Access Console starts communicating to the Veeam Backup Service running on the tenant backup server.

> **NOTE**
>
> In this scenario, the Remote Access Console is deployed in the SP Veeam Cloud Connect infrastructure and communicates directly to the SP backup server. If the Remote Access Console is deployed on a remote machine in an external network, the described steps remain the same. The only difference is that the Remote Access Console will communicate to the SP backup server through the cloud gateway.

Limitations for Remote Access Console

The Remote Access Console has the following limitations:

- The Remote Access Console must be of exactly the same version as Veeam Backup & Replication installed on the tenant backup server.

  In case versions differ, the Remote Access console will display a notification offering to establish a remote desktop connection to the tenant backup server. To learn more, see Remote Desktop Connection to Tenant.

- The SP cannot perform the following operations with the Remote Access Console:

  o Perform file-level restore

  o Perform application items restore with Veeam Explorers

  o Perform file copy operations using the **Files** view of the Veeam Backup & Replication console

  To overcome this limitation, the SP can establish a remote desktop connection to the tenant backup server. After that, the SP can perform necessary operations in the Veeam Backup & Replication console deployed locally on the tenant backup server.

Remote Desktop Connection to Tenant

The SP can use the Remote Access Console functionality to connect to the tenant backup server over the Remote Desktop Protocol. In this case, the SP can log on to the Microsoft Windows OS running on the tenant backup server and open the Veeam Backup & Replication console locally on this backup server. This may be required if the SP needs to perform operations that are not supported in the Remote Access Console, such as file-level or application items restore.

To connect to the tenant backup server, Veeam Backup & Replication uses the Remote Desktop Connection client (`mstsc.exe`). Veeam Backup & Replication opens the Remote Desktop Connection client locally on the machine where the Remote Access Console is installed. The Remote Desktop Connection client connects to Remote Desktop Services running on the tenant backup server. The connection is held over the communication channel opened between network redirectors. To learn more, see How Remote Desktop Connection to Tenant Works.

The SP can launch a remote desktop session to the tenant backup server in one of the following ways:

- From the **Cloud Connect** view of the Veeam Backup & Replication console connected to the SP backup server. In this case, the SP can select the necessary tenant and their backup server in the **Tenants** node of the **Cloud Connect** view.

- From the *Open Remote Access Console* window on any machine where the Remote Access Console is installed. After the SP specifies settings to connect to the tenant backup server, they can press and hold the **[CTRL]** key and click **Connect**. Instead of connecting to the tenant backup server with the Remote Access Console, Veeam Backup & Replication will launch the Remote Desktop Connection client.

- If the SP and tenant run different versions of Veeam Backup & Replication on their backup servers, Veeam Backup & Replication will display a warning in the *Open Remote Access Console* window notifying that the Remote Access Console is unable to connect to the tenant backup server. In the warning, Veeam Backup & Replication will display a link to launch the Remote Desktop Connection client.

> **NOTE**
>
> You can also launch the Remote Desktop Connection client from the main menu of the Veeam Backup & Replication console. In this case, Veeam Backup & Replication will open a remote desktop session to the backup server to which the Veeam backup console is connected.

How Remote Desktop Connection to Tenant Works
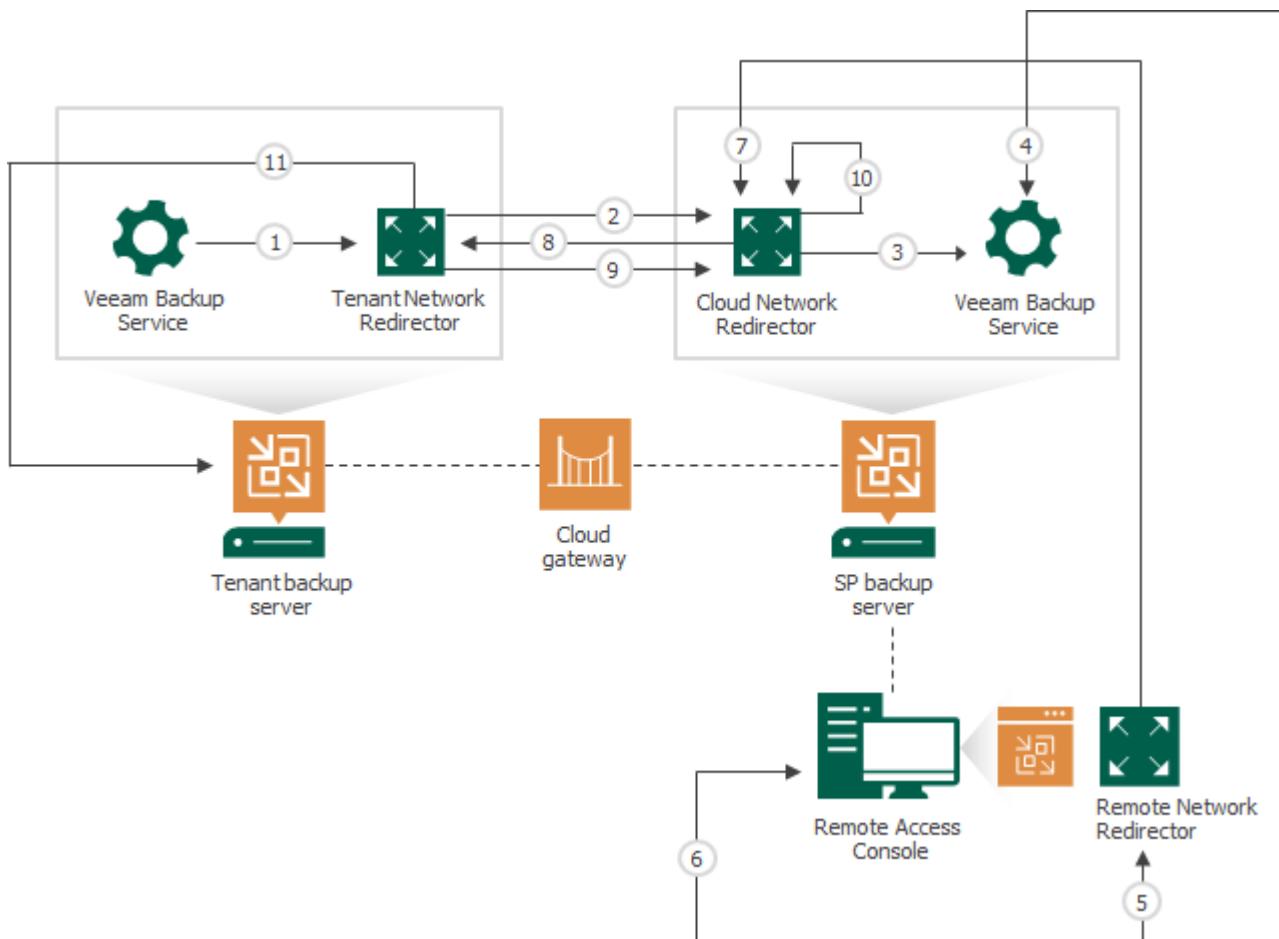
To open and keep a remote connection to the tenant backup server over the Remote Desktop Protocol, Veeam Backup & Replication components communicate in the following way:

1. After the tenant adds the SP in their Veeam Backup & Replication console, the Veeam Backup Service running on the tenant backup server starts the Tenant network redirector.

2. The Tenant network redirector establishes the control connection to the Cloud network redirector that runs on the SP backup server waiting for connections from tenants and Remote network redirectors.

3. The Cloud network redirector accepts the control connection from the Tenant network redirector and reports information about the connected tenant to the Veeam Backup Service running on the SP backup server. The control connection remains open.

4. The Remote Access Console connects to the Veeam Backup Service running on the SP backup server and retrieves information about tenants who have opened control connections to the SP.

5. When the SP starts using the Remote Access Console to connect to the tenant backup server over the RDP protocol, the Remote Access Console starts the Remote network redirector. The Remote Access Console provides to this network redirector information about the cloud gateway and information about the tenant to whose backup server the SP is connecting.

6. The Remote Access Console starts locally the Remote Desktop Connection client (`mstsc.exe`) that is set up to connect to the Remote network redirector.

7. The Remote network redirector accepts connection from Remote Desktop Connection client and connects to the Cloud network redirector. The Remote network redirector provides to the Cloud network redirector information about the tenant to whose backup server the SP is connecting over the RDP protocol. After that, the Remote network redirector starts redirecting requests between the Remote Desktop Connection client and the Cloud network redirector.

8. The Cloud network redirector puts on hold the connection from the Remote Desktop Connection client and notifies the Tenant network redirector over the control connection that the Remote Access Console has requested to connect to the tenant backup server over the RDP protocol.

9. After the Tenant network redirector accepts the request over the control connection, the Tenant network redirector opens the new connection to the Cloud network redirector and provides to this network redirector information about the Remote Access Console that has requested to connect to the tenant backup server over the RDP protocol.

10. The Cloud network redirector accepts the connection from the Tenant network redirector, opens the awaiting connection from the Remote Desktop Connection client and starts redirecting requests between these connections.

11. Tenant network redirector connects to Remote Desktop Services running in the tenant backup server OS and starts redirecting requests between opened connections. The SP gains access to the tenant backup server OS over the RDP protocol.

Tenant Backup to Tape

The SP can write backups created by a tenant in a cloud repository to a tape media. This allows the SP to offer additional tier of data protection to their tenants: the tenant will have one copy of the backed-up data in a cloud repository, and another copy of the backed-up on a tape media on the SP side. In case some important data in the cloud repository becomes unavailable, the tenant can ask the SP to restore the necessary data from tape.

The SP can also use the tenant backup to tape functionality to offer a separate data protection scenario — Tape as a Service. If a tenant is required to keep backups of their data on a tape media, they can request to copy their backups to tape and obtain the tape media from the SP without the need to deploy and maintain their own tape infrastructure.

The ability to archive tenant backups to tape can also help the SP protect their own infrastructure against disasters that may result in loss of tenant data.

Veeam Backup & Replication supports backup to tape for all types of tenant backups: backups created by VM backup jobs, Veeam Agent backup jobs and backup copy jobs that process VM backups and Veeam Agent backups.

All tasks within the tenant backup to tape scenario are performed by the SP. The tenant is unaware of the tape infrastructure deployed on the SP side. The tenant cannot view or manage backup to tape jobs configured by the SP, and perform operations with backups created by these jobs.

Getting Started with Tenant Backup to Tape

To back up tenant data to tape, the SP must complete the following steps:

1. Configure the Veeam Cloud Connect Backup infrastructure. For details, see Getting Started with Veeam Cloud Connect Backup.

2. Connect tape devices and add a tape server to the backup infrastructure on the SP backup server. For details, see Connecting Tape Devices and Adding Tape Server sections in the Veeam Backup & Replication User Guide.

3. Create one or more GFS media pools that will be used as targets for tenant backup to tape jobs. For details, see the Creating GFS Media Pools section in the Veeam Backup & Replication User Guide.

4. Configure and run a tenant backup to tape job. For details, see Creating Tenant Backup to Tape Job.

5. In case some tenant data in a cloud repository becomes missing or corrupted, you can restore the necessary data from tape. For details, see Restoring Tenant Data from Tape.

Tenant Backup to Tape Job

To back up tenant data to tape, you must create and run tenant backup to tape jobs. Technically, a tenant backup to tape job is a variant of a backup to tape job targeted at a GFS media pool. For more information about GFS media pools, see the GFS Media Pools section in the Veeam Backup & Replication User Guide.

As a source for a tenant backup to tape job, you can specify the following types of objects:

- All tenants

- One or more specific tenants

- One or more cloud repositories of the same tenant or different tenants

Backups created by tenant backup to tape jobs become available in the **Backups** > **Tape** node of the SP Veeam backup console. Such backups are not displayed in the tenant Veeam backup console.

> **NOTE**
>
> Consider the following:
>
> - Tenant backup to tape jobs process only backups created by jobs or mapped to jobs configured on tenant backup servers. Imported backups are skipped from processing.
> - If you use the Capacity Tier functionality to offload tenant data to an object storage repository, keep in mind that backup to tape jobs copy to tape active backup chains only (that is, backup chains that reside in performance tier). Inactive backup chains offloaded to an object storage repository are not processed by backup to tape jobs. To learn more about Capacity Tier support in Veeam Cloud Connect, see Support for Capacity Tier.

Data Restore from Tenant Backups on Tape

Veeam Backup & Replication offers the following scenarios for restore of tenant data from tape:

- **Restore to the original location**. In this scenario, Veeam Backup & Replication restores tenant backups to the original cloud repository. The existing backups are overwritten. After restore, Veeam Backup & Replication maps tenant jobs to the restored backup chains.

- **Restore to a new location**. In this scenario, Veeam Backup & Replication restores tenant backups to another cloud repository specified by the SP. This option may be useful if you do not want to overwrite all tenant backups in the original cloud repository.

- **Export backup files to disk**. In this scenario, Veeam Backup & Replication restores tenant backups to a specified folder located on a server in the SP Veeam backup infrastructure.

> **NOTE**
>
> If the tenant backup resides in capacity tier, and immutability is enabled for data blocks in capacity tier, you cannot use this backup to restore data to the original location. If you restore data from this backup to a new location, and specify the same original repository and new repository, Veeam Backup & Replication will automatically keep the original tenant data. You cannot choose to overwrite the original data with backed-up data from tape.

The SP can restore data of one tenant or several tenants simultaneously. The SP can restore all tenant data backed-up by a tenant backup to tape job or choose what data to restore. To do this, the SP can select for restore the following objects:

- Tenant

- Cloud repository

- Tenant job that created backup in the cloud repository

> **TIP**
>
> To restore tenant data from tape, the SP can also pass the tape media that contains tenant data to the tenant. In this case, the tenant can add the tape media to their Veeam backup infrastructure and use the Veeam backup console to perform regular restore operations from tape. To learn more, see the Tape Devices Support section in the Veeam Backup & Replication User Guide.

IPv6 Support

Veeam Backup & Replication supports IPv6 communication for Veeam Cloud Connect infrastructure components. This functionality is enabled by default in new installations of Veeam Backup & Replication 12. If the SP has upgraded Veeam Backup & Replication from an earlier version of the product, they can enable this functionality manually on the SP backup server. For details, see Enabling IPv6 Communication.

The following rules apply to IPv6 support in Veeam Cloud Connect:

- After the SP enables IPv6 communication, they can add cloud gateways to the Veeam Cloud Connect infrastructure in the NAT mode only and must specify an external DNS name in the cloud gateway settings. For details, see Specify Network Settings.

- The SP and tenant can specify whether to use IPv6 addresses for network extension appliances. The following scenarios for are available:

  o Use an IPv4 interface

  o Use an IPv6 interface

  o Use both IPv4 and IPv6 interfaces

  The SP and tenant can choose whether to assign an IPv4 or IPv6 address automatically, or specify it manually.

  The SP configures the SP network extension appliance when subscribing a standalone tenant account to a hardware plan or when configuring a VMware Cloud Director tenant account. For details, see Registering Tenant Accounts.

  The tenant configures the network extension appliance when adding the SP in the tenant Veeam backup console. For details, see Connecting to Service Providers.

- The SP can add IPv6 addresses to the pool of public IP addresses that will be available to tenant VM replicas, and can allocate them in the properties of the tenant account. For details, see Managing Public IP Addresses.

- The tenant can specify IPv6 addresses for default gateways whose settings Veeam Backup & Replication uses to enable communication with external networks during full site failover.

- For tenant VMs replicated to a cloud host, Veeam Backup & Replication detects IPv6 settings only if application-aware processing is enabled in the properties of the replication job or CDP policy that processes these VMs. These settings are required to map the tenant production network to the network for VM replicas on the SP side.

- During partial site failover, Veeam Backup & Replication establishes separate VPN tunnels for IPv4 and IPv6 communication between network extension appliances.

Enabling IPv6 Communication

If you have upgraded from an earlier version of Veeam Backup & Replication and want to allow communication over the IPv6 protocol in the Veeam Cloud Connect infrastructure, you must enable this option in the Veeam Backup & Replication settings.
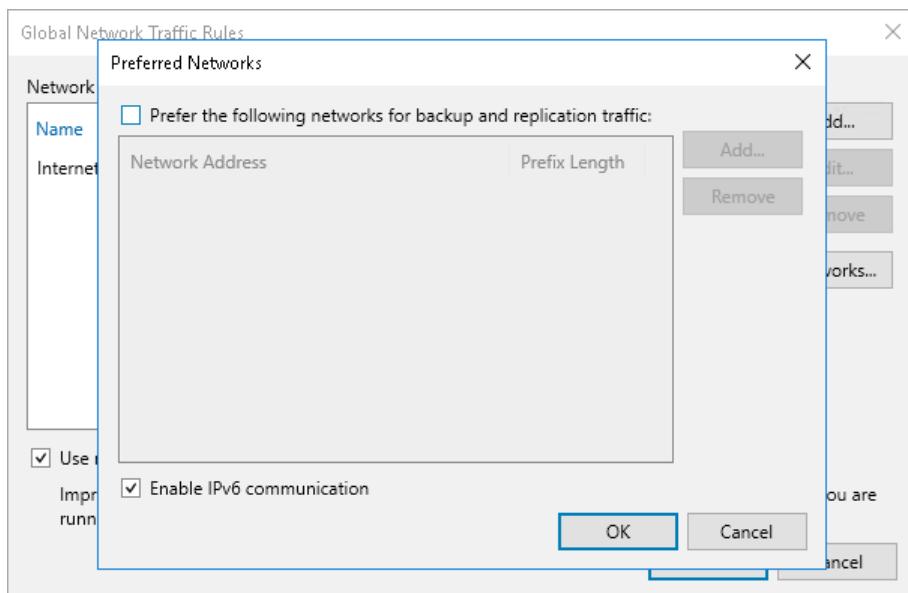
To enable IPv6 communication:

1. In the Veeam backup console on the SP backup server, from the **Main Menu**, select **Network Traffic Rules**.

2. In the **Global Network Traffic Rules** window, click **Networks**.

3. In the **Preferred Networks** window, select the **Enable IPv6 communication** check box.

4. Click **OK**.

> **NOTE**
>
> Consider the following:
>
> - After the SP enables IPv6 communication in the Veeam Cloud Connect infrastructure, the SP and tenant must redeploy network extension appliances that were deployed earlier to use IPv6 addresses for these components.
>
> - If the SP wants to disable IPv6 communication in the Veeam Cloud Connect infrastructure, they must disable IPv6 interfaces in the properties of network extension appliances before performing this operation. Otherwise, Veeam Backup & Replication will display a message with the list of network extension appliances that must be reconfigured.

Planning and Preparation

This section covers the list of system requirements to the Veeam Cloud Connect infrastructure and describes ports that must be open on backup infrastructure components.

System Requirements

Make sure that servers on which you plan to deploy Veeam Cloud Connect infrastructure components meet system requirements listed below.

Cloud Gateway

Specification	Requirement
Hardware	*CPU*: x86 or x86-64 processor. *Memory*: OS requirements plus Cloud Gateway Service requirements. A single connection from a tenant consumes around 512 KB of memory. 1 GB of memory in a cloud gateway can be used to receive up to 2,000 concurrent connections. *Disk Space*: 300 MB. *Network*: 1 Gbps LAN.
OS	32-bit and 64-bit versions of the following operating systems are supported[1]: • Microsoft Windows Server 2022 • Microsoft Windows Server 2019 • Microsoft Windows Server 2016 • Microsoft Windows Server Semi-Annual Channel (versions 1803 to 22H2) • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2012 • Microsoft Windows 11 (versions 21H2, 22H2) • Microsoft Windows 10 (versions 1909 to 22H2)

[1] Server Core installations of Microsoft Windows Server OSes are supported.

Veeam Backup Server

To learn about system requirements for Veeam backup servers deployed on the SP side and tenant side, see the System Requirements section in the Veeam Backup & Replication User Guide.

In addition to requirements listed in the Veeam Backup & Replication User Guide, the SP backup server must meet the following requirements:

Specification	Requirement
Hardware	*Memory*: 8 GB RAM minimum, 16 GB RAM for installations with more than 100 parallel tenant tasks.

The following recommendations help improve data processing performance for the SP backup server:

Specification	Recommendation
SQL Database	It is recommended to use an SQL Database installed on a dedicated server. The following versions of PostgreSQL are supported: • PostgreSQL 14.x • PostgreSQL 15 and 15.1 (version 15.1 is included in the Veeam Backup & Replication setup) The following versions of Microsoft SQL Server are supported: • Microsoft SQL Server 2022 Standard or Enterprise Edition • Microsoft SQL Server 2019 Standard or Enterprise Edition • Microsoft SQL Server 2017 Standard or Enterprise Edition • Microsoft SQL Server 2016 Standard or Enterprise Edition

For installations with more than 100 parallel tenant tasks, consider performance tuning. To learn more, see Performance Tuning.

Cloud Repository

To learn about system requirements for backup repositories used as cloud repositories, see the System Requirements section in the Veeam Backup & Replication User Guide.

WAN Accelerator

To learn about system requirements for WAN accelerators deployed on the SP side and on tenant side, see the System Requirements section in the Veeam Backup & Replication User Guide.

Performance Tuning

For high loads (about 100 parallel tasks), it is recommended that Veeam Cloud Connect service providers meet the following requirements to provide stable operation:

1. Backup quotas should be created on a Windows based backup repository.

2. Make sure that all tenants run the latest version of Veeam Backup & Replication and Veeam Agents.

> **NOTE**
>
> For higher loads (300 parallel tasks and more), see guidelines on Veeam Community Forums.

Ports

The following table describes network ports that must be opened to ensure proper communication of the Veeam Cloud Connect infrastructure components.

To learn what ports are required for other Veeam Backup & Replication components in the Veeam Cloud Connect infrastructure, see the Ports section in the Veeam Backup & Replication User Guide.

From	To	Protocol	Port	Notes
Cloud gateway	SP backup server	TCP	6169	Port on the SP backup server used to listen to cloud commands from the tenant side. Tenant cloud commands are passed to the Veeam Cloud Connect Service through the cloud gateway.
		TCP	8190, 8191	Port on the SP backup server used by SP-side network redirector(s) to connect to the Remote Access Console and establish a Remote Desktop Connection to tenant.
		TCP	2500 to 5000	Port range used during transfer of the Veeam Service Provider Console agent from the SP backup server to the tenant backup server.
	SP backup repository	TCP	2500 to 3300	Default range of ports used as data transmission channels. For every TCP connection that a job uses, one port from this range is assigned. **Note:** This range of ports applies to newly installed Veeam Backup & Replication starting from version 10.0, without upgrade from previous versions. If you have upgraded from an earlier version of the product, the range of ports from 2500 to 5000 applies to the already added components.

From	To	Protocol	Port	Notes
	SP backup proxy	TCP	2500 to 3300	Default range of ports used as data transmission channels. For every TCP connection that a job uses, one port from this range is assigned. For replication of Microsoft Hyper-V VMs, the SP backup proxy resides on the target Hyper-V host. For replication of VMware vSphere VMs, the role of the backup proxy can be assigned to the backup server or another machine in the Veeam backup infrastructure. **Note:** This range of ports applies to newly installed Veeam Backup & Replication starting from version 10.0, without upgrade from previous versions. If you have upgraded from an earlier version of the product, the range of ports from 2500 to 5000 applies to the already added components.
	Provider-side network extension appliance	UDP	1195	Port used to establish secure VPN connection for network extension during partial site failover. If a tenant has several IP networks, additional odd ports should be opened starting from 1195 — one port per tenant's IP network. For example, a tenant *Tenant1* replicates VMs that are connected to 3 IP networks. In the Veeam Cloud Connect infrastructure, the SP deployed a network extension appliance for *Tenant1*. In this case, the SP needs to open between the network extension appliance and the cloud gateway the following ports: *1195, 1197, 1199*.
	WAN accelerator	TCP	6165	Default port used for data transfer between WAN accelerators.

From	To	Protocol	Port	Notes
	Veeam Service Provider Console server	TCP	9999	Port on the Veeam Service Provider Console server used to communicate with the tenant backup server. Communication between tenant backup servers and Veeam Service Provider Console server goes through cloud gateways.
SP backup server	Cloud gateway	TCP	6160	Default port used by the Veeam Installer Service for deployment of the Veeam Cloud Gateway Service and during failover operations.
		TCP	6168	Port on the cloud gateway used to listen for cloud commands from the Veeam Cloud Connect Service. The service cloud commands from the Veeam Cloud Connect Service are sent to set up, delete and check the status of data transport channels between tenants and the cloud repository.
	Provider-side network extension appliance	TCP	22	Port used for communication with the network extension appliance.
		ICMP	—	SP backup server needs access to the SP network extension appliance over ICMP.
	Domain controller	TCP and UDP	389	Port used for LDAP connections to Active Directory domain controllers for Active Directory tenants authentication.
		TCP	636	Ports used for LDAPS connections to Active Directory domain controllers for Active Directory tenants authentication.
	WAN accelerator	TCP	6164	Controlling port for RPC calls.
		TCP	6220	Port used for traffic control (throttling) for tenants that use WAN accelerators.

From	To	Protocol	Port	Notes
SP backup repository (or gateway server)	Cloud gateway	TCP and UDP	6180	Port used for connections during the following operations: • Creating a replica from a cloud backup • Replica seeding from a cloud backup
SP Veeam Backup & Replication console	SP backup server	TCP	10003	Port used by the Veeam Backup & Replication console to connect to the backup server when managing the Veeam Cloud Connect infrastructure.
Tenant backup server	Cloud gateway	TCP and UDP	6180	Port on the cloud gateway used to transport VM data from the tenant side to the SP side (UDP is used only during partial failover of a cloud replica).
	Tenant-side network extension appliance	TCP	22	Port used for communication with the network extension appliance.
	Certificate Revocation Lists	TCP	80 or 443 (most popular)	Tenant backup server needs access to CRLs (Certificate Revocation Lists) of the CA (Certification Authority) who issued a certificate to the SP. Generally, information about CRL locations can be found on the CA website.
	Endpoint used by the Automatic Root Certificates Update component	TCP	443	Port used by the Automatic Root Certificates Update component for communication with the Windows Update endpoint. Applicable to Microsoft Windows 10 and later, Microsoft Windows Server 2016 and later. To learn more, see Microsoft Docs.
Backup server	Veeam Update Notification Server (dev.veeam.com)	TCP	80	Default port used to download information about available updates from the Veeam Update Notification Server over the internet.

From	To	Protocol	Port	Notes
	Veeam License Update Server (autolk.veeam.com)	TCP	443	Default port used for license auto-update.
	Backup server	TCP	10003	Port used for communication with the Veeam Backup Service (locally on the backup server).
Provider-side network extension appliance	Cloud gateway	UDP	1195	Port used to establish secure VPN connection for network extension during partial site failover. If a tenant has several IP networks, additional odd ports should be opened starting from 1195 — one port per tenant's IP network. For example, a tenant *Tenant1* replicates VMs that are connected to 3 IP networks. In the Veeam Cloud Connect infrastructure, the SP deployed a network extension appliance for *Tenant1*. In this case, the SP needs to open between the network extension appliance and the cloud gateway the following ports: *1195, 1197, 1199*.
Tenant-side network extension appliance	Cloud gateway	TCP and UDP	6180	Port used to carry tenant VM traffic from the tenant network extension appliance to the SP network extension appliance through the cloud gateway.
Tenant backup proxy (VMware vSphere) or Hyper-V server / off-host backup proxy (Microsoft Hyper-V)	Cloud gateway	TCP and UDP	6180	Port used for VM data transport to the cloud repository by backup jobs.

From	To	Protocol	Port	Notes
Tenant backup repository (Microsoft Windows server / Linux server / gateway server for CIFS share)	Cloud gateway	TCP and UDP	6180	Port used for VM data transport to the cloud repository by backup copy jobs.
Tenant VMware CDP proxy	Cloud gateway	TCP and UDP	6180	Port used for VM data transport by CDP policies targeted at the cloud host. For the complete list of ports used in the CDP infrastructure, see the CDP Components section in the Veeam Backup & Replication User Guide.
Remote Access Console (SP LAN)	SP backup server	TCP	8191	Port used for communication with the Veeam Cloud Connect Service and SP-side network redirector(s).
		TCP	9392	Port used for communication with the Veeam Backup Service.
		TCP	10003	Port used for communication with the Veeam Backup Service.
Remote Access Console (Internet)	Cloud gateway	TCP	6180	Default port used for communication with the SP Veeam Cloud Connect Service and SP-side network redirector(s).
	Certificate Revocation Lists	TCP	80 or 443 (most popular)	Remote Access Console needs access to CRLs (Certificate Revocation Lists) of the CA (Certification Authority) who issued a certificate to the SP. Generally, information about CRL locations can be found on the CA website.

From	To	Protocol	Port	Notes
Tenant desktop computer or portable device	Veeam Cloud Connect Portal	TCP	6443	Port used for accessing Veeam Cloud Connect Portal by tenants. Veeam Cloud Connect Portal is installed on the SP Veeam Backup Enterprise Manager server as an optional component. It should be published on the internet by the SP administrator.
Tenant Hyper-V server	Cloud gateway	TCP and UDP	6180	Port used for data transport during full VM restore.

Veeam Product Versions

SP and tenants can run different versions of Veeam Backup & Replication on their Veeam backup servers. Veeam products on the SP and tenant side must meet the following requirements:

- Veeam Backup & Replication versions must support the Veeam Cloud Connect functionality.

- The SP Veeam backup server must run the same or later version of Veeam Backup & Replication than the tenant Veeam backup server.

  This applies to major product versions. Within Veeam Backup & Replication version 12, the SP and tenant can use any product build. It is recommended, however, that the SP and tenant install latest hotfixes and updates on the backup server.

- Veeam Backup & Replication 12 running on the SP backup server is compatible with the following versions of Veeam products running on the tenant side:

  - Veeam Backup & Replication 10a with Cumulative Patch P20210609 (build 10.0.1.4854) and later

  - Veeam Agent for Microsoft Windows 5.0 (build 5.0.0.4301) and later

  - Veeam Agent for Linux 5.0 (build 5.0.0.4318) and later

  - Veeam Agent for Mac 1.0.1 (build 1.0.1.822) and later

If the SP or tenant plan to upgrade Veeam Backup & Replication, the upgrade process must start on the SP side. The upgrade process should be performed in the following way:

1. The SP upgrades Veeam Backup & Replication on the SP backup server. The upgrade procedure does not differ from a regular one. To learn more, see the Upgrading to Veeam Backup & Replication 12 section in the Veeam Backup & Replication User Guide.

2. After Veeam Backup & Replication on the SP side is upgraded, the tenant can perform the same upgrade procedure on the tenant backup server.

Tenants who run earlier versions of Veeam Backup & Replication can continue using cloud resources provided to them by the SP who has upgraded Veeam Backup & Replication. However, some Veeam Cloud Connect functionality introduced in the current version of Veeam Backup & Replication may be not available to these tenants.

Considerations and Limitations

Before you start using the Veeam Cloud Connect functionality, consider prerequisites and limitations listed in this section.

Veeam Cloud Connect Backup

Veeam Backup & Replication has the following limitations for Veeam Cloud Connect Backup.

Backup, Backup Copy and Restore

- Veeam Backup & Replication does not support backup copy jobs if the cloud repository is used as a source backup repository. The backup copy job must use a backup repository configured locally on the tenant side as a source one.

- Transaction log backup is not supported for backup jobs targeted at the cloud repository. You can back up transaction logs only with backup copy jobs in the immediate copy mode.

  Note that cloud repositories backed by object storage systems are not supported by transaction log backup copy jobs.

- Instant VM Recovery, multi-OS file-level restore, restore to Microsoft Azure, Amazon EC2 and Nutanix AHV from backups in the cloud repository are not supported on the tenant side.

  Instant Recovery from VM backups and Veeam Agent backups is supported on the SP side. To learn more, see Instant Recovery from Tenant Backups.

- Removed GFS restore points might remain displayed in the Veeam Backup & Replication UI on the tenant side. To refresh the list of restore points, disable the job that created the restore points and rescan the SP in the tenant Veeam backup console.

- The *Copy backup* and *Move backup* operations to, from and between cloud repositories are not supported.

- In the scenario where the SP uses backup repositories that support immutability as cloud repositories, tenant backups become immutable for the number of days specified in the backup repository settings. Veeam Backup & Replication does not delete tenant backups within a job session or by the background retention job until both the retention period and immutability period end for these backups. The tenant should be aware of the fact that because of immutability, their backups may remain in the cloud repository for the longer period than specified in the job settings.

> **NOTE**
>
> Veeam Cloud Connect does not support NAS backup.

File Operations

Tenants can manually copy backup files to and from the cloud repository using the **Files** view in the Veeam Backup & Replication console. Scheduled file copy jobs are not supported.

Scale-Out Backup Repositories Used as Cloud Repositories

Consider the following:

- The SP cannot expose a scale-out backup repository as a cloud repository if unlimited number of concurrent tasks is specified for at least one extent added to this scale-out backup repository.

- Tenants cannot use the **Files** view in the Veeam Backup & Replication console to copy backup files to and from a scale-out backup repository exposed as a cloud repository. Such cloud repositories are displayed in the tenant Veeam Backup & Replication console in the read-only mode.

Deduplicating Storage Appliances Used as Cloud Repositories

It is not recommended to use deduplicating storage appliances as cloud repositories. To protect VM data that is backed up to the cloud repository, tenants are likely to use data encryption. For deduplicating storage appliances, encrypted data blocks appear as different though they may contain duplicate data. Thus, deduplicating storage appliances will not provide the expected deduplication ratio. To learn more, see the Data Encryption section in the Veeam Backup & Replication User Guide.

If the SP uses a deduplicating storage appliance as a cloud repository, the SP must consider the following limitations.

General

To keep track of tenant quota consumption, Veeam Backup & Replication uses information about the size of backed-up data reported by a backup repository. A backup repository calculates the size of backed-up data based on the size of source data before deduplication. As a result, the actual size of tenant backup data in the cloud repository may be significantly smaller than the reported used space. The difference depends on whether the tenant uses data encryption and on the backup repository type.

This approach leads to the following consequences:

- The tenant does not gain advantage from using data deduplication other than native deduplication and compression provided by Veeam and performed within a backup job.

- Tenant backup jobs may fail to back up data to a cloud repository even in case deduplicating storage has free storage space.

  To overcome this limitation, it is recommended that the SP over-provisions storage space on the deduplicating storage appliance used as a cloud repository.

Consider the following example:

- The tenant backs up VMs whose total size is 80 GB.

- The tenant quota size is 100 GB, and it is allocated on a deduplicating storage appliance used as a cloud repository.

- On deduplicating storage, tenant VM backup data consumes 30 GB.

In this case, the backup repository will display that used storage space is 80 GB, and the tenant will be able to back up additional 20 GB, and not 70 GB. To let the tenant back up the total amount of 100 GB of data, the SP needs to use over-provisioning.

Dell Data Domain

The length of forward incremental and forever forward incremental backup chains that contain one full backup and a set of subsequent incremental backups cannot be greater than 60 restore points. To overcome this limitation, the tenant can do the following:

- For backup jobs, the tenant can schedule full backups (active or synthetic) to split the backup chain into shorter series. For example, to perform backups at 30-minute intervals, 24 hours a day, the tenant must schedule synthetic full backups every day. In this scenario, intervals immediately after midnight may be skipped due to duration of synthetic processing.

- For backup copy jobs, the tenant can specify the necessary number of restore points in the backup copy job settings. The number of restore points in the backup chain must be less than 60.

If the SP plans to use Dell Data Domain as a cloud repository, it is strongly recommended that the SP informs tenants about limitations for the backup chain length.

HPE StoreOnce

Veeam Backup & Replication does not support usage of HPE StoreOnce deduplicating storage appliances as cloud repositories.

If the SP plans to use a scale-out backup repository as a cloud repository, they should consider the following limitations:

- The SP cannot add an HPE StoreOnce appliance as an extent to a scale-out repository that is used as a cloud repository.

- The SP cannot use a scale-out backup repository as a cloud repository if an HPE StoreOnce appliance is added as an extent to this scale-out backup repository.

Object Storage Repositories Used as Cloud Repositories

To learn about considerations and limitations for the backup to object storage functionality, see Backup to Object Storage.

Veeam Cloud Connect Replication

Veeam Backup & Replication has the following limitations for Veeam Cloud Connect Replication.

Snapshot-Based Replication

- Veeam Cloud Connect Replication does not support DHCP. To allow a VM replica on the cloud host to be accessible over the network after failover, a replicated VM must have a static IP address.

- Automatic network settings detection is supported for Microsoft Windows VMs only. For cloud replication of non-Windows VMs, a tenant should specify network mapping settings and public IP addressing rules manually.

- A tenant cannot specify Re-IP rules for VM replicas on the cloud host. At the process of the replication job configuration, if a tenant selects the Re-IP option and then selects the cloud host as a replication target, Veeam Backup & Replication will disable the Re-IP option.

- Pick datastore option is not supported for replication jobs targeted at the cloud host.

- A tenant can restore VM guest OS files from a VM replica on the cloud host only to a Microsoft Windows file system.

- [For Microsoft Hyper-V VMs] Cloud replication of Shielded VMs is not supported. Replicas of such VMs can run only on guarded Hyper-V hosts that have access to Host Guardian Service deployed on the tenant side.

- Replication of encrypted VMs to a cloud host is not supported.

- If the SP uses a vSAN datastore as a target storage for tenant VM replicas, Veeam Backup & Replication will display double quota usage.

Replication to VMware Cloud Director

Before you start using VMware Cloud Director in the Veeam Cloud Connect infrastructure, consider the following prerequisites and limitations for VMware Cloud Director support:

- Veeam Cloud Connect supports VMware Cloud Director versions 10.1 to 10.4.

- If you plan to add more than one VMware Cloud Director server to the Veeam Cloud Connect infrastructure, make sure that names of VMware Cloud Director organizations and organization user accounts are unique within all VMware Cloud Director servers. Configurations with multiple Cloud Director servers that have identical organization and organization user account names are not supported.

Continuous Data Protection (CDP)

To learn about prerequisites and limitations for CDP with Veeam Backup & Replication, see the Requirements and Limitations section in the Veeam Backup & Replication User Guide.

In addition, Veeam Backup & Replication has the following limitations for CDP in the Veeam Cloud Connect infrastructure.

- For the CDP to VMware vSphere scenario: the minimum required ESXi version on the SP and tenant side is 6.5 Update 2.

- For the CDP to VMware Cloud Director scenario:

    o On the SP side, the minimum required ESXi version is 7.0.

    o On the tenant side, the minimum required ESXi version is 6.5 Update 2.

    o You must not use the same vApp as a target for both a snapshot-based replication job and a CDP policy.

    o Organization VDC must have a CDP-ready storage policy. If no such policy is configured, Veeam Backup & Replication will check whether the default storage policy may be used for CDP and create a CDP-ready policy based on this storage policy. Mind that the *Any* storage policy is not supported for CDP.

    If a CDP-ready policy exists in VMware vSphere, Veeam Backup & Replication will import it to VMware Cloud Director and use it for CDP.

Naming Conventions

Do not use Microsoft Windows reserved names for names of backup repositories, jobs, tenants and other objects created in Veeam Backup & Replication: CON, PRN, AUX, NUL, COM1, COM2, COM3, COM4, COM5, COM6, COM7, COM8, COM9, LPT1, LPT2, LPT3, LPT4, LPT5, LPT6, LPT7, LPT8 and LPT9. If you use a reserved name, Veeam Backup & Replication may not work as expected. To learn more about naming conventions in Microsoft Windows, see Microsoft Docs.

Licensing for Service Providers

Veeam Cloud & Service Providers (VCSPs) use rental licenses in the Veeam Backup & Replication infrastructure. Veeam Software provides VCSPs with the following types of rental license:

- Veeam Cloud Connect license. Technically, the Veeam Cloud Connect license is the rental license with the *Cloud Connect Provider = Yes* field in the license key file. The SP uses this type of license on the SP backup server. The SP must not install this license on tenant backup servers. To learn more, see Offsite Backup and Disaster Recovery (BaaS and DRaaS).

- Rental Veeam Backup & Replication license. The rental Veeam Backup & Replication license contains the *Cloud Connect Provider = No* field in the license key file. The SP uses this type of license on tenant backup servers in the Managed Service scenario. To learn more, see Managed Service.
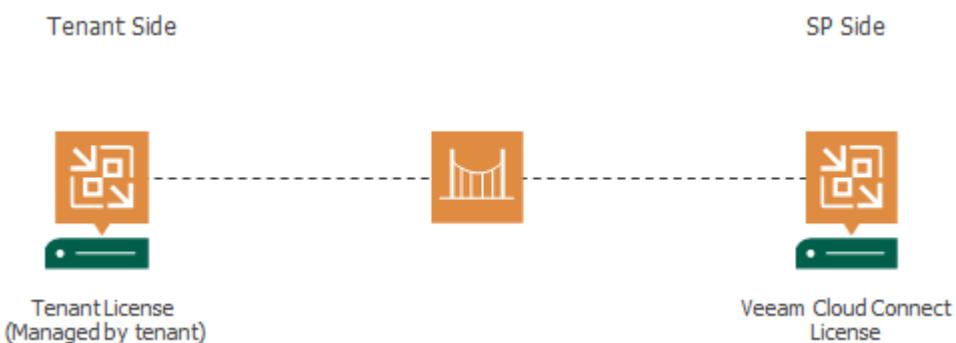
Offsite Backup and Disaster Recovery (BaaS and DRaaS)

The Veeam Cloud Connect functionality allows the SP to provide offsite backup and disaster recovery services to tenants. To enable the Veeam Cloud Connect functionality, the SP must install the Veeam Cloud Connect license on the SP backup server. After that, the SP can configure the Veeam Cloud Connect infrastructure and provide backup and replication resources to tenants.

Veeam Cloud Connect offers the following data protection scenarios:

- Backup as a Service (Veeam Cloud Connect Backup). This scenario is intended for tenants who have Veeam Backup & Replication, Veeam Agent for Microsoft Windows or Veeam Agent for Linux deployed and want to back up and copy machines to the cloud. In this scenario, Veeam products on the tenant side may have any type of paid license installed. To learn more, refer to the product documentation on Veeam Help Center.

- Disaster Recovery as a Service (Veeam Cloud Connect Replication). This scenario is intended for tenants who have Veeam Backup & Replication deployed and want to replicate VMs to the cloud. In this scenario, Veeam backup servers on the tenant side may have any type of paid license installed in Veeam Backup & Replication. To learn more, see the Types of Licenses section in the Veeam Backup & Replication User Guide.

In these scenarios, tenant machines processed in Veeam Backup & Replication consume both licenses: the *Veeam Cloud Connect license* and the license installed on the tenant backup server.

Managed Service (MSP Backup)

SPs can provide backup and replication services to tenants who want to protect data of their virtual or physical machines and do not want to manage the Veeam backup infrastructure on their own account. In terms of Veeam products, this scenario is referred to as *Managed Service*, and the SP providing services within this scenario is referred to as *Managed Service Provider (MSP)*. In this scenario, the SP deploys Veeam Backup & Replication and/or Veeam Agents on the tenant side, configures and manages backup and replication jobs and charges tenants for processing tenant machines. The SP typically performs these operations on-site or remotely using a web-based UI.

In the Managed Service scenario, in the Veeam products deployed on the tenant side, the SP must install a Rental Veeam Backup & Replication license for the total number of instances for workloads that the tenant plans to protect. In case the SP provides offsite backup and disaster recovery within this scenario, the *Veeam Cloud Connect license* on the SP side and the *Rental Veeam Backup & Replication license* on the tenant side are consumed according to the following rules:

- Tenant machines processed by backup jobs and backup copy jobs targeted at a cloud repository consume the *Rental Veeam Backup & Replication license* and do not consume the *Veeam Cloud Connect license*. To learn more, see Rental Machines Licensing.

- Tenant machines processed by replication jobs targeted at a cloud host consume both the *Veeam Cloud Connect license* and the *Rental Veeam Backup & Replication license*.

Veeam Cloud Connect License

To enable the Veeam Cloud Connect functionality, the SP must install the *Veeam Cloud Connect license* on the SP backup server. For SPs, the Veeam Cloud Connect functionality is licensed per points. Points are units (or tokens) that the SP can use to protect tenant workloads. The SP must obtain a license for the total number of points that is sufficient to protect tenant workloads.

The SP can use points in the license to protect tenant workloads of the following types:

- *Cloud Connect VMs* — VMs backed up to a cloud repository by backup jobs configured in Veeam Backup & Replication.

- *Cloud Connect Replicas* — VMs replicated to a cloud host by replication jobs configured in Veeam Backup & Replication.

- *Cloud Connect Workstations* — physical or virtual workstations backed up to a cloud repository by Veeam Agent backup jobs configured Veeam Agent or Veeam Backup & Replication.

- *Cloud Connect Servers* — physical or virtual servers backed up to a cloud repository by Veeam Agent backup jobs configured in Veeam Agent or Veeam Backup & Replication.

The *Veeam Cloud Connect license* is consumed by protected workloads. A protected workload is a virtual or physical machine that has at least one restore point created by a tenant in the past 31 days. Every protected workload consumes points in the license. The number of points that a workload requires depends on the workload type. For more information, see Veeam Rental Licensing and Usage Reporting Guide.

This licensing model allows the SP to obtain a license with a certain number of points without knowing in advance what types of workloads tenants plan to protect.

Consider the following:

- The Veeam Cloud Connect license does not allow to back up and replicate VMs with the jobs configured on the SP Veeam backup server. If the SP used such scenario with previous versions of Veeam Backup & Replication, they must follow the SP Veeam backup server split procedure. To learn more, see this Veeam KB article.

- Combining regular Veeam backup infrastructure and Veeam Cloud Connect infrastructure on the same backup server is supported only for the *Veeam Cloud Connect for the Enterprise* scenario. For more information, see this Veeam webpage.

- If a tenant has a *Rental Veeam Backup & Replication license* installed on the tenant backup server, Veeam Backup & Replication does not consider tenant machines processed by backup and/or backup copy jobs as protected workloads. Instead, Veeam Backup & Replication treats such machines as *rental machines*. In contrast to protected workloads, rental machines consume the tenant license and do not consume the SP license. To learn more, see Rental Machines Licensing.

- The SP can also obtain and install on the SP backup server a *Free Veeam Service Provider Console license*. A license of this type is intended for SPs who want to use Veeam Backup & Replication only for Remote Monitoring and Management with Veeam Service Provider Console or for offering Office 365 Backup as a Service with Veeam Backup for Microsoft 365. For more information, see Veeam Rental Licensing and Usage Reporting Guide.

New Workloads

To provide more flexibility and introduce a trial period for tenant workload processing, Veeam Backup & Replication offers the concept of *new workloads*. New workloads are workloads that were processed for the first time within the current calendar month. For example, Veeam Backup & Replication processes 7 machines in November. In December, Veeam Backup & Replication processes the same 7 machines plus 2 new machines. In December, these 2 machines are considered as new workloads.

New workloads are counted separately from existing workloads and do not consume points in the license during the month when they were introduced. On the first day of the new month, the number of points related to new workloads is added to the total number of used points, and the new points counter is reset. New workloads are included in a license usage report for informational purposes.

License Expiration

The *Veeam Cloud Connect license* period is set in accordance with the chosen licensing program.

To ensure a smooth license update procedure, Veeam Backup & Replication offers to the SP a 60-day grace period after the license expires. Upon license expiration, the SP can process all tenant workloads for the duration of the grace period.

During the grace period, Veeam Backup & Replication will show a warning that the SP needs to update the license.

- During the first month of a grace period, a message box is displayed once a week when the Veeam Backup & Replication console opens.

- During the second month, a message box is displayed each time the Veeam Backup & Replication console opens.

After the grace period is over, tenant workloads are no longer processed. To continue using Veeam Backup & Replication, the SP must purchase a new license.

The grace period is also valid for situations when the number points used by tenant workloads exceeds the total number of licensed points. To learn more, see Exceeding License Limit.

Exceeding License Limit

In some situations, the number of used points may exceed the license limit. For example, this may happen when some machines are temporarily processed for testing reasons and stop being processed after some time.

For the *Veeam Cloud Connect license*, Veeam Backup & Replication allows the SP to manage up to 20 more points or 20% more points (depending on which number is greater) than specified in the license, plus the number of new points from the previous calendar month. Consider the following examples:

- The licensed number of points is 50, during the previous calendar month the SP processed 10 new points. In this case, the license limit may be exceeded by 30 points — 10 new points from the previous month plus 20 points (20 is greater than 10, which makes 20% of 50).

- The licensed number of points is 200, during the previous calendar month the SP processed 10 new points. In this case, the license limit may be exceeded by 50 points — 10 new points from the previous month plus 40 points (40 makes 20% of 200 and is greater than 20).

Until the license limit is not exceeded for more than 20% or 20 points, plus the number of new points from the previous month, Veeam Backup & Replication continues to process all protected workloads with no restrictions. Newly added workloads are processed on the First In First Out basis when free license slots appear due to older workloads no longer being processed.

When the license is exceeded by more than 10% or 10 points, Veeam Backup & Replication displays a notification with the number of exceeded points and the number of points by which the license can be further exceeded. Veeam Backup & Replication displays this warning once a week when backup console opens.

If the license limit is exceeded for more than 20% or 20 points, plus the number of new points from the previous month, all workloads that use points exceeding the licensed number plus the allowed increase are no longer processed. Each time the backup console opens, Veeam Backup & Replication displays a notification with the number of points by which the license is exceeded.

Rental Machines Licensing

Tenant machines backed up with a *Rental Veeam Backup & Replication license* installed on the tenant backup server do not consume the Veeam Cloud Connect license installed on the SP backup server.

- If a tenant backs up a server or workstation with Veeam Agent that uses a rental license, the SP can host cloud backups of that server or workstation with no additional license fee for Veeam Cloud Connect Backup.

- Likewise, if a tenant backs up a VM with a *Rental Veeam Backup & Replication license*, the SP can host cloud backups of that VM with no additional license fee for Veeam Cloud Connect Backup.

With this functionality, SPs who manage Veeam backup infrastructure on the tenant side can deliver a complete managed backup service, including backup to the cloud, for a single license fee based on the protected machine type, regardless of its size. There is no need to pay an additional license fee for Veeam Cloud Connect Backup.

Tenant machines are considered as *rental machines* in case the tenant creates a backup in a cloud repository of the SP in the following way:

- Creates a VM backup with a backup job configured in Veeam Backup & Replication.

- Creates a backup of a physical or virtual machine with a Veeam Agent backup job.

- Creates a copy of a VM backup with a backup copy job configured in Veeam Backup & Replication.

- Creates a copy of a Veeam Agent backup with a backup copy job configured in Veeam Backup & Replication.

Veeam Backup & Replication running on the SP backup server counts rental machines according to the following rules:

- Rental machines do not consume the *Points* counter in the SP license.

- Rental machines are not included in monthly license usage reports for the SP license.

- Rental machines appear in tenant machine counts in the SP backup console and Veeam Cloud Connect report.

For example, *Tenant 1* uses Veeam Backup & Replication and Veeam Agent for Microsoft Windows with rental licenses installed to back up 2 VMs and 1 server to the cloud repository. *Tenant 2* uses Veeam Backup & Replication and Veeam Agent for Microsoft Windows with subscription licenses installed to back up 6 VMs and 2 servers to the cloud repository. In this case, the SP license will be consumed by 6 backed-up VMs and 2 servers processed by *Tenant 2*. 2 VMs and 1 server processed by *Tenant 1* will be considered as rental machines and will not appear in the SP license.

In the tenant machine counts of the SP backup console, as well as in the SP Veeam Cloud Connect report, Veeam Backup & Replication will display the total number of 8 backed-up VMs and 3 servers — the number of machines processed by *Tenant 2* plus the number of rental machines processed by *Tenant 1*.

Rental Veeam Backup & Replication License

For the MSP Backup scenario where the SP controls the Veeam Backup & Replication infrastructure on the tenant side and manages tenant machines, the SP must install a *Rental Veeam Backup & Replication license* on the tenant Veeam backup server. The *Rental Veeam Backup & Replication license* is a full license with the license expiration date set according to the chosen rental program (normally from 1 to 12 months from the date of issue) that can be automatically updated upon expiration. To learn more, see Updating Licenses.

The *Rental Veeam Backup & Replication license* is consumed by protected workloads. A protected workload is a virtual or physical machine that has at least one restore point created by a tenant in the past 31 days.

With the *Rental Veeam Backup & Replication license*, Veeam Backup & Replication processes workloads of the following types:

- *Virtual Machines* — VMs processed by backup and replication jobs configured in Veeam Backup & Replication.

- *Workstations* — physical or virtual machines processed by backup jobs configured in the Workstation edition of Veeam Agent for Microsoft Windows or Veeam Agent for Linux.

- *Servers* — physical or virtual machines processed by backup jobs configured in the Server edition of Veeam Agent for Microsoft Windows or Veeam Agent for Linux.

Every protected workload consumes points in the license. The number of points that a workload requires depends on the workload type. For more information, see Veeam Licensing Policy.

License consumption does not depend on the number of jobs that process protected workloads. For example, if a tenant processes the same VM with multiple jobs, this VM is still considered as 1 protected workload.

Protected workloads are counted regardless of the type of jobs (backup or replication) that process these workloads. For example, if a tenant processes the same VM with a backup job and a replication job, this VM is considered as 1 protected workload.

New Workloads

To provide more flexibility and introduce a trial period for tenant workload processing, Veeam Backup & Replication offers the concept of *new workloads*. New workloads are workloads that were processed for the first time within the current calendar month. For example, Veeam Backup & Replication processes 7 machines in November. In December, Veeam Backup & Replication processes the same 7 machines plus 2 new machines. In December, these 2 machines are considered as new workloads.

New workloads are counted separately from existing workloads and do not consume points in the license during the month when they were introduced. On the first day of the new month, the number of points related to new workloads is added to the total number of used points, and the new points counter is reset. New workloads are included in a license usage report for informational purposes.

License Usage with Multiple Veeam Backup Servers

The SP can install one *Rental Veeam Backup & Replication license* on multiple tenant Veeam backup servers. When a license file is assigned to a Veeam backup server, this backup server receives an *Installation ID*. An *Installation ID* is a unique identifier that is used to track the fact of using the same license file on multiple installations of Veeam Backup & Replication.

A *Rental Veeam Backup & Replication license* installed on multiple tenant Veeam backup servers counts all managed VMs that are processed on those backup servers. For example, if the SP installs a *Rental Veeam Backup & Replication license* for 10 VMs on 2 different tenant backup servers, they can manage 10 VMs in total (not 10 VMs for each tenant and 20 VMs in total).

> **NOTE**
>
> Rules for *Rental Veeam Backup & Replication license* usage on multiple backup servers may vary depending on the region. For details, contact your sales representative.

License Expiration

Veeam Backup & Replication offers a 60-day grace period to ensure a smooth license update procedure. Upon license expiration, the tenant can use the *Rental Veeam Backup & Replication license* to process all workloads for the duration of the grace period.

During the grace period, Veeam Backup & Replication will show a warning that the *Rental Veeam Backup & Replication license* must be updated.

- During the first month of a grace period, a message box is displayed once a week when the Veeam Backup & Replication console opens.

- During the second month, a message box is displayed each time the Veeam Backup & Replication console opens.

After the grace period is over, tenant workloads are no longer processed. To continue using Veeam Backup & Replication, the SP must obtain a new *Rental Veeam Backup & Replication license*.

Exceeding License Limit

In some situations, the number of used points may exceed the license limit. For example, this may happen when some machines are temporarily processed for testing reasons and stop being processed after some time.

For the *Rental Veeam Backup & Replication license*, Veeam Backup & Replication offers the 60-day grace period. Within this period, the *Rental Veeam Backup & Replication license* allows the tenant to use up to 20 more points or 20% more points than specified in the license (depending on which resulting number of points is greater), plus the number of new points from the previous calendar month.

Consider the following examples:

- Example 1. The licensed number of points is 50, and during the previous calendar month the tenant used 10 new points.

  In this example, the license limit may be exceeded by 30 points. This number includes 10 new points from the previous month and 20 additional points (20% of 50 licensed points makes 10 points, and 20 is greater than 10).

- Example 2. The licensed number of points is 200, and during the previous calendar month the tenant used 10 new points.

  In this example, the license limit may be exceeded by 50 points. This number includes 10 new points from the previous month and 40 additional points (20% of 200 licensed points makes 40 points, and 40 is greater than 20).

Until the license limit is exceeded for more than 20% or 20 points, plus the number of new points from the previous month, Veeam Backup & Replication continues to process all protected workloads with no restrictions. Newly added workloads are processed on the First In First Out basis when free license slots appear due to older workloads no longer being processed. When the license is exceeded by more than 10% or 10 points, Veeam Backup & Replication displays a notification with the number of exceeded points and the number of points by which the license can be further exceeded. Veeam Backup & Replication displays this warning once a week when backup console opens.

If the license limit is exceeded for more than 20% or 20 points, plus the number of new points from the previous month, all workloads that use points exceeding the licensed number plus the allowed increase are no longer processed. Every time the backup console opens, Veeam Backup & Replication displays a notification with the number of points by which the license is exceeded.
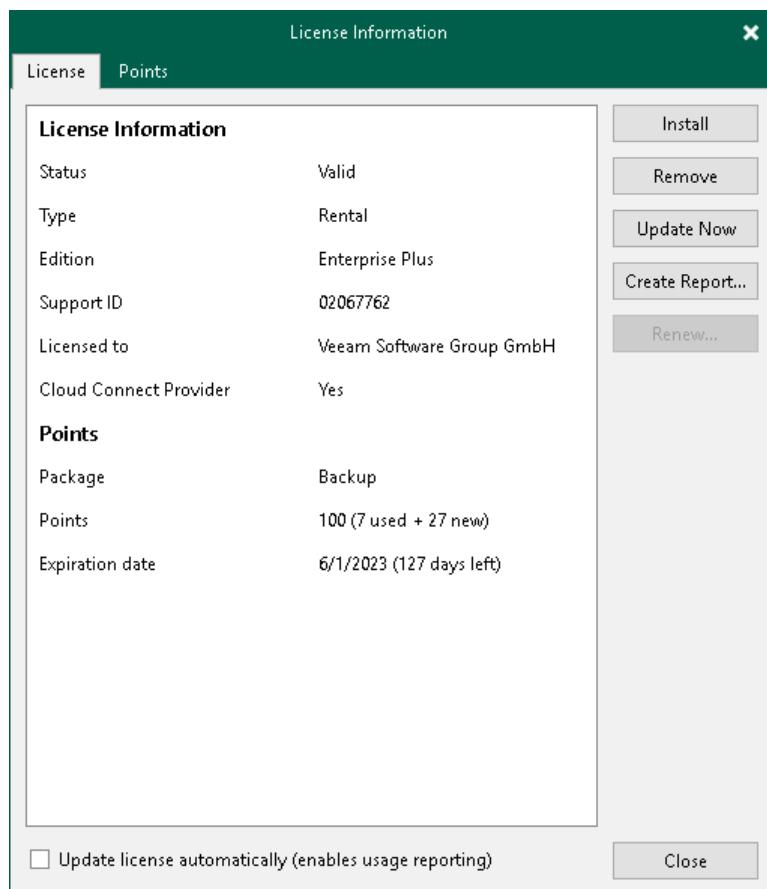
Installing License

When you install Veeam Backup & Replication on the SP side, you must specify a path to the *Veeam Cloud Connect license* file (LIC) that you have obtained from Veeam. If the SP manages tenant workloads, you also need to install Veeam Backup & Replication on the tenant side and specify a path to the *Rental Veeam Backup & Replication license* file. You can skip this step and install the license when the product is set up.

To view information about the currently installed license, select **License** from the main menu of the Veeam Backup & Replication console.

To install a new license or change the license:

1. From the main menu, select **License**.

2. In the **License Information** window, in the **License** tab, click **Install** and specify a path to the license file.

Updating License

Veeam Cloud Connect license and *Rental Veeam Backup & Replication license* support automatic license update. Instead of installing the license file manually after updates to the license, you can instruct Veeam Backup & Replication to communicate with the Veeam licensing server, download the license file from it and install the new license on the Veeam backup server.

> **IMPORTANT**
>
> Enabling license auto update activates Automatic License Usage Reporting. You cannot use license auto update without automatic usage reporting.

The new license key differs from the previously installed license key in the license expiration date and support expiration date. If you obtain a license for a new (for example, greater) number of points, the **Points** counter in the new license also displays the new number of licensed points.
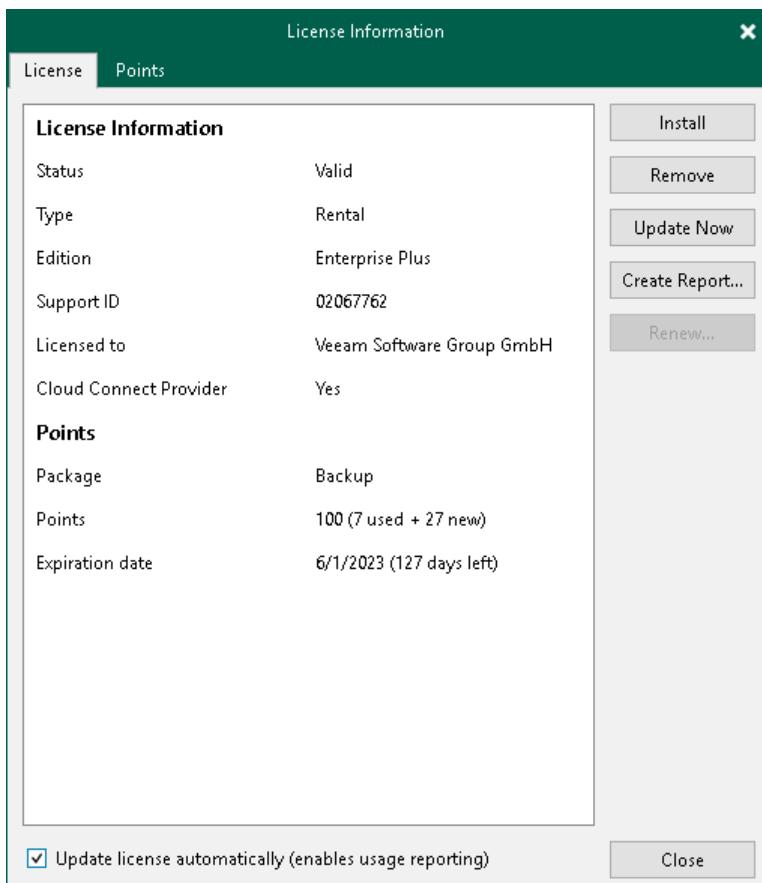
To learn more about the automatic license update process, see the Updating License Automatically section in the Veeam Backup & Replication User Guide.

By default, the automatic license update feature is deactivated. To enable it, do the following:

1. From the main menu, select **License**.

2. In the **License Information** window, in the **License** tab, select the **Update license automatically** check box.

> **TIP**
>
> If you do not want to enable automatic license update, after you obtain a new license, you can click the **Update Now** button to update the license manually.

Tenant Machine Count

Veeam Backup & Replication offers several ways to view information about protected tenant workloads — machines processed by tenant jobs targeted at cloud repositories and cloud hosts.

- **License**. The SP can view the number of tenant machines that consume points in the license. To learn more, see Viewing License Information.

- **License usage report**. Veeam Backup & Replication displays the number of tenant machines that use points in the license in the license usage report. The SP can view monthly reports generated automatically by Veeam Backup & Replication or generate the report manually when needed. To learn more, see Managing License Usage Reports.

The SP can also use Veeam PowerShell and Veeam Backup Enterprise Manager REST API to obtain information about protected tenant workloads.

- Veeam PowerShell displays the total number of tenant machines (excluding rental machines and new workloads) that have been processed by Veeam Backup & Replication in the past 31 days and use points in the license. To learn more, see the Get-VBRCloudTenant section in the Veeam PowerShell Reference.

- Veeam Backup Enterprise Manager REST API displays the number of machines per tenant that have been processed by Veeam Backup & Replication in the past 31 days and use points in the license. The number of rental machines and the number of new workloads are displayed separately for each tenant. To learn more, see the following sections in the Veeam Backup Enterprise Manager REST API Reference:

    o /cloud/tenants/{ID}

    o GET /cloud/tenants/{ID}/freelicenseCounters

> **NOTE**
>
> Consider the following:
>
> - If the SP manages the Veeam backup infrastructure using Veeam Service Provider Console, they can view information about protected tenant workloads in Veeam Service Provider Console. For more information, refer to the Veeam Service Provider Console documentation.
>
>   For example, if you use Veeam Service Provider Console REST API v3, see the Get All Companies and Get Usage of Veeam Backup & Replication Licenses by Tenant sections in the Veeam Service Provider Console REST API Reference.
>
> - The SP can also view the number of tenant machines whose backups and replicas consume resources in the SP Veeam Cloud Connect infrastructure. Veeam Backup & Replication displays this information in the **Tenants** node of the **Cloud Connect** view in the SP backup console. To learn more, see Viewing Resource Consumption by Tenant Machines.

Viewing License Information

You can view information about protected tenant workloads in the **License Information** window.

To view license information:

1. From the main menu, select **License**.

2. In the **License Information** window, click the **Points** tab.

3. View information about protected tenant workloads. Veeam Backup & Replication displays information about workloads of the following types:

   o *Cloud Connect (VMs)* — VMs backed up to a cloud repository by backup jobs configured in Veeam Backup & Replication.

   o *Cloud Connect (Replicas)* — VMs replicated to a cloud host by replication jobs configured in Veeam Backup & Replication.

   o *Cloud Connect (Workstations)* — physical or virtual workstations backed up to a cloud repository by Veeam Agent backup jobs configured Veeam Agent or Veeam Backup & Replication.

   o *Cloud Connect (Servers)* — physical or virtual servers backed up to a cloud repository by Veeam Agent backup jobs configured in Veeam Agent or Veeam Backup & Replication.

Reducing Number of Used Points

The number of used points in the *Veeam Cloud Connect license* can reduce for one of the following reasons:

- The SP removes a tenant account. As a result, all workloads of the tenant stop using points in the Veeam Cloud Connect license, and the number of points used by the tenant workloads is revoked for other tenants. To learn more, see Deleting Tenant Accounts.

- The SP resets the machine count for the tenant. As a result, the number of tenant machines stop using points in the Veeam Cloud Connect license, and the equal number of points is revoked for this tenant or other tenants. To learn more, see Resetting Tenant Machine Count.

- A tenant removes backups and replicas created for one or several machines on the cloud repository and cloud host. As a result, the number of machines for which backups and replicas were deleted stop using points in the SP license, and the equal number of points is revoked for this tenant or other tenants. However, when a tenant runs a job that processes a machine for which backup and replica were deleted, such a machine starts using points in the license, and the number of used points in the Veeam Cloud Connect license increases.

To reduce the number of used points in a *Rental Veeam Backup & Replication license* installed on a tenant backup server, the SP can revoke the license from some workloads. The revoke procedure does not differ from the one for a regular per-instance license. To learn more, see the Revoking License section in the in the Veeam Backup & Replication User Guide.

Resetting Tenant Machine Count

To revoke tenant machines from the license, the SP can reset the tenant machine count. Tenant machine count reset can be useful in the following situations:

- The tenant re-installs Veeam Backup & Replication or deploys a new Veeam Backup & Replication database. In this situation, Veeam Backup & Replication does not automatically revoke tenant machines from the license. If the tenant wants to back up or replicate the same machines with a new Veeam Backup & Replication instance, these machines will get new IDs and will be considered as new protected workloads. As a result, the same machines will use points in the license twice.

- The number of used points has exceeded the number of points in the license. The SP can revoke tenant machines for some time, until the SP gets a new license for a greater number of machines. Tenant machines are revoked on a temporary basis. When the tenant starts a backup, backup copy or replication job, machines processed by these jobs become protected workloads and consume the license.

- The tenant has a dynamic virtual infrastructure. For example, if the tenant constantly creates and deletes VMs, the SP can control the number of points used by these VMs.
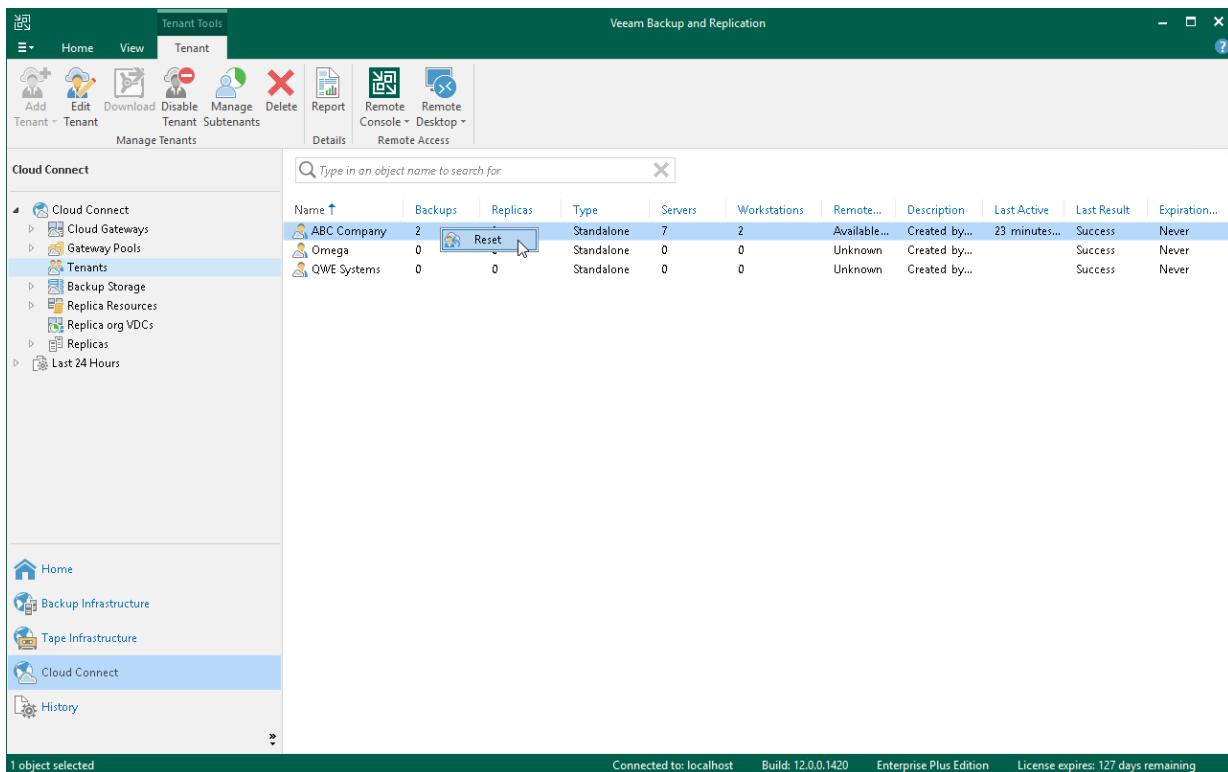
When the tenant machine count is reset, tenant machines whose backups and replicas are stored on the cloud repository and cloud hosts are "removed" from the license. The SP can provide the cloud service for the equal number of machines to other tenants or the same tenant.

Machine count reset applies to the license only and does not remove information about tenant machines from the SP Veeam backup console. This lets the SP monitor tenant quota consumption. After the SP resets the tenant machine count, they can still view the number of machines processed by the tenant in the **Tenants** node of the **Cloud Connect** view. To learn more, see Viewing Resource Consumption by Tenant Machines.

Machine count reset does not remove tenant backups from the cloud repository. The tenant can restore data from such backups. Tenant VM replicas also remain on the cloud host when the tenant machine count is reset.

To reset the tenant machine count:

1. Open the **Cloud Connect** view.

2. In the inventory pane, click the **Tenants** node.

3. In the working area, select the necessary tenant account.

4. Press and hold the **[CTRL]** key, right-click the tenant account and select **Reset**.

License Usage Reporting

The SP must periodically submit a license usage report. This process happens monthly, starting from the first day of the month.

- For the *Veeam Cloud Connect license*, the SP reports the number of used points (excluding points used by new workloads). The report also contains the license information and the number of machines backed up and replicated per tenant. The report serves as a basis for issuing invoices for the Veeam Cloud Connect rental program.

  The report does not include rental machines. To learn more, see Rental Machines Licensing.

- For the *Rental Veeam Backup & Replication license*, the SP reports the number of used points (excluding points used by new workloads). The report also contains the license information, the number of processed machines (VMs, workstations and servers) and information about machines and jobs that process these machines.

Veeam Backup & Replication allows the SP to submit license usage reports from the Veeam backup console. Keep in mind, however, that license usage reporting through the product UI does not replace other reporting processes. For example, if the SP uses Veeam Service Provider Console to manage the Veeam backup infrastructure, they collect license usage reports in Veeam Service Provider Console and submit reports using the VCSP Pulse portal (or an aggregator reporting portal). For more information, see Veeam Rental Licensing and Usage Reporting Guide.

Veeam Backup & Replication offers two methods of license usage reporting:

- **Automatic reporting** — the recommended usage reporting method. The method is used when license auto update is enabled. To learn more, see Automatic License Usage Reporting.

- **Manual reporting** — the usage reporting method intended for Veeam backup servers that do not have permanent connection to the internet. Manual reporting is used when license auto update is disabled. To learn more, see Manual License Usage Reporting.

The SP can review and adjust the usage report before submitting it to Veeam. To learn more, see Managing License Usage Reports.

> **NOTE**
>
> In the MSP Backup scenario, if the same *Rental Veeam Backup & Replication license* is installed on multiple tenant backup servers, the SP must send individual license usage reports from each backup server. If tenant backup servers are connected to Veeam Backup Enterprise Manager, a single report containing license usage information from each backup server will be generated on the Veeam Backup Enterprise Manager server. In this case, the SP must send information about the license usage from Veeam Backup Enterprise Manager.
>
> If the SP uses Veeam Service Provider Console to manage the Veeam backup infrastructure, they collect license usage reports in Veeam Service Provider Console. To learn more, see Veeam Rental Licensing and Usage Reporting Guide.

Automatic License Usage Reporting

When license auto update is enabled for the *Veeam Cloud Connect license* or *Rental Veeam Backup & Replication license*, license usage reporting is performed in the following way:

1. Veeam Backup & Replication collects statistics on the current license usage and sends it periodically to the Veeam License Update server on the web (autolk.veeam.com). The collected data includes information on the maximum number of points used over the past week (high watermark). New workloads and rental machines are not included in the weekly statistics. The process runs in the background mode, once a week at a random time and day.

2. On the first day of the new month (at 12:00 AM GMT), Veeam Backup & Replication generates a report based on the current number of used points. The report is saved to the `Reports` subfolder in the log folder on the Veeam backup server. The default path to the folder is `%ProgramData%\Veeam\Backup\Reports`.

   > **NOTE**
   >
   > Consider the following:
   >
   > - [For the Rental Veeam Backup & Replication license] If the backup server is connected to Veeam Backup Enterprise Manager that is deployed on a dedicated server, the report is saved to the log folder on the Veeam Backup Enterprise Manager server. The default path to the folder is `%ProgramData%\Veeam\Backup\Reports`.
   > - You can change the default path to the log folder with a registry key. For more information, contact Veeam Customer Support. After you change the default path, license usage reports will be saved to the new path.
   > - If the SP uses Veeam Service Provider Console to manage the Veeam backup infrastructure, they collect license usage reports in Veeam Service Provider Console. For more information, see Veeam Rental Licensing and Usage Reporting Guide.

3. Veeam Backup & Replication informs the SP about the generated report with the notification window in the Veeam Backup & Replication console.

4. The SP can review, adjust if necessary and send the report to Veeam. The SP can also postpone the sending of the report. To learn more, see Managing License Usage Reports.

   If the SP doesn't send the report, on the eleventh day of the month, Veeam Backup & Replication will send the report automatically.

   Keep in mind that automatic license usage reporting does not replace manual reporting through the VCSP Pulse portal (or an aggregator reporting portal). For more information, see Veeam Rental Licensing and Usage Reporting Guide.

By comparing the number of points in the monthly report with the automatically collected weekly statistics, Veeam can make a decision on whether to allow license update for the SP. If the monthly usage report does not deviate from the highest watermark value significantly, the SP license will be updated.

Manual License Usage Reporting

When license auto update is disabled for the *Veeam Cloud Connect license* or *Rental Veeam Backup & Replication license*, license usage reporting is performed in the following way:

1. On the first day of the new month (at 12:00 AM GMT), Veeam Backup & Replication generates a report based on the current license usage. The report is saved to the `Reports` subfolder in the log folder on the Veeam backup server. The default path to the folder is `%ProgramData%\Veeam\Backup\Reports`.

   > **NOTE**
   >
   > Consider the following:
   >
   > - [For the Rental Veeam Backup & Replication license] If the backup server is connected to Veeam Backup Enterprise Manager that is deployed on a dedicated server, the report is saved to the log folder on the Veeam Backup Enterprise Manager server. The default path to the folder is `%ProgramData%\Veeam\Backup\Reports`.
   > - You can change the default path to the log folder with a registry key. For more information, contact Veeam Customer Support. After you change the default path, license usage reports will be saved to the new path.
   > - If the SP uses Veeam Service Provider Console to manage the Veeam backup infrastructure, they collect license usage reports in Veeam Service Provider Console. For more information, see Veeam Rental Licensing and Usage Reporting Guide.

2. Veeam Backup & Replication informs the SP about the generated report with the notification window in the Veeam Backup & Replication console.

3. The SP can review, adjust if necessary and save the report locally for future submission. To learn more, see Managing License Usage Reports.

> **IMPORTANT**
>
> In case of manual reporting, Veeam Backup & Replication does not automatically send monthly license usage reports. The SP must send the report to Veeam before the day defined by the agreement with Veeam or the Aggregator (if any is involved). The default day is the tenth day of the month.

Managing License Usage Reports

On the first day of the month, Veeam Backup & Replication generates a license usage report. The report is based on the current number of used points. The SP can perform the following actions with the license usage report:

- [For automatic reporting] Submit the license usage report to Veeam

- Review the license usage report

- Save the license usage report

- Adjust the number of processed VMs in the report

- Postpone the review of the report

The SP can also generate the report manually to view information about current license usage. To learn more, see Generating License Usage Report.
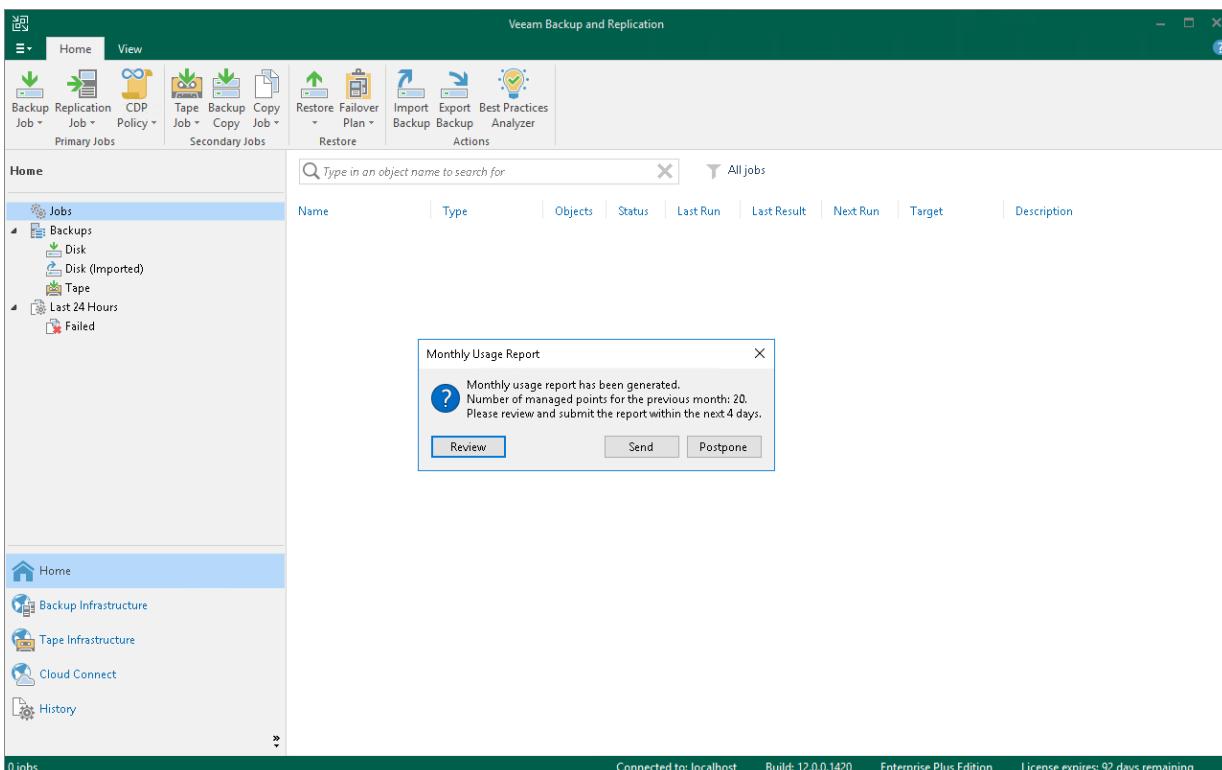
Submitting License Usage Report

On the first day of the month, when you launch the Veeam Backup & Replication console, a window opens notifying that the license usage report has been generated. The notification reflects the number of used points for the previous month. The notification also displays the number of days within which the report must be submitted.

In case of automatic license usage reporting, you can submit the report immediately without review. To submit the report, click **Send**.

> **NOTE**
>
> Submission of the license usage report from the Veeam Backup & Replication console is not available for manual reporting.

Reviewing License Usage Report

You can review a license usage report before sending it to Veeam. To review a report:

1. Open the **Monthly Usage Report** window:

   o [For automatic reporting] In the notification window informing that the report is generated, click **Review**.

   o [For manual reporting] In the notification window informing that the report is generated, click **Review Now**.

2. In the **Monthly Usage Report** window, check the number of reported points.

   o For the Veeam Cloud Connect license, the report contains the following data:

   ▪ License information: Veeam Backup & Replication edition, license expiration date, name of the company to which the license was issued, support ID and installation ID.

   ▪ The number of points used by each type of protected workloads (backed-up and replicated VMs, workstations and servers) and the total number of used points.

   ▪ For each type of protected workloads, the report displays the number of points used by each tenant.

   ▪ For each type of protected workloads, the report also displays the number of new objects that are not included in the report.

- o For the Rental Veeam Backup & Replication license, the report contains the following data:

  - License information: Veeam Backup & Replication edition, license expiration date, name of the company to which the license was issued, support ID and installation ID.

  - The number of points used by each type of protected workloads (VMs, servers and workstations) and the total number of used points.

  - For each type of protected workloads, the report displays information about processed machines and jobs that process these machines.

  - For each type of protected workloads, the report also displays the number of new objects that are not included in the report.

In case of automatic license usage reporting, you can submit the report immediately after review. To submit the report, in the **Monthly Usage Report** window, click **Send**.

You can save the report to the specified folder. To learn more, see Saving License Usage Report.

If you want to change the number of reported VMs, you can adjust the report. To learn more, see Adjusting License Usage Report.

Saving License Usage Report

If you perform manual license usage reporting, you must save the license usage report after review for future submission. You can also save the report in case of automatic reporting, for example, to keep a copy of the report in the desired folder. You can choose to save the report to a file in the PDF format or JSON format.

To save a license usage report:

1. Open the **Monthly Usage Report** window:

   o [For automatic reporting] In the notification window informing that the report is generated, click **Review**.

   o [For manual reporting] In the notification window informing that the report is generated, click **Review Now**.

2. In the **Monthly Usage Report** window, click **Save As**.

3. In the **Save As** window, browse to the folder to which you want to save the report, specify a name and format for the file of the report and click **Save**.

Adjusting License Usage Report

You can change the number of reported VMs before submitting a license usage report. The process of license usage report adjustment differs depending on the type of license that you use — *Veeam Cloud Connect license* or *Rental Veeam Backup & Replication license*.

Adjusting Usage Report for Veeam Cloud Connect License

You can reduce the number of VMs in a license usage report for the Veeam Cloud Connect license. You can adjust the number of backed-up and replicated VMs individually for every tenant. For every change in the report, you must specify a reason.

> **NOTE**
>
> In the monthly usage report, you cannot change the number of workstations and servers for which tenants have created Veeam Agent backups in the cloud repository.
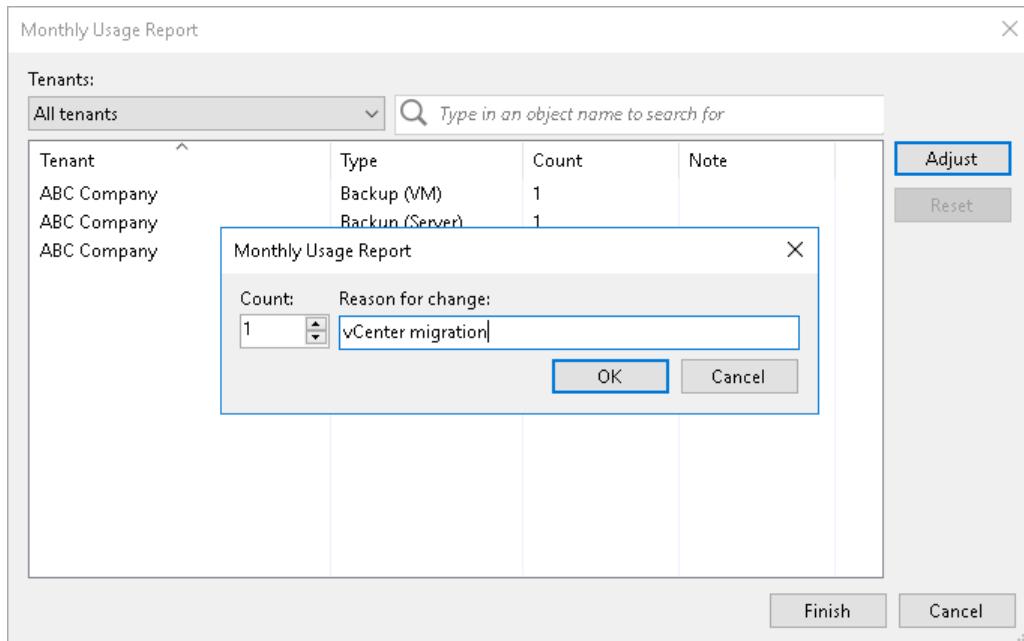
To adjust a report:

1. Open the **Monthly Usage Report** window:

   o [For automatic reporting] In the notification window informing that the report is generated, click **Review**.

   o [For manual reporting] In the notification window informing that the report is generated, click **Review Now**.

2. In the **Monthly Usage Report** window, click **Adjust**.

3. In the list of tenants, select the tenant for which you want to change the number of VMs and click **Adjust**.

   By default, the list of tenants contains names of all tenant accounts whose VMs are included in the report. To quickly find the necessary tenant, you can use the search field at the top of the window. You can also select the tenant account from the drop-down list in the **Tenants** field.

4. In the displayed window, in the **Count** field, change the number of reported VMs.

5. In the **Reason for change** field, provide a reason for adjusting the number of reported VMs.

6. Click **OK**, then click **Finish**. The change will be reflected in the report.

> **TIP**
>
> To reset changes introduced in the report, in the report adjustment window, click **Reset**.

Adjusting Usage Report for Rental License

You can remove specific managed VMs from a license usage report for the *Rental Veeam Backup & Replication license*. When you remove a VM from the report, you can also remove this VM from all jobs to which this VM is added. For every VM removal, you must specify a reason.
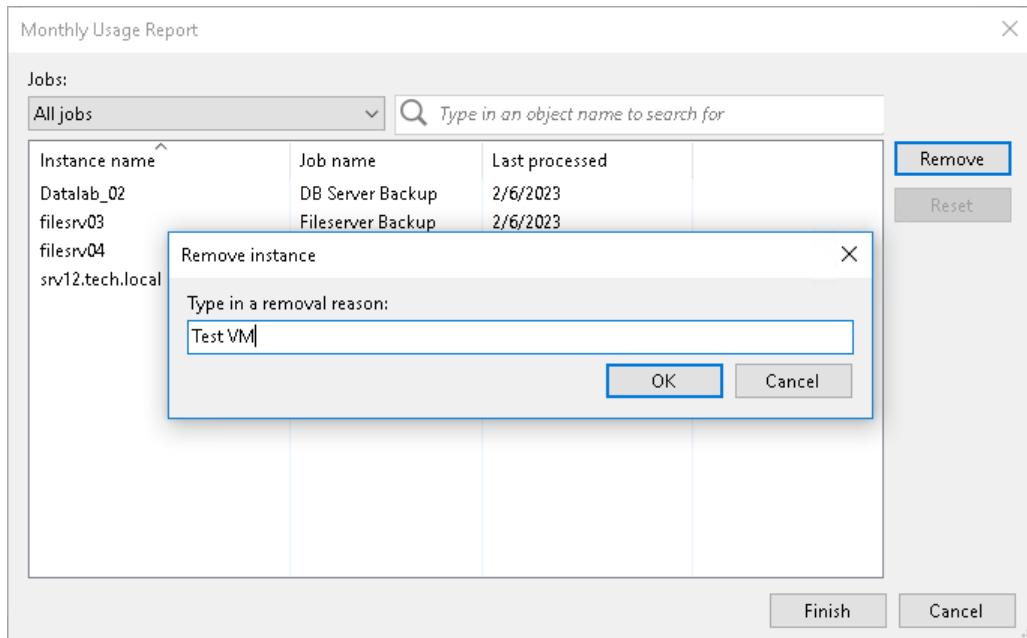
To adjust a report:

1. Open the **Monthly Usage Report** window:

   o [For automatic reporting] In the notification window informing that the report is generated, click **Review**.

   o [For manual reporting] In the notification window informing that the report is generated, click **Review Now**.

2. In the **Monthly Usage Report** window, click **Adjust**.

3. In the list of VMs, select the VM that you want to remove from the report and click **Remove**.

   By default, the list of VMs contains all managed VMs included in the report. To quickly find the necessary VM, you can use the search field at the top of the window. You can also select a job from the drop-down list in the **Jobs** field to view a list of VMs added to a specific job.

4. In the displayed window, in the **Type in a removal reason** field, provide a reason for removing the VM from the report.

5. Click **OK**, then click **Finish**. The change will be reflected in the report.

> **TIP**
>
> To reset changes introduced in the report, in the report adjustment window, click **Reset**.
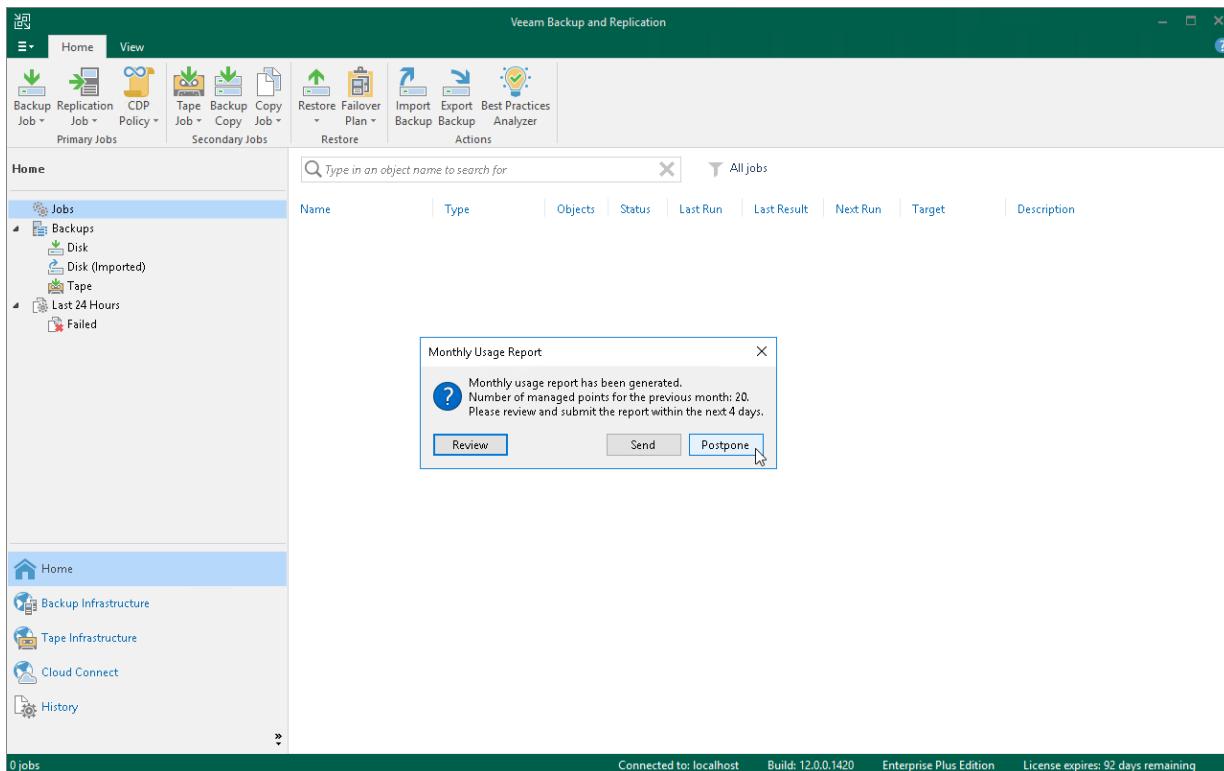
Postponing License Usage Report Review

You can postpone the license usage report review. When you postpone the report review, Veeam Backup & Replication will close the *Monthly Usage Report* notification window. Veeam Backup & Replication will display this notification every time you open the Veeam Backup & Replication console until the report is sent to Veeam.

For automatic license usage reporting, if you do not send the report to Veeam within 10 days, Veeam Backup & Replication will send the report automatically on the eleventh day of the month. If you perform manual reporting, you must send the report before the day defined by the agreement with Veeam or your Aggregator (if any is involved). The default day is the tenth day of the month.

To postpone the report review:

- [For automatic reporting] In the notification window informing that the report is generated, click **Postpone**.

- [For manual reporting] In the notification window informing that the report is generated, click **Postpone Review**.

Generating License Usage Report

The SP can manually generate a license usage report. In contrast to periodic license usage reports that reflect license usage for the previous calendar month, the manually generated report reflects license usage for the last 31 days prior to the time when the report was generated. The report helps the SP monitor current license usage: the SP can generate a report on a specific day of the month, compare the current report with the previous monthly report and predict license usage that will be reflected in the next monthly report.
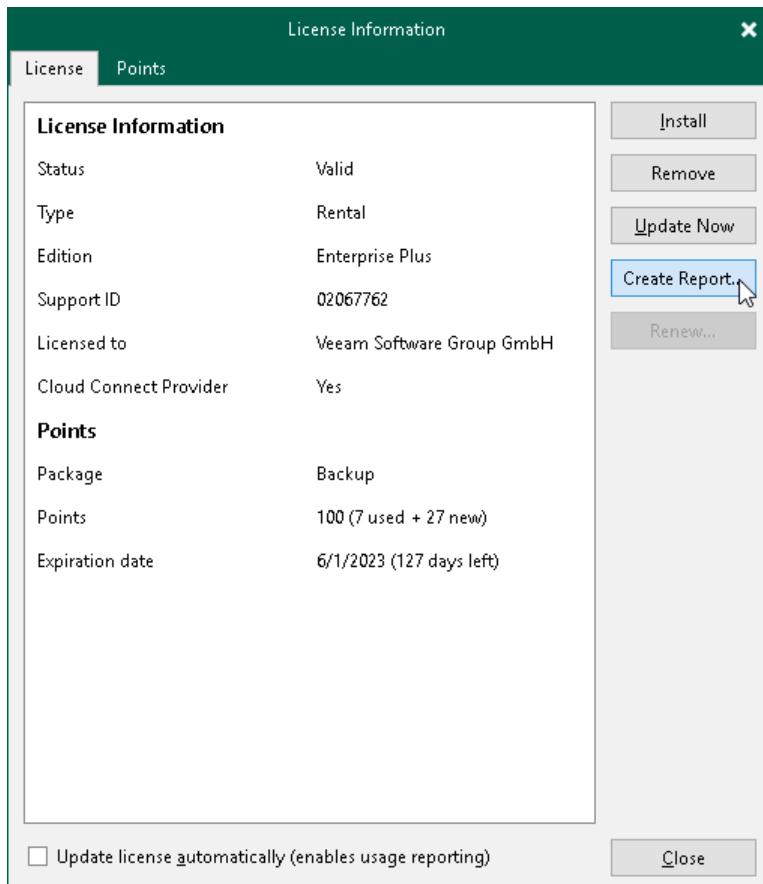
The report displays information about current license usage in the similar way as the monthly usage report. The report contains the following data:

- License information: Veeam Backup & Replication edition, license expiration date, name of the company to which the license was issued and support ID.

- The number of instances used by each type of protected workloads (backed-up and replicated VMs, workstations and servers) and the total number of used instances.

- For each type of protected workloads, the report displays the number of instances used by each tenant.

- For each type of protected workloads, the report also displays the number of new objects that are not included in the report.

The SP cannot submit a manually generated license usage report to Veeam. This report is intended for monitoring purposes only.

To generate a license usage report:

1. From the main menu, select **License**.

2. In the **License Information** window, in the **License** tab, click **Create Report**.

Guide for Service Providers

The Veeam Cloud Connect Administrator Guide is intended for SPs who expose cloud repository resources and provide disaster recovery as a service to their customers using the Veeam Cloud Connect functionality in Veeam Backup & Replication. The Administrator Guide describes main tasks that the SP must take to set up the necessary infrastructure and manage it, and provides information about licensing specifics for SPs.

Setting Up SP Veeam Cloud Connect Infrastructure

As part of the Veeam Cloud Connect infrastructure configuration process, the SP can perform the following tasks:

- Deploy the SP Veeam backup server.
- Manage TLS certificates.
- Add cloud gateways and cloud gateway pools.
- Configure cloud repositories.
- Configure hardware plans.
- Manage VLANs.
- Manage public IP addresses.
- Manage network extension appliance credentials.
- Register tenant accounts.
- Configure target WAN accelerators.
- Deploy Veeam Cloud Connect Portal.

Deploying SP Veeam Backup Server

To deploy the SP Veeam backup server, you must install Veeam Backup & Replication on a Microsoft Windows server on the SP side.

The installation process of Veeam Backup & Replication in the Veeam Cloud Connect infrastructure is the same as the installation process in a regular Veeam backup infrastructure. To learn more about system requirements, required permissions and the installation process workflow, see the Deployment section in the Veeam Backup & Replication User Guide.

In addition to requirements listed in the product documentation, the SP Veeam backup server must meet the following requirements:

1. On the SP Veeam backup server, a Veeam Cloud Connect license must be installed. Other types of licenses do not support the Veeam Cloud Connect functionality.

2. The SP Veeam backup server must have access to all components of the Veeam Cloud Connect infrastructure deployed on the SP side. These include:

   o Backup repositories that will be used as cloud repositories

   o Managed servers that will be used for configuring replication resources (cloud hosts)

   o Cloud gateways

   o [Optional] Target WAN accelerators

3. If the SP plans to use Veeam Backup for Microsoft Office 365 to provide Mail Backup as a Service to tenants, the SP must install Veeam Backup for Microsoft Office 365 on the SP backup server. The SP backup server and Veeam Backup for Microsoft Office 365 backup proxy should be in the same (or trusted) domain. For further information, refer to the Veeam Backup for Microsoft Office 365 User Guide.

> **IMPORTANT**
>
> It is recommended that the SP regularly creates encrypted backups of the SP Veeam backup server configuration database. With the encryption option enabled, Veeam Backup & Replication will include in the configuration backup passwords for tenant accounts created on the SP backup server. As a result, if the configuration data becomes corrupted for some reason, after configuration restore, the SP will not have to specify new passwords for registered tenant accounts.
>
> To learn more, see the Creating Encrypted Configuration Backups section in Veeam Backup & Replication User Guide.

Managing TLS Certificates

The procedure of TLS certificate creation and management is performed by the SP on the SP Veeam backup server.

When you deploy the Veeam Cloud Connect infrastructure, you must first specify what TLS certificate must be used to establish a secure connection between parties. Veeam Backup & Replication offers the following options for TLS certificates:

- You can use Veeam Backup & Replication to generate a self-signed TLS certificate. To learn more, see Generating Self-Signed Certificates.

- You can select an existing TLS certificate from the certificates store. To learn more, see Importing Certificates from Certificate Store.

- You can import a TLS certificate from a file in the PFX format. To learn more, see Importing Certificates from PFX Files.

> **NOTE**
>
> After you specify TLS certificate settings in the Veeam Cloud Connect infrastructure, when you launch the **Manage Certificate** wizard once again, Veeam Backup & Replication also offers an option to keep the currently used certificate. To do this, select the **Keep existing certificate** option at the **Certificate Type** step of the wizard.
>
> You can use this option to check information about the currently installed certificate, such as name, expiration date, thumbprint and serial number.

Generating Self-Signed Certificates

You can use Veeam Backup & Replication to generate a self-signed certificate for authenticating parties in the Veeam Cloud Connect infrastructure.

To generate TLS certificates, Veeam Backup & Replication employs the RSA Full cryptographic service provider by Microsoft Windows installed on the Veeam backup server. The created TLS certificate is saved to the *Shared* certificate store. The following types of users can access the generated TLS certificate:

- User who created the TLS certificate

- LocalSystem user account

- Local Administrators group
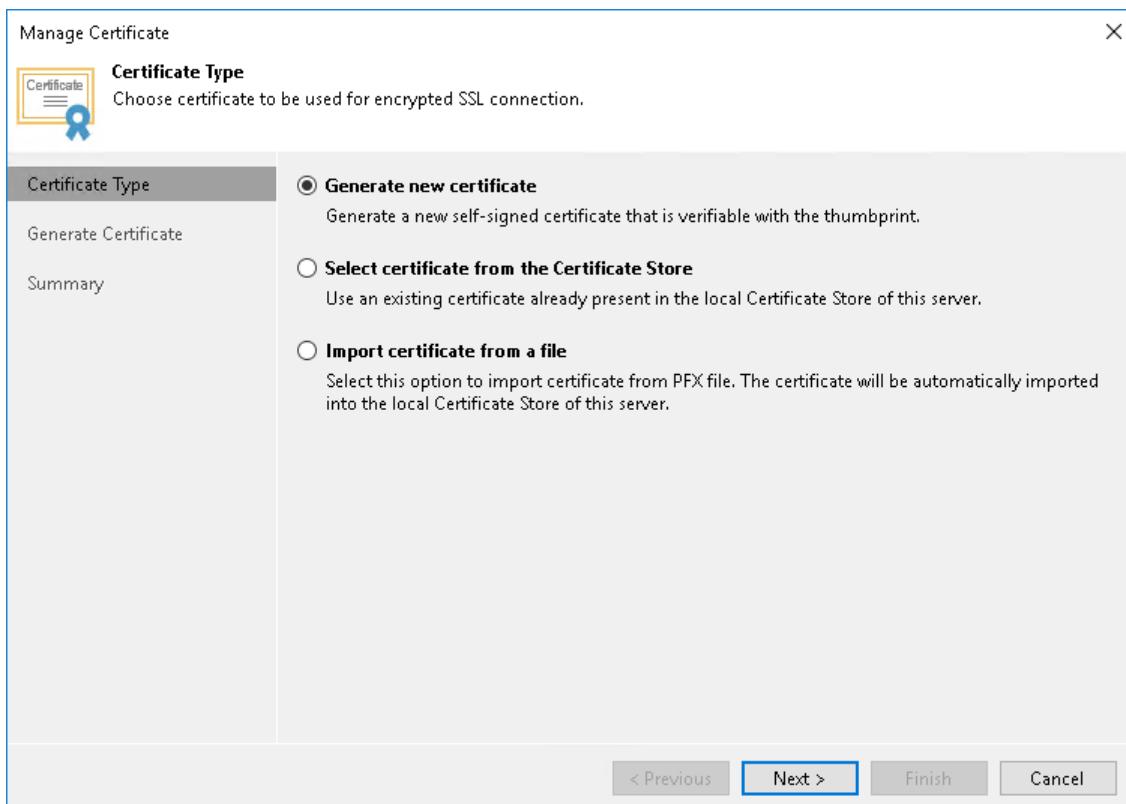
If you use a self-signed TLS certificate generated by Veeam Backup & Replication, you do not need to take any additional actions to deploy the TLS certificate on the tenants side. When the tenant adds the SP to Veeam Backup & Replication, a matching TLS certificate with a public key is installed on the tenant Veeam backup server automatically. During the procedure of SP adding, Veeam Backup & Replication retrieves the TLS certificate with a public key from the SP Veeam backup server and saves this TLS certificate to the Veeam Backup & Replication database used by tenant Veeam backup server. Veeam Backup & Replication gets the saved TLS certificate from the database when needed.
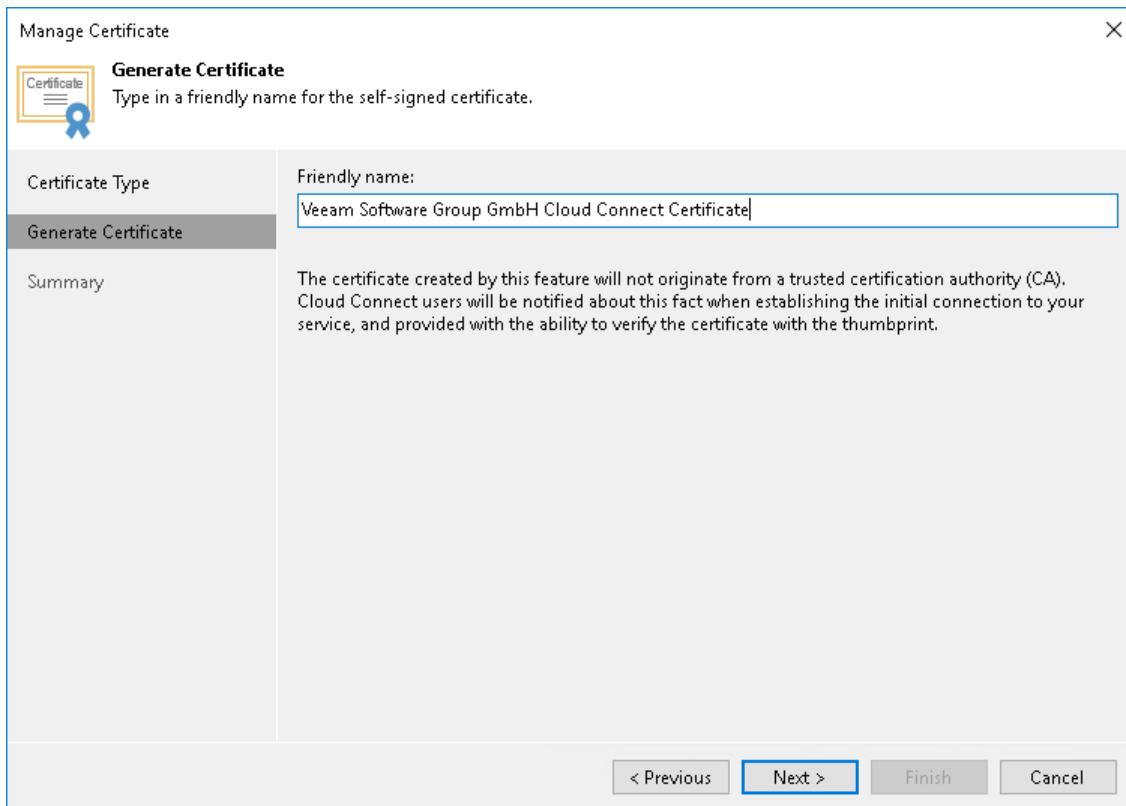
> **NOTE**
>
> When you generate a self-signed TLS certificate with Veeam Backup & Replication, you cannot include several aliases to the certificate and specify a custom value in the *Subject* field. The *Subject* field value is taken from the Veeam Backup & Replication license installed on the Veeam backup server.

To generate a self-signed TLS certificate:
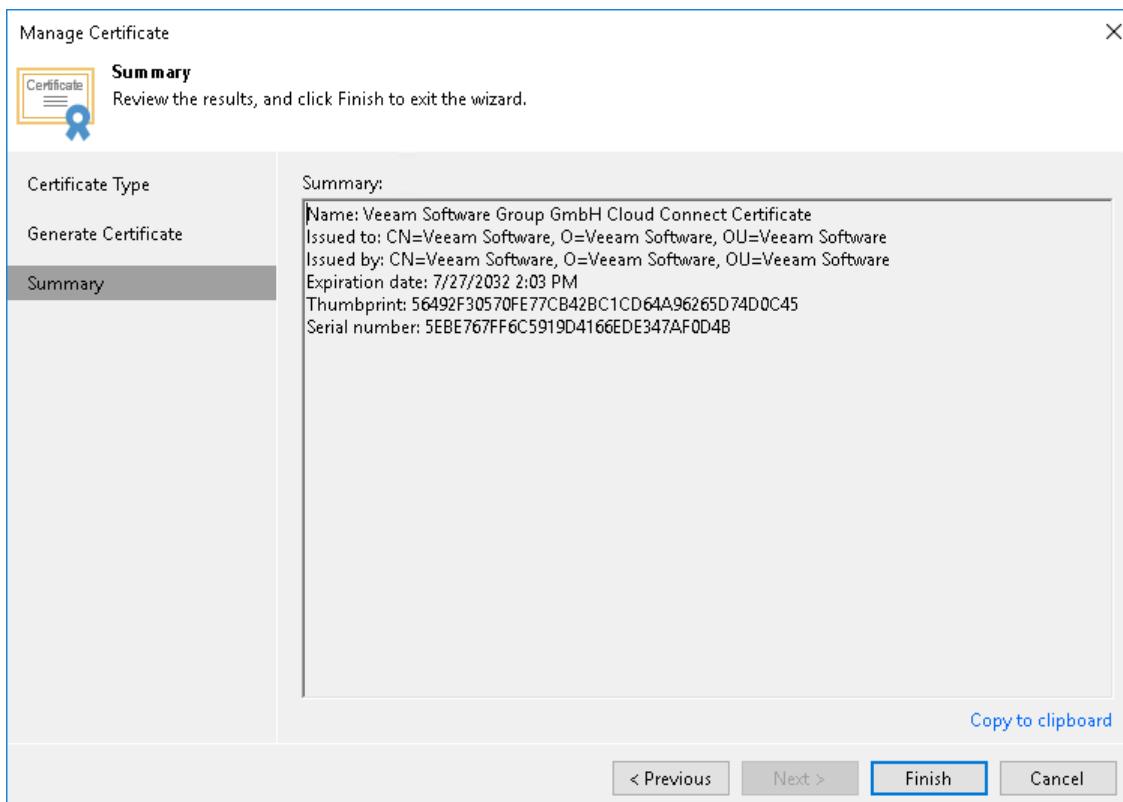
1. Open the **Cloud Connect** view.

2. Click the **Cloud Connect** node in the inventory pane and click **Manage Certificates** in the working area. You can also right-click the **Cloud Connect** node in the inventory pane and select **Manage certificates**.

3. At the **Certificate Type** step of the wizard, select **Generate new certificate**.

4. At the **Generate Certificate** step of the wizard, specify a friendly name for the created self-signed TLS certificate.

5. At the **Summary** step of the wizard, review the certificate properties. Use the **Copy to clipboard** link to copy and save information about the generated TLS certificate. You can send the copied information to your tenants so that they can verify the TLS certificate with the certificate thumbprint.

6. Click **Finish**. Veeam Backup & Replication will save the generated certificate in the *Shared* certificate store on the Veeam backup server.

Importing Certificates from Certificate Store
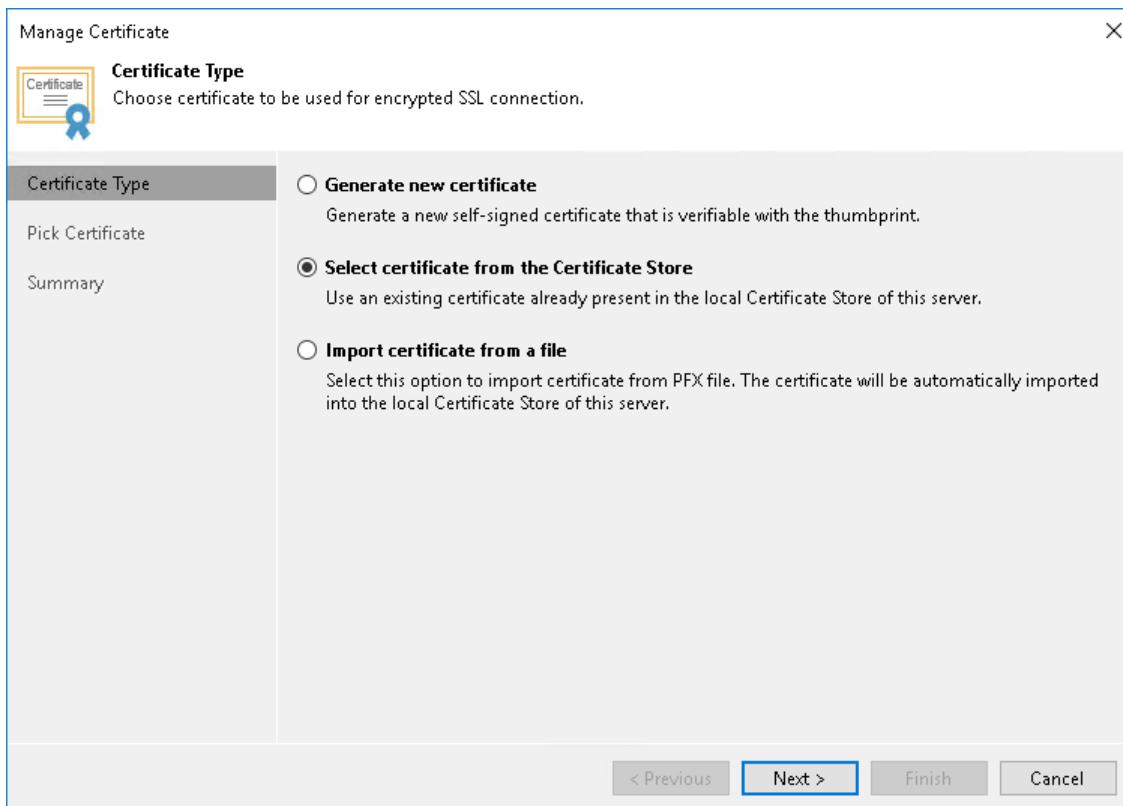
If your organization has a TLS certificate signed by a CA and the TLS certificate is located in the Microsoft Windows Certificate store, you can use this certificate for authenticating parties in the Veeam Cloud Connect infrastructure.
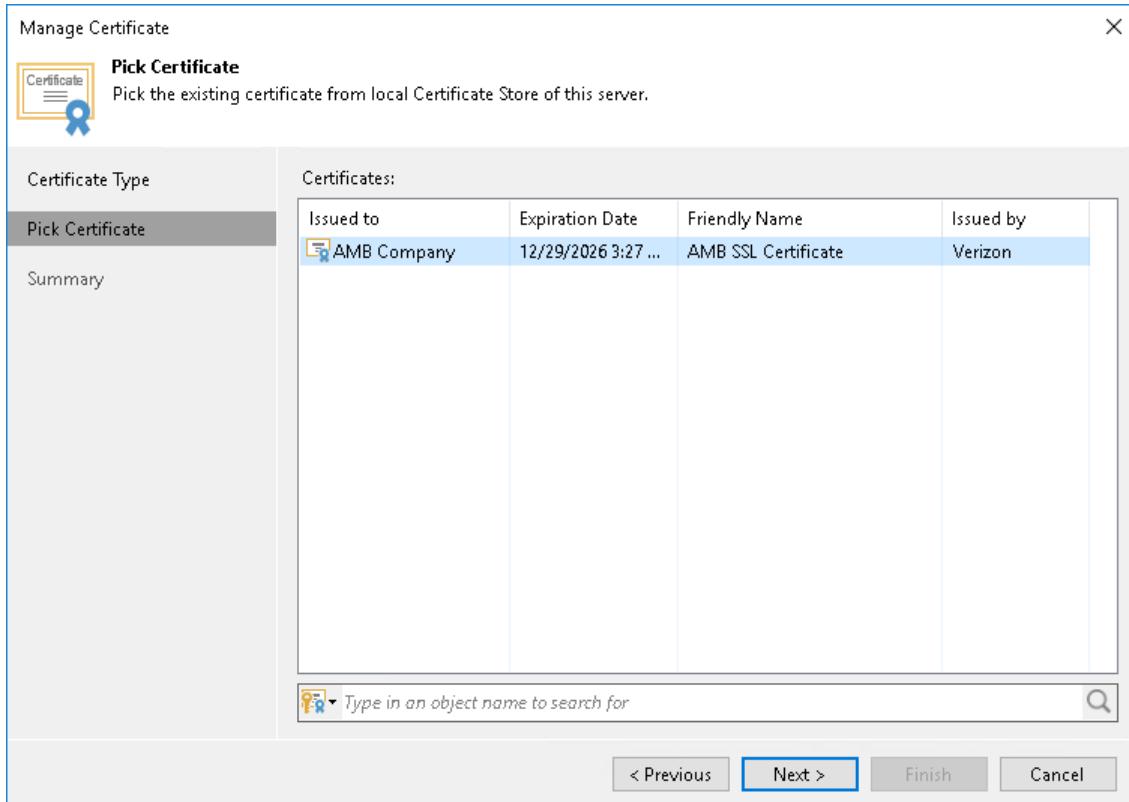
> **IMPORTANT**
>
> The account under which the Veeam Cloud Connect Service runs (by default, the Local System account) must have access to the certificate private key. In the opposite case, the certificate will not be installed.

To select a certificate from the Microsoft Windows Certificate store:

1. Open the **Cloud Connect** view.

2. Click the **Cloud Connect** node in the inventory pane and click **Manage Certificates** in the working area. You can also right-click the **Cloud Connect** node in the inventory pane and select **Manage certificates**.

3. At the **Certificate Type** step of the wizard, choose **Select certificate from the Certificate Store**.

4. At the **Pick Certificate** step of the wizard, select a TLS certificate that you want to use. The certificate must be installed in the *Local Computer\Personal* certificate store. You can select only certificates that contain both a public key and a private key. Certificates without private keys are not displayed in the list.

5. At the **Summary** step of the wizard, review the certificate properties.

6. Click **Finish** to apply the certificate.

Importing Certificates from PFX Files

You can import a TLS certificate in the following situations:

- Your organization uses a TLS certificate signed by a CA and you have a copy of this certificate in a file of PFX format.

- You have generated a self-signed TLS certificate in the PFX format with a third-party tool and you want to import it to Veeam Backup & Replication.
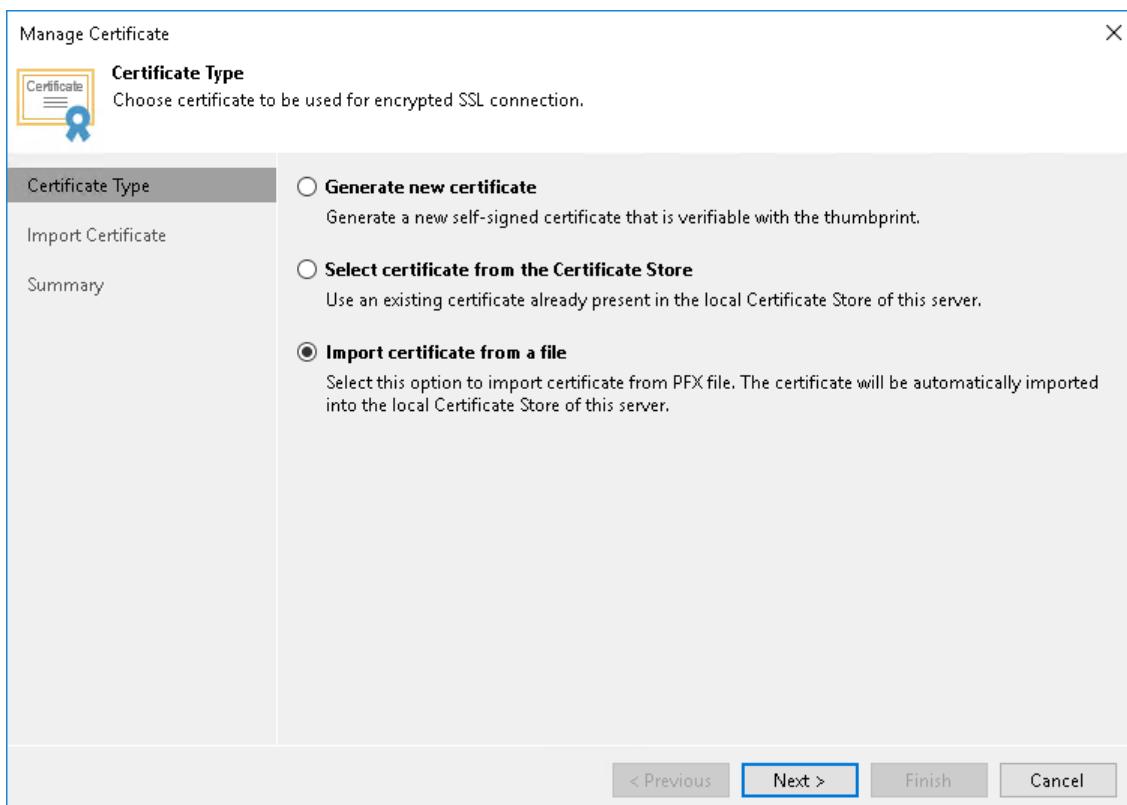
> **IMPORTANT**
>
> Consider the following:
>
> - The TLS certificate must pass validation on the SP Veeam backup server. In the opposite case, you will not be able to import the TLS certificate.
> - If a PFX file contains a certificate chain, only the end entity certificate will be imported.
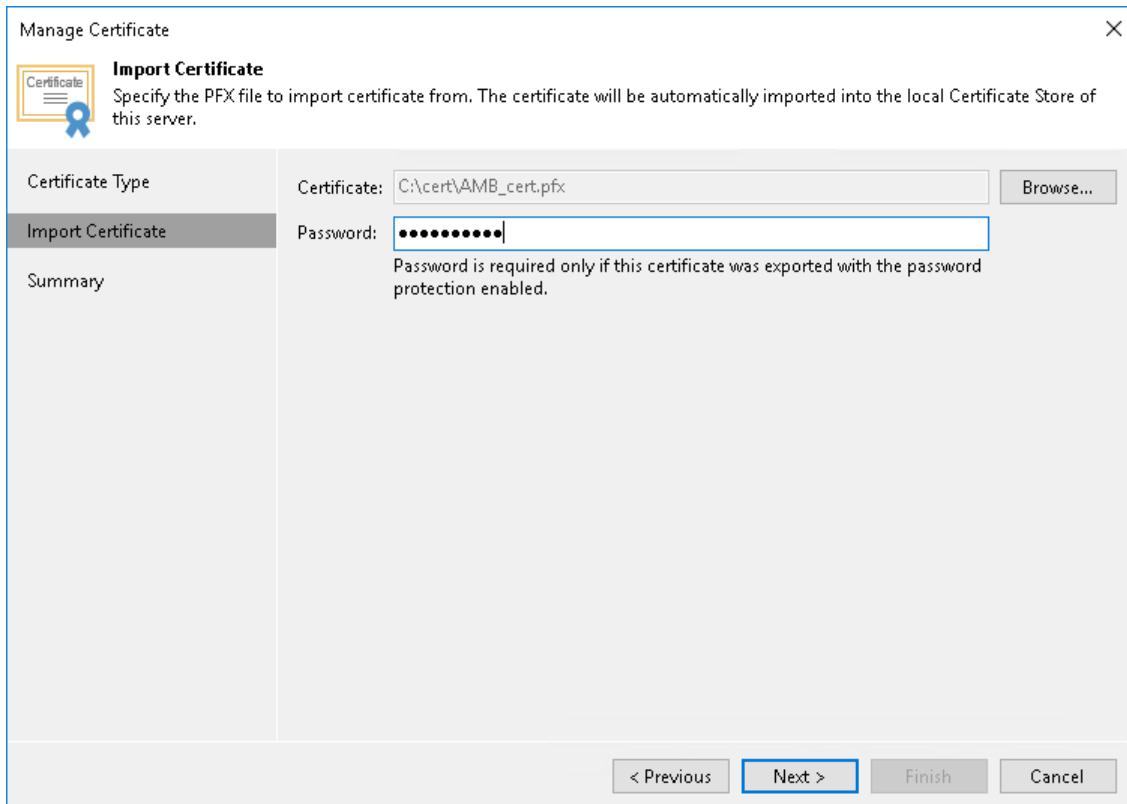
To import a TLS certificate from a PFX file:

1. Open the **Cloud Connect** view.

2. Click the **Cloud** node in the inventory pane and click **Manage Certificates** in the working area. You can also right-click the **Cloud Connect** node in the inventory pane and select **Manage certificates**.

3. At the **Certificate Type** step of the wizard, choose **Import certificate from a file**.

4. At the **Import Certificate** step of the wizard, specify a path to the PXF file.

5. If the PFX file is protected with a password, specify the password in the **Password** field.

6. At the **Summary** step of the wizard, review the certificate properties. Use the **Copy to clipboard** link to copy and save information about the TLS certificate. You can send the copied information to your tenants so that they can verify the TLS certificate with the certificate thumbprint.

7. Click **Finish** to apply the certificate.

What You Do Next

After installing a TLS certificate on the SP Veeam backup server, the SP can send the copied information about the TLS certificate so that tenants can save the certificate thumbprint for TLS certificate verification.

This step can be performed in Veeam Cloud Connect infrastructure that uses a self-signed TLS certificate. If you use a TLS certificate signed by a CA, skip this step. Signed TLS certificates are trusted without additional verification.

Adding Cloud Gateways

The procedure of cloud gateway configuration is performed by the SP on the SP Veeam backup server.

When you configure the Veeam Cloud Connect infrastructure, you must deploy at least one cloud gateway. Cloud gateways are network appliances that route traffic between tenants' Veeam backup servers and SP cloud infrastructure components. The role of a cloud gateway can be assigned to any Microsoft Windows server, including the Veeam backup server.

You can deploy one or several cloud gateways. Several cloud gateways can be set up for scalability purposes, to balance the traffic load in the Veeam Cloud Connect infrastructure.

Before You Begin
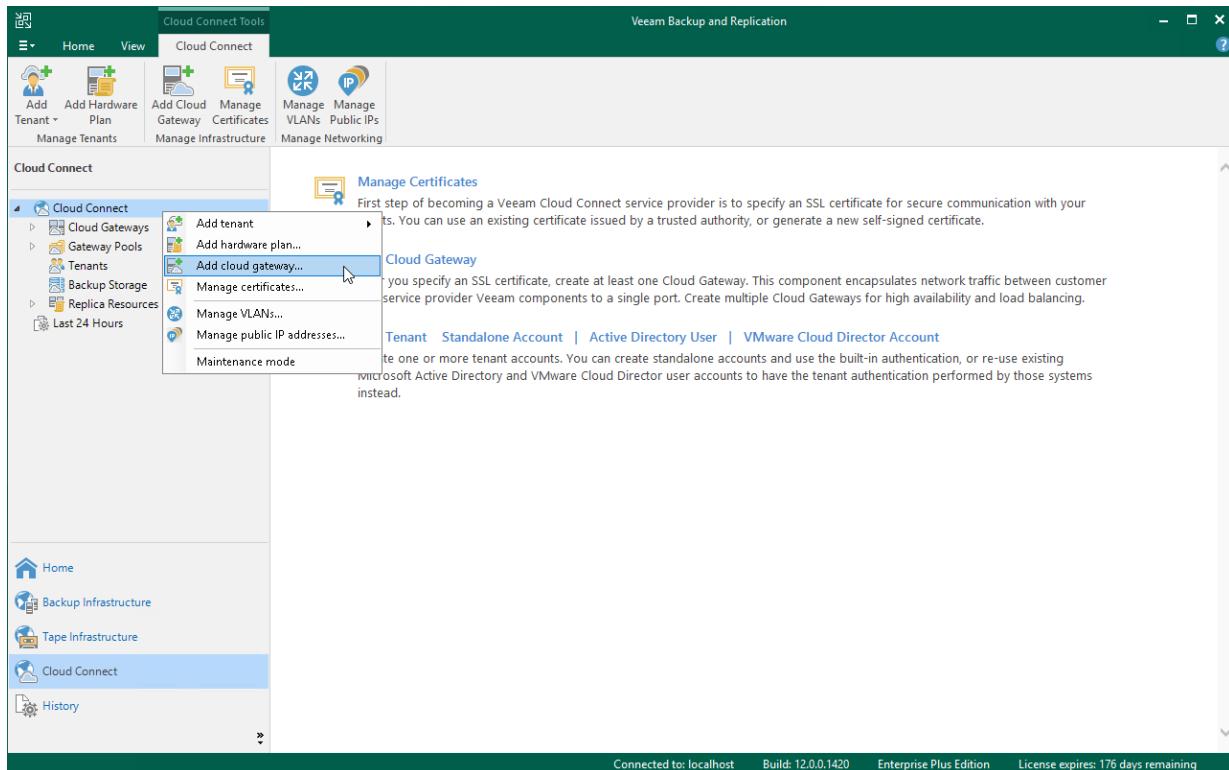
Before you add a cloud gateway, check the following prerequisites:

1. The server that will perform the role of a cloud gateway must meet the following requirements:

    o The cloud gateway can be a physical or virtual machine.

    o The cloud gateway must run Microsoft Windows OS.

    To learn more, see System Requirements.

2. A TLS certificate must be installed on the SP Veeam backup server.

Step 1. Launch New Gateway Wizard

To launch the **New Cloud Gateway** wizard, do one of the following:
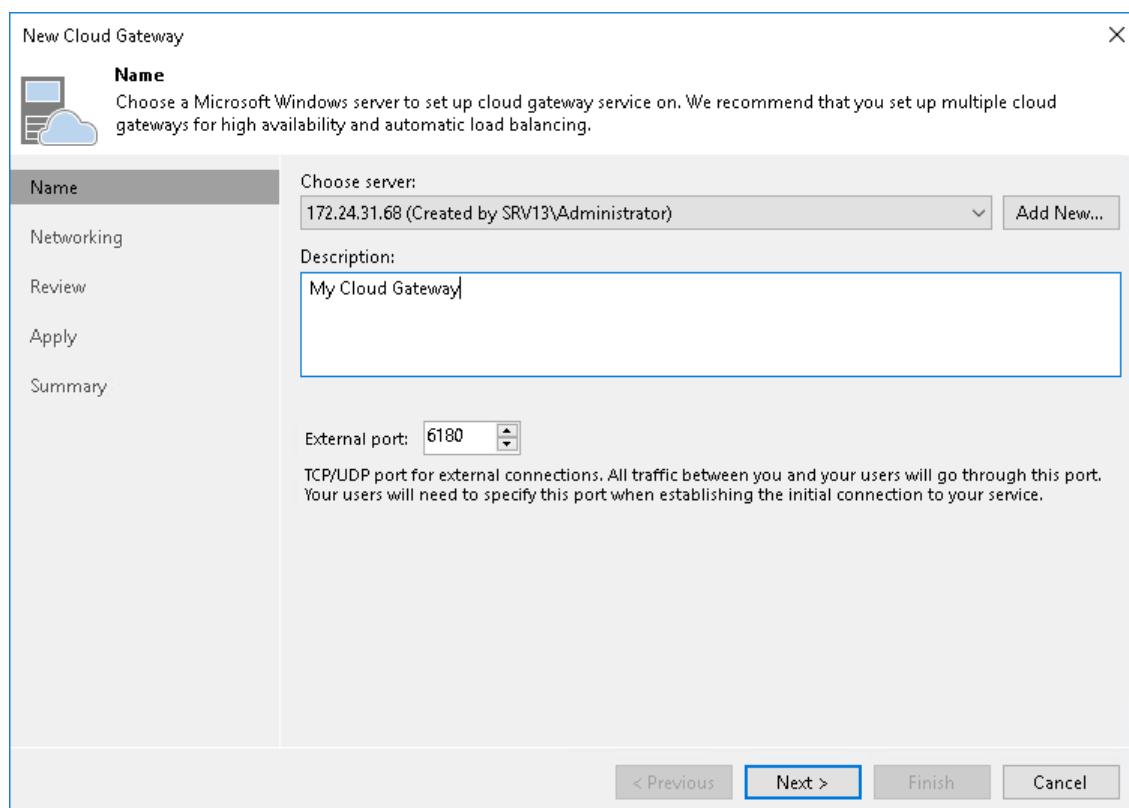
- Open the **Cloud Connect** view. Click the **Cloud Connect** node in the inventory pane and click **Add Cloud Gateway** in the working area.

- Open the **Cloud Connect** view. Click **Add Cloud Gateway** on the ribbon.

- Open the **Cloud Connect** view. Right-click the **Cloud Gateways** node in the inventory pane or right-click anywhere in the working area and select **Add cloud gateway**.

Step 2. Choose Server

At the **Name** step of the wizard, specify settings of a server that will be used as a cloud gateway.

1. From the **Choose server** list, select a Microsoft Windows server that will perform the role of a cloud gateway. You can select any server added to Veeam Backup & Replication or assign the cloud gateway role to the Veeam backup server itself.

   If the server is not added yet, click **Add New** to open the **New Windows Server** wizard.

2. In the **Description** field, provide a description for the cloud gateway. The default description contains information about the user who added the cloud gateway, date and time when the cloud gateway was added.

3. In the **External port** field, specify a TCP/IP port over which tenant Veeam backup servers will communicate with the cloud gateway. By default, port number 6180 is used.

Step 3. Specify Network Settings

At the **Networking** step of the wizard, select the network mode that will be used by the cloud gateway to communicate with Veeam backup servers on the tenant side.

You can choose between two network modes: NAT mode or direct mode.

- If a cloud gateway is located in the local network behind the NAT gateway:

    a. Select **Located behind NAT or uses external DNS name**.

    b. In the **DNS name** field, specify a DNS name of the NAT gateway.

       You must specify an individual DNS name for each cloud gateway that you add to the Veeam Cloud Connect infrastructure.

    c. In the **Internal port** field, specify a port on the local network behind the NAT used for listening to connections from tenants. By default, port 6180 is used.

    d. On your NAT gateway, configure the port forwarding rule for TCP and UDP protocols: from an incoming port (specified in the **External port** field at the previous step of the wizard) to the port on the local network used for listening to connections (specified at the **Incoming port** field at this step of the wizard). For example, if you use default port number values, you must configure the following port forwarding rule: *from port 6180 to port 6180*.

- If a cloud gateway has a direct network connection to Veeam backup servers on the tenant side, select **This server is connected directly to the Internet**. From the NIC list, select a network adapter on the cloud gateway server that will be used to communicate with tenants' Veeam backup servers.

Consider the following:

- If you use a TLS certificate verified by a CA to establish a secure connection between Veeam Cloud Connect infrastructure components, it is recommended that you choose **Located behind NAT or uses external DNS name** mode for all cloud gateways, including those that have direct network connection to the internet. To learn more, see Network Settings with Verified TLS Certificates.

- Each cloud gateway must have its own public IPv4 address, regardless of whether the IP address is directly configured on the cloud gateway itself (direct mode) or on a NAT gateway in front of it (NAT mode). To resolve public DNS names of cloud gateways to IP addresses, the SP must create on the DNS server a separate A record for each IP address. For example:

```
gateway01.tech.com "A" record to 198.51.100.1
gateway02.tech.com "A" record to 198.51.100.2
```

    Configurations with one DNS record for multiple IP addresses are not supported.
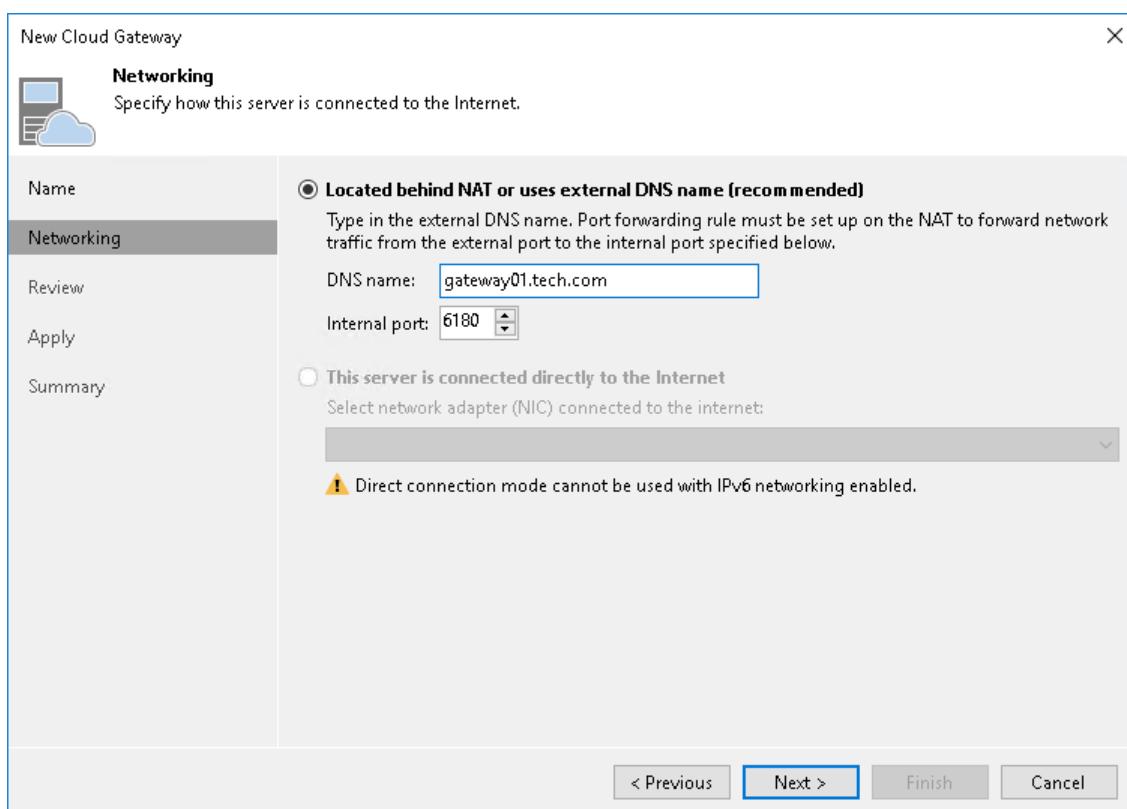
    The SP can use one public DNS name for their Veeam Cloud Connect infrastructure and provide the tenant with this DNS name instead of DNS names of cloud gateways. In this case, the SP must create DNS records for both public Veeam Cloud Connect DNS name and DNS names of cloud gateways. For example:

```
provider.tech.com "A" record to 198.51.100.1
provider.tech.com "A" record to 198.51.100.2
gateway01.tech.com "A" record to 198.51.100.1
gateway02.tech.com "A" record to 198.51.100.2
```

> **NOTE**
>
> For the scenario where the SP assigns cloud gateway pools to tenants and provides the tenant with a public Veeam Cloud Connect DNS name to connect to the SP, make sure that the public DNS name does not resolve to IP addresses of cloud gateways included in cloud gateway pools that are not available to the tenant.

- Public DNS names (recommended) or IP addresses of all cloud gateways must be accessible to all tenants and subtenants who work with the SP. Some of the cloud gateways may be temporarily unavailable, for example, due to a failure or for maintenance purposes. However, it is not recommended that one or more IP addresses of a cloud gateway are permanently available only to the limited number of tenants. Such configuration may impact performance of jobs created by tenants and subtenants.

- You cannot use the direct mode if IPv6 communication is enabled in the Veeam Backup & Replication settings. To learn more about support for IPv6 communication, see IPv6 Support.
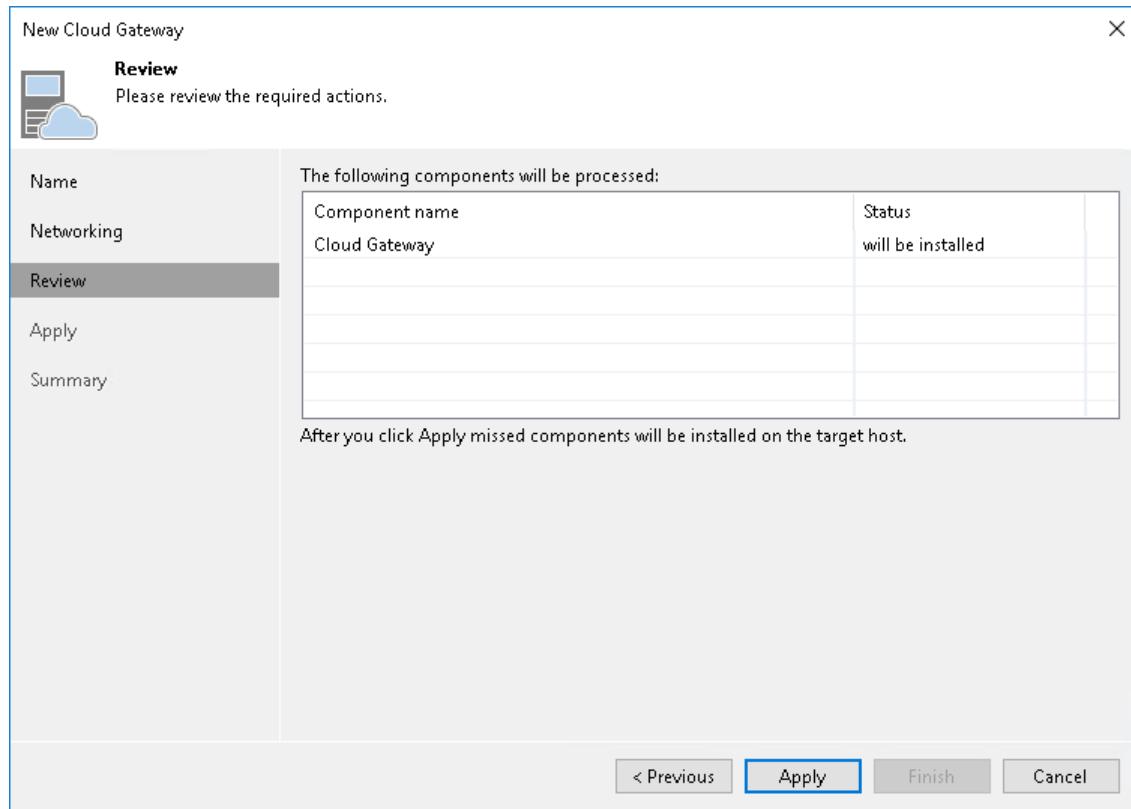
Network Settings with Verified TLS Certificates

If you use a verified TLS certificate in your Veeam Cloud Connect infrastructure, it is recommended that you configure a cloud gateway in the following way:

1. DNS names of all cloud gateways in Veeam Cloud Connect infrastructure must be associated with the verified TLS certificate.

2. For all cloud gateways, specify the following network settings in the **New Cloud Gateway** wizard:

   a. Select **Located behind NAT or uses external DNS name**.

   b. In the **DNS name** field, specify an external DNS name of the cloud gateway (in case of direct connection) or a DNS name of the NAT gateway (if a cloud gateway is located behind the NAT gateway).

   c. In the **Internal port** field, specify a port used for listening to connections from tenants:

      ▪ If a cloud gateway has a direct connection to the internet, specify the same port that was specified in the **External port** field at the previous step of the wizard. By default, port 6180 is used.

      ▪ If a cloud gateway is located in the local network behind the NAT gateway, specify the same port that is specified in the port forwarding rule on your NAT gateway.
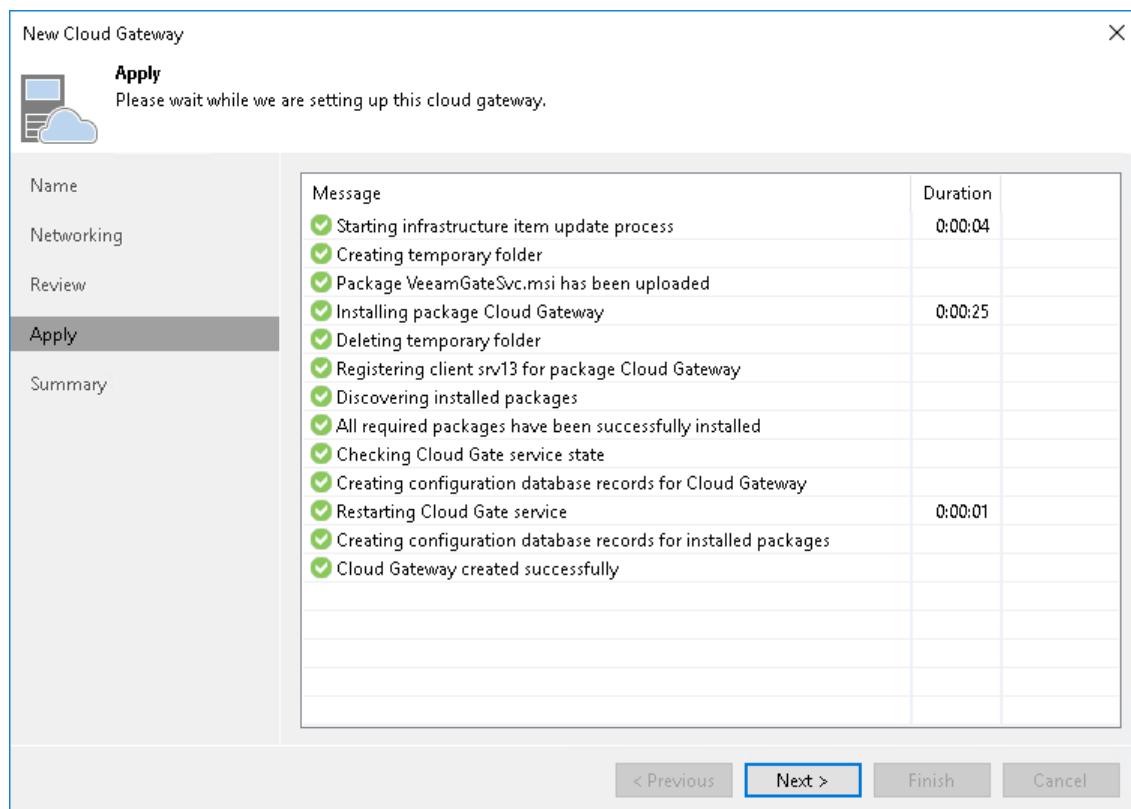
Step 4. Review Cloud Gateway Settings

At the **Review** step of the wizard, review the components that will be installed on the cloud gateway server.

Step 5. Assess Results
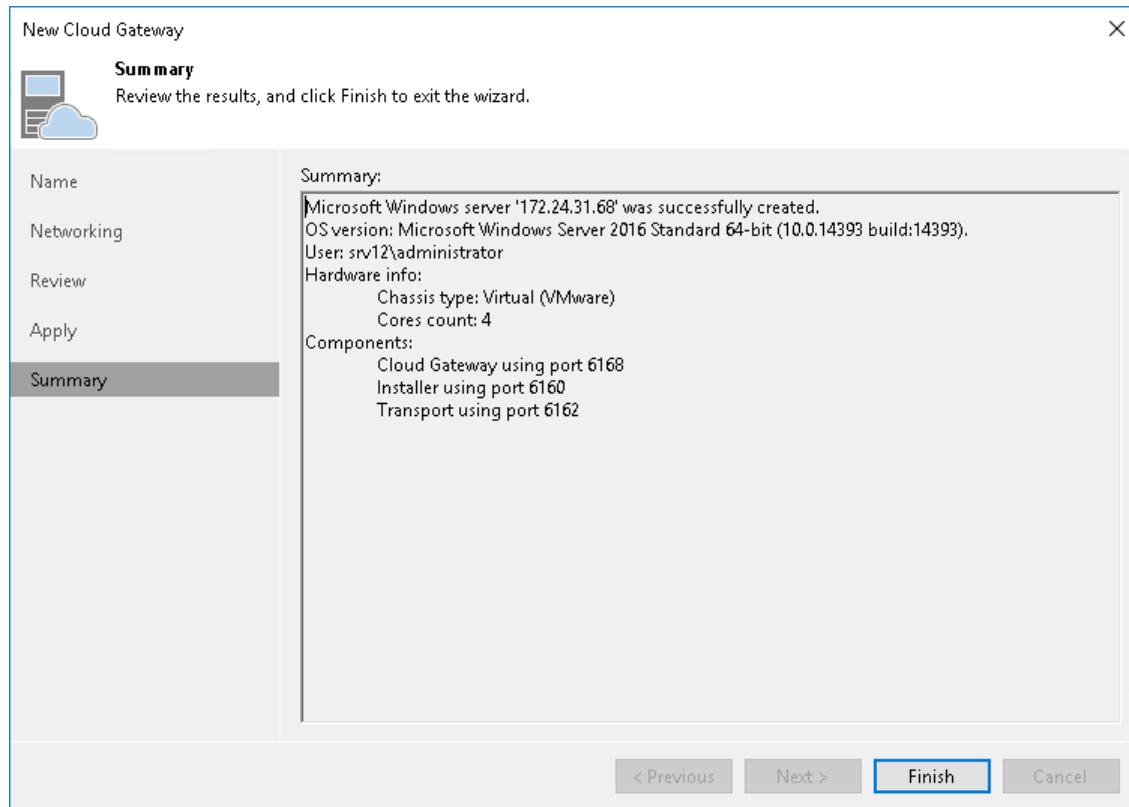
At the **Apply** step of the wizard, Veeam Backup & Replication will install the components on the cloud gateway server. Wait for the required operations to complete and click **Next** to continue.

Step 6. Finish Working with Wizard

At the **Summary** step of the wizard, complete the procedure of cloud gateway configuration.

1. Review the information about the added cloud gateway.

2. Click **Finish** to exit the wizard.

Configuring Cloud Gateway Pools

The procedure of cloud gateway pool configuration is performed by the SP on the SP Veeam backup server.

You can organize cloud gateways deployed in the Veeam Cloud Connect infrastructure into cloud gateway pools. Usage of cloud gateway pools allows you to assign dedicated cloud gateways to specific tenants.

You can configure one or more cloud gateway pools in the Veeam Cloud Connect infrastructure. Each cloud gateway pool can contain one or more cloud gateways.

Before You Begin
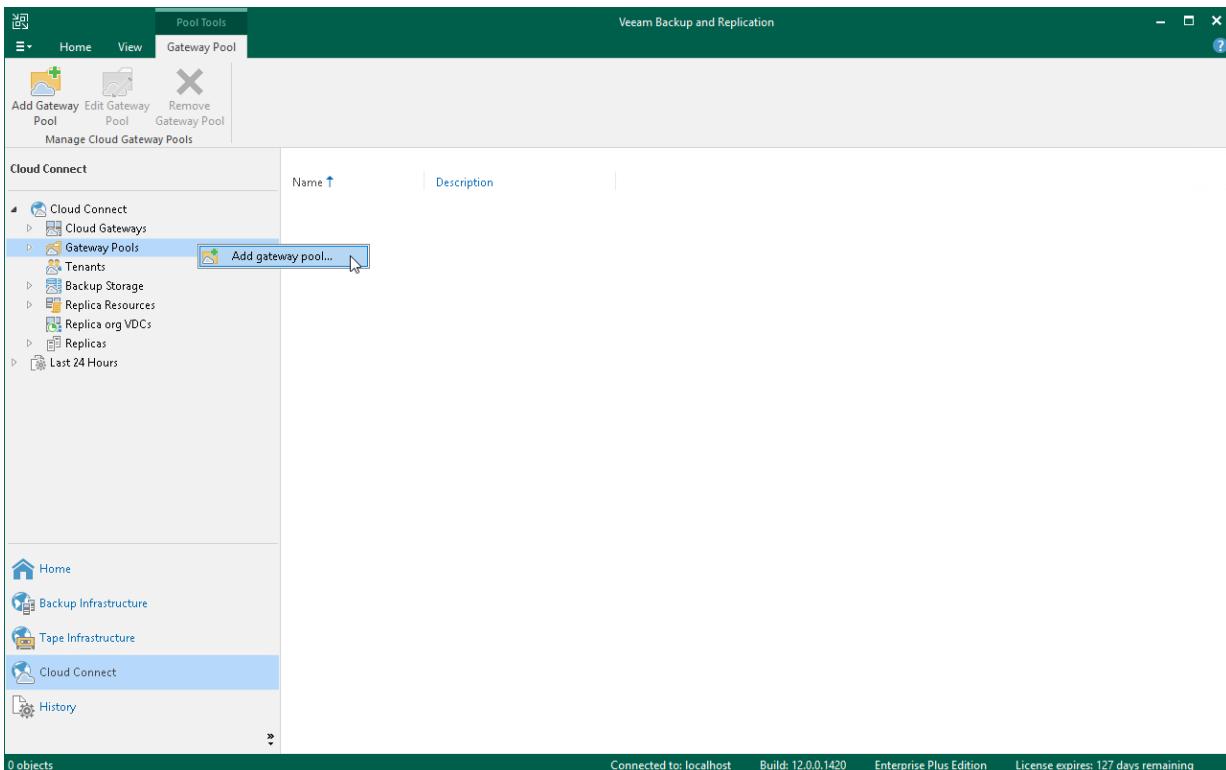
Before you configure a cloud gateway pool, check the following prerequisites:

1. A TLS certificate must be installed on the SP Veeam backup server.

2. Cloud gateways that you want to add to the cloud gateway pool must be deployed in the Veeam Cloud Connect infrastructure.

Step 1. Launch New Gateway Pool Wizard

To launch the **New gateway pool** wizard, do one of the following:
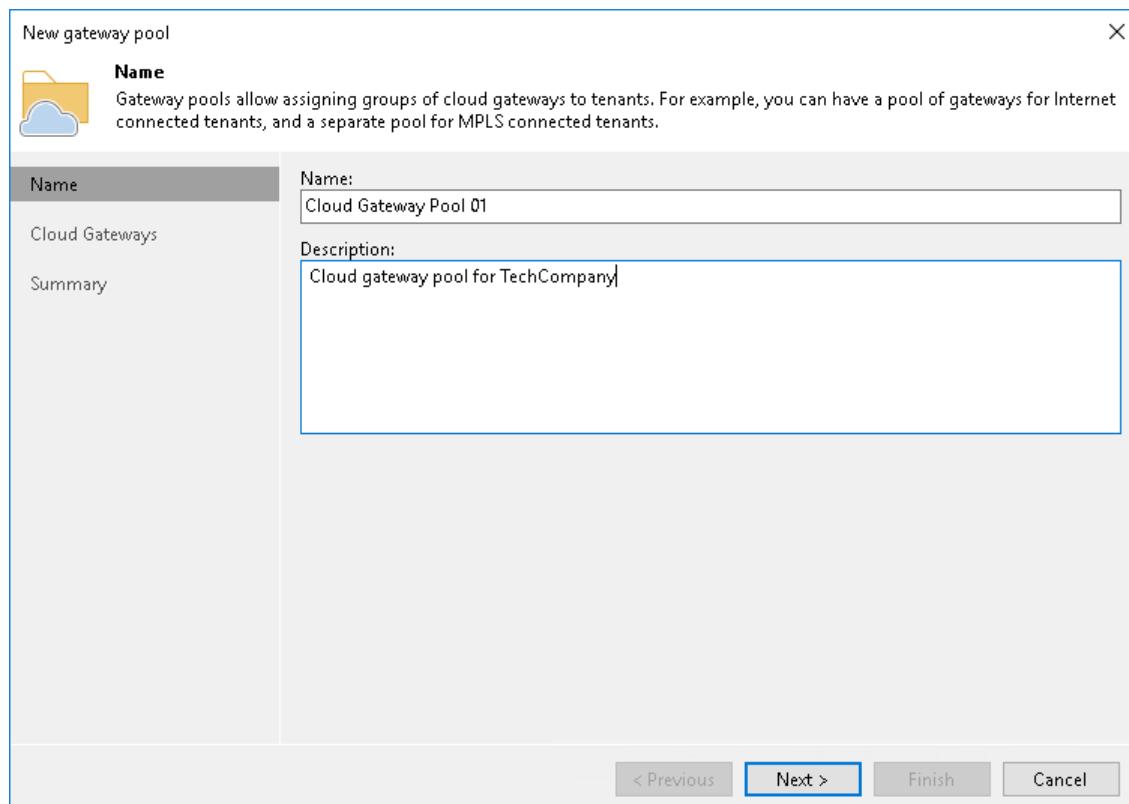
- Open the **Cloud Connect** view. Click the **Gateway Pools** node in the inventory pane and click **Add Gateway Pool** on the ribbon.

- Open the **Cloud Connect** view. Right-click the **Gateway Pools** node in the inventory pane and select **Add gateway pool**.

Step 2. Specify Cloud Gateway Pool Name and Description

At the **Name** step of the wizard, specify a name and description for the cloud gateway pool.

1. In the **Name** field, specify a name for the cloud gateway pool.

2. In the **Description** field, provide a description for future reference. The default description contains information about the user who added the cloud gateway pool, date and time when the cloud gateway pool was added.
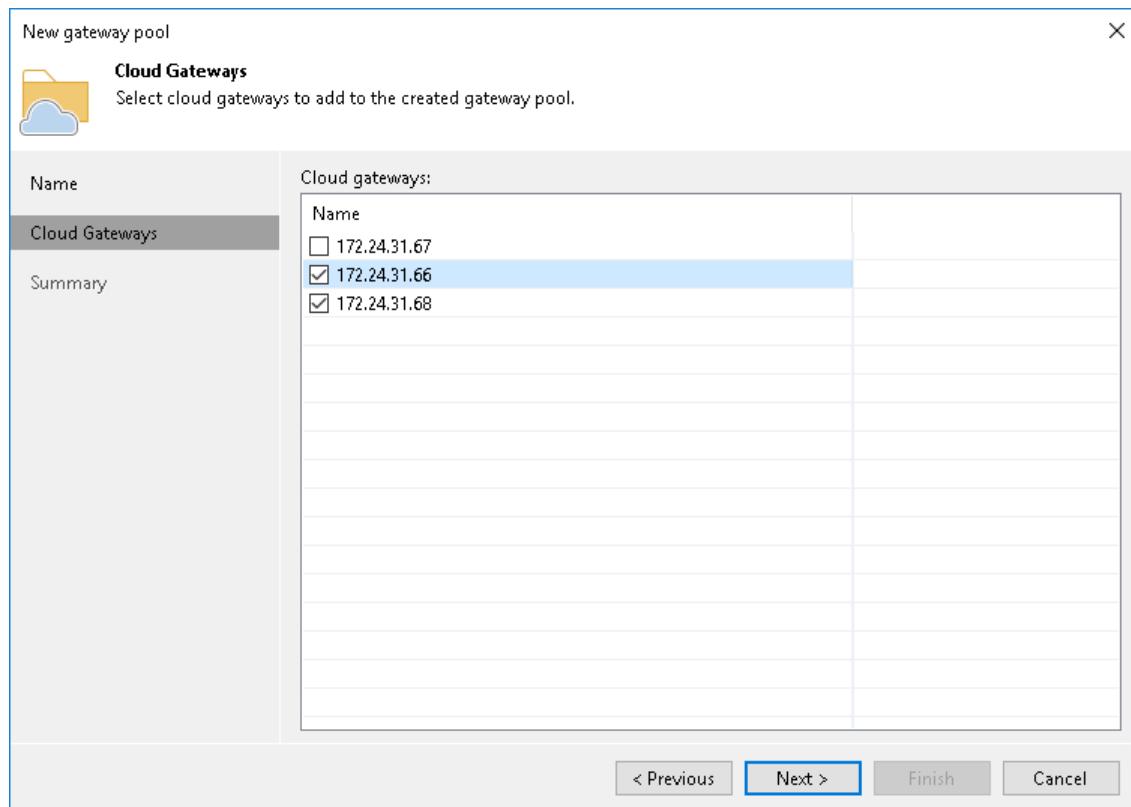
Step 3. Select Cloud Gateways

At the **Cloud Gateways** step of the wizard, from the **Cloud gateways** list, select one or more cloud gateways that you want to add to the cloud gateway pool.
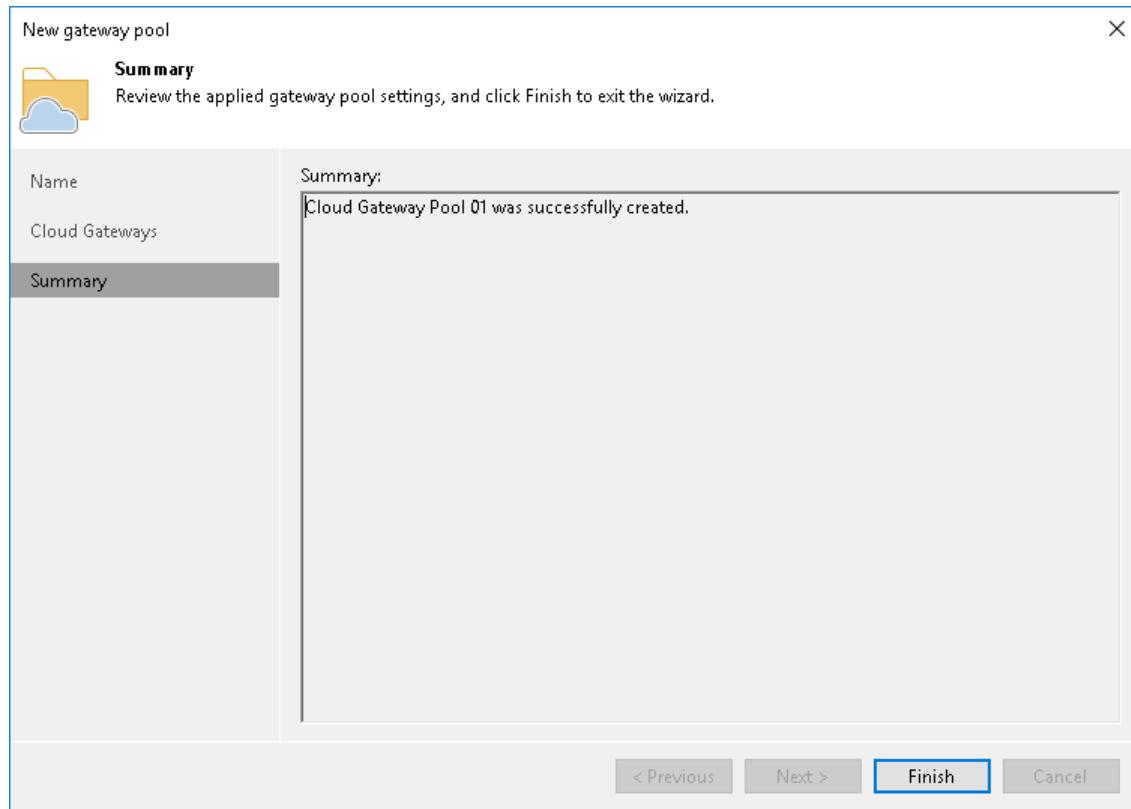
> **NOTE**
>
> The **Cloud gateways** list contains cloud gateways that are not added to any cloud gateway pool yet. Cloud gateways that are already added to a cloud gateway pool are not displayed in the list. You cannot add a cloud gateway that is a part of a cloud gateway pool to another cloud gateway pool

Step 4. Finish Working with Wizard

At the **Summary** step of the wizard, complete the procedure of cloud gateway pool configuration.

1. Review the information about the added cloud gateway pool.

2. Click **Finish** to exit the wizard.

What You Do Next

After you create a cloud gateway pool, you must do the following:

1. Assign the created cloud gateway pool to the tenant in the properties of the tenant account. To learn more, see Specify Bandwidth Settings.

2. Pass to the tenant a DNS name or IP address of one or more cloud gateways added to the cloud gateway pool.

Only those tenants to whom the cloud gateway pool is assigned can use cloud gateways added to this cloud gateway pool. Other tenants will be able to use individual cloud gateways that are not added to any cloud gateway pool.

Configuring Cloud Repositories

You can configure one or several backup repositories in your backup infrastructure and use them as cloud repositories.

A cloud repository is a regular backup repository configured on the SP side. When the SP creates a tenant account, the SP can assign a storage quota (allocates some amount of storage space) on this backup repository for the tenant. The tenant can be assigned different quotas on different backup repositories. As soon as the tenant connects to the SP, Veeam Backup & Replication retrieves information about all quotas for this tenant and displays a list of available cloud repositories in the tenant backup infrastructure.

You can use the following types of backup repositories as cloud repositories:

- Microsoft Windows server with a local or directly attached storage

- Linux server with local, directly attached or mounted NFS storage

- SMB (CIFS) or NFS shared folder

  Keep in mind that NFS share backup repository is supported starting from Veeam Backup & Replication 10. Tenants who run earlier versions of the product cannot create backups in backup repositories of this type.

- Deduplicating storage appliance: Dell Data Domain, ExaGrid and Quantum DXi

- Scale-out backup repository

You can use a simple backup repository and/or scale-out backup repository as a cloud repository.
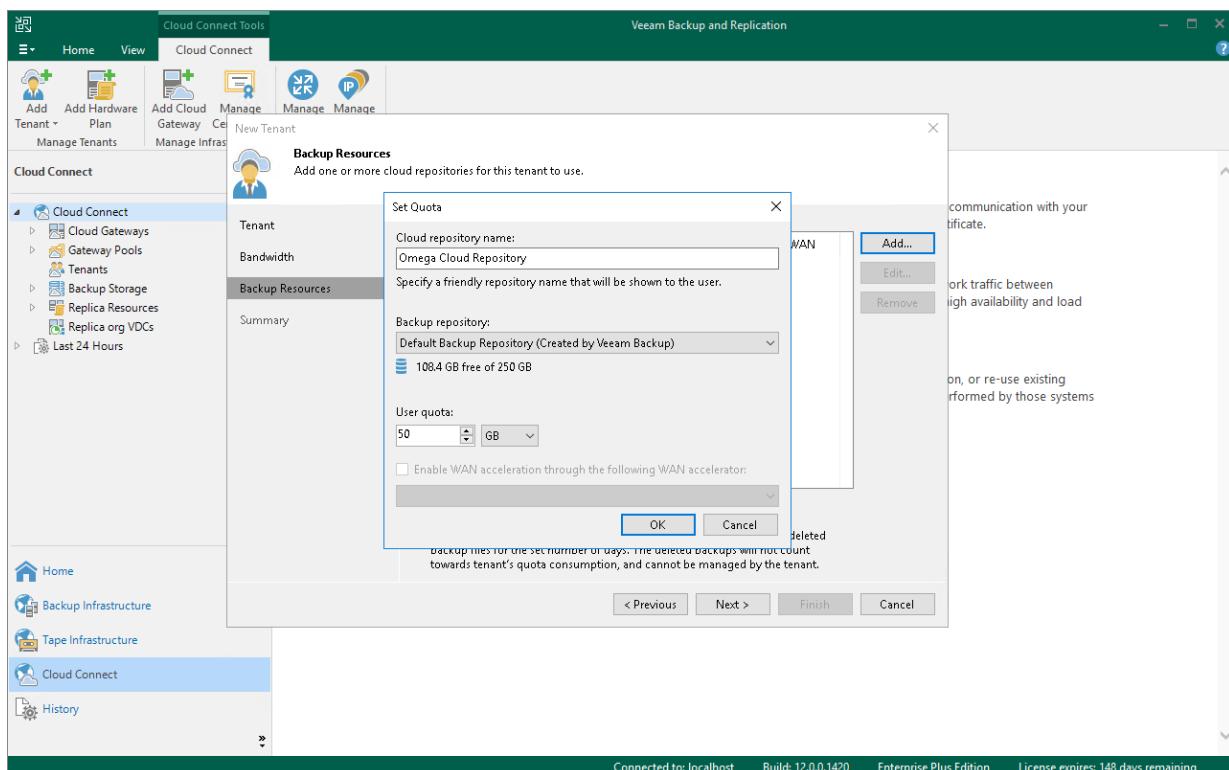
The configuration process for backup repositories in the Veeam Cloud Connect infrastructure does not differ from the same process in a regular Veeam backup infrastructure. To learn more, see Adding Backup Repositories and Adding Scale-Out Backup Repositories sections in the Veeam Backup & Replication User Guide.

> **IMPORTANT**
>
> When the SP exposes a new simple backup repository as a cloud repository, the SP should make sure that the location of this repository does not appear to be a subfolder of another backup repository location. For example, if the SP has already specified the `E:\Backups` folder as a location of a backup repository, the SP must not configure other backup repositories in the following locations: `E:\Backups\Tenants`, `E:\Backups\Cloud`, and so on. After a tenant or the SP performs a rescan operation for a backup repository configured in this way, information about tenant backups in the configuration database on the SP backup server will become corrupted.

> **NOTE**
>
> Veeam Backup & Replication does not apply the **Limit maximum concurrent tasks** option to backup repositories used as cloud repositories. For Veeam Cloud Connect Backup, the maximum allowed number of concurrent tasks is defined per tenant in the properties of the tenant account. For details, see Specify Bandwidth Settings.

Configuring Hardware Plans

To expose cloud hosts to tenants, you must configure one or more hardware plans in the Veeam Cloud Connect infrastructure.

A hardware plan is a set of computing, storage and network resources in the SP virtualization environment that the SP can expose as a target for tenant VM replicas. When the SP creates a tenant account, the SP can subscribe the tenant to a hardware plan. The tenant can be subscribed to different hardware plans that utilize resources on different SP's virtualization hosts.

For tenants, hardware plans appear as cloud hosts on which tenants can create VM replicas. As soon as the tenant connects to the SP, Veeam Backup & Replication retrieves information about all hardware plans to which the SP subscribed this tenant and displays a list of cloud hosts that become available in the tenant backup infrastructure.

You can configure hardware plans on the following virtualization platforms:

- VMware host or cluster

- Hyper-V host or cluster

Adding Hardware Plans

You can configure one or several hardware plans in your Veeam Cloud Connect infrastructure.

Before You Begin

Before you add a new hardware plan, check the following prerequisites:

1. A TLS certificate must be installed on the SP Veeam backup server.

2. Virtualization hosts that will provide resources to tenants through a hardware plan must be added to the backup infrastructure.

3. The process of configuring a hardware plan differs depending on virtualization environment — VMware vSphere or Microsoft Hyper-V. Thus, separate wizards are used to configure hardware plans for different virtualization environments:

   o The **New VMware Hardware Plan** wizard — to configure a VMware hardware plan.

   o The **New Hyper-V Hardware Plan** wizard — to configure a Hyper-V hardware plan.

   The description of a hardware plan setup process is illustrated primarily with the figures from the **New VMware Hardware Plan** wizard. However, all the described steps except for those specified, are the same for configuring both VMware and Hyper-V hardware plans.

4. It is recommended that you plan network resources in advance and configure a range of VLANs that will be reserved for Veeam Cloud Connect Replication before configuring a hardware plan. To learn more, see Managing VLANs.

Limitations for VMware Hardware Plans

To configure a VMware hardware plan that will use resources of a vCenter Server cluster, you must use the Enterprise or Enterprise Plus edition of the VMware vSphere infrastructure. DRS functionality must be enabled on the vCenter Server cluster. Standard VMware vSphere edition does not support creating resource pools in clusters.

This limitation does not apply to standalone ESXi hosts managed by vCenter Server.

Limitations for Hyper-V Hardware Plans
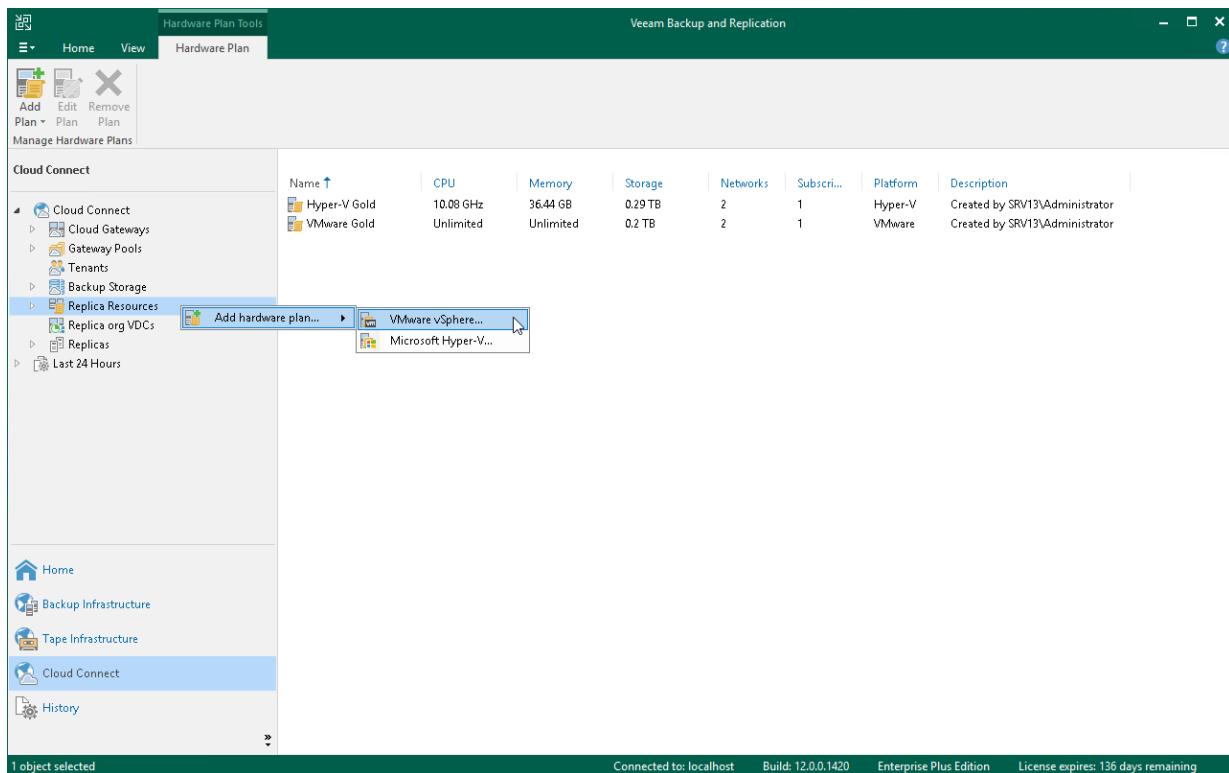
Before you add a new Hyper-V hardware plan, consider the following limitations:

- Standalone Hyper-V hosts that run Nano Server installations of the Microsoft Windows Server 2016 OS cannot be used for configuring hardware plans.

- The following types of Hyper-V clusters are not supported for exposing resources through hardware plans:

  - o Clusters with server nodes that run Nano Server installations of the Microsoft Windows Server 2016 OS

  - o Clusters with the Cluster Operating System Rolling Upgrade feature enabled

  - o Multi-domain and Workgroup Clusters

- After you subscribe a tenant to a Hyper-V hardware plan, you cannot rename the virtual switch in Microsoft Hyper-V infrastructure that is used by VM replicas. If you rename the virtual switch, replication jobs targeted at the cloud host that use the renamed virtual switch will fail.

- Usage of a Microsoft SMB3 shared folder as a storage for VM replicas is not supported in the Veeam Cloud Connect infrastructure.

Step 1. Launch New Hardware Plan Wizard

To launch the **New VMware Hardware plan** or **New Hyper-V Hardware plan** wizard, do one of the following:
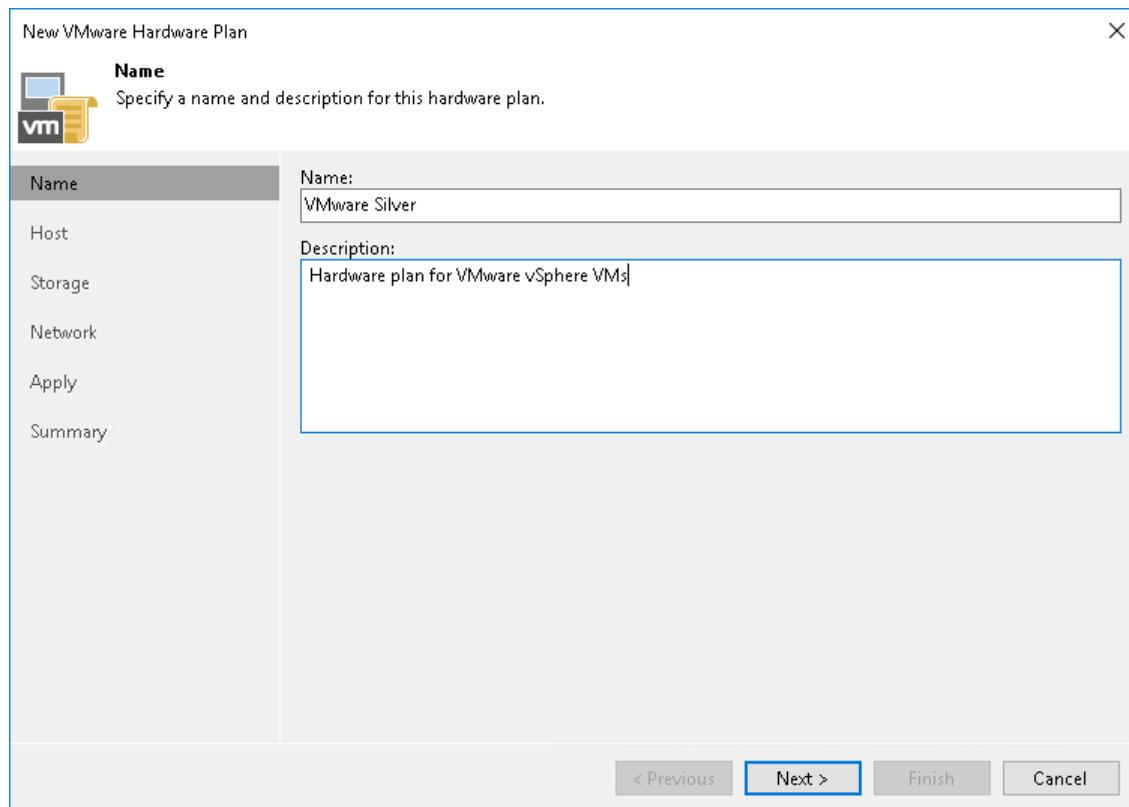
- Open the **Cloud Connect** view. Click **Add Plan** on the ribbon and select **VMware vSphere** or **Microsoft Hyper-V**.

- Open the **Cloud Connect** view. Click the **Replica Resources** node in the inventory pane, click **Add Plan** on the ribbon and select **VMware vSphere** or **Microsoft Hyper-V**.

- Open the **Cloud Connect** view. Right-click the **Replica Resources** node in the inventory pane or right-click anywhere in the working area and select **Add hardware plan** > **VMware vSphere** or **Add hardware plan** > **Microsoft Hyper-V**.

Step 2. Specify Hardware Plan Name and Description

At the **Name** step of the wizard, specify a name and description for the hardware plan.

1. In the **Name** field, specify a name for the hardware plan.

2. In the **Description** field, provide a description for future reference. The default description contains information about the user who added the hardware plan, date and time when the hardware plan was added.

Step 3. Specify Host or Cluster
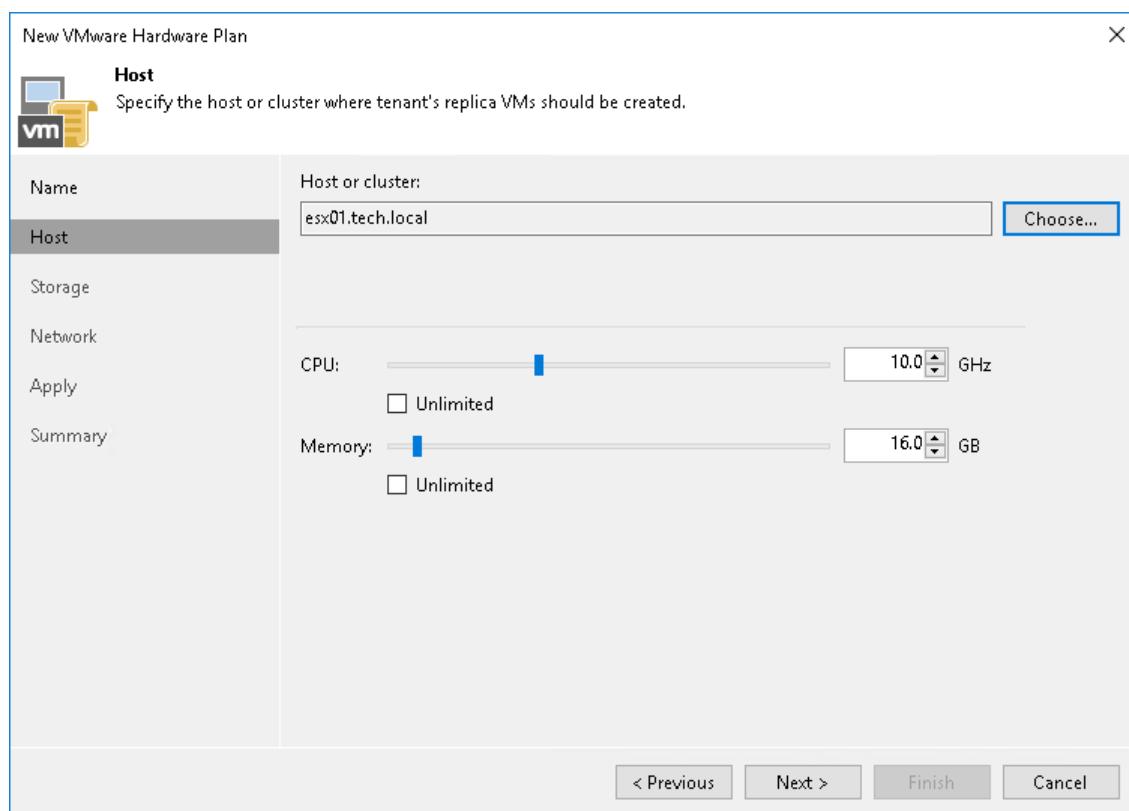
At the **Host** step of the wizard, specify a host or cluster on which you want to configure a replication target.

1. In the **Host or cluster** section, click **Choose** and select the host in the SP virtualization environment on which Veeam Backup & Replication will register VM replicas created by replication jobs targeted at the cloud host.

2. In the **CPU** section, specify the limit of CPU resources that can be utilized by all VM replicas on the cloud host provided to the tenant through the created hardware plan. To let the tenant utilize all CPU resources available on the selected host, select the **Unlimited** check box.

   > **NOTE**
   >
   > The SP should make sure that the amount of resources available for tenant VMs is sufficient for VM operation. For Hyper-V hardware plans, the limit of CPU resources must be greater than the total amount of CPU frequency on all tenant VM processor units. If the source host on the tenant side has more CPU resources than the target host on the SP side, tenant VMs may fail to start after failover due to shortage of resources.

3. In the **Memory** section, specify the limit of RAM that can be utilized by all VM replicas on the cloud host provided to the tenant through the created hardware plan. To let the tenant utilize all memory resources available on the selected host, select the **Unlimited** check box.

Step 4. Specify Storage Settings

At the **Storage** step of the wizard, specify the storage on which Veeam Backup & Replication will store files of tenant VM replicas.
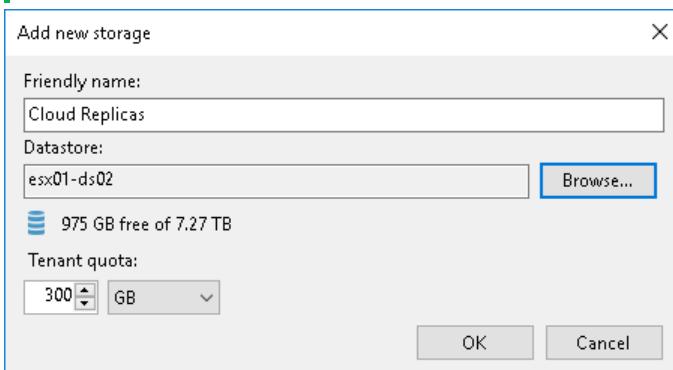
1. In the **Storage** section, click **Add** to open the **Add new storage** window.

2. In the **Friendly name** field, specify a name of the storage that will be displayed to a tenant.

3. [For a VMware hardware plan] In the **Datastore** section, click **Browse** and select a datastore on which to allocate storage resources for VM replicas.

> **NOTE**
>
> If you specified a cluster as a source of CPU and RAM resources for tenant VM replicas at the **Host** step of the wizard, you must use a shared datastore or datastore cluster as a storage for VM replica files. Datastores that can be accessed by a single host are not displayed in the list of available datastores at the **Storage** step of the wizard.
>
> Consider the following:
>
> - In the list of available datastores, Veeam Backup & Replication displays shared datastores that can be accessed by multiple hosts. Make sure that the shared datastore that you plan to use as a storage for tenant VM replicas is accessible by all cluster nodes.
> - Veeam Backup & Replication considers datastores in a datastore cluster as datastores accessible by multiple hosts. Make sure that all datastores in the datastore cluster that you plan to use as a storage for tenant VM replicas are accessible by all cluster nodes.
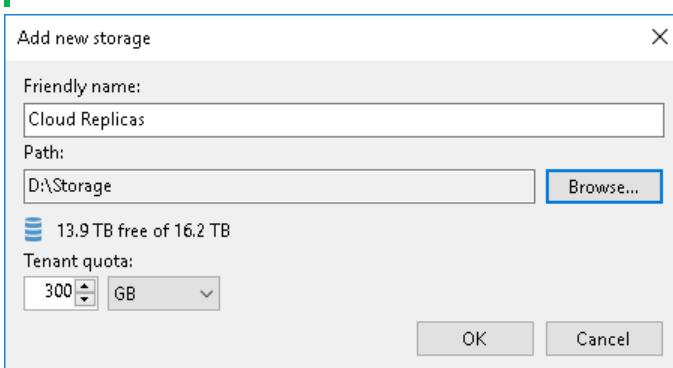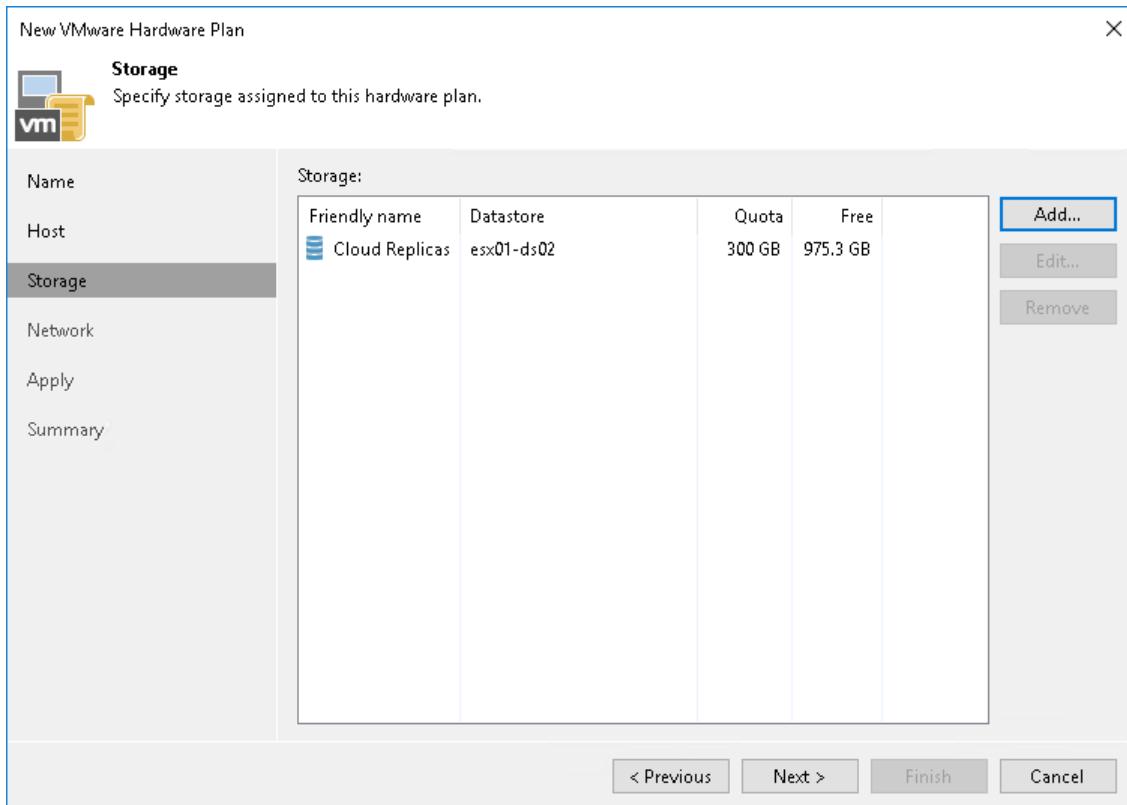
4. [For a Hyper-V hardware plan] In the **Path** section, click **Browse** and specify a path to a folder on the volume that will be used for storing VM replica files.

> **NOTE**
>
> You cannot specify a Microsoft SMB3 shared folder as a storage for tenant VM replicas.

5. In the **Tenant quota** section, specify the amount of disk space for the cloud host that will be provided to the tenant through the created hardware plan.

6. Click **OK**.
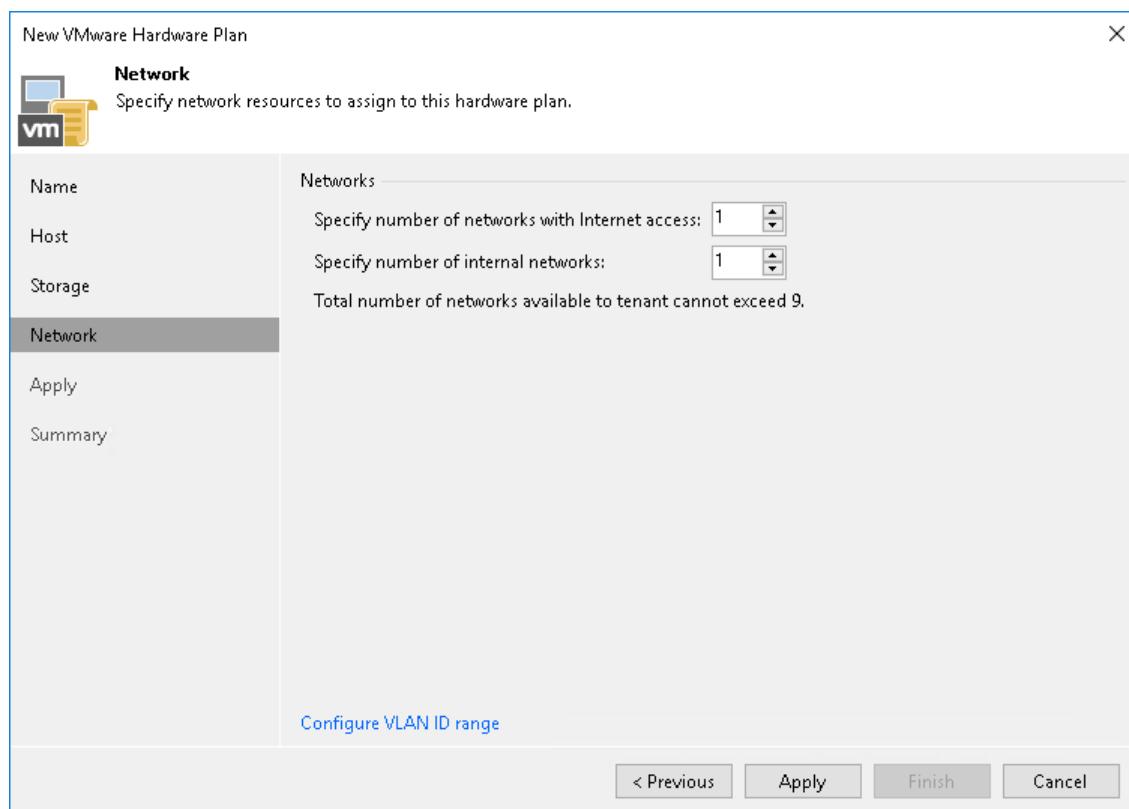
Step 5. Specify Network Settings

At the **Network** step of the wizard, specify network settings for the hardware plan.

1. [Optional] If you have not configured a range of VLANs that will be used for providing network resources to VM replicas on cloud hosts in advance before configuring a hardware plan, click the **Configure VLAN ID range** link at the bottom of the wizard window. Then use the **VLANs Configuration** dialog window to allocate the necessary number of VLANs on the virtualization host that was selected at the **Host** step of the wizard.
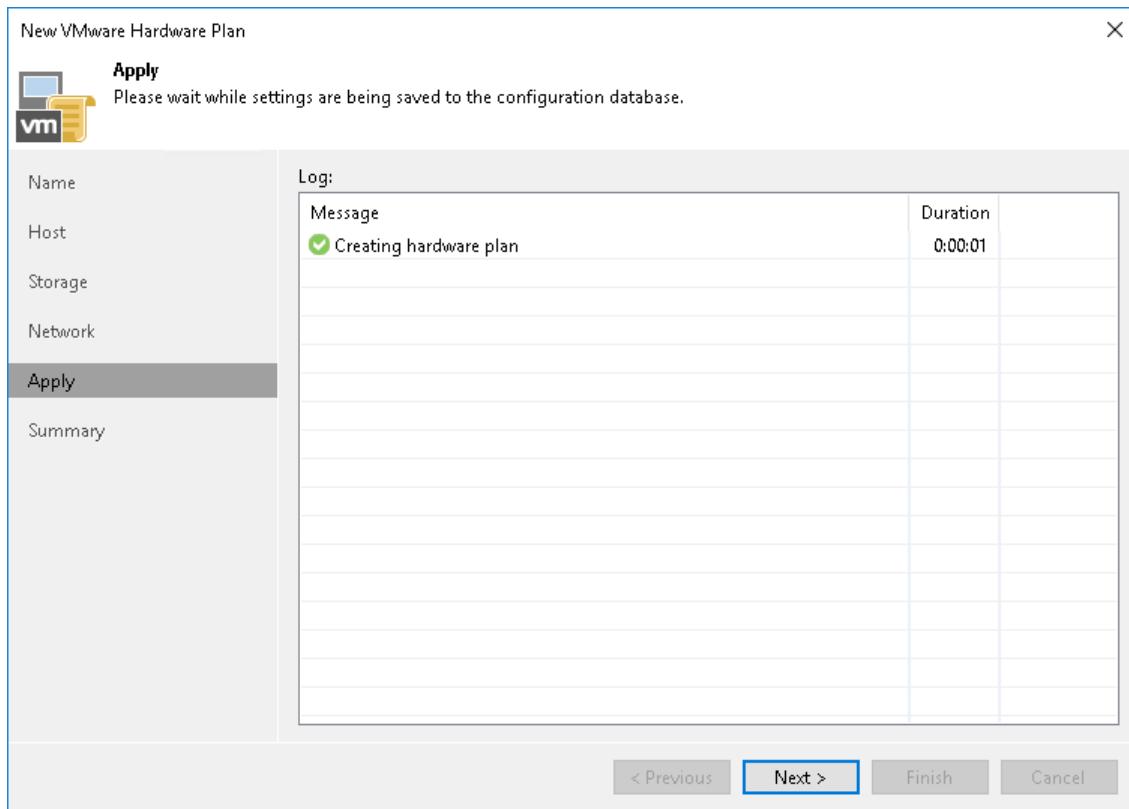
   To learn more about the VLAN range configuration process, see Managing VLANs.

2. In the **Specify number of networks with internet access** field, specify the number of IP networks with internet access that will be available for tenant VM replicas on the cloud host.

3. In the **Specify number of internal networks** field, specify the number of IP networks without internet access that will be available for tenant VM replicas on the cloud host.
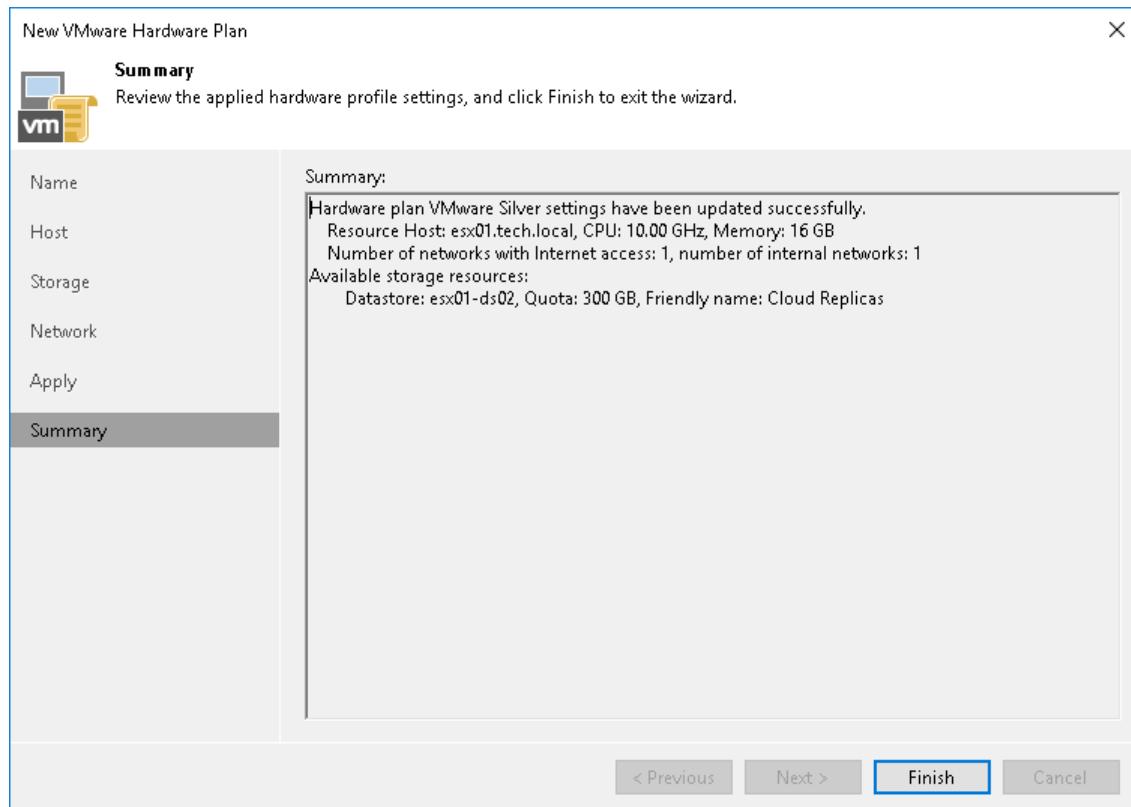
Step 6. Assess Results

At the **Apply** step of the wizard, Veeam Backup & Replication will create the configured hardware plan. Wait for the operation to complete and click **Next** to continue.

Step 7. Finish Working with Wizard

At the **Summary** step of the wizard, review the information about the created hardware plan and click **Finish** to exit the wizard.

Managing Hardware Plans

You can edit settings of hardware plans that you configured and remove unused hardware plans from the Veeam Cloud Connect infrastructure.

Editing Hardware Plan Settings

You can edit settings of hardware plans you have configured.

> **NOTE**
>
> When Veeam Backup & Replication saves new hardware plan settings to the configuration database, resources provided to tenants through the edited hardware plan will become temporarily unavailable to tenants. VM replicas in *Failover* state after partial site failover will also become temporarily inaccessible.

To edit settings of a hardware plan:

1. Open the **Cloud Connect** view.

2. In the inventory pane, click the **Replica Resources** node.

3. Do one of the following:

   - Select the necessary hardware plan in the working area and click **Edit Plan** on the ribbon or right-click the necessary hardware plan and select **Edit Hardware Plan**.

   - Select the necessary hardware plan in the inventory pane and click **Edit Plan** on the ribbon or right-click the necessary hardware plan and select **Edit hardware plan**.

4. Edit hardware plan settings as required.

NOTE

You cannot reduce the number of networks with internet access and the number of internal networks in the hardware plan when editing hardware plan settings.

Removing Hardware Plans
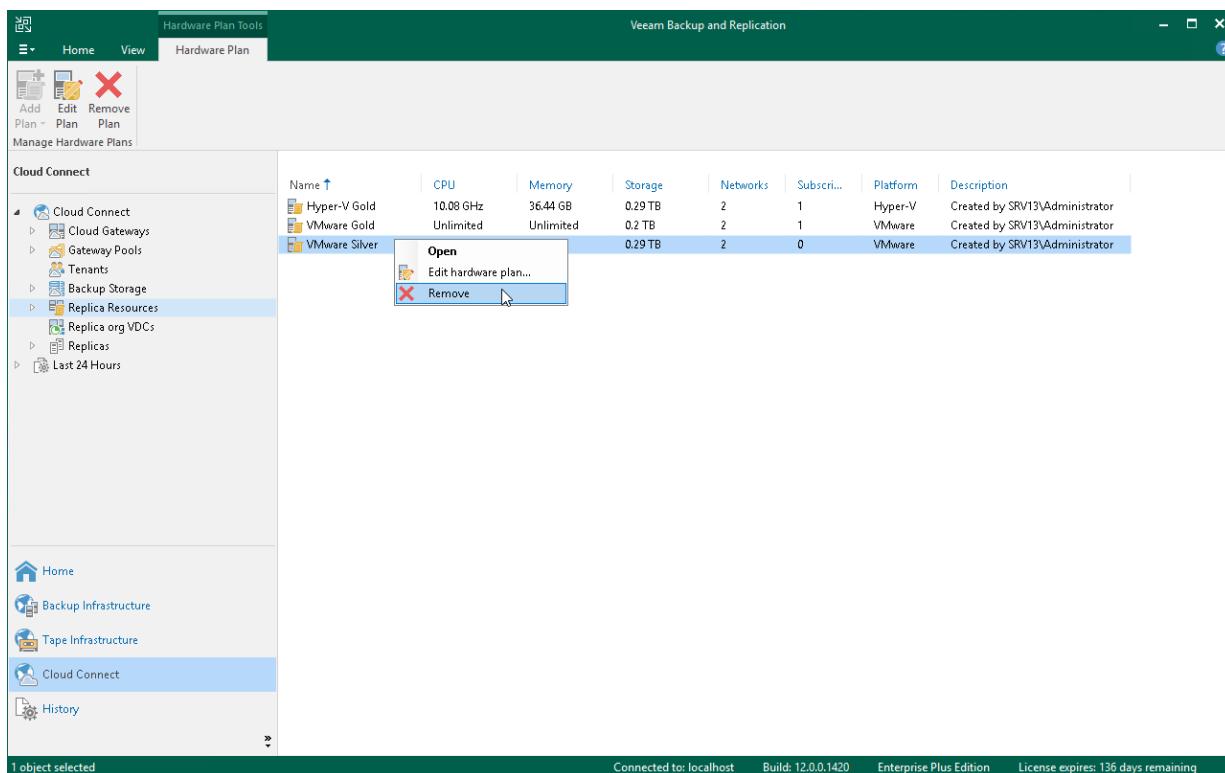
You can remove hardware plans you have configured.

> **NOTE**
>
> Before removing a hardware plan, you must first unsubscribe from this hardware plan all tenants who use resources provided through the hardware plan.

To remove a hardware plan:

1. Open the **Cloud Connect** view.

2. In the inventory pane, click the **Replica Resources** node.

3. Do one of the following:

   o Select the necessary hardware plan in the working area and click **Remove Plan** on the ribbon or right-click the necessary hardware plan and select **Remove**.

   o Select the necessary hardware plan in the inventory pane and click **Remove Plan** on the ribbon or right-click the necessary hardware plan and select **Remove**.

Managing VLANs

To enable networking for tenant VM replicas, the SP should configure physical switches to which hosts or clusters that will provide resources for hardware plans are connected. The SP must allocate on the physical switch a range of VLANs and reflect these settings in the Veeam Backup & Replication console using the **VLANs Configuration** dialog window.

In Veeam Backup & Replication, the SP can specify VLANs with internet access and VLANs without internet access. VLANs without internet access can be used as internal networks that let VM replicas communicate to each other after full site failover and to production VMs after partial site failover. For VLANs with internet access, Veeam Backup & Replication can also route traffic to the internet through the network adapter (vNIC) on the network extension appliance that is connected to the SP production network.

For example, if the SP plans to configure a hardware plan on the host named *Host1* that is connected to physical switch named *Switch1*, the SP can pre-configure on the *Switch1* a range of VLANs with IDs from *1* to *20*. In the Veeam Backup & Replication console, the SP should reflect those values in accordance, for example, specify *1–10* as a range of VLANs with internet access and *11–20* as a range of VLANs without internet access.

When the SP subscribes the tenant to the hardware plan, Veeam Backup & Replication configures on the network extension appliance that is deployed on the SP side the number of network adapters (vNICs) equal to the number of networks in the hardware plan. Each network adapter connects to the dedicated VLAN from the reserved range. As a result, Veeam Backup & Replication can map every production tenant VM network to the dedicated VLAN on the SP side.

As part of the VLAN configuration process, the SP can perform the following tasks:

- Add a VLAN range in Veeam Backup & Replication.

- Edit a VLAN range added in Veeam Backup & Replication.

- Remove a VLAN range added in Veeam Backup & Replication.

> **NOTE**
>
> Consider the following:
>
> - The total number of VLANs reserved for Veeam Cloud Connect Replication in the SP network infrastructure must be equal to or exceed the total number all tenant production networks.
> - If the SP allocates resources for a hardware plan on a VMware or Hyper-V cluster, the SP should also configure physical switches so that they provide a trunk to broadcast traffic for all configured VLANs.
> - The SP does not need to allocate VLANs in Veeam Backup & Replication if the SP uses VMware Cloud Director to provide replication resources to tenants. Instead, the SP allocates the necessary number of networks in the properties of the organization VDC that will be used as a cloud host for tenant VM replicas.
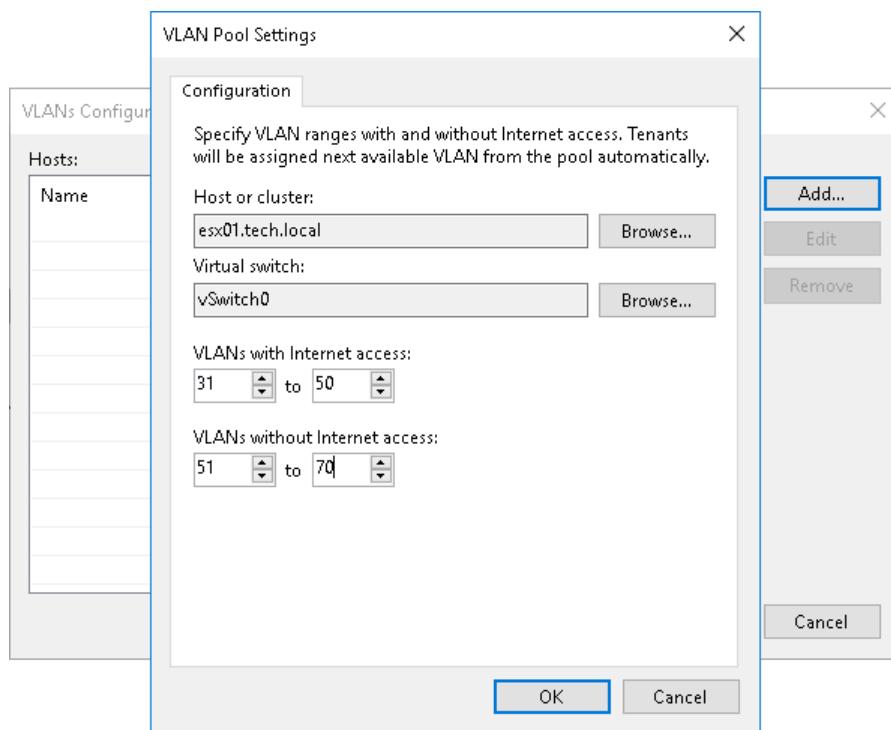
> **TIP**
>
> It is recommended that the SP plans network resources allocation and configures VLAN ranges in the Veeam Backup & Replication console in advance, prior to configuring hardware plans. However, the SP can also access the **VLANs Configuration** window when the SP performs the following tasks:
>
> - Configures network resources for a hardware plan. To learn more, see Specify Network Settings.
> - Subscribes a tenant to a hardware plan. To learn more, see Allocate Replication Resources.

Adding VLAN Ranges

To add a VLAN range in Veeam Backup & Replication:

1. Open the **VLANs Configuration** window in one of the following ways:

   o Open the **Cloud Connect** view, click the **Cloud Connect** node and click **Manage VLANs** on the ribbon.

   o Open the **Cloud Connect** view, right-click the **Cloud Connect** node and select **Manage VLANs**.

2. In the **VLANs Configuration** window, click **Add**.

3. In the **VLAN Pool Settings** window, click **Browse** next to the **Host or cluster** field and select a host or cluster on which you plan to configure a replication target.

4. Click **Browse** next to the **Virtual switch** field and select a virtual switch configured on the selected host on which to reserve VLANs for Veeam Cloud Connect Replication.

5. In the **VLANs with Internet access** fields, specify the first and the last VLAN ID in the range of VLANs that you plan to use for providing networks with internet access to VM replicas on the cloud host.

6. In the **VLANs without Internet access** fields, specify the first and the last VLAN ID in the range of VLANs that you plan to use for providing networks without internet access to VM replicas on the cloud host.

7. Click **OK**.
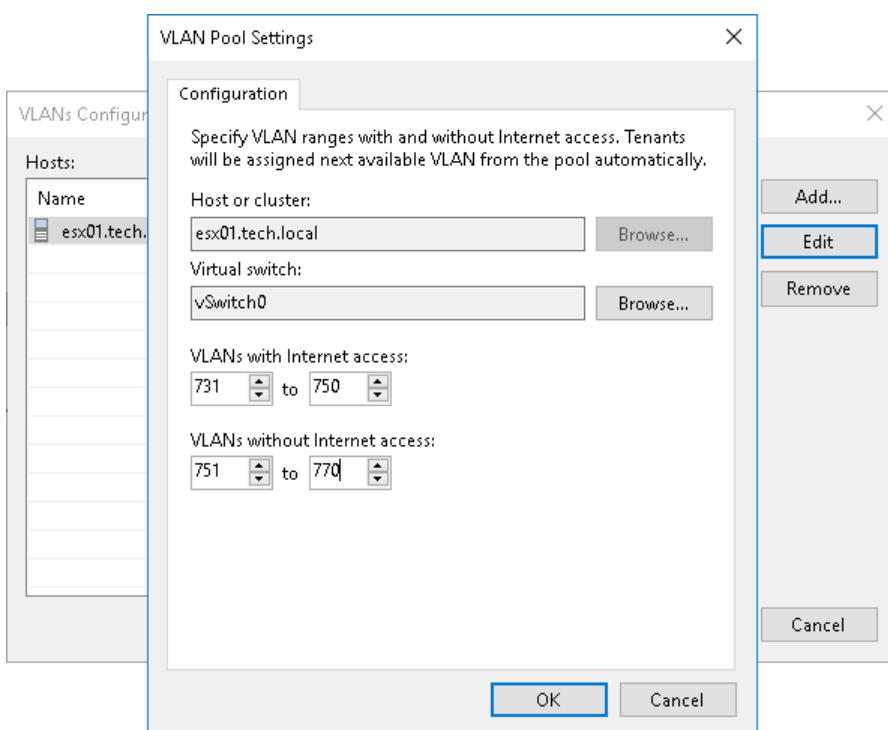
Editing VLAN Ranges

You can edit VLAN ranges configured in Veeam Backup & Replication, if necessary. When you change a VLAN range, tenants to whom VLANs from this range are already allocated will continue to use these VLANs. Veeam Backup & Replication will allocate new VLANs in the edited VLAN range only to those tenants who are subscribed to a hardware plan after the VLAN range was edited.

For example, you change the VLAN range from *1000–2000* to *3000–4000*. In this case, VLANs *1000, 1001,* and so on that are already allocated to tenants will continue to be used by these tenants. Tenants whom the SP subscribes to a hardware plan after the VLAN range was changed will receive VLANs from the new VLAN range: *3000*, *3001*, and so on.

To edit a VLAN range:

1. Open the **VLANs Configuration** window in one of the following ways:

   o Open the **Cloud Connect** view, click the **Cloud Connect** node and click **Manage VLANs** on the ribbon.

   o Open the **Cloud Connect** view, right-click the **Cloud Connect** node and select **Manage VLANs**.

2. In the **VLANs Configuration** window, select the host or cluster for which you want to edit a VLAN range, and click **Edit**.

3. If you want to reserve VLANs on another virtual switch configured on the selected host, in the **VLAN Pool Settings** window, click **Browse** next to the **Virtual switch** field and select the necessary virtual switch.

4. In the **VLANs with Internet access** and **VLANs without Internet access** fields, edit VLAN ranges as required.

5. Click **OK**.
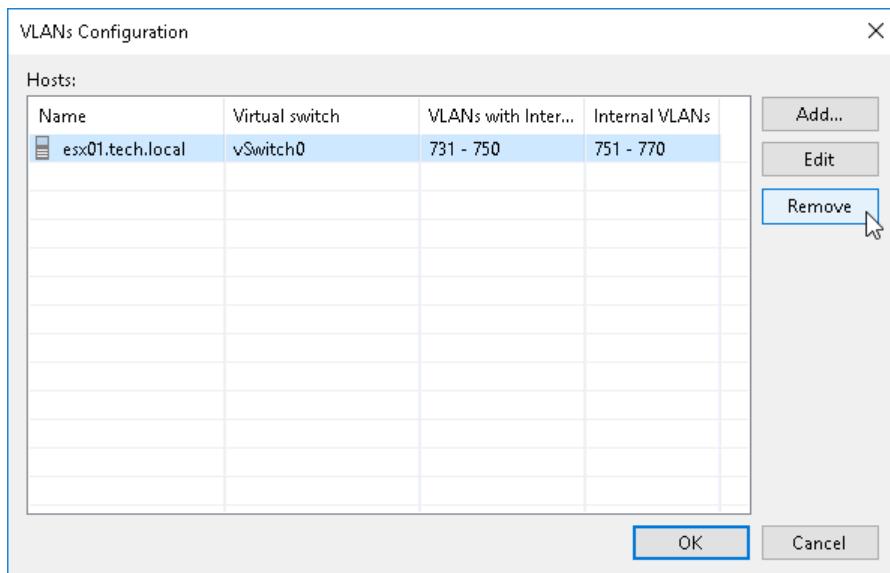
Removing VLAN Ranges

You can remove a VLAN range configured in Veeam Backup & Replication, if necessary. When you remove a VLAN range, tenants to whom VLANs from this range are already allocated will continue to use these VLANs.

To remove a VLAN range:

1. Open the **VLANs Configuration** window in one of the following ways:

   o Open the **Cloud Connect** view, click the **Cloud Connect** node and click **Manage VLANs** on the ribbon.

   o Open the **Cloud Connect** view, right-click the **Cloud Connect** node and select **Manage VLANs**.

2. In the **VLANs Configuration** window, select the host or cluster for which you want to remove a VLAN range, and click **Remove**.

3. In the displayed window, click **Yes**. Then click **OK**.

Managing Public IP Addresses

It might be required that one or several replica VMs should be accessible from the internet after full site failover. To accomplish this, all VM replicas on the cloud host that need to be accessed from the internet must have public IP address.

With Veeam Backup & Replication, the SP can allocate in their network infrastructure a pool of public IP addresses and provide one or several public IP addresses from this pool to the tenant. The tenant can specify public IP addressing settings at the process of the cloud failover plan configuration.

When the tenant's production VM fails over to its replica on the cloud host during full site failover, Veeam Backup & Replication assigns a specified public IP address to the network extension appliance on the SP side. The network extension appliance redirects traffic from this public IP address to the IP address of a VM replica in the internal VM replica network. As a result, a VM replica on the cloud host can be accessed from the internet.

To allocate a pool of public IP addresses, the SP can specify individual IP addresses or IP address ranges. The SP can add to the pool both IPv4 and IPv6 addresses.
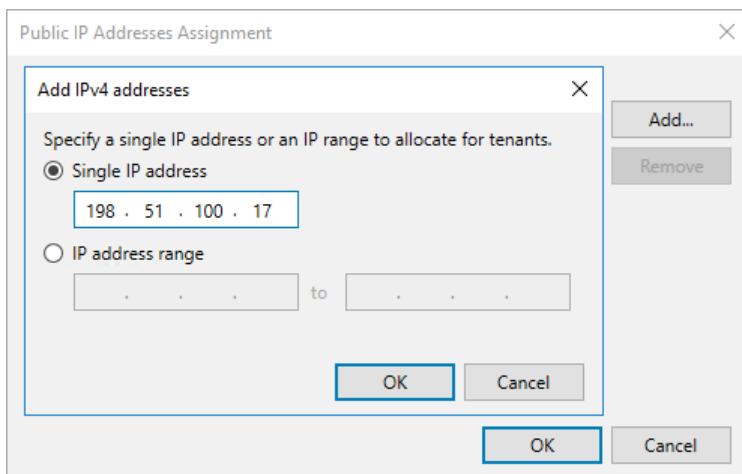
Consider the following:

- The SP does not need to allocate public IP addresses in Veeam Backup & Replication if the SP uses VMware Cloud Director to provide replication resources to tenants. Instead, the SP configures the NSX Edge gateway in the properties of the organization VDC that will be used as a cloud host for tenant VM replicas.

- To enable access to a tenant VM replica by a public IP address, the SP must properly configure port forwarding to the SP network extension appliance in the production network infrastructure.

- It is recommended that the SP plans network resource allocation and allocates public IP addresses in advance. However, the SP can also create or edit a pool of available public IP addresses when subscribing a tenant to a hardware plan. To learn more, see Specify Network Extension Settings.
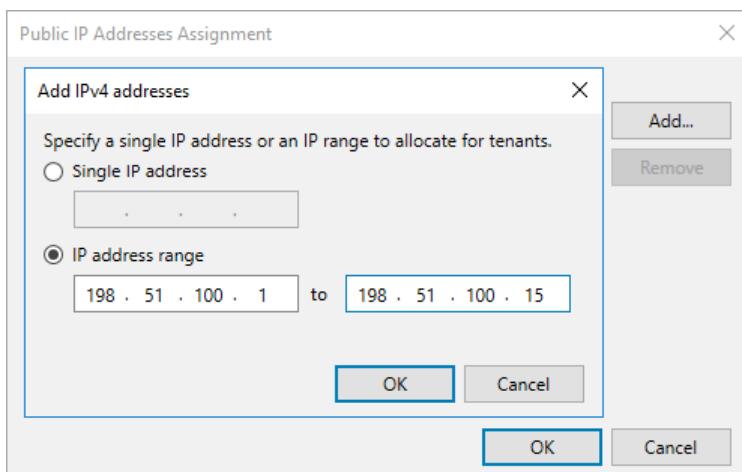
Managing IPv4 Addresses

To configure a pool of public IPv4 addresses:

1. Open the **Public IP Addresses Assignment** window in one of the following ways:

   o Open the **Cloud Connect** view, click the **Cloud Connect** node and click **Manage Public IPs** on the ribbon.

   o Open the **Cloud Connect** view, right-click the **Cloud Connect** node and select **Manage public IP addresses**.

2. In the **Public IP Addresses Assignment** window, click **Add** and select **IPv4 addresses**.

3. In the **Add IPv4 addresses** window, do either of the following:

   o If you want to add to the pool of public IP addresses one IP address, make sure that the **Single IP address** option is selected and specify the necessary IP address.

   o If you want to add to the pool of public IP addresses several IP addresses at a time, select the **IP address range** option and specify the first and the last IP address of the range.
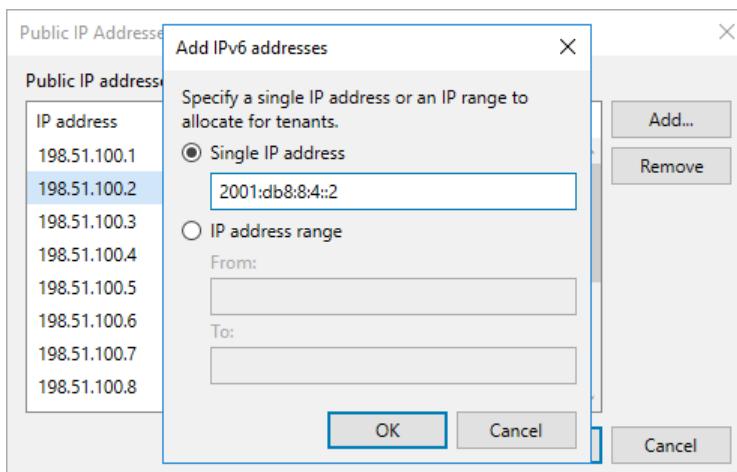
4. Click **OK**.
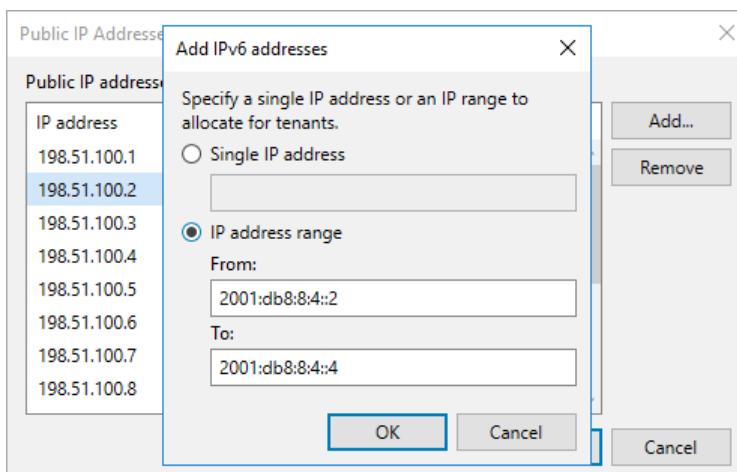
Managing IPv6 Addresses

To configure a pool of public IPv6 addresses:

1. Open the **Public IP Addresses Assignment** dialog window in one of the following ways:

   o Open the **Cloud Connect** view, click the **Cloud Connect** node and click **Manage Public IPs** on the ribbon.

   o Open the **Cloud Connect** view, right-click the **Cloud Connect** node and select **Manage public IP addresses**.

2. In the **Public IP Addresses Assignment** window, click **Add** and select **IPv6 addresses**.

3. In the **Add IPv6 addresses** window, do either of the following:

   o If you want to add to the pool of public IP addresses one IP address, make sure that the **Single IP address** option is selected and specify the necessary IP address.

   o If you want to add to the pool of public IP addresses several IP addresses at a time, select the **IP address range** option and specify the first and the last IP address of the range.

4. Click **OK**.

Managing Network Extension Appliance Credentials

Veeam Backup & Replication connects to the network extension appliance using service credentials — credentials for the root account on the Linux-based network extension appliance VM. You can use these credentials to log on to the network extension appliance VM. This may be useful if you need to configure the network extension appliance manually, for example, for troubleshooting reasons.

It is strongly recommended that you change the password for the root account before subscribing tenants to hardware plans and deploying network extension appliances. You can change the password in the service credentials record using the Credentials Manager.

> **IMPORTANT**
>
> Do not change the password for the service credentials record after you deploy the network extension appliance. If you change the password, all network extension appliances that are already deployed on cloud hosts will become inoperative and need to be redeployed. To learn more, see Redeploying Network Extension Appliance.

To specify a password for the root account of the network extension appliance VM:
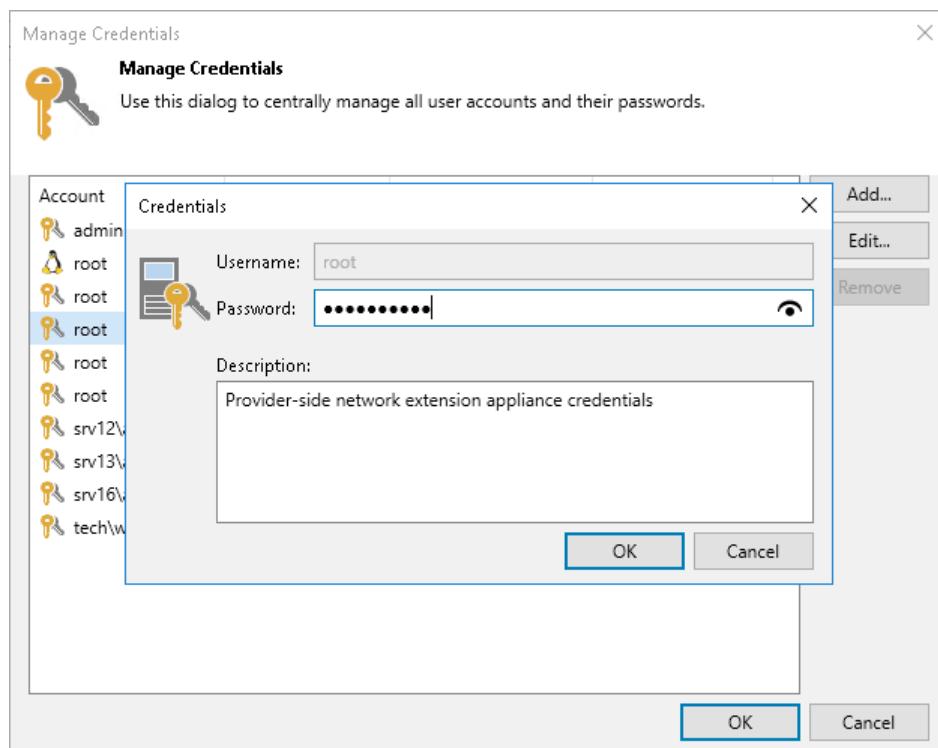
1. From the main menu, select **Credentials and Passwords** > **Datacenter Credentials**.

2. Select the **Provider-side network extension appliance credentials** record and click **Edit**.

3. Veeam Backup & Replication will display a warning notifying that you will need to redeploy existent network extension appliances after you change the password. Click **Yes** to confirm your intention.

4. In the **Password** field, enter a password for the root account. To view the entered password, click and hold the eye icon on the right of the **Password** field.

   The specified password will be assigned to the root account of every network extension appliance VM that will be deployed on the SP side.

5. In the **Description** field, if necessary, change the default description for the edited credentials record.

6. Click **OK** to save the specified password.

> **NOTE**
>
> It is also recommended that tenants change the password for the root account of the tenant-side network extension appliance before connecting to the SP. To learn more, see Managing Credentials.

Registering Tenant Accounts

The procedure of tenant accounts registration is performed by the SP on the SP Veeam backup server.

To let a tenant work with Veeam Cloud Connect backup and replication resources, you must register a tenant account on the SP Veeam backup server. Tenants with registered tenant accounts have access to cloud repositories and cloud hosts. Tenants without accounts cannot connect to the SP and use Veeam Cloud Connect resources.

The SP can create tenant accounts of the following types:

- Standalone tenant account — a regular tenant account. Tenants with account of this type can create backups in a cloud repository and create VM replicas on a cloud host provided to the tenant through a hardware plan.

- Active Directory tenant account — a tenant account that provides access to a cloud repository for Active Directory users. Tenants with account of this type can create Veeam Agent backups in a cloud repository. To learn more about this scenario, see Active Directory Tenant Account.

- VMware Cloud Director tenant account — a tenant account that provides access to VMware Cloud Director resources of the SP. Tenants with account of this type can create backups in a cloud repository and create VM replicas on a cloud host provided to the tenant through an organization VDC. To learn more about this scenario, see VMware Cloud Director Support.

> **NOTE**
>
> Consider the following:
>
> - When you create a tenant account, remember to save a user name and password for the created account. You must pass this data to your tenant. When adding the SP on the tenant Veeam backup server, the tenant must enter the user name and password for the tenant account registered on the SP side.
>
>   This does not apply to Active Directory tenant accounts. For accounts of this type, tenant-side users connect to the SP using their Active Directory account credentials.
>
> - By default, in case the SP backup server is managed by Veeam Service Provider Console version 5.0 or later, you cannot create tenant accounts in Veeam Backup & Replication. You can change this setting in Veeam Service Provider Console. To learn more, see the Managing Veeam Cloud Connect Servers section in the Guide for Service Providers.

Configuring Standalone Tenant Account

To let a tenant work with Veeam Cloud Connect backup and replication resources, you must register a tenant account on the SP Veeam backup server. Tenants with registered tenant accounts have access to cloud repositories and cloud hosts. Tenants without accounts cannot connect to the SP and use Veeam Cloud Connect resources.

Before You Begin
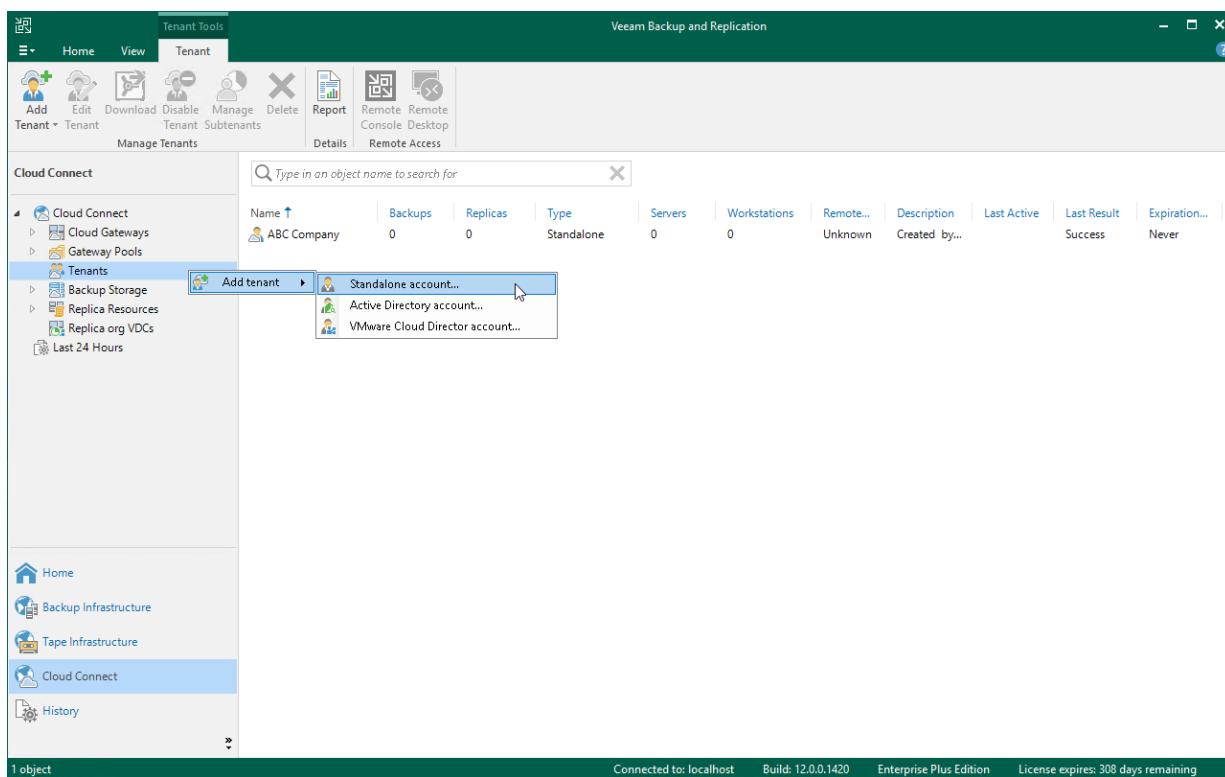
Before you add a new tenant account, check the following prerequisites:

- A TLS certificate must be installed on the SP Veeam backup server.

- At least one cloud gateway must be added in the Veeam Cloud Connect infrastructure on the SP backup server.

- Backup repositories that you plan to use as cloud repositories must be added to your backup infrastructure. When you create a tenant account, you can allocate storage resources for the tenant only on those backup repositories that are currently added to Veeam Backup & Replication.

- Hardware plans that you plan to provide to a tenant must be configured in your Veeam Cloud Connect infrastructure. When you create a tenant account, you can subscribe the tenant only to those hardware plans that are currently configured in Veeam Backup & Replication.

- You can subscribe one tenant to several hardware plans that utilize resources of the same virtualization platform — VMware vSphere or Microsoft Hyper-V. To make it possible for the tenant to replicate VMware and Hyper-V VMs simultaneously, the SP must create two different tenant accounts for the same tenant.

- If tenants will work with the cloud repository and/or the cloud host over WAN accelerators, the target WAN accelerator must be properly configured on the SP side.

- It is recommended that you change the password for the root account of network extension appliances before subscribing tenants to hardware plans. You can change the password using the Credentials Manager. To learn more, see Managing Network Extension Appliance Credentials.

Step 1. Launch New Tenant Wizard

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

- Open the **Cloud Connect** view. Click **Add Tenant** > **Standalone account** on the ribbon.

- Open the **Cloud Connect** view. Click the **Cloud Connect** node in the inventory pane and click the **Standalone Account** link in the working area.

- Open the **Cloud Connect** view. Right-click the **Cloud Connect** node in the inventory pane and select **Add tenant** > **Standalone account**.

- Open the **Cloud Connect** view. Click the **Tenants** node in the inventory pane and click **Add Tenant** > **Standalone account** on the ribbon.

- Open the **Cloud Connect** view. Right-click the **Tenants** node in the inventory pane or right-click anywhere in the working area and select **Add tenant** > **Standalone account**.
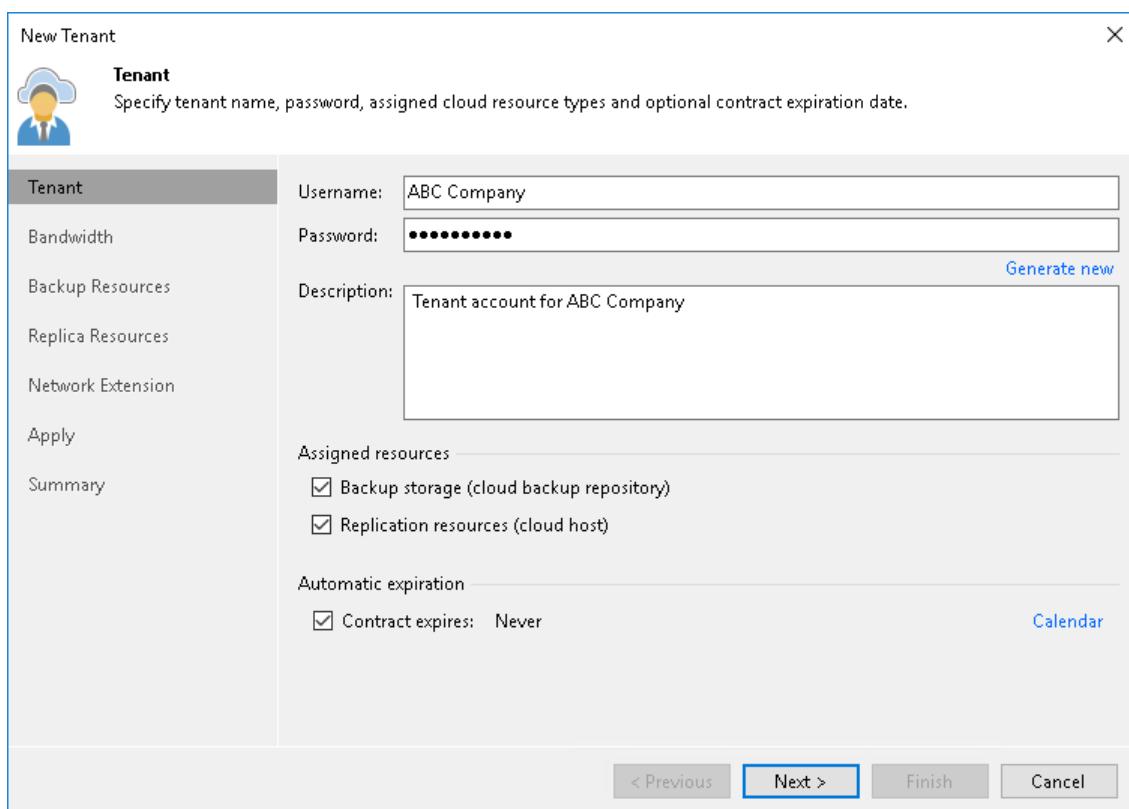
Step 2. Specify Tenant Settings

At the **Tenant** step of the wizard, specify tenant account and lease settings for the tenant. Lease settings apply to all quotas and hardware plans assigned to the tenant.

1. In the **Username** field, specify a name for the created tenant account. The user name must meet the following requirements:

    o   The maximum length of the user name is 128 characters. It is recommended that you create short user names to avoid problems with long paths to backup files on the cloud repository.

    o   The user name may contain space characters.

    o   The user name must not contain the following characters: ,\/:*?\"<>|=;@& as well as Unicode characters.

    o   The user name must not end with the period character [.].

2. In the **Password** field, provide the password for the tenant account. You can enter your own password or click the **Generate new** link at the bottom of the field. In the latter case, Veeam Backup & Replication will generate a safe password. You will be able to get a copy the generated password at the last step of the wizard.

3. In the **Description** field, specify a description for the created tenant account. The default description contains information about the user who created the account, date and time when the account was created.

4. In the **Assigned resources** section, select what types of Veeam Cloud Connect resources you want to provide to the tenant:

    o   **Backup storage** — Cloud Connect Backup resources. With this option enabled, the **New Tenant** wizard will include an additional **Backup Resources** step. At the **Backup Resources** step of the wizard, you can assign a quota on the cloud repository to the tenant. To learn more, see Allocate Backup Resources.

    o   **Replication resources** — Cloud Connect Replication resources. With this option enabled, the **New Tenant** wizard will include an additional **Replica Resources** step. At the **Replica Resources** step of the wizard, you can subscribe the tenant to a hardware plan. To learn more, see Allocate Replica Resources.

5. To specify lease settings for the tenant account, select the **Contract expires** check box and click the **Calendar** link. In the **Select expiration date** window, select a date when the lease period must terminate.

    If you do not select the **Contract expires** option, the tenant will be able to use Veeam Cloud Connect resources for an indefinite period of time.

Step 3. Specify Bandwidth Settings

At the **Bandwidth** step of the wizard, specify task and bandwidth limitation settings for the tenant. Limiting bandwidth and parallel data processing capabilities for tenants helps avoid overload of cloud gateways, backup proxies, backup repositories and network equipment on the SP side.

1. In the **Max concurrent tasks** field, specify the maximum number of concurrent tasks for the tenant. If this value is exceeded, Veeam Backup & Replication will not start a new task until one of current tasks finishes. To learn more, see Parallel Data Processing.

   > **NOTE**
   >
   > The specified number of concurrent tasks will be available to the tenant regardless of the number of concurrent tasks defined in the properties of a cloud repository exposed to this tenant.

2. To limit the data traffic coming from the tenant side to the SP side, select the **Limit network traffic from this tenant to** check box. With this option enabled, you can specify the maximum speed for transferring tenant data to the SP side.

   This option also applies to the traffic coming from a cloud repository in the replica from backup and replica seeding scenarios.

3. In the **Gateway pool** field, specify what cloud gateways will be available to the tenant. By default, the tenant can use cloud gateways that are not added to any cloud gateway pool. To use this option, make sure that *Automatic selection* is displayed in the **Gateway pool** field.

   If you want to assign a cloud gateway pool to the tenant, click **Choose** on the right of the **Gateway pool** field and select one or more cloud gateway pools. To learn more, see Assigning Cloud Gateway Pools.

# Assigning Cloud Gateway Pools

You can assign to the tenant one or more cloud gateway pools configured in the Veeam Cloud Connect infrastructure. After you assign a cloud gateway pool to the tenant, communication between the tenant backup server and Veeam Cloud Connect infrastructure components in the SP side will be possible only through cloud gateways added to this pool. You can also allow the tenant to fail over to a cloud gateway that is not added to a cloud gateway pool. This may be useful in a situation where all cloud gateways in the cloud gateway pool assigned to the tenant are unavailable for some reason.

To assign a cloud gateway pool to the tenant:

1. At the **Bandwidth** step of the wizard, click **Choose** on the right of the **Gateway pool** field.

2. In the **Gateway Pool** window, select **Use the selected gateway pools**.

3. In the list of available cloud gateway pools, select check boxes next to one or more pools that you want to assign to the tenant. The list of available cloud gateway pools contains pools that you configured in the Veeam Cloud Connect infrastructure.

   To select or clear all check boxes in the list at once, you can use the **Select All** and **Clear All** buttons.

4. [Optional] You can allow the tenant to fail over to a cloud gateway that is not added to the selected cloud gateway pool in case all cloud gateways in the pool are unavailable for some reason. To do this, select the **Failover to other cloud gateways if all gateways from the selected pool are unavailable** check box.

5. Click **OK**.

Step 4. Allocate Backup Resources

The **Backup Resources** step of the wizard is available if you selected the **Backup storage** option at the Tenant step of the wizard. You can use this step to specify cloud repository quota settings for the created tenant account. You can assign to the tenant a single quota on one cloud repository or several quotas on different cloud repositories.

To assign a cloud repository quota:

1. Click **Add** on the right of the **Cloud repositories** list.

2. In the **Cloud repository name** field of the **Set Quota** window, enter a friendly name for the cloud repository you want to present to the tenant. The name you enter will be displayed in the list of backup repositories at tenant's side.

3. From the **Backup repository** list, select a backup repository in your backup infrastructure whose space resources must be allocated to the tenant.

4. In the **User quota** field, specify the amount of space you want to allocate to the tenant on the selected backup repository.

5. [For tenants who plan use WAN accelerators] Select the **Enable WAN acceleration through the following WAN accelerator** check box and choose a target WAN accelerator configured at the SP side. The source WAN accelerator is configured on the tenant side. The tenant will select the source WAN accelerator on their side when configuring a backup copy job.

6. Click **OK**.

7. Repeat steps 1–6 for all backup repositories in your backup infrastructure whose resources you want to allocate to the tenant.

8. If you want to protect tenant backups against unwanted deletion, select the **Keep deleted backup files for <N> days** check box and specify the number of days to keep a backup in the recycle bin after a backup is deleted by the tenant. To learn more, see Insider Protection.

NOTE

Consider the following:

- With the **Keep deleted backup files for <N> days** option enabled, Veeam Backup & Replication will disable retention policy for deleted VMs specified in the properties of a tenant backup job. To avoid keeping redundant data in a cloud repository, it is recommended that the SP enables the **Use per-VM backup files** option in the properties of the backup repository whose storage resources the SP exposes to tenants as cloud repositories.
- If the **Keep deleted backup files for <N> days** option is enabled in the properties of the tenant account, and the **Use per-VM backup files** option is not enabled in the properties of the backup repository whose storage resources the SP exposes to the tenant, the tenant will be unable to remove individual VMs from backups in the cloud repository. When the tenant starts the *Delete from disk* operation for a specific VM in the backup, the operation will complete with an error.
- The **Keep deleted backup files for <N> days** option is not available if the SP allocates to the tenant a quota on an object storage repository.

Step 5. Allocate Replication Resources

The **Replica Resources** step of the wizard is available if you selected the **Replication resources** option at the Tenant step of the wizard. You can use this step to subscribe the created tenant account to the hardware plan.

To subscribe a tenant to a hardware plan:

1. Click **Add** on the right of the **Hardware plans** list and select *VMware or Hyper-V*.

2. From the **Select hardware plan** list in the **Add replication resource** window, select a hardware plan to which you want to subscribe the tenant.

3. [For tenants who plan to use WAN accelerators] Select the **Enable WAN acceleration through the following WAN accelerator** check box and choose a target WAN accelerator configured at the SP side. The source WAN accelerator is configured on the tenant side. The tenant will select the source WAN accelerator on their side when configuring a replication job.

4. Click **OK**.

5. Repeat steps 1–4 for all hardware plans to which you want to subscribe the tenant.

6. Select the **Use Veeam network extension capabilities during partial and full site failover** option to allocate network resources for performing failover tasks. With this option enabled, the **New Tenant** wizard will include the additional Network Extension step.

7. To configure range of VLANs that will be used for providing isolated IP networks for tenant VM replicas on the cloud host, click the **Manage network settings** link. Then use the **VLANs Configuration** window to specify the necessary number of VLANs on the virtualization host that provides resources for the hardware plan to which the tenant is subscribed. To learn more, see Managing VLANs.

Step 6. Specify Network Extension Settings

The **Network Extension** step of the wizard is available if you selected the **Use Veeam network extension capabilities during partial and full site failover** option at the Replica Resources step of the wizard. You can use this step to specify network settings for the network extension appliance that Veeam Backup & Replication will deploy on the SP side.

Veeam Backup & Replication deploys the network extension appliance on the SP virtualization host that provides resources for the hardware plan to which the SP subscribes the tenant. VM replicas on the cloud host use the SP network extension appliance:
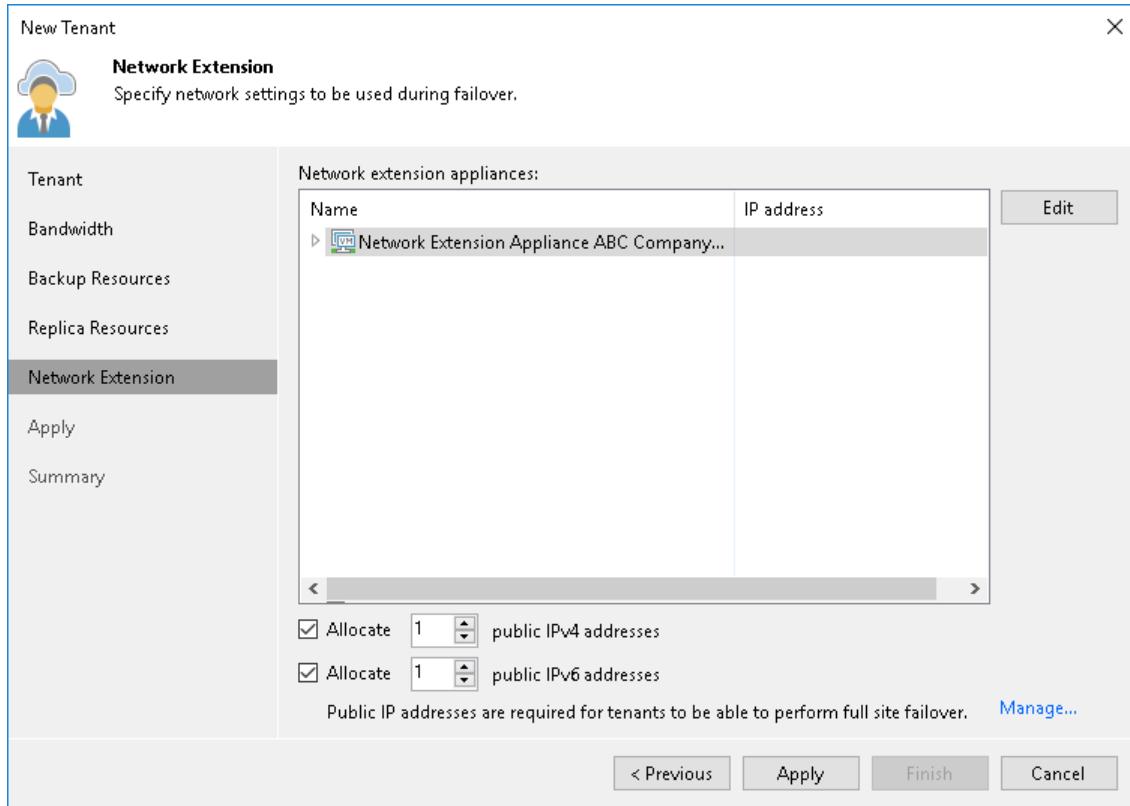
- To communicate to VMs in the production site after partial site failover.

- To communicate to the internet after full site failover.

At the **Network Extension** step of the wizard, the SP configures one network adapter (vNIC) on the network extension appliance. This network adapter connects the network extension appliance to the external network where SP backup infrastructure components reside.

To set up the network extension appliance:

1. Click **Edit** on the right of the **Network extension appliances** list.

2. In the **Network Settings** window, in the **Network extension appliance** field, check and edit if necessary the name for the network extension appliance.

3. Click the **Browse** button next to the **External network** field and select the SP production network to which the SP Veeam Backup & Replication infrastructure components are connected.

4. Specify the IP addressing settings for the configured network extension appliance:

   o To assign an IP address automatically in case there is a DHCP server in your network, make sure that the *Obtain automatically* value is displayed in the **IPv4 address** and **IPv6 address** fields.

   o To manually assign a specific IP address to the appliance, click **Configure** and specify network settings for the appliance. For details, see Specifying Network Settings.

5. Click **OK**.

6. [Optional] If you have not reserved in advance the necessary number of public IP addresses that can be assigned to VM replicas, click the **Manage** link to add one or several IP addresses to the pool of available public IP addresses. To learn more, see Managing Public IP Addresses.

7. Select the **Allocate <N> public IPv4 addresses** option and specify the number of public IPv4 addresses to provide VM replicas with the ability to be accessed from the internet after full site failover. Veeam Backup & Replication will automatically assign to the tenant the specified number of IPv4 addresses from the reserved pool. A tenant will be able to map an available public IPv4 address to a VM replica at the process of the cloud failover plan configuration. To learn more, see Specify Public IP Addressing Rules.

8. Select the **Allocate <N> public IPv6 addresses** option and specify the number of public IPv6 addresses to provide VM replicas with the ability to be accessed from the internet after full site failover. Veeam Backup & Replication will automatically assign to the tenant the specified number of IPv6 addresses from the reserved pool. A tenant will be able to map an available public IPv6 address to a VM replica at the process of the cloud failover plan configuration. To learn more, see Specify Public IP Addressing Rules.

Specifying Network Settings

To specify network settings for the network extension appliance:

1. In the **Network Settings** window, click **Configure**.

2. To manually assign a specific IPv4 address to the appliance, do the following:

   a. On the **IPv4** tab, make sure that the **Enable IPv4 interface** check box is selected.

   b. Select the **Use the following IP address** option and specify the following network settings:

      ▪ IP address

      ▪ Subnet mask

      ▪ Default gateway

   Alternatively, if you want to assign an IPv4 address automatically, make sure that the **Obtain an IP address automatically** option is selected on the **IPv4** tab.

   If you do not want the network extension appliance to use an IPv4 address, clear the **Enable IPv4 interface** check box.

3. If you want to assign an IPv6 address to the appliance, do the following:

   a. Click the **IPv6** tab.

   b. Make sure that the **Enable IPv6 interface** check box is selected.

   c. Select the **Use the following IP address** option and specify the following network settings:

      ▪ IP address

      ▪ Subnet mask (prefix length)

      ▪ Default gateway

   Alternatively, if you want to assign an IPv6 address automatically, make sure that the **Obtain an IP address automatically** option is selected on the **IPv6** tab.

   If you do not want the network extension appliance to use an IPv6 address, clear the **Enable IPv6 interface** check box.

4. Click **OK**.

Step 7. Assess Results

The **Apply** step is available if you selected the **Replication resources** option at the **Tenant** step of the wizard.

At this of the wizard, Veeam Backup & Replication will assign the cloud resources to the tenant. Wait for the required operations to complete and click **Next** to continue.

Step 8. Finish Working with Wizard

At the **Summary** step of the wizard, complete the procedure of tenant account registration.

1. Click the **Copy password to clipboard** link at the bottom of the wizard window. You must send the copied password to the tenant so that the tenant can connect to the SP using the created tenant account.

2. Review the information about the added tenant account and click **Finish** to exit the wizard.

What You Do Next

After the SP creates a tenant account, the SP must communicate the following information to the tenant:

1. User name and password for the created account.

2. Full DNS name or IP address of the cloud gateway over which the tenant will communicate with the Veeam Cloud Connect infrastructure:

   o If the SP did not assign a cloud gateway pool to the tenant, the SP can provide information about any cloud gateway configured in the Veeam Cloud Connect infrastructure that is not part of a cloud gateway pool. When the tenant adds the SP in the tenant Veeam backup console, the Veeam backup server on tenant side will obtain a list of all cloud gateways that are not added to a cloud gateway pool. If the primary cloud gateway is unavailable, the Veeam backup server on the tenant side will fail over to another cloud gateway from the list.

   o If the SP assigned a cloud gateway pool to the tenant, the SP can provide information about any cloud gateway added to this gateway pool. When the tenant adds the SP in the tenant Veeam backup console, the Veeam backup server on tenant side will obtain a list of all cloud gateways in the pool. If the primary cloud gateway is unavailable, the Veeam backup server on the tenant side will fail over to another cloud gateway in the same pool.

3. External port for the cloud gateway (if the SP has specified a non-default port).

4. [If Dell Data Domain is used as a cloud repository] Information about the backup chain limitations. The length of forward incremental and forever forward incremental backup chains that contain one full backup and a set of subsequent incremental backups cannot be greater than 60 restore points. To overcome this limitation, tenants can schedule full backups (active or synthetic) to split the backup chain into shorter series. For example, to perform backups at 30-minute intervals, 24 hours a day, tenants must schedule synthetic full backups every day. In this scenario, intervals immediately after midnight may be skipped due to the duration of synthetic processing.

Configuring Active Directory Tenant Account

To provide a user of an Active Directory domain with access to cloud repository resources, you must register an Active Directory tenant account on the SP Veeam backup server. Tenants with registered Active Directory tenant accounts can connect to the SP in Veeam Agent for Microsoft Windows using their AD credentials and create Veeam Agent backups in a cloud repository. Tenants with accounts of other types can use subtenant accounts to back up data with Veeam Agent.

Before You Begin
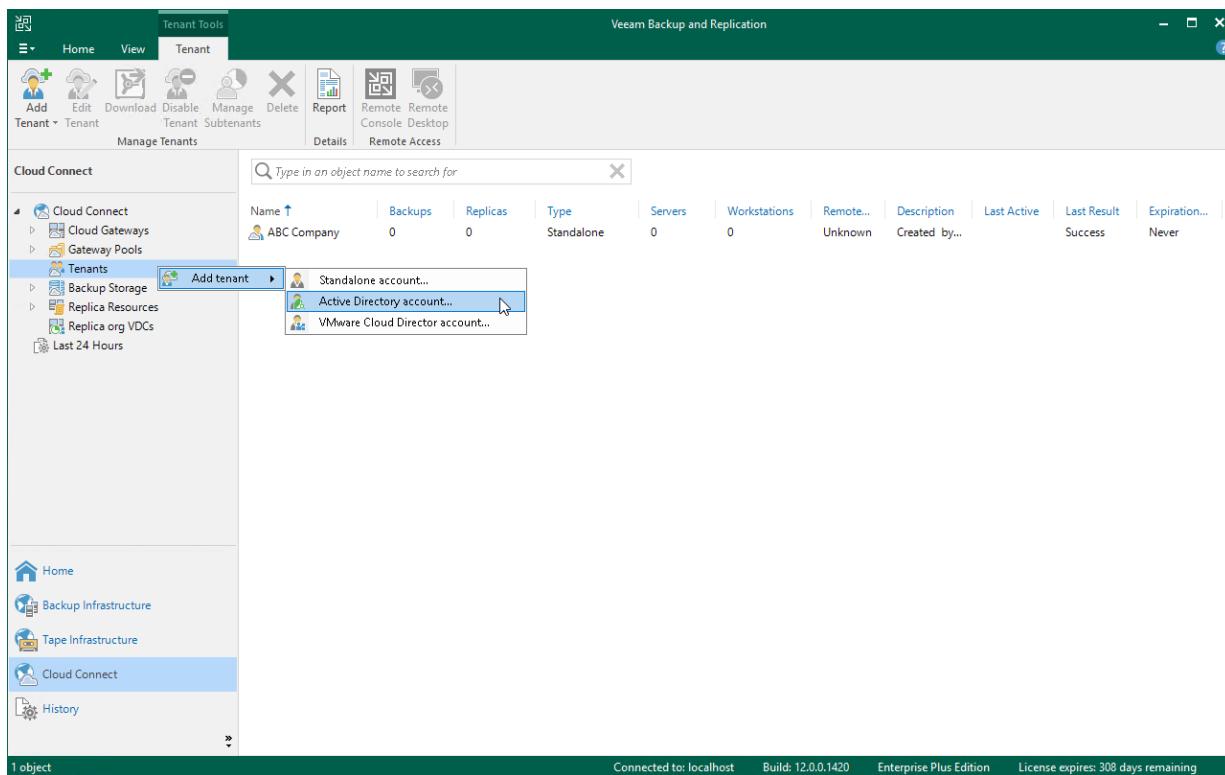
Before you add a new Active Directory tenant account, check the following prerequisites:

- A TLS certificate must be installed on the SP Veeam backup server.

- At least one cloud gateway must be added in the Veeam Cloud Connect infrastructure on the SP backup server.

- Backup repositories that you plan to use as cloud repositories must be added to your backup infrastructure. When you create a tenant account, you can allocate storage resources for the tenant only on those backup repositories that are currently added to Veeam Backup & Replication.

- You must have access to the domain controller of an Active Directory domain for whose user you want to create a tenant account. You will be able to select an account to connect to the domain controller when adding the Active Directory tenant account.

- Make sure that you have familiarized yourself with considerations and limitations for the Active Directory tenant account functionality.

Step 1. Launch New Tenant Wizard

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

- Open the **Cloud Connect** view. Click **Add Tenant** > **Active Directory account** on the ribbon.

- Open the **Cloud Connect** view. Click the **Cloud Connect** node in the inventory pane and click the **Active Directory User** link in the working area.

- Open the **Cloud Connect** view. Right-click the **Cloud Connect** node in the inventory pane and select **Add tenant** > **Active Directory account**.

- Open the **Cloud Connect** view. Click the **Tenants** node in the inventory pane and click **Add Tenant** > **Active Directory account** on the ribbon.

- Open the **Cloud Connect** view. Right-click the **Tenants** node in the inventory pane or right-click anywhere in the working area and select **Add tenant** > **Active Directory account**.

Step 2. Specify Tenant Settings

At the **AD Account** step of the wizard, specify tenant account and lease settings for the tenant. Lease settings apply to all quotas assigned to the tenant.

1. Click **Change** next to the **Domain** field.

2. In the **Specify Domain** window, specify settings of the Active Directory domain for whose user you want to create a tenant account:

   a. In the **Domain DNS name** field, type a name of the domain or domain controller.

   It is recommended to specify domain DNS name to allow automatic LDAP connection failover between domain controllers.

   b. In the **Port** field, specify a port number over which Veeam Backup & Replication will communicate with a domain controller that uses the LDAP protocol. By default, Veeam Backup & Replication uses port 389.

   You can also use the LDAPS (Secure LDAP) protocol if domain controllers in the domain are configured to use it. To communicate with a domain controller over the LDAPS protocol, Veeam Backup & Replication uses port 636.

   c. From the **Account** list, select a user account that will be used for LDAP connections to domain controllers.

   By default, the *Veeam backup service account* option is selected in the **Account** list. With this option selected, Veeam Backup & Replication will use the account under which the Veeam Backup Service runs to connect to a domain controller.

   The *Veeam backup service account* option is intended for the scenario where the SP backup server is a member of the domain whose AD accounts you want to use as tenant accounts or a domain that trusts this domain. In other cases, select a specific account that is a member of the *Domain Users* group in the target domain.

   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 the Credentials Manager section in the Veeam Backup & Replication User Guide.
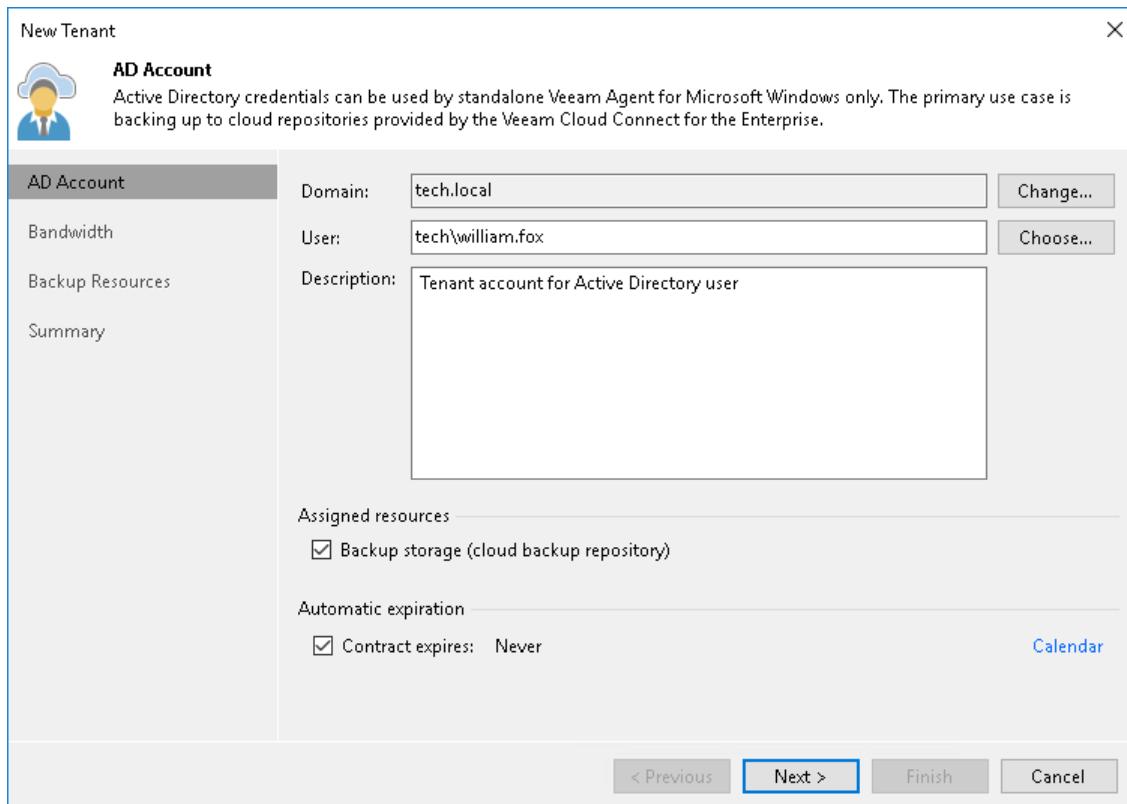
   d. Click **OK** to close the **Specify Domain** window.

3. Click **Choose** next to the **User** field and specify an Active Directory user account for which you want to create a tenant account.

   Alternatively, type an account name in the *DOMAIN\Username* format.

   Note that it can be possible to specify the account name in the *Username* format. However, it is not recommended to use this format.

4. In the **Description** field, specify a description for the created tenant account. The default description contains information about the user who created the account, date and time when the account was created.

5. To assign cloud repository resources to the tenant account, select the **Backup storage** check box. You will be able to specify cloud repository quota settings at the Backup Resources step of the wizard.

   Note that you cannot assign replication resources to an Active Directory tenant account.

6. To specify lease settings for the tenant account, select the **Contract expires** check box and click the **Calendar** link. In the **Select expiration date** window, select a date when the lease period must terminate.

If you do not select the **Contract expires** option, the tenant will be able to use Veeam Cloud Connect resources for an indefinite period of time.

Step 3. Specify Bandwidth Settings

At the **Bandwidth** step of the wizard, specify task and bandwidth limitation settings for the tenant. Limiting bandwidth and parallel data processing capabilities for tenants helps avoid overload of cloud gateways, backup proxies, backup repositories and network equipment on the SP side.

1. In the **Max concurrent tasks** field, specify the maximum number of concurrent tasks for the tenant. If this value is exceeded, Veeam Backup & Replication will not start a new task until one of current tasks finishes. To learn more, see Parallel Data Processing.

   > **NOTE**
   >
   > The specified number of concurrent tasks will be available to the tenant regardless of the number of concurrent tasks defined in the properties of a cloud repository exposed to this tenant.

2. To limit the data traffic coming from the tenant side to the SP side, select the **Limit network traffic from this tenant to** check box. With this option enabled, you can specify the maximum speed for transferring tenant data to the SP side.

   This option also applies to the traffic coming from a cloud repository in the replica from backup and replica seeding scenarios.

3. In the **Gateway pool** field, specify what cloud gateways will be available to the tenant. By default, the tenant can use cloud gateways that are not added to any cloud gateway pool. To use this option, make sure that the *Automatic selection* option is displayed in the **Gateway pool** field.

   If you want to assign a cloud gateway pool to the tenant, click **Choose** on the right of the **Gateway pool** field and select one or more cloud gateway pools. To learn more, see Assigning Cloud Gateway Pools.

Assigning Cloud Gateway Pools

You can assign to the tenant one or more cloud gateway pools configured in the Veeam Cloud Connect infrastructure. After you assign a cloud gateway pool to the tenant, communication between the tenant backup server and Veeam Cloud Connect infrastructure components in the SP side will be possible only through cloud gateways added to this pool. You can also allow the tenant to fail over to a cloud gateway that is not added to a cloud gateway pool. This may be useful in a situation where all cloud gateways in the cloud gateway pool assigned to the tenant are unavailable for some reason.

To assign a cloud gateway pool to the tenant:

1. At the **Bandwidth** step of the wizard, click **Choose** on the right of the **Gateway pool** field.

2. In the **Gateway Pool** window, select **Use the selected gateway pools**.

3. In the list of available cloud gateway pools, select check boxes next to one or more pools that you want to assign to the tenant. The list of available cloud gateway pools contains pools that you configured in the Veeam Cloud Connect infrastructure.

   To select or clear all check boxes in the list at once, you can use the **Select All** and **Clear All** buttons.

4. [Optional] You can allow the tenant to fail over to a cloud gateway that is not added to the selected cloud gateway pool in case all cloud gateways in the pool are unavailable for some reason. To do this, select the **Failover to other cloud gateways if all gateways from the selected pool are unavailable** check box.

5. Click **OK**.

Step 4. Allocate Backup Resources

The **Backup Resources** step of the wizard is available if you selected the **Backup storage** check box at the AD Account step of the wizard. At this step of the wizard, specify cloud repository quota settings for the created tenant account. You can assign to the tenant a single quota on one cloud repository or several quotas on different cloud repositories.
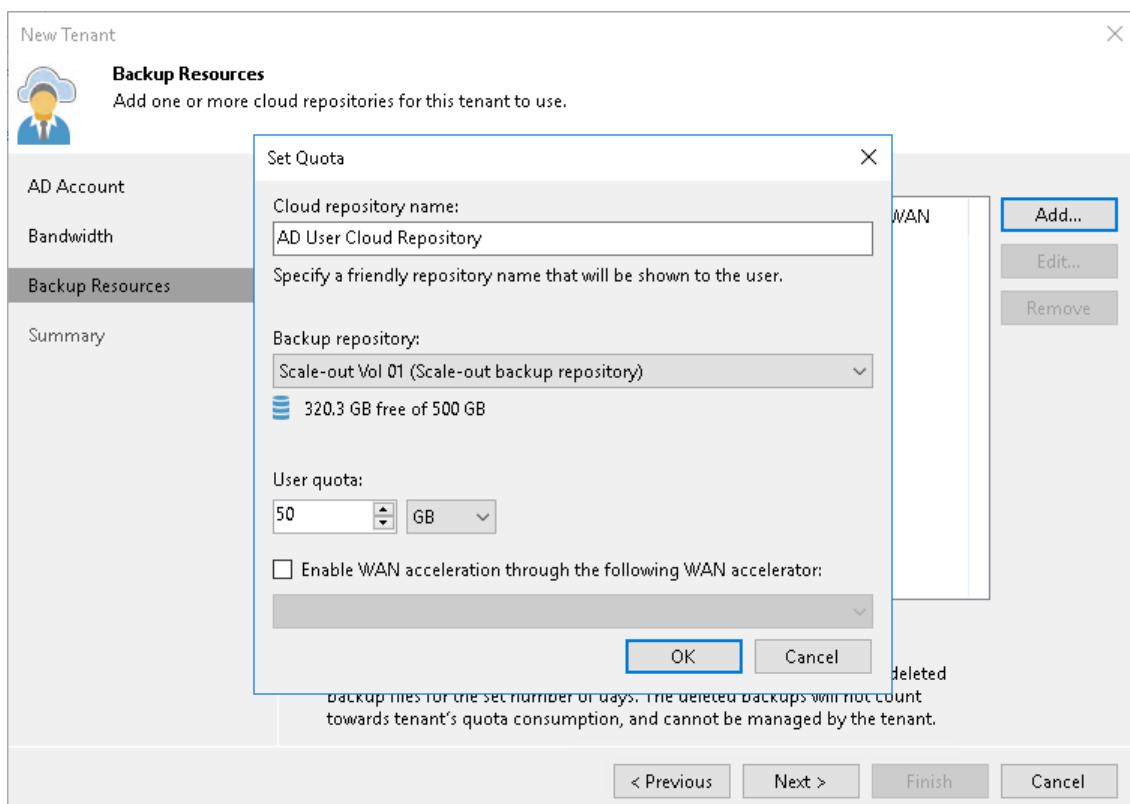
To assign a cloud repository quota:

1. Click **Add** on the right of the **Cloud repositories** list.

2. In the **Cloud repository name** field of the **Set Quota** window, enter a friendly name for the cloud repository you want to present to the tenant. The name you enter will be displayed in the list of backup repositories on the tenant side.

3. From the **Backup repository** list, select a backup repository in your backup infrastructure whose space resources must be allocated to the tenant.

4. In the **User quota** field, specify the amount of space you want to allocate to the tenant on the selected backup repository.

5. Click **OK**.

6. Repeat steps 1–5 for all backup repositories in your backup infrastructure whose resources you want to allocate to the tenant.

7. If you want to protect tenant backups against unwanted deletion, select the **Keep deleted backup files for <N> days** check box and specify the number of days to keep a backup in the recycle bin after a backup is deleted by the tenant. To learn more, see Insider Protection.

NOTE

Consider the following:
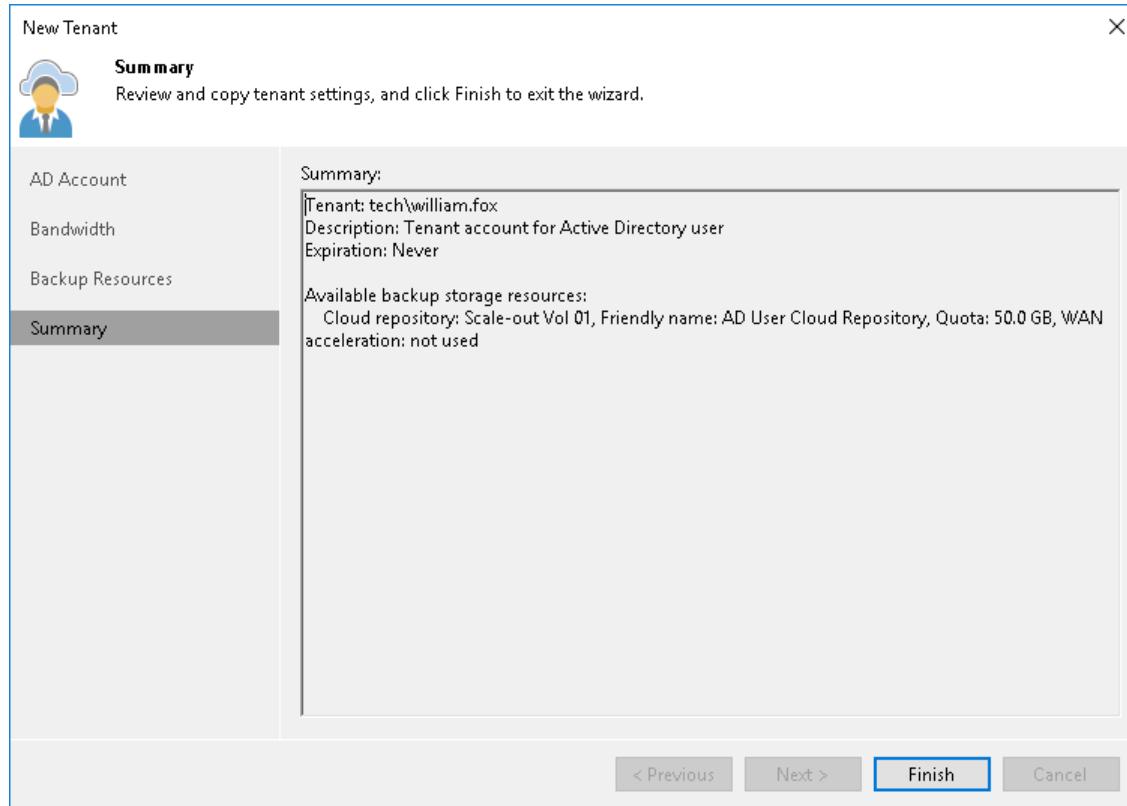
- The **Enable WAN acceleration through the following WAN accelerator** option does not apply to Active Directory tenant accounts. Tenants with accounts of this type connect to the SP in Veeam Agent for Microsoft Windows and cannot specify a source WAN accelerator in Veeam Agent.
- With the **Keep deleted backup files for <N> days** option enabled, Veeam Backup & Replication will disable retention policy for deleted VMs specified in the properties of a tenant backup job. To avoid keeping redundant data in a cloud repository, it is recommended that the SP enables the **Use per-VM backup files** option in the properties of the backup repository whose storage resources the SP exposes to tenants as cloud repositories.
- If the **Keep deleted backup files for <N> days** option is enabled in the properties of the tenant account, and the **Use per-VM backup files** option is not enabled in the properties of the backup repository whose storage resources the SP exposes to the tenant, the tenant will be unable to remove individual VMs from backups in the cloud repository. When the tenant starts the *Delete from disk* operation for a specific VM in the backup, the operation will be completed with an error.
- The **Keep deleted backup files for <N> days** option is not available if the SP allocates to the tenant a quota on an object storage repository.

Step 5. Finish Working with Wizard

At the **Summary** step of the wizard, complete the procedure of tenant account registration.

1. Review the information about the added tenant account.

2. Click **Finish** to exit the wizard.

What You Do Next

After the SP creates a tenant account, the SP must communicate the following information to the tenant:

1. Full DNS name or IP address of the cloud gateway over which the tenant will communicate with the Veeam Cloud Connect infrastructure:

   o If the SP did not assign a cloud gateway pool to the tenant, the SP can provide information about any cloud gateway configured in the Veeam Cloud Connect infrastructure that is not part of a cloud gateway pool. When the tenant adds the SP in the tenant Veeam backup console, the Veeam backup server on tenant side will obtain a list of all cloud gateways that are not added to a cloud gateway pool. If the primary cloud gateway is unavailable, the Veeam backup server on the tenant side will fail over to another cloud gateway from the list.

   o If the SP assigned a cloud gateway pool to the tenant, the SP can provide information about any cloud gateway added to this gateway pool. When the tenant adds the SP in the tenant Veeam backup console, the Veeam backup server on tenant side will obtain a list of all cloud gateways in the pool. If the primary cloud gateway is unavailable, the Veeam backup server on the tenant side will fail over to another cloud gateway in the same pool.

2. External port for the cloud gateway (if the SP has specified a non-default port).

3. [If Dell Data Domain is used as a cloud repository] Information about the backup chain limitations. The length of backup chains that contain one full backup and a set of subsequent incremental backups cannot be greater than 60 restore points. To overcome this limitation, tenants can schedule full backups (active or synthetic) to split the backup chain into shorter series. For example, to perform backups at 30-minute intervals, 24 hours a day, tenants must schedule synthetic fulls every day. In this scenario, intervals immediately after midnight may be skipped due to the duration of synthetic processing.

Configuring VMware Cloud Director Tenant Account

To let a tenant work with a cloud host that utilizes VMware Cloud Director resources, you must register a VMware Cloud Director tenant account on the SP Veeam backup server. Tenants with registered VMware Cloud Director accounts have access to organization VDCs exposed as cloud hosts for tenant VM replicas. Tenants without VMware Cloud Director accounts cannot create VM replicas on cloud hosts that utilize VMware Cloud Director resources of the SP.

Before You Begin
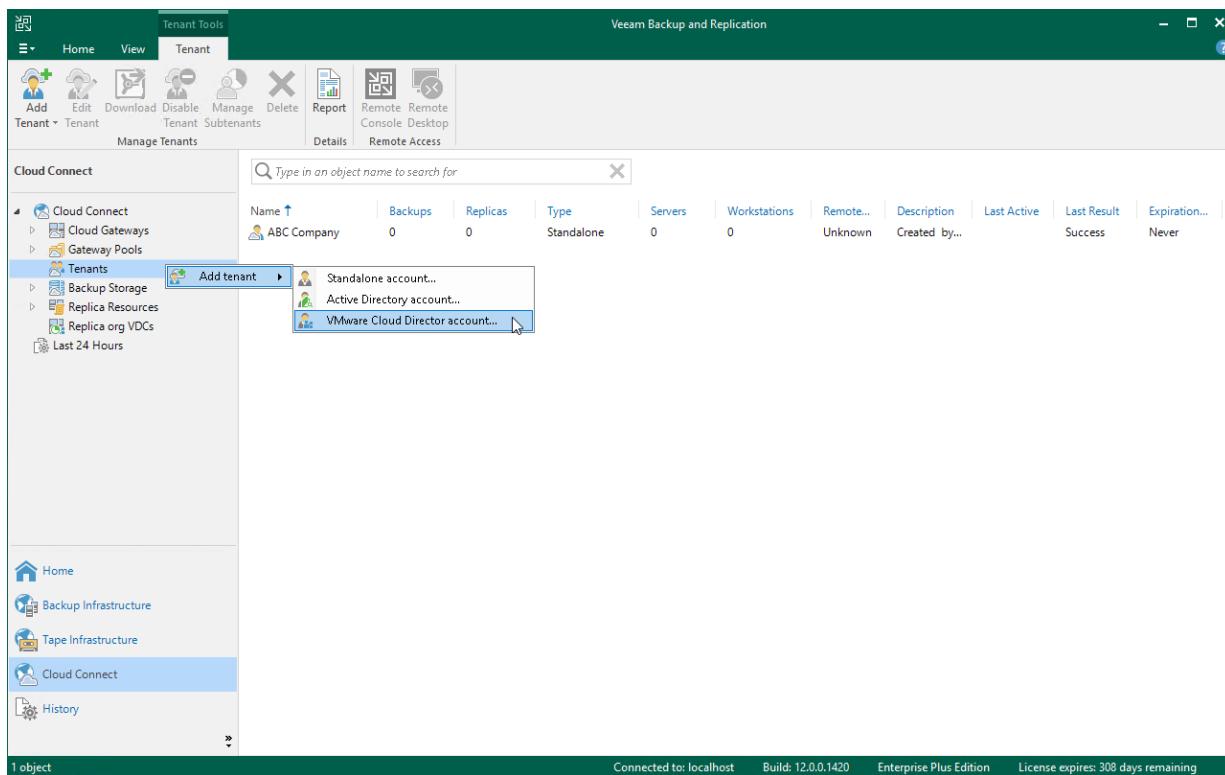
Before you add a new VMware Cloud Director tenant account, check the following prerequisites and limitations:

- A TLS certificate must be installed on the SP Veeam backup server.

- At least one cloud gateway must be added in the Veeam Cloud Connect infrastructure on the SP backup server.

- The VMware Cloud Director Server must be added to the Veeam backup infrastructure on the SP backup server.

- The organization whose organization VDCs you plan to provide as a cloud host for tenant VM replicas must be created in VMware Cloud Director.

- The organization administrator user account must be created for the organization in VMware Cloud Director.

- Organization VDC that you plan to provide as a cloud host for tenant VM replicas must be allocated to the organization in VMware Cloud Director.

- An NSX Edge Gateway or IPsec VPN connection must be configured for the organization in VMware Cloud Director (in case you plan to use VMware Cloud Director resources to provide network access to tenant VM replicas after failover).

- Backup repositories that you plan to use as cloud repositories must be added to your backup infrastructure. When you create a tenant account, you can allocate storage resources for the tenant only on those backup repositories that are currently added to Veeam Backup & Replication.

- If tenants will work with the cloud repository and/or the cloud host over WAN accelerators, the target WAN accelerator must be properly configured on the SP side.

- If you plan to provide network resources for VMware Cloud Director replicas, it is recommended that you change the password for the root account of network extension appliances before you create the first VMware Cloud Director tenant account in the Veeam Cloud Connect infrastructure. You can change the password using the Credentials Manager. To learn more, see Managing Network Extension Appliance Credentials.

Step 1. Launch New Tenant Wizard

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

- Open the **Cloud Connect** view. Click **Add Tenant** > **VMware Cloud Director account** on the ribbon.

- Open the **Cloud Connect** view. Click the **Cloud Connect** node in the inventory pane and click the **VMware Cloud Director Account** link in the working area.

- Open the **Cloud Connect** view. Right-click the **Cloud Connect** node in the inventory pane and select **Add tenant** > **VMware Cloud Director account**.

- Open the **Cloud Connect** view. Click the **Tenants** node in the inventory pane and click **Add Tenant** > **VMware Cloud Director account** on the ribbon.

- Open the **Cloud Connect** view. Right-click the **Tenants** node in the inventory pane or right-click anywhere in the working area and select **Add tenant** > **VMware Cloud Director account**.

Step 2. Specify Organization Settings

At the **Organization** step of the wizard, specify tenant account settings for the tenant.

1. Click **Choose** on the right of the **Organization** field.

2. In the **Select Organization** window, select the VMware Cloud Director organization whose organization VDC resources you want provide to the tenant as cloud hosts.

3. In the **Description** field, specify a description for the created tenant account. The default description contains information about the user who created the account, date and time when the account was created.

4. In the **Assigned resources** section, select what types of Veeam Cloud Connect resources you want to provide to the tenant:

   - **Backup storage** — Veeam Cloud Connect Backup resources. With this option enabled, the **New Tenant** wizard will include an additional **Backup Resources** step. At the **Backup Resources** step of the wizard, you can assign a quota on the cloud repository to the tenant. To learn more, see Allocate Backup Resources.

   - **Replica resources** — Veeam Cloud Connect Replication resources. With this option enabled, the **New Tenant** wizard will include an additional **Replica Resources** step. At the **Replica Resources** step of the wizard, you can select an organization VDC that will act as a cloud host for tenant VM replicas. To learn more, see Allocate Replica Resources.

> **NOTE**
>
> You cannot specify lease settings for VMware Cloud Director tenant accounts. Lease settings for a VMware Cloud Director organization are managed in VMware Cloud Director.

Step 3. Specify Bandwidth Settings

At the **Bandwidth** step of the wizard, specify task and bandwidth limitation settings for the tenant. Limiting bandwidth and parallel data processing capabilities for tenants helps avoid overload of cloud gateways, backup proxies, backup repositories and network equipment on the SP side.

1. In the **Max concurrent tasks** field, specify the maximum number of concurrent tasks for the tenant. If this value is exceeded, Veeam Backup & Replication will not start a new task until one of current tasks finishes. To learn more, see Parallel Data Processing.

   > **NOTE**
   >
   > The specified number of concurrent tasks will be available to the tenant regardless of the number of concurrent tasks defined in the properties of a cloud repository exposed to this tenant.

2. To limit the data traffic coming from the tenant side to the SP side, select the **Limit network traffic from this tenant to** check box. With this option enabled, you can specify the maximum speed for transferring tenant data to the SP side.

   This option also applies to the traffic coming from a cloud repository in the replica from backup and replica seeding scenarios.

3. In the **Gateway pool** field, specify what cloud gateway(s) will be available to the tenant. By default, the tenant can use cloud gateways that are not added to any cloud gateway pool. To use this option, make sure that *Automatic selection* is displayed in the **Gateway pool** field.

   If you want to assign a cloud gateway pool to the tenant, click **Choose** on the right of the **Gateway pool** field and select one or more cloud gateway pools. To learn more, see Assigning Cloud Gateway Pools.

Assigning Cloud Gateway Pools

You can assign to the tenant one or more cloud gateway pools configured in the Veeam Cloud Connect infrastructure. After you assign a cloud gateway pool to the tenant, communication between the tenant backup server and Veeam Cloud Connect infrastructure components in the SP side will be possible only through cloud gateways added to this pool. You can also allow the tenant to fail over to a cloud gateway that is not added to a cloud gateway pool. This may be useful in a situation where all cloud gateways in the cloud gateway pool assigned to the tenant are unavailable for some reason.

To assign a cloud gateway pool to the tenant:

1. At the **Bandwidth** step of the wizard, click **Choose** on the right of the **Gateway pool** field.

2. In the **Gateway Pool** window, select **Use the selected gateway pools**.

3. In the list of available cloud gateway pools, select check boxes next to one or more pools that you want to assign to the tenant. The list of available cloud gateway pools contains pools that you configured in the Veeam Cloud Connect infrastructure.

   To select or clear all check boxes in the list at once, you can use the **Select All** and **Clear All** buttons.

4. [Optional] You can allow the tenant to fail over to a cloud gateway that is not added to the selected cloud gateway pool in case all cloud gateways in the pool are unavailable for some reason. To do this, select the **Failover to other cloud gateways if all gateways from the selected pool are unavailable** check box.

5. Click **OK**.

Step 4. Allocate Backup Resources

The **Backup Resources** step of the wizard is available if you selected the **Backup storage** option at the Organization step of the wizard. You can use this step to specify cloud repository quota settings for the created tenant account.

The procedure of assigning backup resources to a VMware Cloud Director tenant account does not differ from the same procedure for a simple tenant account. You can assign to the tenant a single quota on one cloud repository or several quotas on different cloud repositories.

To assign a cloud repository quota:

1. Click **Add** on the right of the **Cloud repositories** list.

2. In the **Cloud repository name** field of the **Set Quota** window, enter a friendly name for the cloud repository you want to present to the tenant. The name you enter will be displayed in the list of backup repositories at tenant's side.

3. From the **Backup repository** list, select a backup repository in your backup infrastructure whose space resources must be allocated to the tenant.

4. In the **User quota** field, specify the amount of space you want to allocate to the tenant on the selected backup repository.

5. [For tenants who plan to use WAN accelerators] Select the **Enable WAN acceleration through the following WAN accelerator** check box and choose a target WAN accelerator configured at the SP side. The source WAN accelerator is configured on the tenant side. The tenant will select the source WAN accelerator on their side when configuring a backup copy job.

6. Click **OK**.

7. Repeat steps 1–6 for all backup repositories in your backup infrastructure whose resources you want to allocate to the tenant.

8. If you want to protect tenant backups against unwanted deletion, select the **Keep deleted backup files for <N> days** check box and specify the number of days to keep a backup in the recycle bin after a backup is deleted by the tenant. To learn more, see Insider Protection.

> **NOTE**
>
> Consider the following:
>
> - With the **Keep deleted backup files for <N> days** option enabled, Veeam Backup & Replication will disable retention policy for deleted VMs specified in the properties of a tenant backup job. To avoid keeping redundant data in a cloud repository, it is recommended that the SP enables the **Use per-VM backup files** option in the properties of the backup repository whose storage resources the SP exposes to tenants as cloud repositories.
> - If the **Keep deleted backup files for <N> days** option is enabled in the properties of the tenant account, and the **Use per-VM backup files** option is not enabled in the properties of the backup repository whose storage resources the SP exposes to the tenant, the tenant will be unable to remove individual VMs from backups in the cloud repository. When the tenant starts the *Delete from disk* operation for a specific VM in the backup, the operation will complete with an error.
> - The **Keep deleted backup files for <N> days** option is not available if the SP allocates to the tenant a quota on an object storage repository.

Step 5. Allocate Replication Resources

The **Replica Resources** step of the wizard is available if you selected the **Replication resources** option at the Organization step of the wizard. At this step of the wizard, specify what organization VDC will be used to provide resources to tenant VM replicas.

To assign an organization VDC to the tenant:

1. In the **Organization VDC** list, review organization VDCs that will be available to the tenant as cloud hosts. By default, Veeam Backup & Replication displays in this list all organization VDCs allocated to the organization in VMware Cloud Director. If you do not want to provide some of the organization VDCs to the tenant as cloud hosts, select the necessary organization VDC and click **Remove**.

2. [For tenants who plan to use WAN accelerators] Specify WAN acceleration settings for organization VDCs that will be used as a target for tenant VM replicas:

   a. In the **Organization VDC** list, select the organization VDC for which you want to enable WAN acceleration, and click **Edit**.

   b. In the **Edit VDC org** window, select the **Enable WAN acceleration through the following WAN accelerator** check box and choose a target WAN accelerator configured at the SP side. The source WAN accelerator is configured at tenant's side. The tenant will select the source WAN accelerator at their side when configuring a replication job.

   c. Click **OK**.

   d. Repeat steps a–c for all organization VDCs for which you want to enable WAN acceleration.

3. Select the **Use Veeam network extension capabilities during partial and full site failover** check box to allocate network resources for performing failover tasks. With this option enabled, the **New Tenant** wizard will include the additional Network Extension step.

    If you use an NSX Edge gateway or IPsec VPN connection to enable network access to tenant VM replicas after failover, you do not need to deploy the network extension appliance in the Veeam Cloud Connect infrastructure. Instead, you must configure an NSX Edge gateway or IPsec VPN connection in VMware Cloud Director. Make sure that the **Use Veeam network extension capabilities during partial and full site failover** check box is cleared, and then click **Apply** to proceed to the next step of the wizard.

Step 6. Specify Network Extension Settings
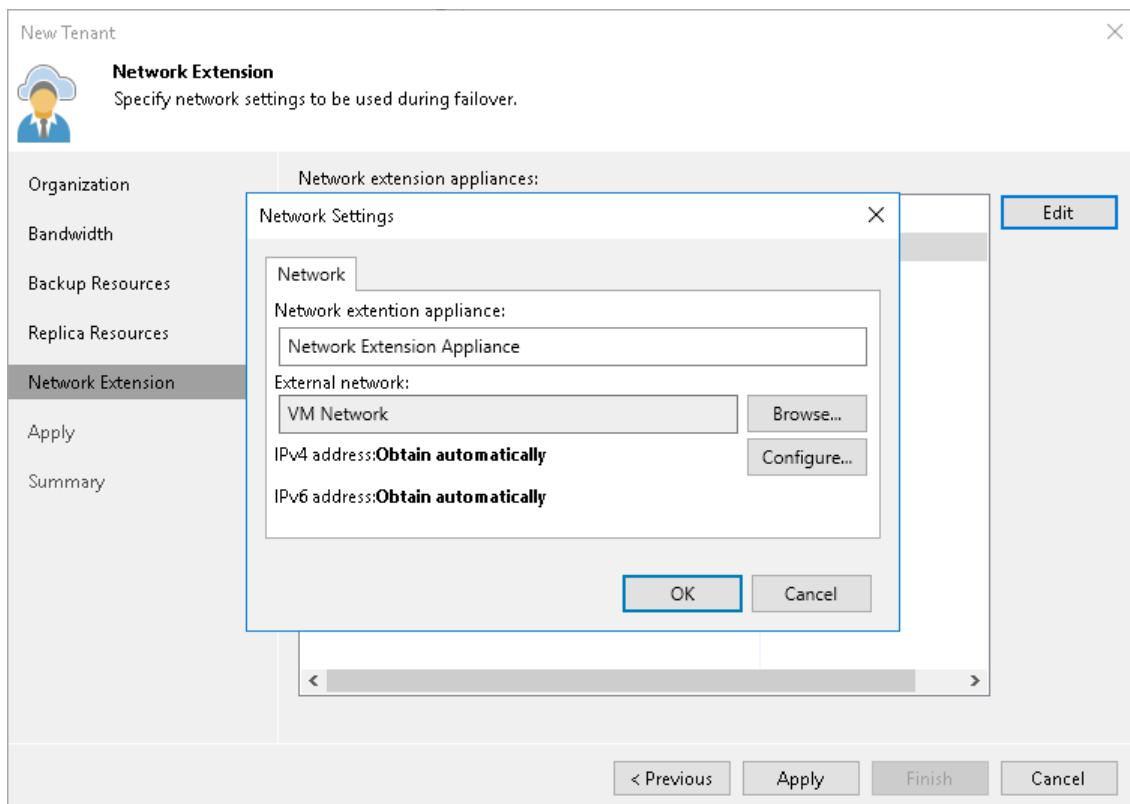
The **Network Extension** step of the wizard is available if you selected the **Use Veeam network extension capabilities during partial and full site failover** option at the Replica Resources step of the wizard. You can use this step to specify network settings for the network extension appliance that Veeam Backup & Replication will deploy on the SP side.

Veeam Backup & Replication deploys the SP network extension appliance in the organization VDC specified as a target for tenant VM replicas. VM replicas on the cloud host will use the SP network extension appliance to communicate to VMs in the production site after partial site failover.

At the **Network Extension** step of the wizard, the SP configures one network adapter (vNIC) on the network extension appliance. This network adapter connects the network extension appliance to the external network where SP backup infrastructure components reside.

To set up the network extension appliance:

1. Click **Edit** on the right of the **Network extension appliances** list.

2. In the **Network extension appliance** field of the **Network Settings** window, check and edit if necessary the name for the network extension appliance.

3. Click the **Browse** button in the **External network** field and select the SP production network to which the SP Veeam Backup & Replication infrastructure components are connected.

4. Specify the IP addressing settings for the configured network extension appliance:

   o To assign an IP address automatically in case there is a DHCP server in your network, make sure that the *Obtain automatically* value is displayed in the **IPv4 address** and **IPv6 address** fields.

   o To manually assign a specific IP address to the appliance, click **Configure** and specify network settings for the appliance. For details, see Specifying Network Settings.

5. Click **OK**.

Specifying Network Settings

To specify network settings for the network extension appliance:

1. In the **Network Settings** window, click **Configure**.

2. To manually assign a specific IPv4 address to the appliance, do the following:

   a. On the **IPv4** tab, make sure that the **Enable IPv4 interface** check box is selected.

   b. Select the **Use the following IP address** option and specify the following network settings:

      - IP address

      - Subnet mask

      - Default gateway

   Alternatively, if you want to assign an IPv4 address automatically, make sure that the **Obtain an IP address automatically** option is selected on the **IPv4** tab.

   If you do not want the network extension appliance to use an IPv4 address, clear the **Enable IPv4 interface** check box.

3. If you want to assign an IPv6 address to the appliance, do the following:

   a. Click the **IPv6** tab.

   b. Make sure that the **Enable IPv6 interface** check box is selected.

   c. Select the **Use the following IP address** option and specify the following network settings:

      - IP address

      - Subnet mask (prefix length)

      - Default gateway

Alternatively, if you want to assign an IPv6 address automatically, make sure that the **Obtain an IP address automatically** option is selected on the **IPv6** tab.

If you do not want the network extension appliance to use an IPv6 address, clear the **Enable IPv6 interface** check box.

4. Click **OK**.

Step 7. Assess Results

The **Apply** step is available if you selected the **Replication resources** option at the **Organization** step of the wizard.

At this step of the wizard, Veeam Backup & Replication will assign the cloud resources to the tenant. Wait for the required operations to complete and click **Next** to continue.

Step 8. Finish Working with Wizard

At the **Summary** step of the wizard, complete the procedure of tenant account registration.

1. Review the information about the added tenant account.

2. Click **Finish** to exit the wizard.

What You Do Next

After the SP creates a tenant account, the SP must communicate the following information to the tenant:

1. User name and password for the created account. For VMware Cloud Director tenant accounts, the user name and password for the tenant account is the user name and password for the organization administrator account of the VMware Cloud Director organization whose resources the SP exposes to the tenant. The user name of the tenant account is specified in the *Organization\Username* format.

2. Full DNS name or IP address of the cloud gateway over which the tenant will communicate with the Veeam Cloud Connect infrastructure.

   o If the SP did not assign a cloud gateway pool to the tenant, the SP can provide information about any cloud gateway configured in the Veeam Cloud Connect infrastructure that is not part of a cloud gateway pool. When the tenant adds the SP in the tenant Veeam backup console, the Veeam backup server on tenant side will obtain a list of all cloud gateways that are not added to a cloud gateway pool. If the primary cloud gateway is unavailable, the Veeam backup server on the tenant side will fail over to another cloud gateway from the list.

   o If the SP assigned a cloud gateway pool to the tenant, the SP can provide information about any cloud gateway added to this gateway pool. When the tenant adds the SP in the tenant Veeam backup console, the Veeam backup server on tenant side will obtain a list of all cloud gateways in the pool. If the primary cloud gateway is unavailable, the Veeam backup server on the tenant side will fail over to another cloud gateway in the same pool.

3. External port for the cloud gateway (if the SP has specified a non-default port).

4. [If Dell Data Domain is used as a cloud repository] Information about the backup chain limitations. The length of forward incremental and forever forward incremental backup chains that contain one full backup and a set of subsequent incremental backups cannot be greater than 60 restore points. To overcome this limitation, tenants can schedule full backups (active or synthetic) to split the backup chain into shorter series. For example, to perform backups at 30-minute intervals, 24 hours a day, tenants must schedule synthetic fulls every day. In this scenario, intervals immediately after midnight may be skipped due to the duration of synthetic processing.

Configuring Target WAN Accelerators

To optimize VM traffic going to the Veeam Cloud Connect infrastructure during the backup copy and replication jobs, the SP and tenants can configure WAN accelerators on their sides.

WAN accelerators in the Veeam Cloud Connect infrastructure must be configured in the following way:
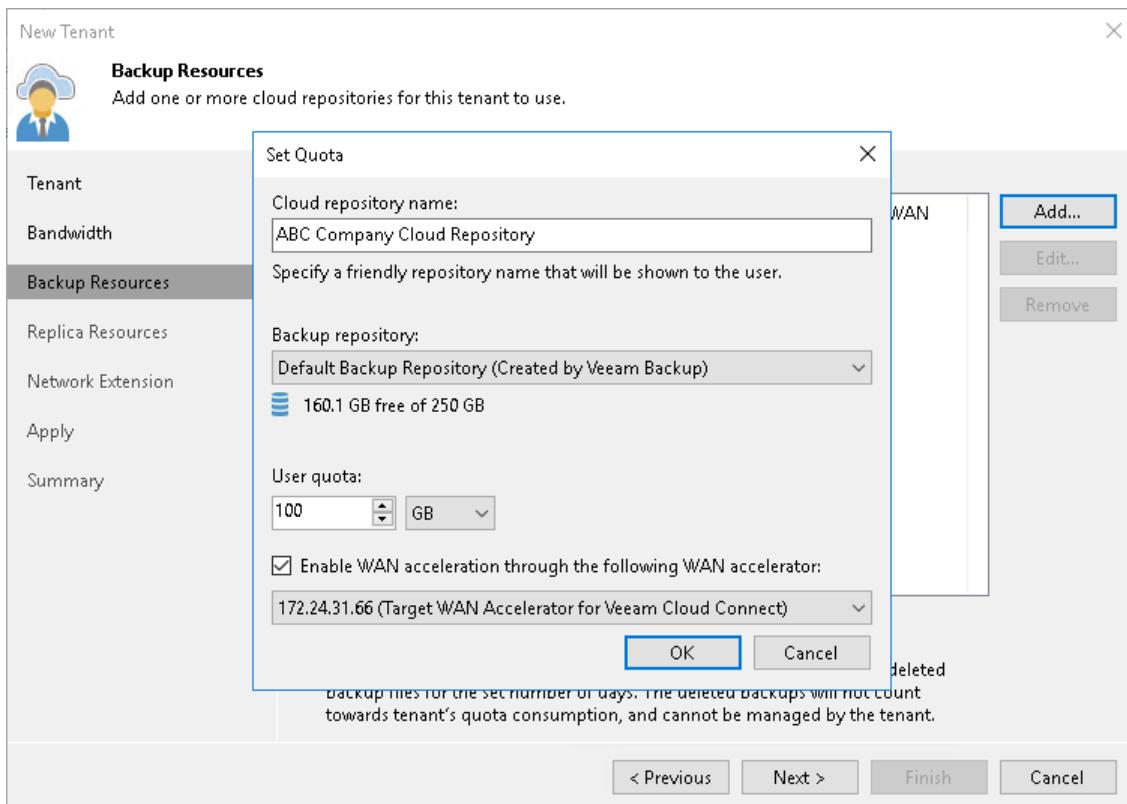
- The source WAN accelerator is configured on the tenant side. Every tenant who plans to work with the cloud repository and cloud hosts using WAN accelerators must configure at least one WAN accelerator on their side.

- The target WAN accelerator is configured on the SP side.
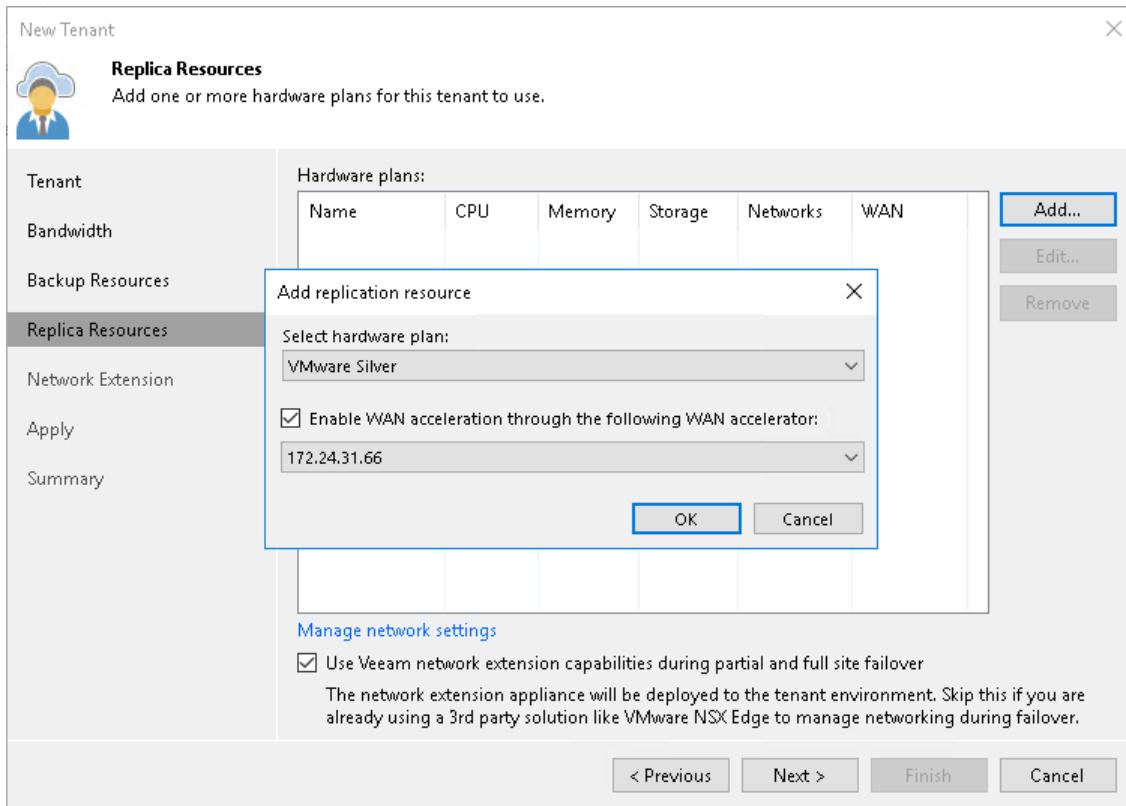
> **NOTE**
>
> Veeam Backup & Replication does not use tenant backups to populate global cache on the SP side.

When the SP creates a tenant account, the SP can define if the tenant should be able to use a WAN accelerator deployed on the SP side:

- For backup copy jobs targeted at the cloud repository

- For replication jobs targeted at the cloud host

As soon as the tenant connects to the SP, Veeam Backup & Replication retrieves the following information to identify if cloud resources available to this tenant can or cannot use WAN acceleration:

- Information about all quotas on cloud repositories assigned to the tenant

- Information about all cloud hosts provided to the tenant through hardware plans

If the cloud repository and/or cloud host can use WAN acceleration, the tenant can configure a source WAN accelerator on the tenant side and create backup copy and/or replication jobs that will work using WAN accelerators.

The configuration process for WAN accelerators in the Veeam Cloud Connect infrastructure is the same as in a regular Veeam backup infrastructure. To learn more, see the Adding WAN Accelerators section in the Veeam Backup & Replication User Guide.

Deploying Veeam Cloud Connect Portal

To deploy Veeam Cloud Connect Portal in the SP backup infrastructure, you must install this component as part of the Veeam Backup Enterprise Manager installation. To do this, select the **Add Cloud Connect Portal for Service Providers** check box at the **Data Locations** step of the Veeam Backup Enterprise Manager setup wizard. For details, see the Specify Data Locations section in the Veeam Backup Enterprise Manager User Guide.

After you install Veeam Backup Enterprise Manager, you must configure Veeam Cloud Connect Portal so that Veeam Cloud Connect Portal becomes accessible over the internet.

To enable access to Veeam Cloud Connect Portal:

1. Configure network settings for Veeam Cloud Connect Portal. As part of this step, you must specify the following settings:

   o Provide Veeam Cloud Connect Portal with public IP address.

   o Specify DNS name for Veeam Cloud Connect Portal.

   o Configure the NAT gateway and other components of the SP network infrastructure to allow traffic exchange between the internet and Veeam Cloud Connect Portal.

2. Add all SP Veeam backup servers on which tenant accounts are registered to Veeam Backup Enterprise Manager. To learn more, see the Adding Backup Server section in the Veeam Backup Enterprise Manager User Guide.

3. Configure security settings for Veeam Cloud Connect Portal as required. As part of this step, you can edit default settings for Veeam Cloud Connect Portal with Internet Information Services (IIS) Manager. For example, you can change the TLS certificate or set up protection against denial of service and brute force attacks. To learn more, see Microsoft Docs.

Managing Tenant Accounts

The SP can perform the following actions with tenant accounts:

- Disable and enable tenant accounts.

- Rename tenant accounts.

- Change passwords for tenant accounts.

- Change resource allocation for tenant accounts.

- Redeploy network extension appliances for tenant accounts.

- View resource consumption by tenant machines.

- Delete tenant accounts.

> **NOTE**
>
> By default, in case the SP backup server is managed by Veeam Service Provider Console version 5.0 or later, you cannot manage tenant accounts in Veeam Backup & Replication. You can change this setting in Veeam Service Provider Console. To learn more, see the Managing Veeam Cloud Connect Servers section in the Guide for Service Providers.

Disabling and Enabling Tenant Accounts

The SP can temporarily disable a tenant account, for example, if the tenant has not made a payment and must not use cloud repository and cloud host resources for some time.

> **NOTE**
>
> For Active Directory tenant accounts, the SP can also perform the disable and enable operations on the Active Directory side. To do this, the SP can disable or enable the Active Directory user account for which the tenant account was created.

When the SP disables a tenant account, the tenant can no longer perform the following operations:

- Run backup and backup copy jobs targeted at the cloud backup repository.

- Run replication jobs targeted at the cloud host.

- Restore data from backups on the cloud repository or copy backup files from the cloud repository.

- Perform failover and failback tasks with VM replicas on the cloud host.

All current sessions for the tenant are terminated; all tenant VMs become inactive and the equal number of VMs in the SP license is revoked for other tenants.

To disable a tenant account:

1. Open the **Cloud Connect** view.

2. In the inventory pane, click the **Tenants** node.

3. In the working area, select the necessary tenant account and click **Disable Tenant** on the ribbon. You can also right-click the account in the working area and select **Disable**.

To enable a disabled account:

1. Open the **Cloud Connect** view.

2. In the inventory pane, click the **Tenant** node.

3. In the working area, select the necessary tenant account and click **Disable Tenant** on the ribbon once again. You can also right-click the account in the working area and select **Disable**.

Renaming Tenant Accounts

The SP can rename a tenant account, for example, if the SP wants to change the user name to a more friendly one.

When the SP renames a tenant account, it is not enough to simply change the user name in the tenant account properties. The SP must also rename the folder with tenant backups on the cloud repository and make sure that the tenant reconnects to the SP under the new name. In this case, Veeam Backup & Replication will be able to save backups to the backup chain that already exists on the cloud backup repository, and the tenant will be able to restore data from previously created backups.

To rename a tenant account (performed by the SP on the SP Veeam backup server):

1. Open the **Cloud Connect** view.

2. In the inventory pane, click **Tenants**.

3. In the working area, right-click the necessary tenant and select **Properties**.

4. At the **Tenant** step of the **Edit Tenant** wizard, specify a new name in the **Username** field.

5. Click **Finish** to save the changes.

6. [For Veeam Cloud Connect Backup] On the cloud repository, rename a subfolder where tenant backups are stored. For example, if the tenant was named *Tenant1*, and you changed the user name to *Tenant2*, you must find the *Tenant1* subfolder on the cloud repository and rename it to *Tenant2*.

> **NOTE**
>
> For object storage repositories, renaming of the subfolder with tenant backups is not supported. In case the SP provides the tenant with an object storage repository as a cloud repository, after the SP renames the tenant account, tenant backup jobs will create a full backup in the cloud repository.
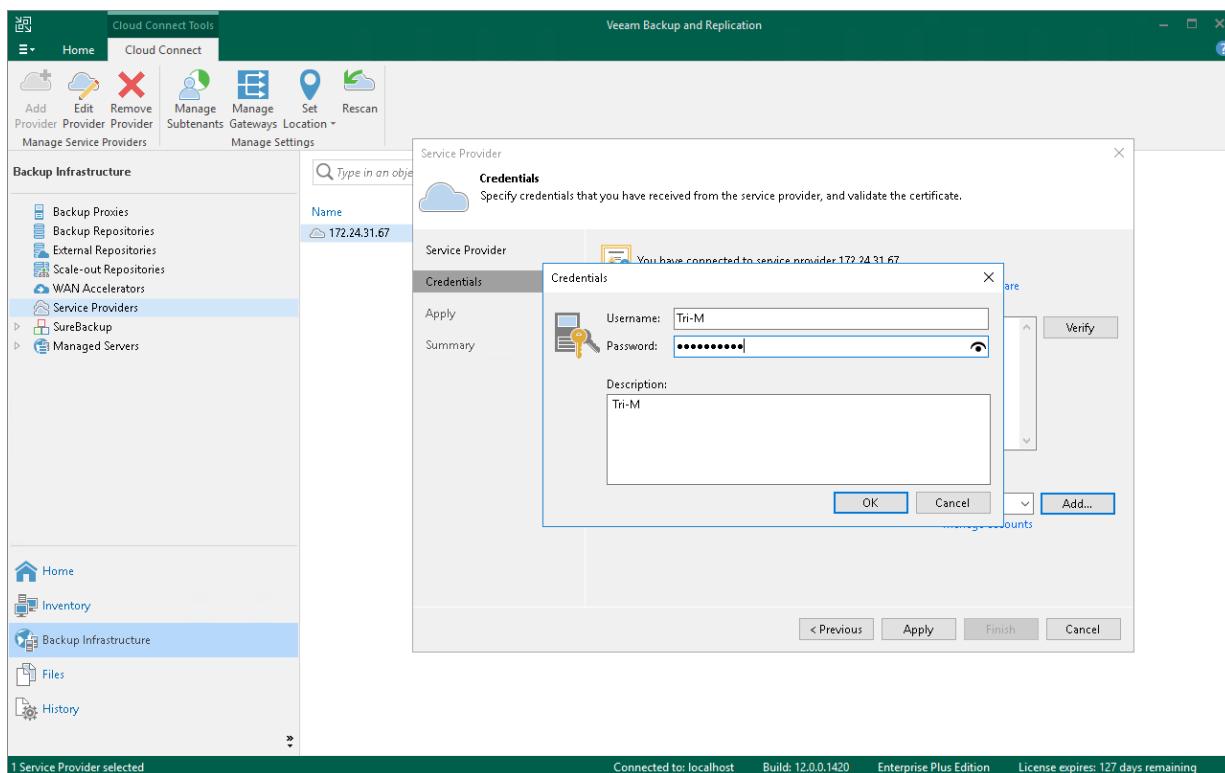
7. Inform the tenant about the user name change and make sure that the tenant reconnects to the SP under this name.

To reconnect to the SP (performed by the tenant on the tenant Veeam backup server):

1. Open the **Backup Infrastructure** view.

2. In the inventory pane, click the **Service Providers** node.

3. In the working area, right-click the SP and select **Properties**.

4. At the **Credentials** step of the wizard, click **Add** next to the **Credentials** field and specify a new user name and password to connect to the SP. You must specify the password that you used before, unless the SP has changed the password together with the user name.

5. Follow the next steps of the wizard without changing default settings. At the **Summary** step of the wizard, click **Finish**.

> **IMPORTANT**
>
> The tenant must reconnect to the SP only after the SP renames the subfolder with tenant backups on the cloud repository. In the opposite case, tenant backup job sessions will be failing.

Changing Password for Tenant Account on SP Side

The SP can change the password for the tenant account.
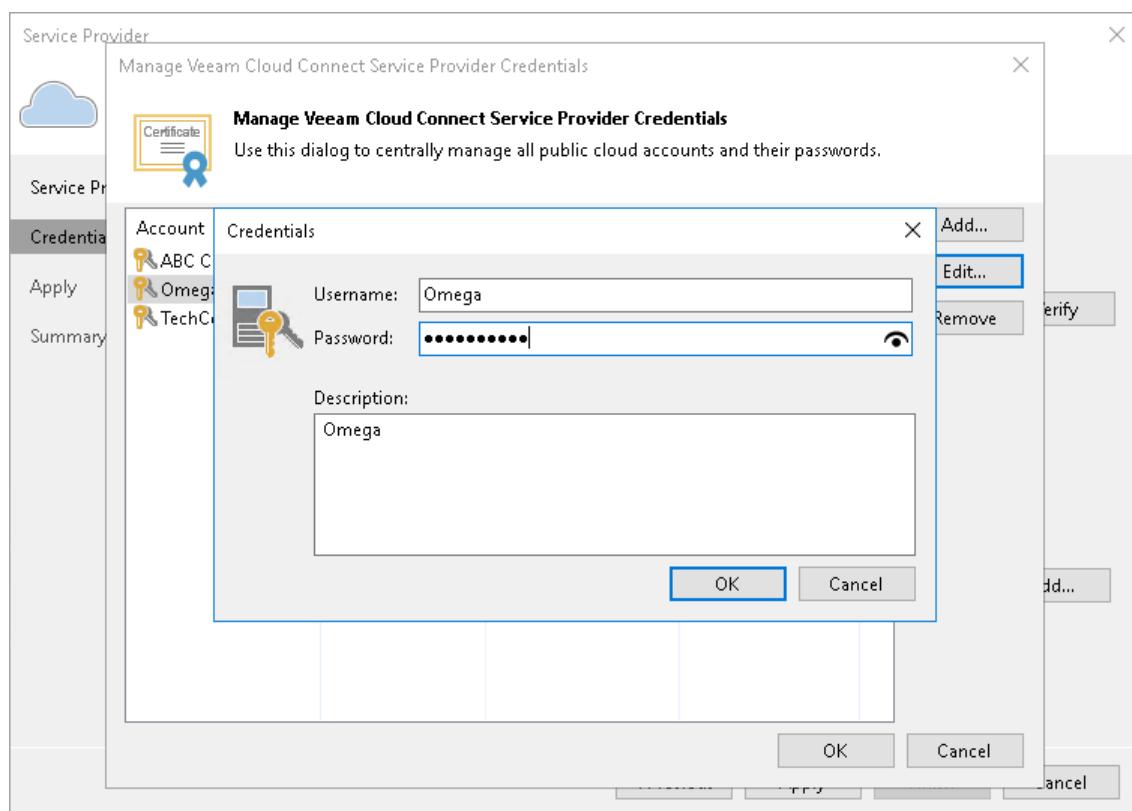
> **NOTE**
>
> Consider the following:
>
> - The tenant can also change the password for the tenant account using the Veeam backup console on the tenant backup server. To learn more, see Changing Password for Tenant Account.
> - You cannot use the Veeam backup console to change the password for a VMware Cloud Director tenant account. For such accounts, passwords are managed in VMware Cloud Director.

To change a password for the tenant account (performed by the SP on the SP Veeam backup server):

1. Open the **Cloud Connect** view.

2. In the inventory pane, click **Tenants**.

3. In the working area, right-click the necessary tenant and select **Properties**.

4. At the **Tenant** step of the **Edit Tenant** wizard, specify a new password in the **Password** field or click the **Generate new** link at the bottom of the field. In the latter case, Veeam Backup & Replication will generate a safe password. You will be able to get a copy the generated password at the last step of the wizard.

5. At the **Summary** step of the **Edit Tenant** wizard, click the **Copy password to clipboard** link at the bottom of the wizard window and click **Finish** to save the changes.

6. Inform the tenant about the password change and make sure that the tenant reconnects to the SP using the new password.

To reconnect to the SP (performed by the tenant on tenant Veeam backup server):

1. Open the **Backup Infrastructure** view.

2. In the inventory pane, click the **Service Providers** node.

3. In the working area, right-click the SP and select **Properties**.

4. At the **Credentials** step of the **Service Provider** wizard, click the **Manage accounts** link at the bottom of the **Credentials** field.

5. In the **Manage Veeam Cloud Connect Service Provider Credentials** window, click **Edit**.

6. In the displayed window notifying that the edited credentials are used to connect to the SP, click **Yes**.

7. In the **Credentials** window, enter a new password in the **Password** field and click **OK**.

8. Follow the next steps of the **Service Provider** wizard without changing default settings. At the **Summary** step of the wizard, click **Finish**.

Changing Resource Allocation for Tenant Account

The SP can change a set of resources provided to a tenant account. For example:

- Enable or disable access to backup and replication resources

- Add or remove storage quotas on the cloud repository

- Subscribe or unsubscribe tenants to/from hardware plans

To edit resources provided to a tenant account (performed by the SP on the SP Veeam backup server):

1. Open the **Cloud Connect** view.

2. In the inventory pane, click **Tenants**.

3. In the working area, right-click the necessary tenant and select **Properties**.

4. At the **Tenant** step of the **Edit Tenant** wizard, in the **Assigned resources** section, select what types of Veeam Cloud Connect resources you want to provide to the tenant:

   o **Backup storage** — with this option enabled, you can assign a quota on the cloud repository to the tenant. To learn more, see Allocate Backup Resources.

   o **Replication resources** — with this option enabled, you can subscribe the tenant to a hardware plan. To learn more, see Allocate Replica Resources.

5. At the **Backup Resources** and **Replica Resources** steps of the wizard, edit backup and replication resources settings as required.

6. At the **Summary** step of the wizard, click **Finish** to save the changes.
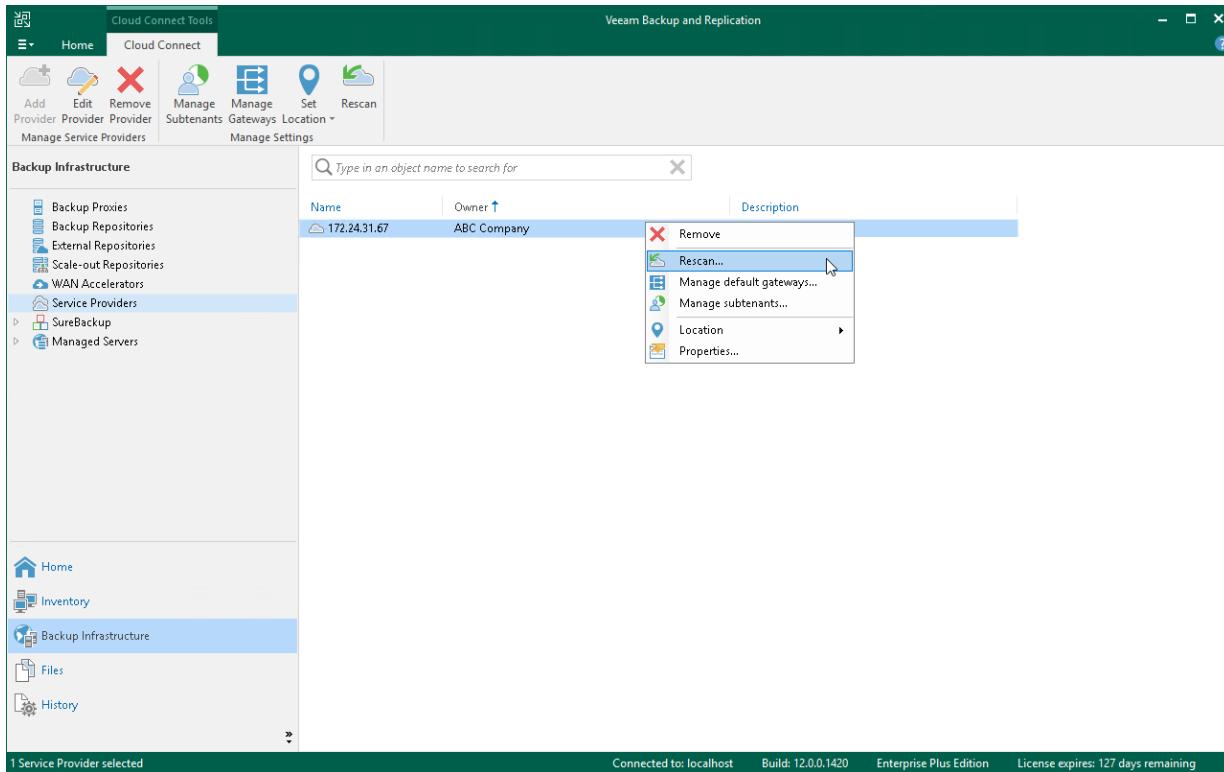
To start working with a new set of resources, the tenant must perform one of the following operations:

- *Rescan the SP*. This operation is sufficient in case the SP added resources to the tenant account, for example, assigned a quota on the cloud repository to the tenant account or assigned replication resources to the tenant account.

- *Reconnect to the SP*. This operation is required in case the SP removed resources from the tenant account.

   This operation is also required in case the SP assigned replication resources to the tenant, and the tenant wants to configure and deploy the network extension appliance. Alternatively, the tenant can rescan the SP. In this case, Veeam Backup & Replication will prompt to deploy the network extension appliance later, when the tenant performs failover to a VM replica on the cloud host.

After the tenant rescans the SP or reconnects to the SP, Veeam Backup & Replication will retrieve information about available backup storage and hardware plans and display cloud repositories and cloud hosts in the tenant Veeam Backup & Replication console.

To rescan the SP (performed by the tenant on the tenant Veeam backup server):

1. Open the **Backup Infrastructure** view.

2. In the inventory pane, click the **Service Providers** node.

3. In the working area, select the SP and click **Rescan** on the ribbon or right-click the SP and select **Rescan**.
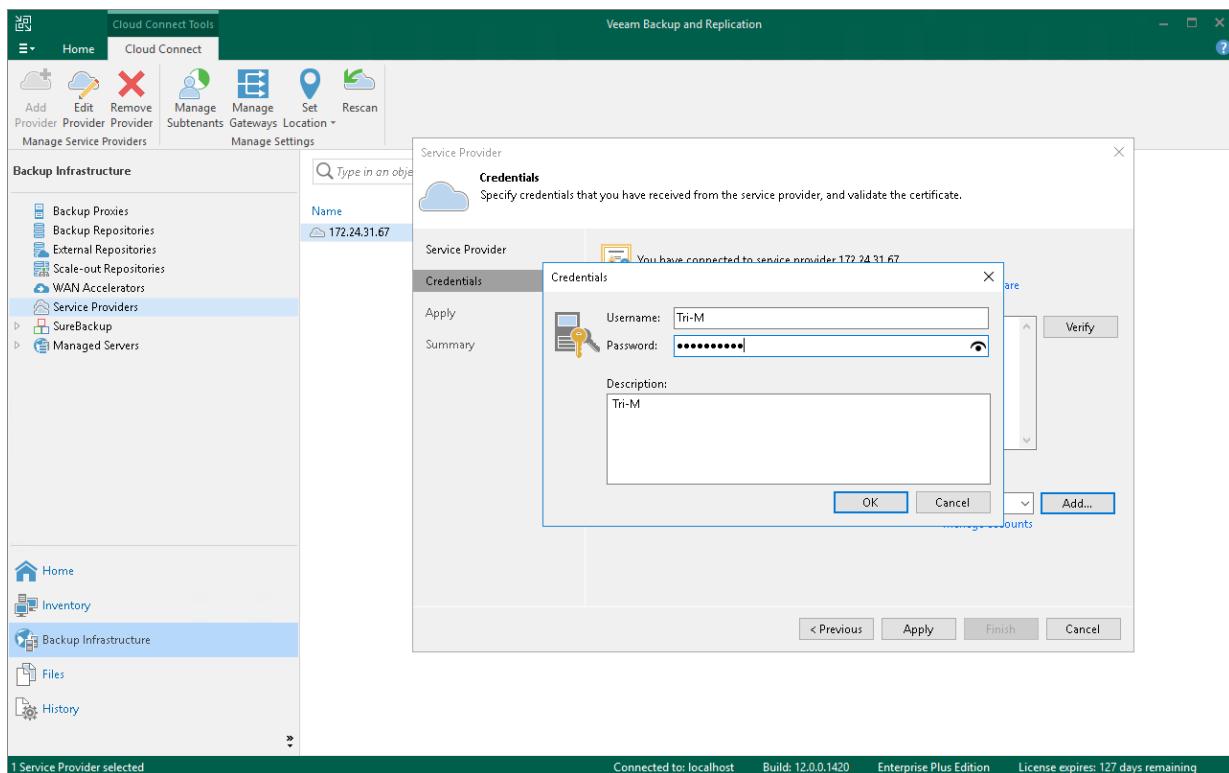
To reconnect to the SP (performed by the tenant on the tenant Veeam backup server):

1. Open the **Backup Infrastructure** view.

2. In the inventory pane, click the **Service Providers** node.

3. In the working area, select the SP and click **Edit Provider** on the ribbon or right-click the SP and select **Properties**.

4. Follow the steps of the **Service Provider** wizard. At the **Summary** step of the wizard, click **Finish**. To learn more, see Connecting to Service Providers.

> **NOTE**
>
> If the SP assigned replication resources to the tenant, the tenant may need to configure and deploy the network extension appliance at the **Network Extension** step of the **Service Provider** wizards. To learn more, see Configure Network Extension Appliances.
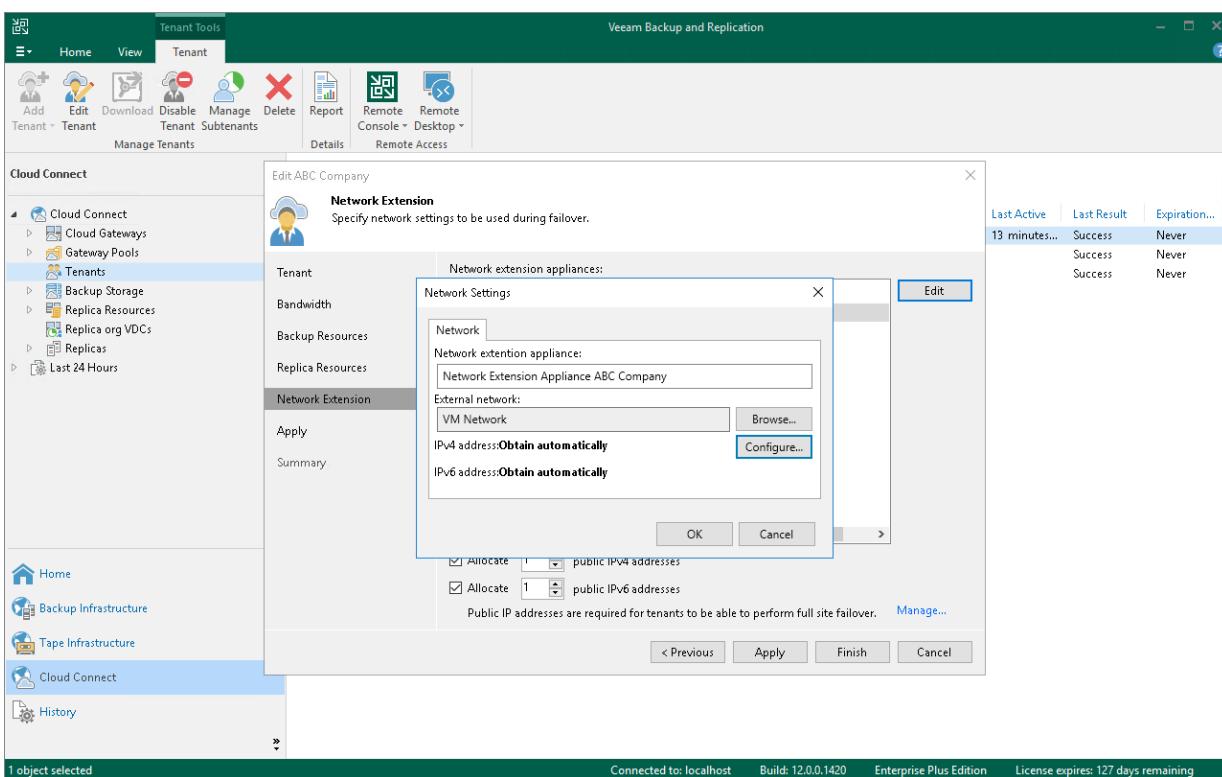
Redeploying Network Extension Appliance

The SP can redeploy a network extension appliance for a tenant account. This may be necessary when the network extension appliance becomes inoperative or when the SP changes the password in the network extension appliance credentials record after one or several appliances are already deployed.

To redeploy the network extension appliance:

1. Open the **Cloud Connect** view.

2. In the inventory pane, click **Tenants**.

3. In the working area, right-click the necessary tenant and select **Properties**.

4. At the **Network Extension** step of the **Edit Tenant** wizard, in the **Network extension appliances** section, click **Edit** and edit settings for the network extension appliance (for example, change the name of the network extension appliance).

5. Click **Next** to apply new settings. Veeam Backup & Replication will remove a previously deployed network extension appliance and deploy a new network extension appliance VM with new settings. The extension appliance will have root password that is specified in the Credentials Manager.

6. At the **Summary** step of the wizard, click **Finish** to exit the wizard.

Viewing Tenant Account Information

The SP can view information about registered tenant accounts in the Veeam backup console.

To view information about tenant accounts:

1. Open the **Cloud Connect** view.

2. In the inventory pane, click the **Tenants** node.

3. In the working area, view information about tenant accounts. For each tenant account, Veeam Backup & Replication displays information in the following columns:

   - **Name** — name of the tenant account.

   - **Type** — type of the tenant account: *Standalone*, *Active Directory* or *VMware Cloud Director*.

   - **Backup Count** — number of VMs that have backups created by tenant backup jobs.

     > **NOTE**
     >
     > If you use the **Tenants** node to track SP resource consumption by tenant workloads, make sure to read Considerations for Resource Consumption by Tenant Machines.

   - **Replica Count** — number of VMs that have replicas created by tenant replication jobs.

   - **Server Count** — number of servers that have backups created by tenant Veeam Agent backup jobs. A server is a machine processed with the *Server* edition of Veeam Agent.

   - **Workstation Count** — number of workstations that have backups created by tenant Veeam Agent backup jobs. A workstation is a machine processed with the *Workstation* edition of Veeam Agent.

   - **Remote Management** — information about whether the SP can establish a remote connection to the tenant backup server. The tenant backup server is available for remote management if the tenant selected the **Allow this Veeam Backup & Replication installation to be managed by the service provider** check box when adding the SP in the tenant backup console.

   - **Description** — description for the tenant account.

o **Last Active** — time since the latest backup job session, replication job session or restore session was completed.

o **Last Result** — information about the result of the latest session: *Success*, *Warning* or *Failed*.

o **Expiration Date** — date and time when the lease period expires for the tenant. If you did not enable the **Contract expires** option in the properties of the tenant account, the *Never* value is displayed in this column.

Considerations for Resource Consumption by Tenant Machines

You can use the **Tenants** node of the SP backup console to view information about the number of tenant machines whose backups and replicas consume resources in the SP infrastructure. For this scenario, consider the following:

- The **Tenants** node displays information about all tenant machines that currently consume resources in the SP Veeam Cloud Connect infrastructure, including rental machines and new workloads. To learn more, see Rental Machines Licensing and New Workloads.

- The number of machines that consume resources in the SP Veeam Cloud Connect infrastructure may differ from the number of protected workloads that consume the Veeam Cloud Connect license on the SP backup server. The SP must not use information displayed in the **Tenants** node to report license usage to Veeam. To learn about how to view information about protected tenant workloads, see Tenant Machine Count.

- If the tenant processes the same VM with multiple jobs targeted at different quotas (cloud repositories or cloud hosts), this VM is counted as multiple VMs in the SP backup console. This lets the SP monitor consumption of backup and replication resources in the Veeam Cloud Connect infrastructure — the machine count reflects the number of machines that actually consume tenant quotas. In contrast, in the SP Veeam Cloud Connect license and license usage reports, such a VM is considered as 1 VM and uses the number of instances required to process 1 VM.

  For example, the tenant processes 1 VM with 2 backup jobs and 3 replication jobs. In the **Tenants** node of the **Cloud Connect** view in the SP backup console, Veeam Backup & Replication will display 2 VMs in the **Backup Count** column and 3 VMs in the **Replica Count** column. In the **License Information** window, Veeam Backup & Replication will display the number of used instances required to process 1 Veeam Cloud Connect Backup VM and 1 Veeam Cloud Connect Replica VM.

Deleting Tenant Accounts

The SP can delete a tenant account at any time, for example, if the tenant no longer uses resources of the cloud repository.

When the SP deletes a tenant account, Veeam Backup & Replication disables this account and removes it. The tenant account is removed permanently. The SP cannot undo this operation.

When the SP deletes a tenant account, Veeam Backup & Replication displays a warning prompting whether to delete tenant backup data. The SP can choose to delete tenant backups automatically along with the tenant account. Alternatively, the SP can let tenant backup data remain intact in the cloud repository and delete it later manually.

In contradiction to backup data, Veeam Backup & Replication processes VM replicas on the cloud host according to the following rules:

- If a VM replica is powered off at the time when the SP deletes the tenant account, Veeam Backup & Replication unregisters the VM replica on the cloud host and deletes actual replica files from the datastore or volume.

- If a VM replica was powered on as part of a failover operation before the SP deletes the tenant account, Veeam Backup & Replication keeps the VM replica intact on the cloud host.

- If a VM replica was powered on manually before the SP deletes the tenant account, Veeam Backup & Replication powers off the VM replica, unregisters the VM replica on the cloud host and deletes actual replica files from the datastore or volume.
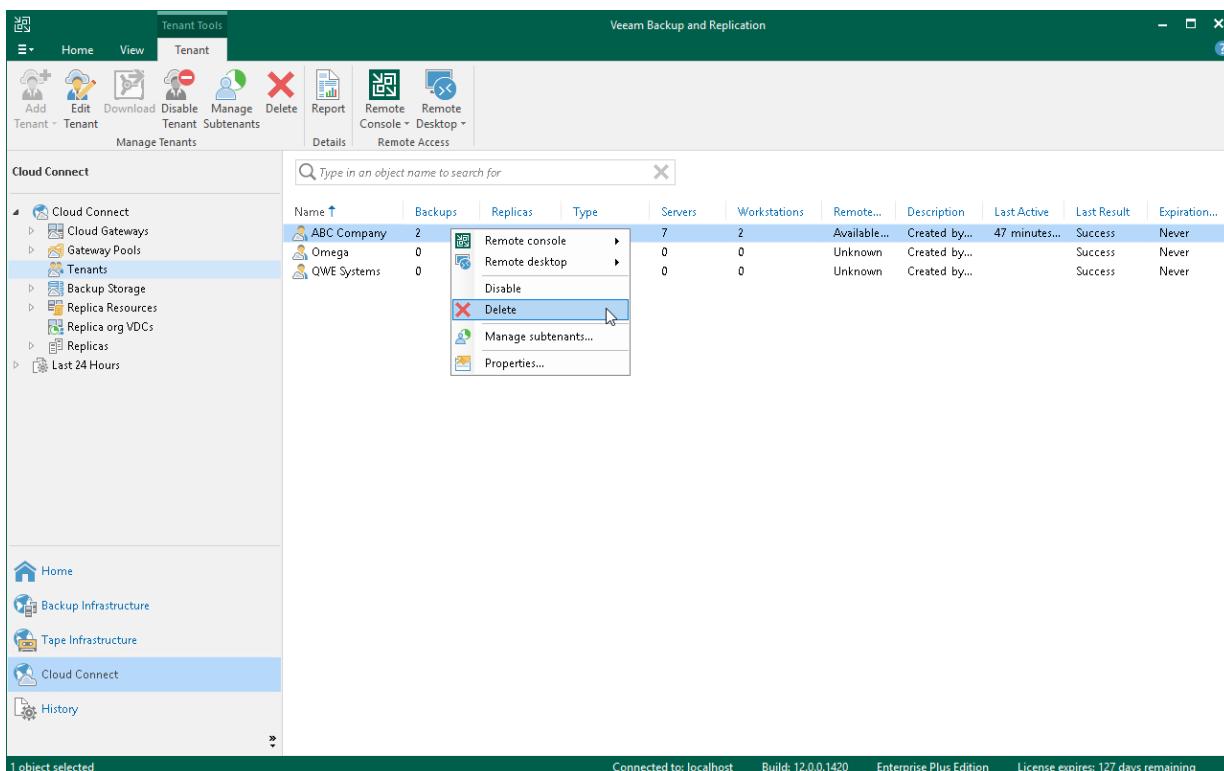
If the cloud repository and cloud host work using WAN accelerators, when the SP deletes a tenant account, Veeam Backup & Replication also deletes data for this tenant from the global cache on the target WAN accelerator.

To delete a tenant account:

1. Open the **Cloud Connect** view.

2. In the inventory pane, click the **Tenants** node.

3. In the working area, select the necessary tenant account and click **Delete** on the ribbon. You can also right-click the account in the working area and select **Delete**.

4. If you want to delete tenant backup data along with the tenant account, in the displayed window, select the **Remove backups** check box.

5. Click **Yes**.

TIP

After you delete a tenant account, the tenant VM count is automatically reset and tenant VMs are revoked from the license. To learn more, see Resetting Tenant VM Count.

Managing Subtenant Accounts on SP Side

To provide subtenants with individual storage quotas on the cloud repository, the SP or tenant must register a subtenant account for each subtenant. The SP can perform the following operations with subtenant accounts:

- Add a subtenant account for a standalone tenant account.

- Add a subtenant account for a VMware Cloud Director tenant account.

- Edit a subtenant account.

- Remove a subtenant account.

> **NOTE**
>
> Veeam Backup & Replication does not offer subtenant functionality for Active Directory tenant accounts. You can use an Active Directory tenant account itself instead of a subtenant account to back up your data with Veeam Agent.

Creating Subtenant Account for Standalone Tenant
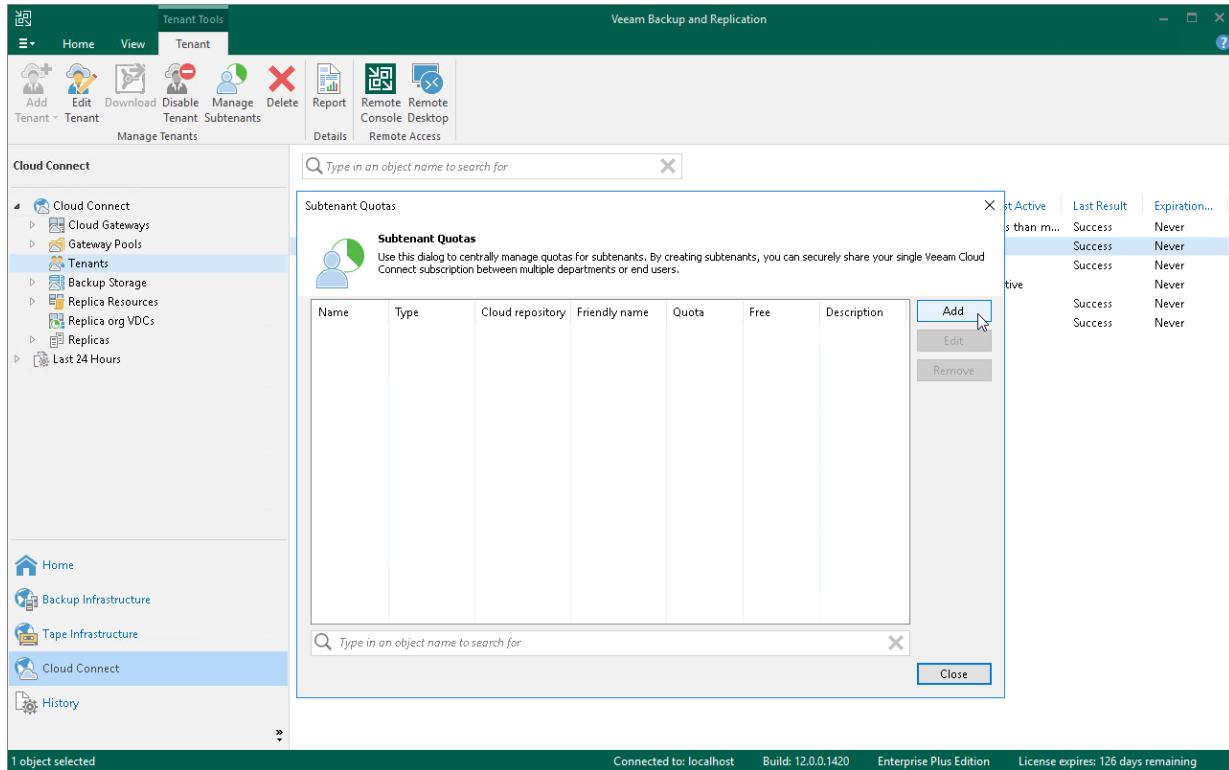
The procedure of subtenant accounts registration can be performed by the SP on the SP Veeam backup server.

When you create a subtenant account for a standalone tenant account, remember to save a user name and password for the created subtenant account. You must pass this data to the subtenant. When configuring a backup job targeted at the cloud repository, the subtenant must enter the user name and password for the subtenant account to connect to the SP backup server.

Step 1. Launch New Subtenant Wizard

To launch the **New subtenant** wizard:

1. Open the **Cloud Connect** view.

2. In the inventory pane, click the **Tenants** node.

3. In the working area, select the necessary tenant and click **Manage Subtenants** on the ribbon or right-click the tenant and select **Manage subtenants**.

4. In the **Subtenant Quotas** window, click **Add**.

Step 2. Specify Subtenant Settings

At the **Account** step of the wizard, specify settings for the created subtenant account:

1. In the **Username** field, specify a name for the created subtenant account. The user name must meet the following requirements:

   - The maximum length of the user name is 128 characters. It is recommended that you create short user names to avoid problems with long paths to backup files on the cloud repository.

   - The user name may contain space characters.

   - The user name must not contain the following characters: , \ / : * ? \ " < > | = ; @ as well as Unicode characters.

   - The user name must not end with the period character [.].

2. In the **Password** field, provide the password for the subtenant account. You can enter your own password or click the **Generate** new link at the bottom of the field. In the latter case, Veeam Backup & Replication will generate a safe password. To get a copy the generated password, click the **Copy to clipboard** link at the bottom of the window.

3. In the **Description** field, specify a description for the created subtenant account.

4. If you want the subtenant account to be created in the disabled state, select the **Subtenant is disabled** check box. In this case, Veeam Backup & Replication will create the subtenant account, but the subtenant will not be able to connect to the SP and create backups on the cloud repository.

Step 3. Allocate Subtenant Quota

At the **Quotas** step of the wizard, specify subtenant quota settings for the created account. You can assign to the subtenant tenant a single quota on a cloud repository assigned to the tenant account.

To assign a subtenant quota:

1. Click **Add** on the right of the **Available user quotas** list.

2. In the **Subtenant Quota** window, in the **Name** field, enter a friendly name for the subtenant quota. The name you enter will be displayed at the subtenant's side.

3. In the **Repository** field, select a cloud repository whose space resources must be allocated to the subtenant.

4. By default, Veeam Backup & Replication allows subtenants to use an entire quota on the cloud repository assigned to the tenant. If you want to limit the amount of storage space that the subtenant can use on the cloud repository, in the **Quota** section, select **Limit size to** and specify the necessary subtenant quota.

   When you consider limiting the subtenant quota, remember to allocate the sufficient amount of storage space for the subtenant. The subtenant quota must comprise the amount of disk space used to store a chain of backup files plus additional space required for performing the backup chain transform operation. Generally, to perform the transform operation, Veeam Backup & Replication requires the amount of disk space equal to the size of a full backup file.

5. Click **OK**.

Step 4. Finish Working with Wizard

At the **Summary** step of the wizard, complete the procedure of subtenant account registration.

1. Click the **Copy to clipboard** link to copy information about the created subtenant account: user name, password, cloud repository and quota. You must send the copied information to a user on the tenant side so that they can use the created subtenant account to configure a backup job targeted at the cloud repository.

2. Click **Finish** to exit the wizard.

Creating Subtenant Account for VMware Cloud Director Tenant

The procedure of subtenant accounts registration can be performed by the SP on the SP Veeam backup server.

After you create a subtenant account for a VMware Cloud Director tenant account, pass the user name of the created account to the subtenant. When configuring a backup job targeted at the cloud repository, the subtenant must enter the user name for the subtenant account to connect to the SP backup server.
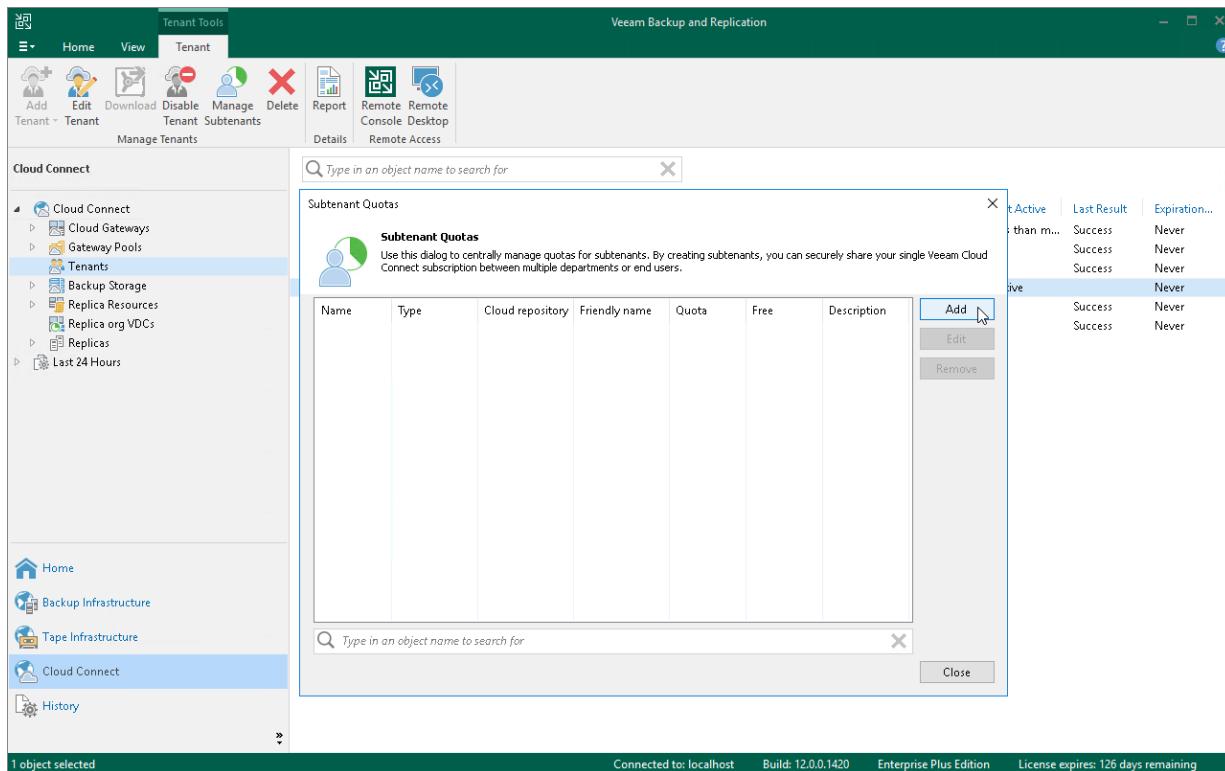
Before You Begin

Before you add a new subtenant account for a VMware Cloud Director tenant account, check the following prerequisite: the Cloud Director user account that you plan use as a subtenant account must be created for the organization in VMware Cloud Director.

Step 1. Launch New Subtenant Wizard

To launch the **New subtenant** wizard:

1. Open the **Cloud Connect** view.

2. In the inventory pane, click the **Tenants** node.

3. In the working area, select the necessary tenant and click **Manage Subtenants** on the ribbon or right-click the tenant and select **Manage subtenants**.

4. In the **Subtenant Quotas** window, click **Add**.

Step 2. Select Cloud Director User

At the **Cloud Director User** step of the wizard, specify settings for the created subtenant account:

1. Click **Add** next to the **Username** field and select a user account of a VMware Cloud Director organization to which you want to allocate a quota on the cloud repository. The user account must be created in advance by the SP in VMware Cloud Director.

2. In the **Description** field, specify a description for the created subtenant account.

3. If you want the subtenant account to be created in the disabled state, select the **Subtenant is disabled** check box. In this case, Veeam Backup & Replication will create the subtenant account, but the subtenant will not be able to connect to the SP and create backups on the cloud repository.

Step 3. Allocate Subtenant Quota

At the **Quotas** step of the wizard, specify subtenant quota settings for the created account. You can assign to the subtenant tenant a single quota on a cloud repository assigned to the tenant account.

To assign a subtenant quota:

1. Click **Add** on the right of the **Available user quotas** list.

2. In the **Subtenant Quota** window, in the **Name** field, enter a friendly name for the subtenant quota. The name you enter will be displayed at the subtenant's side.

3. In the **Repository** field, select a cloud repository whose space resources must be allocated to the subtenant.

4. By default, Veeam Backup & Replication allows subtenants to use an entire quota on the cloud repository assigned to the tenant. If you want to limit the amount of storage space that the subtenant can use on the cloud repository, in the **Quota** section, select **Limit size to** and specify the necessary subtenant quota.

   When you consider limiting the subtenant quota, remember to allocate the sufficient amount of storage space for the subtenant. The subtenant quota must comprise the amount of disk space used to store a chain of backup files plus additional space required for performing the backup chain transform operation. Generally, to perform the transform operation, Veeam Backup & Replication requires the amount of disk space equal to the size of a full backup file.

5. Click **OK**.

Step 4. Finish Working with Wizard

At the **Summary** step of the wizard, complete the procedure of subtenant account registration.

1. Review the information about the added subtenant account.

2. Click **Finish** to exit the wizard.

Editing Subtenant Account

You can edit settings of created subtenant accounts. For example, you may want to reallocate storage quota for the subtenant, change password for the subtenant account of a standalone tenant account, disable or enable the subtenant account.

> **NOTE**
>
> Consider the following:
>
> - You cannot change a user name for the subtenant account.
> - The SP cannot change the password for a managed subtenant account. This operation is available only for the tenant in the tenant backup console.

To edit settings of a subtenant account:

1. Open the **Subtenant Quotas** window in one of the following ways:

   o Open the **Cloud Connect** view. Click the **Tenants** node in the inventory pane, select the necessary tenant in the working area and click **Manage Subtenants** on the ribbon.

   o Open the **Cloud Connect** view. Click the **Tenants** node in the inventory pane, right-click the necessary tenant in the working area and select **Manage subtenants**.

2. In the **Subtenant Quotas** window, select the necessary subtenant account and click **Edit**.

   To quickly find the necessary subtenant account, use the search field at the bottom of the **Subtenant Quotas** window:

   a. Enter the user name of the subtenant account or a part of it in the search field.

   b. Click the **Start search** button on the left or press **[ENTER]**.

3. In the edit subtenant wizard, edit subtenant account settings as required.

Deleting Subtenant Account

You can delete a subtenant account that you created for a standalone or VMware Cloud Director tenant account at any time, for example, if the subtenant no longer uses resources of the cloud repository.

When you delete a subtenant account, Veeam Backup & Replication disables this account and removes it. The subtenant account is removed permanently. You cannot undo this operation.

Subtenant's backup data remain intact on the cloud repository. You can delete subtenant backup data manually later if needed.

> **NOTE**
>
> You cannot delete managed subtenant accounts — subtenant accounts created automatically by Veeam Backup & Replication in the Veeam Agent management scenario.

To delete a subtenant account:

1. Open the **Subtenant Quotas** window in one of the following ways:

   o Open the **Cloud Connect** view. Click the **Tenants** node in the inventory pane, select the necessary tenant in the working area and click **Manage Subtenants** on the ribbon.

   o Open the **Cloud Connect** view. Click the **Tenants** node in the inventory pane, right-click the necessary tenant in the working area and select **Manage subtenants**.

2. In the **Subtenant Quotas** window, select the necessary subtenant account and click **Remove**.

   To quickly find the necessary subtenant account, use the search field at the bottom of the **Subtenant Quotas** window:

   a. Enter the user name of the subtenant account or a part of it in the search field.

   b. Click the **Start search** button on the left or press **[ENTER]**.

Performing Instant Recovery from Tenant Backups

The SP can perform Instant Recovery for tenant workloads, that is, recover workloads from tenant backups in the cloud repository and register them as VMware vSphere VMs.

Before you perform Instant Recovery, check prerequisites and limitations. For details, see Instant Recovery from Tenant Backups.

To perform Instant Recovery:

1. In the SP backup console, launch the Instant Recovery to VMware vSphere wizard.

   a. Open the **Home** view.

   b. In the inventory pane, click the **Backups** node.

   c. In the working area, click the backup whose data you want to restore to a VMware vSphere VM and click **Instant Recovery** on the ribbon or right-click the necessary backup and select **Instant recovery**.

   To select multiple backups, press and hold the **[CTRL]** key, and then click or right-click the necessary backups.

2. In the displayed window, click **Yes** to confirm that the tenant will be disabled during Instant Recovery.

3. Follow the steps of the **Instant Recovery to VMware vSphere** wizard.

The Instant Recovery procedure for tenant backups is similar to the same procedure in the regular Veeam Backup & Replication infrastructure. The difference is that you cannot recover tenant backups to their original location — Instant Recovery in the Veeam Cloud Connect infrastructure is performed to a VMware vSphere VM on the SP virtualization host. Thus, in this scenario the **Instant Recovery to VMware vSphere** wizard does not include the **Restore Mode** step.

To get a detailed description of all Instant Recovery options, see the Performing Instant Recovery to VMware vSphere section in the Veeam Backup & Replication User Guide.

Managing Tenant Data

The SP can perform the following actions with tenant data:

- Move tenant backups to another cloud repository
- Download tenant data from the capacity tier
- Retrieve tenant data from the archive tier
- Manage tenant VM replicas

Moving Tenant Backups to Another Cloud Repository

The SP may need to move tenant data to another cloud repository, for example, if the initial cloud repository is running out of space.

There are two scenarios of moving tenant data:

- Scenario 1: replacing the cloud repository. The SP may want to replace the initial cloud repository with a new cloud repository, for example, with a cloud repository that has more storage capacity. This scenario does not require any actions on the tenant side.

- Scenario 2: adding a new cloud repository. The SP may want to configure a new cloud repository in addition to the initial cloud repository and move tenant data to it. This scenario requires additional actions on the tenant side.
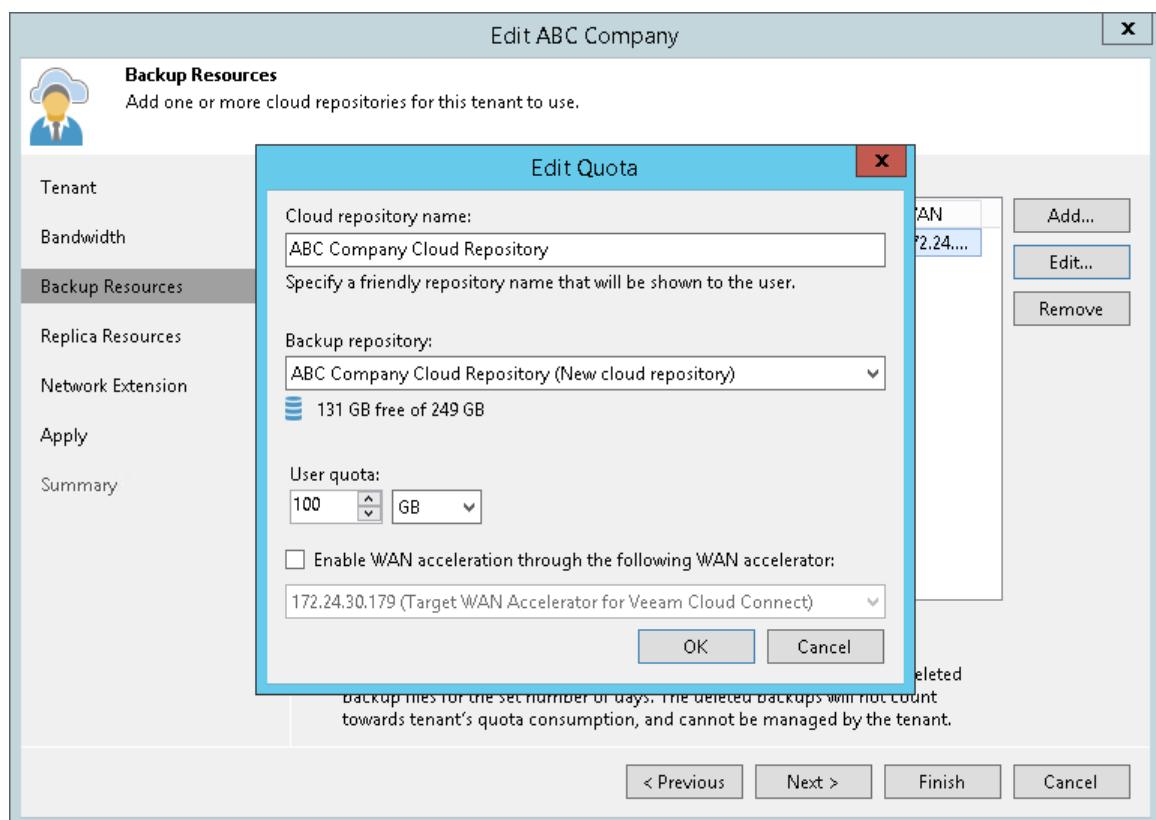
> **NOTE**
>
> Consider the following:
>
> - This section describes the procedure of moving tenant data between regular backup repositories used as cloud repositories. You cannot use this procedure to move tenant backups to a cloud repository that has a scale-out backup repository as a back end. If you need to move tenant data to such repository, contact Veeam Customer Support.
> - If you want to move tenant data from a scale-out backup repository used as a cloud repository to another cloud repository, follow instructions for the Scenario 2. You cannot use the Scenario 1 to move data from this type of backup repository.

Scenario 1. Replacing Cloud Repository

The SP must complete the following tasks:

1. Configure a new backup repository that you plan to use as a cloud repository.

2. Disable the tenant account:

    a. Open the **Cloud Connect** view.

    b. In the inventory pane, click **Tenants**.

    c. In the working area, right-click the tenant account and select **Disable**.

3. Copy a folder with tenant backup files from the initial cloud repository to the new cloud repository.

4. Change resource allocation settings for the tenant on the initial cloud repository:

    a. Open the **Cloud Connect** view.

    b. In the inventory pane, click **Tenants**.

    c. In the working area, right-click the tenant account and select **Properties**.

    d. At the **Backup Resources** step of the wizard, select the initial cloud repository in the list and click **Edit**.

    e. In the **Edit Quota** window, change the underlying backup repository for the initial cloud repository. To do this, from the **Backup repository** list, select the backup repository that you configured at the step 1.

    f. If necessary, you can increase or decrease the tenant quota.

    g. Click **Finish** to save the changes.

5. Enable the tenant account:

    a. Open the **Cloud Connect** view.

    b. In the inventory pane, click **Tenants**.

    c. In the working area, right-click the tenant account and select **Disable**.

If the SP moved tenant data between backup repositories based on servers with different operating systems, the tenant must rescan the cloud repository in the tenant Veeam Backup & Replication console:
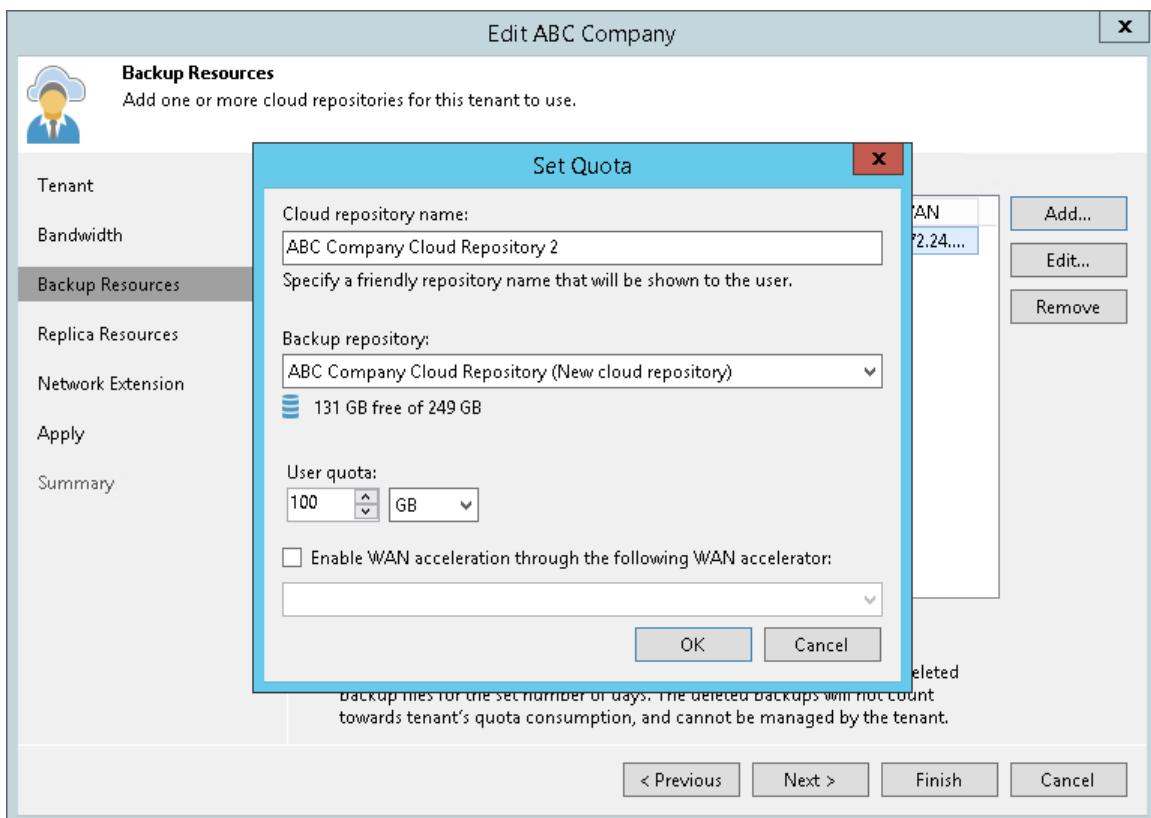
1. In the tenant Veeam backup console, open the **Backup Infrastructure** view.

2. In the inventory pane, click **Backup Repositories**.

3. In the working area, right-click the cloud repository and select **Rescan**.

If the SP changed the tenant quota, the new quota becomes visible to the tenant after the tenant performs a rescan operation for the service provider or cloud repository on their backup server, or after the next job run.

Scenario 2. Adding New Cloud Repository
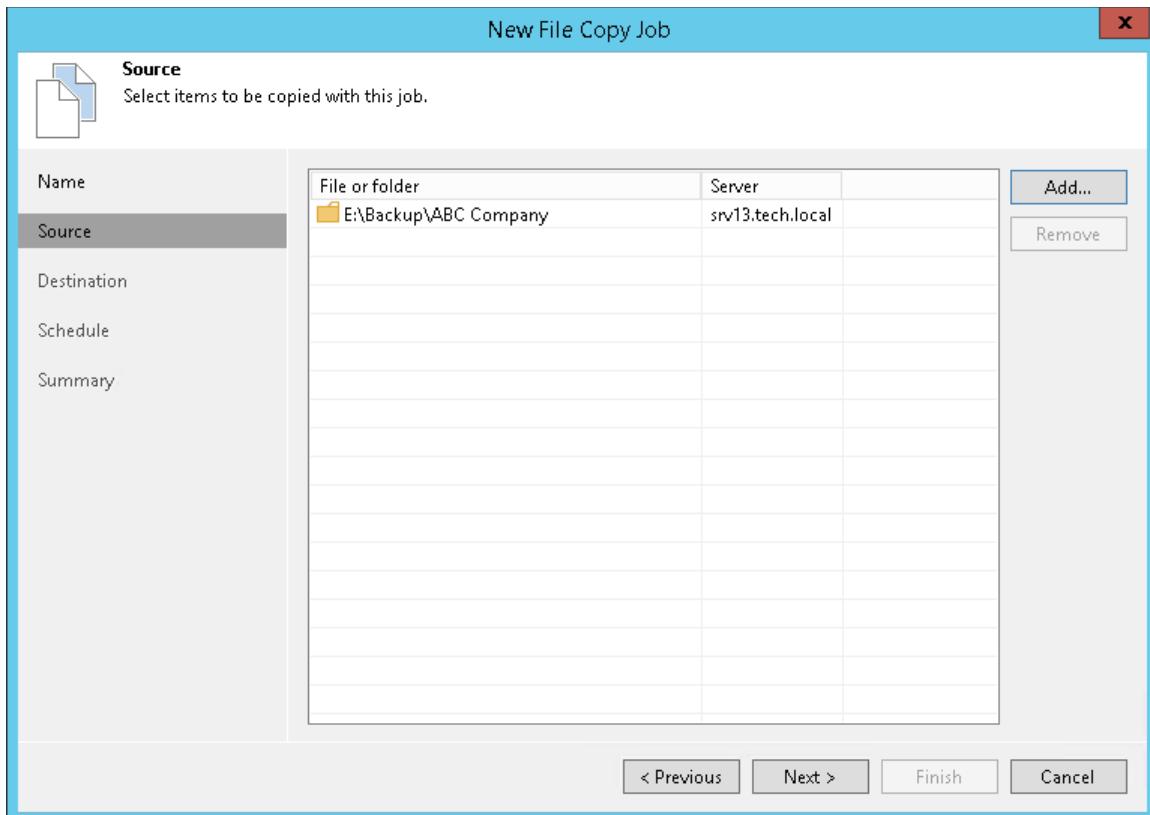
The SP must complete the following tasks:

1. Configure a new backup repository that you plan to use as a cloud repository.

2. On a newly configured cloud repository, allocate resources to the tenant:

    a. Open the **Cloud Connect** view.

    b. In the inventory pane, click **Tenants**.

    c. In the working area, right-click the tenant account and select **Properties**.

    d. At the **Backup Resources** step of the wizard, click **Add** and allocate resources on the new cloud repository to the tenant.

    e. Click **Finish** to save the changes.

3. Disable the tenant account:

    a. Open the **Cloud Connect** view.

    b. In the inventory pane, click **Tenants**.

    c. In the working area, right-click the tenant account and select **Disable**.

4. Copy a folder with tenant backup files from the initial cloud repository to the new cloud repository.

    If you move tenant backups from a scale out backup repository, make sure to copy all folders with tenant backup files from repository extents.
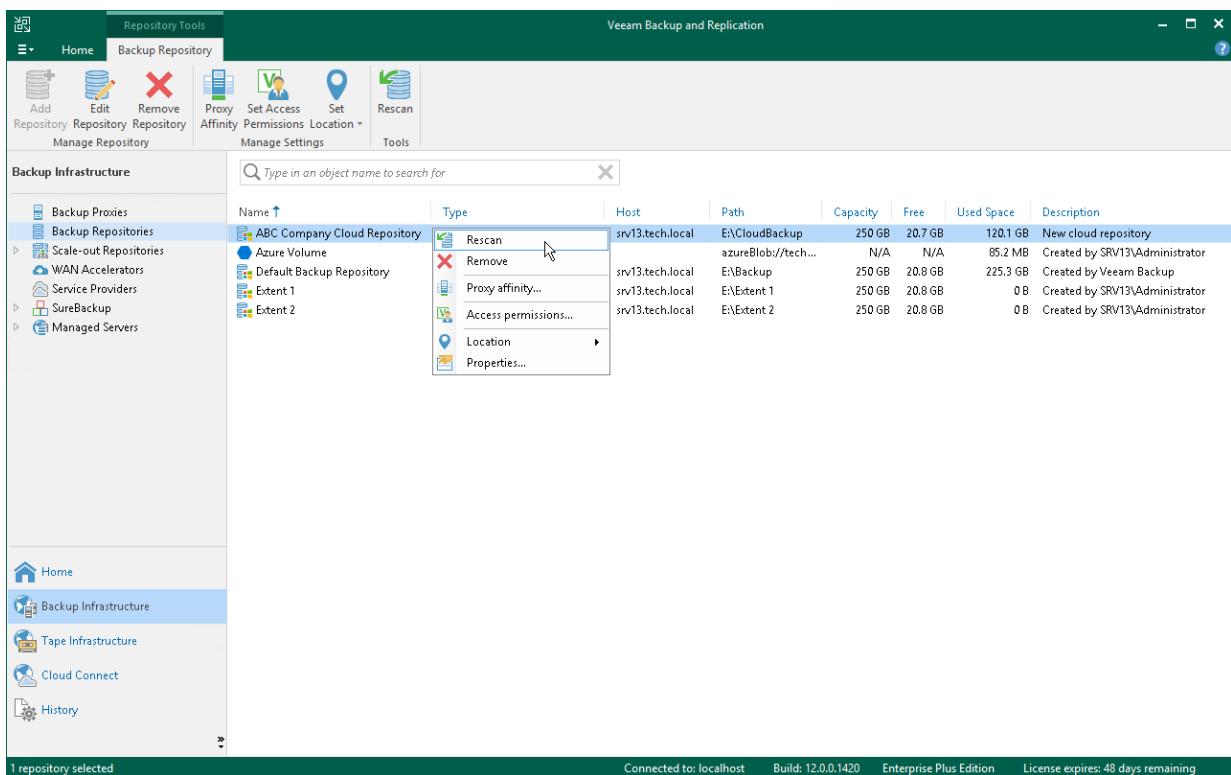
5. Enable the tenant account:

    a. Open the **Cloud Connect** view.

    b. In the inventory pane, click **Tenants**.

    c. In the working area, right-click the tenant account and select **Disable**.

6. Rescan the new cloud repository:

    a. In the SP Veeam Backup & Replication console, open the **Backup Infrastructure** view.

    b. In the inventory pane, click **Backup Repositories**.

    c. In the working area, right-click the backup repository that is exposed as a new cloud repository and select **Rescan**.
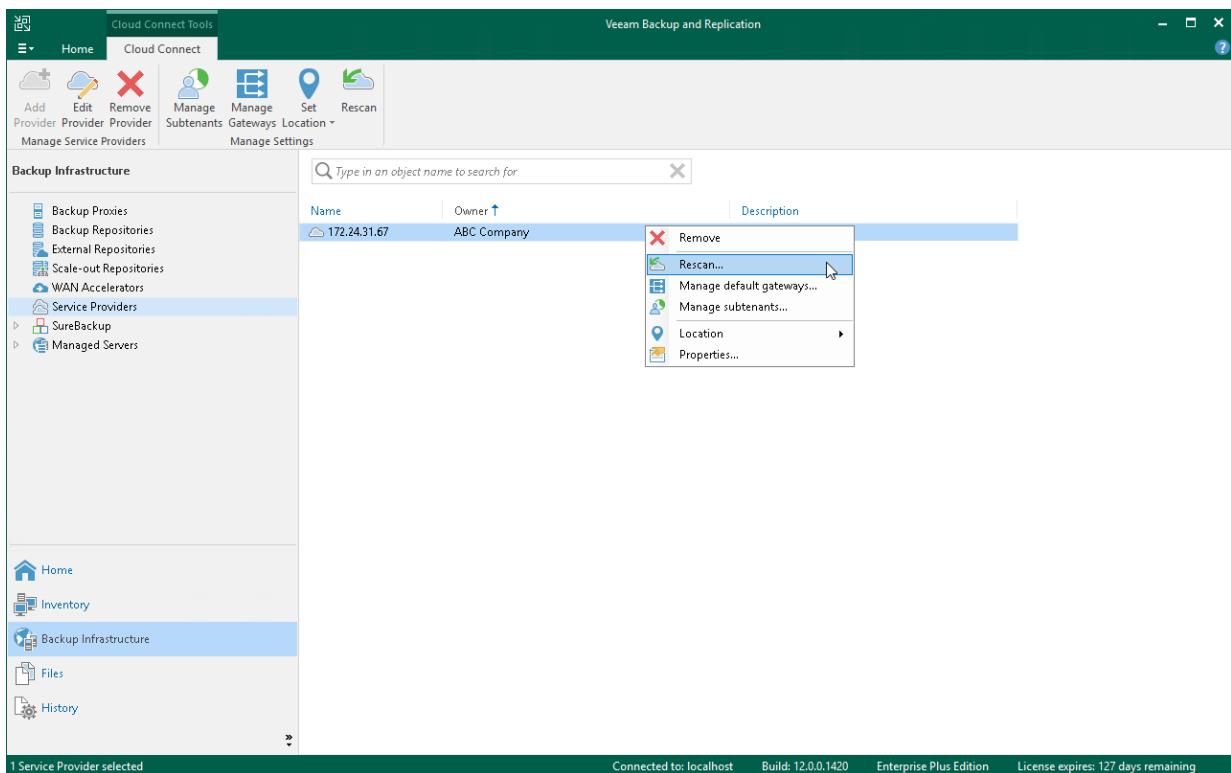
IMPORTANT

Do not delete backup files on the initial cloud repository at this moment. It is strongly recommended that you delete backup files after the tenant completes the data migration procedure on their backup server and ensures no data is lost.

The tenant must complete the following tasks:

1. Rescan the service provider:

   a. In the tenant Veeam Backup & Replication console, open the **Backup Infrastructure** view.

   b. In the inventory pane, click **Service Providers**.

   c. In the working area, right-click the service provider and select **Rescan**.

2. Enumerate backups on the new cloud repository.

Backups that reside in the new cloud repository will appear in the **Home** view next to backups that were created in the initial cloud repository.

Unencrypted backups will be displayed under the **Backups** > **Cloud** node. Encrypted backups will be displayed under the **Backups** > **Cloud (Encrypted)** node. To unlock backups:
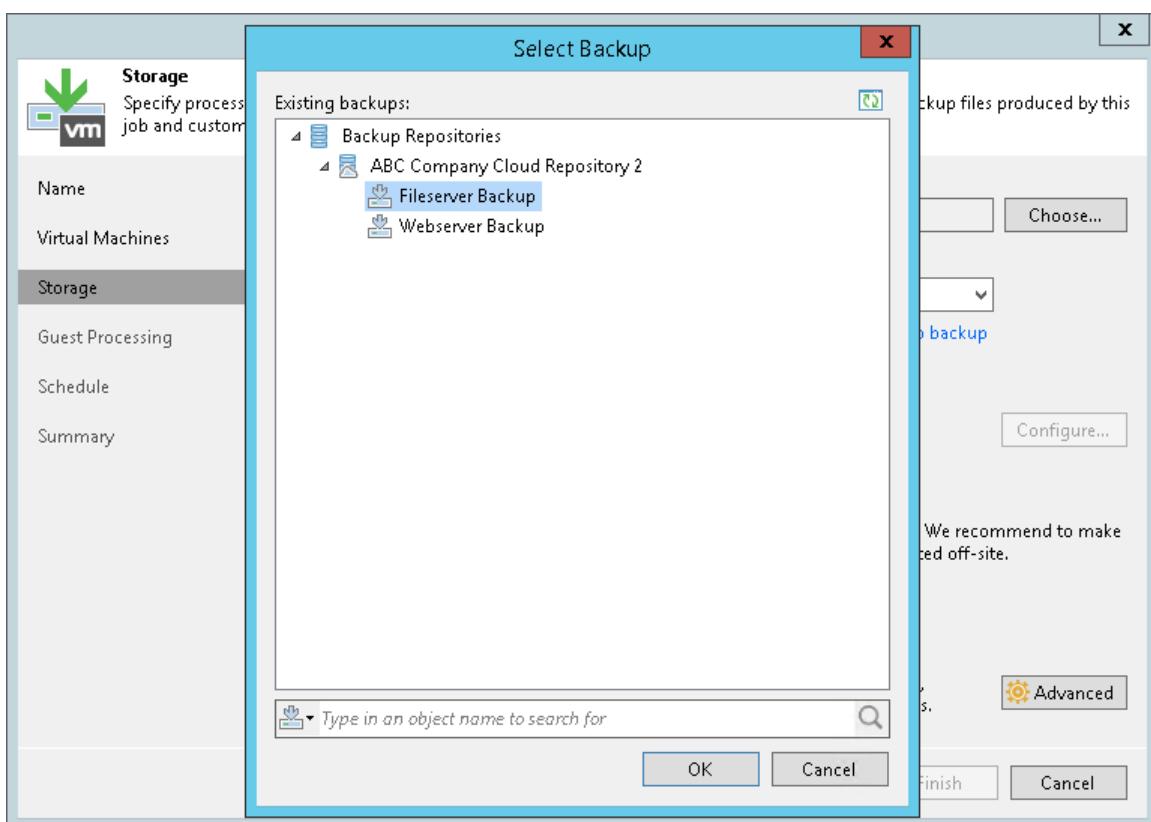
a. Select the **Backups** > **Cloud (Encrypted)** node, right-click the backup in the working area and select **Specify password**.

b. In the **Specify Password** window, type in the password for the backup.

Unlocked backups will be moved under the **Backups** > **Cloud** node.

3. Map backup jobs and backup copy jobs to backups on the new cloud repository:
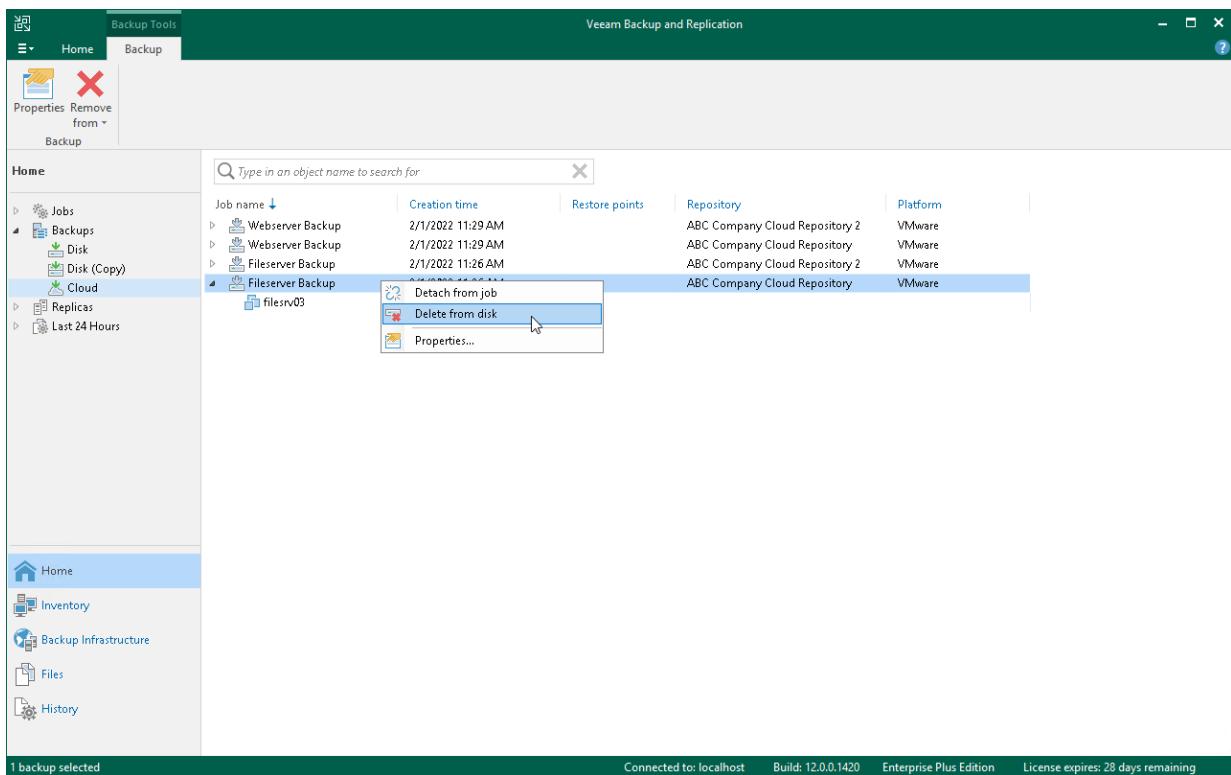
   a. Open the **Home** view.

   b. In the inventory pane, click **Jobs**.

   c. In the working area, right-click the job that you want to edit and select **Edit**.

   d. At the **Storage** (for backup jobs) or **Target** (for backup copy) step of the wizard, select the new cloud repository from the **Backup repository** list.

   e. Click **Map backup**.

   f. In the **Select Backup** window, choose the backup job and click **OK**.

   g. Save the job settings.

   h. Repeat steps c–g for all jobs that whose backups have been moved.

4. After the tenant makes sure that backups have been successfully copied and mapped to jobs, the tenant can delete backup files from the initial cloud repository:

   a. Open the **Home** view.

   b. In the inventory pane, click **Backups** > **Cloud**.

   c. In the working area, right-click the backup job whose backups you want to remove and select **Delete from disk**.

   d. Repeat steps b–c for all jobs whose backups whose backups have been moved.

   > **IMPORTANT**
   >
   > Make sure that you do not delete backup files from the new cloud repository instead of the initial cloud repository.
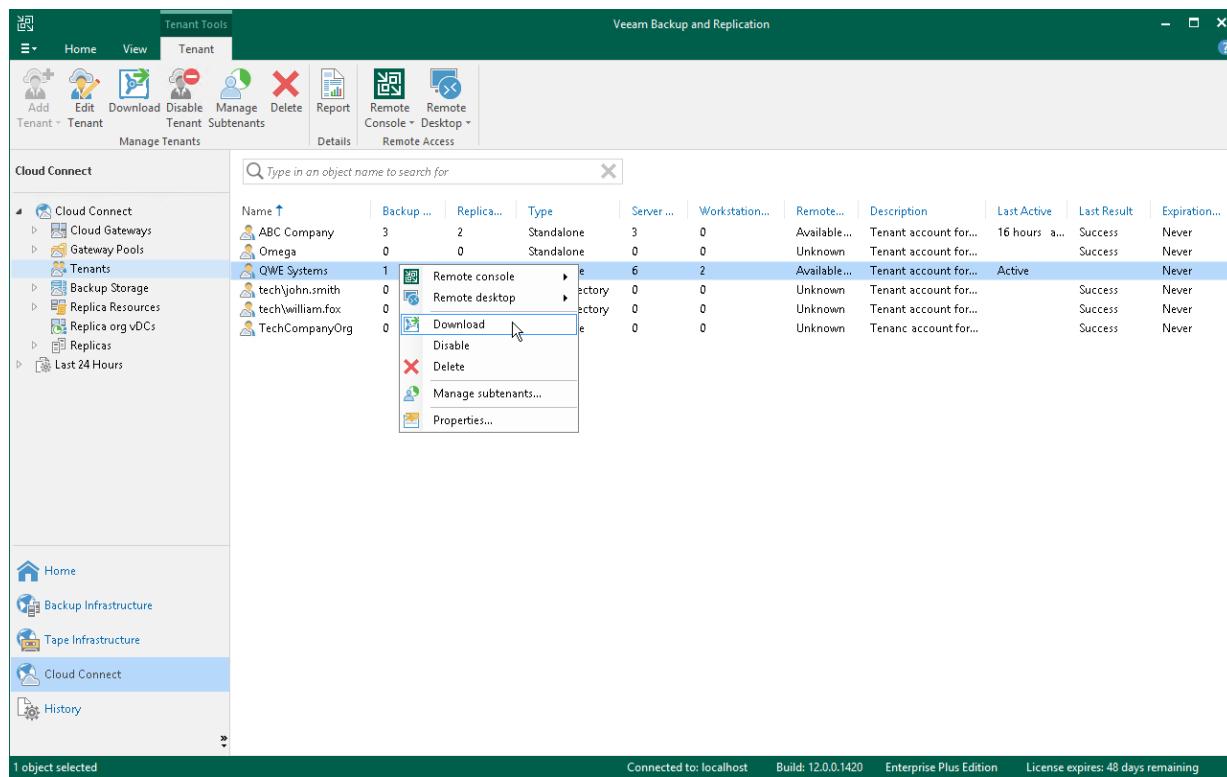
Downloading Tenant Data from Capacity Tier

The SP can download tenant data that was offloaded to an object storage repository back to the on-premises extents of a scale-out backup repository. Veeam Backup & Replication lets the SP download all offloaded tenant backups at once. Downloaded backups remain in the performance tier and cannot be moved back to the capacity tier.

To download tenant data from capacity tier to performance tier:

1. Open the **Cloud Connect** view.

2. In the inventory pane, click the **Tenants** node.

3. In the working area, select the necessary tenant and click **Download** on the ribbon or right-click the tenant and select **Download**.

4. In the displayed window, select what backup files you want to download from the capacity tier to the the on-premises extents:

   o Click **All Backups** to download all tenant backup files.

   o Click **Latest Only** to download tenant backup files pertaining to the latest backup chain only.

5. In the **SOBR Download** window, monitor the progress of the download operation and click **OK**.

Retrieving Tenant Data from Archive Tier

The SP can use the archive tier functionality to extend a scale-out backup repository used as a cloud repository with an additional tier of storage. This can be useful for backup of rarely accessed tenant data: compared to the capacity tier, it is cheaper to store archived data in the archive tier, but more expensive to restore it from the archive tier. For more information on the archive tier functionality, see the Archive Tier section in the Veeam Backup & Replication User Guide.

Archived data must be prepared for restore from the archive tier. To do this, the SP must retrieve the archived data. In contrast to the regular backup scenario where you can retrieve archived data using the Veeam backup console, in the Veeam Cloud Connect Backup scenario, this operation is available with Microsoft PowerShell cmdlets only. To learn more, see the Publish-VBRCloudArchiveRestorePoint section in the Veeam PowerShell Reference.

Managing Tenant VM Replicas

The SP can perform the following operations with tenant VM replicas created with replication jobs targeted at the cloud host:
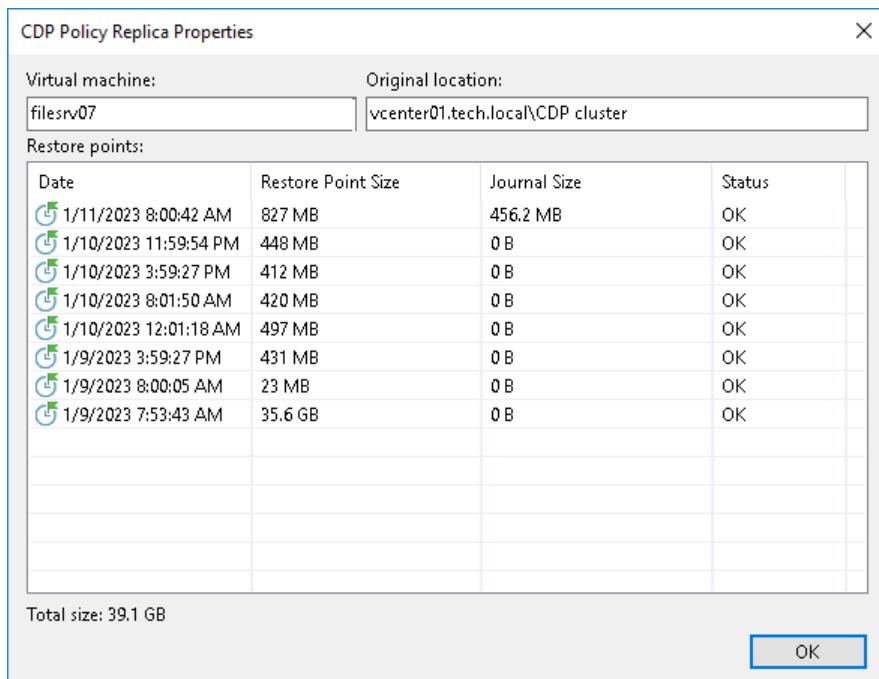
- View properties

- Remove from configuration

- Delete from disks

- Move tenant replicas to another storage

Viewing Properties

You can view summary information about created tenant VM replicas. The summary information provides the following data: available restore points, date of restore points creation, data size, restore point size and replica status.

To view summary information for replicas:

1. Open the **Cloud Connect** view.

2. In the inventory pane, click **Replicas**.

3. In the working area, right-click the necessary VM replica and select **Properties**.

Removing from Configuration

You can use the **Remove from configuration** operation if you want to remove records about tenant VM replicas from the Veeam Backup & Replication console and database. Replicated VMs remain on the cloud host and, if necessary, you can start them manually after **Remove from configuration** operation is performed.
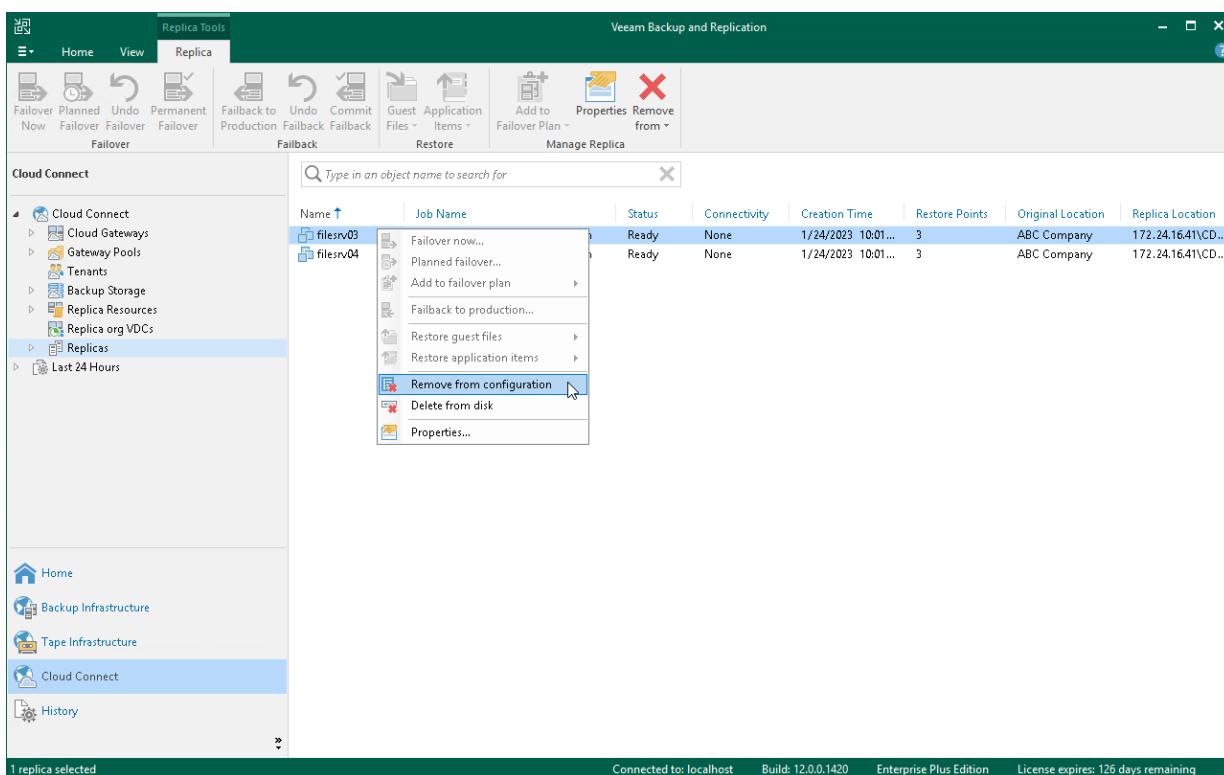
> **IMPORTANT**
>
> After you perform the **Remove from configuration** operation, records about tenant VM replicas will be permanently removed from configuration. You will not be able to reinstate them in the Veeam Backup & Replication console and database.
>
> The tenant will not be able to use VM replicas that remain on the cloud host. To let the tenant use such VM replicas, you will have to map VM replicas to a new replication job. To learn more, see this Veeam KB article.

To remove records about VM replicas from the Veeam Backup & Replication console and database:

1. Open the **Cloud Connect** view.

2. In the inventory pane, click **Replicas**.

3. In the working area, right-click the necessary VM replica and select **Remove from configuration**.
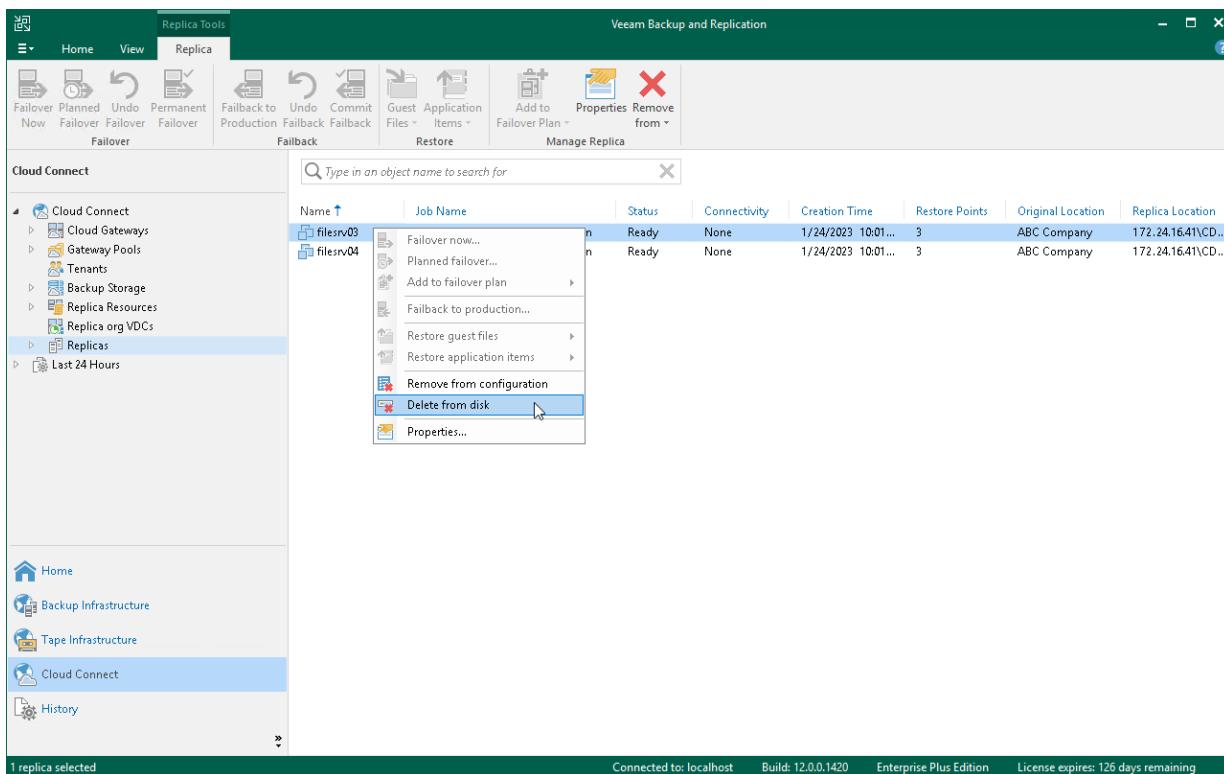
Deleting from Disk

You can use the **Delete from disk** operation if you want to delete records about tenant VM replicas from the Veeam Backup & Replication console and database and, additionally, unregister the VM replica on the cloud host and delete actual replica files from the datastore or volume.

Do not delete tenant VM replicas from the cloud host manually. Use the **Delete from disk** option instead. If you delete VM replicas manually, subsequent replication job sessions will fail.

To remove VM replicas from the cloud host:

1. Open the **Cloud Connect** view.

2. In the inventory pane, click **Replicas**.

3. In the working area, right-click the necessary VM replica and select **Delete from disk**.

Moving Replica Files to Another Location

The SP may need to move tenant VM replica files to another location, for example, if the initial storage is running out of space. This operation can be performed on the VMware vSphere platform as well as on the Microsoft Hyper-V platform.

The operation does not require any actions on the tenant side. For the tenant, VM replica files remain on the same cloud host, in the same cloud storage.

> **IMPORTANT**
>
> It is not recommended that the SP or tenant move tenant VM replicas created in VMware Cloud Director to another vApp. During this operation, all restore points created for VM replicas except for the latest restore point will be deleted.

Before you move tenant replica files, check the following prerequisites:

- The new datastore (for VMware vSphere platform) or storage volume (for Microsoft Hyper-V platform) must be connected to the same host or cluster as the initial datastore/volume.

- All active replication job sessions and failover tasks must be stopped for VM replicas created by tenants whose replica files are moved to another datastore/volume.
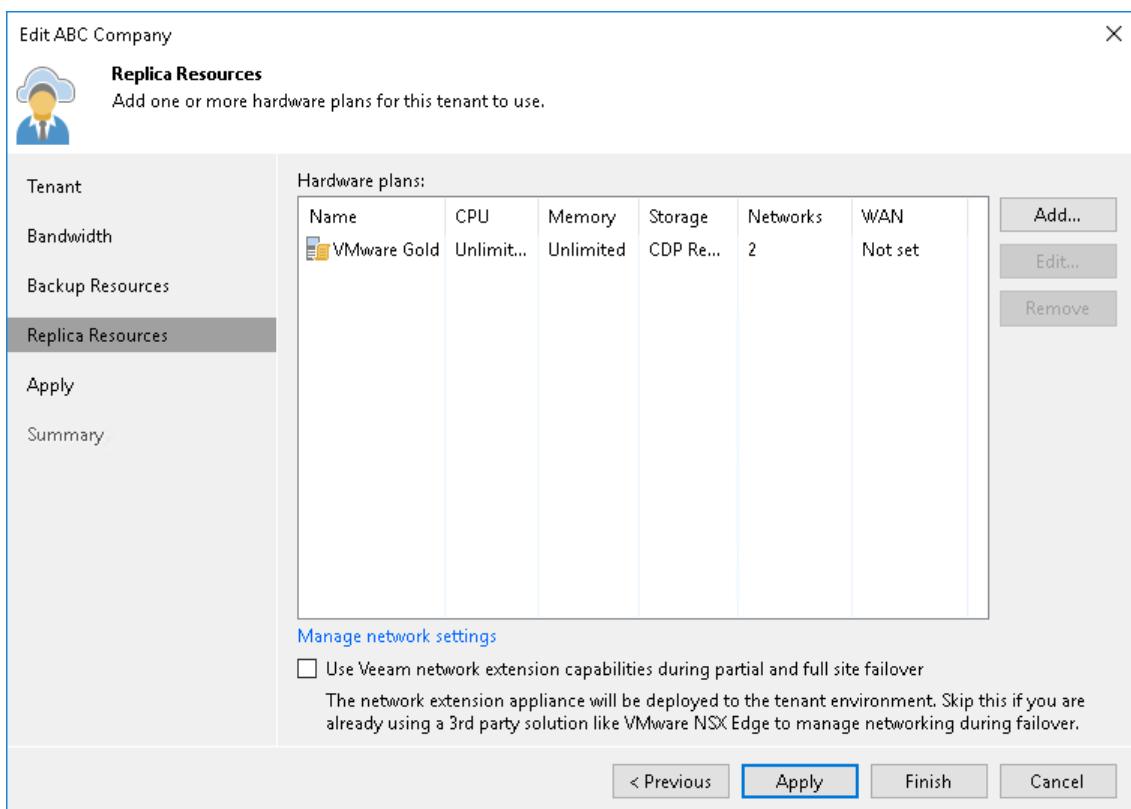
> **NOTE**
>
> When you move tenant replicas to a new location, you must change the storage location in the settings of the hardware plan that utilized storage resources of the initial location (datastore or volume). As a result, you can move to a new location only all replicas created by tenants that are subscribed to this hardware plan at once.
>
> For example, *Tenant 1* and *Tenant 2* are subscribed to the same VMware hardware plan and their VM replica files are kept on the same datastore. In this case, you cannot move replicas created by *Tenant 1* to a new datastore and let replicas created by *Tenant 2* remain on the initial datastore. Instead, you need to move all replicas created by *Tenant 1* and *Tenant 2* to a new datastore.
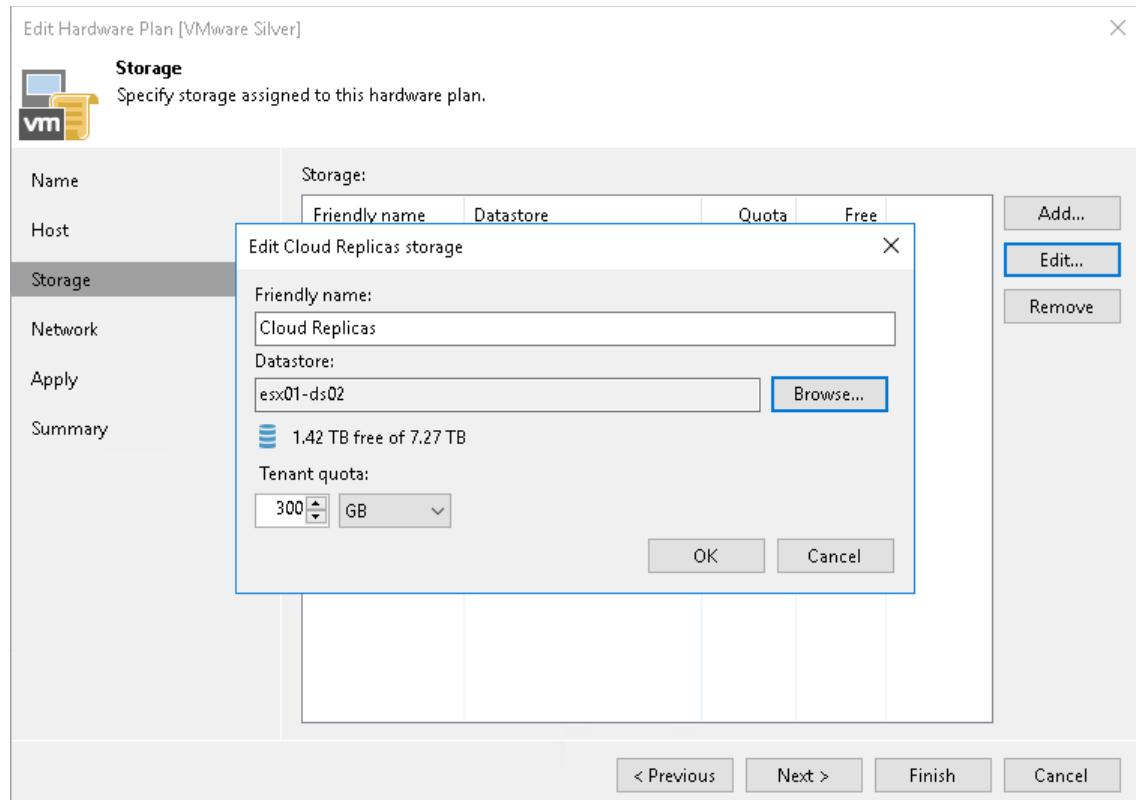
The SP must complete the following tasks:
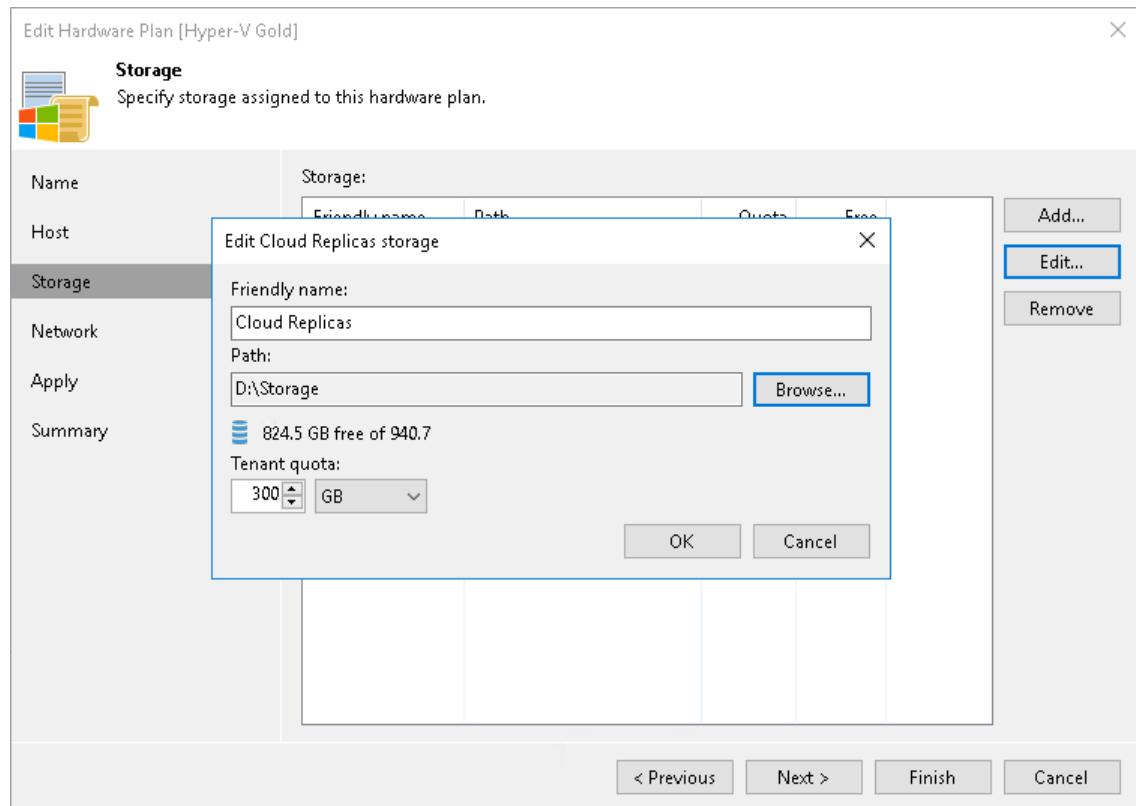
1. Remove the SP-side network extension appliance(s) used by tenant VM replicas in the initial location.

   a. Open the **Cloud Connect** view.

   b. In the inventory pane, click **Tenants**.

   c. In the working area, right-click the necessary tenant and select **Properties**.

   d. At the **Replica Resources** step of the wizard, clear the **Use built-in network management capabilities during failover** check box.

   e. Click **Finish**.

   f. [Optional] If more than one tenant is subscribed to the hardware plan that utilizes storage resources of the initial VM replica location, repeat steps a–e for each tenant whose replicas you plan to move to a new location.

2. Move tenant data from the initial location to the new location:

   o [For VMware vSphere] Use Storage vMotion to move tenant VM replicas to the new datastore.

   o [For Microsoft Hyper-V] Use the *Move* option in Hyper-V Manager (or Failover Cluster Manager) to move tenant VM replicas to a path on the new storage volume.

3. Change storage allocation settings in the hardware plan settings:

   a. Open the **Cloud Connect** view.

   b. In the inventory pane, click **Replica Resources**.

   c. In the working area, right-click the hardware plan for which you want to change storage settings and select **Edit Hardware Plan**.

   d. At the **Storage** step of the wizard, select the cloud storage that uses quota on the initial storage from which VM replicas have been moved and click **Edit**.

   e. In the **Edit Storage** window, change the datastore/path for the cloud storage:

      ▪ [For VMware Hardware Plan] In the **Datastore** section, click **Browse** and select the datastore to which VM replicas have been moved.
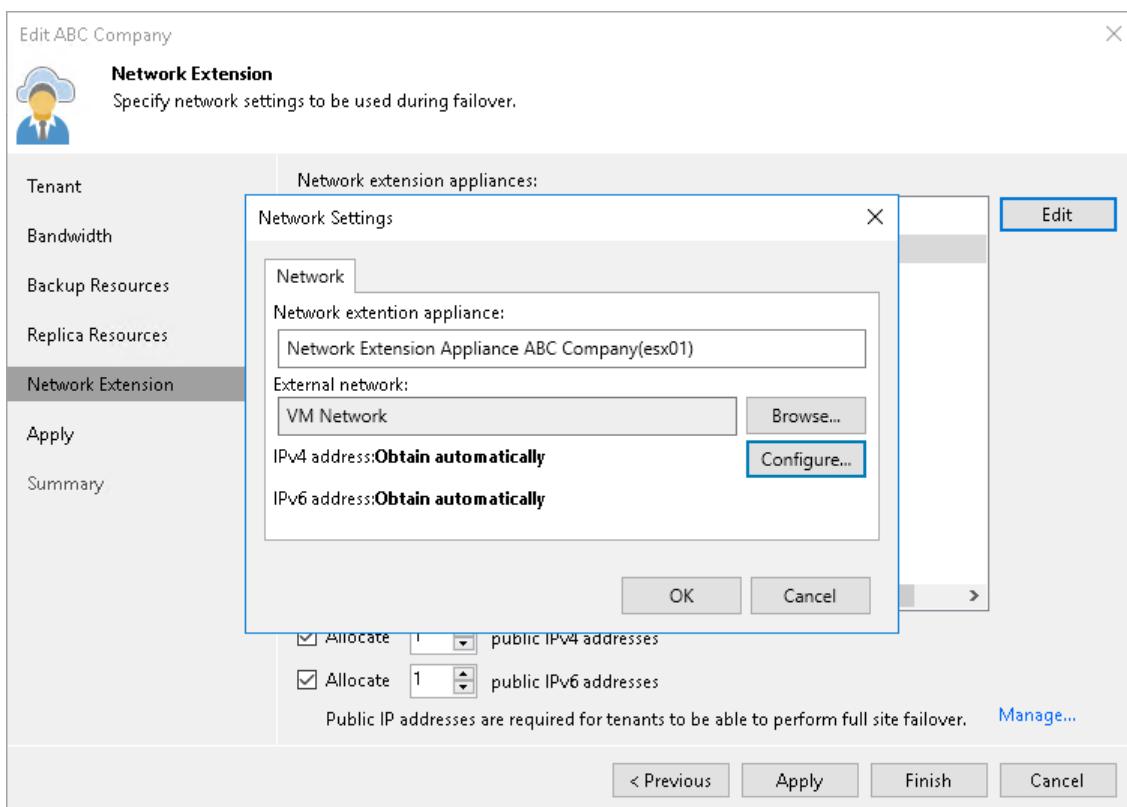
- [For Hyper-V Hardware Plan] In the **Path** section, click **Browse** and specify a path to the folder to which VM replicas have been moved.

f. Click **OK**.

g. At the **Apply** step of the wizard, wait until Veeam Backup & Replication updates the hardware plan settings. Then click **Finish**.

4. Deploy the new SP-side network extension appliance(s) in the new location where you have moved tenant VM replicas.

   a. Open the **Cloud Connect** view.

   b. In the inventory pane, click **Tenants**.

   c. In the working area, right-click the necessary tenant and select **Properties**.

   d. At the **Replica Resources** step of the wizard, select the **Use built-in network management capabilities during failover** check box.

   e. At the **Network Extension** step of the wizard, specify settings for the new SP-side network extension appliance that will be used by tenant VM replicas in the new location. To learn more, see Specify Network Extension Settings.

   f. Click **Apply**. Then click **Finish**.

   g. [Optional] If more than one tenant is subscribed to the hardware plan that utilizes storage resources of the new VM replica location, repeat steps a–e for each tenant whose replicas you have moved to the new location.

Veeam Backup & Replication will deploy the new SP-side network extension appliance(s) on the datastore or storage volume where you have moved tenant VM replicas. Tenants subscribed to the hardware plan will be able to continue running replication jobs and performing failover tasks targeted at the cloud host.

Managing Tenant Cloud Failover Plans

A cloud failover plan created by a tenant is stored in the database on the SP's Veeam Backup & Replication server. The SP can manage tenant cloud failover plans from the Veeam Backup & Replication console on the SP side. This may be useful in case the tenant Veeam backup server is unavailable along with the production site after a disaster.

The SP can perform the following operations with a tenant's cloud failover plan:

- Run a cloud failover plan.

- Test a cloud failover plan.

- Retry a cloud failover plan.

- Undo failover by a cloud failover plan.

- Edit cloud failover plan settings.

- Perform permanent failover.

Running Cloud Failover Plan

With a cloud failover plan, the SP can perform full site failover upon tenant request at any time. During full site failover, tenant VMs fail over to their replicas on the cloud host one by one, as a group. You can fail over to the most recent VM state or select the necessary restore point for VMs in the cloud failover plan.
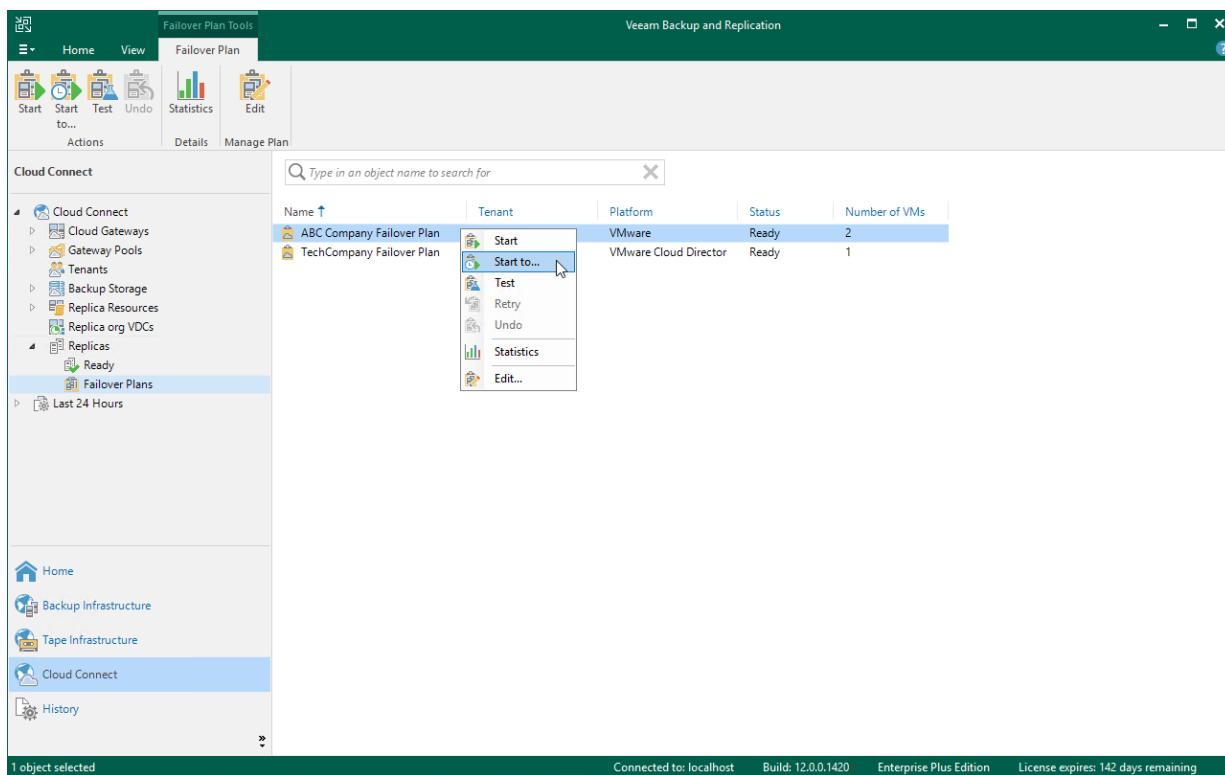
The SP can run a tenant's cloud failover plan from the Veeam Backup & Replication console on the SP Veeam backup server.

To fail over to the VM replicas latest restore point:

1. Open the **Cloud Connect** view.

2. In the inventory pane, expand the **Replicas** node and click **Failover Plans**.

3. In the working area, click the necessary cloud failover plan and click **Start** on the ribbon or right-click the necessary cloud failover plan and select **Start**.

To fail over to a certain restore point:

1. Open the **Cloud Connect** view.

2. In the inventory pane, expand the **Replicas** node and click **Failover Plans**.

3. In the working area, click the necessary cloud failover plan and click **Start to** on the ribbon or right-click the necessary cloud failover plan and select **Start to**.

4. In the displayed dialog box, select the backup date and time. Veeam Backup & Replication will find the closest restore point prior to the entered value for each VM and fail over to it.

Testing Cloud Failover Plan
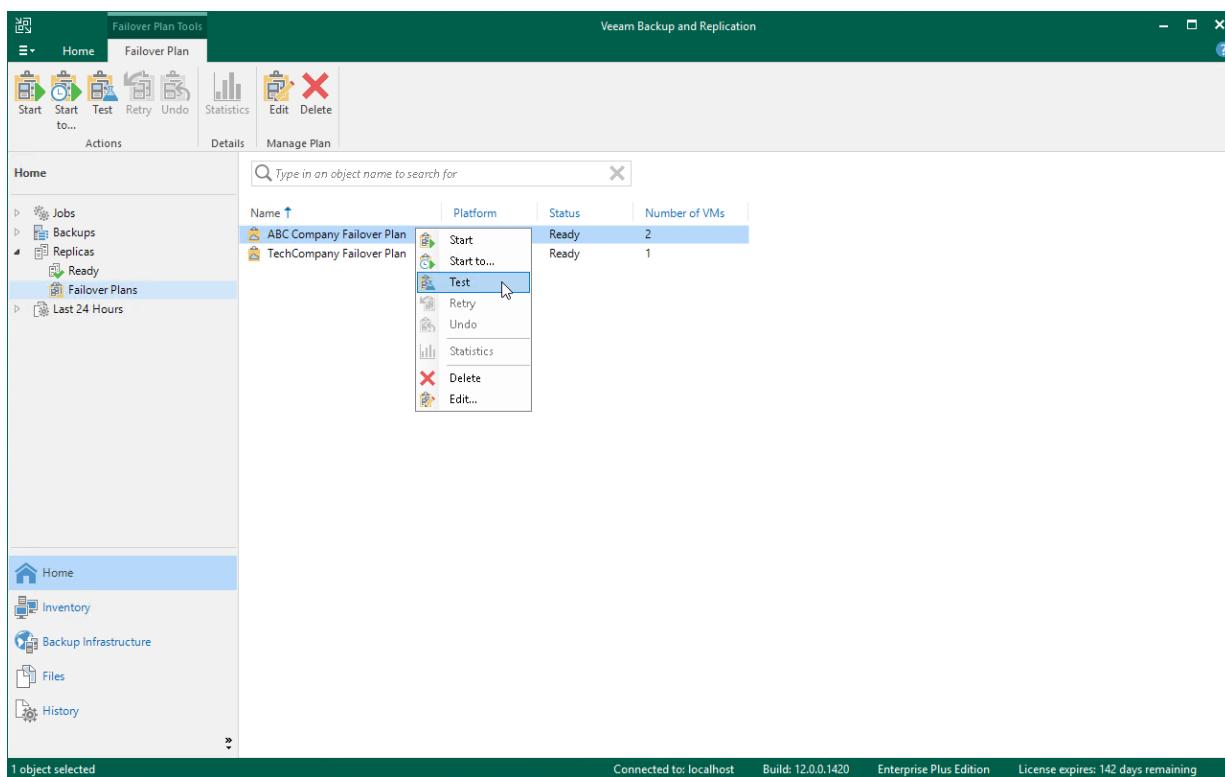
The SP can test a tenant's cloud failover plan to ensure replicated tenant VMs on the cloud host successfully start and can be accessed from external network after failover. When you test a cloud failover plan, Veeam Backup & Replication does not switch from a production VM to its replica. Instead, it reverts every VM replica in the cloud failover plan to the latest restore point, boots the replica operation system, waits for the VM replica to reach a "stabilization point" using the *Stabilization by IP* algorithm and checks if the VM replica responds to ping requests.

> **IMPORTANT**
>
> You can perform the test operation only for cloud failover plans that contain snapshot-based replicas. This operation is not supported for failover plans that contain CDP replicas.

To test a cloud failover plan:

1. Open the **Cloud Connect** view.

2. In the inventory pane, expand the **Replicas** node and click **Failover Plans**.

3. In the working area, right-click the necessary cloud failover plan and select **Test**.
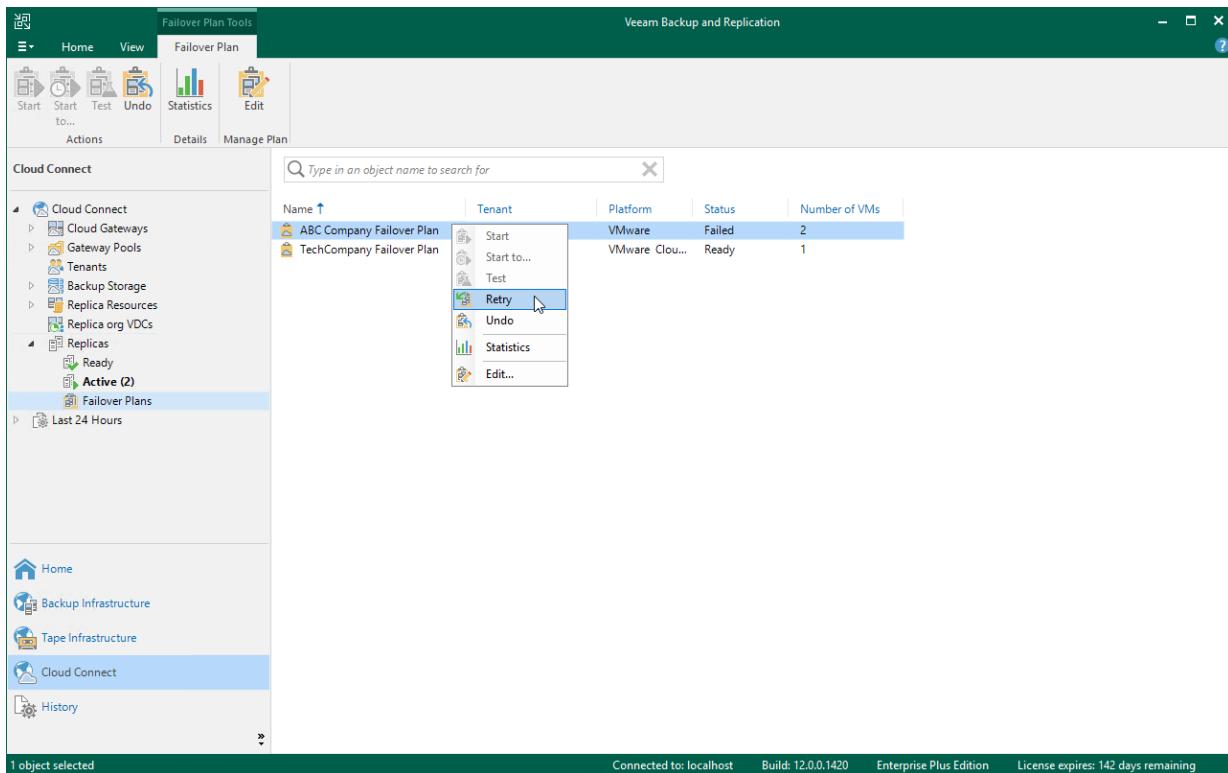
Retrying Cloud Failover Plan

The SP can retry failover by a tenant's cloud failover plan in case the full site failover process fails before all tenant VMs fail over to their replicas on the cloud host.

To retry failover by a cloud failover plan:

1. Open the **Cloud Connect** view.

2. In the inventory pane, expand the **Replicas** node and click **Failover Plans**.

3. In the working area, right-click the necessary cloud failover plan and select **Retry**.
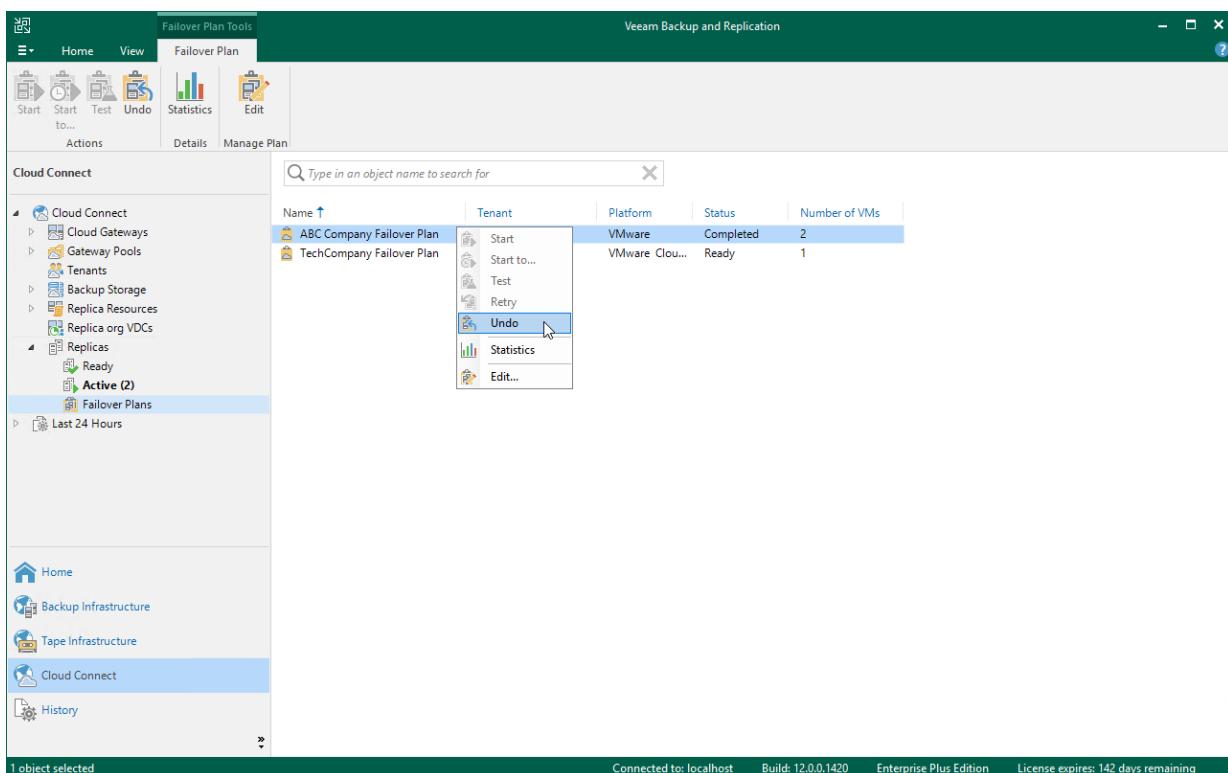
Undoing Failover by Cloud Failover Plan

The SP can undo failover for all tenant VMs added to the cloud failover plan at once. When you undo failover, you switch the workload back to original VMs and discard all changes that were made to tenant VM replicas during failover.

To undo failover by a cloud failover plan:

1. Open the **Cloud Connect** view.

2. In the inventory pane, expand the **Replicas** node and click **Failover Plans**.

3. In the working area, click the necessary cloud failover plan and click **Undo** on the ribbon or right-click the necessary cloud failover plan and select **Undo**.

4. In the displayed window, click **Yes** to confirm the operation.

Editing Cloud Failover Plan Settings

If the SP wants to execute custom scripts before and/or after the tenant's cloud failover plan, the SP must create those scripts in advance and select them in the cloud failover plan settings before the tenant runs the cloud failover plan. For example, the SP may want to send an email to backup administrators before the failover plan is started and/or after the failover operation completes. Veeam Backup & Replication supports script files in BAT and CMD formats and executable files in the EXE format.
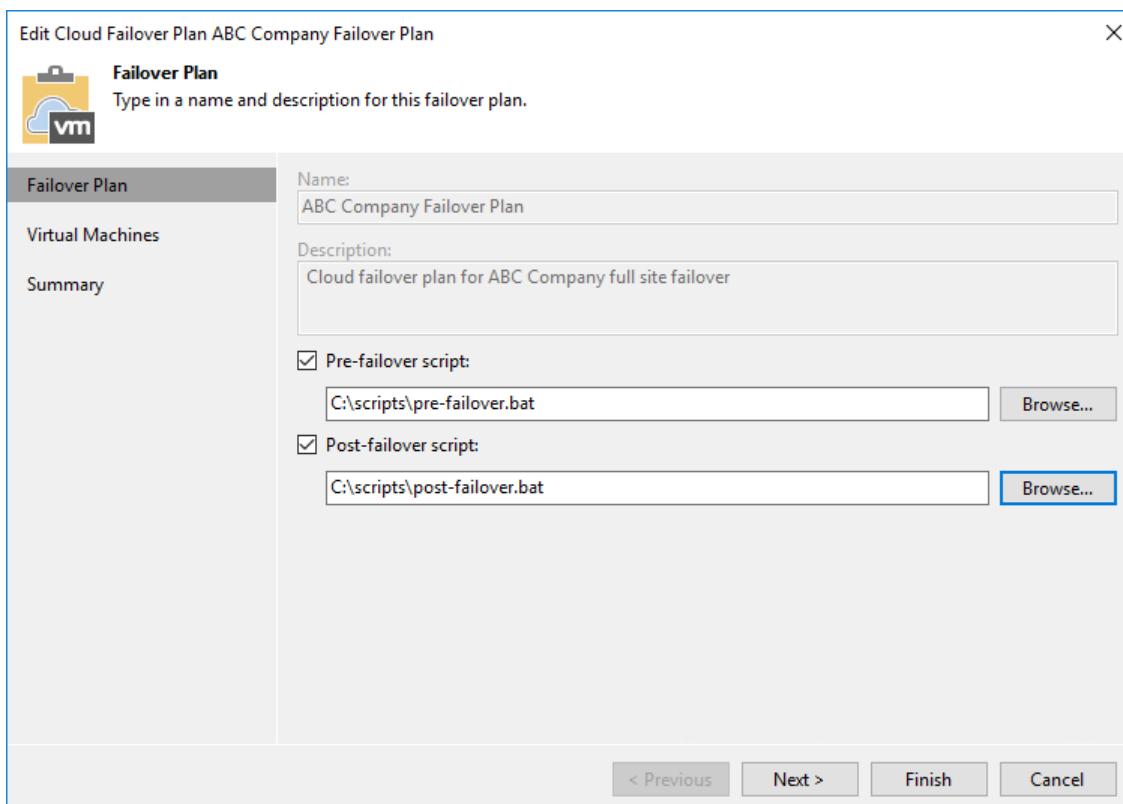
The process of specifying script settings is the same for regular cloud failover plans and cloud failover plans for VMs that have replicas in VMware Cloud Director.

> **NOTE**
>
> In the cloud failover plan settings, the SP can only specify pre-failover and post-failover scripts. The SP cannot change other failover plan settings specified by the tenant.

To edit cloud failover plan settings:

1. Launch the **Edit Cloud Failover Plan** wizard:

    a. Open the **Cloud Connect** view and click **Replicas** > **Failover Plans** in the inventory pane.

    b. In the working area, click the necessary cloud failover plan and click **Edit** on the ribbon or right-click the necessary cloud failover plan and select **Edit**.

2. At the **Failover Plan** step of the wizard, select the **Pre-failover script** and **Post-failover script** check boxes and click **Browse** to choose executable file(s).

3. At the **Virtual Machines** step of the wizard, enumerate virtual machines that the tenant added to the cloud failover plan.

4. At the **Summary** step of the wizard, review the information about the edited hardware plan and click **Finish** to exit the wizard.

Performing Permanent Failover
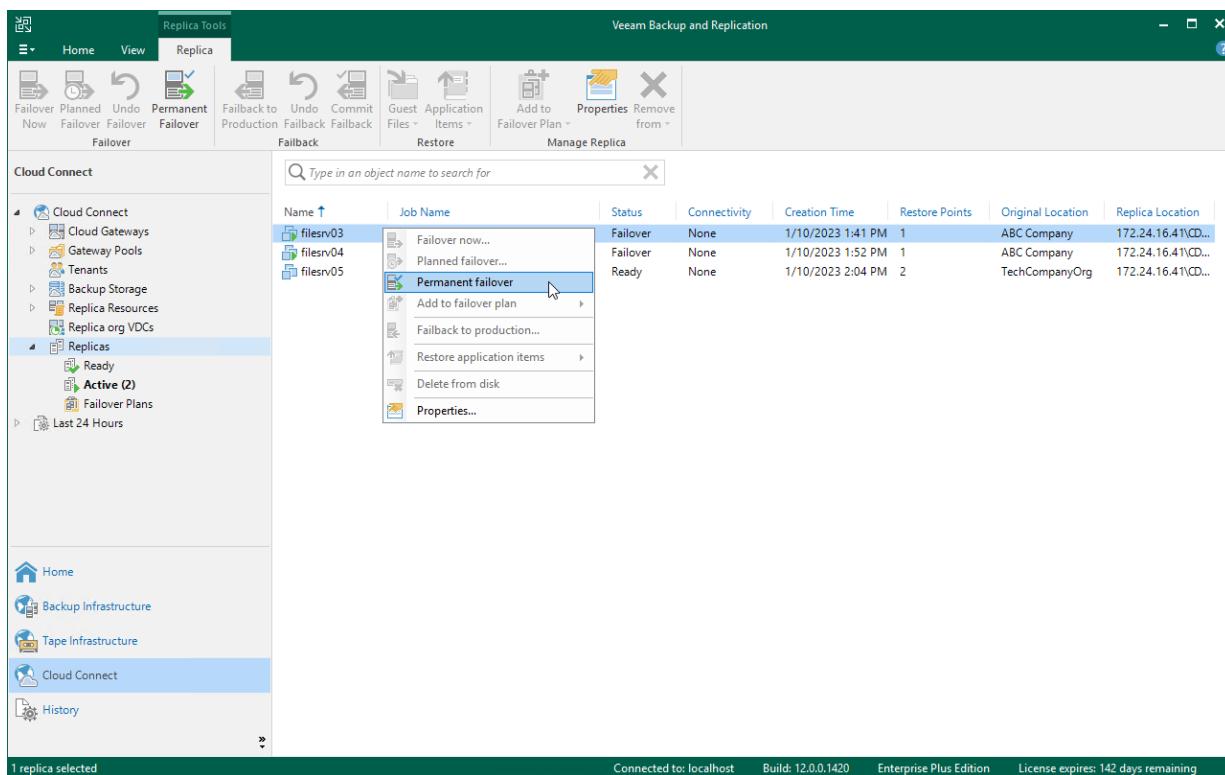
The SP can perform the permanent failover operation if the tenant wants to permanently switch from the original VM to a VM replica on the cloud host and use this replica as the original VM.

To perform permanent failover, do either of the following:

- Open the **Cloud Connect** view, in the inventory pane select **Replicas**. In the working area, select the necessary VM and click **Permanent Failover** on the ribbon.

- Open the **Cloud Connect** view, in the inventory pane select **Replicas**. In the working area, right-click the necessary VM and select **Permanent failover**.

In the displayed window, click **Yes** to confirm the operation.

After the permanent failover operation completes, the VM replica is put to the *Permanent failover* state. To protect the VM replica from corruption after performing permanent failover, Veeam Backup & Replication reconfigures the replication job and adds the original VM to the list of exclusions. When the replication job that processes the original VM starts, the VM will be skipped from processing, and no data will be written to the working VM replica.

Using Remote Access Console

The SP can remotely access the tenant backup server to manage Veeam Backup & Replication deployed on the tenant side. The SP can connect to a tenant backup server in one of the following ways:

- Connect to a tenant backup server with the Remote Access Console.

- Connect to a tenant backup server over the Remote Desktop Protocol.

As part of the remote tenant backup server management process, the SP may also need to perform the following administration tasks:

- Set up Veeam Backup & Replication to accept connections from a remotely deployed Remote Access Console (over the internet).

- Manage credentials used to connect to SP and tenant backup servers.

- Adjust remote desktop connection settings.

Connecting to Tenant with Remote Access Console

To connect to the tenant backup server, the SP must run the Remote Access Console on the SP backup server or dedicated machine.

Before You Begin

Before you use the Remote Access Console to connect to the tenant backup server, complete the following prerequisites:

- Connection with the Remote Access Console to the tenant backup server is possible only if the SP and tenant backup servers have the same build number and the same private fixes of Veeam Backup & Replication installed. Build numbers of Veeam Backup & Replication plug-ins must be the same as well. If the build numbers and/or private fixes differ, remote connection to the tenant backup server may be established over the Remote Desktop Protocol. To learn more, see Launching Remote Desktop Session to Tenant.

- The tenant must enable the **Allow this Veeam Backup & Replication installation to be managed by the service provider** option in the **Service Provider** wizard when connecting to the SP. To learn more, see Specify Cloud Gateway Settings.

- If the machine on which you plan to use the Remote Access Console does not reside in the SP backup infrastructure network, you need to set up Veeam Backup & Replication to accept connections from the Remote Access Console over the internet. To learn more, see Enabling Access to Cloud Gateway.

Step 1. Open Remote Access Console

To connect to the tenant backup server, the SP must open the Remote Access Console. The Remote Access Console is available on the SP backup server or dedicated machine on which the Veeam Backup & Replication is installed.

To open the Remote Access Console, do one of the following:
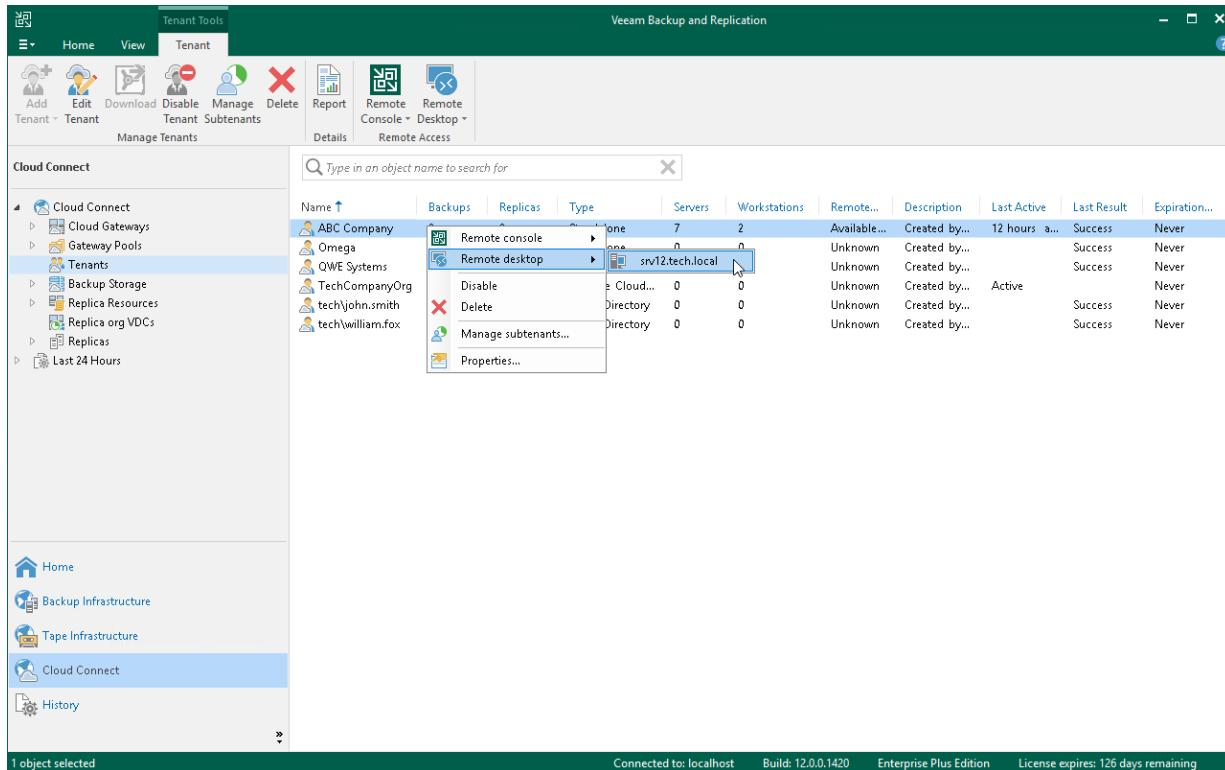
- Double-click the **Veeam Backup & Replication Remote Access Console** icon on the desktop (you can use this option only if you want to open the Remote Access Console on the SP backup server).

- Run the following command:

```
"%ProgramFiles%\Veeam\Backup and Replication\Console\veeam.backup.shell.exe" –TenantRemoteAccess
```

On the SP backup server, the SP can also open the Remote Access Console from the locally installed Veeam Backup & Replication console. In this case, the SP can connect to the backup server of the specific tenant.

To open the Remote Access Console:

1. Open the **Cloud Connect** view.

2. In the inventory pane, click the **Tenants** node.

3. Select the tenant in the working area, click **Remote Console** on the ribbon and select the backup server to which you want to connect or right-click the tenant in the working area, select **Remote console** and select the backup server to which you want to connect.

Step 2. Specify Backup Server Settings

To query information about currently available tenants and access the Cloud network redirector, the Remote Access Console needs to connect to the SP backup server. You must specify connection settings to access the SP backup server in the *Open Remote Access Console* dialog window. The process of specifying SP backup server settings differs depending on the Remote Access Console deployment scenario:

- If the Remote Access Console is deployed in the SP Veeam Cloud Connect infrastructure, you must specify settings to connect directly to the SP backup server. To learn more, see Settings for Direct Connection.

- If the Remote Access Console is deployed on a remote machine in an external network, you must specify settings to connect to the SP backup server through a cloud gateway. To learn more, see Settings for Connection through Cloud Gateway.

Settings for Direct Connection

If you open the Remote Access Console on the SP backup server or dedicated machine connected to the SP backup infrastructure network, you must specify settings to connect directly to the SP backup server. To specify connection settings:

1. In the *Open Remote Access Console* dialog, in the **Cloud Connect server** field, click the **Not set** link.

   > **NOTE**
   >
   > If you have already specified settings to connect to the SP backup server, the link in the *Cloud Connect server* field will contain the name or IP address of the backup server and status of the connection: *Connected* or *Disconnected*.
   >
   > - If the status is *Disconnected*, click the link in the *Cloud Connect server* field to pass to the step 2 below.
   > - If the status is *Connected*, you can pass to specifying tenant backup server settings. To learn more, see Log On to Tenant Backup Server.
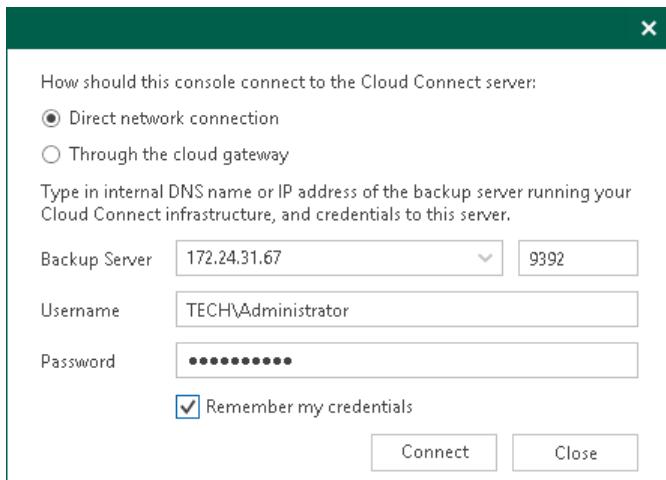
2. In the displayed window, in the **How should this console connect to the Cloud Connect server** field, make sure that the **Direct network connection** option is selected.

3. In the **Backup Server** field, type the name or IP address of the SP backup server or select it from the list of recent connections. If you open the Remote Access Console on the SP backup server, by default, the backup server field contains IP address of this backup server — 127.0.0.1 (localhost).

4. In the **Port** field, enter the port over which you want to connect to the SP backup server. The port number is set at the Port Configuration step of the setup wizard for Veeam Backup & Replication. By default, port 9392 is used.

5. In the **Username** and **Password** fields, enter credentials of the user account that you want to use to connect to the SP backup server. The user account must have the Veeam Backup Administrator role on the SP backup server.

6. To save entered credentials, select the **Remember my credentials** option. Veeam Backup & Replication will save credentials locally in the Credential Manager of the machine on which you are opening the Remote Access Console. Every next time you open the Remote Access Console, Veeam Backup & Replication will automatically connect to the SP backup server using saved credentials.

   You can remove saved credentials at any time you need. To learn more, see Managing Credentials.

7. Click **Connect**.

Settings for Connection Through Cloud Gateway

If the Remote Access Console is deployed on a remote machine connected to an external network, you must specify settings to connect to the SP backup server from the internet through a cloud gateway. To specify connection settings:

1. In the *Open Remote Access Console* dialog, in the **Cloud Connect server** field, click the **Not set** link.

   > **NOTE**
   >
   > If you have already specified settings to connect to the SP backup server, the link in the *Cloud Connect server* field will contain the name or IP address of the backup server and status of the connection: *Connected* or *Disconnected*.
   >
   > - If the status is *Disconnected*, click the link in the *Cloud Connect server* field to pass to the step 2 below.
   > - If the status is *Connected*, you can pass to specifying tenant backup server settings, To learn more, see Log On to Tenant Backup Server.
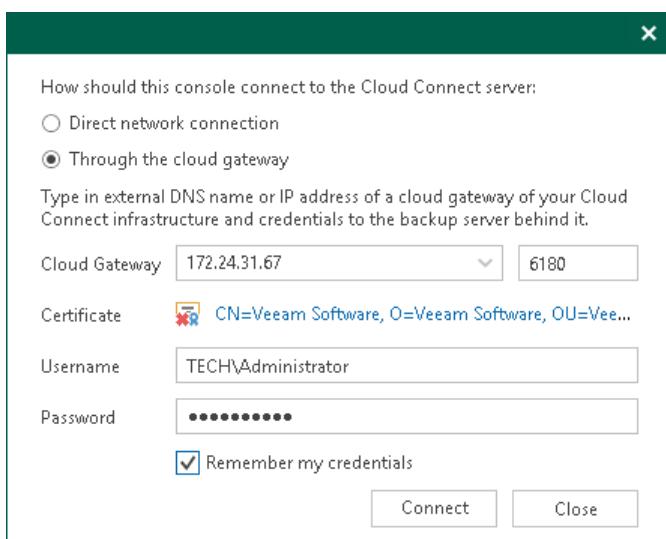
2. In the displayed window, in the **How should this console connect to the Cloud Connect server** field, select the **Through the cloud gateway** option.

3. In the **Cloud Gateway** field, type the name or IP address of the cloud gateway or select it from the list of recent connections.

4. In the **Port** field, enter the port over which you want to connect to the cloud gateway. The port number is set at the **Name** step of the **New Cloud Gateway** wizard. By default, port 6180 is used.

5. In the **Certificate** field, Veeam Backup & Replication will display information about the TLS certificate used to establish a secure connection between Veeam Cloud Connect infrastructure components. To view information about the certificate, click the link in the **Certificate** field.

6. In the **Username** and **Password** fields, enter credentials of the user account that you want to use to connect to the SP backup server. The user account must have the Veeam Backup Administrator role on the SP backup server.

7. To save entered credentials, select the **Remember my credentials** option. Veeam Backup & Replication will save credentials locally in the Credential Manager of the machine on which you are opening the Remote Access Console. Every next time you open the Remote Access Console, Veeam Backup & Replication will automatically connect to the SP backup server using saved credentials.

    You can remove saved credentials at any time you need. To learn more, see Managing Credentials.

8. Click **Connect**.

How should this console connect to the Cloud Connect server:

○ Direct network connection

◉ Through the cloud gateway

Type in external DNS name or IP address of a cloud gateway of your Cloud Connect infrastructure and credentials to the backup server behind it.

Cloud Gateway	172.24.31.67	6180
Certificate	CN=Veeam Software, O=Veeam Software, OU=Vee...	
Username	TECH\Administrator	
Password	••••••••••	

☑ Remember my credentials

Connect   Close

Step 3. Log On to Tenant Backup Server

To log on to Veeam Backup & Replication on the tenant side, you must specify connection settings to access the tenant backup server.

1. In the **Tenant** field, select from the list the user name of the tenant account to whose backup server you want to connect. Tenants who have opened a control connection to the SP and whose backup servers are available for connection with the Remote Access Console automatically appear in this list.

2. In the **Backup server** field, select from the list the name of the tenant backup server to which you want to connect. The list contains names of backup servers that belong to the selected tenant and are available for connection with the Remote Access Console.

3. In the **Username** and **Password** fields, enter credentials of the user account that you want to use to connect to the tenant backup server. The user account must have the Veeam Backup Administrator role on the tenant backup server (or other role that allows the user to perform required operations in Veeam Backup & Replication).

4. To save entered credentials, select the **Remember my credentials** option. Veeam Backup & Replication will save credentials locally in the Credential Manager of the machine on which you are opening the Remote Access Console. Every next time you open the Remote Access Console, Veeam Backup & Replication will automatically connect to the tenant backup server using saved credentials.

   You can remove saved credentials at any time you need. To learn more, see Managing Credentials.

5. To create a shortcut for the connection, click **Save shortcut**. You can create as many shortcuts as you need.

6. Click **Connect**.

Launching Remote Desktop Session to Tenant

You can use the Remote Access Console to open a connection to the tenant backup server over the Remote Desktop Protocol. On the machine where the Remote Access Console is installed, Veeam Backup & Replication will launch the Remote Desktop Connection client allowing you to log on to the OS running on the tenant backup server.

Before connecting to the tenant backup server over Remote Desktop Protocol, check the following prerequisites:

- The OS running on the tenant backup server must be set up to accept remote desktop connections.

- The Remote Access Console must be connected to the SP backup server.

To launch a remote desktop session:

1. Make sure that the Remote Access Console is connected to the SP backup server:

    a. Open the Remote Access Console.

    b. In the *Open Remote Access Console* dialog, check that the link in the **Cloud Connect server** field contains the name or IP address of the SP backup server and the status of the connection is *Connected*. If the status is *Disconnected*, specify settings to connect to the backup server. To learn more, see Connect to the SP backup server.

2. Launch a remote desktop session in one of the following ways:

    o In the Veeam Backup & Replication console running on the SP backup server, in the **Cloud Connect** view, click the **Tenants** node. Select the necessary tenant in the working area, click **Remote Desktop** on the ribbon and select the tenant backup server to which you want to connect.

    o In the Veeam Backup & Replication console running on the SP backup server, in the **Cloud Connect** view, click the **Tenants** node. Right-click the necessary tenant in the working area, select **Remote Desktop** and select the backup server to which you want to connect.

    o In the *Open Remote Access Console* window, make sure that the Remote Access Console is connected to the SP backup server, press and hold the **[CTRL]** key and click **Connect**. Instead of connecting to the tenant backup server with the Remote Access Console, Veeam Backup & Replication will launch the Remote Desktop Connection client.

3. In the **Windows Security** window, specify credentials to connect to the backup server and click **OK**. Veeam Backup & Replication will launch the Remote Desktop Connection client and connect to the backup server.
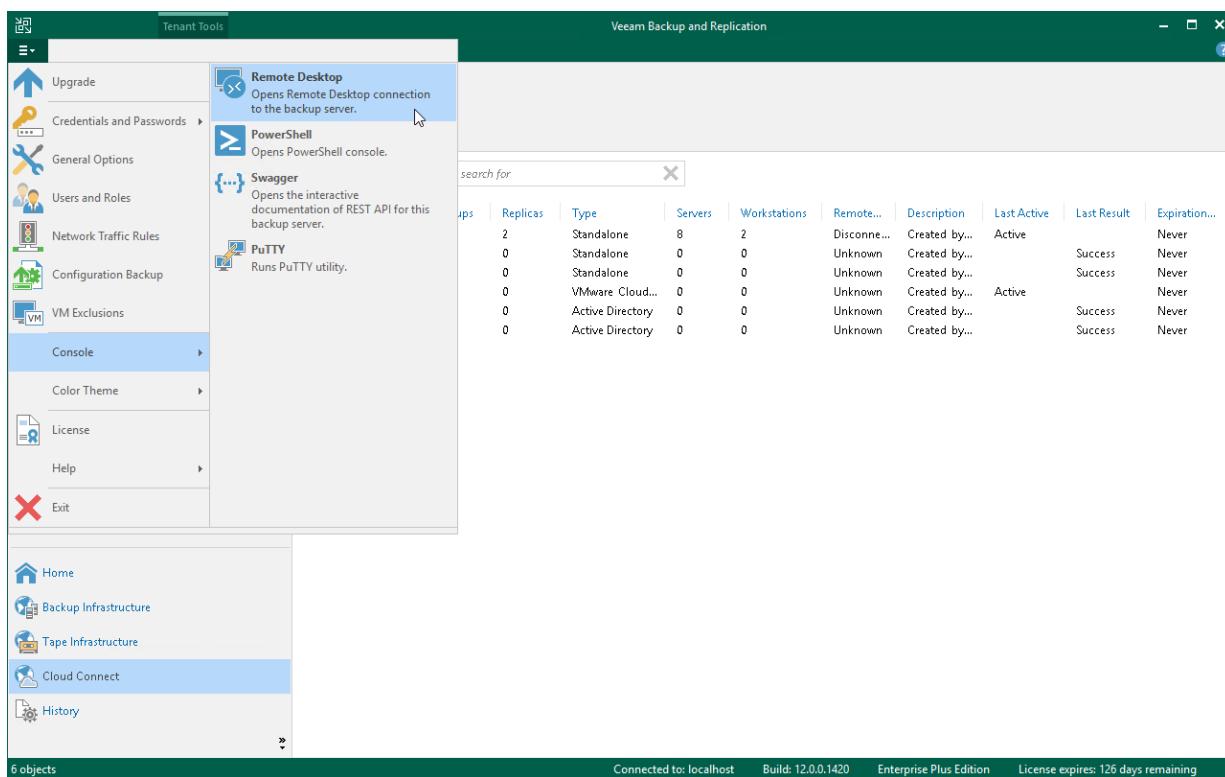
> **TIP**
>
> You can also launch the Remote Desktop Connection client from the main menu of the regular Veeam Backup & Replication console. In this case, Veeam Backup & Replication will open a remote desktop session to the backup server to which this Veeam backup console is currently connected. To learn more, see Establishing Remote Desktop Connection to Backup Server.

Establishing Remote Desktop Connection to Backup Server

You can start a remote desktop session not only to the tenant backup sever, but also to any backup server to which the Veeam Backup & Replication console is currently connected. To connect to a backup server over Remote Desktop Protocol.

1. In the Veeam Backup & Replication console, make sure that the console is connected to the necessary backup server. You can check the name or IP address of the backup server in the status bar of the Veeam backup console window.

2. In the **Main Menu**, select **Console** > **Remote Desktop**.

3. In the **Windows Security** window, specify credentials to connect to the backup server and click **OK**. Veeam Backup & Replication will launch the Remote Desktop Connection client and connect to the backup server.

Enabling Access to Cloud Gateway
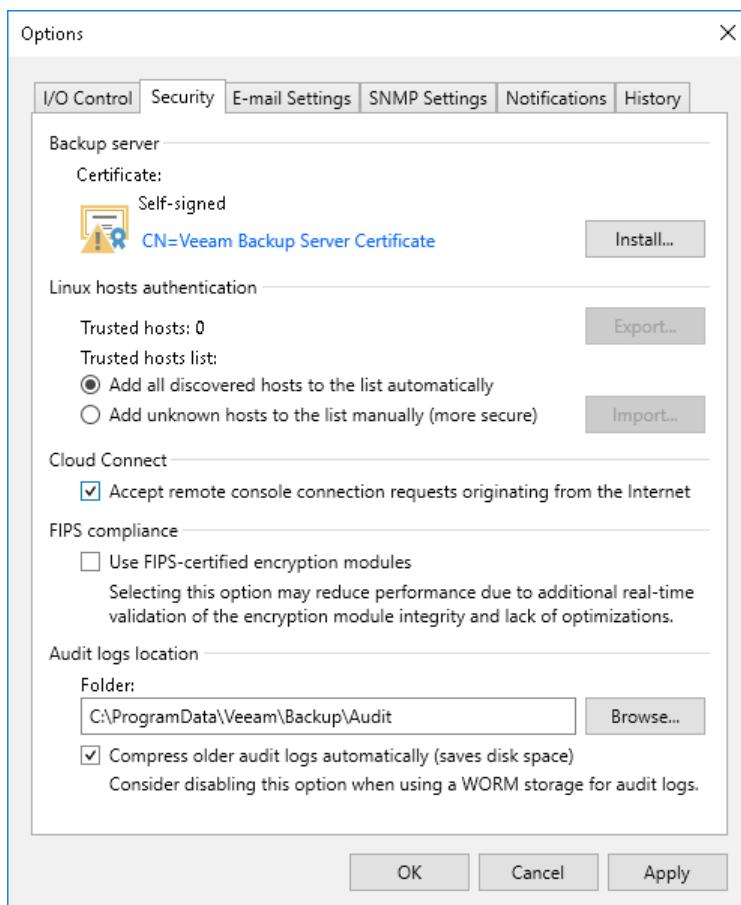
To query information about tenants whose backup servers are available for remote management, the Remote Access Console needs to connect to the SP backup server. If the Remote Access Console is installed on a remote machine connected to an external network (in the internet), the Remote Access Console will communicate with the SP backup server through the cloud gateway. By default, Veeam Backup & Replication does not accept connections from a Remote Access Console over the internet. The SP can enable this functionality in the in the Veeam Backup & Replication settings if necessary.

To enable access to the cloud gateway for the Remote Access Console:

1. On the SP Veeam backup server, open the Veeam Backup & Replication console.

2. From the main menu, select **General Options**.

3. Open the **Security** tab.

4. In the **Cloud Connect** section, select the **Accept remote console connection requests originating from the Internet** check box.

5. Click **OK**.

> **NOTE**
>
> The **Cloud Connect** section is available in the **Security** tab on the SP backup server only, that is, a Veeam backup server on which the Veeam Cloud Connect license is installed.

Managing Credentials
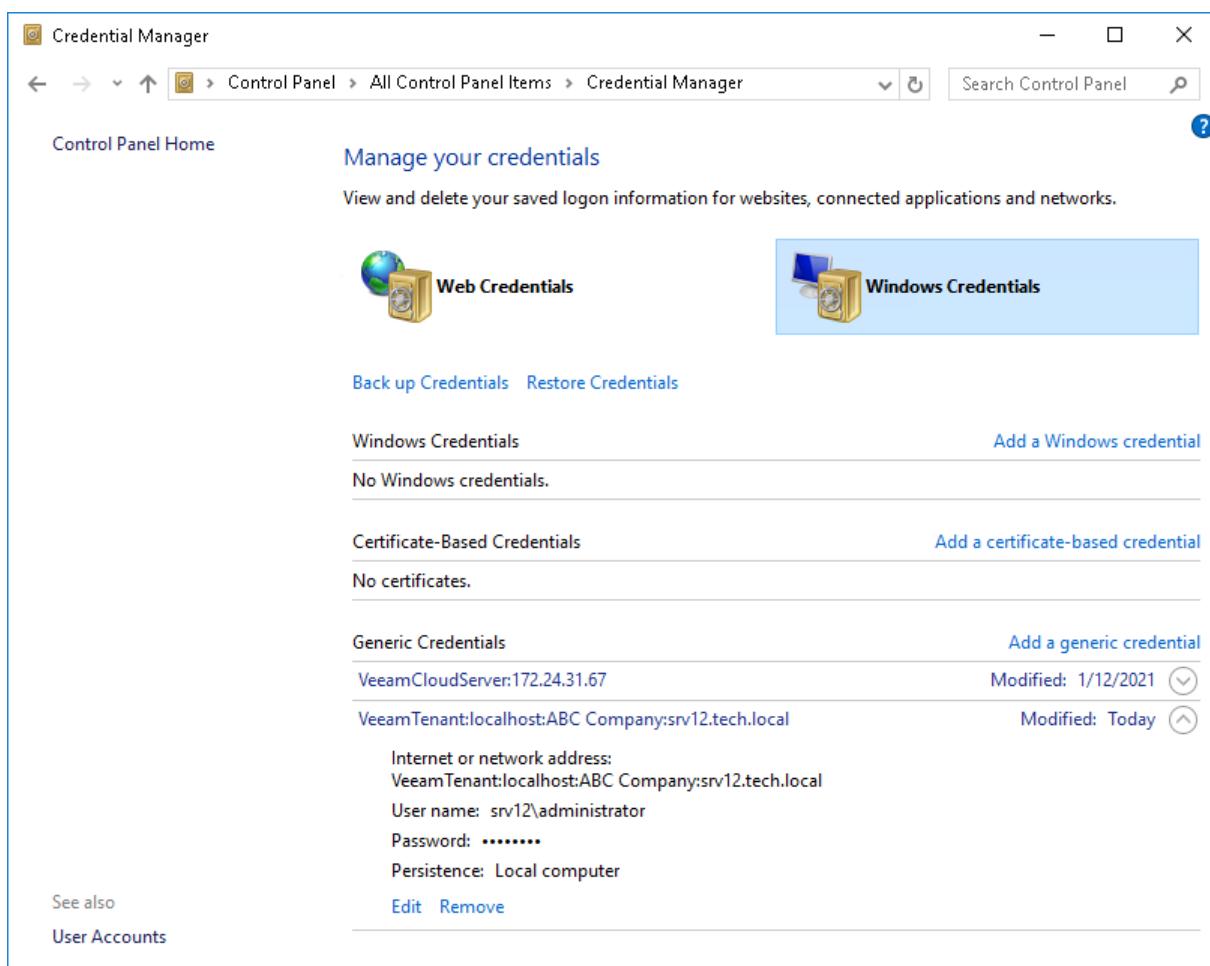
You can instruct Veeam Backup & Replication to save credentials entered in the **Open Remote Access Console** window. Veeam Backup & Replication will save these credentials in the Credential Manager of the machine that runs the Remote Access Console. Every next time you open the Remote Access Console, Veeam Backup & Replication will use saved credentials to automatically connect to the SP and/or tenant backup server.

Saved credentials used for connections to Veeam backup servers appear in the list of Windows Credentials, in the **Generic Credentials** section. For saved credentials, Veeam Backup & Replication creates credential records of the following types:

- **VeeamBackupServer** — credentials used for direct connection to the SP backup server.

- **VeeamCloudServer** — credentials used for connection to the SP backup server through the cloud gateway.

- **VeeamSaveTenant** — credentials used for connection to the tenant backup server.

You can remove saved credentials at any time you need, if necessary. To delete a credentials record:

1. On the machine that runs the Remote Access Console, from the **Start** menu, select **Control Panel** > **Credential Manager**.

2. In the **Credential Manager** window, click **Windows Credentials**.

3. In the **Generic Credentials** section, select the necessary credentials record and click **Remove**.

Adjusting Remote Desktop Connection Settings
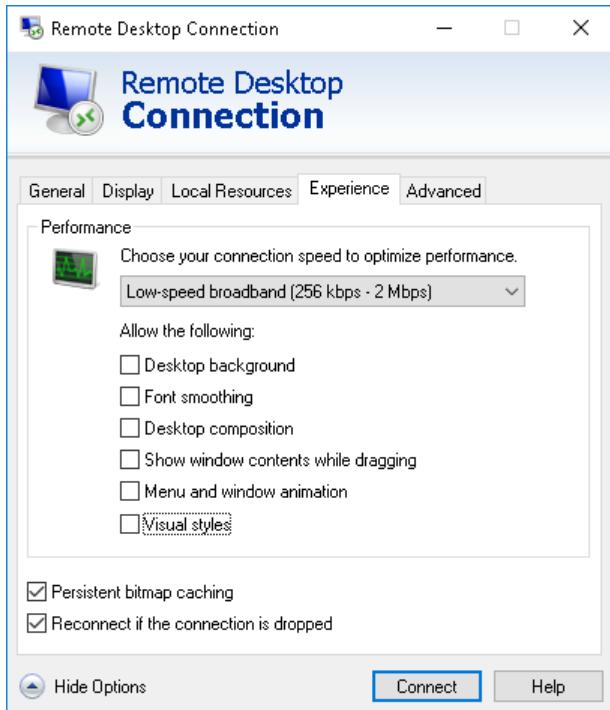
By default, when Veeam Backup & Replication launches the Remote Desktop Connection client, the client uses settings defined for the user account under which you are currently logged on to Microsoft Windows. In case high latency and low bandwidth impacts responsiveness of the Remote Desktop Connection client, you can adjust connection settings in one of the following ways:

- You can change the Remote Desktop Connection client settings and save them to a configuration file of the user account that is currently logged on to Microsoft Windows. By default, connection settings for each user are stored in a hidden file with the name `Default.rdp` that resides in the user's Documents folder, for example, `C:\Users\Administrator\Documents`.

- You can define custom Remote Desktop Connection client settings and save them to a configuration file with the name `VmbpRdpConnection.rdp` in the following product folder: `C:\Program Files\Veeam\Backup and Replication\Console`. In this case, Veeam Backup & Replication will use the necessary settings for the Remote Desktop Connection client regardless of the user account under which the OS is currently running.

To define custom remote desktop connection settings for Veeam Backup & Replication:

1. Open the Remote Desktop Connection client (`mstsc.exe`).

2. In the **Remote Desktop Connection** window, click **Show Options**.

3. Specify connection settings in accordance with quality of the network connection between the machine on which you open a remote desktop session and the tenant backup server. For slow connections, it is recommended that you define the following remote desktop settings:

   a. At the **Display** tab, in the **Colors** section, select the **High Color (16 bit)** option. Using this option might significantly improve performance of the remote desktop client over low bandwidth or high latency connections.

   b. At the **Display** tab, in the **Display configuration** section, reduce the size of the remote desktop.

   c. At the **Experience** tab, clear all check boxes in the **Allow the following** section.

d. At the **Local Resources** tab, in the **Remote audio** section, click **Settings** and disable remote audio playback and recording.

4. At the **General** tab, click **Save as** and save the specified settings to the configuration file:

   a. In the **Save As** window, browse to the `C:\Program Files\Veeam\Backup and Replication\Console` folder.

   b. In the **File name** field, enter the name for the configuration file: `VmbpRdpConnection.rdp`.

   c. Click **Save**.

TIP

You can define a custom name for the remote desktop connection configuration file used by Veeam Backup & Replication. To specify a name for the file, create the registry key `HKEY_LOCAL_MACHINE\SOFTWARE\Veeam\Veeam Backup and Replication\VMBPShellRdpTemplateFilename (REG_SZ)` and enter the name for the file as the key value (for example, `VeeamRdpConnection`).

Note that you can change only the name for the configuration file, but not the full path to this file. The file must reside in the `C:\Program Files\Veeam\Backup and Replication\Console` folder.

Managing SP Backup Server

Veeam Backup & Replication allows the SP to inform tenants about currently running maintenance of the SP backup infrastructure. As part of the maintenance scenario, the SP can perform the following operations on the SP backup server:

- Switch the SP backup server to the Maintenance mode.

- Create a custom Maintenance mode notification.
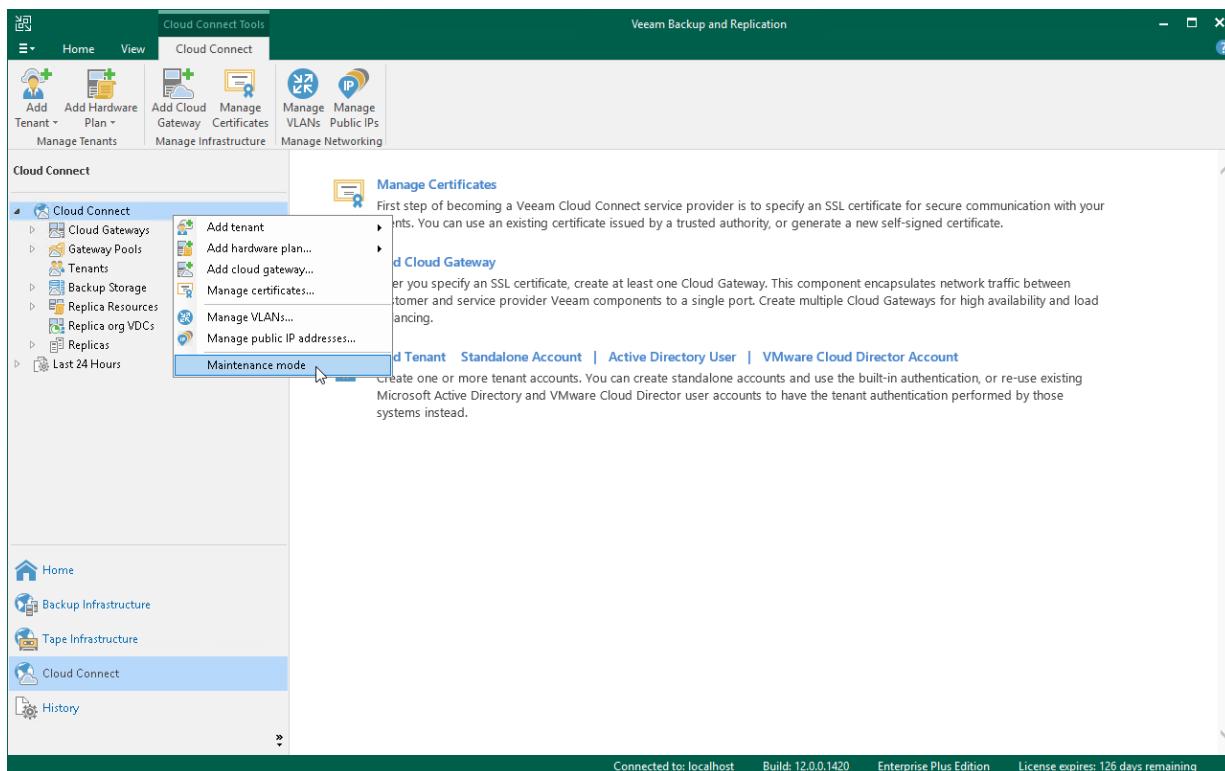
Switching to Maintenance Mode

The SP can switch the SP backup server to the Maintenance mode. When the SP backup server operates In the Maintenance mode, Veeam Backup & Replication notifies tenants who perform backup and/or backup copy jobs that the SP backup server is under maintenance and cloud resources are temporary unavailable.
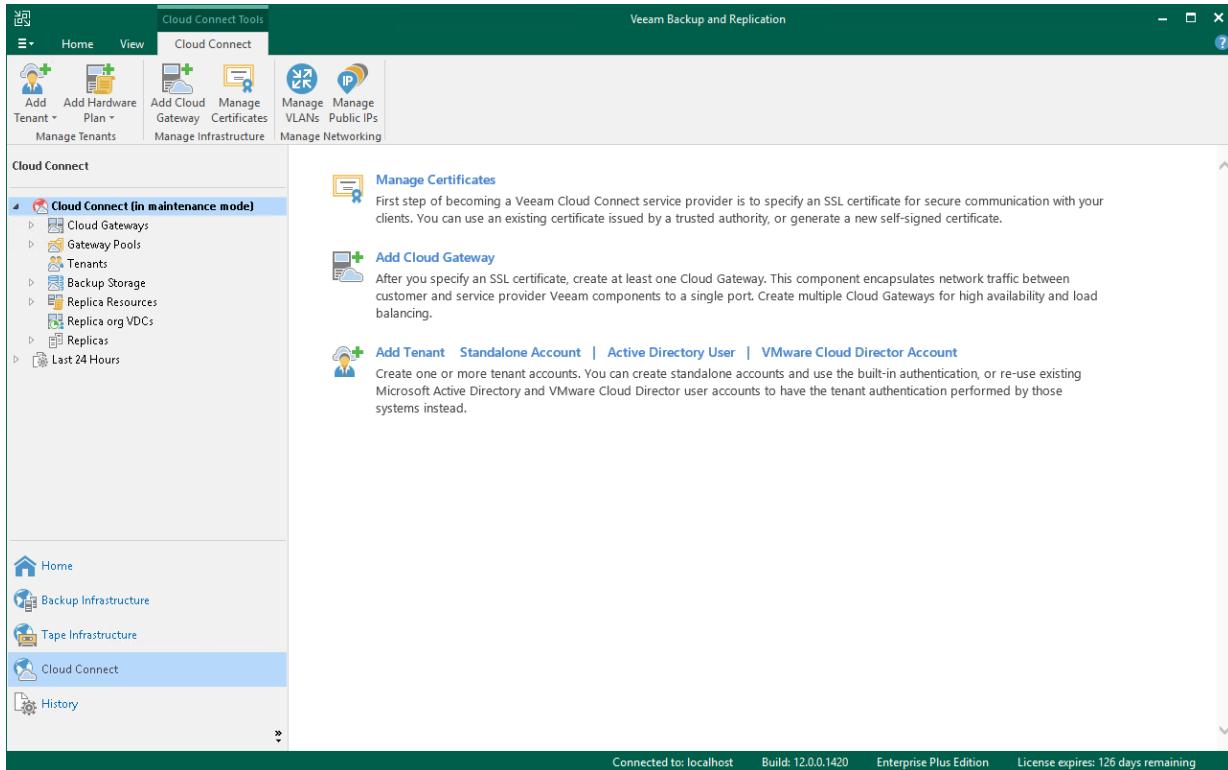
To switch the SP backup server to the Maintenance mode:

1. Open the **Cloud Connect** view.

2. In the inventory pane, right-click the **Cloud Connect** node and select **Maintenance mode**.

3. In the displayed window, click **Yes**.

To bring the SP backup server back to the normal operational mode, right-click the **Cloud Connect** node and select **Maintenance mode** once again.

When the SP backup server is put to the Maintenance mode, Veeam Backup & Replication changes the status of the backup server and displays the Maintenance mode icon in the **Cloud Connect** view of the backup console.

Creating Custom Maintenance Mode Notification

If a tenant backup or backup copy job is performing at the time when the SP backup server is operating in the Maintenance mode, the Maintenance mode notification is displayed in the job statistics window. By default, Veeam Backup & Replication is set up to display the following Maintenance mode notification: *Service provider is currently undergoing scheduled maintenance*. The SP can use the default notification or create a custom message, if necessary. The created notification will be displayed to all tenants who use cloud resources of the SP instead of the default one.

To create a custom Maintenance mode notification:

1. On the SP Veeam backup server, launch the Registry Editor.

2. Navigate to the key: `HKEY_LOCAL_MACHINE\SOFTWARE\Veeam\Veeam Backup and Replication\`.

3. Create a new String Value with the name `CloudMaintenanceModeMessage`, and set its data to the Maintenance mode notification that you want to display on the tenant side.

> **NOTE**
>
> Consider the following:
>
> - Veeam Backup & Replication uses the UTF-8 encoding for the Maintenance mode notification. This lets you include characters of a large number of languages in your custom Maintenance mode message.
> - Veeam Backup & Replication has no limitations on the maximum length of a custom Maintenance mode notification. However, it is recommended to create messages that contain 300 to 350 symbols or less. Longer notifications may be displayed incorrectly in the Veeam Backup & Replication or Veeam Agent for Microsoft Windows user interface.

Working with Tapes

The SP can write backups created by a tenant in a cloud repository to a tape media. Within the tenant backup to tape scenario, the SP can perform the following operations on the SP Veeam backup server:

- Create tenant backup to tape jobs.

- Restore tenant data from tape.

Creating Tenant Backup to Tape Job

To back up tenant data to tape, you must configure a backup to tape job. One job can be used to process data of one tenant or several tenants. You can select the following objects as a source for a backup to tape job intended to process tenant data:

- All tenants

- One or more specific tenants

- One or more cloud repositories of the same tenant or different tenants
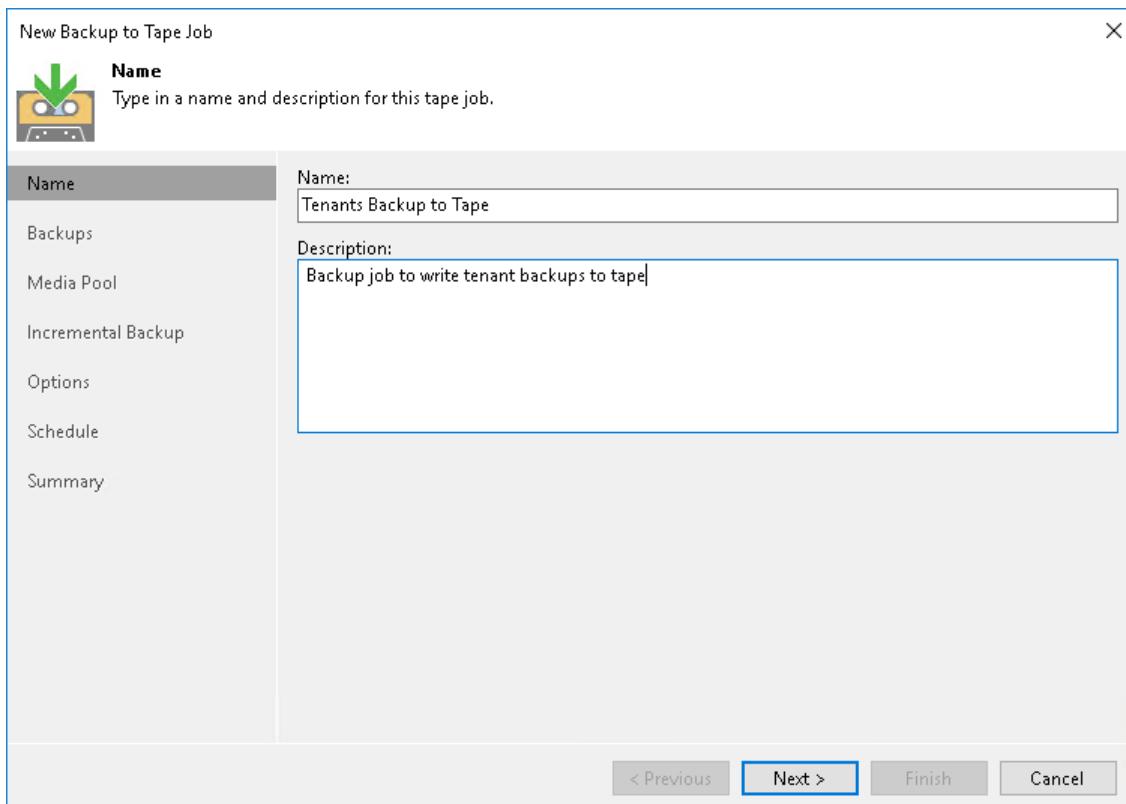
> **NOTE**
>
> This section describes only basic steps that you must take to create a backup to tape job intended to back up tenant data. To get a detailed description of all backup to tape job settings, see the Creating Backup to Tape Jobs section in the Veeam Backup & Replication User Guide.

Before you configure a backup to tape job, complete the following prerequisites:
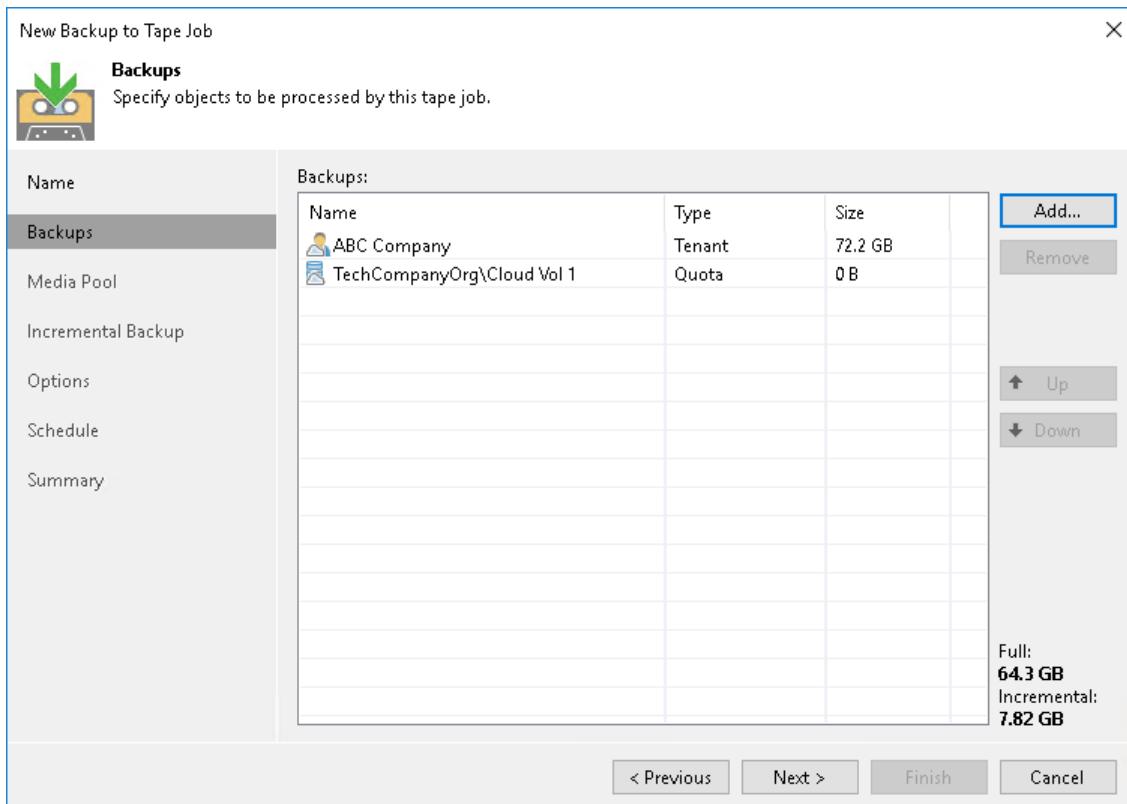
1. You must add a tape server in Veeam Backup & Replication on the SP backup server.

2. You must configure one or more GFS media pools with the necessary media set and retention settings. You can configure media pools in advance, before you launch the **Backup to Tape Job** wizard. You can also configure media pools at the **Media Pool** step of the wizard.

To create a backup to tape job:

1. On the **Home** tab, click **Tape Job** and select **Backups**.

2. At the **Name** step of the wizard, specify a name and description for the backup to tape job.
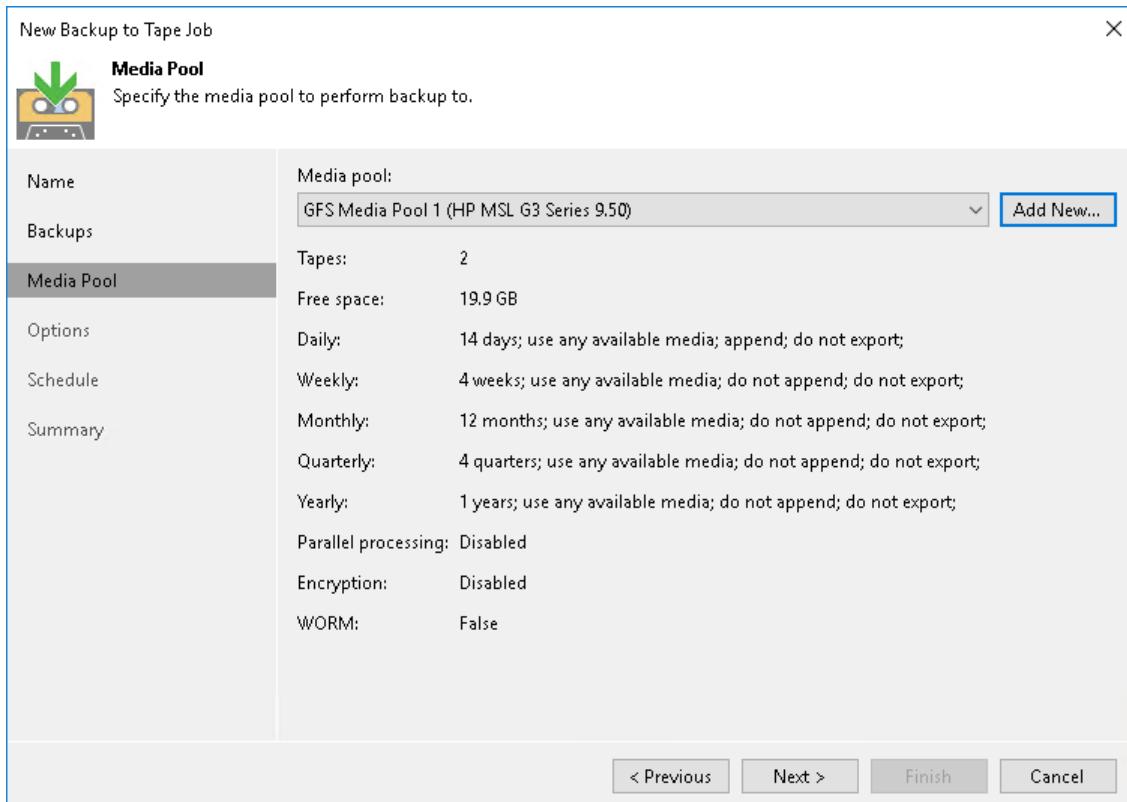
3. At the **Backups** step of the wizard, click **Add** > **Tenants** and select tenants or cloud repositories whose data you want to write to tape.

4. At the **Media Pool** step of the wizard, choose a media pool for tenant backups. You can select only GFS media pools.
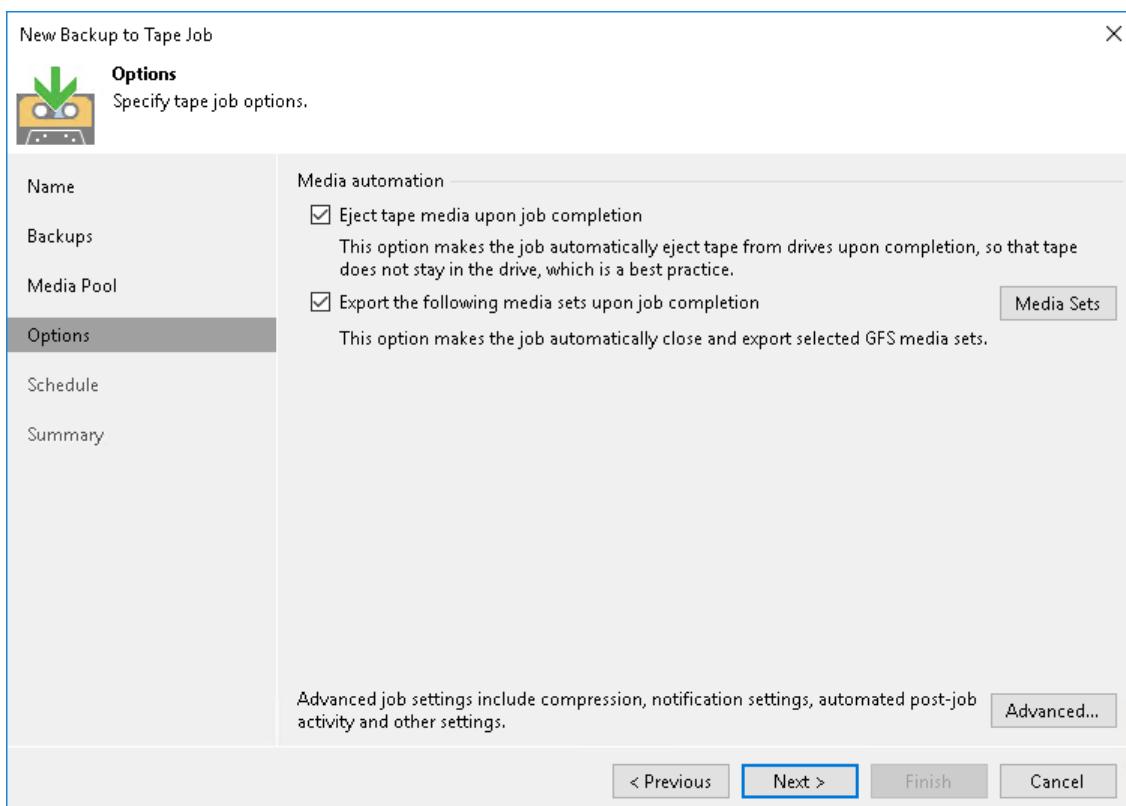
> **TIP**
>
> If you have not previously created a media pool with the required settings, you can click **Add New** and create a new GFS media pool without closing the job wizard. For more details, see Creating GFS Media Pools.

5. At the **Options** step of the wizard, specify archiving and media automation options.

   a. Select the **Eject media upon job completion** check box if the tape should be automatically ejected from the tape drive after the job successfully finishes. The ejected tapes are placed into a free tape device slot. Note that if the job started and failed, the tape will remain in the drive.
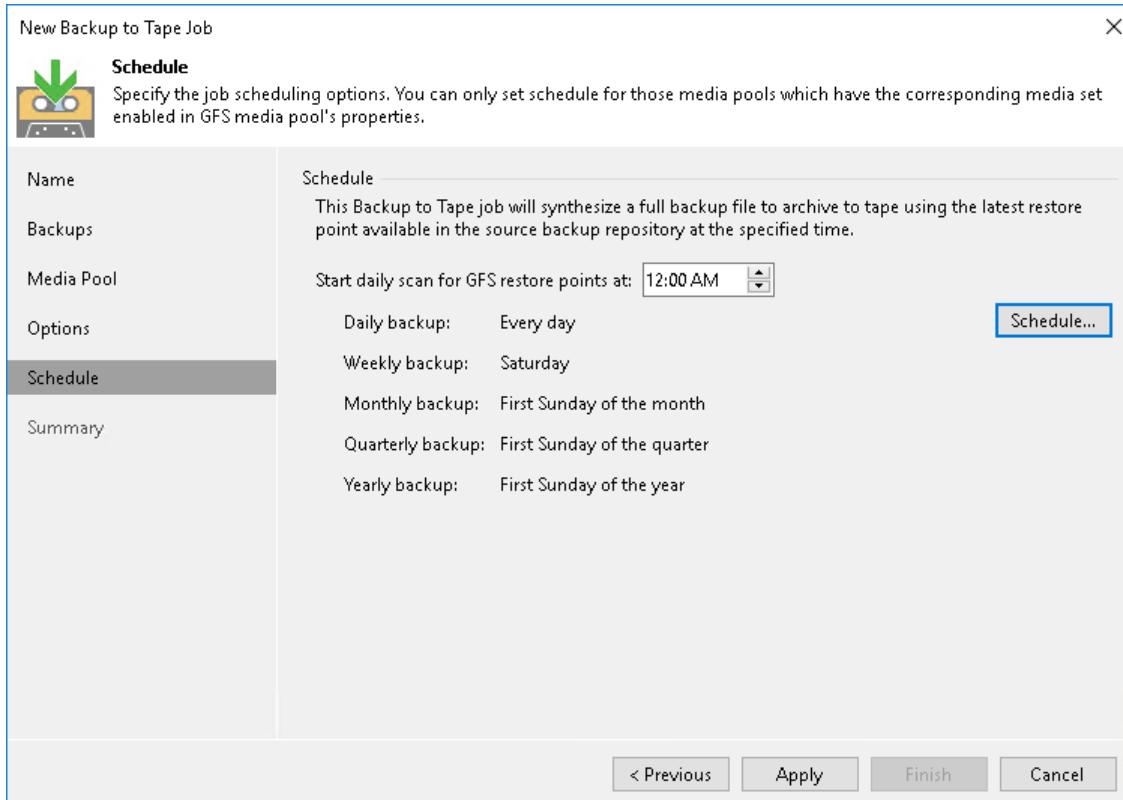
   This option does not prevent the tape job from appending data to this tape. If not configured otherwise in media pool settings, this tape will be placed into a drive on the next tape job run.

   b. Select the **Export the following media sets upon job completion** check box if you want to pull out the tapes with daily, weekly, monthly, quarterly or yearly media sets from the tape device, for example, to move to a storage location. The tape device will eject the tapes that belong to the selected media set.

   Click **Media Sets** and select the media sets that you want to export.
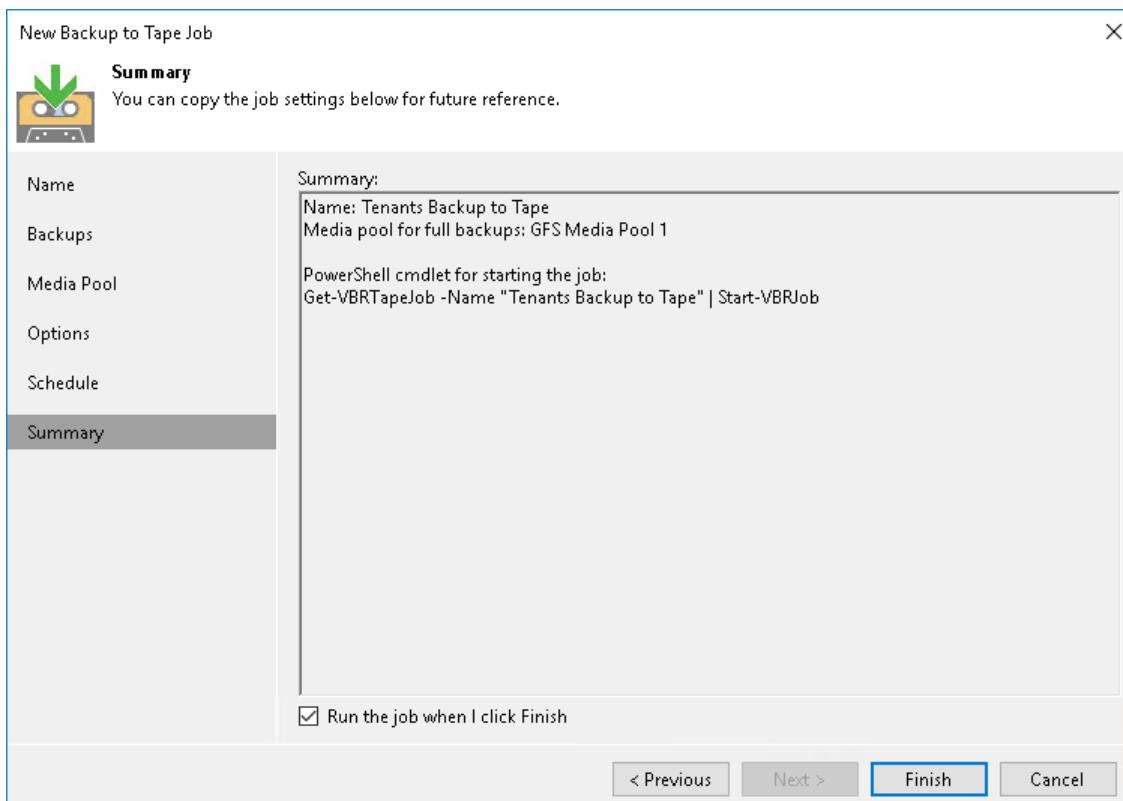
6. Click **Advanced** and specify the necessary settings for the tape job.

7. At the **Schedule** step of the wizard, click **Schedule** and select days for each media set. In the **Start daily scan for GFS restore points at** field, specify the time when the job must start. By default, the GFS job starts at 12:00 AM on the selected day.

8. At the **Summary** step of the wizard, select the **Run the job when I click Finish** check box if you want to start archiving tenant backups to tape right after you complete working with the wizard.

9. Click **Finish**.
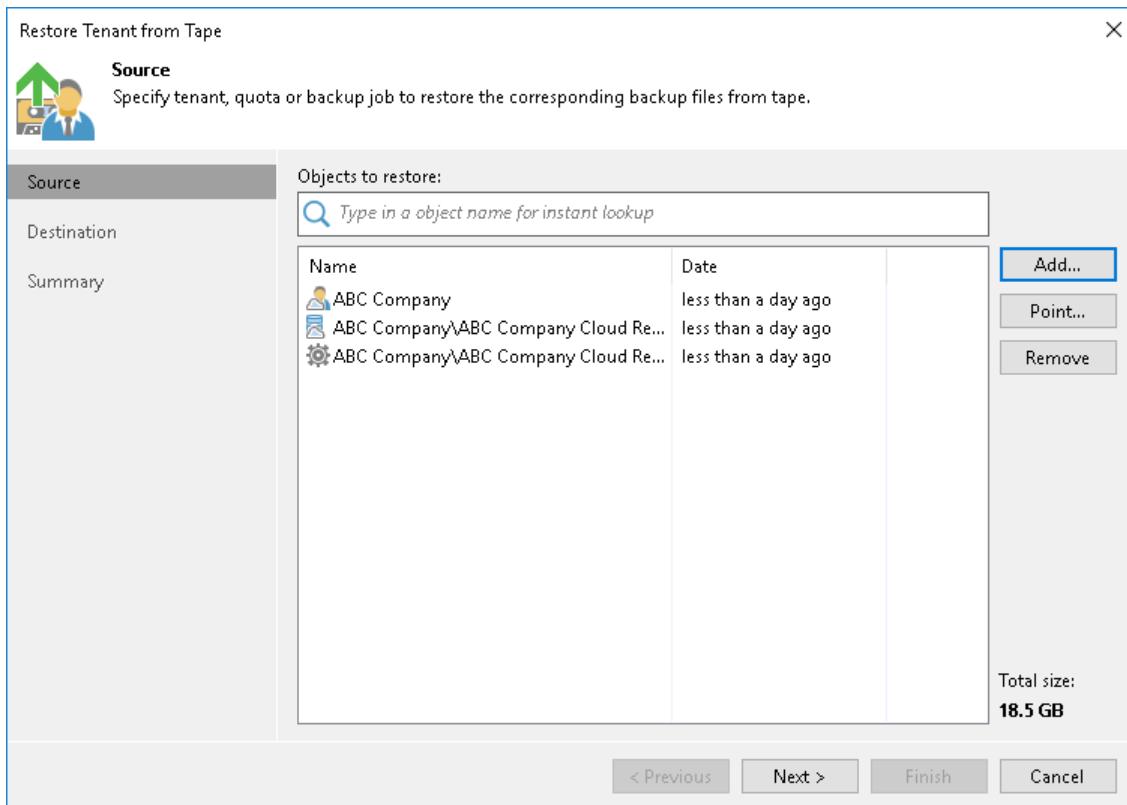
Restoring Tenant Data from Tape

The SP can restore tenant data from tape. The SP can simultaneously restore data of one tenant or multiple tenants, both to the original location or to a new location. Tenant backups can be recovered to the latest state or a specific day.
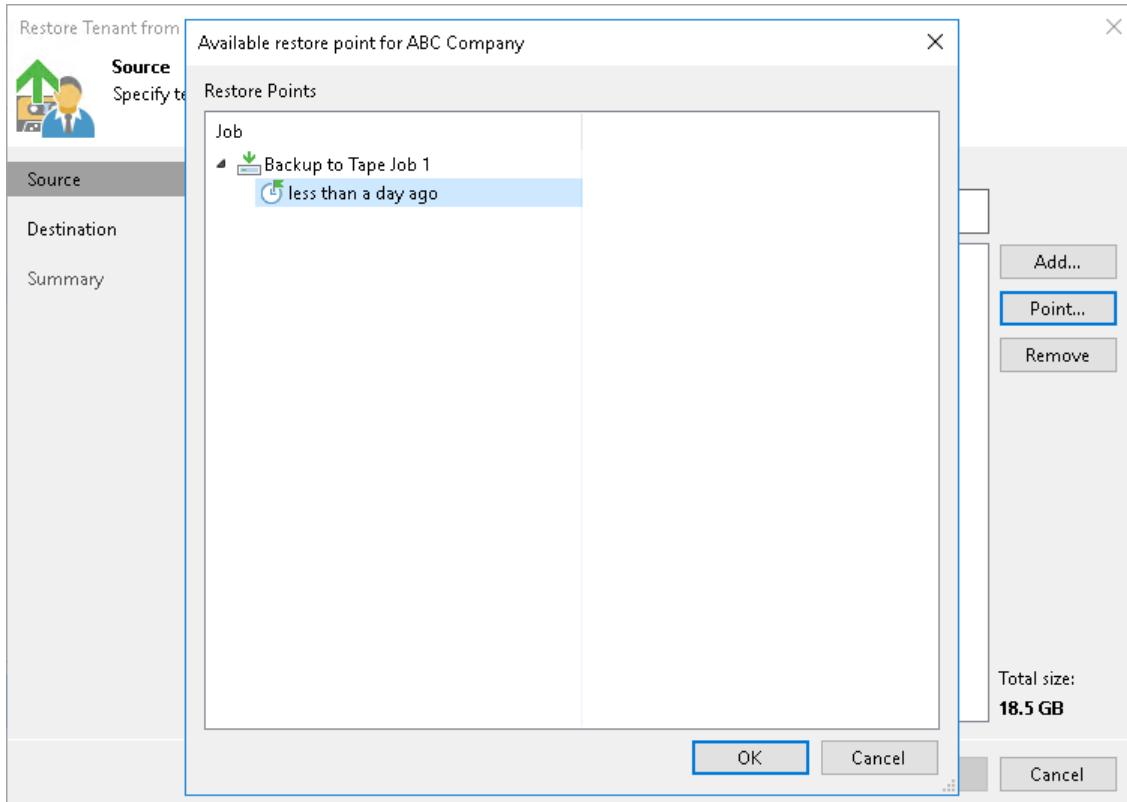
To restore tenant data from tape:

1. Open the **Home** view.

2. Select the **Backups > Tape** node in the inventory pane. Expand the backup to tape job in the working area, right-click the necessary tenant and select **Restore backup from tape to repository**.

3. At the **Source** step of the wizard, select one or more tenants whose data you want to restore.

   To add one or more tenants to the list, click **Add** and select more tenants. For data restore, you can select the tenant itself, specific cloud repository or backup job.

4. By default, Veeam Backup & Replication restores tenant data from the latest restore point. If you want to restore to an earlier state, select the tenant in the list and click **Point**. In the **Restore Points** section, select a restore point from which you want to restore tenant data.

5. At the **Destination** step of the wizard, select where tenant data should be restored:

   o **Restore to the original location**. If you select this option, Veeam Backup & Replication will restore tenant backups to the original cloud repository. The existing backups will be overwritten.

   During the restore process, the tenant account will be disabled. After the restore process is completed, Veeam Backup & Replication will rescan the SP, display restored backups in the tenant backup console and map tenant backup jobs to the restored backup chains.

   > **TIP**
   >
   > Veeam Backup & Replication automatically rescans the SP once in 15 minutes. The tenant can also perform this operation manually in the Veeam backup console.
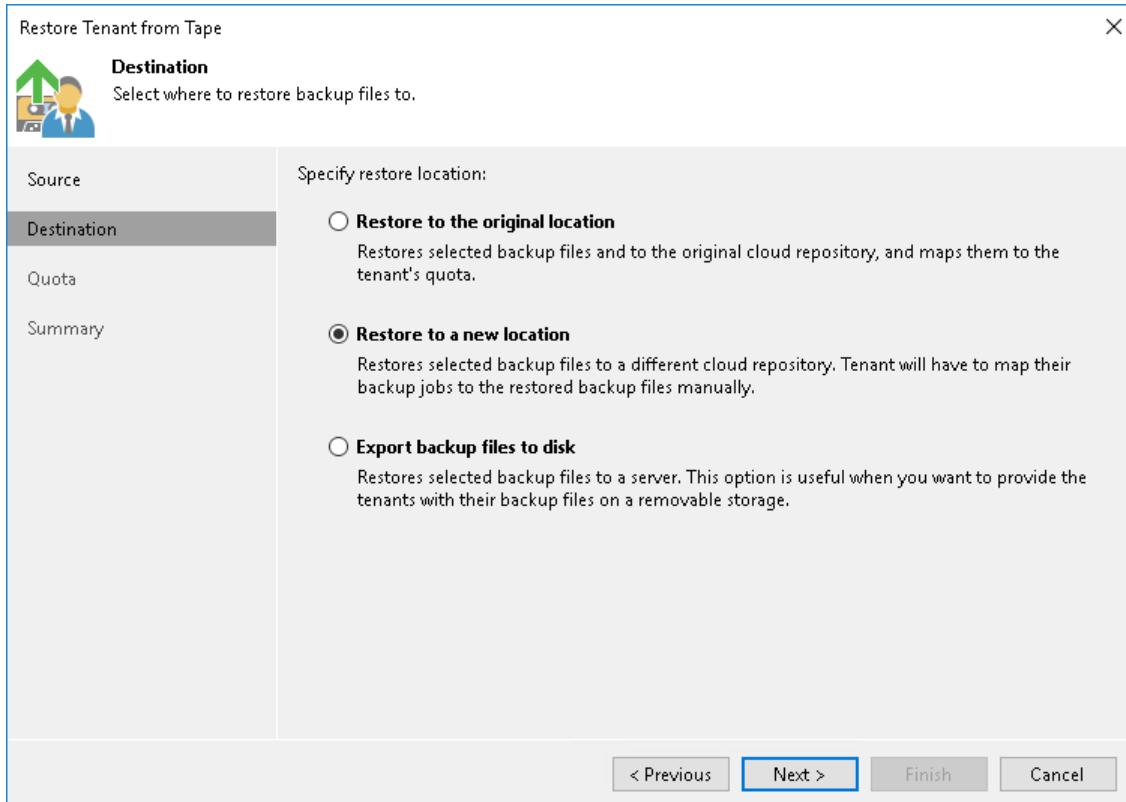
   o **Restore to a new location**. If you select this option, Veeam Backup & Replication will restore tenant backups to another cloud repository. Use this option if you do not want to overwrite tenant backups in the original cloud repository.

   After the restore process is completed, Veeam Backup & Replication will rescan the SP and display restored backups in the tenant backup console.

   o **Export backup files to disk**. If you select this option, Veeam Backup & Replication will export tenant backups to a specified folder on a server in the SP Veeam backup infrastructure.
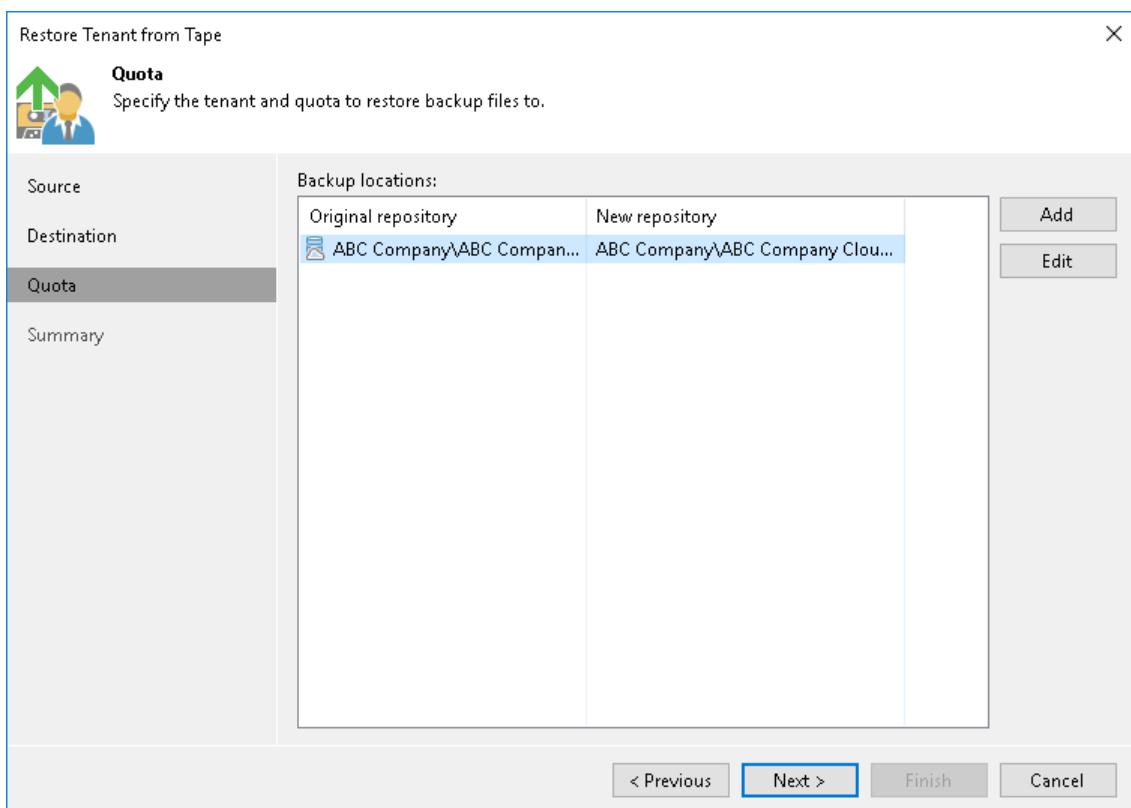
   During this process, Veeam Backup & Replication will save full backup files (VBK) and incremental backup files (VIB) to the specified location. Backup metadata files (VBM) will not be restored from tape.

After the export process is completed, the SP can perform operations with the backup files upon request from a tenant. The tenant cannot access this backup files from the tenant Veeam backup console.
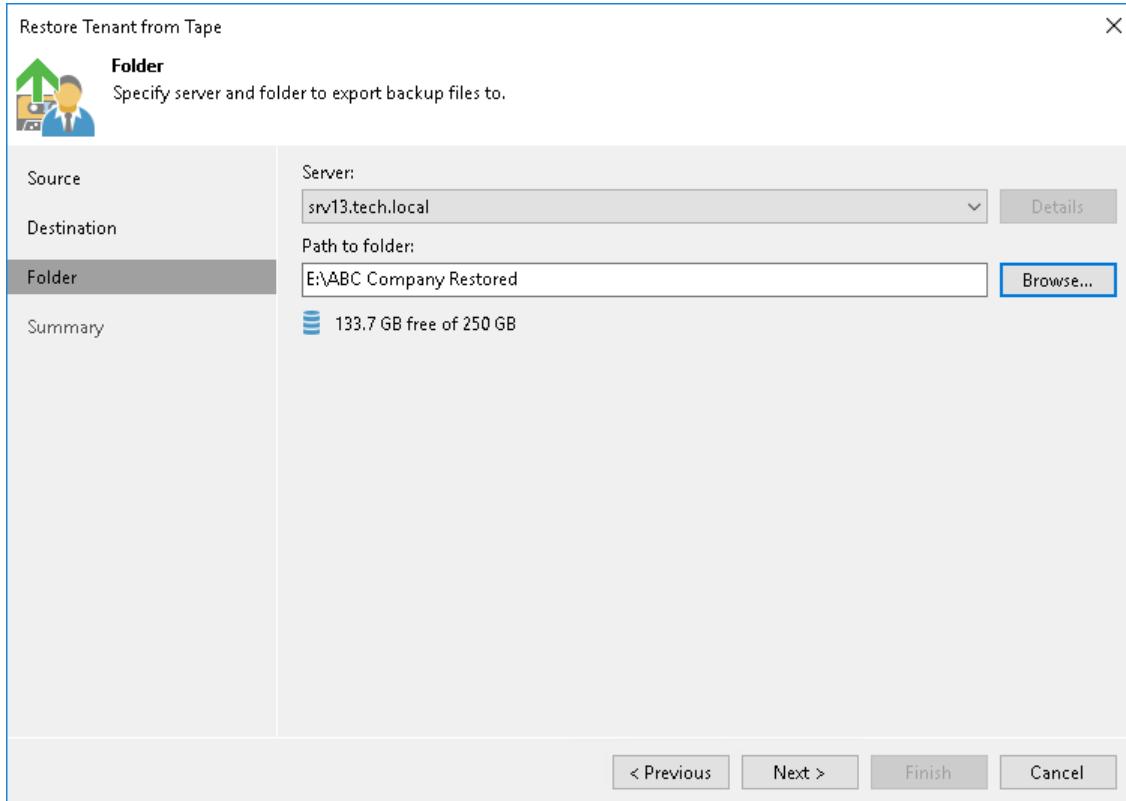
6. If you chose to restore tenant data to a new cloud repository, at the **Quota** step of the wizard, specify the tenant and cloud repository that you want to use as a new location for the restored data:

   a. To create a new tenant and cloud repository without closing the restore wizard, click **Add** and follow the steps of the **New Tenant** wizard. To learn more, see Registering Tenant Accounts.

   b. To specify a new cloud repository where tenant data will be restored, click **Edit** and select the necessary tenant and cloud repository.

   c. If the original cloud repository and a new cloud repository are the same, Veeam Backup & Replication will prompt you to choose whether you want to overwrite tenant data in the original cloud repository.

   - To overwrite original tenant data with data from the backup on tape, in the prompt window, click **Overwrite**.

   - To save tenant data restored from tape next to original tenant data, in the prompt window, click **Keep**.
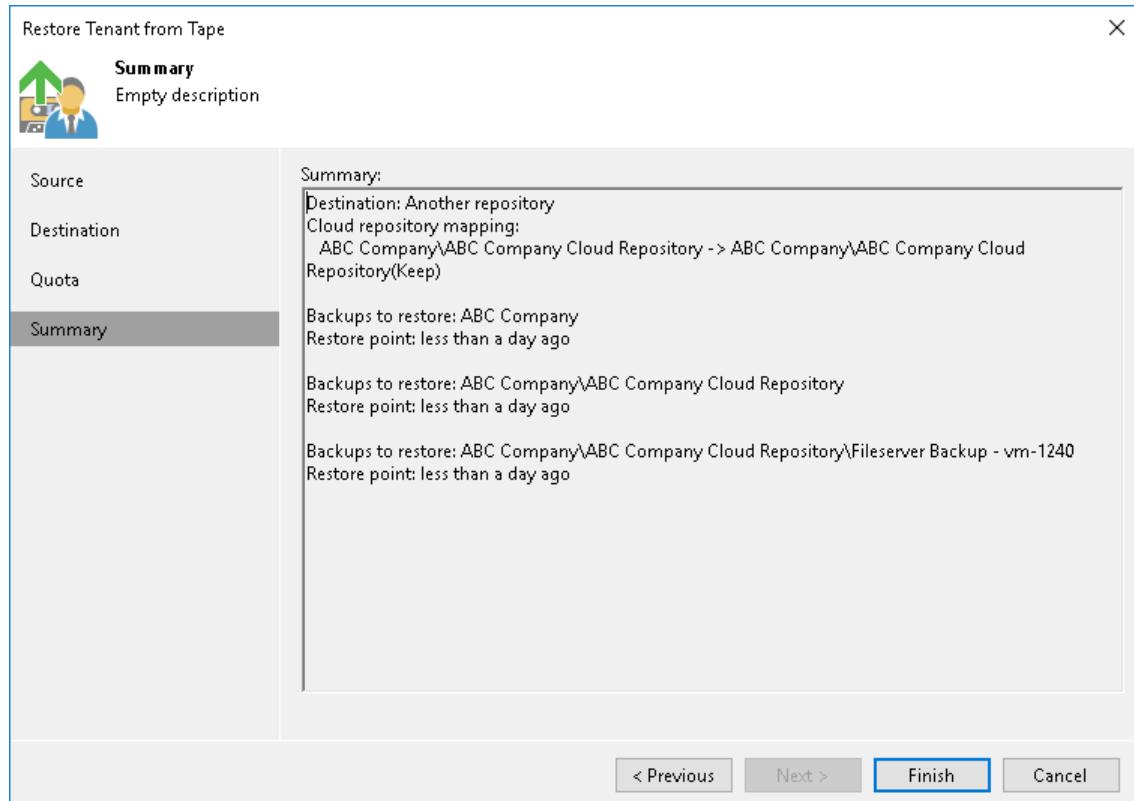
7. If you chose to restore tenant data to a folder, at the **Folder** step of the wizard, specify the server and the folder where you want to restore tenant backup files.

    a. In the **Server** field, select the server from the list of servers added to the Veeam backup infrastructure.

    b. In the **Path to folder** field, specify the folder where you want to place the restored backups.

8. At the **Summary** step of the wizard, review the restore settings.

Restore Tenant from Tape

Summary
Empty description

Source

Destination

Quota

Summary

Summary:

Destination: Another repository
Cloud repository mapping:
  ABC Company\ABC Company Cloud Repository -> ABC Company\ABC Company Cloud
Repository(Keep)

Backups to restore: ABC Company
Restore point: less than a day ago

Backups to restore: ABC Company\ABC Company Cloud Repository
Restore point: less than a day ago

Backups to restore: ABC Company\ABC Company Cloud Repository\Fileserver Backup - vm-1240
Restore point: less than a day ago

< Previous   Next >   Finish   Cancel

9. Click **Finish**.

Reporting

The SP can monitor status of the Veeam Cloud Connect infrastructure and performance of tenant jobs targeted at cloud resources of the SP:

- To track the Veeam Cloud connect infrastructure status, the SP can view the Veeam Cloud Connect report. The SP can use the Veeam Backup & Replication console to generate the ad-hoc report at any time the SP needs. The SP can also set up Veeam Backup & Replication to send the Veeam Cloud Connect report daily by email. To learn more, see Viewing Veeam Cloud Connect Report.

- To track performance of tenant jobs, the SP can view detailed statistics in the job session window. To learn more, see Viewing Tenant Job Statistics.

Viewing Veeam Cloud Connect Report

To track status of the Veeam Cloud Connect infrastructure, the SP can use the Veeam Cloud Connect report. The report provides information about status of the Veeam Cloud Connect infrastructure and activity of tenants who consume cloud resources of the SP. The report helps the SP ensure that there are enough resources in the Veeam Cloud Connect infrastructure to guarantee the flawless performance of tenant jobs.

Information in the Veeam Cloud Connect report reflects the status of the Veeam Cloud Connect infrastructure at the point in time when the report is generated. The SP can generate the report in one of the following ways:

* The SP can use the Veeam Backup & Replication console to generate the ad-hoc report at any time the SP needs. The report will open in the web browser. The generated report can contain information about activity of all tenants who use cloud resources of the SP or a specific tenant. To learn more, see Generating Report.

* The SP can enable automatic report delivery by email. In this case, Veeam Backup & Replication will automatically generate and send the report daily to the SP. The report will contain information about activity of all tenants who use cloud resources of the SP. To learn more, see Enabling Email Reporting.

The report provides the following information:

* The **Infrastructure status** section shows a message describing the overall status of the Veeam Cloud Connect infrastructure:

    o *OK.*

    o *Reaching capacity. Please do not add new tenants into this Veeam Cloud Connect infrastructure.* — Veeam Backup & Replication displays this message if the Veeam Cloud Connect Service requires longer time to respond to requests from the tenant backup server, that is:

        ▪ [For ad-hoc report] If the time interval between an incoming request from the tenant backup server and a response to this request from the Veeam Cloud Connect Service reached the maximum of 5 to 10 minutes at least once within the 24-hour period. Veeam Backup & Replication starts the first 24-hour period with the start of the Veeam Cloud Connect Service on the SP backup server. The moment when the ad-hoc report is generated does not start the new 24-hour period.

        ▪ [For daily report] If the time interval between an incoming request from the tenant backup server and a response to this request from the Veeam Cloud Connect Service reached the maximum of 5 to 10 minutes at least once within the 24-hour period since the previous daily report.

    o *Out of capacity. Please migrate some of the existing tenants into a different Veeam Cloud Connect infrastructure.* — Veeam Backup & Replication displays this message if the Veeam Cloud Connect Service requires very long time to respond to requests from the tenant backup server, that is:

        ▪ [For ad-hoc report] If the time interval between an incoming request from the tenant backup server and a response to this request from the Veeam Cloud Connect Service reached the maximum of 10 minutes or more at least once within the 24-hour period. Veeam Backup & Replication starts the first 24-hour period with the start of the Veeam Cloud Connect Service on the SP backup server. The moment when the ad-hoc report is generated does not start the new 24-hour period.

        ▪ [For daily report] If the time interval between an incoming request from the tenant backup server and a response to this request from the Veeam Cloud Connect Service reached the maximum of 10 minutes or more at least once within the 24-hour period since the previous daily report.

- The **Backup** section shows information about consumption of cloud repository resources by tenant(s): the user name of the tenant account, the number of VMs in backups stored on the cloud repository, the name of the cloud repository and the name of the backup repository whose resources the SP exposes as a cloud repository, storage quota assigned to the tenant, the amount of used and free space on the cloud repository, the last time when the tenant was active and the date when the tenant account expires.

- The **Replication** section shows information about consumption of cloud host resources by tenant(s): the user name of the tenant account, the number of VMs replicated to the cloud host, hardware plan, amount of provisioned CPU, memory and storage resources, the last time when the tenant was active and the date when the tenant account expires.

- The **Agent** section shows information about consumption of cloud repository resources by Veeam Agent backups created by tenant(s): the user name of the tenant account, the number of workstations and servers whose backups are stored on the cloud repository, the name of the cloud repository and the name of the backup repository whose resources the SP exposes as a cloud repository, storage quota assigned to the tenant, the amount of used and free space on the cloud repository, the last time when the tenant was active and the date when the tenant account expires.

In the **Total** field of the *Backup*, *Replication* and *Agents* sections, Veeam Backup & Replication displays the total number of processed machines:

- For a report that includes information about all tenants who use cloud resources of the SP, the total number of backed-up VMs, replicated VMs, backed-up workstations and servers reflects the number of machines processed by all tenants (including rental machines).

- For a report that includes information about a specific tenant, the total number of backed-up VMs, replicated VMs, backed-up workstations and servers equals the number of machines processed by this tenant (including rental machines).

> **NOTE**
>
> The Veeam Cloud Connect report does not include machines for which no restore points were created during the last 30 days or more.

Infrastructure status:
OK

Backup

User	Number of VM	Repository Name	Repository	Total quota	Used space	Free space	Last active	Expiration date
ABC Company	2	ABC Company Cloud Repository	Default Backup Repository	100.00 GB	72.31 GB	27.69 GB	13 hours ago	never
TOTAL	**2**							

Replication

User	Number of VM	Hardware Plan	Memory	CPU	Storage	Last active	Expiration date
ABC Company	2	VMware Gold	10.00 GB (unlimited)	2 vCPUs (Unlimited)	35 %	4 minutes ago	never
Omega	0	Hyper-V Gold	0 %	0 vCPUs (10.08 GHz)	0 %	never	never
QWE Systems	0	Hyper-V Gold	0 %	0 vCPUs (10.08 GHz)	0 %	never	never
TechCompanyOrg	0	TechCompanyOrgVDC	0 %	0 vCPUs (6.49 GHz)	1 %	never	never
TOTAL	**2**						

Agent

User	Workstation	Server	Repository Name	Repository	Total quota	Used space	Free space	Last active	Expiration date
ABC Company	2	8	ABC Company Cloud Repository	Default Backup Repository	100.00 GB	72.31 GB	27.69 GB	13 hours ago	never
TOTAL	**2**	**8**							

Veeam Backup & Replication 12.0.0.1364

Generating Report

To view the Veeam Cloud Connect report that displays information about all tenants of the SP:

1. Open the **Cloud Connect** view.

2. In the inventory pane, click **Tenants** and click **Report** on the ribbon.

To view the Veeam Cloud Connect report that displays information about a specific tenant:

1. Open the **Cloud Connect** view.

2. In the inventory pane, click **Tenants**.

3. In the working area, select the tenant account and click **Report** on the ribbon.

Enabling Email Reporting

The SP can set up Veeam Backup & Replication to send the Veeam Cloud Connect report daily by email. To receive information about the Veeam Cloud Connect infrastructure status in email reports, the SP must enable and configure global email notification settings in Veeam Backup & Replication. To learn more, see the Configuring Global Email Notification Settings section in the Veeam Backup & Replication User Guide.

Once email notifications are configured, Veeam Backup & Replication will send the Veeam Cloud Connect report daily to an email address specified in the global email notification settings. By default, Veeam Backup & Replication sends the report at the time when global email notification settings were enabled. For example, if the SP enables email notifications at 12:00 AM, Veeam Backup & Replication will send the report daily at 12:00 AM.

Viewing Tenant Job Statistics

When a tenant runs a backup, backup copy or replication job targeted at a cloud repository or cloud host, Veeam Backup & Replication saves the jobs statistics and operation data to the configuration database on the SP backup server. In contrast to regular job statistics, for tenant jobs, Veeam Backup & Replication saves only such data that helps the SP monitor performance of the Veeam Cloud Connect infrastructure and determine possible performance bottlenecks. Sensitive information about tenant backup infrastructure, such as names of processed VMs, VM disks or backup infrastructure components, is not passed to the SP side.

The SP can view real-time statistics for currently performed tenant jobs and view results of job sessions performed within last 24 hours.

Veeam Agent Backup Job Statistics

In the SP backup console, the SP can view statistics for Veeam Backup & Replication jobs only: VM backup jobs, Veeam Agent backup jobs managed by the backup server, backup copy jobs and replication jobs.

For Veeam Agent backup jobs that run on Veeam Agent computers (configured in Veeam Agent operating in the standalone mode or defined in a backup policy), Veeam Backup & Replication does not display detailed statistics for security purposes. For such jobs, only basic information about a backup job session is available in the SP backup console. This information includes the job name, job session status, session start and end time, name of the tenant or subtenant account under which the job was started and the amount of sent and received data. Detailed statistics on the job session is available in the Veeam Agent control panel on the Veeam Agent computer.

Viewing Real-Time Statistics

The SP can view detailed statistics on VM backup, backup copy and replication job sessions performed by tenants within last 24 hours.

To view real-time statistics for a job, do one of the following:

- Open the **Cloud Connect** view, in the inventory pane select **Last 24 hours** or **Running**. In the working area, double-click the job.

- Open the **Cloud Connect** view, in the inventory pane select **Last 24 hours** or **Running**. In the working area, right-click the job and select **Statistics**.

- Open the **Cloud Connect** view, in the inventory pane select **Last 24 hours** or **Running**. In the working area, select the job and click **Statistics** on the ribbon.
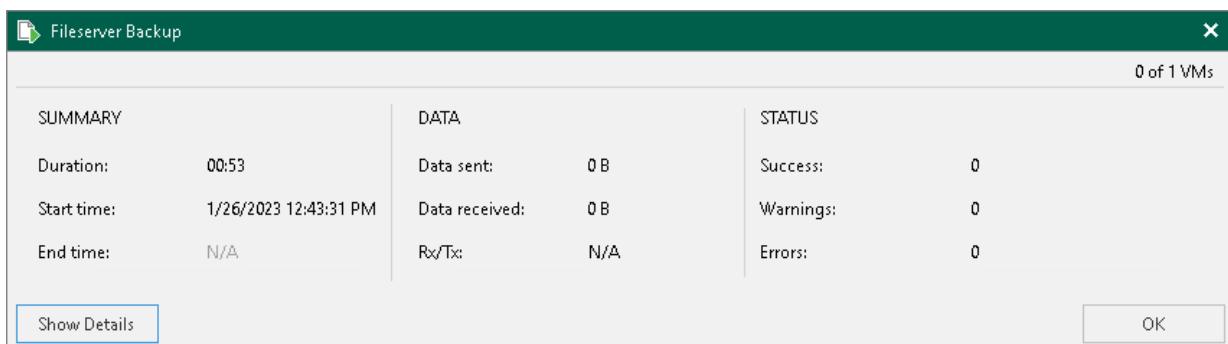
> **NOTE**
>
> The **Statistics** option is unavailable for Veeam Agent backup jobs. To learn more, see Veeam Agent Backup Job Statistics.

The real-time statistics provides detailed data on job sessions: duration, start and end time, amount of sent and received data and details of the session performance, for example, warnings and errors that have occurred in the process of operation.

In addition to overall job statistics, the real-time statistics provides information on each object processed with the job. To view the processing progress for a specific object, select it in the list on the left.

> **TIP**
>
> To collapse and expand the real-time statistics window, use **Hide Details** and **Show Details** buttons at the bottom left corner of the window.

Statistics Counters

Veeam Backup & Replication displays jobs statistics for the following counters:

- At the top of the window, Veeam Backup & Replication displays the number of VMs in the job and the number of processed VMs.

- The **Summary** box shows general information about the job:

  o **Duration** — time from the job start till the current moment or job end.

  o **Start time** — time of the job start.

  o **End time** — time of the job end.

- The **Data** box shows information about processed VM data:

  o **Data sent** — amount of data sent from the SP side to the tenant side.

  o **Data received** — amount of data transferred from the tenant side to the SP side.

  o **Rx/Tx** — data transfer speed (displayed for currently running jobs only).

- The **Status** box shows information about the job results. This box informs how many tasks have completed with the *Success*, *Warning* and *Error* statuses (1 task per 1 VM).

- The pane at the lower left corner shows a list of objects included in the job. For tenant jobs, Veeam Backup & Replication displays the list according to the following rules:

  o The tenant selected the **Allow this Veeam Backup & Replication installation to be managed by the service provider** check box at the **Service Provider** step of the **Service Provider** wizard when connecting to the SP. In this case, Veeam Backup & Replication displays in the list names of objects included in the job.

  o The tenant did not select the **Allow this Veeam Backup & Replication installation to be managed by the service provider** check box at the **Service Provider** step of the **Service Provider** wizard when connecting to the SP. In this case, Veeam Backup & Replication does not display names of objects included in the job. Instead, it displays identifiers for the objects that Veeam Backup & Replication saves in the configuration database.

- The pane at the lower right corner shows a list of operations performed during the job. To see a list of operations for a specific object included in the job, click the object in the pane on the left. To see a list of operations for the whole job, click anywhere on the blank area in the left pane.

Viewing Job Session Results

The SP can view detailed statistics on VM backup, backup copy and replication job sessions performed by tenants within last 24 hours.

To view statistics for a selected job session, do either of the following:

- Open the **Cloud Connect** view. In the inventory pane, select **Last 24 Hours**, **Success**, **Warning** or **Failed**. In the working area, double-click the necessary job session.

- Open the **Cloud Connect** view. In the inventory pane select **Last 24 Hours**, **Success**, **Warning** or **Failed**. In the working area, right-click the necessary job session and select **Statistics**.

- Open the **Cloud Connect** view, in the inventory pane select **Last 24 Hours**, **Success**, **Warning** or **Failed**. In the working area, select the job and click **Statistics** on the ribbon.

> **NOTE**
>
> The **Statistics** option is unavailable for Veeam Agent backup jobs. To learn more, see Veeam Agent Backup Job Statistics.

Guide for Tenants

The Veeam Cloud Connect User Guide is intended for tenants who want to store their data in the cloud repository or replicate their VMs to the cloud host configured with the help of the Veeam Cloud Connect functionality in Veeam Backup & Replication. The User Guide describes main steps that tenants must take to set up Veeam Cloud Connect infrastructure components and work with cloud repositories and cloud hosts exposed by SPs.

Setting Up Tenant Veeam Cloud Connect Infrastructure

To be able to use cloud repository and cloud replication resources, you must set up Veeam Cloud Connect infrastructure components on the tenant side.

As part of the configuration process, you must perform the following tasks:

1. Deploy the tenant Veeam backup server.

2. Connect source virtualization hosts.

3. Find a service provider.

4. Connect to a service provider.

5. [For Veeam Cloud Connect Replication] Specify default gateways.

6. [Optional] Configure source WAN accelerator.

Once you have performed these tasks, you can configure data protection jobs in Veeam Backup & Replication and target them at the cloud repository or cloud host.

Deploying Tenant Veeam Backup Server

To deploy the tenant Veeam backup server, you must install Veeam Backup & Replication on a Microsoft Windows server on your side.

The installation process of Veeam Backup & Replication in the Veeam Cloud Connect infrastructure is the same as the installation process in a regular Veeam backup infrastructure. To learn more about system requirements, required permissions and the installation process workflow, see the Deployment section in the Veeam Backup & Replication User Guide.

In addition to requirements listed in the product documentation, the tenant Veeam backup server must meet the following requirements:

- The tenant Veeam backup server must have any type of paid license installed. The Community edition of Veeam Backup & Replication does not support the Veeam Cloud Connect functionality. That is, you cannot create backup and replication jobs targeted at cloud resources of the SP; data recovery operations from the cloud are supported.

- The tenant Veeam backup server must have access to all components that will take part in data protection and disaster recovery tasks. These include a gateway server configured on the SP side, source virtualization hosts and source WAN accelerator (optional).

Connecting Source Virtualization Hosts

You must connect to the Veeam backup server virtualization hosts on which VMs that you plan to back up or replicate to the cloud are located.

Veeam Backup & Replication lets you connect the following types of hosts:

- VMware vCenter Server

- Standalone ESXi host

- VMware Cloud Director server

- SCVMM

- Microsoft Hyper-V cluster

- Standalone Microsoft Hyper-V host

If a host is managed by VMware vCenter Server, SCVMM or is a part of a cluster, it is recommended that you connect servers or clusters, not a standalone host. If you move VMs between hosts, you will not have to re-configure jobs existing in Veeam Backup & Replication. Veeam Backup & Replication will automatically locate migrated VMs and continue processing them as usual.

> **NOTE**
>
> Veeam Cloud Connect does not support the scenario in which the SP and tenant connect the same host to Veeam backup servers deployed on the SP and tenant sides. You should not use the same host as a source host and target host for cloud backup and replication tasks (for example, for evaluation purposes).

The host connection process in the Veeam Cloud Connect infrastructure is the same as the host connection process in a regular Veeam backup infrastructure. To learn more, see Adding VMware vSphere Servers and Adding Microsoft Hyper-V Servers sections in the Veeam Backup & Replication User Guide.

Finding Service Providers
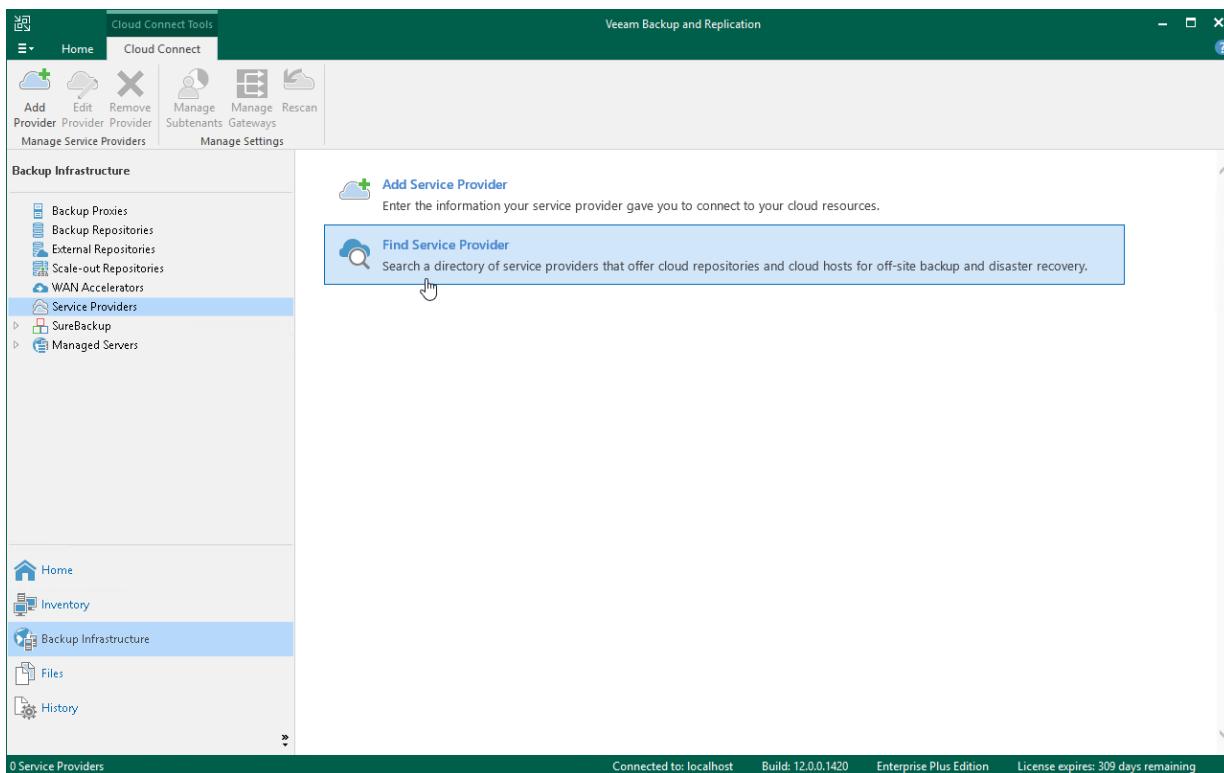
You can look for SPs who offer Backup as a Service and/or Disaster Recovery as a Service using Veeam Backup & Replication. The list of SPs is published on the Veeam website and constantly updated. You can select the necessary SP from the list and contact this SP to get the cloud repository service.

> **NOTE**
>
> This operation is unavailable if you have already added at least one SP in the Veeam backup console.

To find an SP:

1. Open the **Backup Infrastructure** view.

2. Select the **Service Providers** node in the inventory pane.

3. Click **Find Service Provider** in the working area. A page of the Veeam website will open in your web browser. Use the filter on the webpage to find the necessary SP by the type of provided cloud services, SP datacenter location or virtualization platform.

Connecting to Service Providers

The procedure of SP adding is performed by the tenant on tenant's Veeam backup server.

> **IMPORTANT**
>
> The SP cannot add itself as a SP in the Veeam Backup & Replication console deployed on the SP backup server.

To use Veeam Cloud Connect resources for data protection and disaster recovery tasks, you must add a SP to Veeam Backup & Replication. After you add a SP, Veeam Backup & Replication will retrieve information about backup and replication resources allocated to you, and cloud repositories and cloud hosts will become visible in your Veeam backup console. After that, you can start working with cloud resources.

Before You Begin
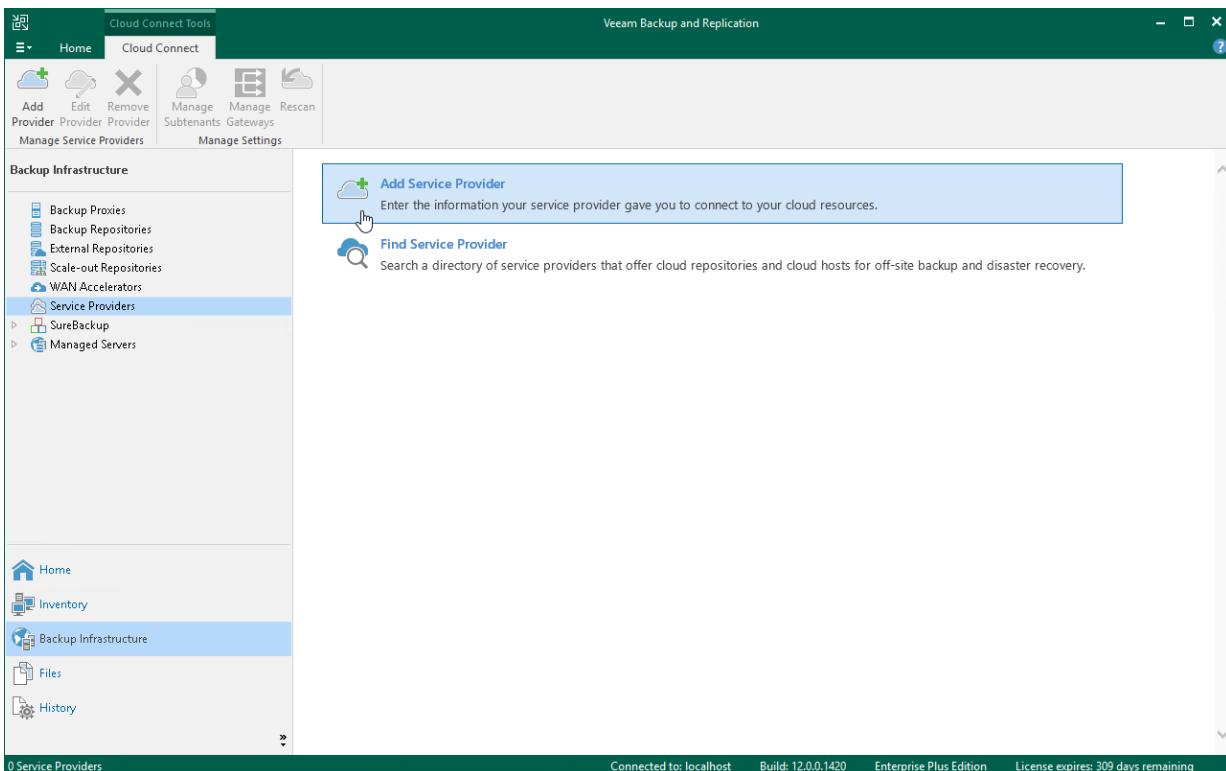
Before you add a SP, complete the following prerequisites:

1. Make sure that the SP has provided you with the following information:

   a. You have a user name and password for your tenant account registered at the SP Veeam backup server.

   b. You have a full DNS name or IP address of the cloud gateway over which you will communicate with the Veeam Cloud Connect infrastructure.

   c. You have a port over which to connect to the cloud gateway (if the SP specified a non-default port).

   d. [Optional] You have a TLS certificate thumbprint that you can use for TLS certificates verification.

2. [For standalone tenant accounts] It is recommended that you change the password for the root account of the tenant-side network extension appliance before connecting to the SP. You can change the password in the service credentials record using the Credentials Manager. This operation is performed in the similar way as on the SP side. To learn more, see Managing Tenant Network Extension Appliance Credentials.

Step 1. Launch Service Provider Wizard

To launch the **Service Provider** wizard, do one of the following:

- Open the **Backup Infrastructure** view. Select the **Service Providers** node in the inventory pane and click **Add Provider** on the ribbon.

- Open the **Backup Infrastructure** view. Right-click the **Service Providers** node in the inventory pane and select **Add service provider**.

- Open the **Backup Infrastructure** view. Select the **Service Providers** node in the inventory pane and click **Add Service Provider** in the working area.

Step 2. Specify Cloud Gateway Settings

At the **Service Provider** step of the wizard, specify settings for the cloud gateway that the SP has provided to you.

1. In the **DNS name or IP address** field, enter a full DNS name or IP address of the cloud gateway.

2. In the **Port** field, specify the port over which the tenant Veeam backup server will communicate with the cloud gateway. By default, port 6180 is used.

3. In the **Description** field, provide a description for the SP you are adding.

4. Select the **Allow this Veeam Backup & Replication installation to be managed by the service provider** check box if the SP should manage the tenant Veeam backup server under the Backup as a Service agreement.

   If you select this option, Veeam Backup & Replication will install the remote management agent on the tenant Veeam backup server. The SP will be able to manage this backup server with Veeam Service Provider Console.

   If you select this option, Veeam Backup & Replication on the SP side will also display names of objects included in tenant backup jobs instead of replacing object names with identifiers. To learn more, see Viewing Real-Time Statistics.

> **IMPORTANT**
>
> If the SP has several cloud gateways, you must specify settings of only one gateway to connect to the SP. Veeam Backup & Replication will automatically retrieve information about all other cloud gateways and will use them for transferring data to/from the cloud repository and/or cloud host.

Step 3. Verify TLS Certificate and Specify User Account Settings

At the **Credentials** step of the wizard, verify TLS certificate settings and specify settings for the tenant account that you want to use to connect to the cloud repository.
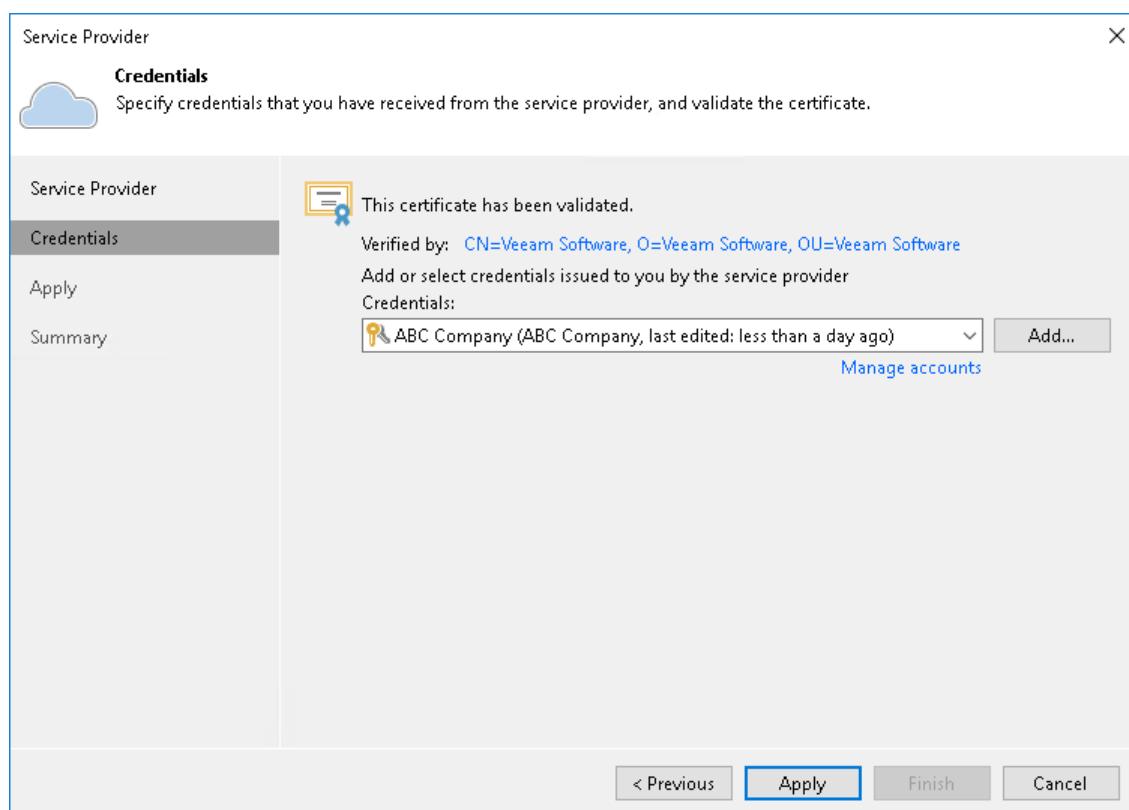
1. At the top of the wizard window, Veeam Backup & Replication displays information about the TLS certificate obtained from the SP side. You can view the certificate settings and verify the TLS certificate.

   TLS certificate verification is optional. You can use this option to verify self-signed TLS certificates. TLS certificates signed by the CA do not require additional verification.

   o To view the TLS certificate, click the certificate link.

   o To verify if the TLS certificate with a thumbprint, copy the thumbprint you obtained from the SP to the Clipboard and enter it to the **Fingerprint for certificate verification** field. Click **Verify**. Veeam Backup & Replication will check if the thumbprint you enter matches the thumbprint of the obtained TLS certificate.

2. From the **Credentials** list, select credentials for the tenant account that the SP has provided to you. If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right to add necessary credentials.

> **NOTE**
>
> If the SP allocated to you replication resources in VMware Cloud Director, you must provide credentials for the VMware Cloud Director tenant account in one of the following formats: *Organization\Username* or *Username@Organization*. For example: *TechCompanyOrg\Administrator* or *Administrator@TechCompanyOrg*.

Step 4. Enumerate Cloud Repository Resources

At the **Resources** step of the wizard, Veeam Backup & Replication will automatically enumerate resources provided to the tenant on the cloud repository and display the results in the wizard window.

Enumeration of storage resources on the cloud repository may take some time. Wait for the processing to complete and click **Next**.

Step 5. Enumerate Cloud Replication Resources

At the **Replica Resources** step of the wizard, Veeam Backup & Replication will automatically enumerate computing, storage and network resources provided to the tenant for processing tenant VM replicas. Replication resources can be provided to the tenant in one of the following ways:

- Through hardware plans.

  If you add the SP using credentials of a standalone tenant account, available replication resources will be displayed in the **Available hardware plans** list.

- Through organization VDCs.

    If you add the SP using credentials of a VMware Cloud Director tenant account, available replication resources will be displayed in the **Available organization VDC** list.

Enumeration of replication resources may take some time. Wait for the processing to complete and click **Next**.

Step 6. Configure Network Extension Appliances

At the **Network Extension** step of the wizard, Veeam Backup & Replication will display network extension appliance that will be deployed on the tenant side. This network extension appliance will be used for establishing and maintaining connection between production VMs and VM replicas on the cloud host after partial site failover.

In the **Network extension appliances** section of the **Network Extension** step of the wizard, you can view default network extension settings, edit settings for the network extension appliance and add one or several network extension appliances in case there are multiple IP networks in your production environment. To learn more, see Network Extension Appliance.
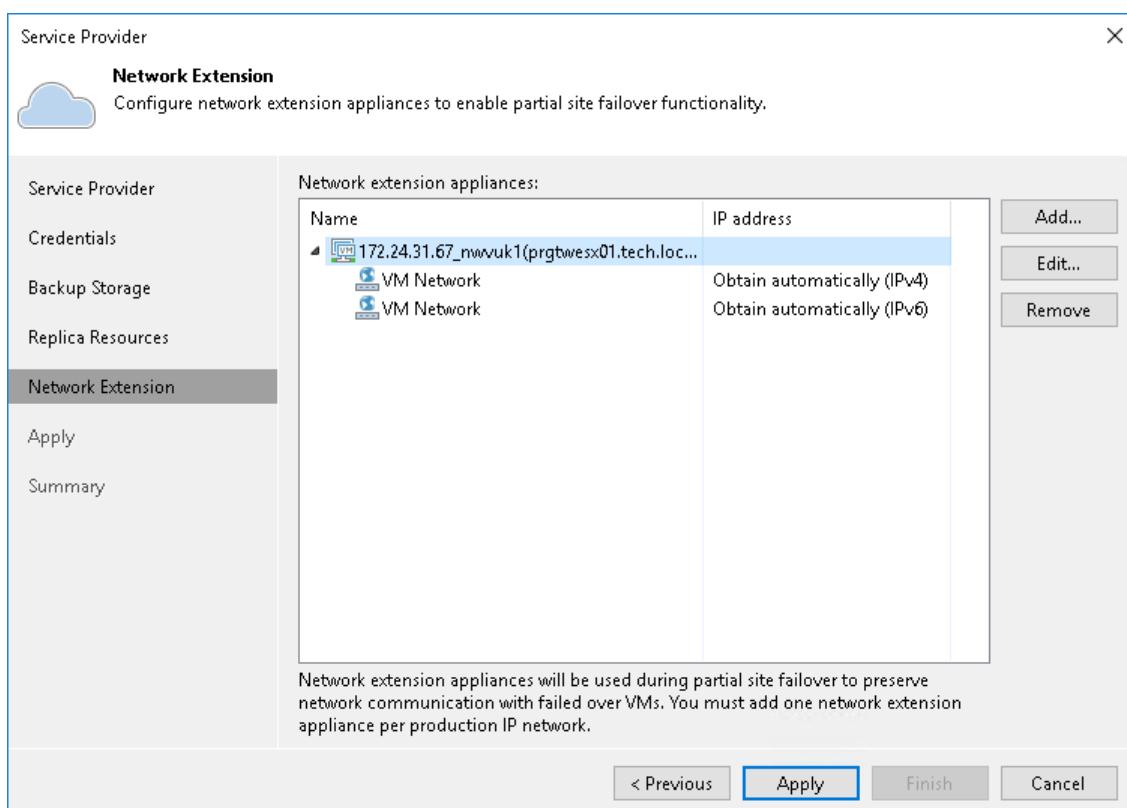
> **NOTE**
>
> Consider the following.
>
> - If you do not plan to perform partial site failover, you can remove the network extension appliance from the **Network extension appliances** list and proceed to the next step of the wizard. In this case, Veeam Backup & Replication will not deploy the network extension appliance on the source virtualization host.
> - If you add the SP using credentials of the VMware Cloud Director tenant account, and the SP uses an NSX Edge Gateway or IPsec VPN connection to enable network access to your VM replicas after failover, you do not need to deploy the network extension appliance. Click **Remove** next to the **Network extension appliances** list, and then click **Apply** to proceed to the next step of the wizard.

The process of configuring the network extension appliance differs depending on the virtualization platform whose VMs you want to replicate to the cloud: VMware vSphere or Microsoft Hyper-V.

- Configuring Network Extension Appliance for VMware vSphere

- Configuring Network Extension Appliance for Microsoft Hyper-V

Configuring Network Extension Appliance for VMware vSphere

To configure the network extension appliance that will deployed on the source VMware vSphere host:

1. Open the **Network Extension Appliance Configuration** window. To do this, do one of the following:

   o To configure a new network extension appliance, click **Add**.

   o To edit settings of the extension appliance that is already in the **Network extension appliances** list, select that network extension appliance and click **Edit**.

2. In the **Network Extension Appliance Configuration** window, in the **Host** section, click **Choose** and select the host on which the network extension appliance must be deployed. That is the source host from which your production VMs will be replicated to the cloud host.

3. In the **Resource pool** section, click **Choose** and select the resource pool in which the network extension appliance VM must be placed.

4. In the **Datastore** section, click **Choose** and select the datastore on which to keep files of the network extension appliance VM.

   > **NOTE**
   >
   > You cannot deploy a network extension appliance on the following types of storage:
   >
   > - VMware Virtual Volumes (VVol)
   > - Datastore Cluster
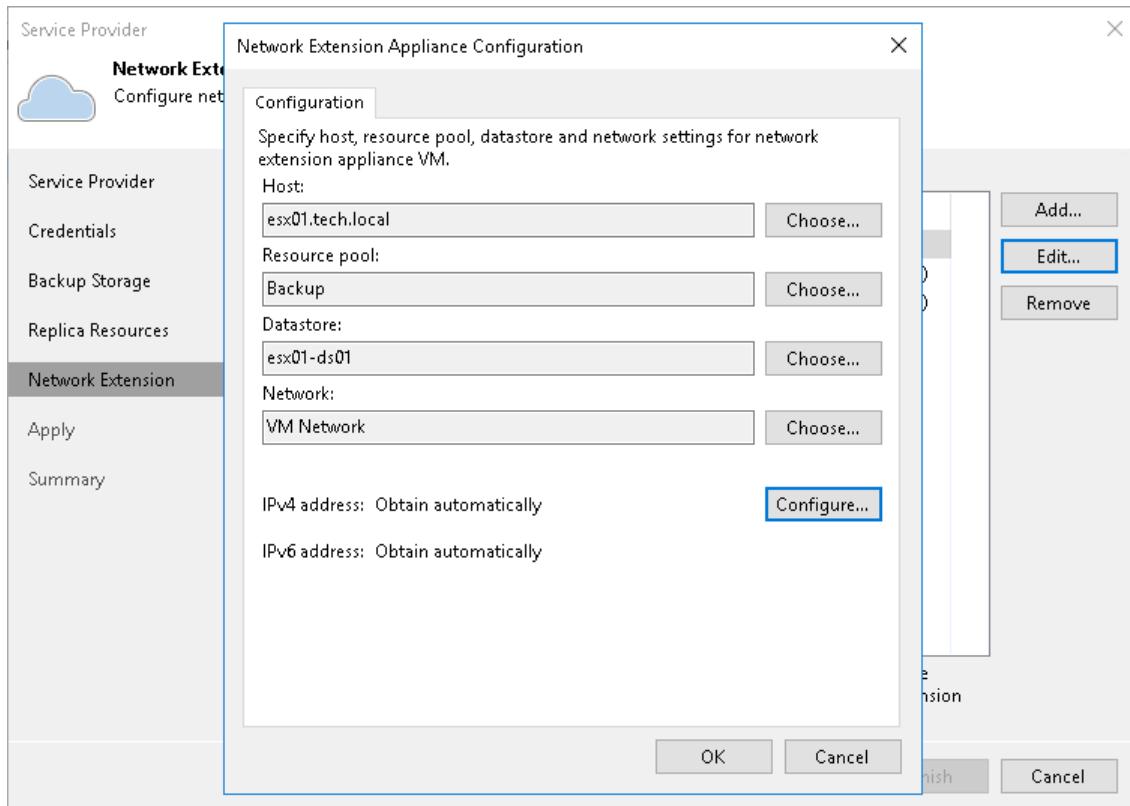
5. In the **Network** section, click **Choose** and select the virtual switch to which production VMs on the source host are connected.

6. Specify the IP addressing settings for the appliance.

   o To assign an IP address automatically in case there is a DHCP server in your network, make sure that the *Obtain automatically* value is displayed in the **IPv4 address** and **IPv6 address** fields.

   o To manually assign a specific IP address to the appliance, click **Configure** and specify network settings for the appliance. For details, see Specifying Network Settings.

7. Click **OK**.

Configuring Network Extension Appliance for Microsoft Hyper-V
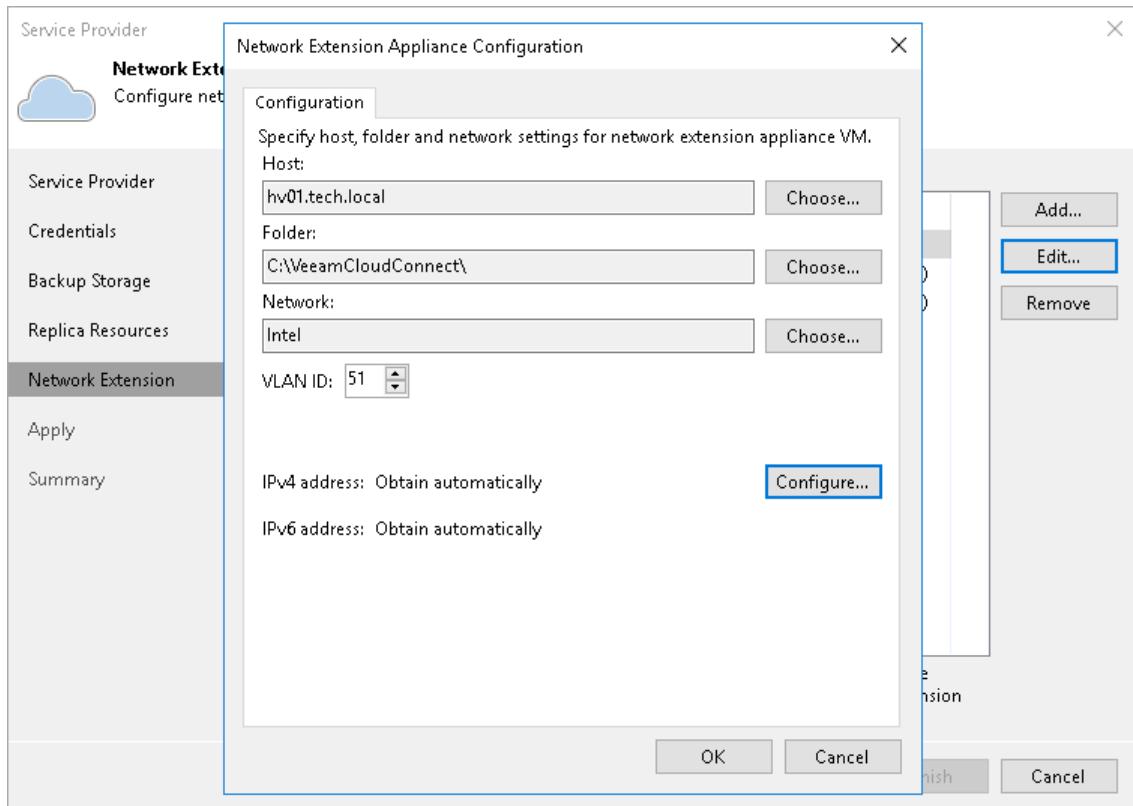
To configure the network extension appliance that will deployed on the source Microsoft Hyper-V host:

1. Open the **Network Extension Appliance Configuration** window. To do this, do one of the following:

   o To configure a new network extension appliance, click **Add**.

   o To edit settings of the extension appliance that is already in the **Network extension appliances** list, select that network extension appliance and click **Edit**.

2. In the **Network Extension Appliance Configuration** window, in the **Host** section, click **Choose** and select the host on which the network extension appliance must be deployed. That is the source host from which your production VMs will be replicated to the cloud host.

3. In the **Folder** section, click **Choose** and specify the path to the folder on the storage to keep files of the network extension appliance VM.

4. In the **Network** section, click **Choose** and select the virtual switch to which production VMs on the source host are connected.

5. In the **VLAN ID** field, specify the VLAN ID of the network on the selected virtual switch to which VMs that you plan to replicate are connected.

6. Specify the IP addressing settings for the appliance.

   o To assign an IP address automatically in case there is a DHCP server in your network, make sure that the *Obtain automatically* value is displayed in the **IPv4 address** and **IPv6 address** fields.

   o To manually assign a specific IP address to the appliance, click **Configure** and specify network settings for the appliance. For details, see Specifying Network Settings.

7. Click **OK**.

Specifying Network Settings

To specify network settings for the network extension appliance:

1. In the **Network Extension Appliance Configuration** window, click **Configure**.

2. To manually assign a specific IPv4 address to the appliance, do the following:

   a. On the **IPv4** tab, make sure that the **Enable IPv4 interface** check box is selected.

   b. Select the **Use the following IP address** option and specify the following network settings:

      ▪ IP address

      ▪ Subnet mask

      ▪ Default gateway

   Alternatively, if you want to assign an IPv4 address automatically, make sure that the **Obtain an IP address automatically** option is selected on the **IPv4** tab.

   If you do not want the network extension appliance to use an IPv4 address, clear the **Enable IPv4 interface** check box.

3. If you want to assign an IPv6 address to the appliance, do the following:

   a. Click the **IPv6** tab.

   b. Make sure that the **Enable IPv6 interface** check box is selected.

   c. Select the **Use the following IP address** option and specify the following network settings:

      ▪ IP address

      ▪ Subnet mask (prefix length)

      ▪ Default gateway

   Alternatively, if you want to assign an IPv6 address automatically, make sure that the **Obtain an IP address automatically** option is selected on the **IPv6** tab.

   If you do not want the network extension appliance to use an IPv6 address, clear the **Enable IPv6 interface** check box.

4. Click **OK**.

Step 7. Assess Results

At the **Apply** step of the wizard, Veeam Backup & Replication will save information about resources available from your SP and deploy the specified number of network extension appliances on your production host. Wait for the required operations to complete and click **Next** to continue.

Step 8. Finish Working with Wizard

At the **Summary** step of the wizard, complete the procedure of SP adding.

1. Review the configuration information on the added SP.

2. Click **Finish** to exit the wizard.

Changing Password for Tenant Account

You can change the password for the tenant account whose credentials you obtained from the SP.

This operation is performed by the tenant in the tenant Veeam Backup & Replication console.
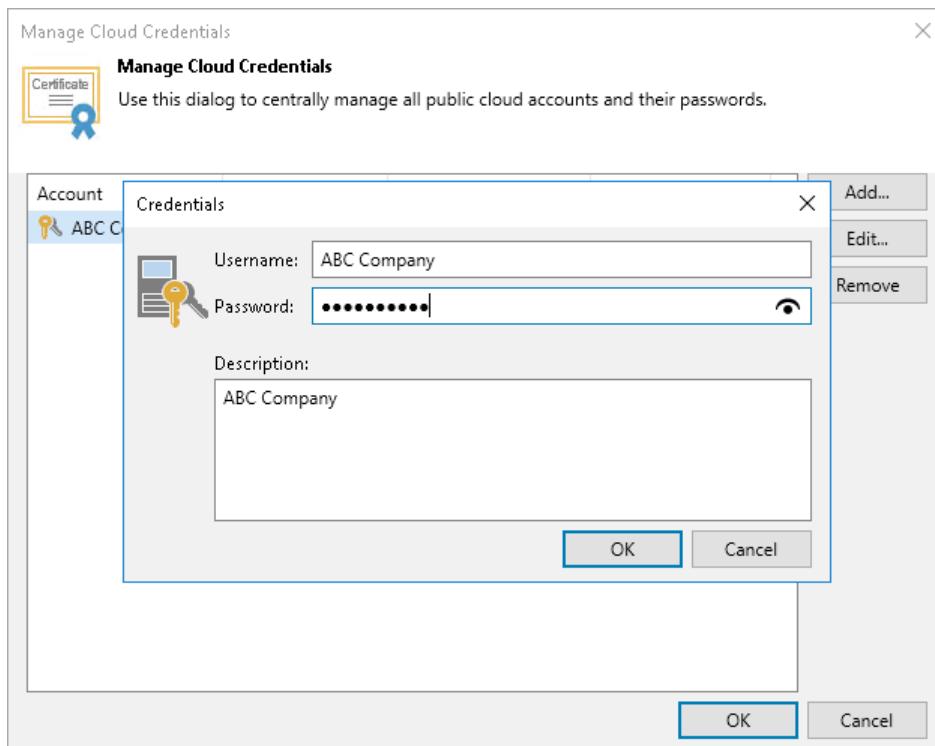
> **NOTE**
>
> You cannot change the password for a VMware Cloud Director tenant account. For such accounts, passwords are managed by the SP in VMware Cloud Director.

To change a password for the tenant account:

1. In the tenant Veeam Backup & Replication console, from the main menu, select **Credentials and Passwords** > **Cloud Credentials**.

2. In the **Manage Cloud Credentials** window, select the user name of the tenant account whose password you want to change and click **Edit**.

3. Veeam Backup & Replication will display a notification informing that tenant credentials are currently used to connect to the SP. In the notification window, click **Yes**.

4. In the **Credentials** window, in the **Password** field, enter a new password for the tenant account and click **OK**.

   To view the entered password, you can click and hold the eye icon on the right of the field.

5. In the **Current Password** field, enter the current password of the tenant account and click **OK**.

6. In the **Manage Cloud Credentials** window, click **OK**.

Managing Subtenant Accounts on Tenant Side

To provide subtenants with individual storage quotas on the cloud repository, you must register a subtenant account for each subtenant. Typically, the procedure of subtenant accounts registration is performed by the tenant on the tenant Veeam backup server. The SP can also manage subtenant accounts for the specific tenant. To learn more, see Managing Subtenant Accounts on SP Side.

You can perform the following operations with subtenant accounts:

- Add a subtenant account for a standalone tenant account.

- Add a subtenant account for a VMware Cloud Director tenant account.

- Edit a subtenant account.

- Remove a subtenant account.

Creating Subtenant Account for Standalone Tenant

Typically, the procedure of subtenant accounts registration is performed by the tenant on the tenant Veeam backup server.

When you create a subtenant account, remember to save a user name and password for the created subtenant account. You must pass this data to the end user who will use the subtenant account. When configuring a Veeam Agent backup job targeted at the cloud repository, the user must enter the user name and password for the subtenant account to connect to the SP backup server.

Before You Begin

Before you add a new subtenant account, check the following prerequisites:

- You must be connected to the SP whose cloud repository you want to expose to subtenants. When you create a subtenant account, you can allocate storage quota only on those cloud repositories that are provided to your tenant account by the SP.

- You can allocate only one storage quota per subtenant account. To provide a user with multiple quotas on the same or different cloud repositories, you must create different subtenant accounts for the same user.

Step 1. Launch New Subtenant Wizard

To launch the **New subtenant** wizard:

1. Open the **Subtenant Quotas** window in one of the following ways:

   o Open the **Backup Infrastructure** view, click the **Backup Repositories** node in the inventory pane, select the cloud repository in the working area and click **Manage Subtenants** on the ribbon.

   o Open the **Backup Infrastructure** view, click the **Backup Repositories** node in the inventory pane, right-click the cloud repository in the working area and select **Manage subtenants**.

   o Open the **Backup Infrastructure** view. Click the **Service Providers** node in the inventory pane, select the service provider in the working area and click **Manage Subtenants** on the ribbon.

   o Open the **Backup Infrastructure** view, click the **Service Providers** node in the inventory pane, right-click the service provider in the working area and select **Manage subtenants**.

2. In the **Subtenant Quotas** window, click **Add**.

Step 2. Specify Subtenant Settings

At the **Account** step of the wizard, specify settings for the created subtenant account:

1. In the **Username** field, specify a name for the created subtenant account. The user name must meet the following requirements:

    o   The maximum length of the user name is 128 characters. It is recommended that you create short user names to avoid problems with long paths to backup files on the cloud repository.

    o   The user name may contain space characters.

    o   The user name must not contain the following characters: , \ / : * ? \ " <> | =; @ as well as Unicode characters.

    o   The user name must not end with the period character [.].

2. In the **Password** field, provide the password for the subtenant account. You can enter your own password or click the **Generate** new link at the bottom of the field. In the latter case, Veeam Backup & Replication will generate a safe password. To get a copy the generated password, click the **Copy to clipboard** link at the bottom of the window.

3. In the **Description** field, specify a description for the created subtenant account.

4. If you want the subtenant account to be created in the disabled state, select the **Subtenant is disabled** check box. In this case, Veeam Backup & Replication will create the subtenant account, but the subtenant will not be able to connect to the SP and create backups on the cloud repository.

Step 3. Allocate Subtenant Quota

At the **Quotas** step of the wizard, specify subtenant quota settings for the created account. You can assign to the subtenant tenant a single quota on a cloud repository assigned to the tenant account.

To assign a subtenant quota:

1. Click **Add** on the right of the **Available user quotas** list.

2. In the **Subtenant Quota** window, in the **Name** field, enter a friendly name for the subtenant quota. The name you enter will be displayed at the subtenant's side.

3. In the **Repository** field, select a cloud repository whose space resources must be allocated to the subtenant.

4. By default, Veeam Backup & Replication allows subtenants to use an entire quota on the cloud repository assigned to the tenant. If you want to limit the amount of storage space that the subtenant can use on the cloud repository, in the **Quota** section, select **Limit size to** and specify the necessary subtenant quota.

   When you consider limiting the subtenant quota, remember to allocate the sufficient amount of storage space for the subtenant. The subtenant quota must comprise the amount of disk space used to store a chain of backup files plus additional space required for performing the backup chain transform operation. Generally, to perform the transform operation, Veeam Backup & Replication requires the amount of disk space equal to the size of a full backup file.

5. Click **OK**.

Step 4. Finish Working with Wizard

At the **Summary** step of the wizard, complete the procedure of subtenant account registration.

1. Click the **Copy to clipboard** link to copy information about the created subtenant account: user name, password, cloud repository and quota. You must send the copied information to a user on the tenant side so that they can use the created subtenant account to configure a backup job targeted at the cloud repository.

2. Click **Finish** to exit the wizard.

Creating Subtenant Account for VMware Cloud Director Tenant

Typically, the procedure of subtenant accounts registration is performed by the tenant on the tenant Veeam backup server.

After you create a subtenant account, pass the user name of the created account to your subtenant. When configuring a backup job targeted at the cloud repository, the subtenant must enter the user name for the subtenant account to connect to the SP backup server.

Before You Begin

Before you add a new subtenant account, check the following prerequisites:

- You must be connected to the SP whose cloud repository you want to expose to subtenants. When you create a subtenant account, you can allocate storage quota only on those cloud repositories that are provided to your tenant account by the SP.

- You can allocate only one storage quota per subtenant account. To provide a user with multiple quotas on the same or different cloud repositories, you must create different subtenant accounts for the same user.

- The Cloud Director user account that you plan use as a subtenant account must be created for the organization in VMware Cloud Director.

Step 1. Launch New Subtenant Wizard

To launch the **New subtenant** wizard:

1. Open the **Subtenant Quotas** window in one of the following ways:

   o Open the **Backup Infrastructure** view, click the **Backup Repositories** node in the inventory pane, select the cloud repository in the working area and click **Manage Subtenants** on the ribbon.

   o Open the **Backup Infrastructure** view, click the **Backup Repositories** node in the inventory pane, right-click the cloud repository in the working area and select **Manage subtenants**.

   o Open the **Backup Infrastructure** view. Click the **Service Providers** node in the inventory pane, select the service provider in the working area and click **Manage Subtenants** on the ribbon.

   o Open the **Backup Infrastructure** view, click the **Service Providers** node in the inventory pane, right-click the service provider in the working area and select **Manage subtenants**.

2. In the **Subtenant Quotas** window, click **Add**.

Step 2. Select Cloud Director User

At the **Cloud Director User** step of the wizard, specify settings for the created subtenant account:

1. Click **Add** next to the **Username** field and select a user account of a VMware Cloud Director organization to which you want to allocate a quota on the cloud repository. The user account must be created in advance by the SP in VMware Cloud Director.

2. In the **Description** field, specify a description for the created subtenant account.

3. If you want the subtenant account to be created in the disabled state, select the **Subtenant is disabled** check box. In this case, Veeam Backup & Replication will create the subtenant account, but the subtenant will not be able to connect to the SP and create backups on the cloud repository.

Step 3. Allocate Subtenant Quota

At the **Quotas** step of the wizard, specify subtenant quota settings for the created account. You can assign to the subtenant tenant a single quota on a cloud repository assigned to the tenant account.

To assign a subtenant quota:

1. Click **Add** on the right of the **Available user quotas** list.

2. In the **Subtenant Quota** window, in the **Name** field, enter a friendly name for the subtenant quota. The name you enter will be displayed at the subtenant's side.

3. In the **Repository** field, select a cloud repository whose space resources must be allocated to the subtenant.

4. By default, Veeam Backup & Replication allows subtenants to use an entire quota on the cloud repository assigned to the tenant. If you want to limit the amount of storage space that the subtenant can use on the cloud repository, in the **Quota** section, select **Limit size to** and specify the necessary subtenant quota.

   When you consider limiting the subtenant quota, remember to allocate the sufficient amount of storage space for the subtenant. The subtenant quota must comprise the amount of disk space used to store a chain of backup files plus additional space required for performing the backup chain transform operation. Generally, to perform the transform operation, Veeam Backup & Replication requires the amount of disk space equal to the size of a full backup file.

5. Click **OK**.

Step 4. Finish Working with Wizard

At the **Summary** step of the wizard, complete the procedure of subtenant account registration.

1. Review the information about the added subtenant account.

2. Click **Finish** to exit the wizard.

Editing Subtenant Account

You can edit settings of created subtenant accounts. For example, you may want to reallocate storage quota for the subtenant, change password for the subtenant account of a standalone tenant account, disable or enable the subtenant account.

> **NOTE**
>
> Mind the following:
>
> - You cannot change a user name for the subtenant account.
> - If you open the *Subtenant Quotas* window from the *Backup Repositories* node, you cannot select a cloud repository on which to allocate storage quota for the edited subtenant account.

To edit settings of a subtenant account:

1. Open the **Subtenant Quotas** window in one of the following ways:

   - Open the **Backup Infrastructure** view, click the **Backup Repositories** node in the inventory pane, select the cloud repository in the working area and click **Manage Subtenants** on the ribbon.

   - Open the **Backup Infrastructure** view, click the **Backup Repositories** node in the inventory pane, right-click the cloud repository in the working area and select **Manage subtenants**.

   - Open the **Backup Infrastructure** view. Click the **Service Providers** node in the inventory pane, select the service provider in the working area and click **Manage Subtenants** on the ribbon.

   - Open the **Backup Infrastructure** view, click the **Service Providers** node in the inventory pane, right-click the service provider in the working area and select **Manage subtenants**.

2. In the **Subtenant Quotas** window, select the necessary subtenant account and click **Edit**.

   To quickly find the necessary subtenant account, use the search field at the bottom of the **Subtenant Quotas** window:

   a. Enter the user name of the subtenant account or a part of it in the search field.

   b. Click the **Start search** button on the left or press **[ENTER]**.

3. In the **Edit subtenant** wizard, edit subtenant account settings as required.

Deleting Subtenant Account

You can delete a subtenant account that you created at any time, for example, if the subtenant no longer uses resources of the cloud repository.

When you delete a subtenant account, Veeam Backup & Replication disables this account and removes it. The subtenant account is removed permanently. You cannot undo this operation.

Subtenant's backup data remain intact on the cloud repository. You can delete subtenant backup data manually later if needed.

> **NOTE**
>
> You cannot delete managed subtenant accounts — subtenant accounts created automatically by Veeam Backup & Replication in the Veeam Agent management scenario.

To delete a subtenant account:

1. Open the **Subtenant Quotas** window in one of the following ways:

   o Open the **Backup Infrastructure** view, click the **Backup Repositories** node in the inventory pane, select the cloud repository in the working area and click **Manage Subtenants** on the ribbon.

   o Open the **Backup Infrastructure** view, click the **Backup Repositories** node in the inventory pane, right-click the cloud repository in the working area and select **Manage subtenants**.

   o Open the **Backup Infrastructure** view. Click the **Service Providers** node in the inventory pane, select the service provider in the working area and click **Manage Subtenants** on the ribbon.

   o Open the **Backup Infrastructure** view, click the **Service Providers** node in the inventory pane, right-click the service provider in the working area and select **Manage subtenants**.

2. In the **Subtenant Quotas** window, select the necessary subtenant account and click **Remove**.

   To quickly find the necessary subtenant account, use the search field at the bottom of the **Subtenant Quotas** window:

   a. Enter the user name of the subtenant account or a part of it in the search field.

   b. Click the **Start search** button on the left or press **[ENTER]**.

Managing Network Extension Appliance

You can perform the following operations with the tenant-side network extension appliance:

- Manage network extension appliance credentials

- Redeploy a network extension appliance

Managing Credentials

Veeam Backup & Replication connects to the network extension appliance using service credentials — credentials for the root account on the Linux-based network extension appliance VM. You can use these credentials to log on to the network extension appliance VM. This may be useful if you need to configure the network extension appliance manually, for example, for troubleshooting reasons.

It is recommended that you change the password in the service credentials record before connecting to the SP and deploying network extension appliances. You can change the password using the Credentials Manager.
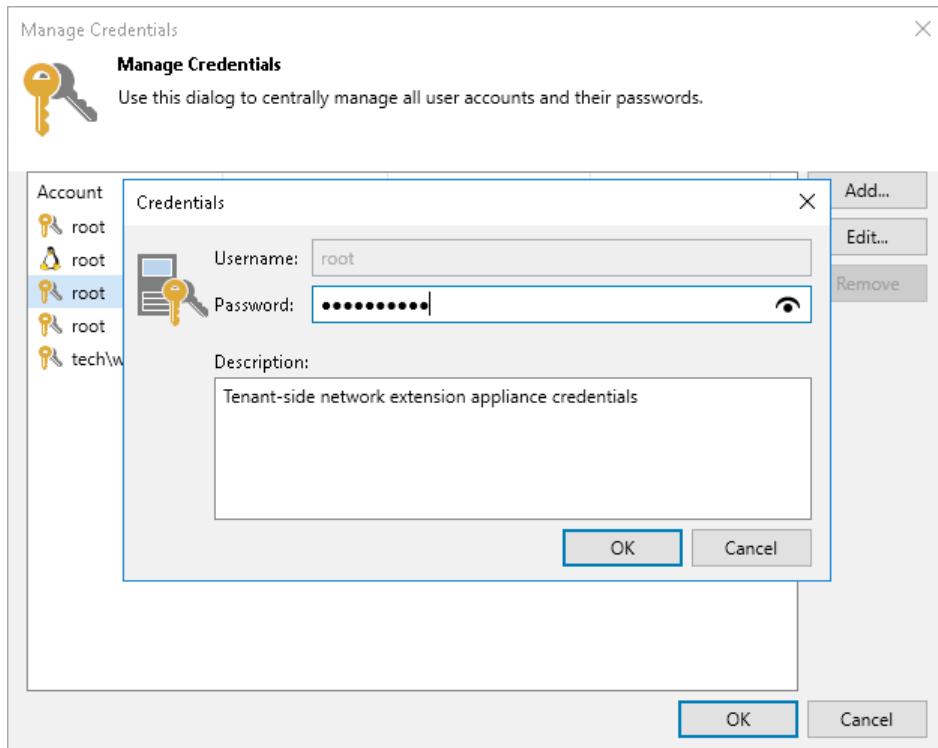
> **NOTE**
>
> If you change the password after the network extension appliance is deployed, you will need to redeploy the network extension appliance. To learn more, see Redeploying Network Extension Appliance.

To change a password for the root account of network extension appliance VMs:

1. From the main menu, select **Credentials and Passwords** > **Datacenter Credentials**.

2. Select the **Tenant-side network extension appliance credentials** record and click **Edit**.

3. Veeam Backup & Replication will display a warning notifying that you will need to redeploy existent network extension appliances after you change the password. Click **Yes** to confirm your intention.

4. In the **Password** field, enter a password for the root account. To view the entered password, click and hold the eye icon on the right of the **Password** field.

   The specified password will be assigned to the root account of every network extension appliance VM that will be deployed on the source virtualization host.

5. In the **Description** field, if necessary, change the default description for the edited credentials record.

6. Click **OK** to save the specified password.
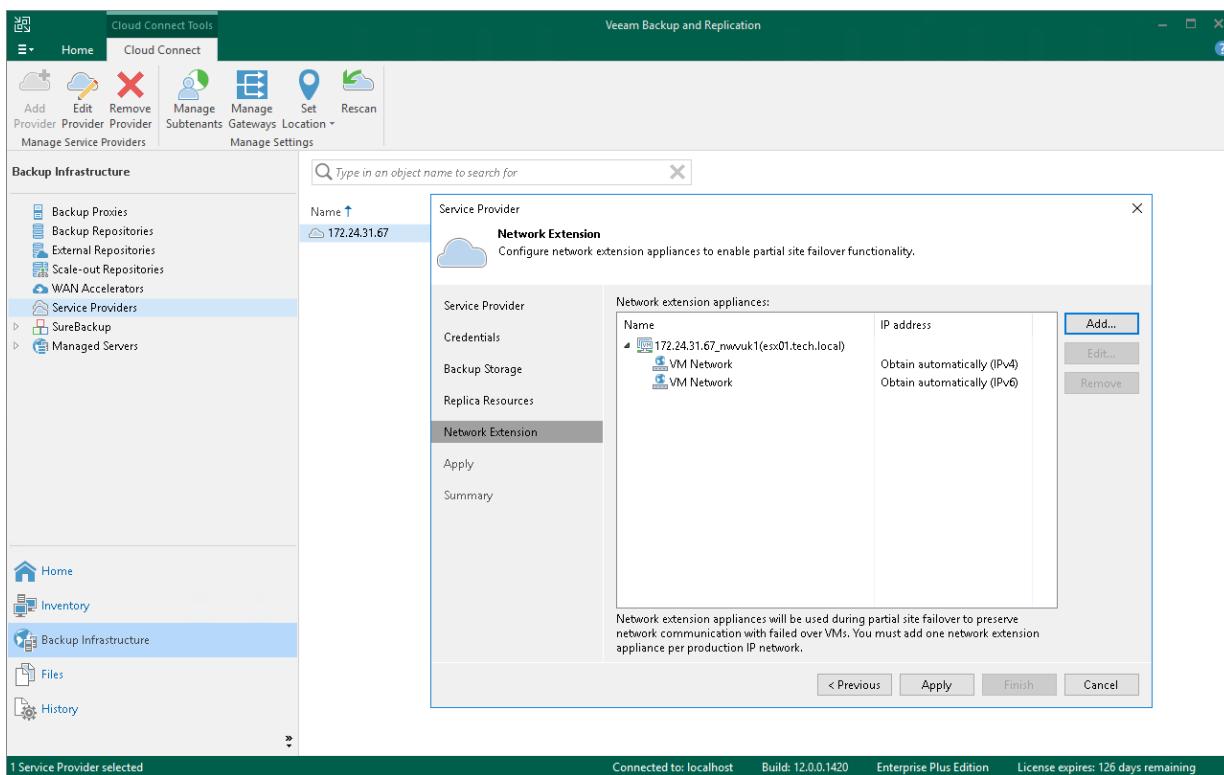
Redeploying Network Extension Appliance

You can redeploy the network extension appliance on the source host. This may be necessary when the network extension appliance becomes inoperative or when you change the password in the network extension appliance credentials record after one or several appliances are already deployed.

To redeploy the network extension appliance:

1. Open the **Backup Infrastructure** view.

2. In the inventory pane, click **Service Providers**.

3. In the working area, right-click the necessary service provider and select **Properties**.

4. At the **Network extension** step of the **Service Provider** wizard, in the **Network extension appliances** section, select the network extension appliance and click **Remove**.

5. If you deployed several network extension appliances on the source host and need to redeploy these appliances after changing the password, repeat step 3 for every appliance in the **Network extension appliances** list.

6. Click **Add** and configure the new network extension appliance as required. To learn more, see Configuring Network Extension Appliance.

7. Proceed to the **Summary** step of the wizard and click **Finish** to exit the wizard.

Managing Default Gateways

After full site failover, Veeam Backup & Replication uses the network extension appliance on the cloud host as a default gateway between a VM replica network and external networks. To route traffic that goes to and from VM replicas, the network extension appliance uses network settings of the default gateway in the production VM network.
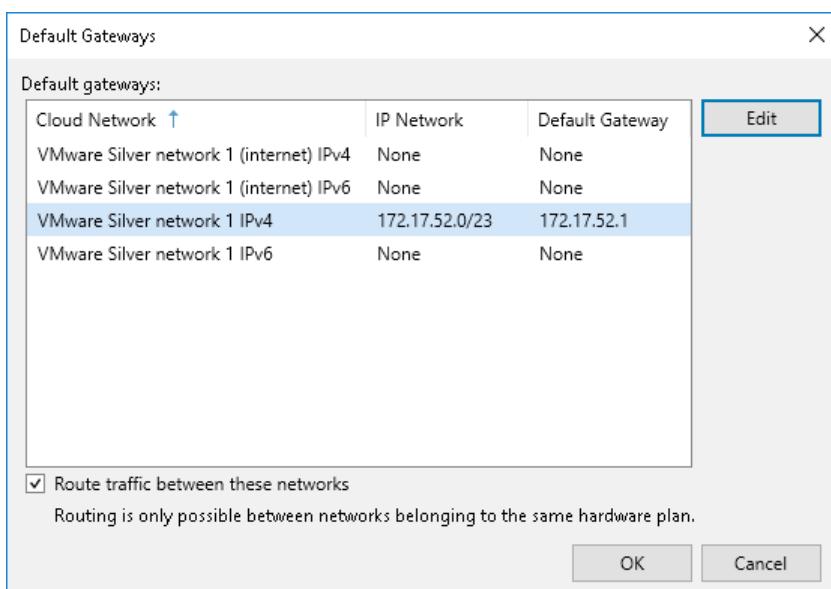
During the first run of the replication job targeted at the cloud host, Veeam Backup & Replication detects network settings of replicated VMs and automatically saves information about default gateways that are used in every detected production network. You can check and, if necessary, edit default gateway settings in the Veeam Backup & Replication console. The specified settings will be used by the network extension appliance after failover.

When you specify the default gateway, Veeam Backup & Replication saves its settings in the Veeam Backup & Replication database on the SP side. After full site failover, Veeam Backup & Replication assigns the specified default gateway settings to the network extension appliance on the cloud host. As a result, VM replicas on the cloud host communicate to the internet in the same way as VMs in the production site.
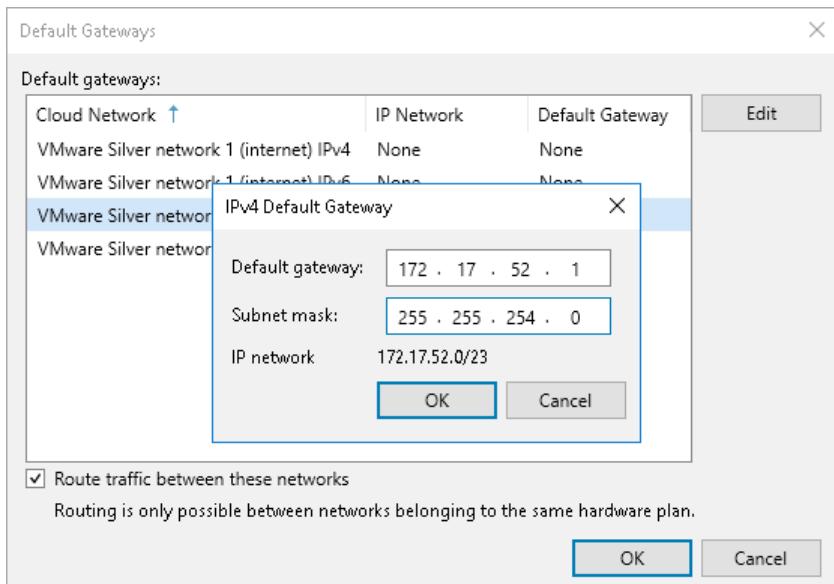
Network extension appliance can also route traffic between several networks provided for VM replicas through the same hardware plan.

To manage default gateways:
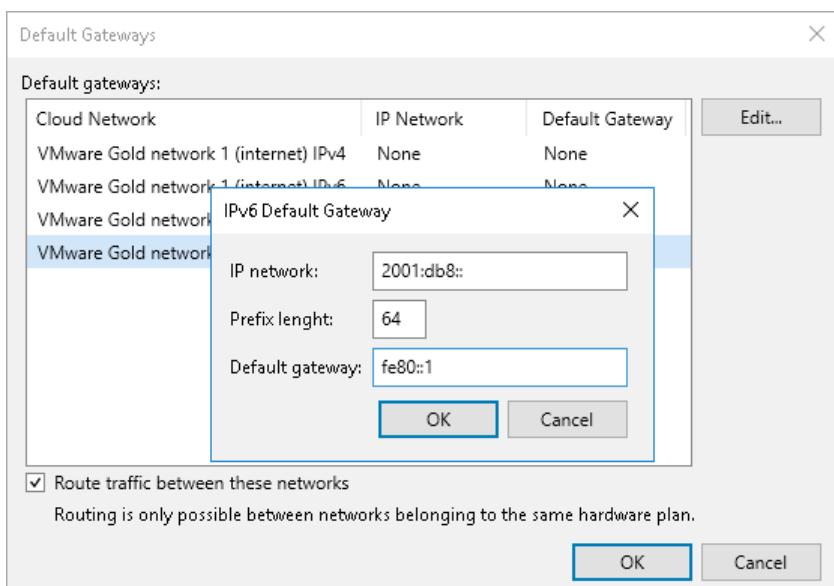
1. Open the **Backup Infrastructure** view.

2. In the inventory pane, click the **Service Providers** node.

3. In the working area, select the service provider and click **Manage Gateways** on the ribbon or right-click the service provider and select **Manage default gateways**.

4. In the **Default Gateways** window, select the virtual cloud network provided for your VM replicas through the hardware plan and click **Edit**.

5. [For IPv4 networks] In the **IPv4 Default Gateway** window, specify the IP address of the default gateway that is used in your production site and subnet mask of the production network, and click **OK**.

6. [For IPv6 networks] In the **IPv6 Default Gateway** window, specify the production IPv6 network, prefix length and IP address of the default gateway, and click **OK**.

7. Select the **Route traffic between these networks** option if the SP subscribed you to a hardware plan with several networks available to your VM replicas and you want Veeam Backup & Replication to route traffic between these networks. This may be useful if your production site runs multiple interdependent VMs connected to several networks.

8. Click **OK**.

Configuring Source WAN Accelerators

To optimize VM traffic going to the Veeam Cloud Connect infrastructure during the backup copy and replication jobs, the SP and tenants can configure WAN accelerators on their sides.

WAN accelerators in the Veeam Cloud Connect infrastructure must be configured in the following way:

- The source WAN accelerator is configured on the tenant side. Every tenant who plans to work with the cloud repository and cloud hosts using WAN accelerators must configure at least one WAN accelerator on their side.

- The target WAN accelerator is configured on the SP side.

When the SP creates a tenant account, the SP can define if the tenant should be able to utilize a WAN accelerator deployed on the SP side. As soon as you connect to the SP, Veeam Backup & Replication retrieves the following information to identify if cloud resources available to you can or cannot use WAN acceleration:

- Information about all quotas on cloud repositories assigned to you by the SP

- Information about all cloud hosts provided to you by the SP through hardware plans

If the cloud repository and/or cloud host can use WAN acceleration, you can configure a source WAN accelerator on your side and create backup copy and/or replication jobs that will work using WAN accelerators.

The configuration process for WAN accelerators in the Veeam Cloud Connect infrastructure is the same as the configuration process in a regular Veeam backup infrastructure. To learn more, see the Adding WAN Accelerators section in Veeam Backup & Replication User Guide.

Viewing Cloud Hosts
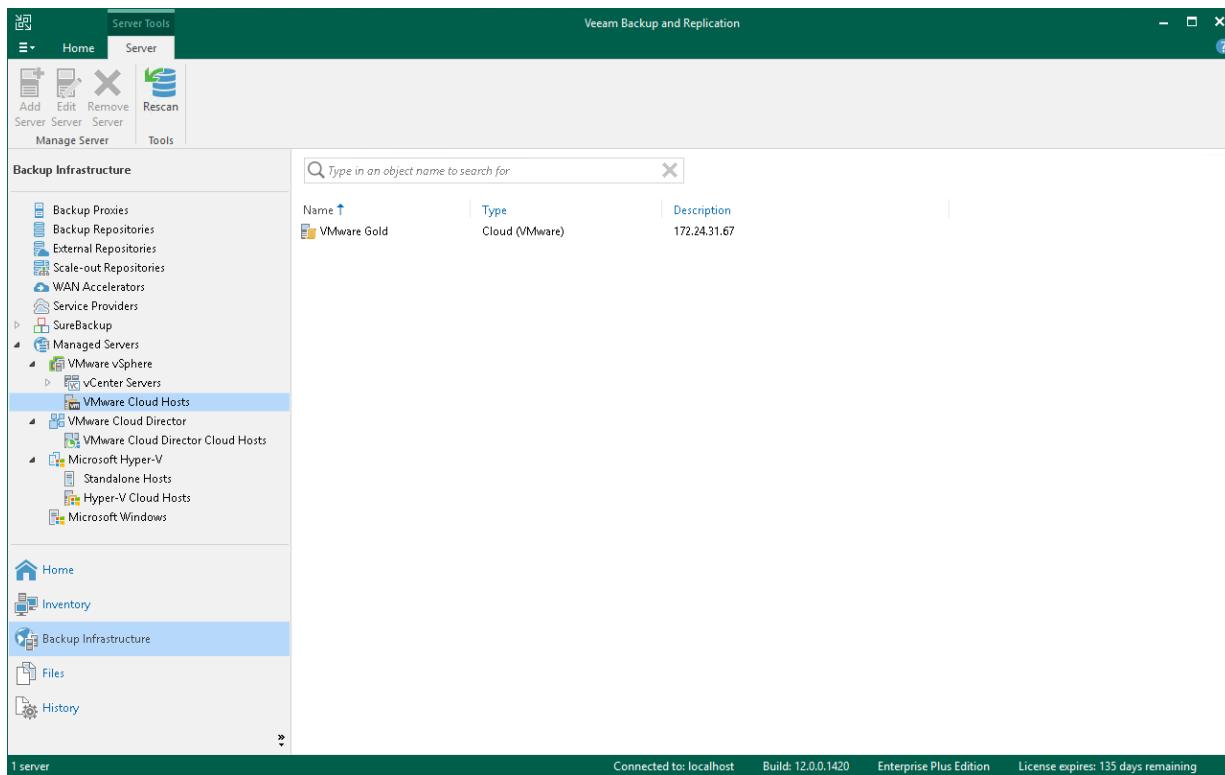
After tenant connects to the SP, cloud hosts provided to the tenant appear in the tenant Veeam backup console.

To view the available cloud hosts:

1. Open the **Backup Infrastructure** view.

2. In the inventory panel, expand the **Managed Servers** node.

   o Cloud hosts provided to the tenant through a VMware vSphere hardware plan are displayed under the **VMware vSphere** > **VMware Cloud Hosts** node.

   o Cloud hosts provided to the tenant through a Microsoft Hyper-V hardware plan are displayed under the **Microsoft Hyper-V** > **Hyper-V Cloud Hosts** node.

   o Cloud hosts provided to the tenant through a VMware Cloud Director organization VDC are displayed under the **VMware Cloud Director** > **VMware Cloud Director Cloud Hosts** node.

If the tenant has set up the Veeam Cloud Connect Replication infrastructure, they can configure replication jobs targeted at the cloud host.

If the SP and tenant have set up the CDP infrastructure, the tenant can configure CDP policies targeted at a VMware vSphere cloud host or VMware Cloud Director cloud host.

Using Cloud Repositories

After you have set up the Veeam Cloud Connect infrastructure, you can proceed to performing data protection and disaster recovery tasks using the cloud repository.

Performing Backup

You can perform the following data protection tasks with the cloud repository in Veeam Backup & Replication:

- VM backup

- VMware Cloud Director backup (for VMware vSphere platform)

- Veeam Agent backup

- Backup copy (To a cloud repository only. Backup copy from a cloud repository is not supported.)

Creating VM Backup Jobs

In Veeam Backup & Replication, backup is a job-driven process. To back up VMs, you must configure a backup job. The backup job defines how, where and when to back up VM data. One job can be used to process one or several VMs.

Veeam Backup & Replication backs up a VM image as a whole: it copies VM data at a block level unlike traditional backup tools that process guest OS files separately. Veeam Backup & Replication retrieves VM data from the source storage, compresses and deduplicates it and writes to the backup repository in Veeam's proprietary format. You can use the image-level backup for all types of data restore scenarios: restore a full VM, VM guest OS files and folders, VM files and VM virtual disks (for VMware VMs only) from the backup file.
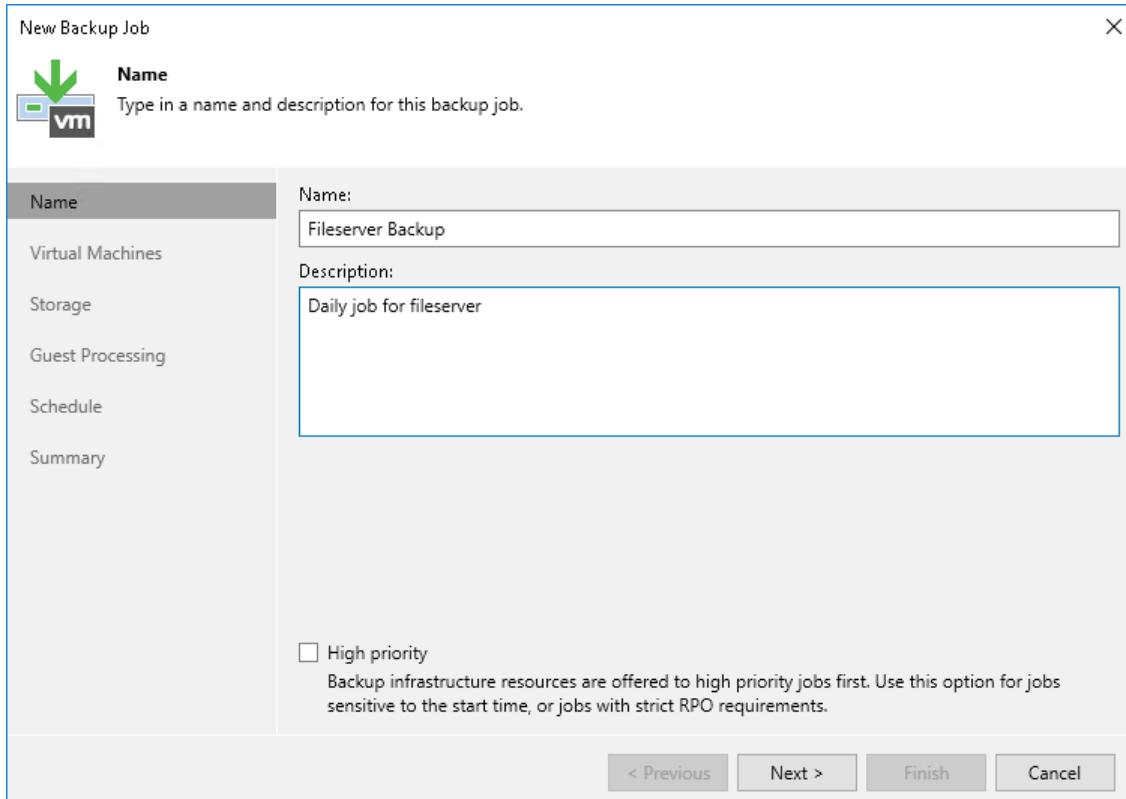
Veeam Backup & Replication conducts both full and incremental backup. During the first run of a backup job, Veeam Backup & Replication creates a full VM backup (VBK). All subsequent job cycles produce incremental backups: VIB if forward incremental backup is used or VRB if reversed incremental backup is used. The number of increments kept on disk depends on retention policy settings.
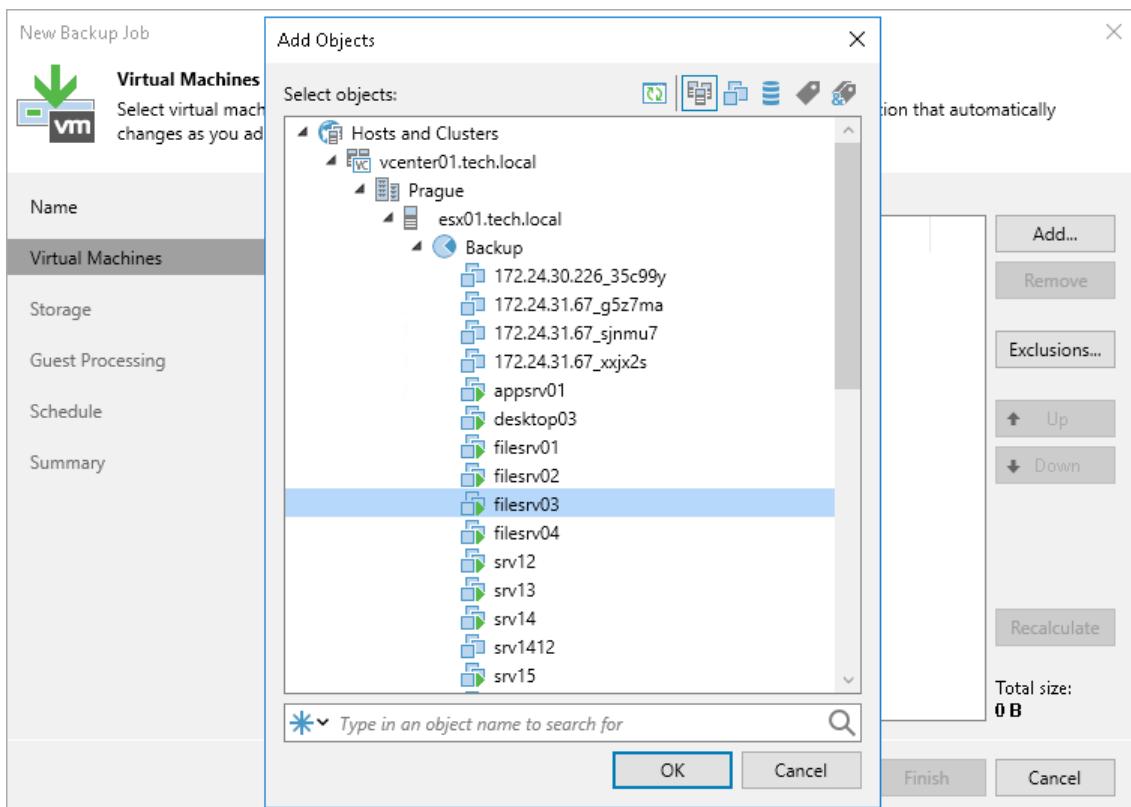
> **NOTE**
>
> This section describes only basic steps that you must take to create a VM backup job targeted at a cloud repository. To get a detailed description of all backup job settings, see the Creating Backup Jobs section in the Veeam Backup & Replication User Guide.

To create a backup job:
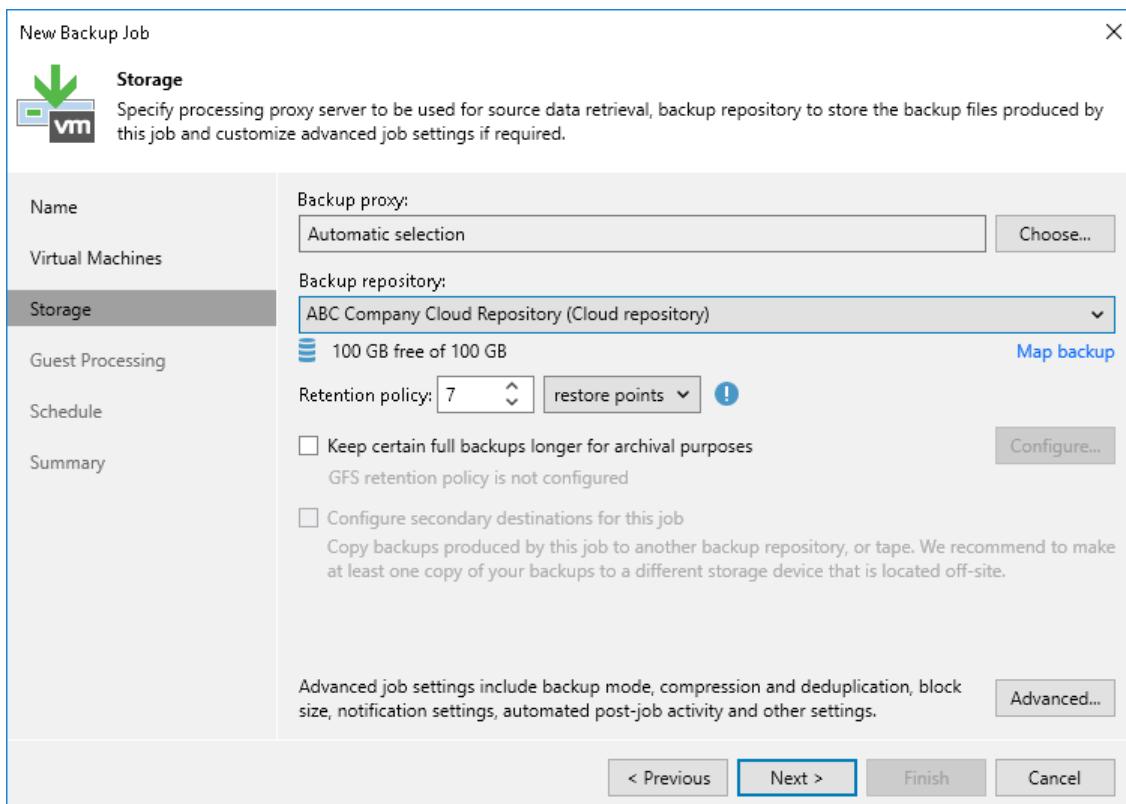
1. On the **Home** tab, click **Backup Job** and select **Virtual machine** > **VMware vSphere** or **Virtual machine** > **Microsoft Hyper-V**.

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, click **Add** and select VMs and VM containers that you want to back up. To quickly find the necessary object, use the search field at the bottom of the **Add Objects** window.

4. If you want to exclude VMs from the VM container or back up only specific VM disks, click **Exclusions** and specify what objects you want to exclude.

5. At the **Storage** step of the wizard, from the **Backup repository** list, select the cloud repository to which you plan to store the backup file.

6. In the **Retention policy** field, specify how many restore points you want to keep on the cloud repository. To do this, in the **Retention policy** field, specify the number of restore points or the number of days for which you want to store backup files on the cloud repository. If you want to use the GFS (Grandfather-Father-Son) retention scheme, you can also specify how weekly, monthly and yearly full backups must be retained.
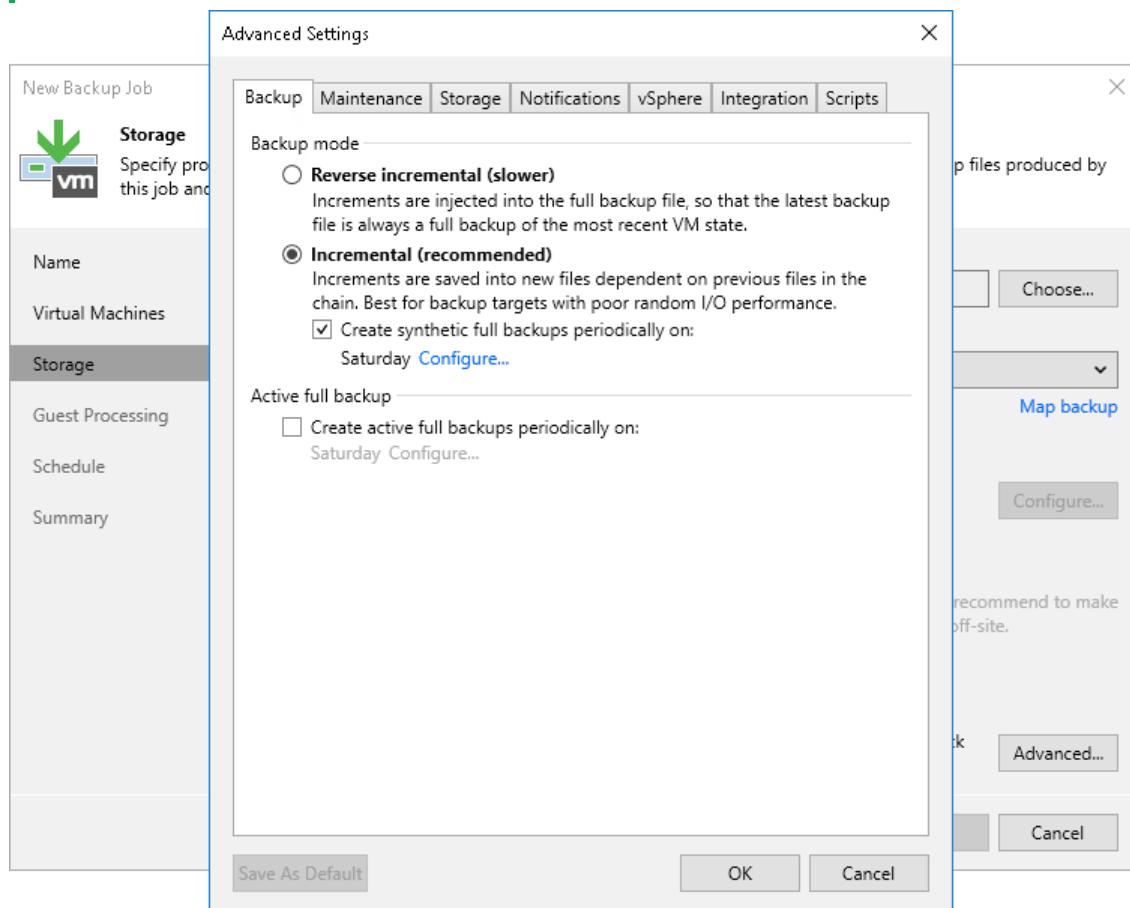
7. Click **Advanced**.
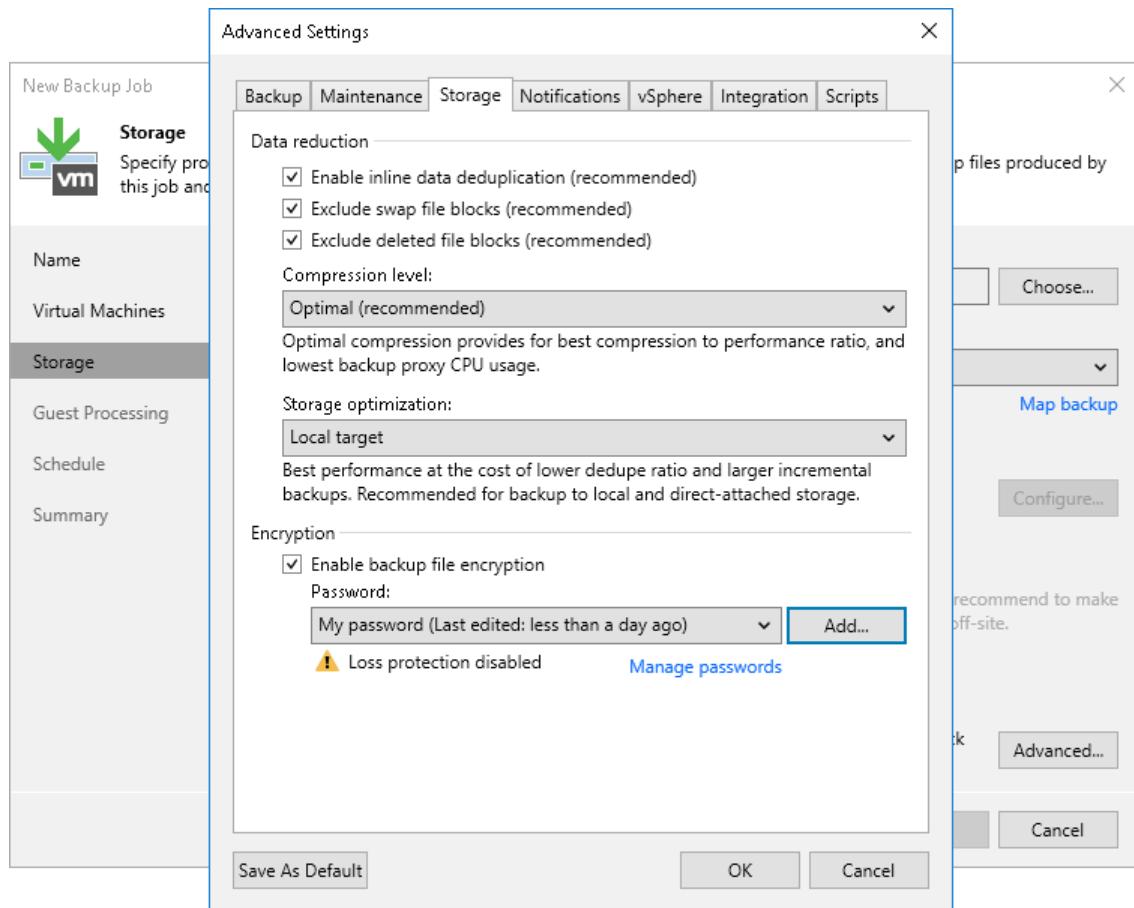
8. On the **Backup** tab, select what type of the backup chain you want to create: forward incremental or reverse incremental. You can also choose to periodically create synthetic full backups (for the forward incremental backup method only) and active full backups.
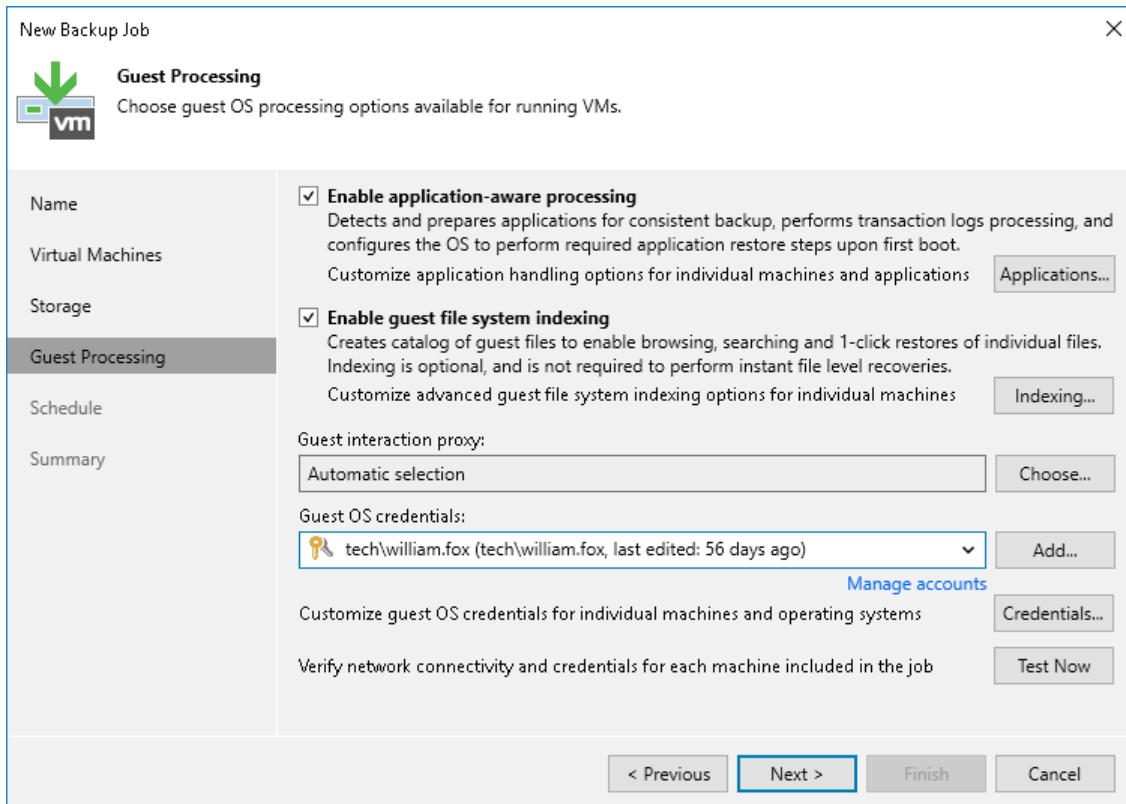
> **NOTE**
>
> The reverse incremental backup method is not recommended for backup jobs targeted at the cloud repository. The process of a full backup file rebuild requires higher I/O load. This may impact the backup job performance, especially in case of low bandwidth or high latency network connection between the tenant side and SP side. To learn more, see Veeam Backup & Replication Best Practices.

9. To encrypt the resulting backup file on the cloud repository, on the **Storage** tab, select the **Enable backup file encryption** check box. From the **Password** field, select a password that you want to use to encrypt the backup file. If you have not created a password beforehand, click **Add** or use the **Manage passwords** link to specify a new password.

10. To create a transactionally consistent backup of VMs, at the **Guest Processing** step of the wizard, select the **Enable application-aware processing** check box.

11. Click **Add** next to the Guest OS credentials list and specify credentials for a user account with local administrator privileges on the VM guest OS. By default, Veeam Backup & Replication uses the same credentials for all VMs added to the job. If some VM requires a different user account, click **Credentials** and enter custom credentials for the necessary VM.

12. Click **Applications**, select the necessary VM and click **Edit**. On the **General** tab, in the **Applications** section, specify the VSS behavior scenario:

   o Select **Require successful processing** if you want Veeam Backup & Replication to stop the backup process if any VSS errors occur.

   o Select **Try application processing, but ignore failures** if you want to continue the backup process even if VSS errors occur. This option is recommended to guarantee completion of the job. The created backup image will not be transactionally consistent, but crash consistent.

   o Select **Disable application processing** if you do not want to enable quiescence for the VM at all.

13. [For Microsoft SQL, Oracle and PostgreSQL VMs] In the **VSS Settings** section, specify how Veeam Backup & Replication must handle database logs:

   o Select **Process transaction logs with this job** if you want Veeam Backup & Replication to handle Microsoft SQL Server transaction logs or Oracle archived logs. With this option enabled, Veeam Backup & Replication will offer a choice of log processing options on the **SQL** and **Oracle** tabs.

   o Select **Perform copy only** if you use native application means or a third-party tool to process transaction logs. Veeam Backup & Replication will create a copy-only backup for the selected VM. The copy-only backup preserves a chain of full/differential backup files and transaction logs. To learn more, see Microsoft Docs.
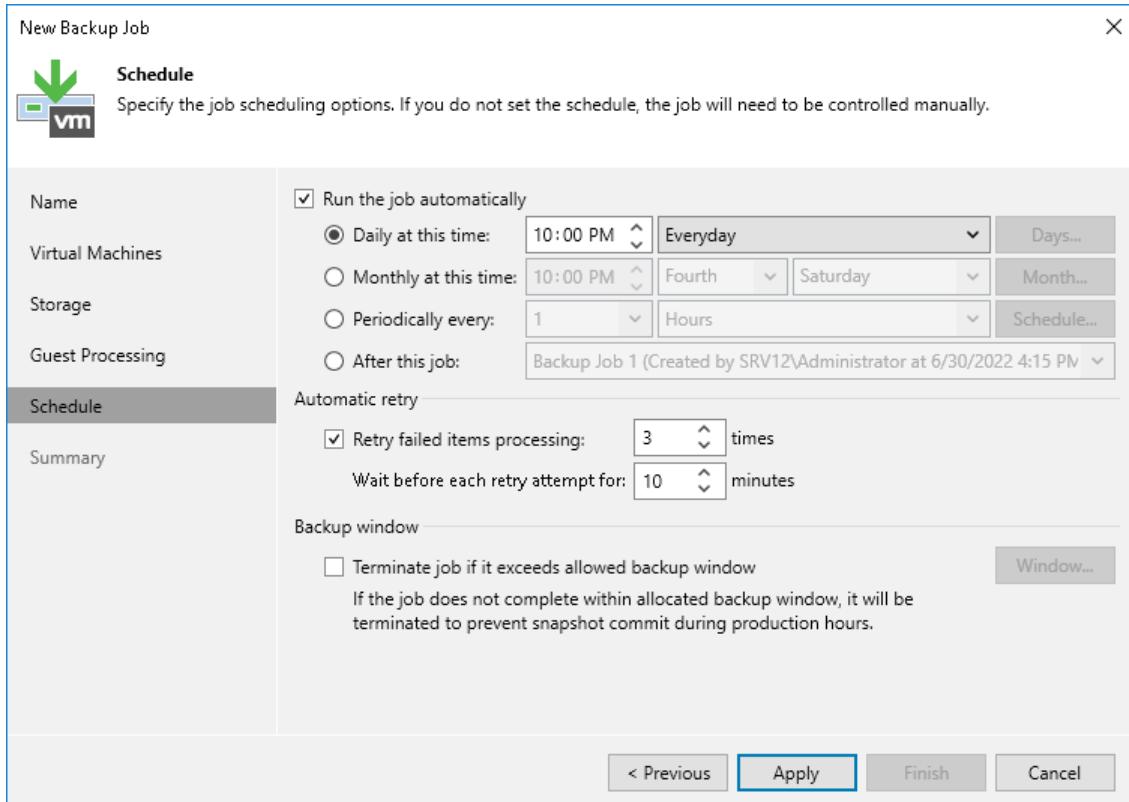
NOTE

You cannot enable log backup options in the properties of a backup job targeted at the cloud repository. For Microsoft SQL Server, you can enable transaction log truncation options only. For Oracle, you can choose whether to delete archived logs.

If you want to store database log backups in the cloud repository, you can do the following:

1. Configure a backup job targeted at a regular backup repository.
2. Configure a backup copy job targeted at a cloud repository. In the properties of the backup copy job, select the **Immediate copy** option, select the job created at the step 1 as a source backup job and enable the **Include database transaction log backups** option. For details, see Creating Backup Copy Jobs.

14. At the **Schedule** step of the wizard, select the **Run the job automatically** check box and specify the necessary scheduling settings for the job. If you do not select this check box, you will have to run the backup job manually to create a backup file in the cloud.

15. At the **Summary** step of the wizard, select the **Run the job when I click Finish** check box if you want to start the created job right after you complete working with the wizard.

16. Click **Finish**.

Creating VMware Cloud Director Backup Jobs

VMware Cloud Director backup is practically the same as a regular VM backup. The VMware Cloud Director backup job aggregates main settings for the backup task and defines when, what, how and where to back up.

You can perform the VMware Cloud Director backup job for single VMs and for VM containers, that, in terms of VMware Cloud Director, are the following:

- vApp

- Organization VDC

- Organization

- VMware Cloud Director instance

Just like a regular backup job, the VMware Cloud Director backup job can be scheduled or run manually.

Creating Veeam Agent Backup Jobs

Veeam Backup & Replication lets you create a Veeam Agent backup job targeted at a cloud repository. You can use the Veeam backup console to create Veeam Agent backup jobs of the following types:

- Veeam Agent backup job managed by the backup server

- Backup policy, or Veeam Agent backup job managed by Veeam Agent

Before you configure a Veeam Agent backup job, you must deploy Veeam Agent on computers whose data you want to back up. To learn more, see the Working with Protection Groups section in the Veeam Agent Management Guide.

> **NOTE**
>
> Consider the following:
>
> - This section describes the procedure of creating a backup job for Veeam Agent managed by Veeam Backup & Replication. For information about how to create a backup job for Veeam Agent operating in the standalone mode, see the Creating Backup Jobs section in the Veeam Agent for Microsoft Windows User Guide.
> - This section describes only basic steps that you must take to create a Veeam Agent backup job targeted at a cloud repository. To get a detailed description of all Veeam Agent backup job settings, see the Creating Veeam Agent Backup Jobs section in the Veeam Agent Management Guide.
> - The procedure of configuring a Veeam Agent backup job differs depending on the type of machines that the job will process: Microsoft Windows machines, Linux machines or Mac machines. Backup of IBM AIX machines and Oracle Solaris machines to a cloud repository is not supported. This section describes the procedure for a backup job that includes Microsoft Windows machines; however, the description focuses on the steps that are identical for all supported types of machines.
> - For backup to a cloud repository in the Veeam Agent management scenario, Veeam Backup & Replication uses managed subtenant accounts. For more information, see the Managed Subtenant Account section in this guide and the Backup to Veeam Cloud Connect Repository section in the Veeam Agent Management Guide.

To create a Veeam Agent backup job:

1. On the **Home** tab, click **Backup Job** and select **Windows computer** or **Linux computer**.

2. At the **Job Mode** step of the **New Agent Backup Job** wizard, specify protection settings for the backup job:

   a. In the **Type** field, select the type of protected computers whose data you want to back up with Veeam Agents: *Workstation*, *Server* or *Failover cluster*.
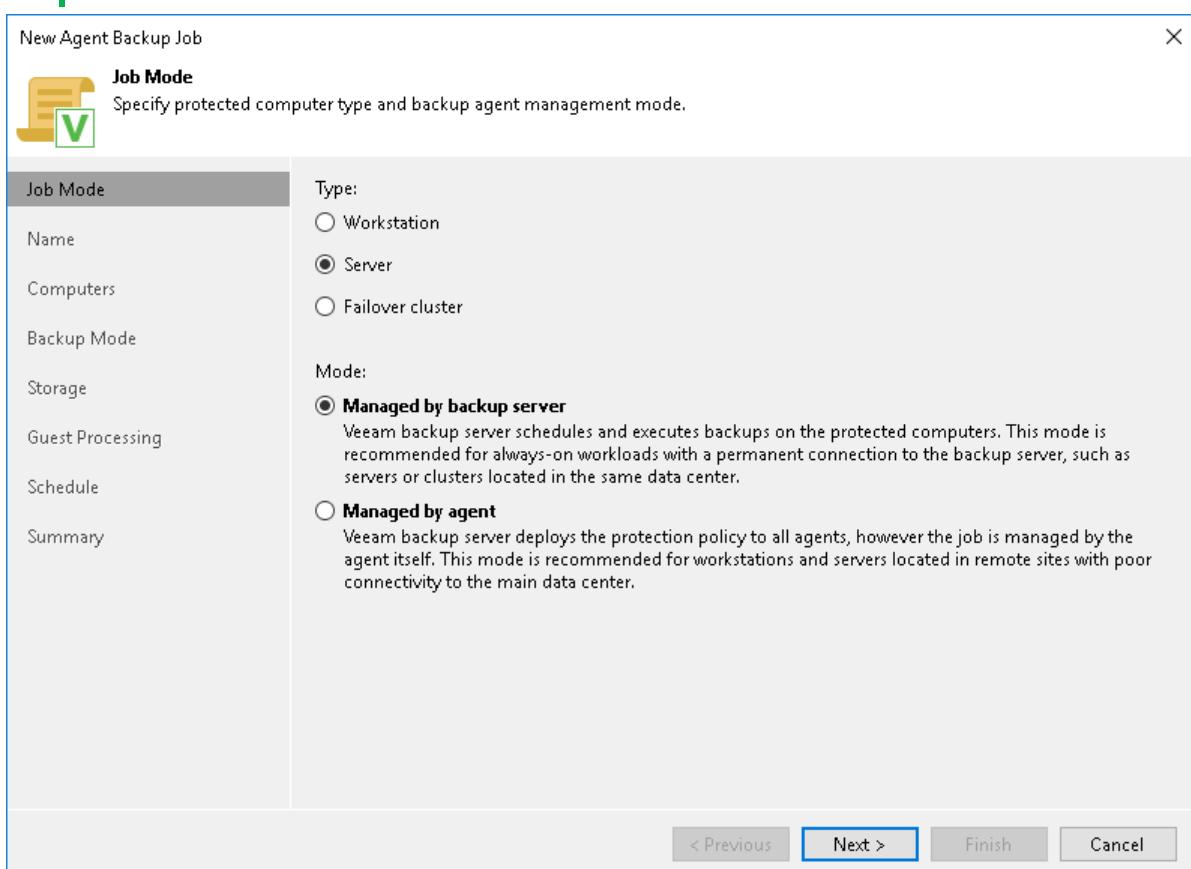
   > **NOTE**
   >
   > The **Failover cluster** option is not available for backup jobs that include Linux computers.

   b. If you selected the **Server** option in the **Type** field, in the **Mode** field, select the job mode:
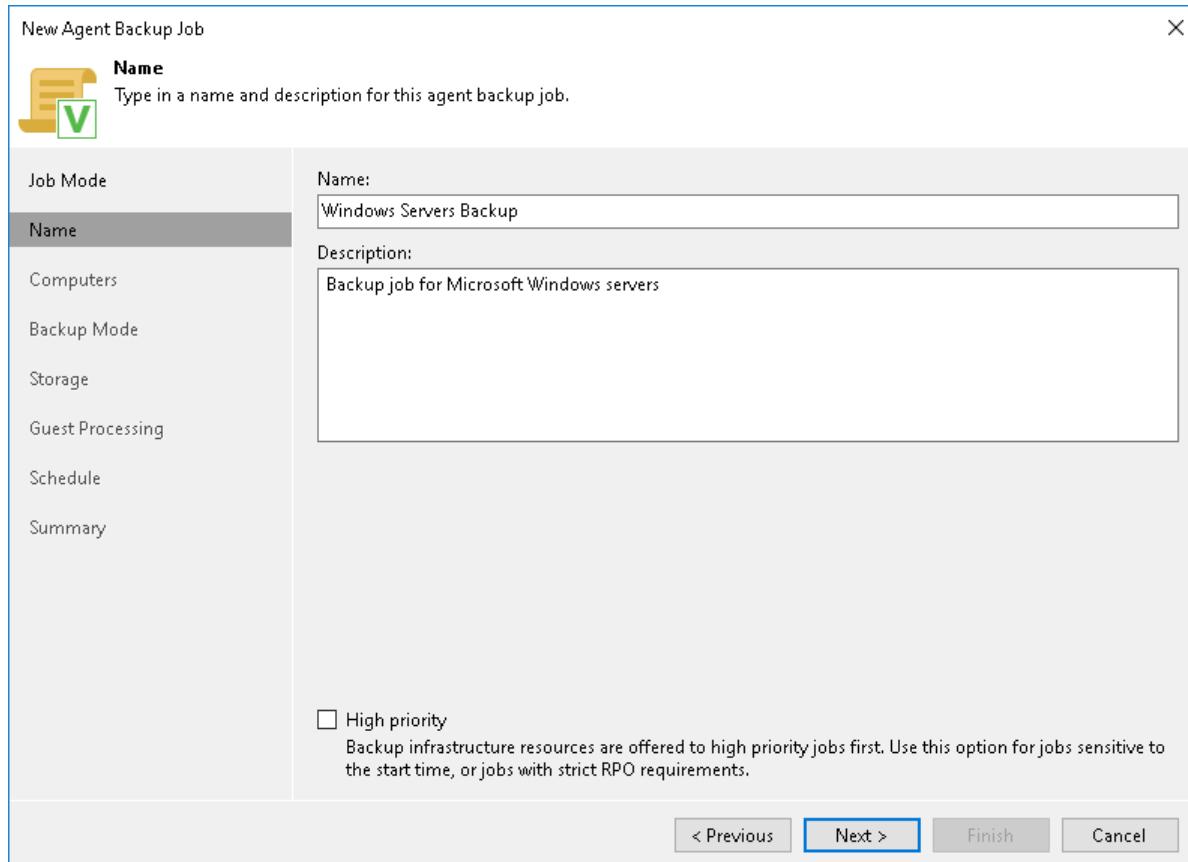
   - **Managed by backup server** — select this option if you want to configure the Veeam Agent backup job managed by the backup server. The backup job will run on the backup server in the similar way as a regular job for VM data backup.

   - **Managed by agent** — select this option if you want to configure the backup policy. The backup policy acts as a saved template that describes configuration of individual Veeam Agent backup jobs that run on protected computers.
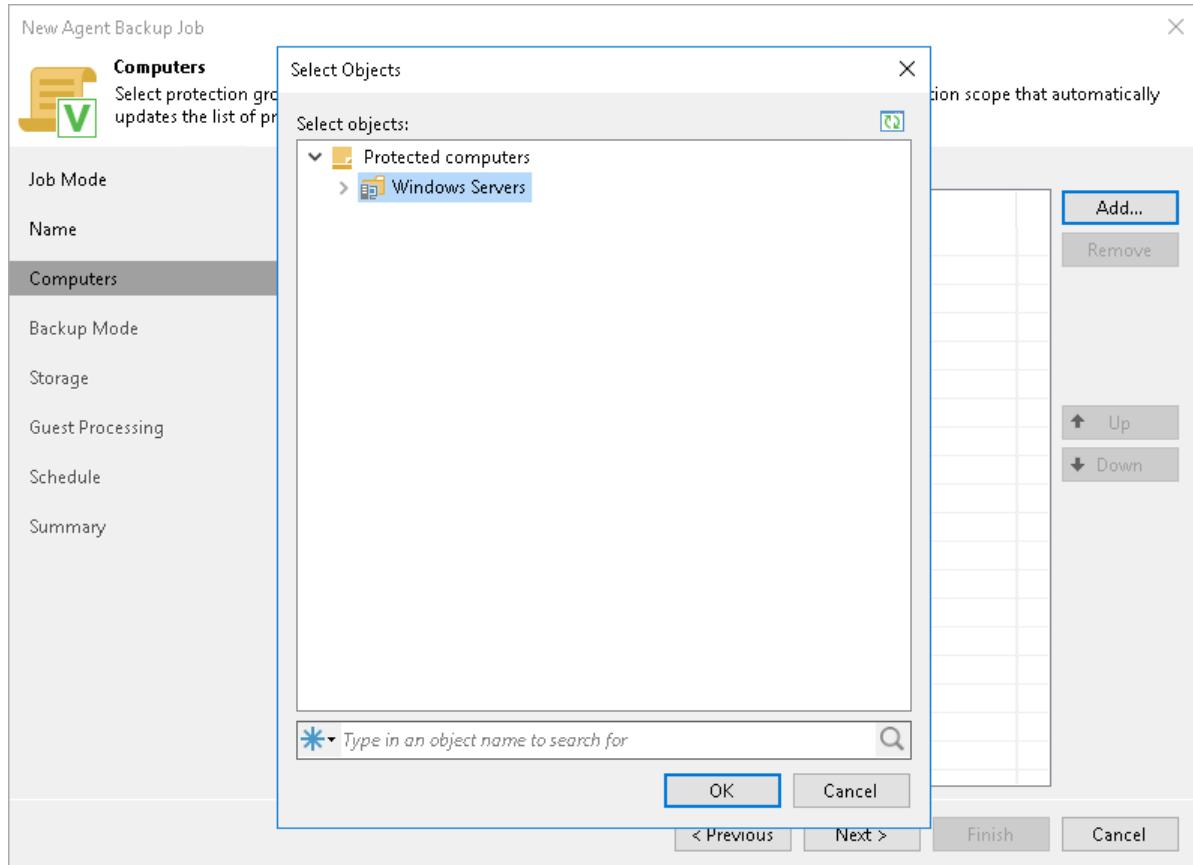
   > **NOTE**
   >
   > The **Managed by backup server** option is not available for backup jobs that include Mac computers.

3. At the **Name** step of the wizard, specify a name and description for the backup job.
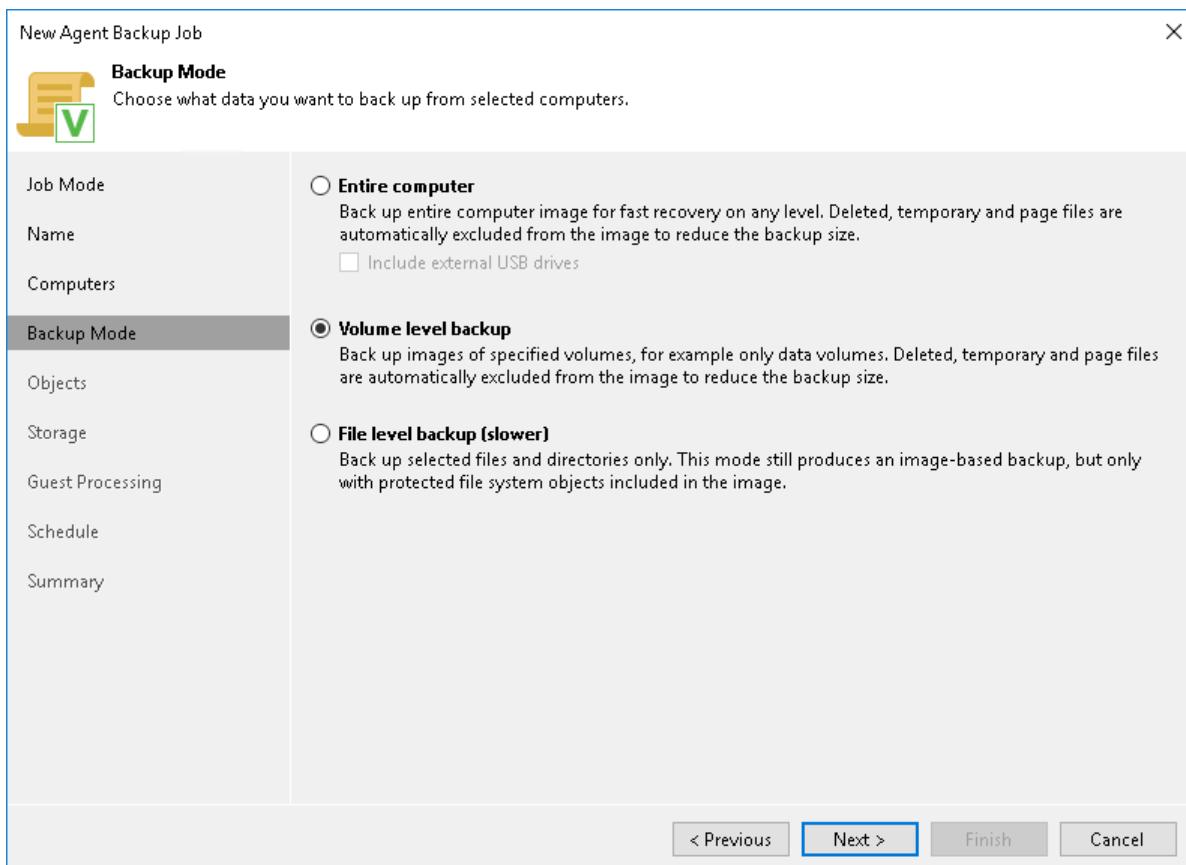
4. At the **Computers** step of the wizard, click **Add** and select one or more protection groups or individual computers whose data you want to back up. To quickly find the necessary object, use the search field at the bottom of the **Select Objects** window.
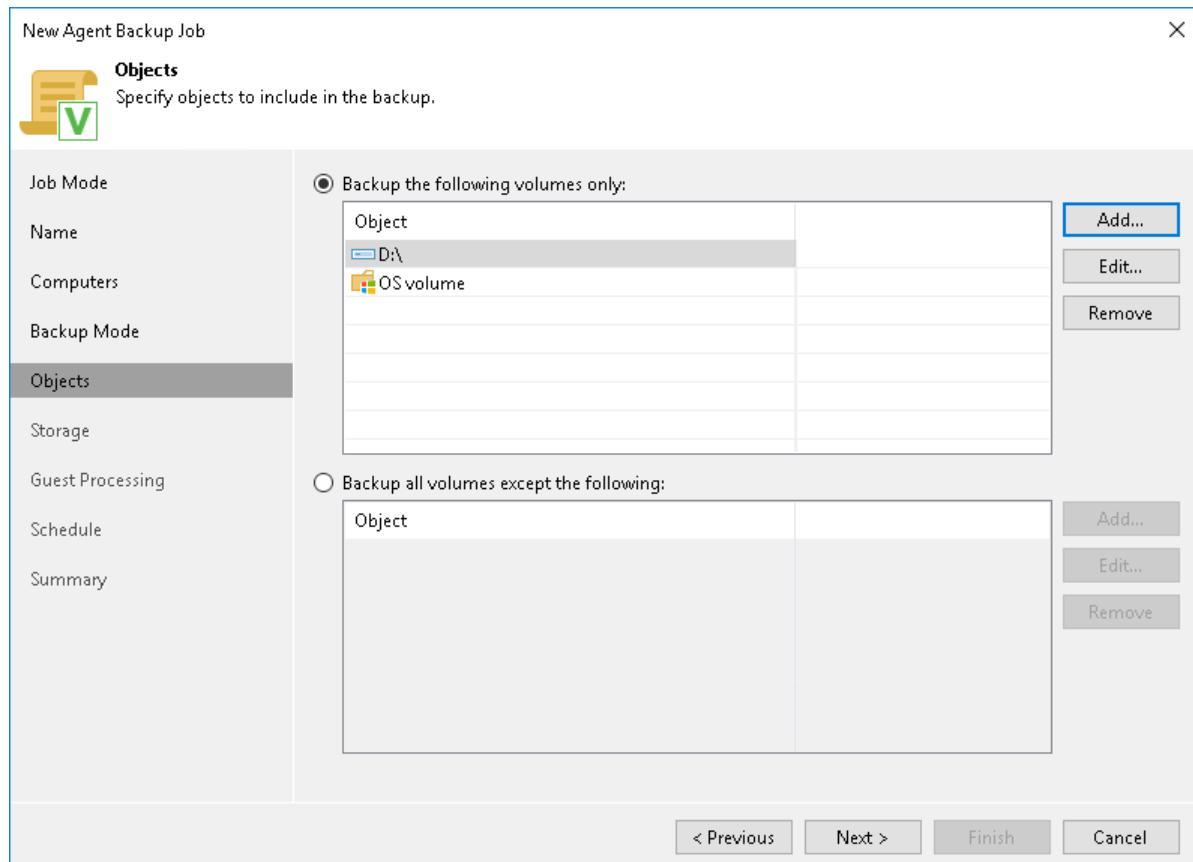
5. At the **Backup Mode** step of the wizard, select the backup mode. You can select one of the following options:

    o **Entire computer** — select this option if you want to create a backup of the entire computer image. When you restore data from such backup, you will be able to recover the entire computer image as well as data on specific computer volumes: files, folders, application data and so on.

    o **Volume level backup** — select this option if you want to create a backup of specific computer volumes, for example, all volumes except the system one. When you restore data from such backup, you will be able to recover data on these volumes only: files, folders, application data and so on.

    o **File level backup** — select this option if you want to create a backup of individual folders on your computer.
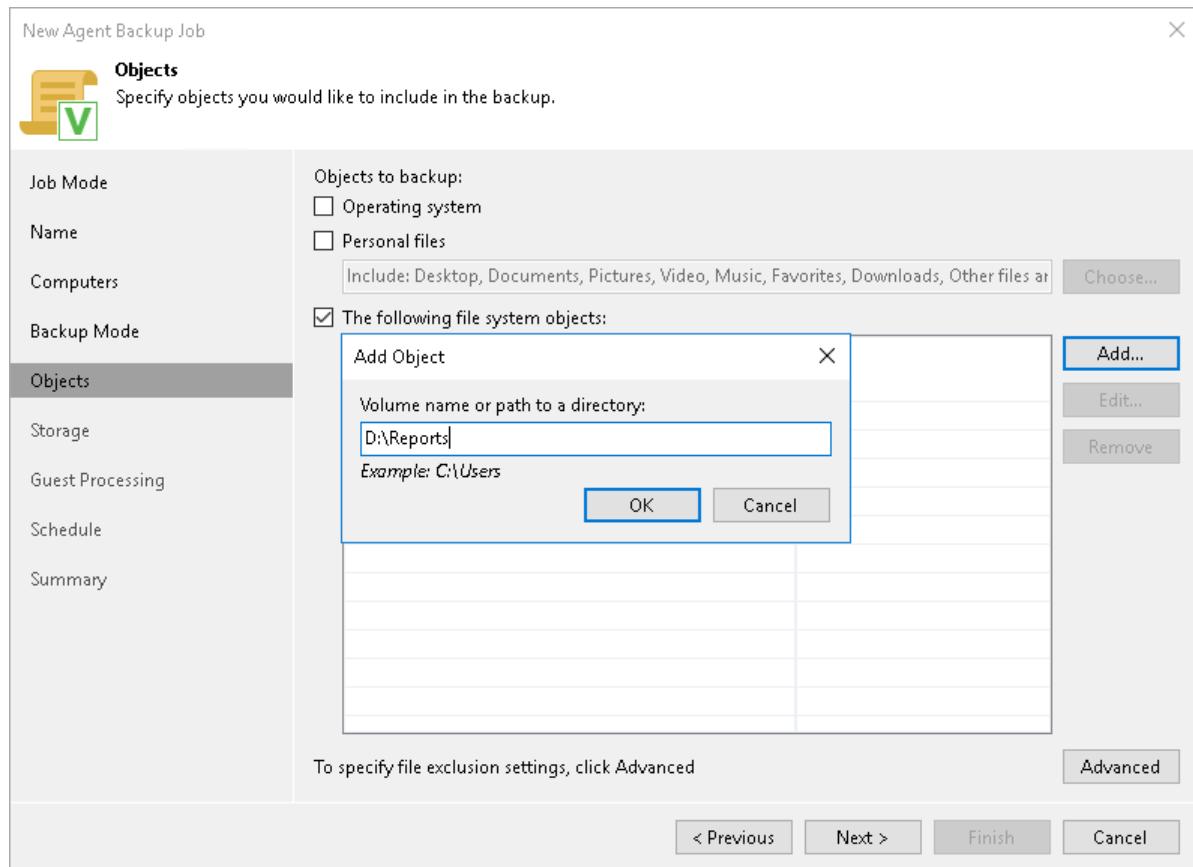
6. If you chose the **Volume level backup** or **File level backup** option at the **Backup Mode** step of the wizard, at the **Objects** step of the wizard, specify the backup scope for the Veeam Agent backup job.

   o For volume-level backup, specify what volumes you want to include in the backup. You can include in the backup operating system data or specific volumes. You can also include in the backup all volumes except for the volume that contains operating system data or selected volumes.
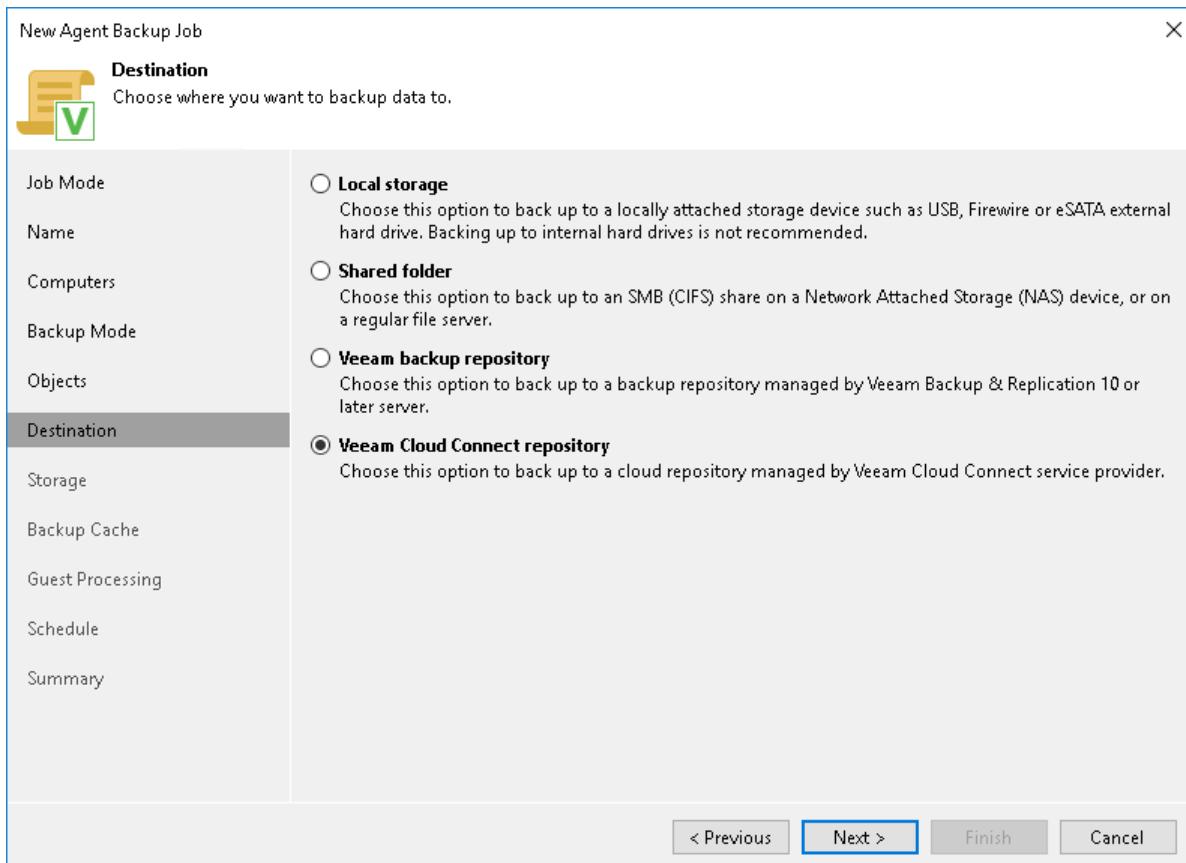
o For file-level backup, specify what folders with files or entire volumes you want to include in the backup. You can include in the backup operating system data, personal files or specific folders or volumes.
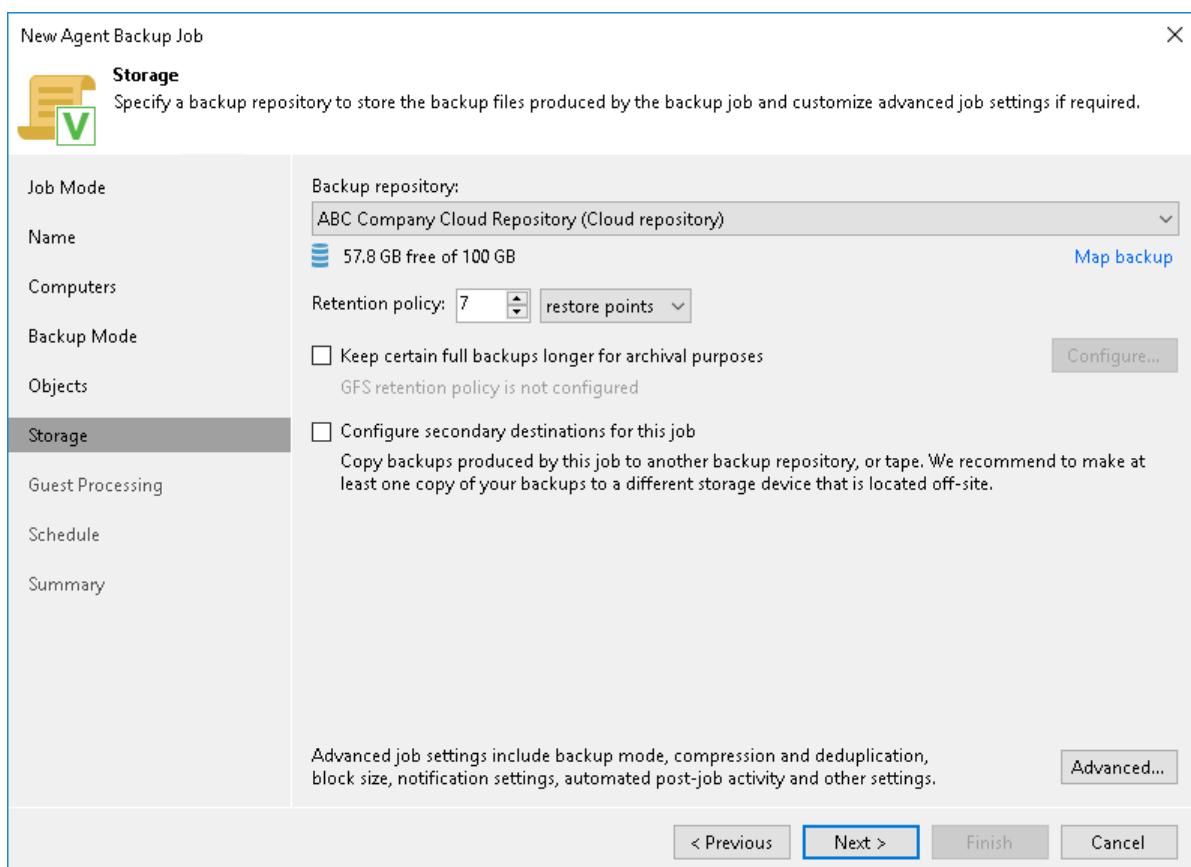
7. [For a backup policy] If you selected the **Managed by agent** option at the **Job Mode** step of the wizard, at the **Destination** step of the wizard, select the **Veeam Cloud Connect repository** option.
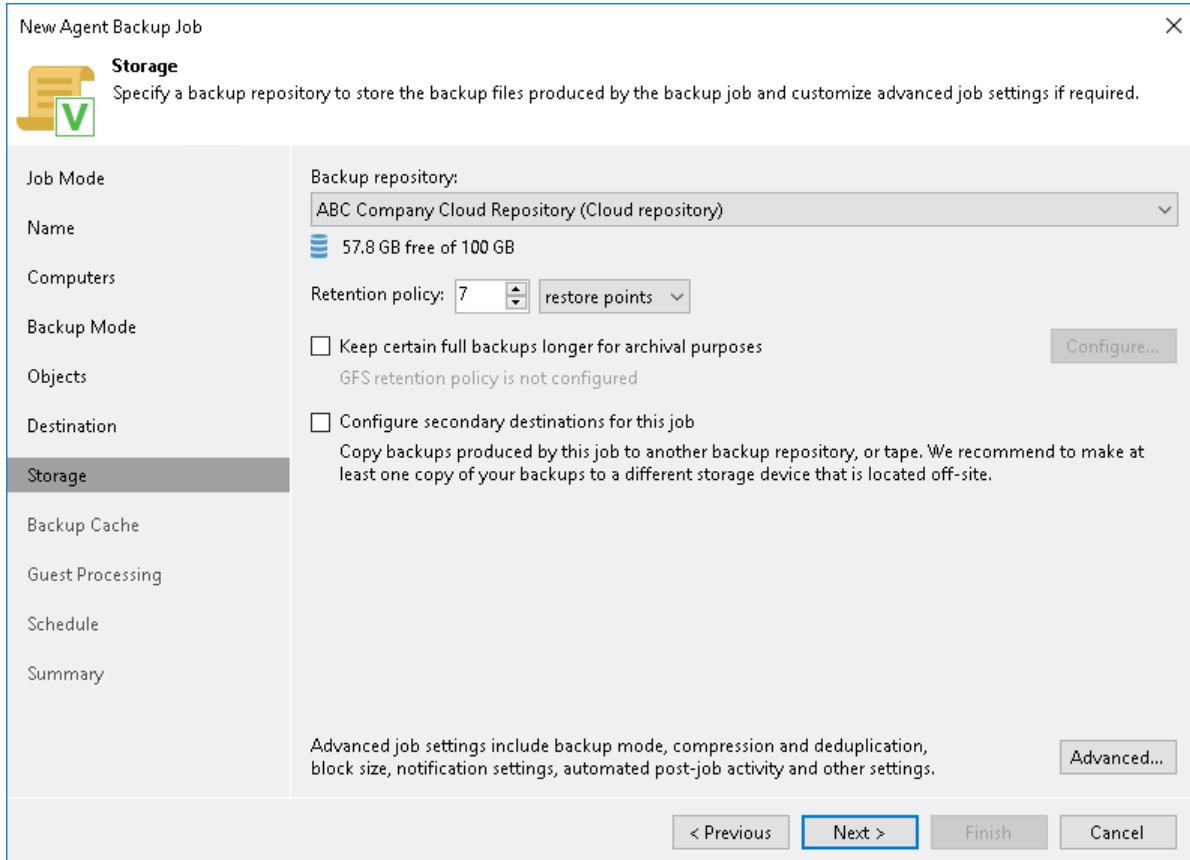
> **NOTE**
>
> If you selected the **Managed by backup server** option at the **Job Mode** step of the wizard, this step will not be displayed. You will immediately proceed to the **Storage** step of the wizard.

8. At the **Storage** step of the wizard, from the **Backup repository** list, select the cloud repository to which you plan to store backup files.

9. Specify how many restore points you want to keep on the cloud repository. To do this, in the **Retention policy** field, specify the number of restore points or the number of days for which you want to store backup files on the cloud repository. If you want to use the GFS (Grandfather-Father-Son) retention scheme, you can also specify how weekly, monthly and yearly full backups must be retained.

   o For a backup job managed by the backup server:

o For a backup policy:

New Agent Backup Job   ✕

Storage
Specify a backup repository to store the backup files produced by the backup job and customize advanced job settings if required.

Job Mode	Backup repository:
Name	ABC Company Cloud Repository (Cloud repository) ▾
Computers	🗄 57.8 GB free of 100 GB
Backup Mode	Retention policy: 7 ▴▾ restore points ▾
Objects	
Destination	☐ Keep certain full backups longer for archival purposes Configure...
Storage	GFS retention policy is not configured
Backup Cache	☐ Configure secondary destinations for this job
Guest Processing	Copy backups produced by this job to another backup repository, or tape. We recommend to make at least one copy of your backups to a different storage device that is located off-site.
Schedule	
Summary	

Advanced job settings include backup mode, compression and deduplication, block size, notification settings, automated post-job activity and other settings.   Advanced...

< Previous   Next >   Finish   Cancel

10. Click **Advanced**.

11. To encrypt the resulting backup file on the cloud repository, on the **Storage** tab, select the **Enable backup file encryption** check box. From the **Password** field, select a password that you want to use to encrypt the backup file. If you have not created a password beforehand, click **Add** or use the **Manage passwords** link to specify a new password.
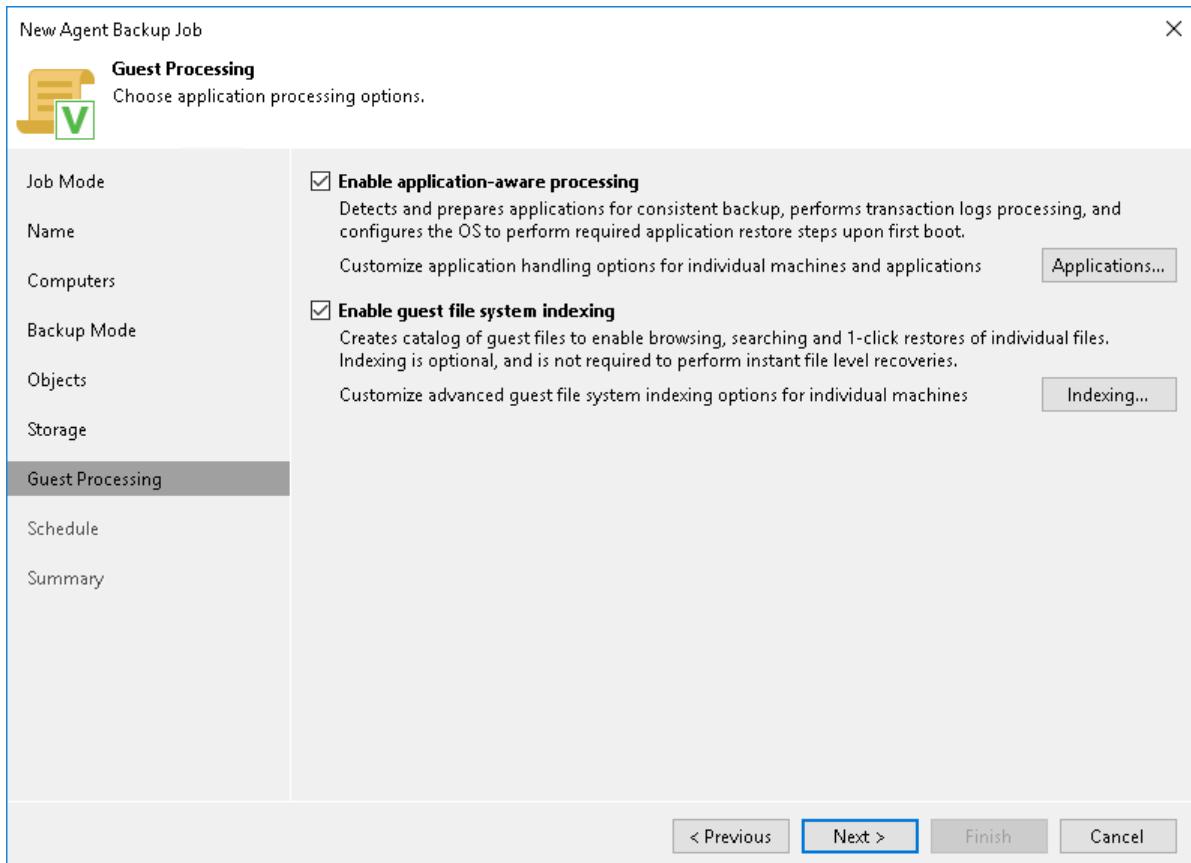
12. [For a backup policy] If you want to enable the backup cache for the backup policy, at the **Backup Cache** step of the wizard, specify backup cache settings.

> **NOTE**
>
> If you selected the **Managed by backup server** option at the **Job Mode** step of the wizard, this step will not be displayed. You will immediately proceed to the next step of the wizard.
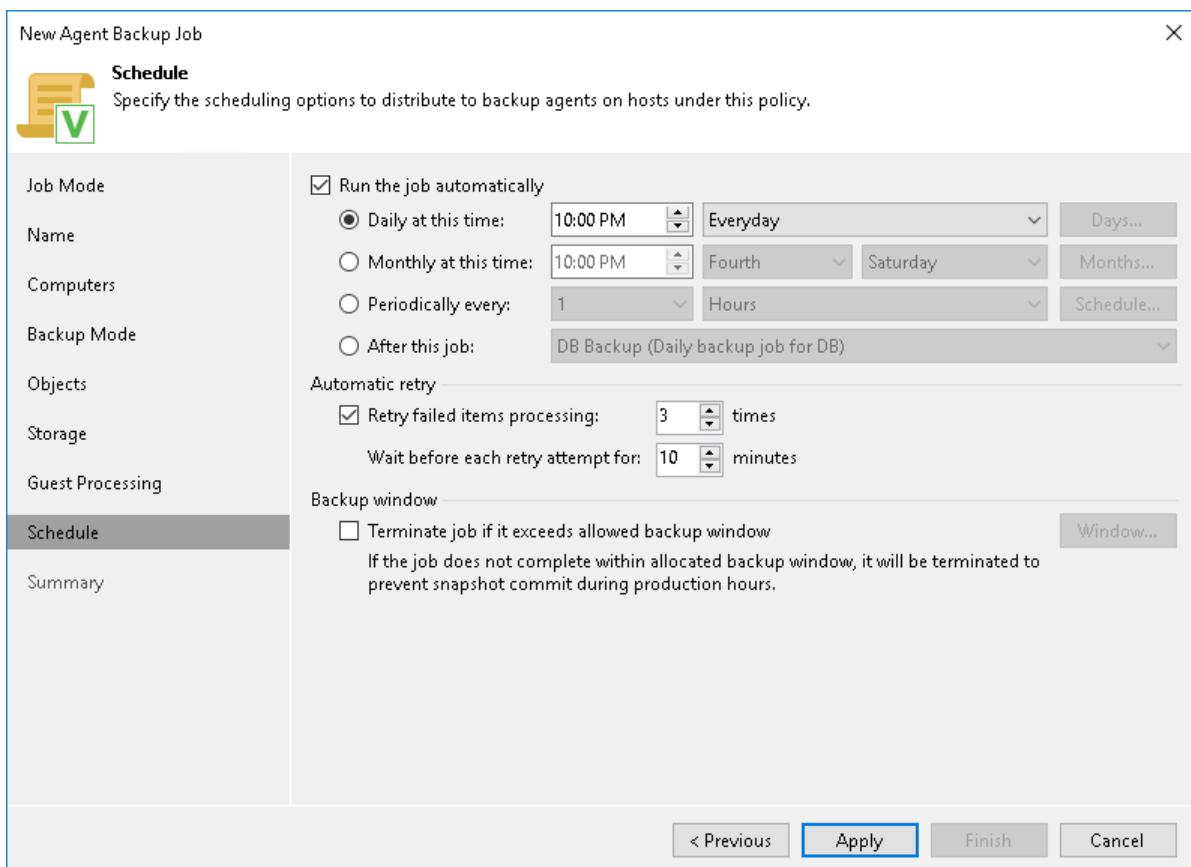
13. If you selected the **Server** or **Failover cluster** option at the **Job Mode** step of the wizard, you can enable application-aware processing settings at the **Guest Processing** step of the wizard. Available guest OS processing settings differ for backup jobs that process Microsoft Windows machines and backup jobs for Linux machines.
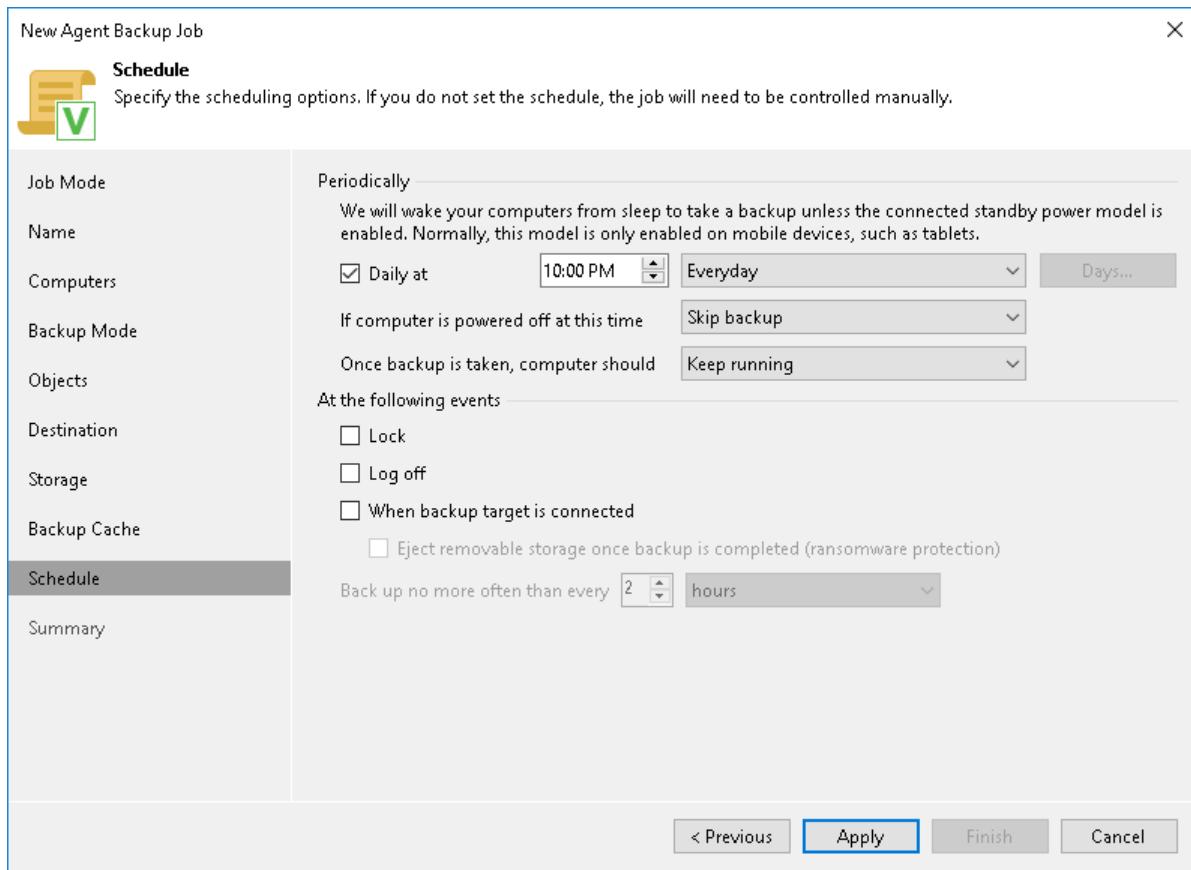
14. At the **Schedule** step of the wizard, specify the schedule according to which you want to perform backup:

    o If you selected the **Server** or **Failover cluster** option at the **Job Mode** step of the wizard, select the **Run the job automatically** check box and specify the necessary scheduling settings for the job. If you do not select this check box, you will have to run the backup job manually to create a backup file in the cloud.

o If you selected the **Workstation** option at the **Job Mode** step of the wizard, you can specify time and days when the backup job must start, as well as settings for events that trigger the backup job launch.

15. [For a backup job managed by the backup server] At the **Summary** step of the wizard, select the **Run the job when I click Finish** check box if you want to start the created job right after you complete working with the wizard.

16. Click **Finish**.

Creating Backup Copy Jobs

To follow the 3-2-1 backup best practice, you can configure a backup copy job and target it at the cloud repository. Backup copy jobs allow you to create several instances of the same backup file in different locations, onsite or offsite. For example, you can configure a backup job to create a VM backup on the local backup repository, and use the backup copy job to copy the created VM backup from the local backup repository to the cloud repository.
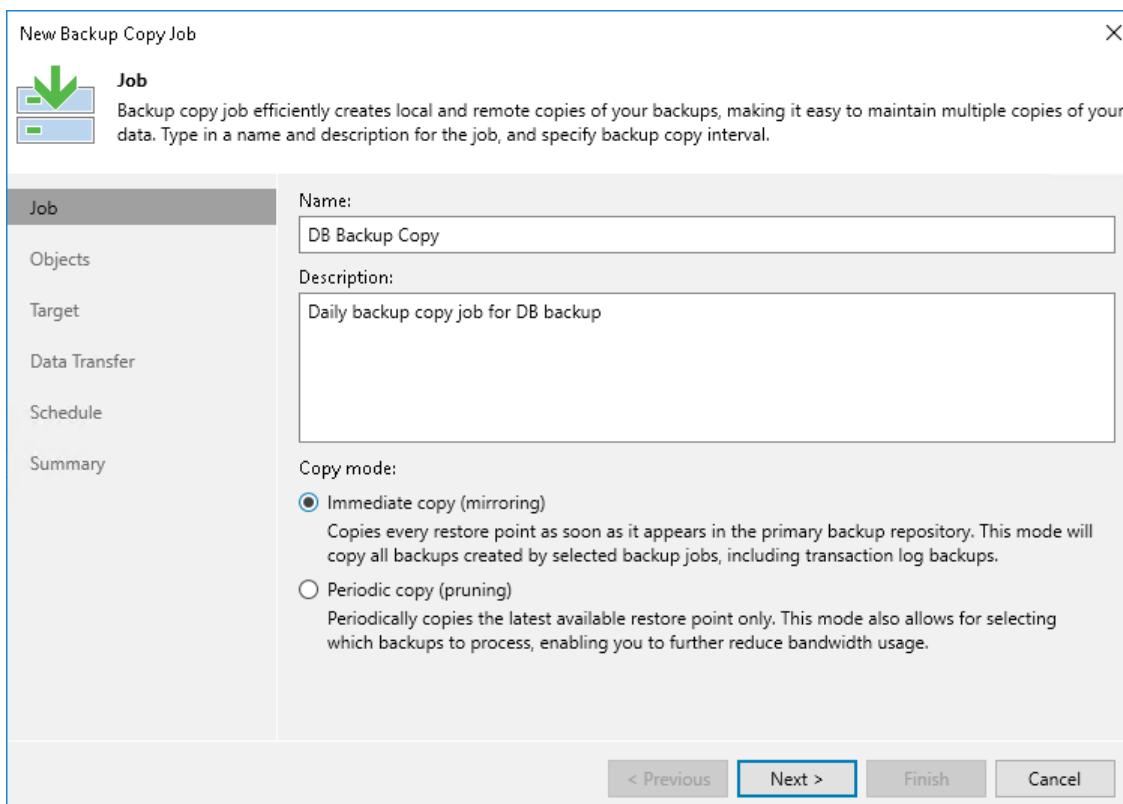
To learn more about backup copy in the Veeam Cloud Connect Backup scenario, see Backup Copy to Cloud Repository.
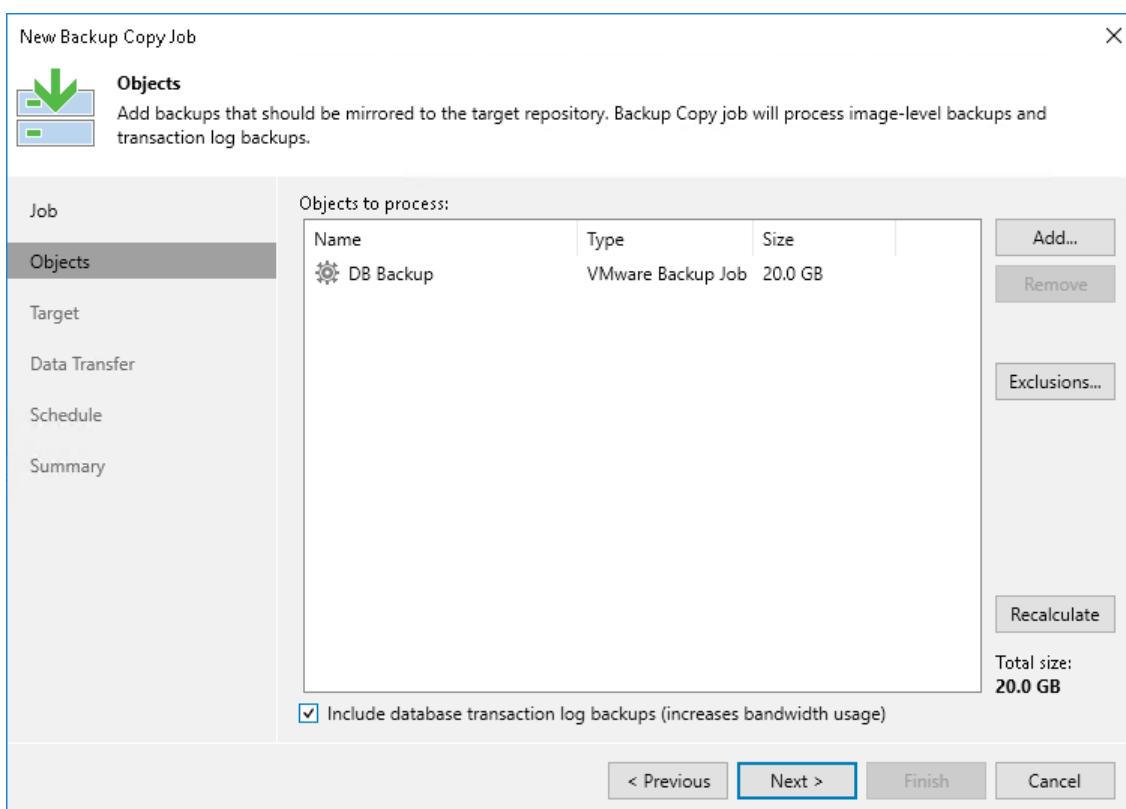
> **NOTE**
>
> This section describes only basic steps that you must take to create a backup copy job. To get a detailed description of all backup copy job settings, see the Creating Backup Copy Jobs section in the Veeam Backup & Replication User Guide.

To create a backup copy job:

1. On the **Home** tab, click **Backup Copy**.

2. At the **Job** step of the wizard, specify a name and description for the backup copy job and select the backup copy mode:

   o Select **Immediate copy** to copy new restore points and, if required, database log backups as soon as they appear in the source backup repository.

   o Select **Periodic copy** to copy the most recent restore points according to a specified schedule.
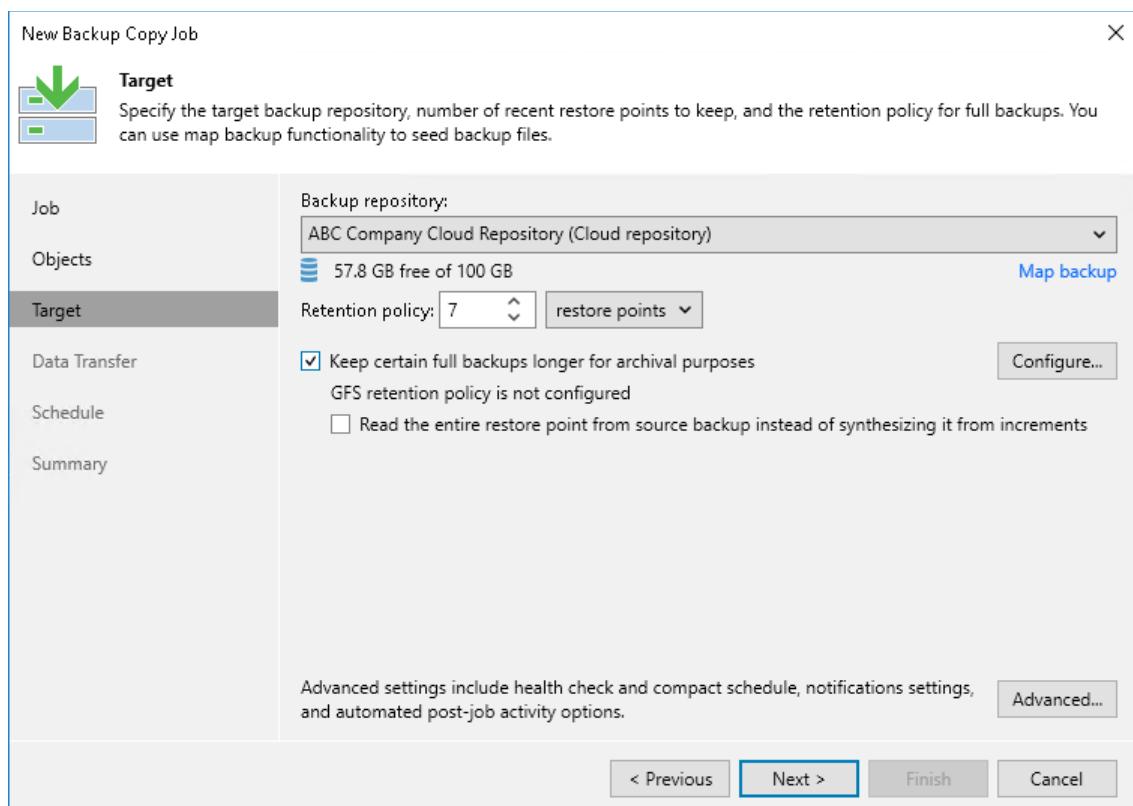
3. At the **Objects** step of the wizard, specify what data Veeam Backup & Replication will copy to the cloud repository.

   o Click **Add** and select **From jobs** to select backup jobs that contain VMs or physical machines whose restore points you want to copy from the local backup repository to the cloud repository.

   To quickly find the necessary object, use the search field at the bottom of the **Select Jobs** window.

   o Click **Add** and select **From repositories** to select backup repositories that contain backups of VMs or physical machines that you want to copy to the cloud repository.

   To quickly find the necessary object, use the search field at the bottom of the **Select Repository** window.

4. [For the immediate copy mode] If you enabled database log backup for the source backup jobs and want to copy log backups to the cloud repository, select the **Include database transaction log backups** check box.
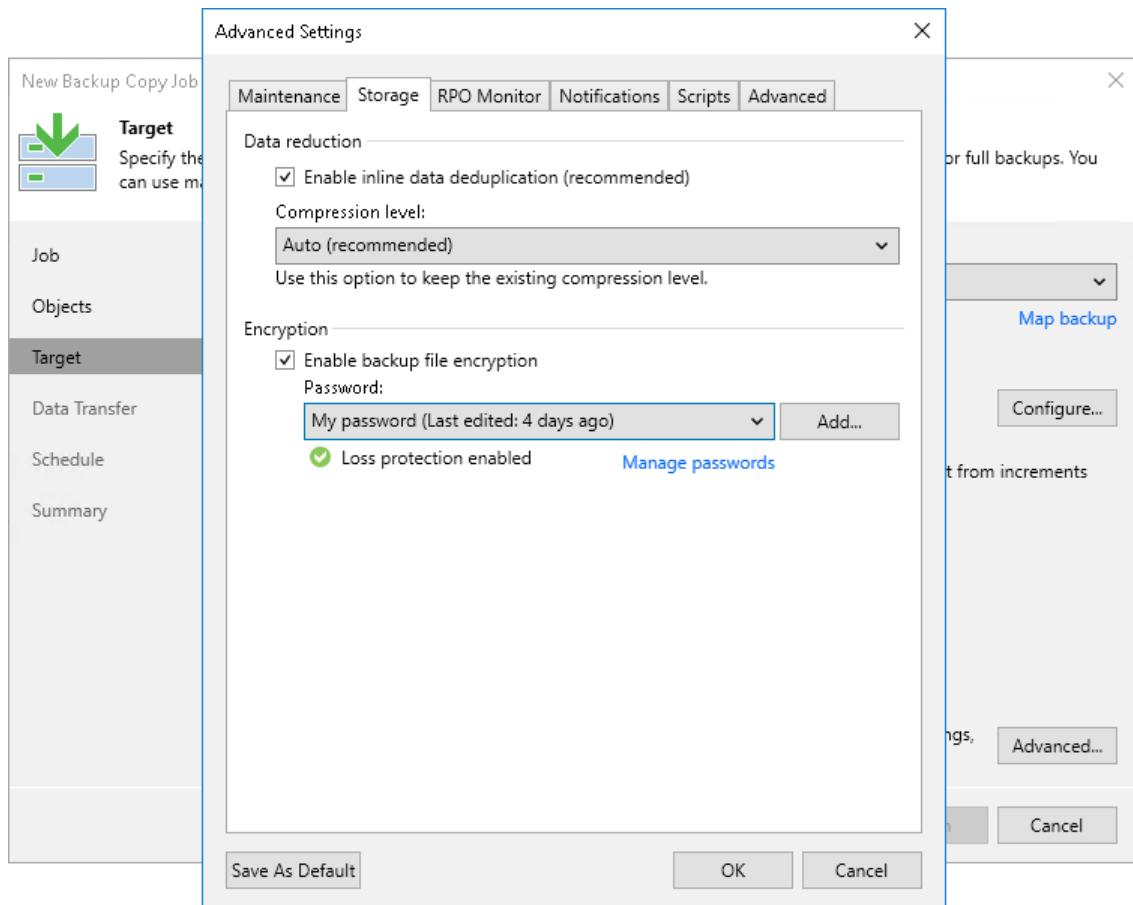
5. If you want to exclude specific VMs from a backup job or backup repository added to the job, click **Exclusions** and specify what objects you want to exclude.

6. At the **Target** step of the wizard, from the **Backup repository** list, select the cloud repository to which you want to copy the backup.

7. To use the GFS (Grandfather-Father-Son) retention scheme, select the **Keep certain full backups longer for archival purposes** check box and click **Configure**. In the **Configure GFS** window, define when to create full backups for archival purposes and how long to keep these backups.

    It is recommended that you enable GFS retention settings for the backup copy job if the SP has enabled the deleted backups protection option in the properties of your tenant account. This way, Veeam Backup & Replication will be able to protect backups created by the job against an attack when a hacker reduces the job's retention policy and creates a few incremental backups to remove backed-up data from the backup chain.
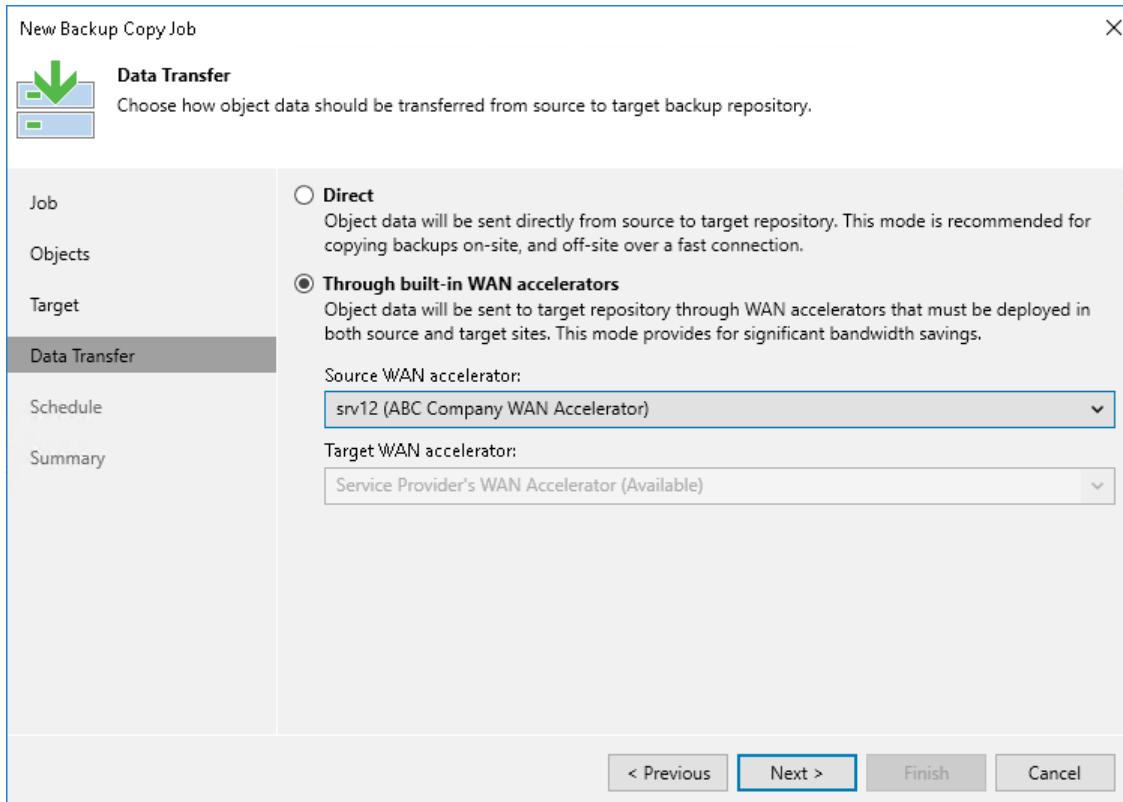
    If you do not enable GFS retention settings for the backup copy job, the job will complete with a warning. In the job statistics window, Veeam Backup & Replication will display a notification advising to use the GFS retention scheme for the job.

8. To encrypt the resulting backup file on the cloud repository, click **Advanced**. On the **Storage** tab, select the **Enable backup file encryption** check box. From the **Password** field, select a password that you want to use to encrypt the backup file. If you have not created a password beforehand, click **Add** or use the **Manage passwords** link to specify a new password.
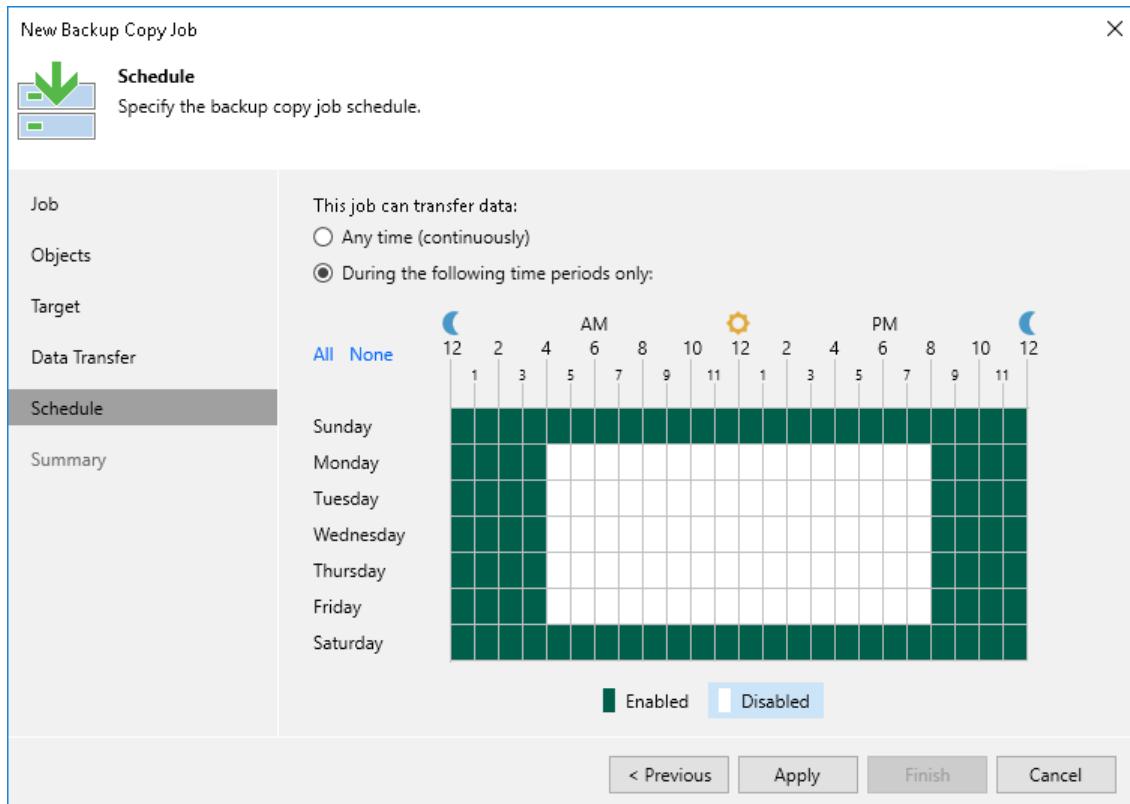
9. At the **Data Transfer** step of the wizard, specify a data transfer path for the backup copy job:

   o If the cloud repository does not use WAN accelerators, select **Direct**.

   o If the cloud repository uses WAN accelerators, select **Through built-in WAN accelerators**. In the **Source WAN accelerator** field, select the WAN accelerator that you have configured on your side.
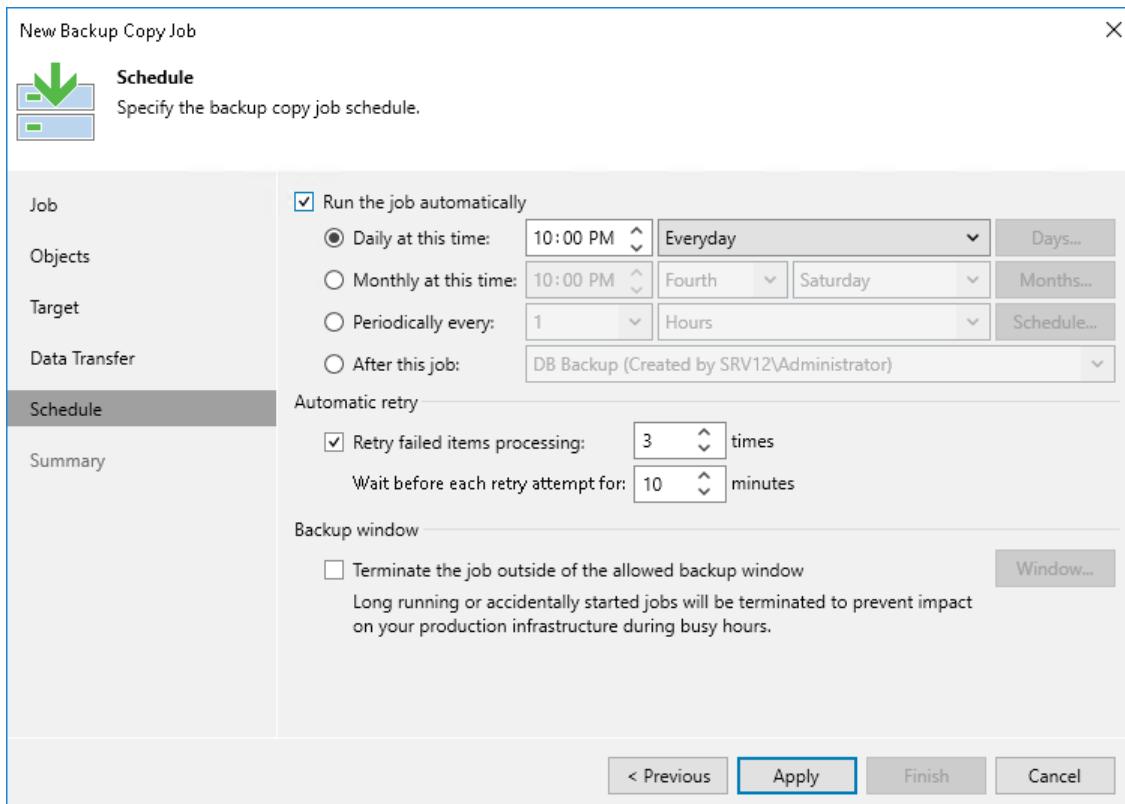
10. At the **Schedule** step of the wizard, specify schedule settings for the backup copy job.

   o [For the immediate copy mode] Define the time span in which the backup copy job must not transport data over the network. You can use this option, for example, to disable the backup copy job during production hours to avoid producing workload on the production environment.

o   [For the periodic copy mode] Select the **Run the job automatically** check box and specify the necessary scheduling settings for the job. If you do not select this check box, you will have to run the backup copy job manually to create a copy of your data in the cloud.

11. At the **Summary** step of the wizard, select the **Enable the job when I click Finish** check box (for the immediate copy mode) or **Run the job when I click Finish** check box (for the periodic copy mode) if you want to start the created job right after you complete working with the wizard.

12. Click **Finish**.

Performing Restore

You can perform the following data recovery tasks with backups that reside the cloud repository:

- Restore:
  - Entire VM restore
  - VMware Cloud Director restore (for VMware vSphere platform)
  - VM files restore
  - VM disks restore (for VMware vSphere platform)
  - VM guest OS files restore (Microsoft Windows FS only. Multi-OS restore is not supported.)
  - Application items restore
  - Volume restore (for Veeam Agent backups)
  - Disk export (for Veeam Agent backups)
  - Guest OS files restore (for Veeam Agent backups)
- Backup export
- File copy (manual operations)

> **NOTE**
>
> Consider the following:
>
> - If you allowed the SP to manage the tenant backup server, the SP can use the SP backup console to perform instant recovery from tenant backups. To learn more, see Performing Instant Recovery from Tenant Backups.
> - If you create Veeam Agent backups in the cloud repository, you can also restore data from such backups using Veeam Recovery Media. To learn more, see the *Restoring from Veeam Recovery Media* sections in the Veeam Agent for Microsoft Windows User Guide and Veeam Agent for Linux User Guide.

Backups created on the cloud repository are displayed under the **Backups** > **Cloud** node in the inventory pane of the **Home** view.

Backups created by Veeam Agent operating in the standalone mode are displayed under the **Agents** node in the working area of the **Backups** > **Cloud** node.

Performing Entire VM Restore
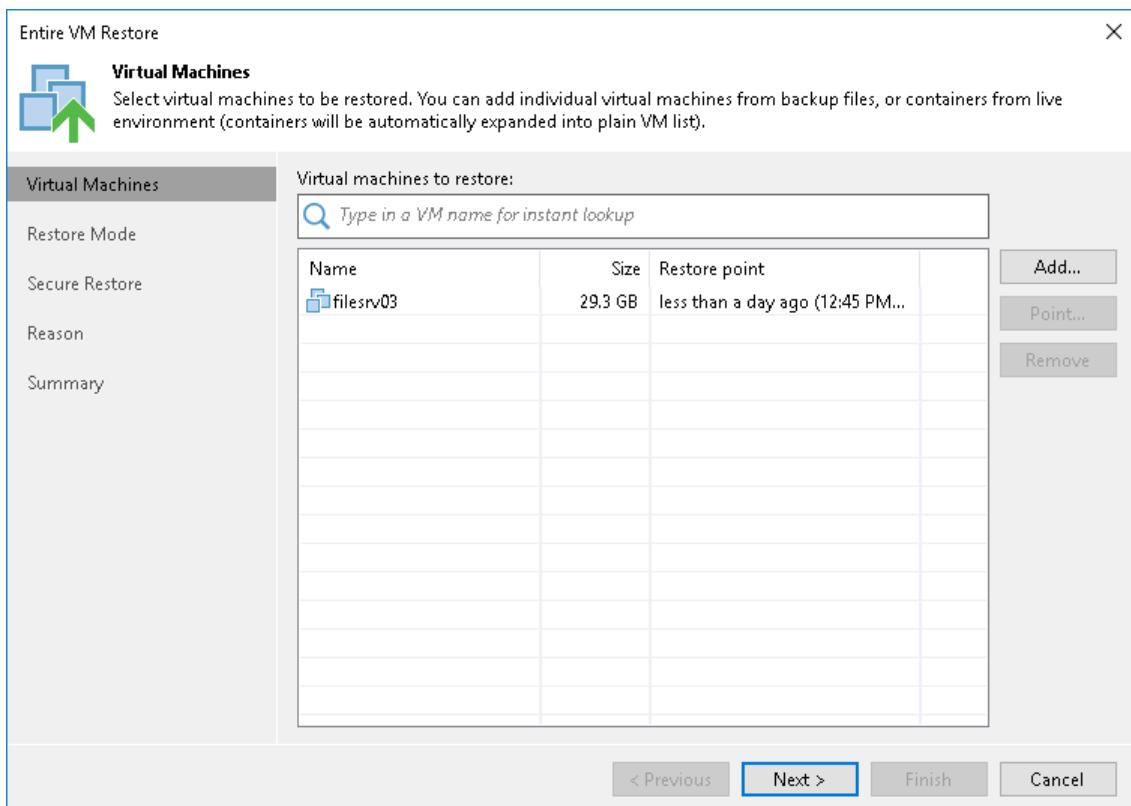
You can restore one VM or several VMs from the backup, both to the original location or to a new location. A VM can be recovered to the latest state or to any good to know point in time.
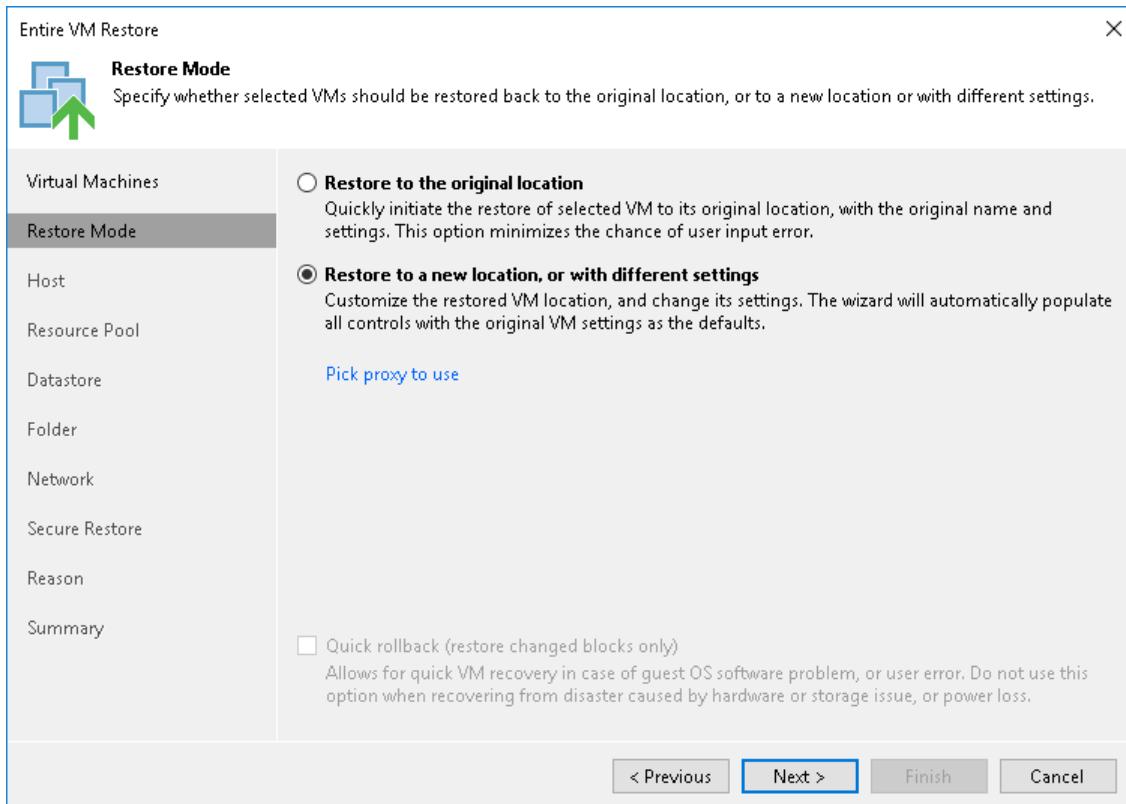
> **NOTE**
>
> This section describes only basic steps that you must take to restore the VM. To get a detailed description of all settings of the restore process, see the Restoring Entire VM section in the Veeam Backup & Replication User Guide.

To restore one or several VMs from the backup:
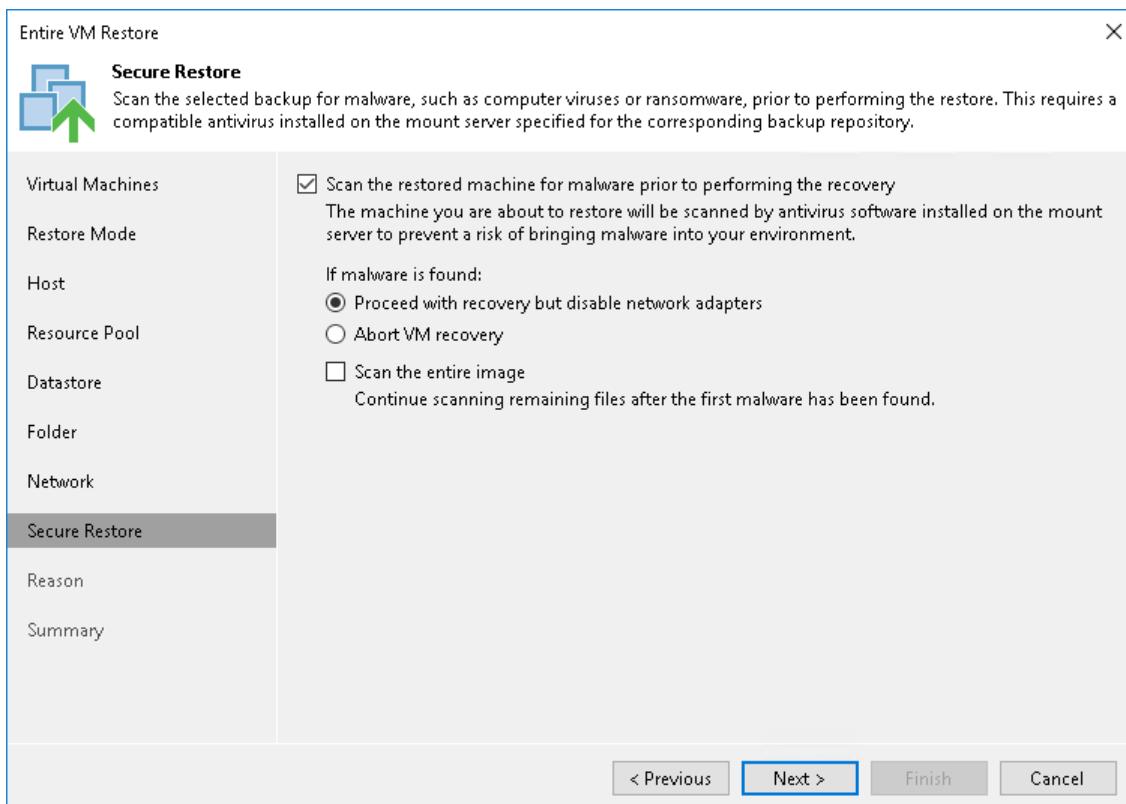
1. Open the **Home** view.

2. Select the **Backups** node in the inventory pane. Expand the backup job in the working area, right-click the necessary VM in the backup job and select **Restore entire VM**.

3. At the **Virtual Machines** step of the wizard, select the VM in the list, click **Point** on the right and select the necessary restore point.
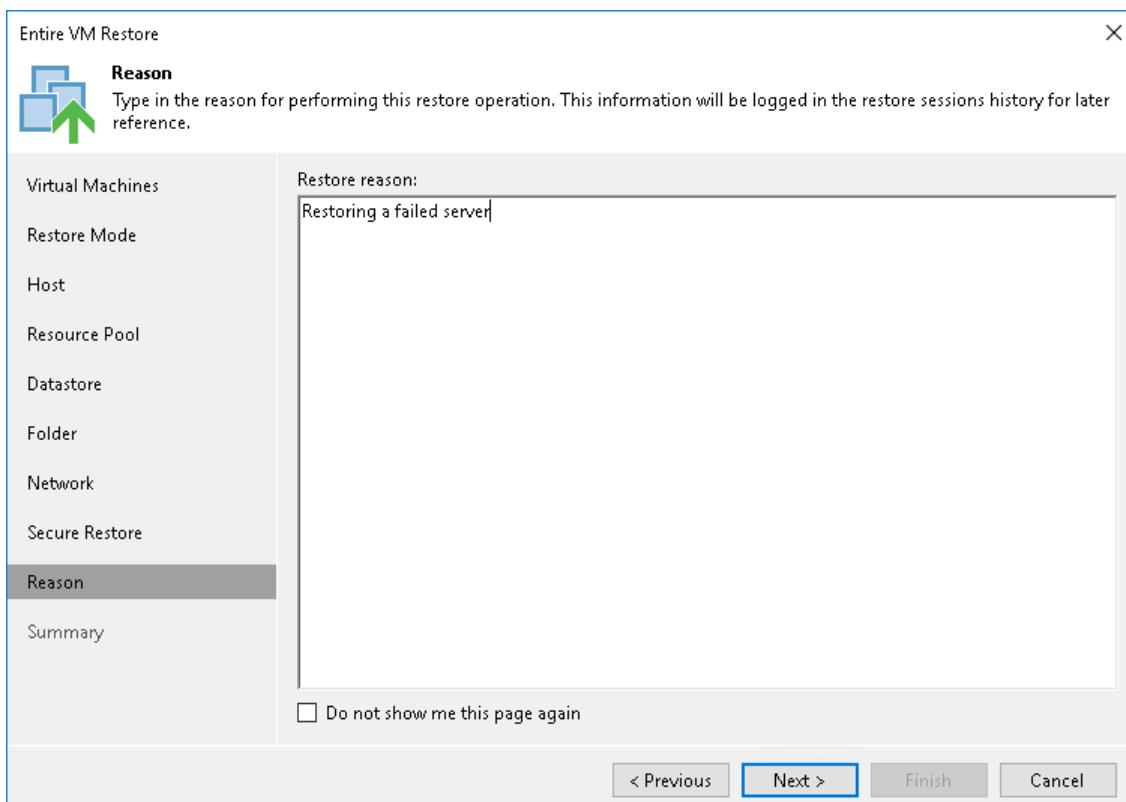
4. At the **Restore Mode** step of the wizard, choose to restore the VM to its original location or to a new location.

5. [For VM restore to the original location] Select the **Quick rollback** check box if you want to use incremental restore for the VM. Veeam Backup & Replication will query CBT to 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. Incremental restore significantly reduces the restore time and has little impact on the production environment.

6. If you have selected to restore the VM to another location, at the next steps of the wizard, define the host, resource pool, datastore and folder to which the VM must be restored and specify to which network(s) the VM must be connected.

7. If you want to scan VM data with antivirus software before restoring the VM to the production environment, at the **Secure Restore** step of the wizard, specify secure restore settings.

8. At the **Reason** step of the wizard, specify the reason for restoring the VM.

9. At the **Summary** step of the wizard, select the **Power on target VM after restoring** check box if necessary.

10. Click **Finish**.

Performing Restore of VMware Cloud Director VMs

The VMware Cloud Director VM restore is practically the same as a regular VM restore. You can restore separate VMs to vApps, as well as VM data.

For restore, Veeam Backup & Replication uses VM metadata saved to a backup file and restores specific VM attributes. As a result, you get a fully-functioning VM in VMware Cloud Director, do not need to import the restored VM to VMware Cloud Director and adjust the settings manually.

Backed up objects can be restored to the same VMware Cloud Director hierarchy or to a different Cloud Director environment. For restore or Cloud Director objects from the cloud repository, the following options are supported:

- Full restore for vApps and VMs

- Restore of VM disks

- Restore of VM files

- Guest OS file-level restore for VMs (Microsoft Windows FS only. Multi-OS restore is not supported.)

Restoring VM Files

You can restore specific VM files from the backup: VMDK, VMX and others (for VMware VMs) and VHD/VHDX, XML and others for Microsoft Hyper-V VMs. This scenario can be used, for example, if one of your VM files is missing or is corrupted and you need to bring it back.
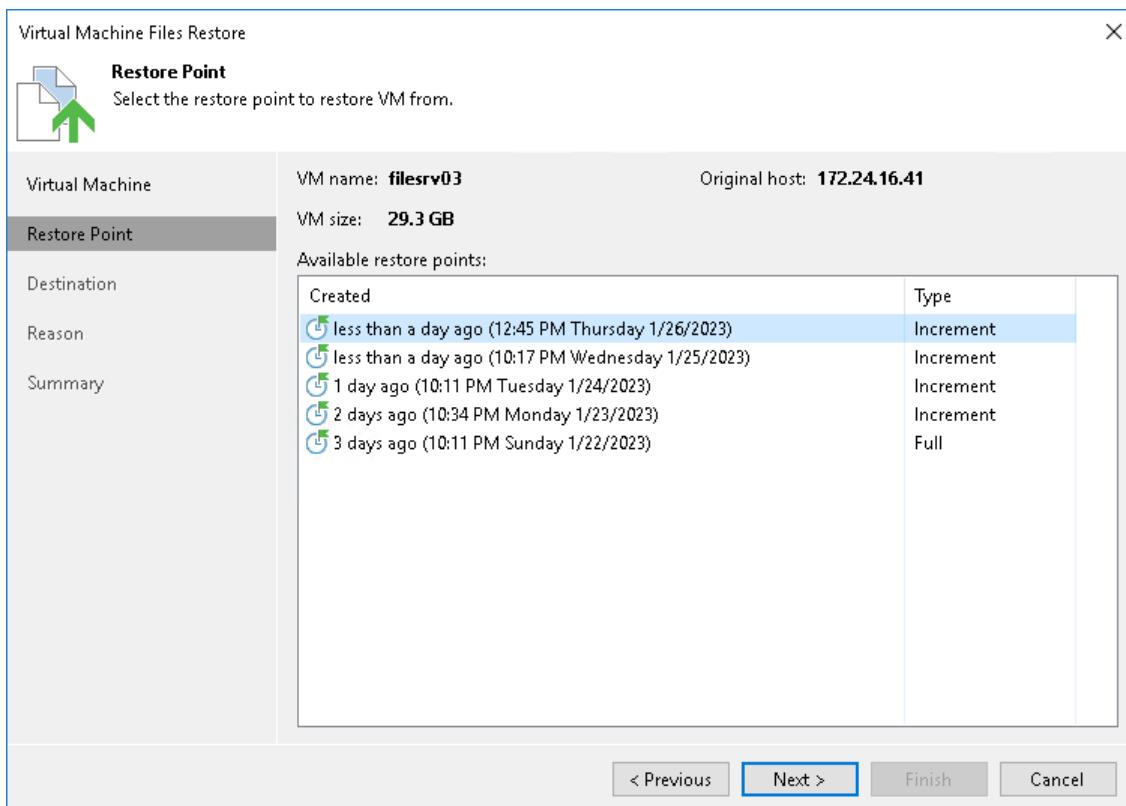
VM files can be recovered to the latest state or to any good to know point in time. You can restore them to the original location or to a new location.
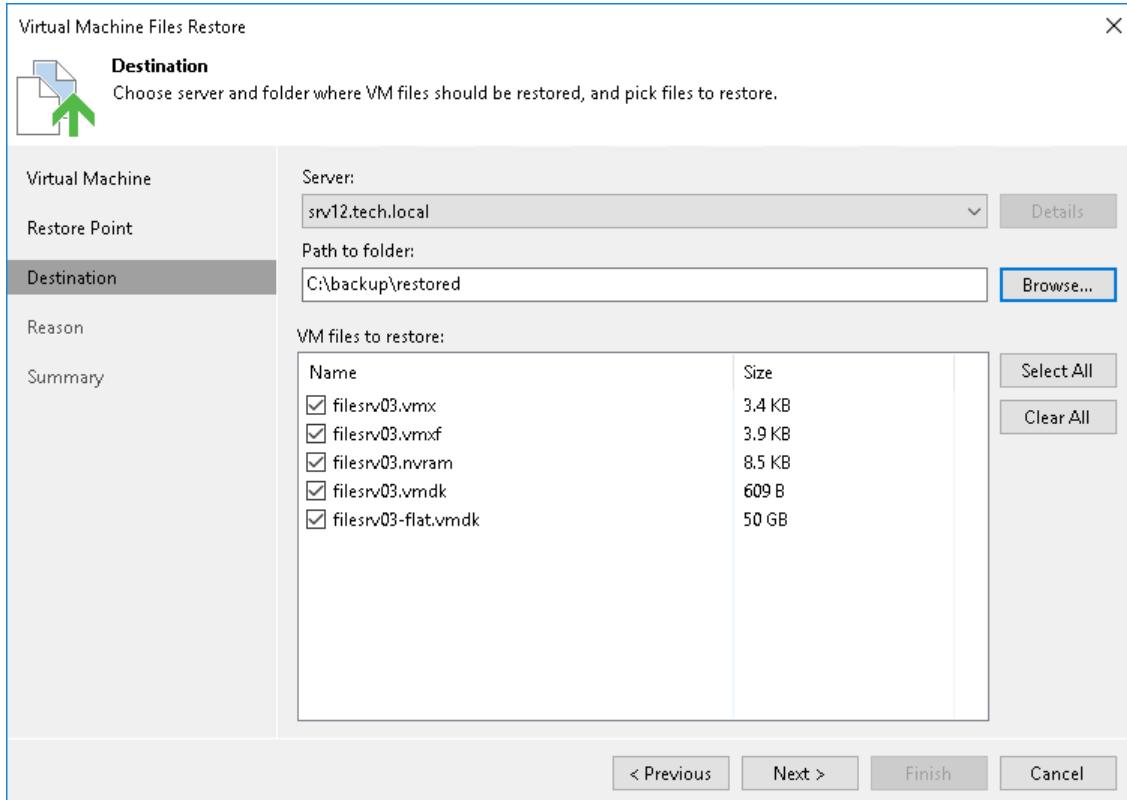
> **NOTE**
>
> This section describes only basic steps that you must take to restore VM files. To get a detailed description of all settings of the restore process, see the Restoring VM Files section in the Veeam Backup & Replication User Guide.

To restore VM files:

1. Open the **Home** view.

2. Select the **Backups** node in the inventory pane. Expand the backup job in the working area, right-click the necessary VM in the backup job and select **Restore VM files**.

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

4. At the **Destination** step of the wizard, select the server to which you want to restore the VM files.

5. Specify a path to a folder on the selected host where VM files must be restored, for example: `C:\backup\restored`.

6. In the **VM files to restore** section, select a check box next to the necessary VM files.

7. At the **Reason** step of the wizard, specify the reason for future reference and click **Next**.

8. At the **Summary** step of the wizard, click **Finish** to restore the VM files.

Restoring VM Disks
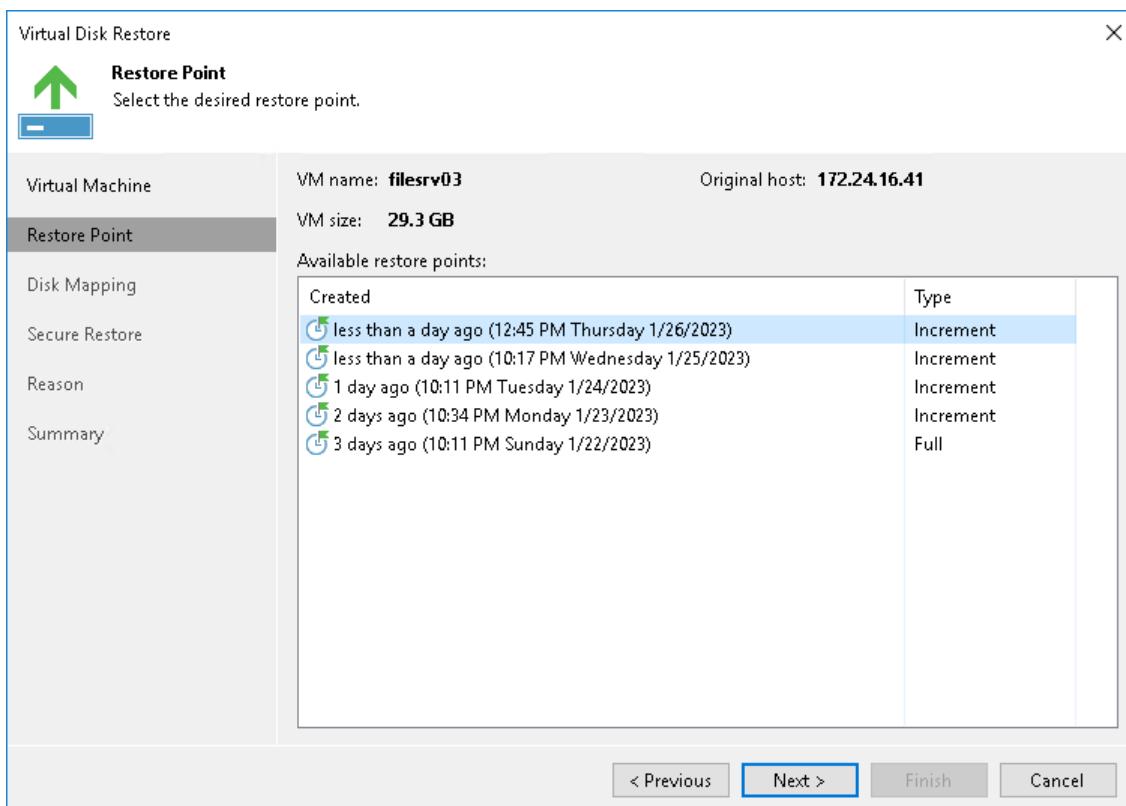
You can restore virtual hard disks of VMware VMs from the backup. The restored disks can be attached to the original VM (for example, if you need to replace a corrupted disk) or mapped to any other VM.
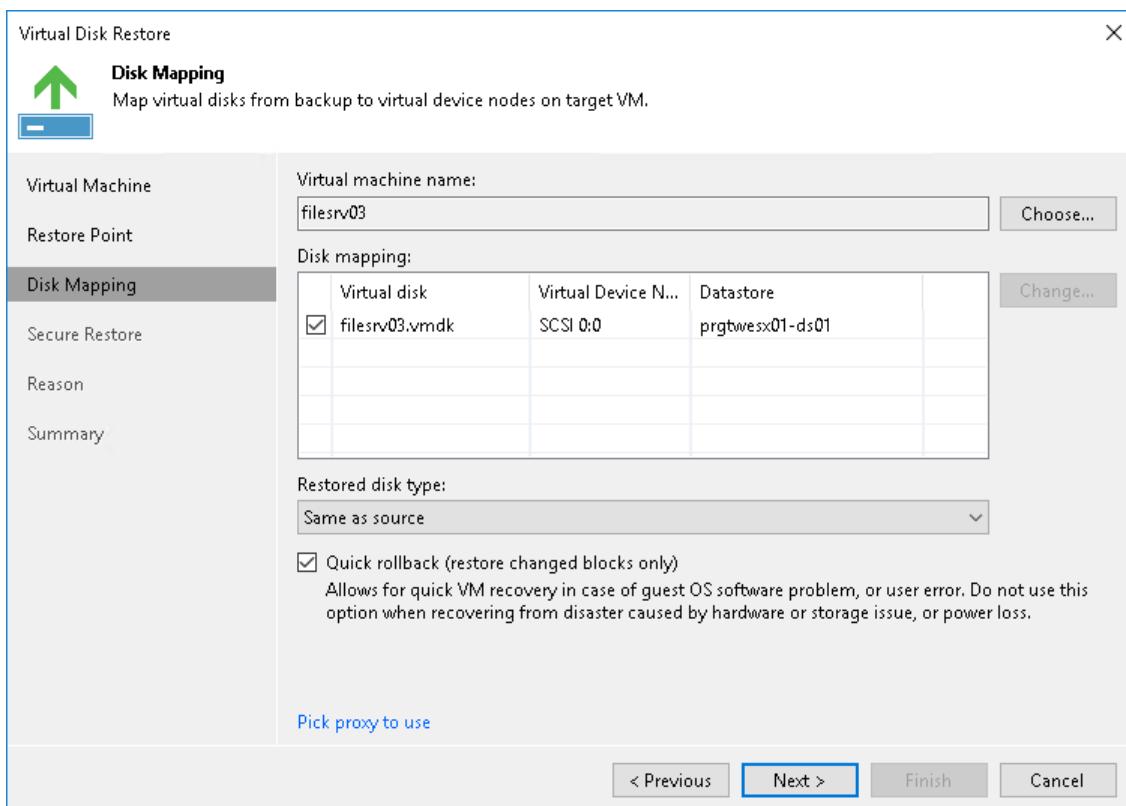
> **NOTE**
>
> This section describes only basic steps that you must take to restore virtual disks of a VM. To get a detailed description of all settings of the restore process, see the Restoring Virtual Disks section in the Veeam Backup & Replication User Guide.

To restore virtual hard disks:
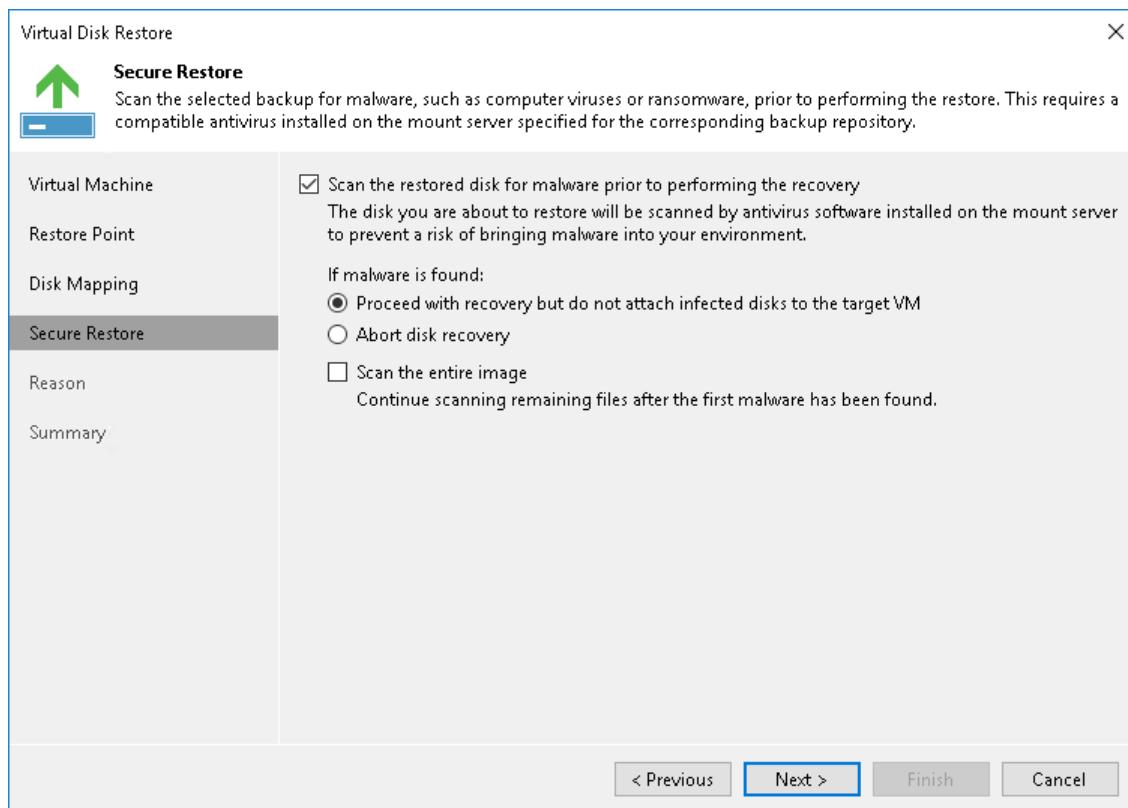
1. Open the **Home** view.

2. Select the **Backups** node in the inventory pane. Expand the backup job in the working area, right-click the necessary VM in the backup job and select **Restore virtual disks**.

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

4. At the **Disk Mapping** step of the wizard, click **Browse** and select the VM to which the restored hard disks must be attached.

5. Select check boxes next to the virtual hard disks that you want to restore.

6. To change the disk format, select the required option from the **Restore disks** list: same as on the original VM, force thin or force thick.

7. Select the VM disk in the list and click **Change**. In the **Virtual Disk Properties** section, select a datastore where the restored hard disk must be located and select a virtual device node.

   o If you want to replace an existing virtual disk, select an occupied virtual node.

   o If you want to attach the restored disk to the VM as a new drive, select a node that is not yet occupied.

8. [For hard disk restore to the original location and with original format] Select the **Quick rollback** check box if you want to use incremental restore for the VM disk. Veeam Backup & Replication will query CBT to get data blocks that are necessary to revert the VM disk to an earlier point in time, and will restore only these data blocks from the backup. Incremental restore significantly reduces the restore time and has little impact on the production environment.

9. If you want to scan VM disk data with antivirus software before restoring VM disks to the production environment, at the **Secure Restore** step of the wizard, specify secure restore settings.

10. At the **Reason** step of the wizard, specify the reason for future reference.

11. At the **Summary** step of the wizard, select the **Power on target VM after restoring** check box if necessary.

12. Click **Finish**.

Restoring VM Guest OS Files

You can restore individual Microsoft Windows guest OS files from backups of Microsoft Windows VMs.
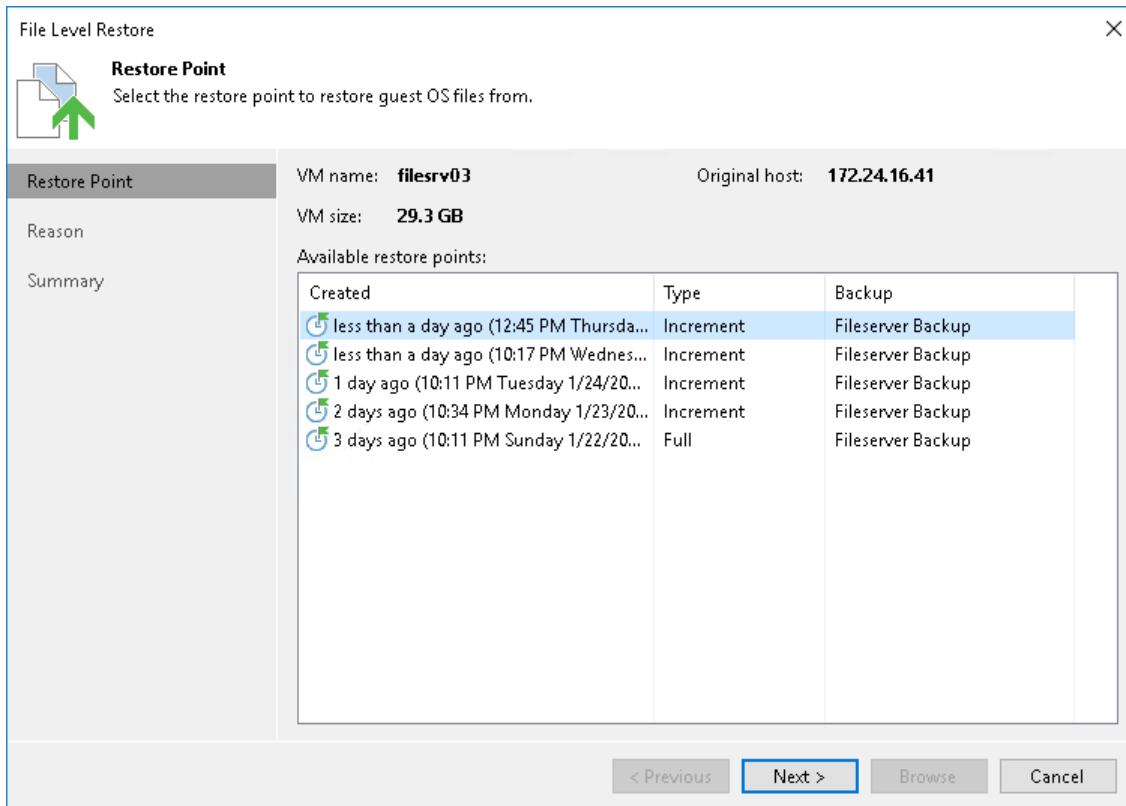
During file-level recovery, Veeam Backup & Replication does not extract the VM image from the backup file. Virtual disks files from the backup are published directly into the Veeam backup server file system with the help of Veeam's proprietary driver. After VM disks are mounted, you can use the Veeam Backup Browser or Microsoft Windows Explorer to copy necessary files and folders to the local machine drive, save them in a network shared folder or point any applications to restored files and work with them as usual.

> **NOTE**
>
> This section describes only basic steps that you must take to restore VM guest OS files. To get a detailed description of all settings of the restore process, see the Guest OS File Recovery section in the Veeam Backup & Replication User Guide.

To restore VM guest OS files of a Microsoft Windows VM from the backup:

1. Open the **Home** view.

2. Select the **Backups** node in the inventory pane. Expand the backup job in the working area, right-click the necessary VM in the backup job and select **Restore guest files** > **Microsoft Windows**.

3. At the **Restore Point** step of the wizard, select the necessary restore point.
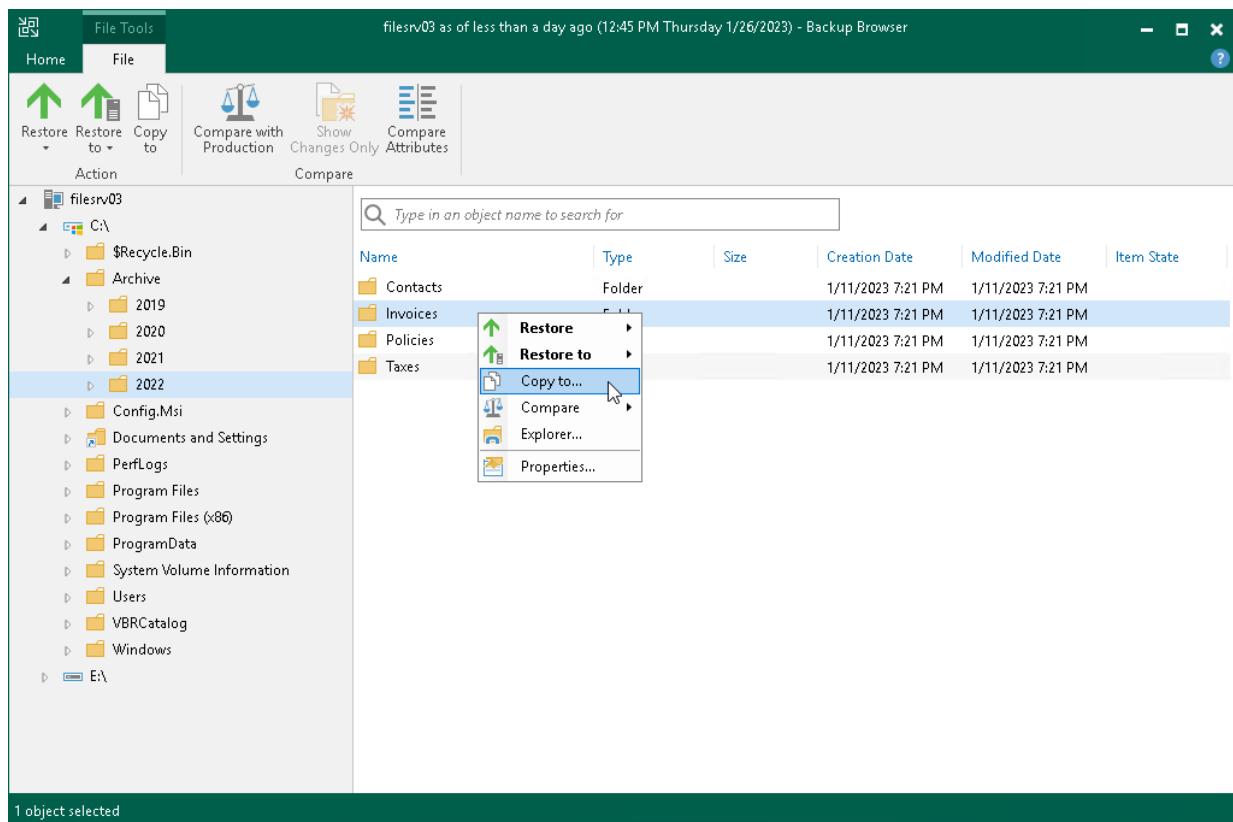
4. At the **Reason** step of the wizard, specify the reason for future reference.

5. Click **Next** and then click **Browse** to finish working with the **File Level Restore** wizard. Veeam Backup & Replication will mount VM disks from the backup to the backup server file system, and display the Veeam Backup Browser.

6. In the Veeam Backup Browser, Veeam Backup & Replication will display the file system tree of the VM. Right-click the necessary file or folder and select the necessary option.

    o To restore a file or folder to its original location on the original VM:

        ▪ Select **Restore** > **Overwrite** if you want to overwrite the original file or folder on the VM guest OS with the file or folder restored from the backup.

        ▪ Select **Restore** > **Keep** if you want to save a file or folder restored from the backup next to the original file or folder. Veeam Backup & Replication will add the *_RESTORED_YYYYMMDD_HHMMSS* postfix to the original file or folder name and save the restored file or folder in the same location where the original file or folder resides.

    o To restore a file or folder to another VM in the Veeam backup infrastructure:

        ▪ Select **Restore to** > **Overwrite** if you want to overwrite the file or folder on the VM guest OS with the file or folder restored from the backup in case the file or folder with the same name resides on the target VM.

        ▪ Select **Restore to** > **Keep** if you want to save a file or folder restored from the backup next to the file or folder on the VM guest OS in case the file or folder with the same name resides on the target VM. Veeam Backup & Replication will add the *_RESTORED_YYYYMMDD_HHMMSS* postfix to the original file or folder name and save the restored file or folder in the specified location.

    If you select one of this options, select the target VM and target path for the restored file or folder, and click **OK**.

o To restore to the original location only those files or folders that have changed on the original VM since the restore point for the backup was created, select **Compare** > **Compare**. Then right-click the file or folder and select one of the following options:

  ▪ Select **Restore changed only** > **Overwrite** if you want to overwrite the original file or folder on the VM guest OS with the file or folder restored from the backup.

  ▪ Select **Restore changed only** > **Keep** if you want to save a file or folder restored from the backup next to the original file or folder. Veeam Backup & Replication will add the *_RESTORED_YYYYMMDD_HHMMSS* postfix to the original file or folder name and save the restored file or folder in the same location where the original file or folder resides.

o To save a file or folder on the local machine or in a network shared folder, select **Copy to**, specify a path to the destination location and click **OK**.

To learn more, see the Finalize Restore section in the Veeam Backup & Replication User Guide.

Restoring Application Items

You can use Veeam Explorers to restore application items from backups created in the cloud repository.

Veeam Backup & Replication lets you restore items of the following applications:

- Microsoft Active Directory
- Microsoft Exchange
- Microsoft SharePoint
- Microsoft SQL Server
- Microsoft OneDrive for Business
- Microsoft Teams
- Oracle
- PostgreSQL

For backups in the cloud repository created by backup jobs with guest processing options enabled, the procedure of application-item restore does not differ from the regular one. To perform application-item restore, do either of the following:

- Open the **Home** view, in the inventory pane select **Backups** > **Cloud**. In the working area, select the necessary machine and click **Application Items** > *<Application>* on the ribbon.

- Open the **Home** view, in the inventory pane select **Backups** > **Cloud**. In the working area, right-click the necessary machine and select **Restore application items** > *<Application>*.

Then follow instructions in the procedure for the required application. For details, see the Application Item Restore section in the Veeam Backup & Replication User Guide.

The list of available data recovery operations differs depending on what Veeam Explorer you use. To learn more, see the Veeam Explorers User Guide.

Restoring Volumes from Veeam Agent Backups

You can use Veeam Backup & Replication to restore a specific computer volume or all volumes from a volume-level backup created with Veeam Agent for Microsoft Windows.

A volume can be restored to its original location or a new location. If you restore the volume to its original location, Veeam Backup & Replication overwrites data on the original volume. If you restore the volume to a new location, and the target disk contains any data, Veeam Backup & Replication overwrites data in the target location with data retrieved from the backup.
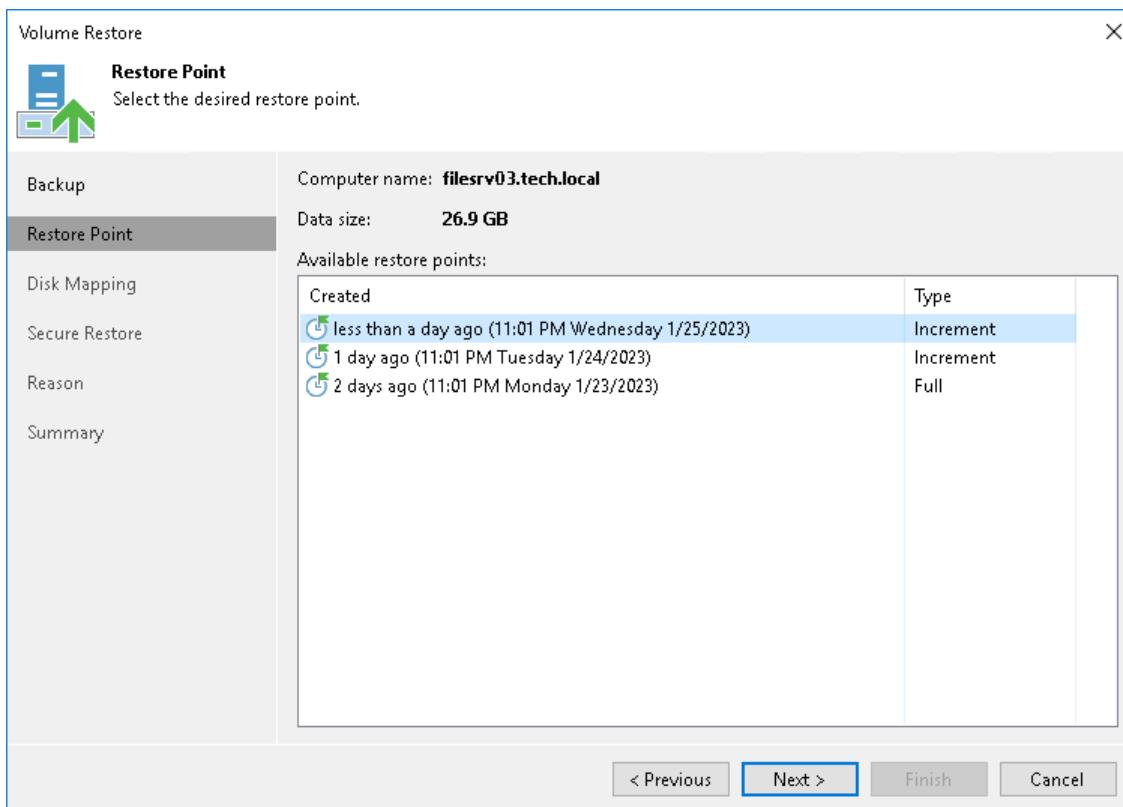
> **NOTE**
>
> This section describes only basic steps that you must take to restore volumes from a Veeam Agent backup. To get a detailed description of all settings of the volume restore process, see the Restoring Volumes section in the Veeam Agent Management Guide.

To restore volumes from a Veeam Agent backup:

1. Open the **Home** view.

2. Select the **Backups** node in the inventory pane. Expand the **Agents** node in the working area, right-click the necessary Veeam Agent backup and select **Volume restore**.

3. At the **Restore Point** step of the wizard, select the necessary restore point.
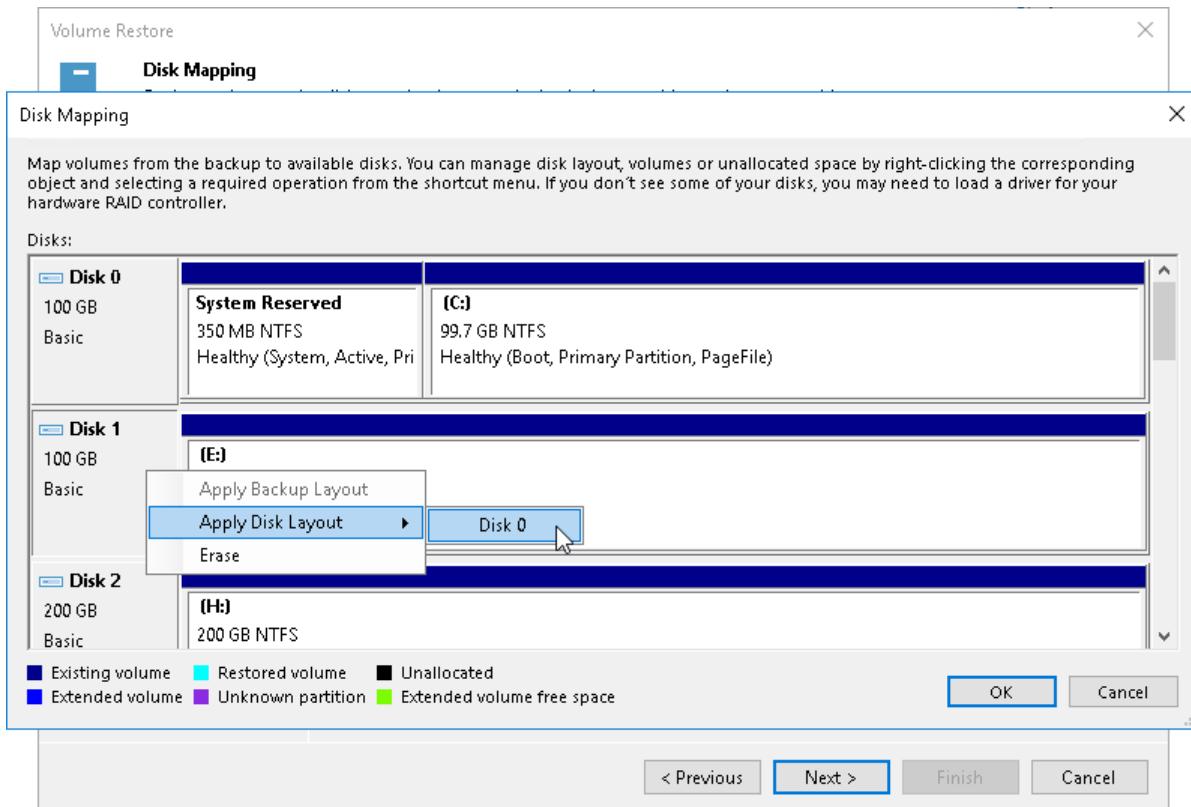
4. At the **Disk Mapping** step of the wizard, select what volumes you want to restore and map volumes from the backup to volumes on the target computer:

   a. Click **Choose** next to the **Destination hosts** field and select the target machine where you want to restore volumes. You can restore volumes only to machines that are added to the Veeam Backup & Replication inventory and run Veeam Agent for Microsoft Windows operating in the managed mode. To learn more, see the Creating Protection Groups section in the Veeam Agent Management Guide.

   b. In the **Disk mapping** section, select check boxes next to volumes that you want to restore from the backup. By default, Veeam Backup & Replication restores volumes to their initial location and maps the restored volumes automatically. If the initial location is unavailable, Veeam Backup & Replication offers to map volumes manually. You can also map volumes manually, for example, if you want to map the restored volume to another computer disk. To do this, at the bottom of the window click the **Customize disk mapping** link.

   c. In the **Disk Mapping** window, specify how volumes must be restored. To do this, right-click the target disk on the left and select the necessary disk layout:
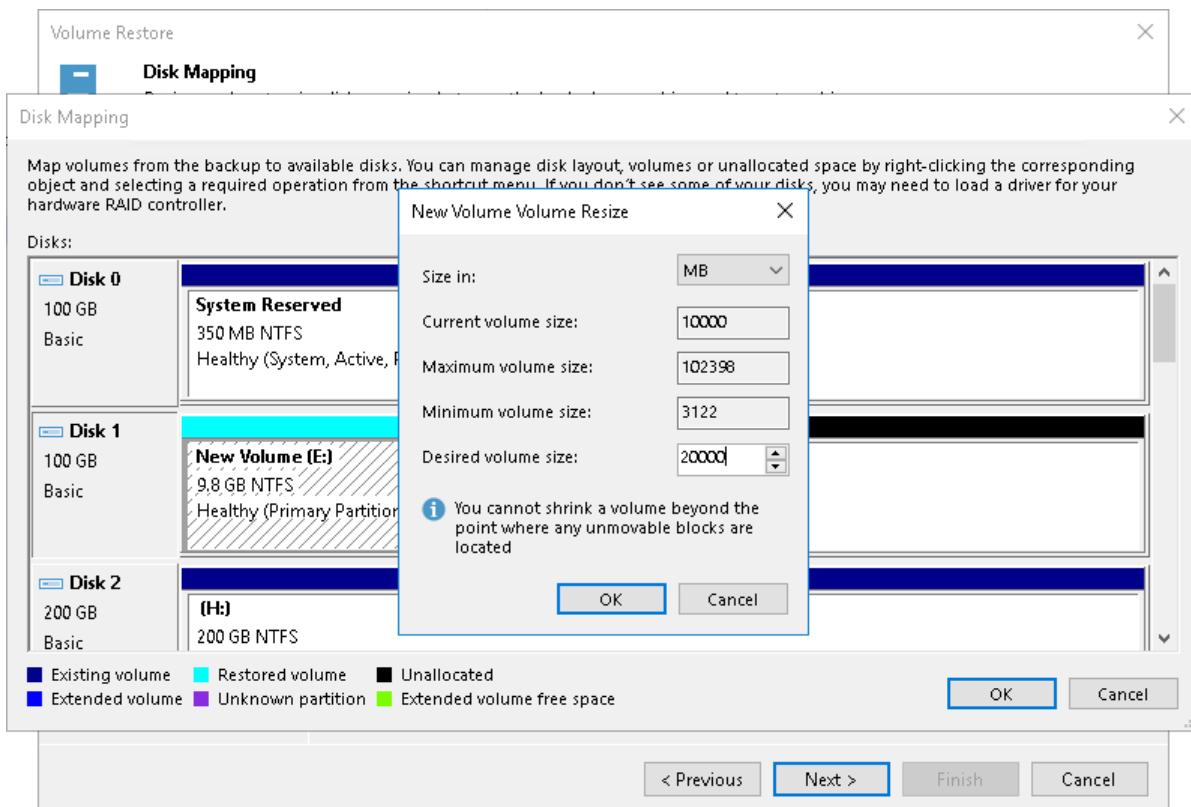
   - **Apply Backup Layout** — select this option if you want to apply to disk the settings that were used on your computer at the moment when you performed backup.

   - **Apply Disk Layout** — select this option if you want to apply to the current disk settings of another disk.

   - **Erase** — select this option if you want to discard the current disk settings.

   Alternatively, you can right-click unallocated disk space in the disk area on the right and select what volume from the backup you want to place on this computer disk.
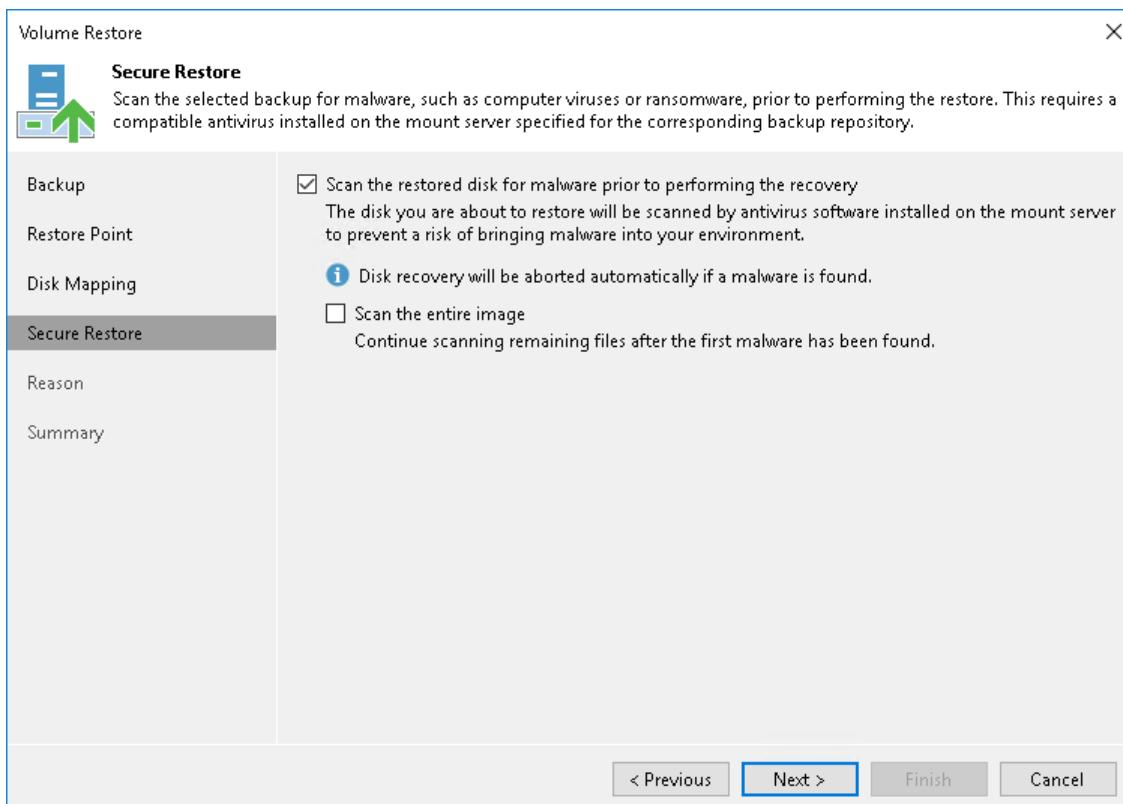
   If you want to change disk layout configured by Veeam Backup & Replication, right-click an automatically mapped volume and select **Remove**. You will be able to use the released space for mapping volumes in your own order.

5. At the **Disk Mapping** step of the wizard, you can set the necessary size for the restored volumes. To do this, right-click the volume in the **Disk Mapping** window and select **Resize**. In the **Volume Resize** window, select the volume size unit and specify the desired size for the restored volume.

6. If you want to scan restored volume data with antivirus software before restoring volumes to the production environment, at the **Secure Restore** step of the wizard, specify secure restore settings.

7. At the **Reason** step of the wizard, enter a reason for restoring computer volumes.

8. At the **Summary** step of the wizard, click **Finish**.

Exporting Disks from Veeam Agent Backups
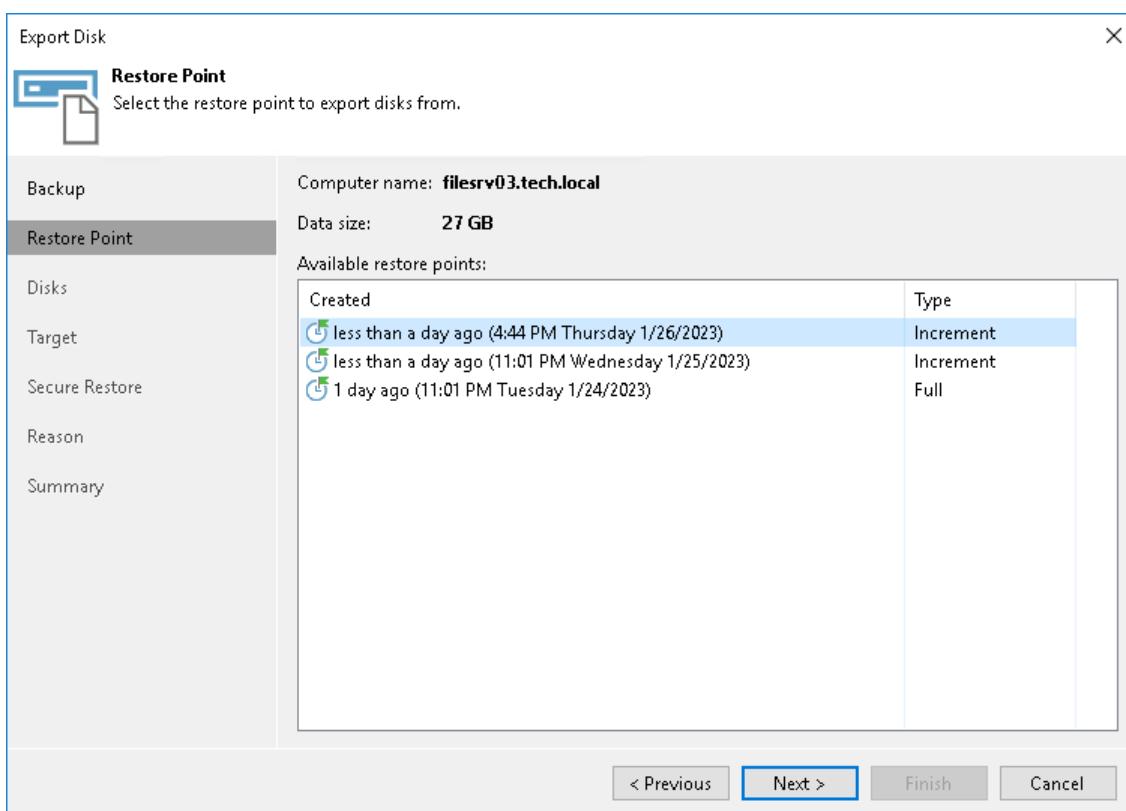
You can export computer disks included in volume-level Veeam Agent backups as virtual disks. The resulting virtual disks can be attached to a virtual machine. Thus, you can recover subtenant data that was originally stored on a physical device to the virtual environment.
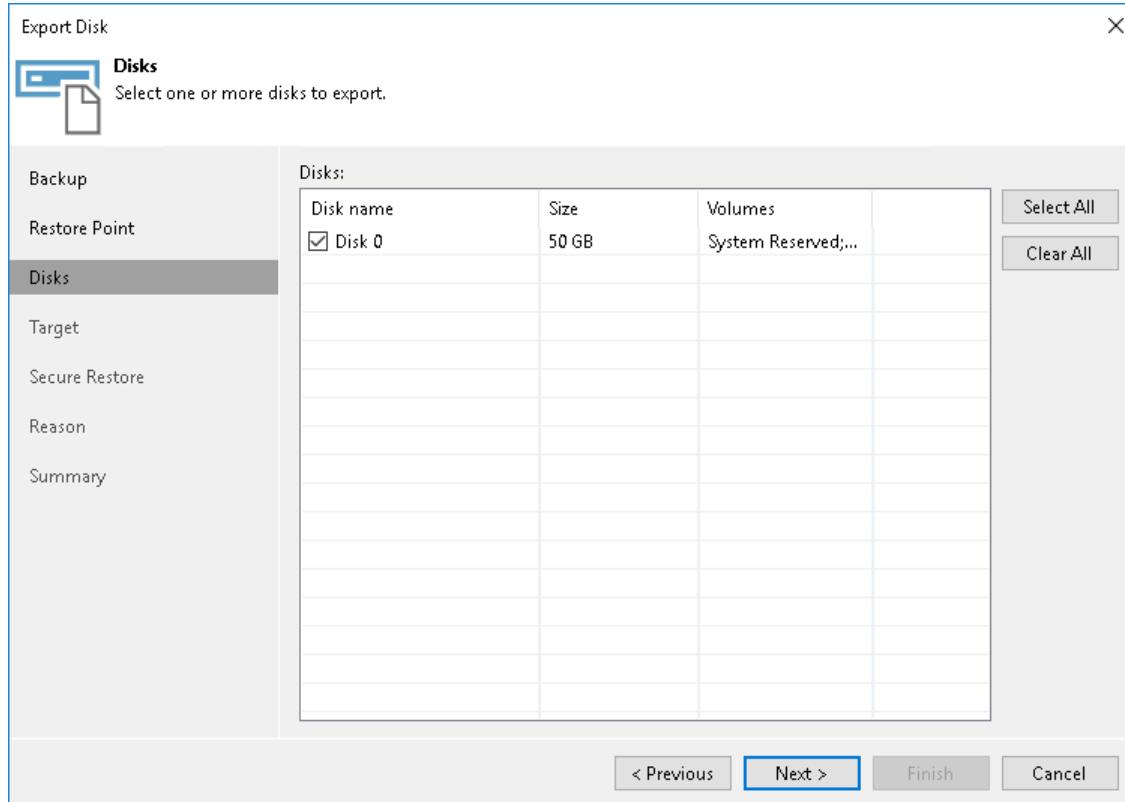
> **NOTE**
>
> This section describes only basic steps that you must take to export disks contained in a Veeam Agent backup. To get a detailed description of all settings of the export process, see the Exporting Disks section in the Veeam Agent for Microsoft Windows User Guide.

To export disks included in a Veeam Agent backup:

1. Open the **Home** view.

2. Select the **Backups** node in the inventory pane. Expand the **Agents** node in the working area, right-click the necessary Veeam Agent backup and select **Export disk content as virtual disks**.

3. At the **Restore Point** step of the wizard, select the necessary restore point.
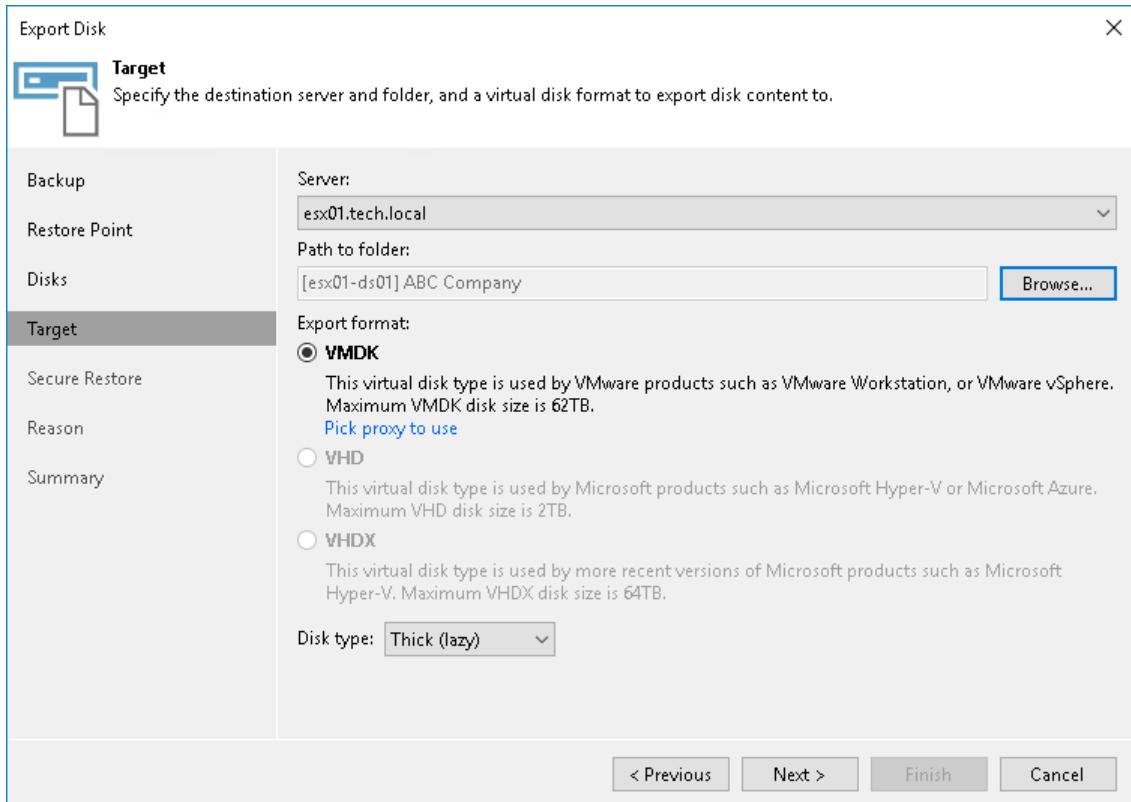
4. At the **Disks** step of the wizard, select check boxes next to the disks that you want to export.
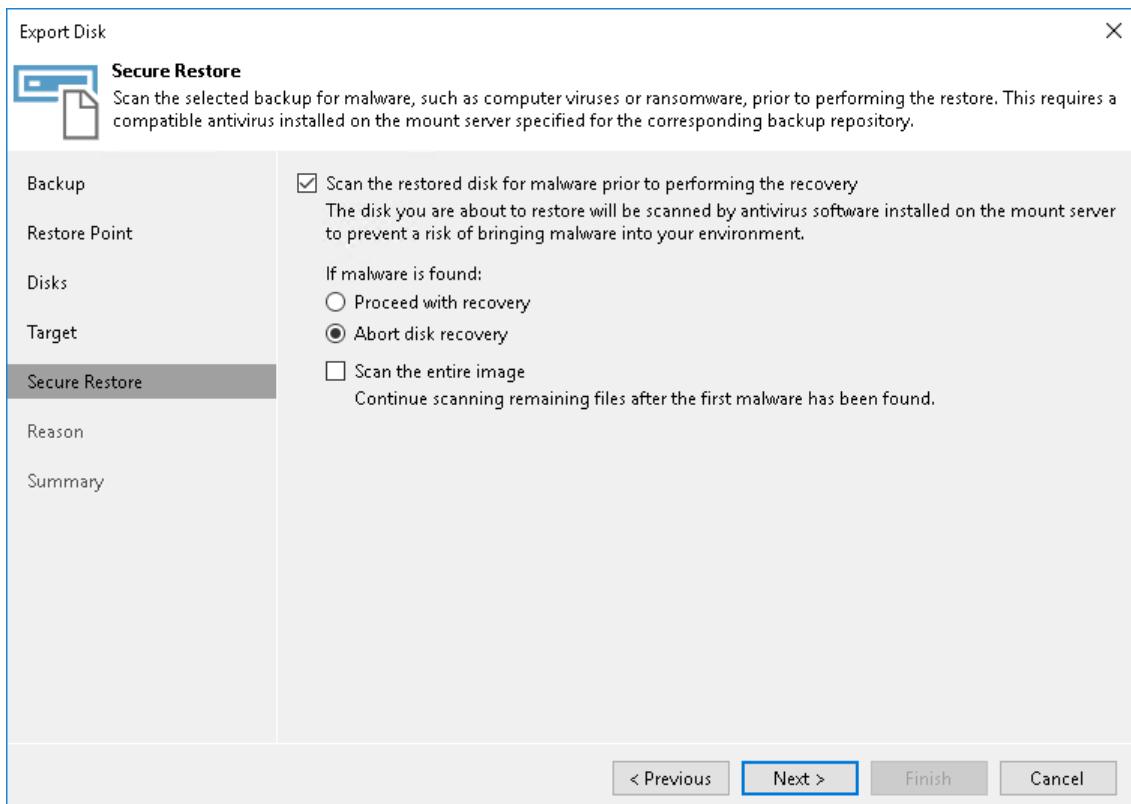
5. At the **Target** step of the wizard, select the destination for disk export and format in which you want to save the resulting virtual disk:

    a. From the **Server** list, select a server on which the resulting virtual disks must be saved. If you plan to save the disks in the VMDK format on a datastore, select an ESXi host to which this datastore is connected.

    b. In the **Path to folder** field, specify a folder on the server or datastore where the virtual disks must be placed.

    c. Select the export format for disks:

        ▪ VMDK — select this option if you want to save the resulting virtual disk in the VMware VMDK format.

        ▪ VHD — select this option if you want to save the resulting virtual disk in the Microsoft Hyper-V VHD format.

        ▪ VHDX — select this option if you want to save the resulting virtual disk in the Microsoft Hyper-V VHDX format (supported by Microsoft Windows Server 2012 and later).

d. [For export of a VMDK disk to an ESXi host] Click the **Pick proxy to use** link to select backup proxies over which backup data must be transported to the target datastore.

e. [For export of a VMDK disk to an ESXi host] From the **Disk Type** drop-down list, select how the resulting disk must be saved: in the thin provisioned or thick provisioned format.

6. If you want to scan restored disk data with antivirus software before exporting disks, at the **Secure Restore** step of the wizard, specify secure restore settings.

7. At the **Reason** step of the wizard, specify the reason for future reference.

8. At the **Summary** step of the wizard, click **Finish**.

Restoring Guest OS Files from Veeam Agent Backups

You can restore individual Microsoft Windows guest OS files from backups of machines created with Veeam Agent for Microsoft Windows.

File-level restore from Veeam Agent backups is performed in the same way as for VM backups. Veeam Backup & Replication publishes computer disks from the backup directly into the Veeam backup server file system. After disks are mounted, you can use the Veeam Backup Browser or Microsoft Windows Explorer to copy necessary files and folders to the local machine drive, save them in a network shared folder or point any application to restored files and work with them as usual.
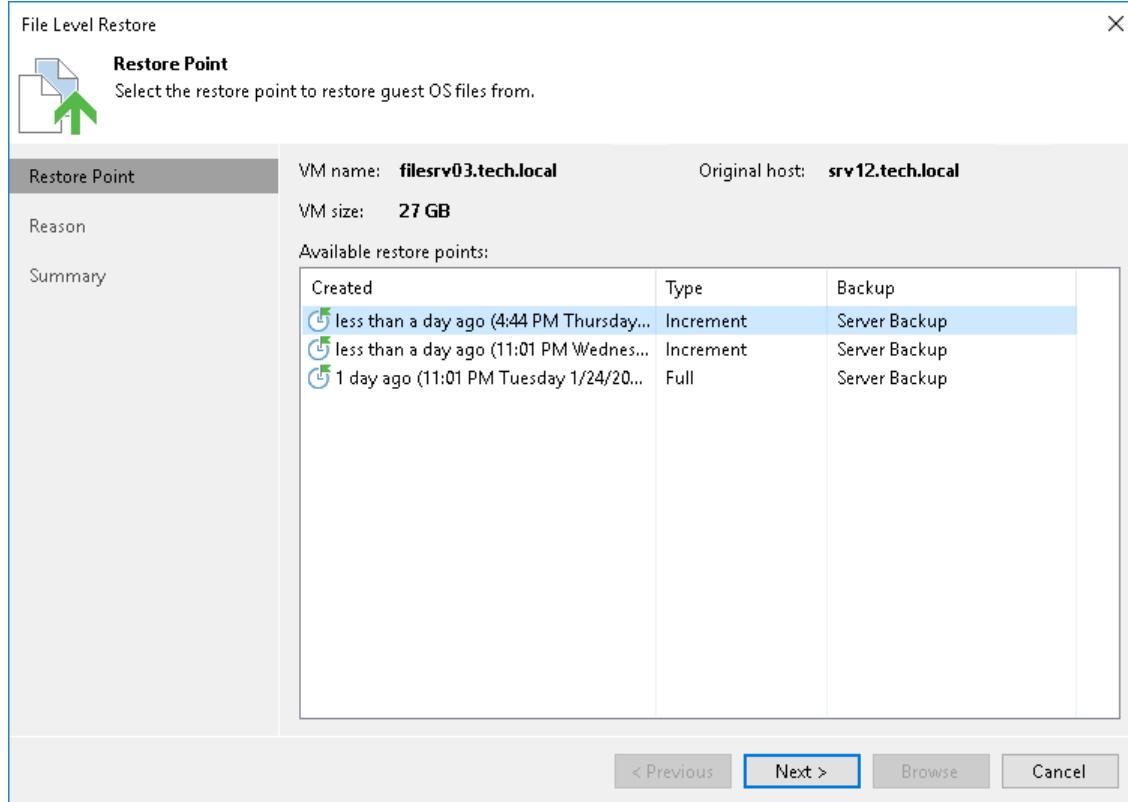
> **NOTE**
>
> This section describes only basic steps that you must take to restore guest OS files from a Veeam Agent backup. To get a detailed description of all settings of the restore process, see the Restoring VM Guest OS Files (FAT, NTFS or ReFS) section in the Veeam Backup & Replication User Guide.

To restore Microsoft Windows guest OS files from a Veeam Agent backup:

1. Open the **Home** view.

2. Click the **Backups** > **Cloud** node in the inventory pane and do either of the following:

    o If you want to restore files from a backup created with a standalone version of Veeam Agent, expand the **Agents** node in the working area, right-click the necessary backup and select **Restore guest files** > **Microsoft Windows**.

    o If you want to restore files from a backup created with Veeam Agent managed by Veeam Backup & Replication, expand the Veeam Agent backup job in the working area, right-click the necessary machine in the job and select **Restore guest files** > **Microsoft Windows**.

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

4. At the **Reason** step of the wizard, specify the reason for future reference.

5. Click **Next** and then click **Browse** to finish working with the File Level Restore wizard. Veeam Backup & Replication will mount Veeam Agent machine disks from the backup to the backup server file system and display the Veeam Backup Browser.

6. In the Veeam Backup Browser, Veeam Backup & Replication will display the file system tree of the backed-up machine. Right-click the necessary file or folder and select one of the following options:

   o To restore a file or folder to its original location on the Veeam Agent machine:

     ▪ Select **Restore** > **Overwrite** if you want to overwrite the original file or folder on the backed-up machine file system with the file or folder restored from the backup.

     ▪ Select **Restore** > **Keep** if you want to save a file or folder restored from the backup next to the original file or folder. Veeam Backup & Replication will add the *_RESTORED_YYYYMMDD_HHMMSS* postfix to the original file or folder name and save the restored file or folder in the same location where the original file or folder resides.

- o To restore to the original location only those files or folders that have changed on the original VM since the restore point for the backup was created, select **Compare** > **Compare**. Then right-click the file or folder and select one of the following options:

  - Select **Restore changed only** > **Overwrite** if you want to overwrite the original file or folder on the backed-up machine file system with the file or folder restored from the backup.

  - Select **Restore changed only** > **Keep** if you want to save a file or folder restored from the backup next to the original file or folder. Veeam Backup & Replication will add the *_RESTORED_YYYYMMDD_HHMMSS* postfix to the original file or folder name and save the restored file or folder in the same location where the original file or folder resides.

- o To save a file or folder on the local machine or in a network shared folder, select **Copy to**, specify a path to the destination location and click **OK**.

  To learn more, see the Finalize Restore section in the Veeam Backup & Replication User Guide.

7. [For restore to the original location] If you restore a file or folder from a backup created with a standalone version of Veeam Agent, Veeam Backup & Replication will prompt you to specify an account to connect to the Veeam Agent machine. In the **Credentials** window, select a user account that has administrative permissions on the target machine. 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 the Credentials Manager section in the Veeam Backup & Replication User Guide.

   If you restore a file or folder from a backup created with Veeam Agent managed by Veeam Backup & Replication, Veeam Backup & Replication will connect to the Veeam Agent machine using credentials of the account specified for the machine in the protection group settings.

8. Click **OK** to restore selected files and folders.

Exporting Backups

You can export data related to a specific restore point in the backup and save it to a standalone full backup (VBK) file. A standalone full backup is not associated with the existing backup chain and subsequent incremental backups. You can use a standalone full backup as an independent restore point for data recovery.

You can export data to a standalone full backup from VM backups and Veeam Agent backups created in a cloud repository. When you export a backup that resides in a cloud repository, the resulting VBK file is saved to the same cloud repository. The backup is saved in a separate subfolder of the folder that contains tenant backups.
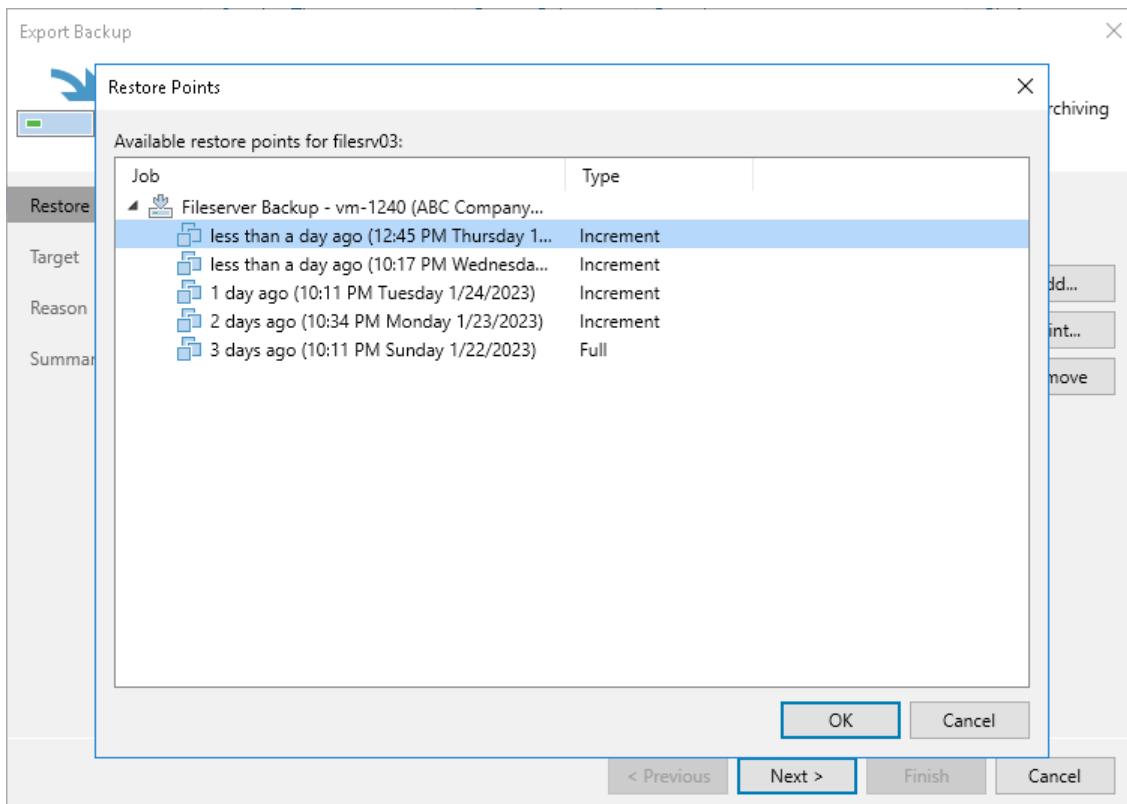
After you export a restore point to a full backup, the resulting full backup becomes available in the tenant Veeam backup console. The tenant can perform the same operations with the standalone full backup as with a regular backup created in a cloud repository.

> **NOTE**
>
> This section describes only basic steps that you must take to export a restore point to a full backup file. To get a detailed description of all settings of the export process, see the Exporting Backups section in the Veeam Backup & Replication User Guide.

To export a restore point to a full backup file:

1. Open the **Home** view.

2. Select the **Backups** node in the inventory pane. Expand the backup job in the working area, right-click the necessary VM or Veeam Agent computer in the backup job and select **Export backup**.

3. At the **Restore Point** step of the wizard, click **Point** and select the necessary restore point.

4. If you want to specify the retention policy for the exported backup, select the **Delete exported backup file automatically check box** and select the desired time period from the drop-down list. After the specified time period expires, Veeam Backup & Replication will automatically delete the exported backup from the cloud repository.

5. At the **Reason** step of the wizard, specify the reason for future reference.

6. At the **Summary** step of the wizard, click **Finish**.

Managing Backups

You can perform the following operations with backups created with backup and backup copy jobs on the cloud repository:

- View properties

- Delete from disk

Viewing Properties

You can view summary information about created backups. The summary information provides the following data: available restore points, date of restore points creation, data size and backup size. For VM backups and backups created by Veeam Agent in the managed mode, Veeam Backup & Replication also displays compression and deduplication ratios.

> **NOTE**
>
> If you enabled data encryption in the backup job settings, and the size of backup files in the **Backup Size** column is larger than the size of the original data in the **Original Size** column, this can mean that your SP configured the cloud repository using Dell Data Domain. Contact the SP, ask him to check the repository settings and clear the **Decompress backup data blocks before storing** check box.

To view summary information for backups:

1. Open the **Home** view.

2. In the inventory pane, click **Cloud** under the **Backups** node.

3. Do either of the following:

   - To view summary information for a VM backup, in the working area, right-click the necessary backup job and select **Properties**.

   - To view summary information for an entire backup related to a Veeam Agent backup job configured in Veeam Backup & Replication (parent backup), in the working area, right-click the necessary backup job and select **Properties**.

   - To view summary information for a backup related to a specific machine in a Veeam Agent backup job configured in Veeam Backup & Replication (child backup), in the working area, expand the necessary backup job, right-click the machine and select **Properties**.

   - To view summary information for a backup created by Veeam Agent operating in the standalone mode, in the working area, right-click the necessary backup under the **Agents** node and select **Properties**.

For VM backups and parent backups created by Veeam Agent in the managed mode, summary information looks in the following way:

For backups created by Veeam Agent in the standalone mode and child backups created by Veeam Agent in the managed mode, summary information looks in the following way:

Deleting from Disk

You can use the **Delete from disk** operation if you want to delete records about backups from the Veeam Backup & Replication console and database and, additionally, delete actual backup files from the cloud repository.

Do not delete backup files from the cloud repository manually. Use the **Delete from disk** option instead. If you delete backup files manually, subsequent backup job sessions will be failing.

To remove backup files from the cloud repository:

1. Open the **Home** view.

2. In the inventory pane, click **Cloud** under the **Backups** node.

3. In the working area, right-click the necessary backup job (or necessary Veeam Agent backup under the **Agents** node) and select **Delete from disk**.

Copying Backups from Cloud Repositories

You can manually copy backup files from the cloud repository to any host or server in your backup infrastructure.

Before you begin the copying operation, make sure that the target host or server is added to the backup infrastructure.

To copy backup files:
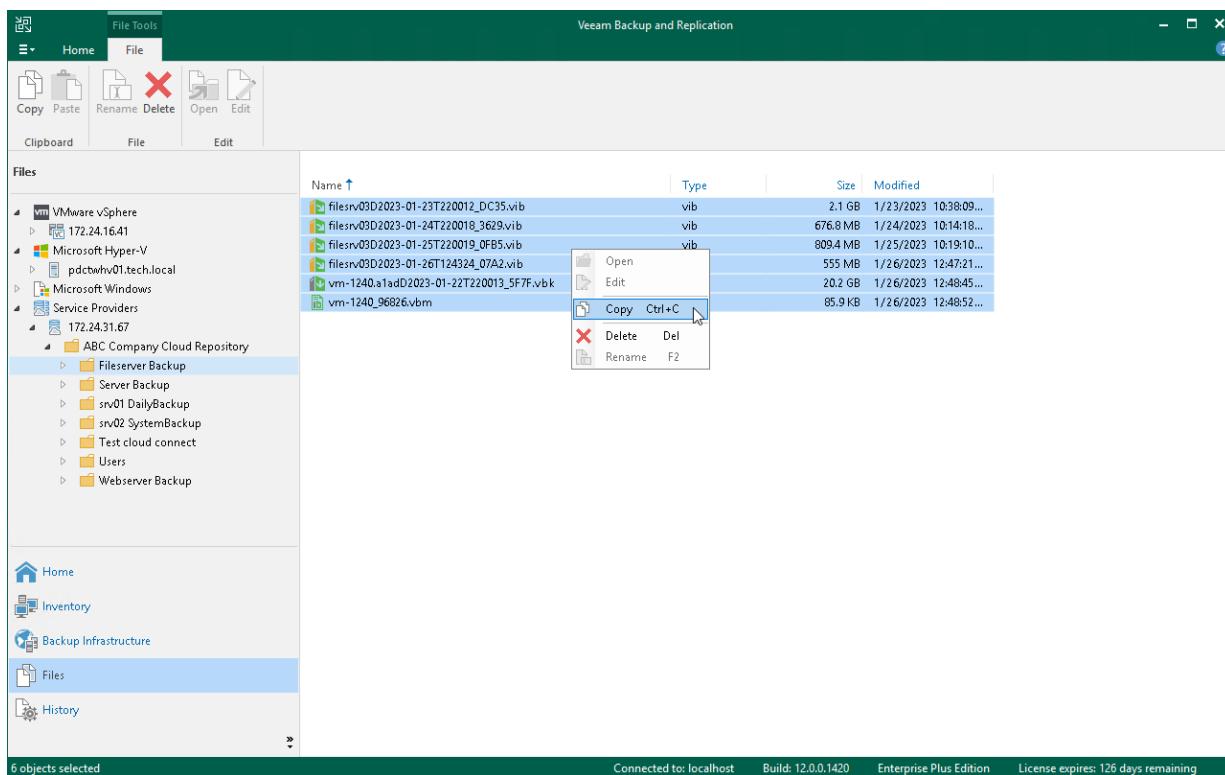
1. Open the **Files** view.

2. In the inventory pane, expand the file tree of the cloud repository under the **Service Providers** node.

3. Right-click backup files that you want to copy and select **Copy**.

4. In the inventory pane, expand the file tree of the target server or host.

5. Right-click a destination folder and select **Paste**.

You can also use a drag-n-drop operation to copy backup files from the cloud repository.

> **NOTE**
>
> You cannot copy backup files from a cloud repository that uses a scale-out backup repository as a back end. To learn more, see Limitations for Cloud Repository.

Using Cloud Hosts

After you have set up the Veeam Cloud Connect infrastructure, you can proceed to performing data protection and disaster recovery tasks using the cloud host provided to you by the SP.

You can perform the following tasks targeted at the cloud host:

- Create a replication job

- Create a CPD policy

- Perform failover:

  o Full site failover

  o Partial site failover

- Perform failback

- Perform data restore (from snapshot-based replicas only):

  o VM guest OS files restore (Microsoft Windows file system only. Multi-OS restore is not supported.)

  o Application items restore

VM replicas created on the cloud host are displayed under the **Replicas** node in the inventory pane of the **Home** view along with regular VM replicas. To identify the replica type, consider the following:

- For snapshot-based replicas registered on the cloud host, Veeam Backup & Replication displays the *Cloud* value in the **Type** column of the working area.

- For CDP replicas registered on the cloud host, Veeam Backup & Replication displays the *CDP* value in the **Type** column of the working area.

Creating Replication Jobs

In Veeam Backup & Replication, replication is a job-driven process. To create VM replicas, you must configure a replication job. The replication job defines how, where and when to replicate VM data. One job can be used to process one VM or several VMs.
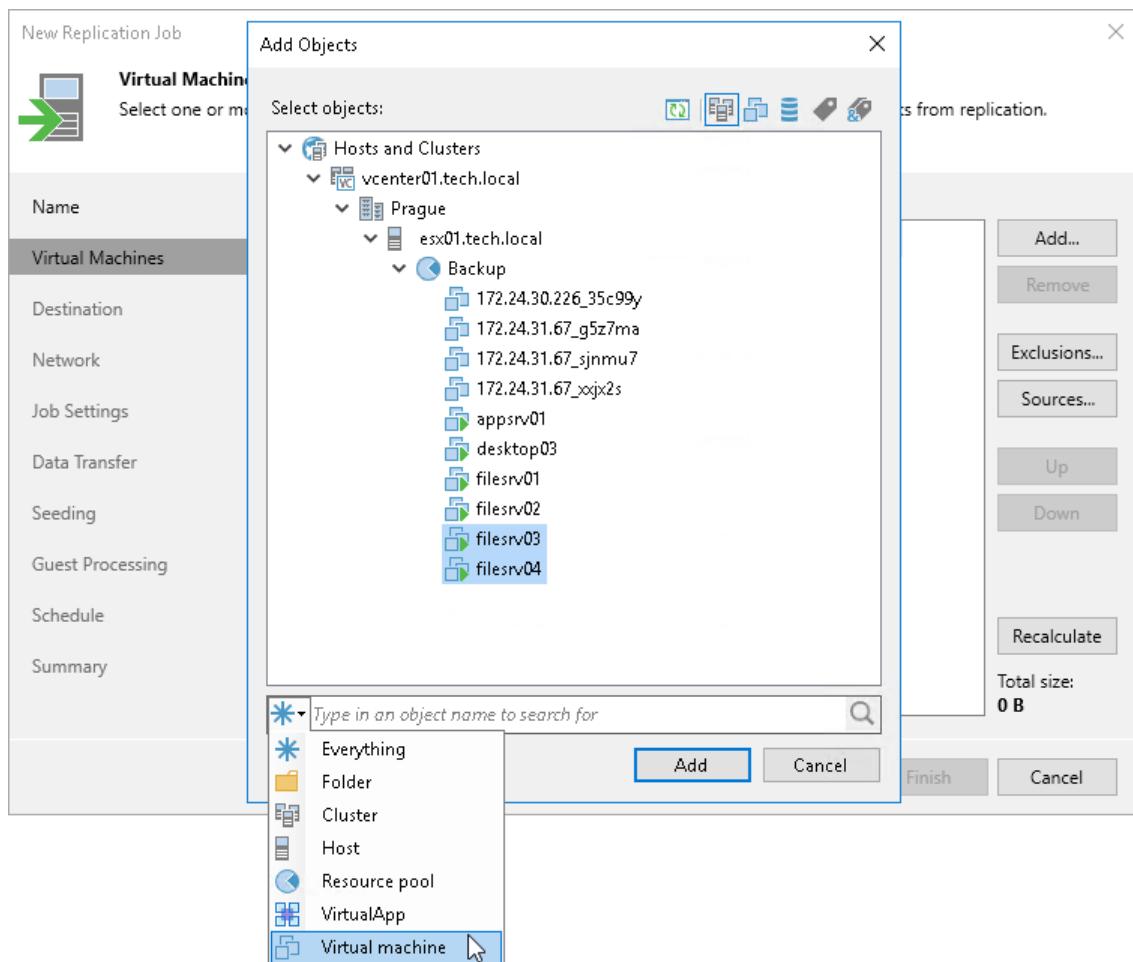
> **NOTE**
>
> This section describes only basic steps that you must take to create a replication job targeted at the cloud host. To get a detailed description of all replication job settings, see the Creating Replication Jobs section in the Veeam Backup & Replication User Guide.

To create a replication job:
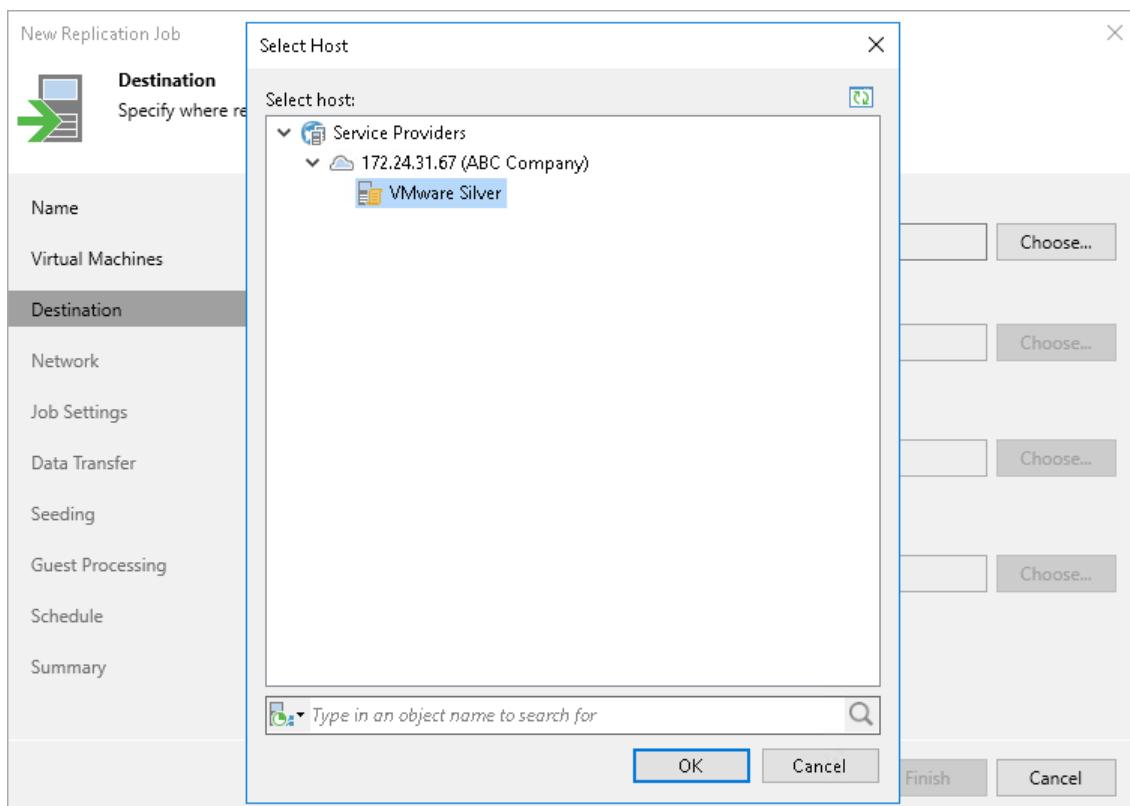
1. On the **Home** tab, click **Replication Job** and select **Virtual machine** > **VMware vSphere** or **Virtual machine** > **Microsoft Hyper-V**.

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

3. If you want to use advanced settings for the job:

   o Select the **Replica seeding** check box to enable the **Seeding** step in the wizard.

   o Select the **Network remapping** check box to enable the **Network** step in the wizard. Veeam Backup & Replication does not currently support automatic connection of a Linux-based VM replica to the network on the cloud host. You must use the **Network** step of the wizard to manually select source and target networks for such replicas.

   o Veeam Backup & Replication does not support re-IP rules for VM replicas on the cloud host. Do not select the **Replica re-IP** check box for the replication job targeted at the cloud host. If you select the **Replica re-IP** option, this option will be disabled when you select the cloud host at the **Destination** step of the wizard.

4. At the **Virtual Machines** step of the wizard, click **Add** and select VMs and VM containers that you want to replicate. To quickly find the necessary object, use the search field at the bottom of the **Add Objects** window.
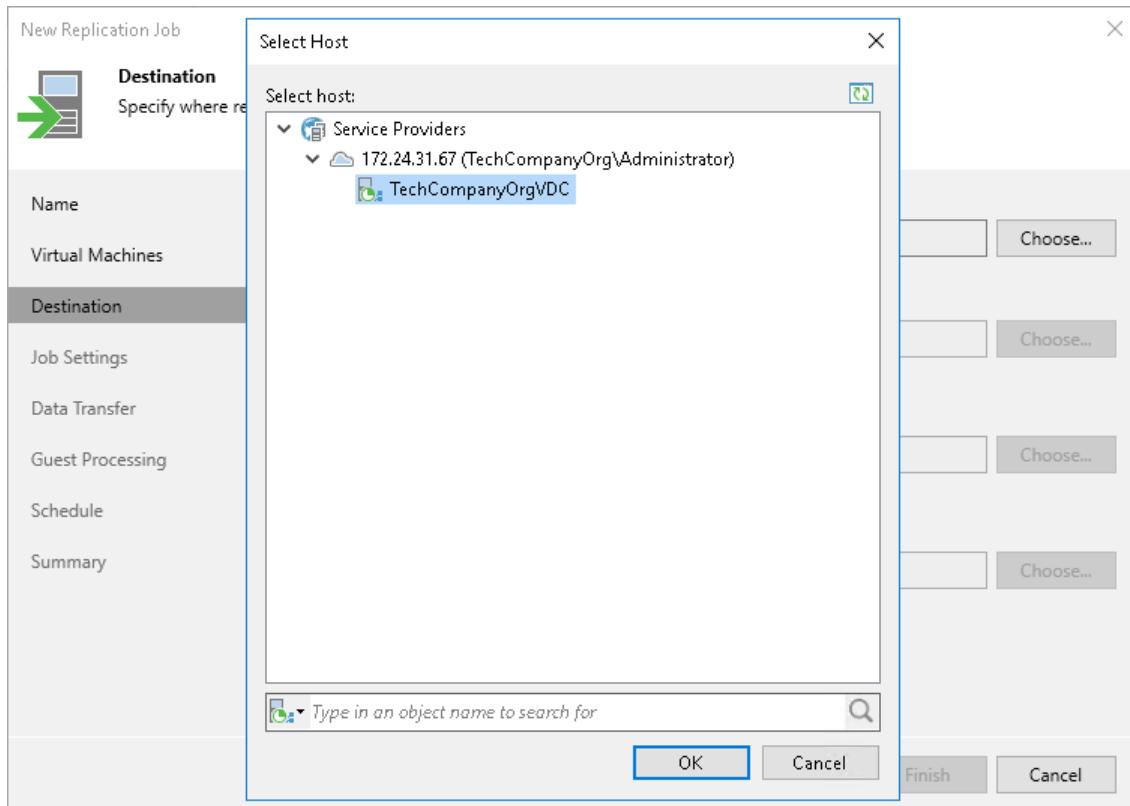
5. If you want to specify the source from which VM data must be read, click **Sources** and select one of the following options:

   o **From production storage**. In this case, Veeam Backup & Replication will retrieve VM data from the production storage connected to the source virtualization host.

   o **From backup files**. In this case, Veeam Backup & Replication will read VM data from a backup chain already existing in the regular backup repository or cloud repository.

6. If you want to exclude VMs from the VM container or replicate only specific VM disks, click **Exclusions** and specify what objects you want to exclude.

7. If you want to define the order in which the replication job must process VMs, select a VM or VM container added to the job and use the **Up** and **Down** buttons on the right to move the VM or VM container up or down in the list.

8. At the **Destination** step of the wizard, in the **Host or cluster** section, click **Choose** and select **Cloud host**. Then select the cloud host allocated to you by the SP:

   o If the SP allocated to you replication resources on a VMware vSphere or Microsoft Hyper-V host, select the cloud host provided to you through a hardware plan.

o If the SP allocated to you replication resources in VMware Cloud Director, select the cloud host provided to you through an organization VDC.
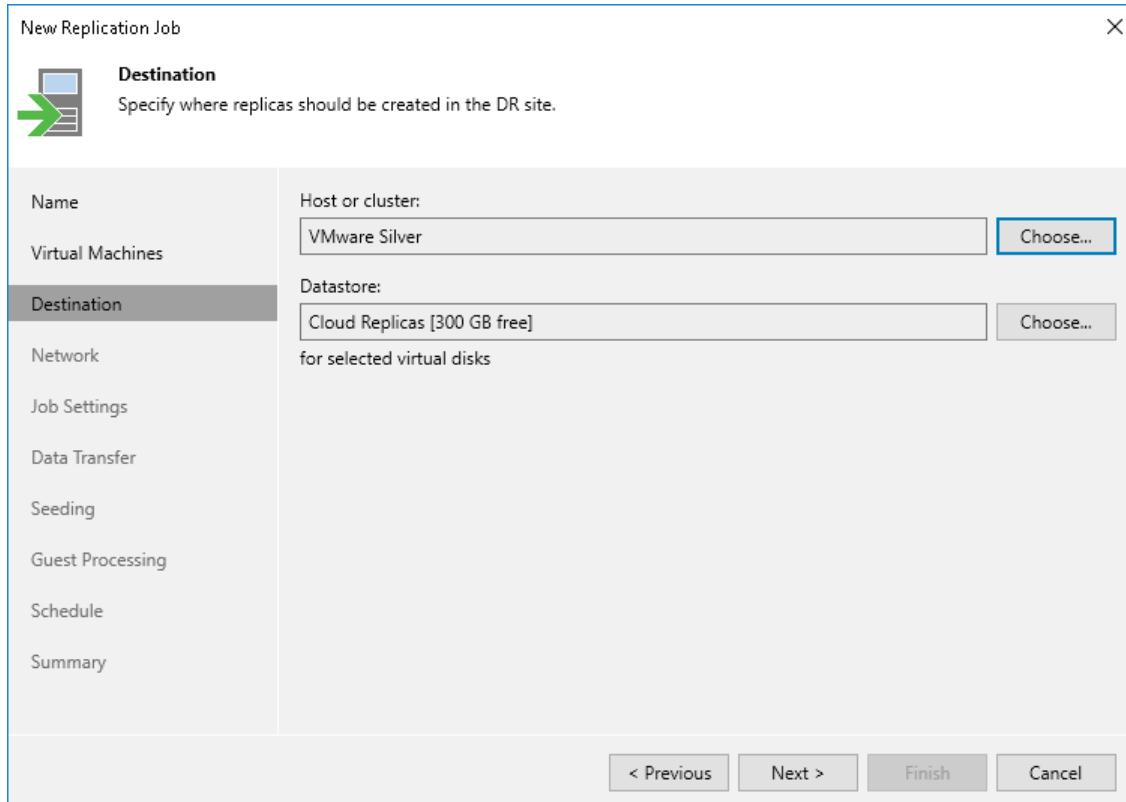
> **NOTE**
>
> After you select an organization VDC, the name of the **Host or cluster** section will change to **Organization VDC**.
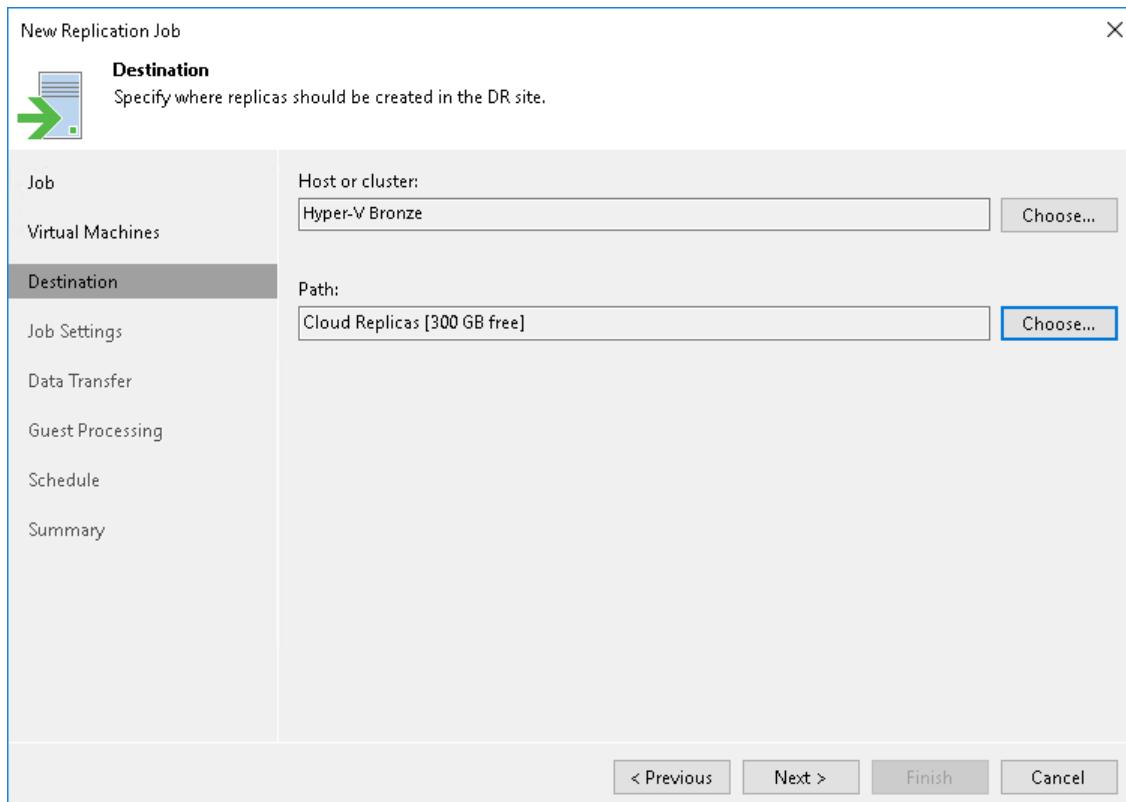
Note that after the replication job is performed for the first time, you will not be able to change the target host for the job.

9. At the **Destination** step of the wizard, select storage resources allocated to you by the SP:
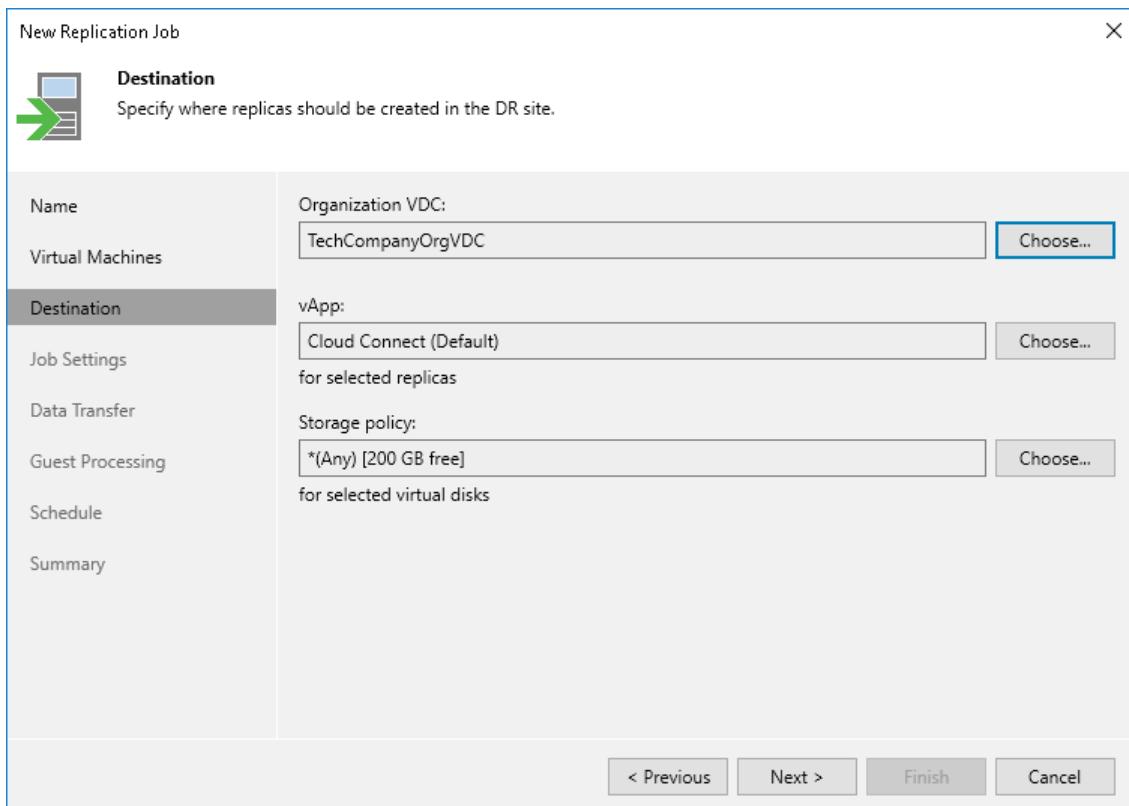
   o [For a VMware replication job] If you want to specify a datastore on which to store VM replicas, in the **Datastore** section, click **Choose** and select the necessary datastore.

   o [For a Hyper-V replication job] If you want to specify a path to the storage on which to store VM replicas, in the **Path** section, click **Choose** and select the necessary storage.

o [For a replication job targeted at VMware Cloud Director] If you want to specify a vApp or storage policy for VM replicas, do the following:

i. In the **vApp** section, click **Choose** and select the necessary vApp.

Note that you must not use the same vApp as a target for both a snapshot-based replication job and a CDP policy.

ii. In the **Storage policy** section, click **Choose** and select the necessary storage policy.

10. At the **Network** step of the wizard, in the **Network mapping** section, click **Add** and select the production network to which VMs in the job are connected and network on the cloud host to which VM replicas must be connected. Repeat this step for every network to which Linux VM replicas must be connected — automatic network mapping for non-Windows VMs is not currently supported in Veeam Cloud Connect Replication.

Specifying network mapping settings may be also required, for example, if the cloud host has fewer networks than the number of networks in the production infrastructure. To learn more, see Network Mapping for Cloud Replicas.

TIP
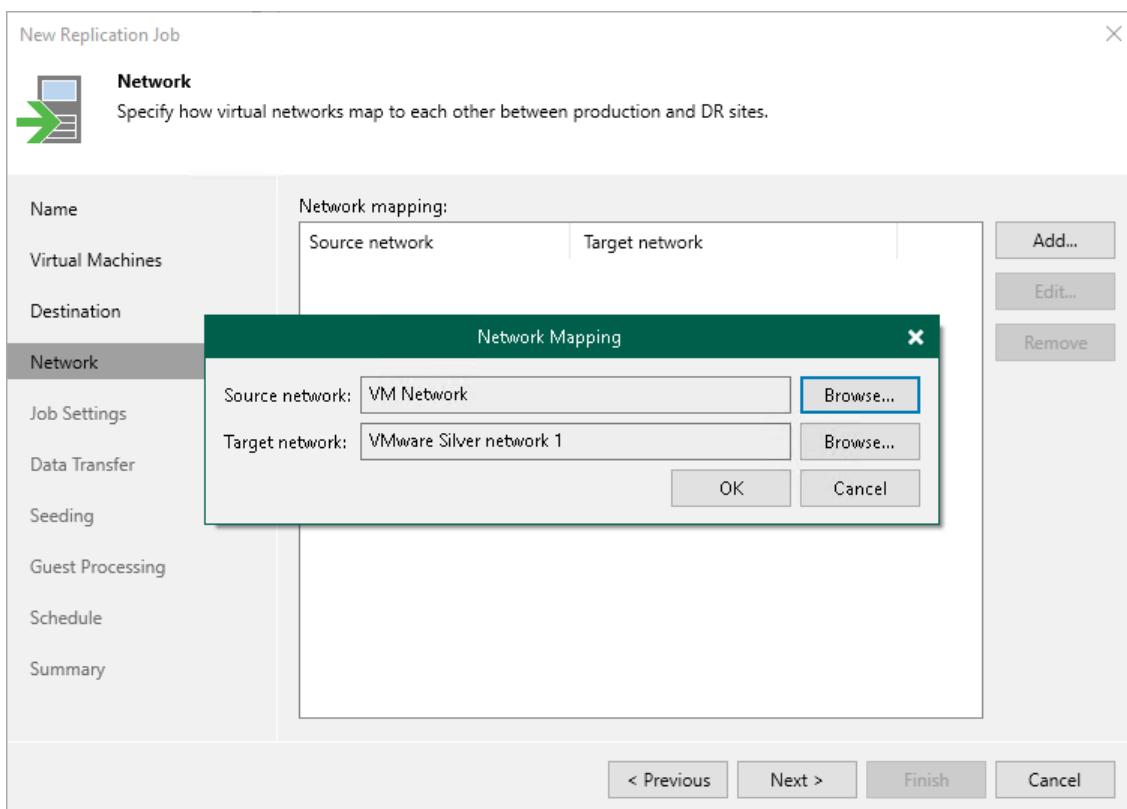
Because Veeam Cloud Connect Replication does not support automatic network mapping for non-Windows VMs, during the job performance, in the list of operations for such VMs included in the job, Veeam Backup & Replication will display a warning that no static IP addresses are detected for the VM. If in fact the VM has a static IP address and network mapping settings are specified for the VM, this warning can be ignored.
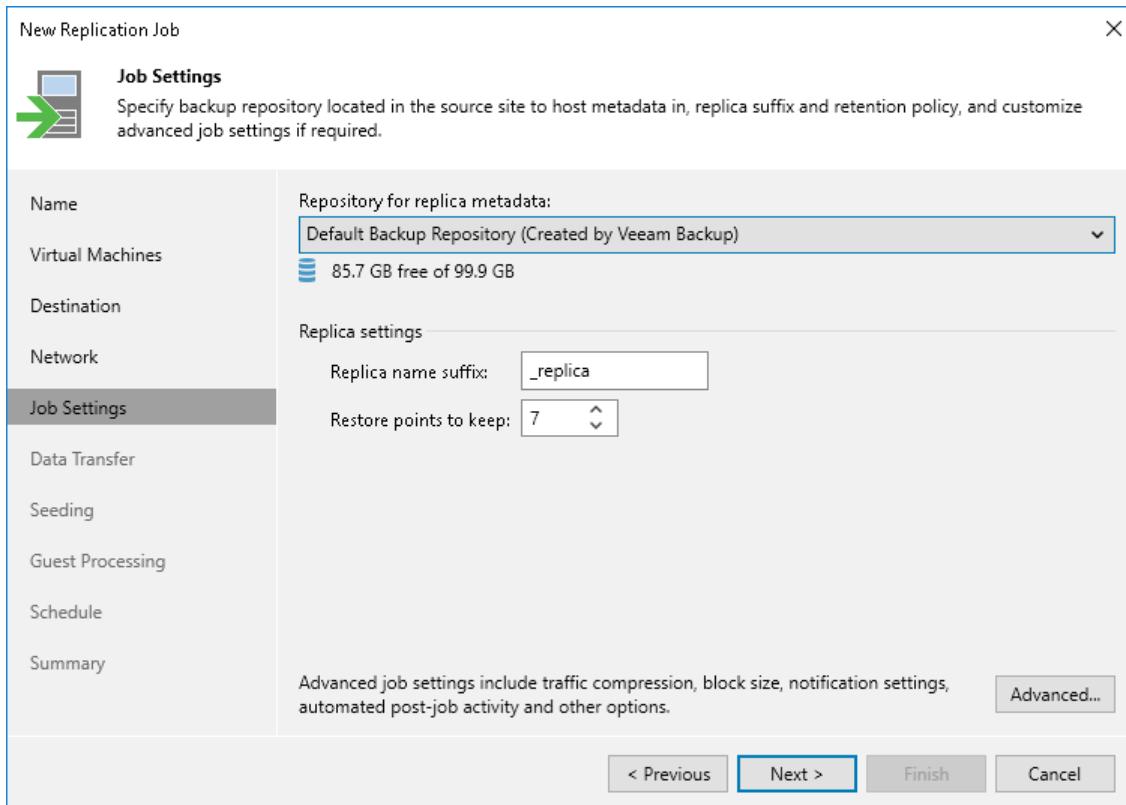
You can instruct Veeam Backup & Replication to suppress the warning. To remove the warning from the job session statistics, on the tenant Veeam backup server, create the registry value `HKEY_LOCAL_MACHINE\SOFTWARE\Veeam\Veeam Backup and Replication\CloudReplicaNoStaticIpSDetectedWarning = 0 (DWORD)` and restart Veeam Backup Service.

NOTE

[For a replication job targeted at VMware Cloud Director] You cannot map a production network to an isolated vApp network in VMware Cloud Director.
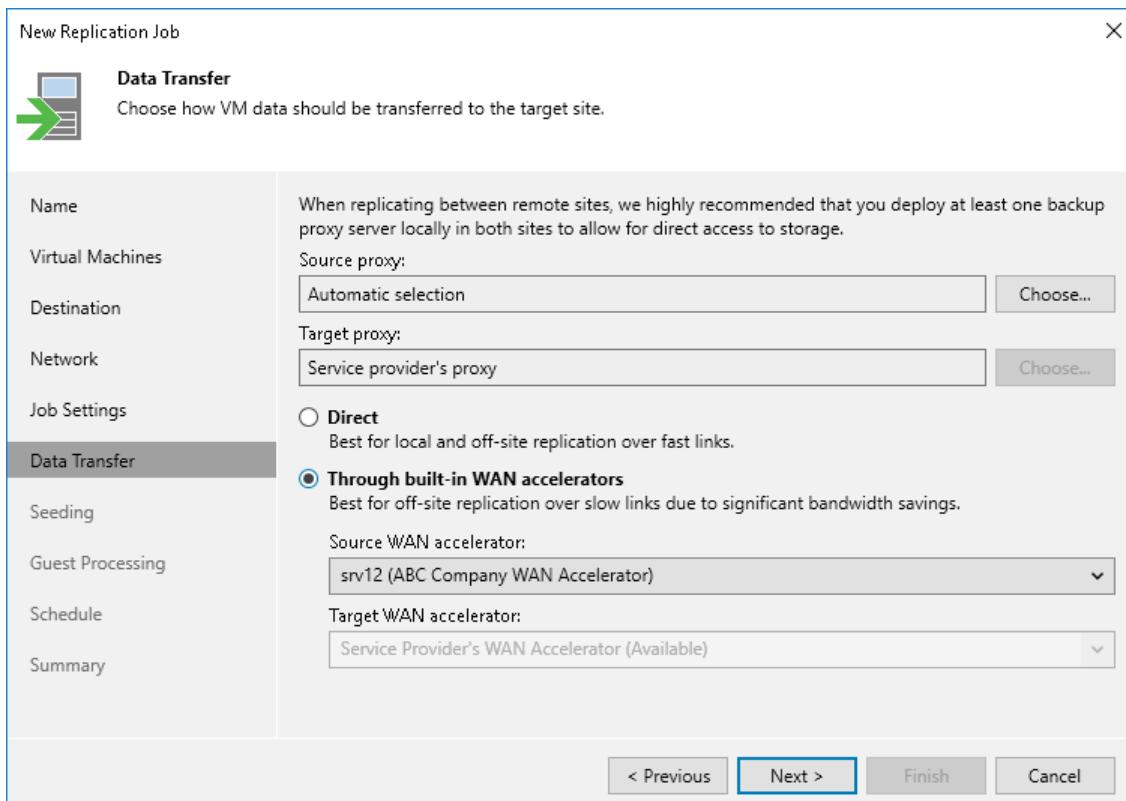
11. At the **Job Settings** step of the wizard, from the **Repository for replica metadata** list, select a regular backup repository that is configured in your backup infrastructure. Veeam Backup & Replication will store in the selected backup repository metadata for VM replicas — checksums of read data blocks required to streamline incremental runs of the replication job.

12. In the **Replica name suffix** field, enter a suffix for the name of VM replicas. To register a VM replica on the target host in the SP site, Veeam Backup & Replication appends the specified suffix to the name of the source VMs.

13. In the **Restore points to keep** field, specify the number of restore points that should be maintained by the replication job. If this number is exceeded, the earliest restore point will be deleted.

14. At the **Data Transfer** step of the wizard, select backup infrastructure components that must be used for the replication process and choose a path for VM data transfer:

   o Click **Choose** next to the **Source proxy** field to select a source backup proxy for the job. You can choose automatic backup proxy selection or assign the source backup proxy explicitly.
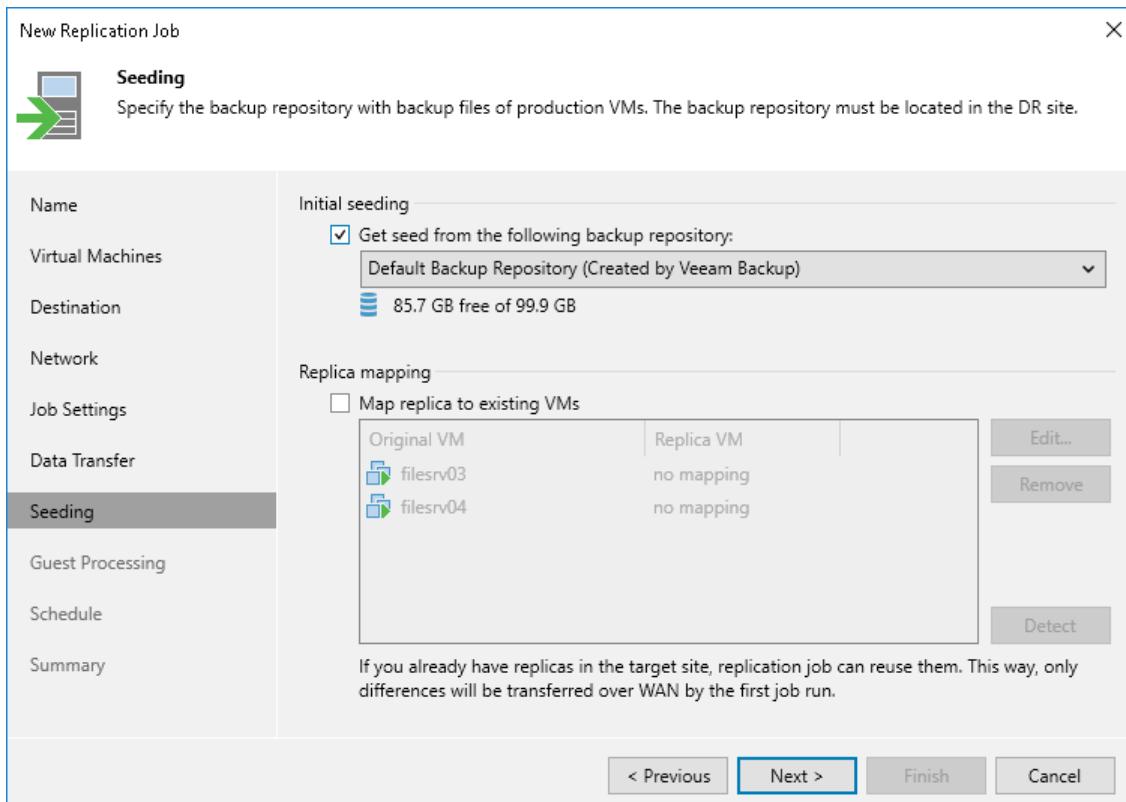
   You cannot specify a target backup proxy for the replication job targeted at the cloud host. During the replication job run, Veeam Backup & Replication will automatically select the target backup proxy configured by the SP in the SP Veeam Backup & Replication infrastructure.

   o To transport VM data directly through one or more backup proxies to the cloud host, select **Direct**.

   o To transport VM data through WAN accelerators, select **Through built-in WAN accelerators**. In the **Source WAN accelerator** field, select the WAN accelerator that you have configured on your side.
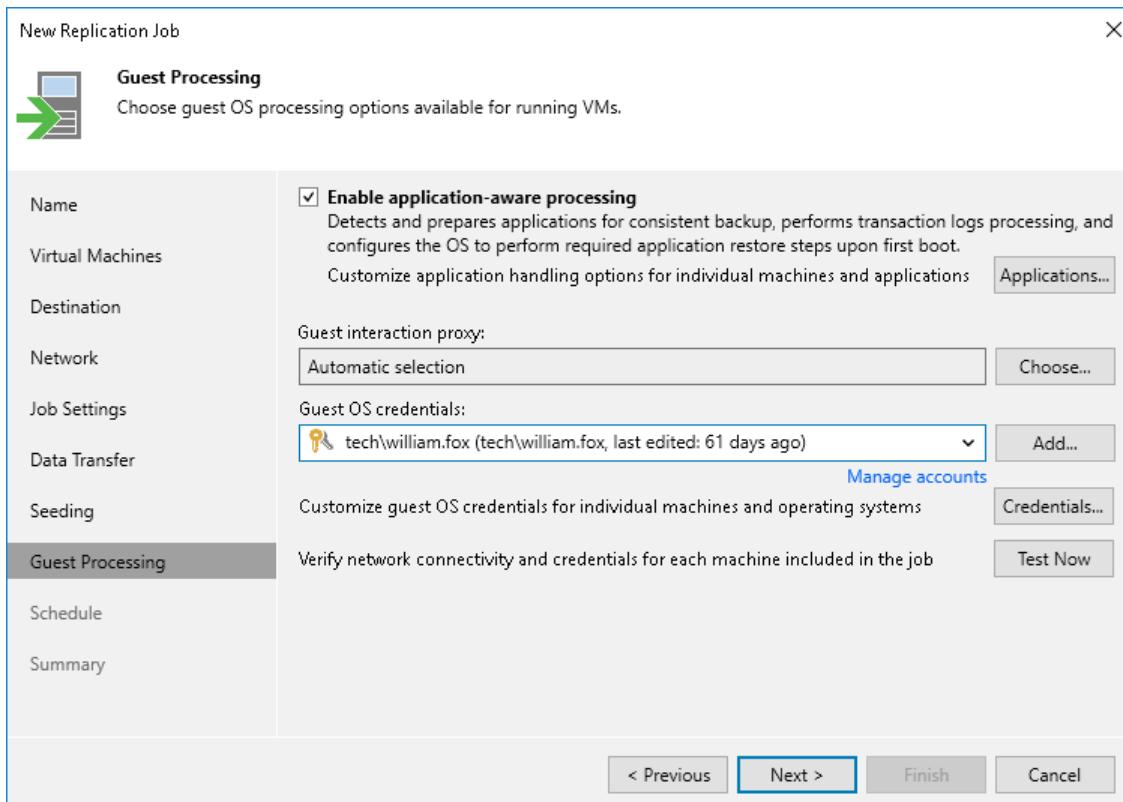
15. At the **Seeding** step of the wizard, configure replica seeding and mapping for the replication job.
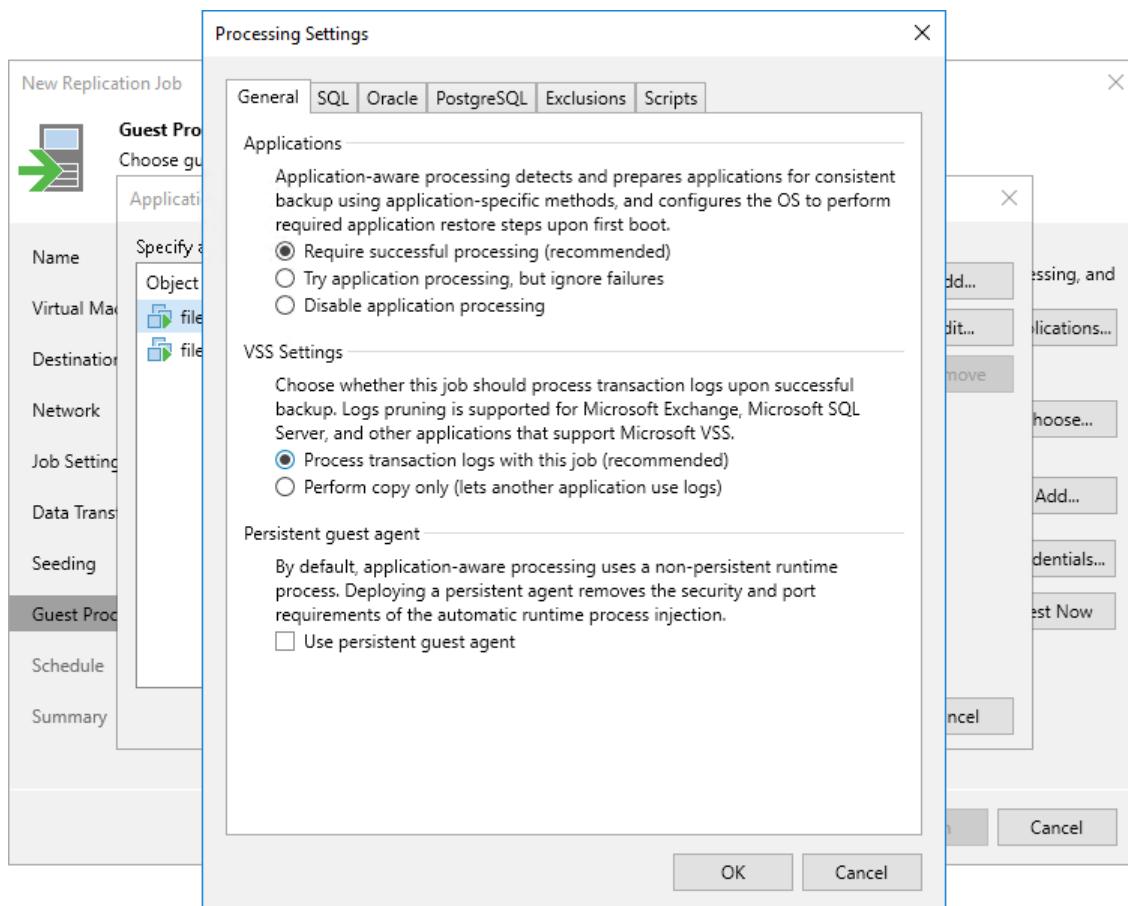
   o In the **Initial seeding** section, select the **Get seed from the following backup repository** check box. From the list of backup repositories, select the regular backup repository or cloud repository where the seed (the full backup) resides. When you start the replication job, Veeam Backup & Replication will attempt to restore all VMs added to the job from the seed that you have specified. If a VM is not found in the seed, the VM will be skipped from replication.

   o In the **Replica mapping** section, select the **Map replicas to existing VMs** check box, select a production VM from the list, click **Edit** and choose an existing VM replica. Replica mapping will reduce the amount of VM data transferred over the network during the first session of the replication job.
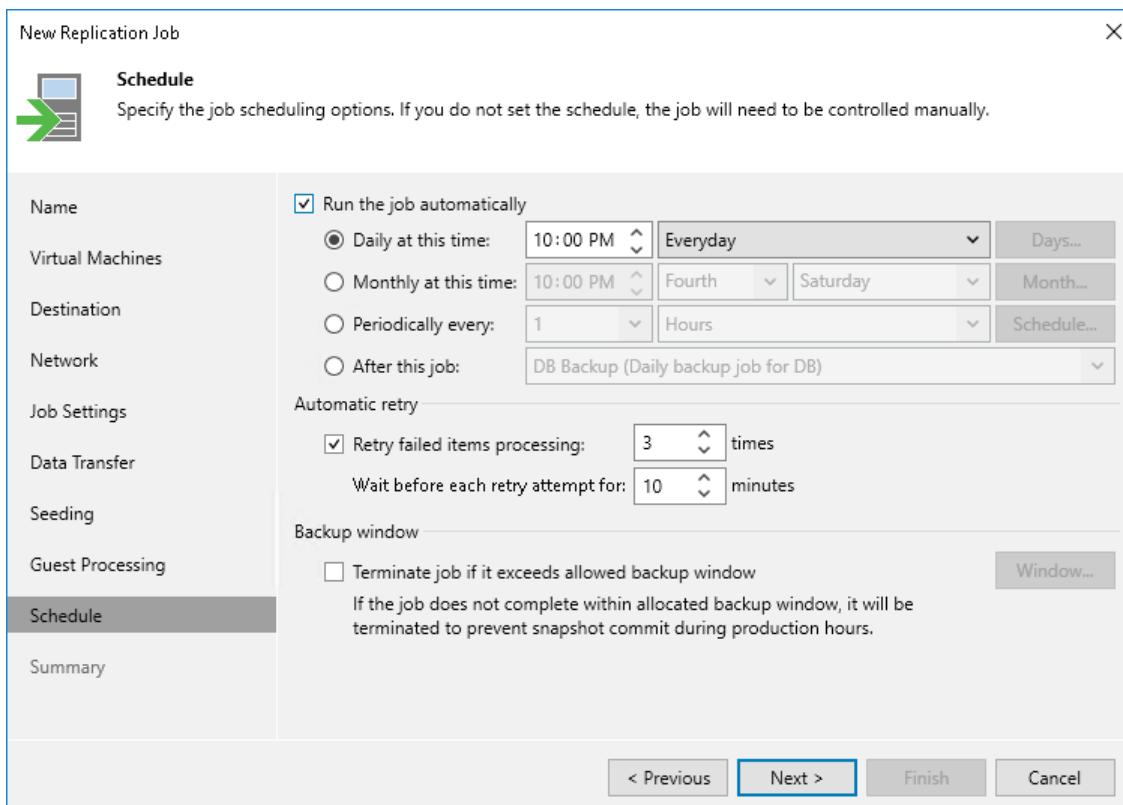
16. At the **Guest Processing** step of the wizard, select the **Enable application-aware processing** check box to create transactionally consistent VM replicas. With application-aware processing enabled, Veeam Backup & Replication can detect network settings of replicated VMs in the most efficient way and use the detected settings for configuring network extension appliances. To learn more, see Network Mapping for Cloud Replicas.

17. Click **Add** next to the **Credentials** list and specify credentials for a user account with local administrator privileges on the VM guest OS. By default, Veeam Backup & Replication uses the same credentials for all VMs added to the job. If some VM requires a different user account, click **Credentials** and enter custom credentials for the necessary VM.

18. Click **Applications**, select the necessary VM and click **Edit**. On the **General** tab, in the **Applications** section, specify the VSS behavior scenario:

    o Select **Require successful processing** if you want Veeam Backup & Replication to stop the backup process if any VSS errors occur.

    o Select **Try application processing, but ignore failures** if you want to continue the backup process even if VSS errors occur. This option is recommended to guarantee completion of the job. The created backup image will not be transactionally consistent, but crash consistent.

    o Select **Disable application processing** if you do not want to enable quiescence for the VM at all.

19. [For Microsoft SQL, Oracle and PostgreSQL VMs] In the **VSS Settings** section, specify how Veeam Backup & Replication must handle transaction logs.

    o Select **Process transaction logs with this job** if you want Veeam Backup & Replication to handle transaction logs. If you enable this option, for Microsoft SQL and Oracle VMs Veeam Backup & Replication will offer a choice of transaction log processing options on the **SQL** and **Oracle** tabs.

    o Select **Perform copy only** if you use native application means or a third-party tool to process transaction logs. Veeam Backup & Replication will create a copy-only backup for the selected VM. The copy-only backup preserves a chain of full/differential backup files and transaction logs. To learn more, see Microsoft Docs.

20. At the **Schedule** step of the wizard, select the **Run the job automatically** check box and specify the necessary scheduling settings for the job. If you do not select this check box, you will have to run the replication job manually to create restore points for VM replicas in the cloud.

21. At the **Summary** step of the wizard, select the **Run the job when I click Finish** check box if you want to start the created job right after you complete working with the wizard.

22. Click **Finish**.

Creating CDP Policies

To create CDP replicas, you must configure a CDP policy. The CDP policy defines which VMs to protect, where to store replicas, how often to create short-term and long-term restore points, and so on. One CDP policy can process one or multiple VMs.

> **NOTE**
>
> This section describes only basic steps that you must take to create a CDP policy targeted at the cloud host. To get a detailed description of all CDP policy settings, see the Creating CDP Policies section in the Veeam Backup & Replication User Guide.

To create a CDP policy:

1. On the **Home** tab, click **CDP Policy** and select **VMware vSphere**.

2. At the **Name** step of the wizard, specify a name and description for the CDP policy.

3. If you want to use advanced settings for the CDP policy:

   o Select the **Replica seeding** check box to enable the **Seeding** step in the wizard.

   o Select the **Network remapping** check box to enable the **Network** step in the wizard. Veeam Backup & Replication does not currently support automatic connection of a Linux-based VM replica to the network on the cloud host. You must use the **Network** step of the wizard to manually select source and target networks for such replicas.

   o Veeam Backup & Replication does not support re-IP rules for VM replicas on the cloud host. Do not select the **Replica re-IP** check box for the CDP policy targeted at the cloud host. If you select the **Replica re-IP** option, this option will be disabled when you select the cloud host at the **Destination** step of the wizard.

4. At the **Virtual Machines** step of the wizard, click **Add** and select VMs and VM containers that you want to replicate. To quickly find the necessary object, use the search field at the bottom of the **Add Objects** window.

> **IMPORTANT**
>
> Mind the following:
>
> - You can replicate only VMs that are turned on, the turned off VMs will be skipped from processing.
> - You cannot add to a CDP policy VMs that were already added to other CDP policies created on the same backup server.
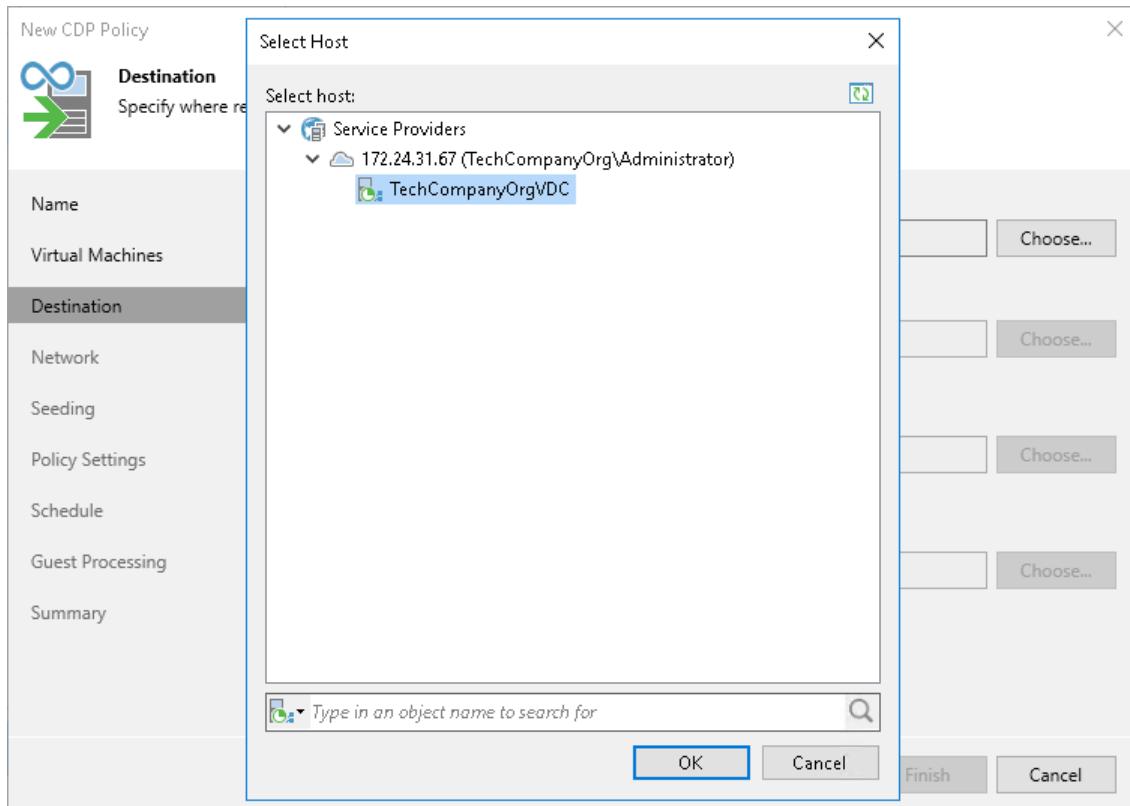
5. If you want to exclude VMs from the VM container or replicate only specific VM disks, click **Exclusions** and specify what objects you want to exclude.

6. If you want to define the order in which the CDP policy must process VMs, select a VM or VM container added to the policy and use the **Up** and **Down** buttons on the right to move the VM or VM container up or down in the list.

7. At the **Destination** step of the wizard, in the **Host or cluster** section, click **Choose** and select **Cloud host**. Then select the cloud host allocated to you by the SP:

   o If the SP allocated to you replication resources on a VMware vSphere host, select the cloud host provided to you through a hardware plan.

o If the SP allocated to you replication resources in VMware Cloud Director, select the cloud host provided to you through an organization VDC.
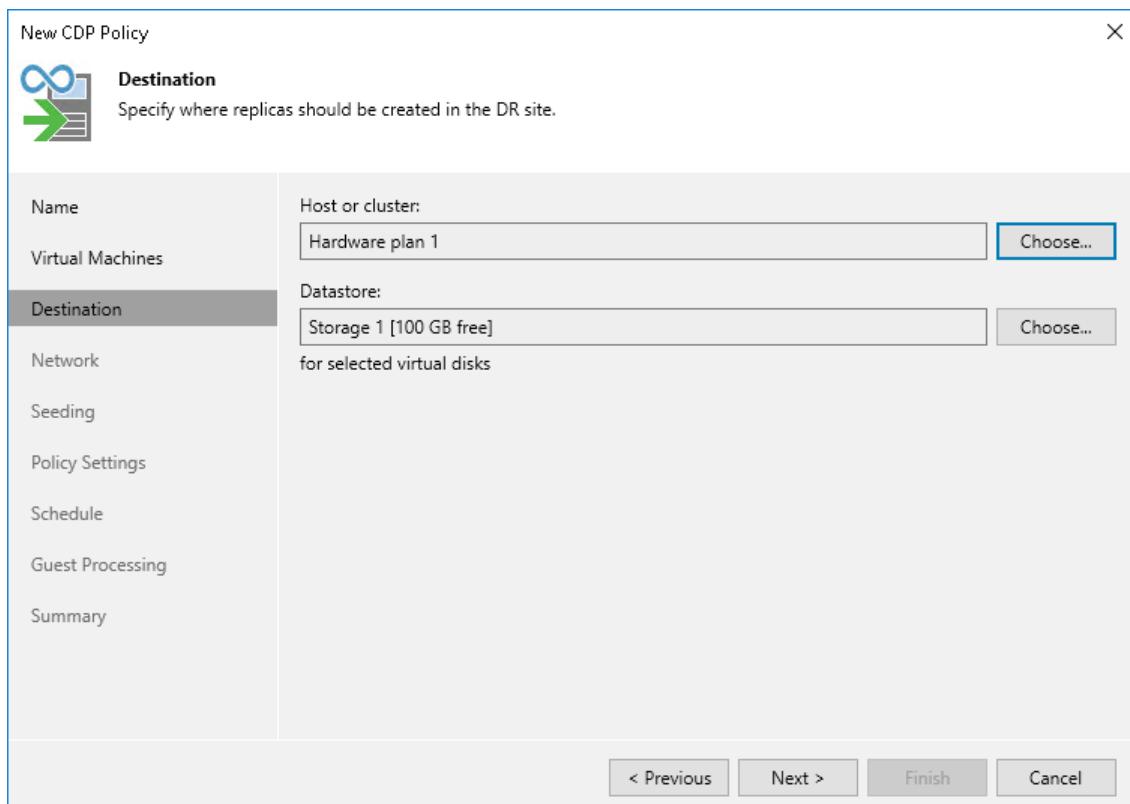
> **NOTE**
>
> After you select an organization VDC, the name of the **Host or cluster** section will change to **Organization VDC**.

Note that after the CDP policy is performed for the first time, you will not be able to change the target host for the CDP policy.

8. At the **Destination** step of the wizard, select storage resources allocated to you by the SP:

   o [For a For a CDP policy targeted at VMware vSphere] If you want to specify a datastore on which to store VM replicas, in the **Datastore** section, click **Choose** and select the necessary datastore.
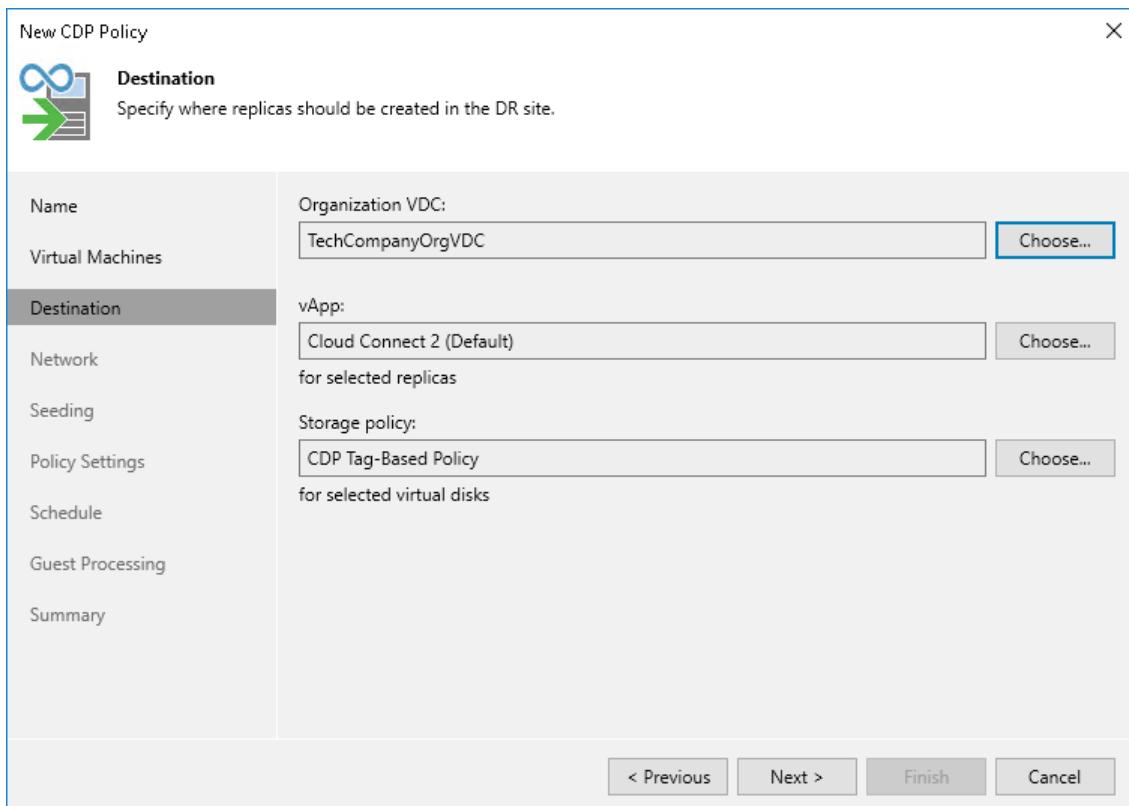
o [For a CDP policy targeted at VMware Cloud Director] If you want to specify a vApp or storage policy for VM replicas, do the following:

   i. In the **vApp** section, click **Choose** and select the necessary vApp.

      Note that you must not use the same vApp as a target for both a CDP policy and a snapshot-based replication job.

   ii. In the **Storage policy** section, click **Choose** and select the necessary storage policy.

9. At the **Network** step of the wizard, in the **Network mapping** section, click **Add** and select the production network to which VMs added to the CDP policy are connected and network on the cloud host to which VM replicas must be connected.

   You must specify network mapping settings in the following cases:

   o If you added Microsoft Windows VMs to the CDP policy and do not plan to enable application-aware processing for these VMs at the **Guest Processing** step of the wizard.

   o If you added Linux VMs to the CDP policy. Automatic network mapping for non-Windows VMs is not currently supported in Veeam Cloud Connect Replication.

   o If the cloud host has fewer networks than the number of networks in the production infrastructure.

   To learn more, see Network Mapping for Cloud Replicas.
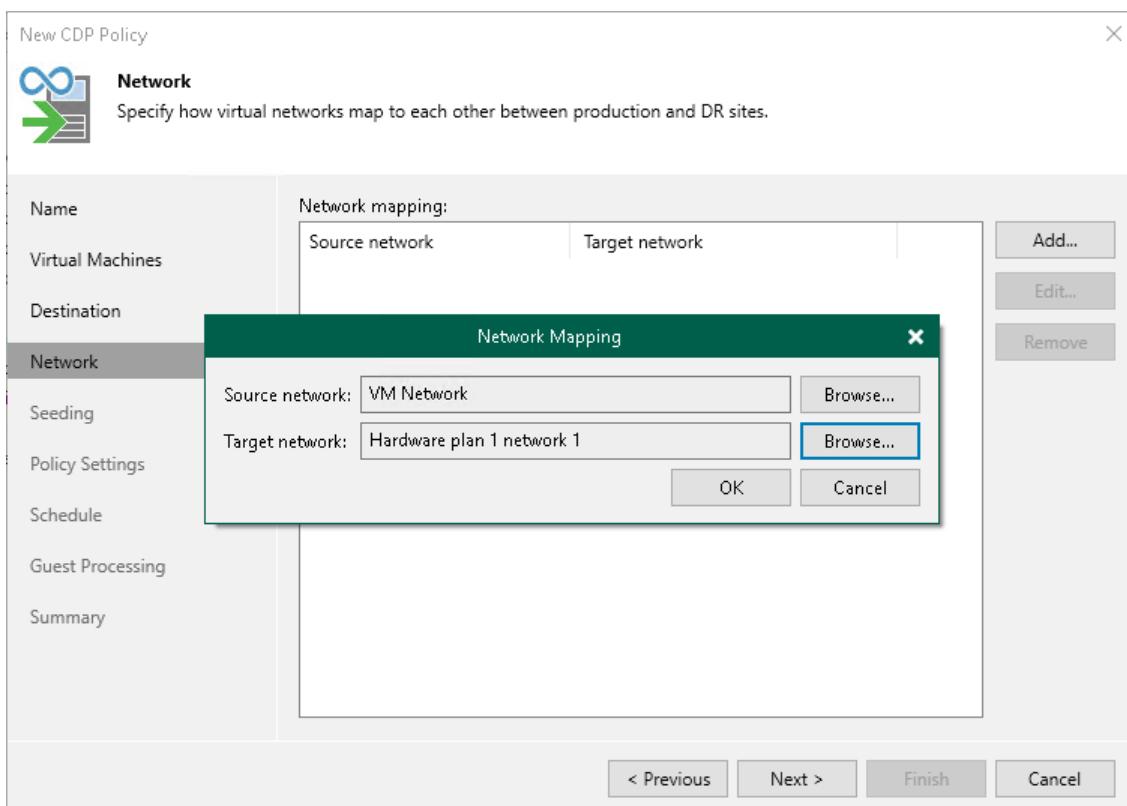
   > **NOTE**
   >
   > [For a CDP policy targeted at VMware Cloud Director] You cannot map a production network to an isolated vApp network in VMware Cloud Director.

TIP
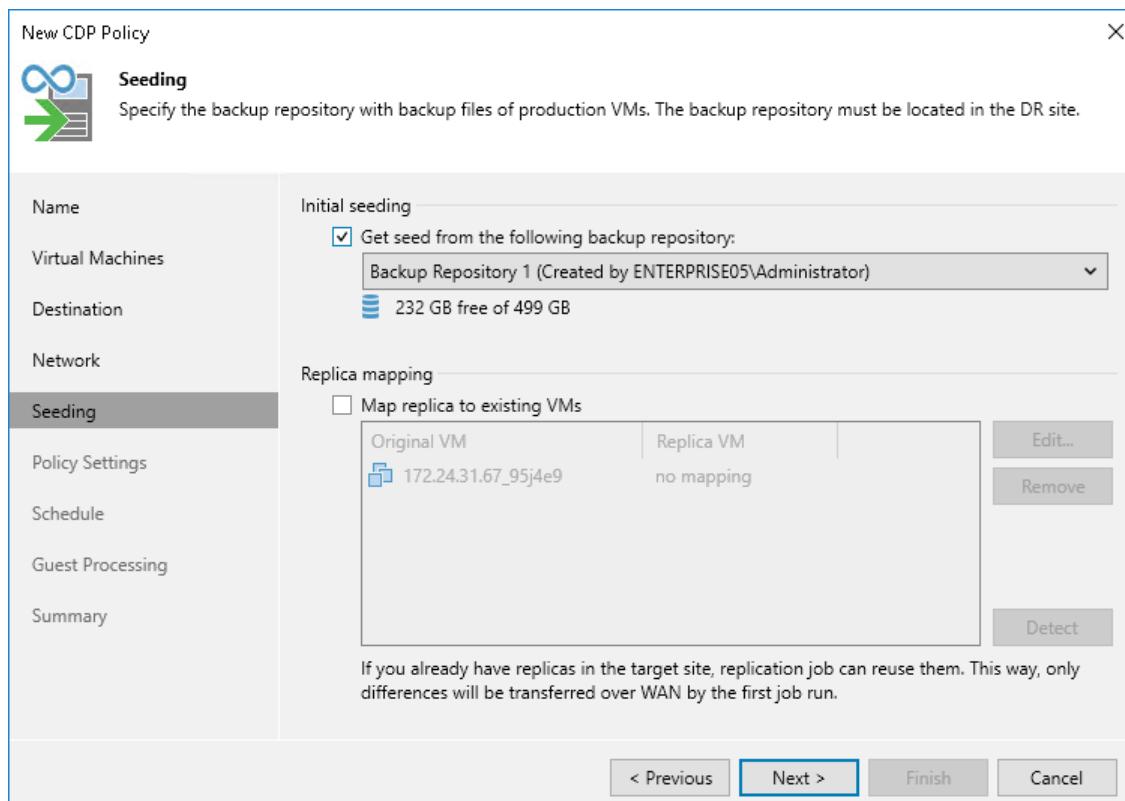
Because Veeam Cloud Connect Replication does not support automatic network mapping for non-Windows VMs, during the CDP policy performance, in the list of operations for such VMs in the CDP policy, Veeam Backup & Replication will display a warning that no static IP addresses are detected for the VM. If in fact the VM has a static IP address and network mapping settings are specified for the VM, this warning can be ignored.

You can instruct Veeam Backup & Replication to suppress the warning. To remove the warning from the CDP policy session statistics, on the tenant Veeam backup server, create the registry value `HKEY_LOCAL_MACHINE\SOFTWARE\Veeam\Veeam Backup and Replication\CloudReplicaNoStaticIpSDetectedWarning = 0 (DWORD)` and restart Veeam Backup Service.

10. At the **Seeding** step of the wizard, configure replica seeding and mapping for the CDP policy.

   o In the **Initial seeding** section, select the **Get seed from the following backup repository** check box. From the list of backup repositories, select the regular backup repository or cloud repository where the seed (the full backup) resides. When you start the CDP policy, Veeam Backup & Replication will attempt to restore all VMs added to the CDP policy from the seed that you have specified. If a VM is not found in the seed, the VM will be skipped from replication.

   o In the **Replica mapping** section, select the **Map replicas to existing VMs** check box, select a production VM from the list, click **Edit** and choose an existing VM replica. Replica mapping will reduce the amount of VM data transferred over the network during the first session of the CDP policy.

11. At the **Policy Settings** step of the wizard, click **Choose** next to the **Source proxy** field to select a source VMware CDP proxy for the CDP policy. You can choose automatic proxy selection or assign the source proxy explicitly.

You cannot specify a target proxy for the CDP policy targeted at the cloud host. During the CDP policy run, Veeam Backup & Replication will automatically select the target CDP proxy configured by the SP in the SP backup infrastructure.

12. In the **Replica name suffix** field, enter a suffix for the name of VM replicas. To register a VM replica on the target host in the SP site, Veeam Backup & Replication appends the specified suffix to the name of the source VMs.

13. At the **Schedule** step of the wizard, configure schedule and retention policy settings for the CDP policy:

a. In the **Recovery Point Objective** field, specify the necessary RPO in seconds or minutes, that is, how often to create short-term restore points. The minimum RPO is 2 seconds, however it can be not optimal if your CDP policy contains many VMs with high workload. The optimal RPO is not less than 15 seconds. The maximum RPO is 60 minutes.

During every specified period, Veeam Backup & Replication will prepare data for short-term restore points for VM replicas and send this data to the target destination. Note that short-term restore points are crash-consistent.

b. To instruct the CDP policy to display a warning or error if a newly created restore points are not transferred to the target within the set RPO, click **Reporting**. Then specify when the policy must display error and warning. If you configured email notification settings, Veeam Backup & Replication will mark the policy with the *Warning* or *Error* status and will also send email notifications.

c. In the **Short-term retention** section, configure the short-term retention policy, that is, specify for how long to store short-term restore points.

d. In the **Long-term retention** section, specify when to create long-term restore points and for how long to store them.

e. To specify time periods when Veeam Backup & Replication must create application-consistent and crash-consistent long-term restore points, click **Schedule**, then click **Crash-consistent** or **Application-consistent** and select the necessary time area. By default, Veeam Backup & Replication creates application-consistent backups if you enable application-aware processing at the **Guest Processing** step of the wizard. If you do not enable application-aware processing, Veeam Backup & Replication will create crash-consistent long-term restore points.
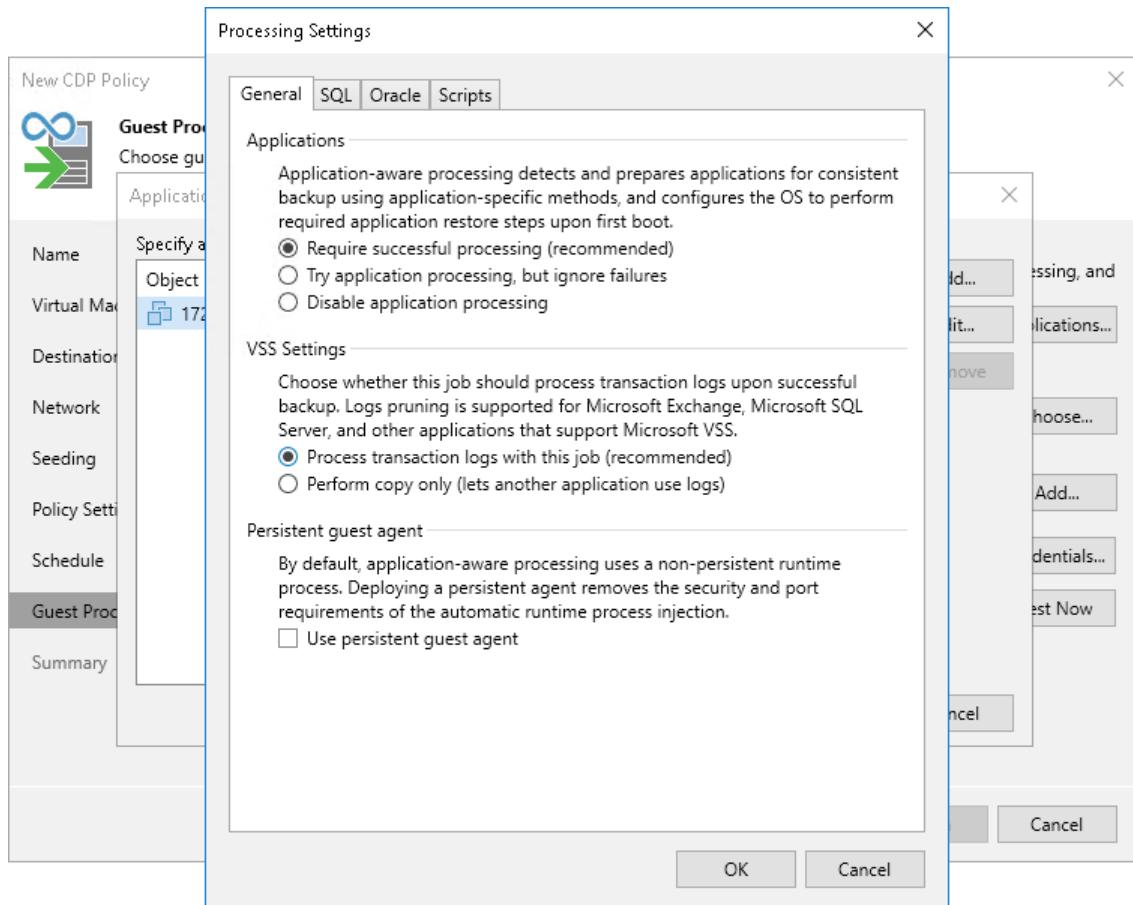
14. At the **Guest Processing** step of the wizard, select the **Enable application-aware processing** check box to create transactionally consistent VM replicas. With application-aware processing enabled, Veeam Backup & Replication can detect network settings of replicated VMs in the most efficient way and use the detected settings for configuring network extension appliances. To learn more, see Network Mapping for Cloud Replicas.

15. Click **Add** next to the **Credentials** list and specify credentials for a user account with local administrator privileges on the VM guest OS. By default, Veeam Backup & Replication uses the same credentials for all VMs added to the CDP policy. If some VM requires a different user account, click **Credentials** and enter custom credentials for the necessary VM.

16. Click **Applications**, select the necessary VM and click **Edit**. On the **General** tab, in the **Applications** section, specify the VSS behavior scenario:

    o Select **Require successful processing** if you want Veeam Backup & Replication to stop the backup process if any VSS errors occur.

    o Select **Try application processing, but ignore failures** if you want to continue the backup process even if VSS errors occur. This option is recommended to guarantee completion of the CDP policy. The created backup image will not be transactionally consistent, but crash consistent.

    o Select **Disable application processing** if you do not want to enable quiescence for the VM at all.

17. [For Microsoft SQL and Oracle VMs] In the **VSS Settings** section, specify how Veeam Backup & Replication must handle transaction logs.

    o Select **Process transaction logs with this job** if you want Veeam Backup & Replication to handle transaction logs. With this option enabled, Veeam Backup & Replication will offer a choice of transaction log processing options on the **SQL** and **Oracle** tabs.

    o Select **Perform copy only** if you use native application means or a third-party tool to process transaction logs. Veeam Backup & Replication will create a copy-only backup for the selected VM. The copy-only backup preserves a chain of full/differential backup files and transaction logs. To learn more, see Microsoft Docs.

> **NOTE**
>
> CDP policies targeted at the cloud host do not support application-aware processing of PostgreSQL VMs.

18. At the **Summary** step of the wizard, select the **Enable the policy when I click Finish** check box if you want to start the created CDP policy right after you complete working with the wizard.

19. Click **Finish**.

Performing Full Site Failover

You can preset scenarios for one-click failover for a group of interdependent production VMs to the cloud host — full site failover. To do this, you must create a cloud failover plan. You must create the cloud failover plan in advance, for example, right after you created VM replicas on a cloud host. In case the whole production site goes offline for any reason, you can run the cloud failover plan to perform full site failover.

Creating Cloud Failover Plans

If you have a number of VMs running interdependent applications, you need to fail over them one by one, as a group. To do this automatically, you can prepare a cloud failover plan.

Before You Begin

Before you create a cloud failover plan, check the following prerequisites and limitations:

- VMs that you plan to include in the failover plan must be successfully replicated at least once.

- You cannot select to use pre-failover and/or post-failover scripts for the cloud failover plan. As tenant cloud failover plans and VM replicas are stored on the SP side, the responsibility to create and manage scripts lays on the SP. To use pre-failover and/or post-failover scripts, the SP must create those scripts in advance and select them in the cloud failover plan settings before you run the cloud failover plan. Veeam Backup & Replication supports script files in BAT and CMD formats and executable files in the EXE format.

- You cannot use the same cloud failover plan for full site failover of snapshot-based replicas and CDP replicas.

Step 1. Launch Cloud Failover Plan Wizard

To launch the **Cloud Failover Plan** wizard, do one of the following:

- On the **Home** tab, click **Failover Plan** and select *Cloud Connect (vSphere) or Cloud Connect (Hyper-V)*.

- Open the **Home** view, click the **Replicas** node in the inventory pane, right-click the **Failover Plans** node and click **Failover plan > Cloud Connect (vSphere)** or **Cloud Connect (Hyper-V)**. This option is available if you have already configured at least one failover plan.

- Open the **Home** view, click the **Replicas** node in the inventory pane, select one or several VMs in the working area, click **Add to Failover Plan** > **New cloud failover plan** on the ribbon or right-click one or several VMs in the working area and select **Add to failover plan** > **New cloud failover plan**. In this case, the selected VMs will be automatically included into the failover plan. You can add other VMs to the failover plan when passing through the wizard steps.

Step 2. Specify Failover Plan Name and Description

At the **Failover Plan** step of the wizard, specify a name and description for the failover plan.

1. In the **Name** field, enter a name for the failover plan.

2. In the **Description** field, provide a description for future reference. The default description contains information about the user who created a failover plan, date and time when the plan was created.

Step 3. Select Virtual Machines
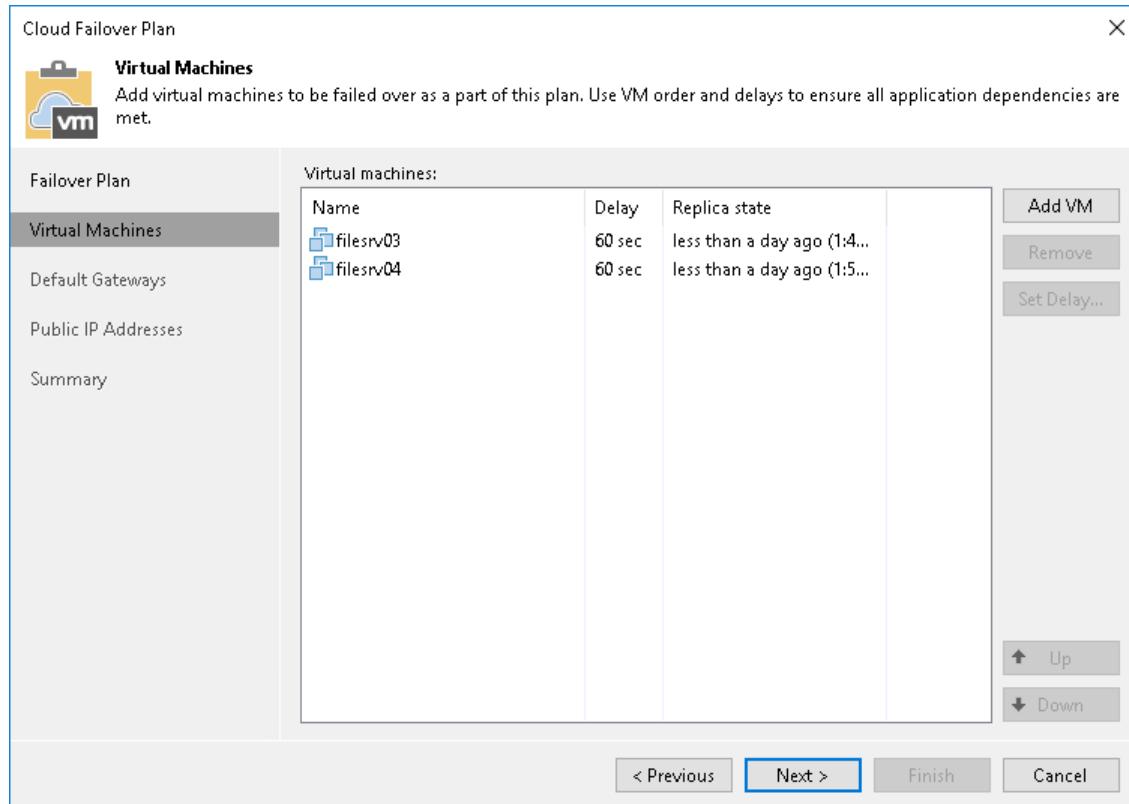
At the **Virtual Machines** step of the wizard, select VMs that you want to add to the cloud failover plan. You can add separate VMs from the list of VMs that are added to the replication jobs targeted at the cloud host.

To add VMs:

1. Click **Add VM**.

2. Browse existing replication jobs targeted at the cloud host and select all VMs or specific VMs from replication jobs.

   To quickly find VMs, you can use the search field at the bottom of the **Select Replica** window. Enter a VM name or a part of it in the search field and click **Start search** or press **[ENTER]**.

3. [Optional] If you want to set a time delay for VM start during failover, select the VM, click **Set Delay** and specify the necessary delay in the **Boot Delay** window. This option may be helpful if you want to make sure that some VMs are already running at the moment dependent VMs start. If you do not specify the time delay, VMs will be started simultaneously.

Step 4. Specify Default Gateways

At the **Default Gateways** step of the wizard, check and, if necessary, specify default gateways in every IP network in the production site that are used by VMs added to the cloud failover plan. The network extension appliance on the cloud host will use network settings of the specified gateways to route traffic between VM replica networks and external networks after full site failover.

Veeam Backup & Replication automatically specifies default gateways in detected production networks during the first run of the replication job targeted at the cloud host. If, for some reason, the list of default gateways at the **Default Gateways** step of the wizard is empty, you should specify default gateways manually.

To specify default gateways, click **Manage default gateways** at the bottom of the **Cloud Failover Plan** wizard window. Then use the **Default Gateways** window to specify default gateway settings. To learn more, see Managing Default Gateways.

Step 5. Specify Public IP Addressing Rules

At the **Public IP Addresses** step of the wizard, specify IP addressing settings for VM replicas. You can create one or several public IP addressing rules to make a VM replica accessible over the internet by a public IP address that the SP has provided to you through the hardware plan.

When your production VM fails over to its replica during full site failover, Veeam Backup & Replication assigns the public IP address that is specified in the rule to the network extension appliance on the cloud host. The network extension appliance redirects traffic from this public IP address to the IP address of a VM replica in the internal VM replica network. As a result, a VM replica for which you have created the public IP addressing rule can be accessed over the internet like a production VM without interrupting the production site operation.
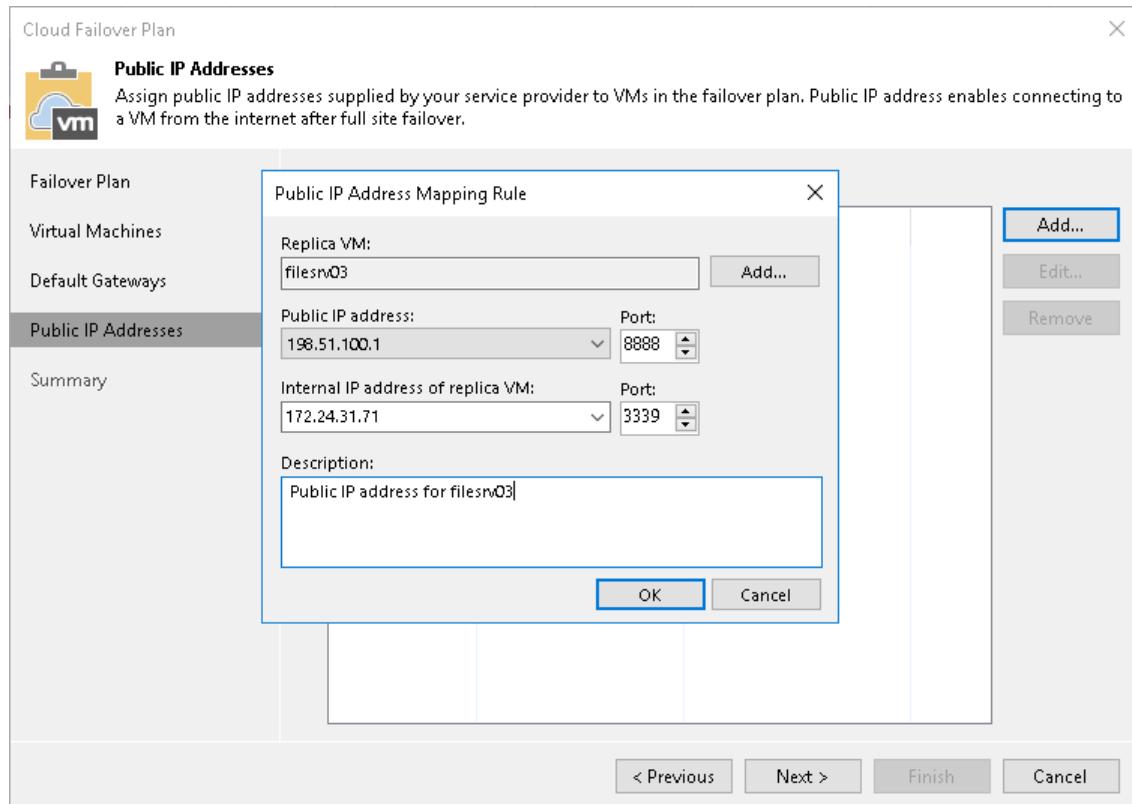
To create a public IP address mapping rule:

1. Select the **Assign public IP addresses to use during full site failover** option and click **Add**.

2. In the **Public IP Address Mapping Rule** window, in the **Replica VM** field, click **Add VM** and select a VM replica that you want to make accessible over the internet.

3. In the **Public IP address** field, select a public IPv4 or IPv6 address from the list of IP addresses allocated to you by the SP. In the **Port** field, specify the number of the port on the SP network extension appliance from which Veeam Backup & Replication will redirect traffic to the VM replica.

   You cannot specify port 22 as a port for the public IP address that is assigned to the network extension appliance. Veeam Backup & Replication uses this port for communication with the network extension appliance.

4. In the **Internal IP address of replica VM** field, select the IP address of the VM replica in the internal network. In the **Port** field, specify the number of the network port on the VM replica to which Veeam Backup & Replication will redirect traffic from the network extension appliance.

   For Linux-based VM replicas, you must specify the internal IP address manually, because Veeam Backup & Replication cannot detect an IP address of a Linux-based VM in the tenant's production network.

5. In the **Description** field, provide a description for future reference.
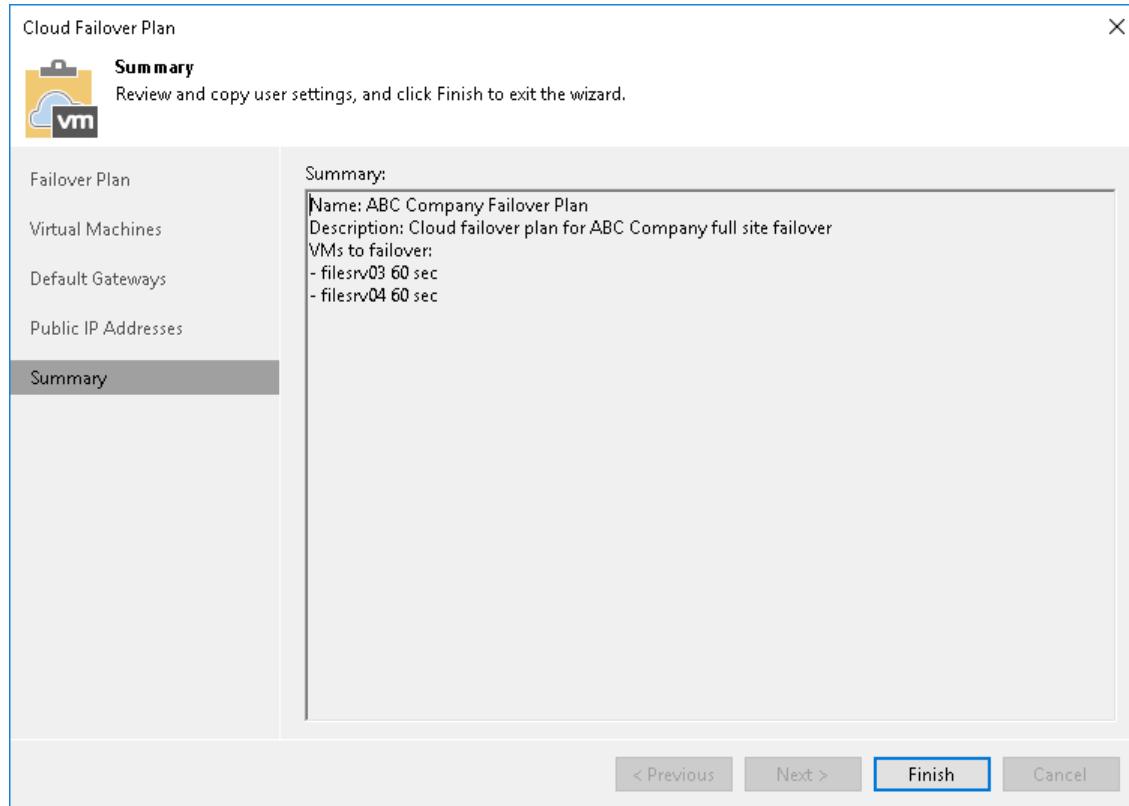
6. Click **OK**.

Step 6. Review Summary and Finish Working with Wizard

At the **Summary** step of the wizard, complete the procedure of a cloud failover plan creation.

1. Review the configuration information on the created cloud failover plan.

2. Click **Finish** to exit the wizard.

Creating Cloud Failover Plans for Replicas in VMware Cloud Director

If you have a number of VMs running interdependent applications, you need to fail over them one by one, as a group. To do this automatically, you can prepare a cloud failover plan.

The process of creating a cloud failover plan for VMs whose replicas reside in VMware Cloud Director differs from the regular one. The difference is that you do not need to specify default gateway settings and public IP addressing rules for such VMs. Network resources required to provide access to VM replicas from the internet after full site failover are managed by the SP in VMware Cloud Director.

Before You Begin

Before you create a cloud failover plan, check the following prerequisites and limitations:

- VMs that you plan to include in the failover plan must be successfully replicated at least once.

- You cannot select to use pre-failover and/or post-failover scripts for the cloud failover plan. As tenant cloud failover plans and VM replicas are stored on the SP side, the responsibility to create and manage scripts lays on the SP. To use pre-failover and/or post-failover scripts, the SP must create those scripts in advance and select them in the cloud failover plan settings before you run the cloud failover plan. Veeam Backup & Replication supports script files in BAT and CMD formats and executable files in the EXE format.

- You cannot use the same cloud failover plan for full site failover of snapshot-based replicas and CDP replicas.

Step 1. Launch Cloud Failover Plan Wizard

To launch the **Cloud Failover Plan** wizard, do one of the following:

- On the **Home** tab, click **Failover Plan** and select **Cloud Connect (vCloud)**.

- Open the **Home** view, click the **Replicas** node in the inventory pane, right-click the **Failover Plans** node and click **Failover plan > Cloud Connect (vCloud)**. This option is available if you have already configured at least one failover plan.

- Open the **Home** view, click the **Replicas** node in the inventory pane, select one or several VMs in the working area, click **Add to Failover Plan > New VMware Cloud Director failover plan** on the ribbon or right-click one or several VMs in the working area and select **Add to failover plan > New VMware Cloud Director failover plan**. In this case, the selected VMs will be automatically included into the failover plan. You can add other VMs to the failover plan when passing through the wizard steps.

Step 2. Specify Failover Plan Name and Description

At the **Failover Plan** step of the wizard, specify a name and description for the cloud failover plan.

1. In the **Name** field, enter a name for the cloud failover plan.

2. In the **Description** field, provide a description for future reference. The default description contains information about the user who created a failover plan, date and time when the plan was created.

Step 3. Select Virtual Machines
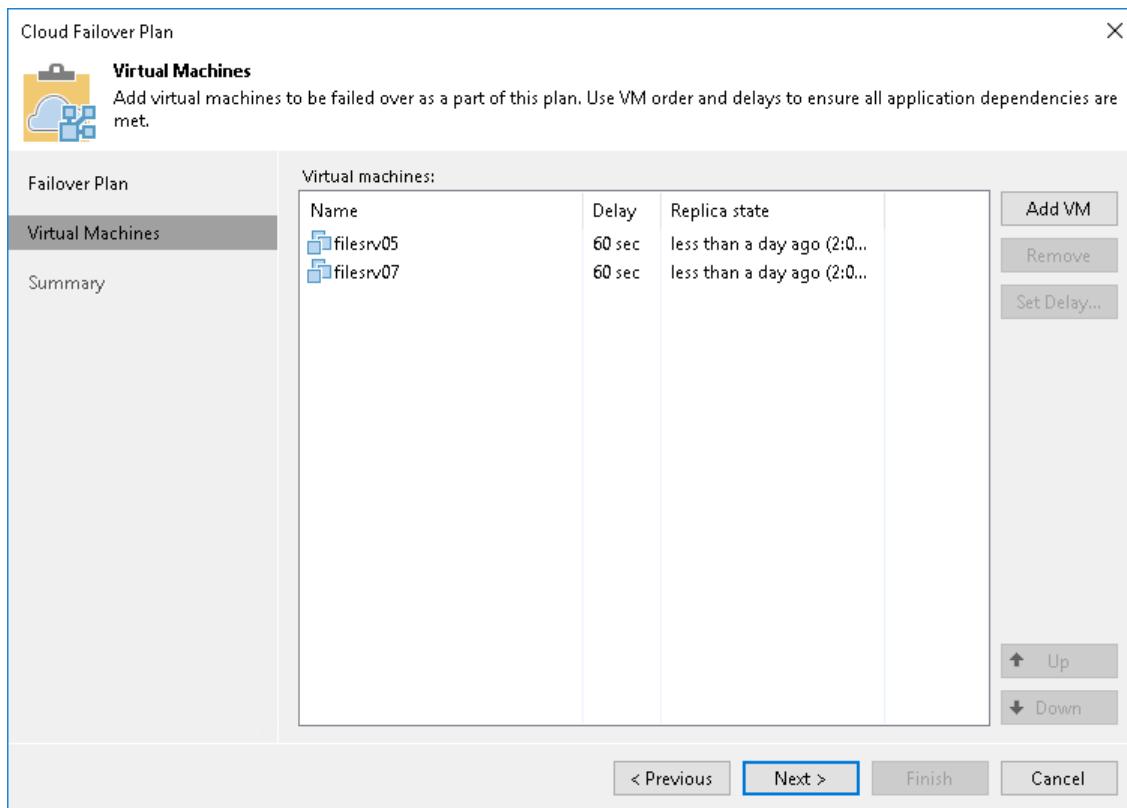
At the **Virtual Machines** step of the wizard, select VMs that you want to add to the cloud failover plan. You can add to a cloud failover plan separate VMs for which a replication job created at least one restore point on a cloud host.

To add VMs:

1. Click **Add VM**.

2. Browse existing replication jobs targeted at the cloud host and select all VMs or specific VMs from replication jobs.

   To quickly find VMs, you can use the search field at the bottom of the **Select Replica** window. Enter a VM name or a part of it in the search field and click **Start search** or press **[ENTER]**.
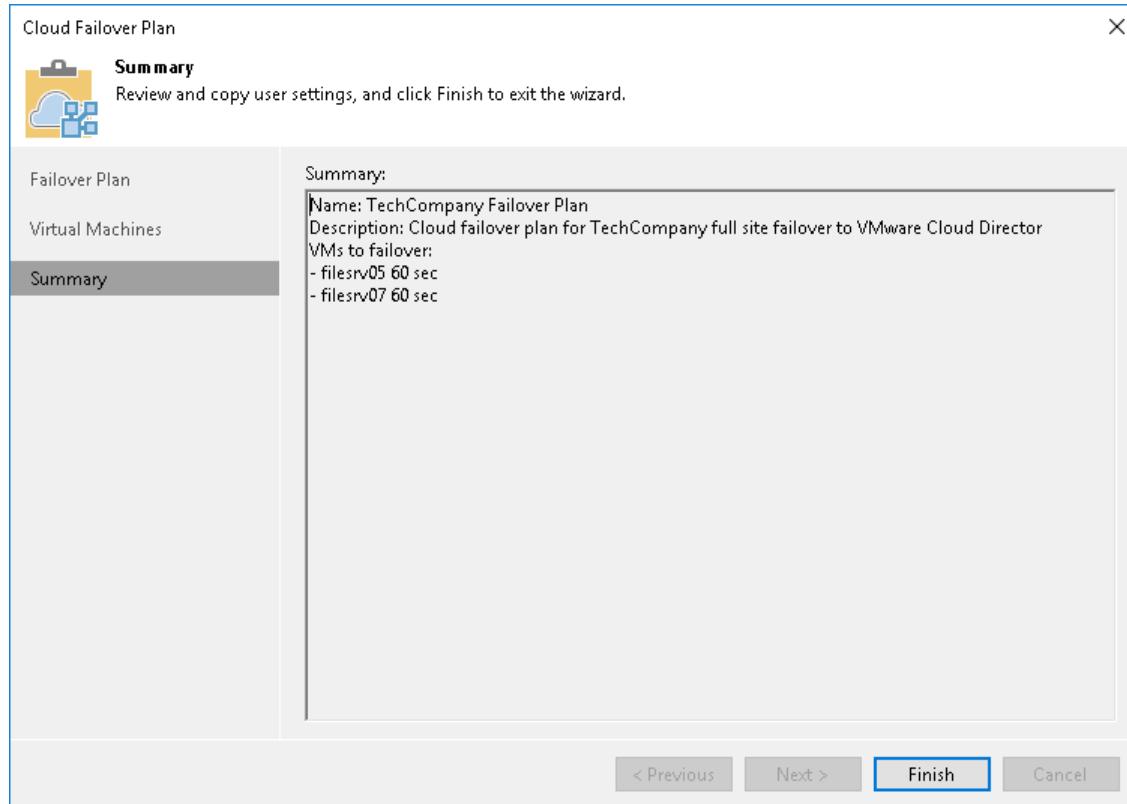
3. [Optional] If you want to set a time delay for VM start during failover, select the VM, click **Set Delay** and specify the necessary delay in the **Boot Delay** window. This option may be helpful if you want to make sure that some VMs are already running at the moment dependent VMs start. If you do not specify the time delay, VMs will be started simultaneously.

Step 4. Review Summary and Finish Working with Wizard

At the **Summary** step of the wizard, complete the procedure of a cloud failover plan creation.

1. Review the configuration information on the created cloud failover plan.

2. Click **Finish** to exit the wizard.

Running Cloud Failover Plan

With a cloud failover plan, you can perform full site failover at any time. During full site failover, tenant VMs fail over to their replicas on the cloud host one by one, as a group. You can fail over to the most recent VM state or select the necessary restore point for VMs in the cloud failover plan.

To fail over to the VM replicas latest restore point:

1. Open the **Home** view.

2. In the inventory pane, expand the **Replicas** node and click **Failover Plans**.

3. In the working area, right-click the necessary cloud failover plan and select **Start**.

To fail over to a certain restore point:

1. Open the **Home** view.

2. In the inventory pane, expand the **Replicas** node and click **Failover Plans**.

3. In the working area, right-click the necessary cloud failover plan and select **Start to**.

4. In the **Choose Restore Point** window, select the backup date and time. Veeam Backup & Replication will find the closest restore point prior to the entered value for each VM and fail over to it.

Testing Cloud Failover Plan

You can test a cloud failover plan to ensure replicated VMs on the cloud host successfully start and can be accessed from external network after failover. When you test a cloud failover plan, Veeam Backup & Replication does not switch from a production VM to its replica. Instead, it reverts every VM replica in the cloud failover plan to the latest restore point, boots the replica operation system, waits for the VM replica to reach a "stabilization point" using the *Stabilization by IP* algorithm and checks if the VM replica responds to ping requests.
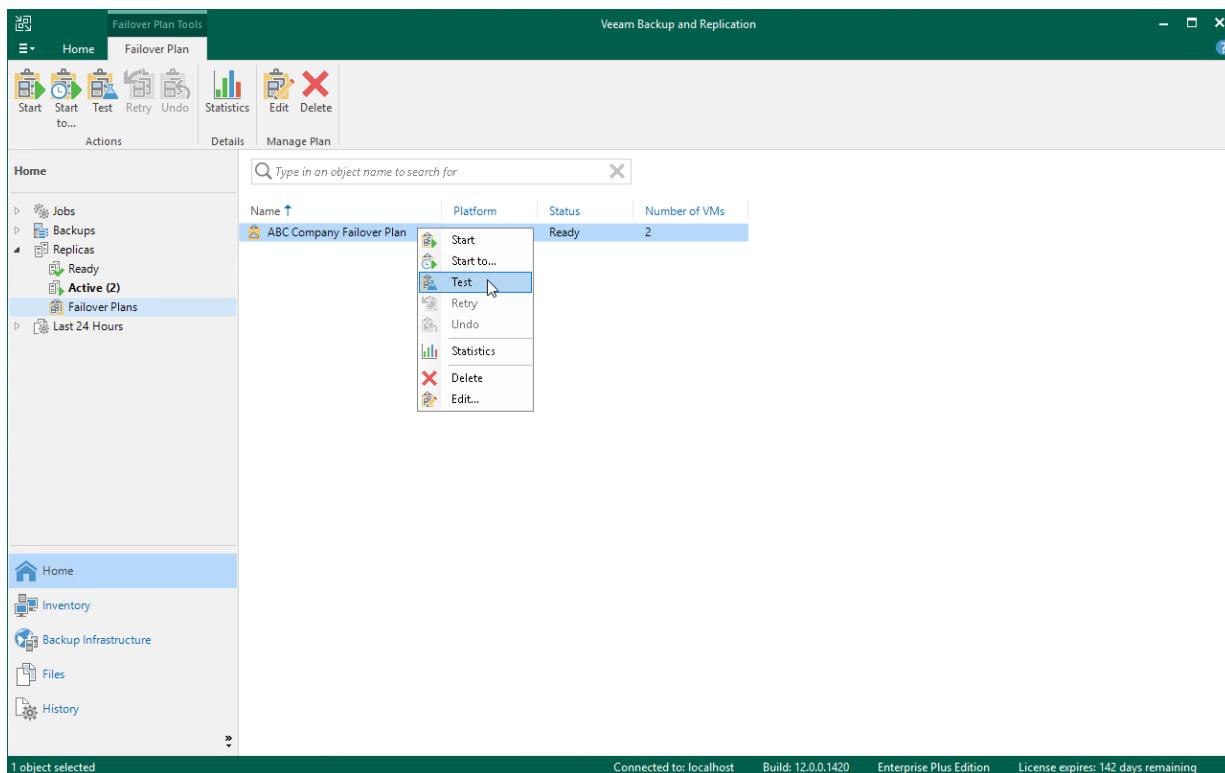
When the test operation is started by the tenant, Veeam Backup & Replication running on the tenant backup server does not communicate with VM replicas on the cloud host directly. Instead, Veeam Backup & Replication passes the command to start the test to the SP backup server, and performs operations with tenant VM replicas from the SP backup server.

> **IMPORTANT**
>
> You can perform the test operation only for cloud failover plans that contain snapshot-based replicas. This operation is not supported for failover plans that contain CDP replicas.

To test a cloud failover plan:

1. Open the **Home** view.

2. In the inventory pane, expand the **Replicas** node and click **Failover Plans**.

3. In the working area, right-click the necessary cloud failover plan and select **Test**.

Retrying Cloud Failover Plan

You can retry a cloud failover plan if one or several VMs fail to failover properly. Veeam Backup & Replication retries the failover operation only for those VMs that do not succeed to failover to their replicas on the cloud host.

To retry a cloud failover plan:

1. Open the **Home** view.

2. In the inventory pane, expand the **Replicas** node and click **Failover Plans**.

3. In the working area, right-click the necessary cloud failover plan and select **Retry**.

Undoing Failover by Cloud Failover Plan

You can undo failover for all VMs added to the cloud failover plan at once. When you undo failover, you switch the workload back to original VMs and discard all changes that were made to VM replicas during failover.

To undo failover by a cloud failover plan:

1. Open the **Home** view.

2. In the inventory pane, expand the **Replicas** node and click **Failover Plans**.

3. In the working area, right-click the necessary cloud failover plan and select **Undo**.

4. In the displayed window, click **Yes** to confirm the operation.

Performing Permanent Failover

To finalize the full site failover process, you can perform permanent failover. With permanent failover, you can permanently switch from the original VM to a VM replica and use the VM replica on the cloud host as the original VM.

To perform permanent failover, do either of the following:

- Open the **Home** view, in the inventory pane select **Replicas**. In the working area, select the necessary VM and click **Permanent Failover** on the ribbon.

- Open the **Home** view, in the inventory pane select **Replicas**. In the working area, right-click the necessary VM and select **Permanent failover**.

In the displayed window, click **Yes** to confirm the operation.

After the permanent failover operation completes, the VM replica is put to the *Permanent failover* state. To protect the VM replica from corruption after performing permanent failover, Veeam Backup & Replication reconfigures the replication job and adds the original VM to the list of exclusions. When the replication job that processes the original VM starts, the VM will be skipped from processing, and no data will be written to the working VM replica.

Editing Cloud Failover Plan Settings

You can edit settings of cloud failover plans that you configured.

To edit cloud failover plan settings:

1. Launch the **Edit Cloud Failover Plan** wizard:

   a. Open the **Home** view and click **Replicas** > **Failover Plans** in the inventory pane.

   b. In the working area, click the necessary cloud failover plan and click **Edit** on the ribbon or right-click the necessary cloud failover plan and select **Edit**.

2. Edit cloud failover plan settings as required.
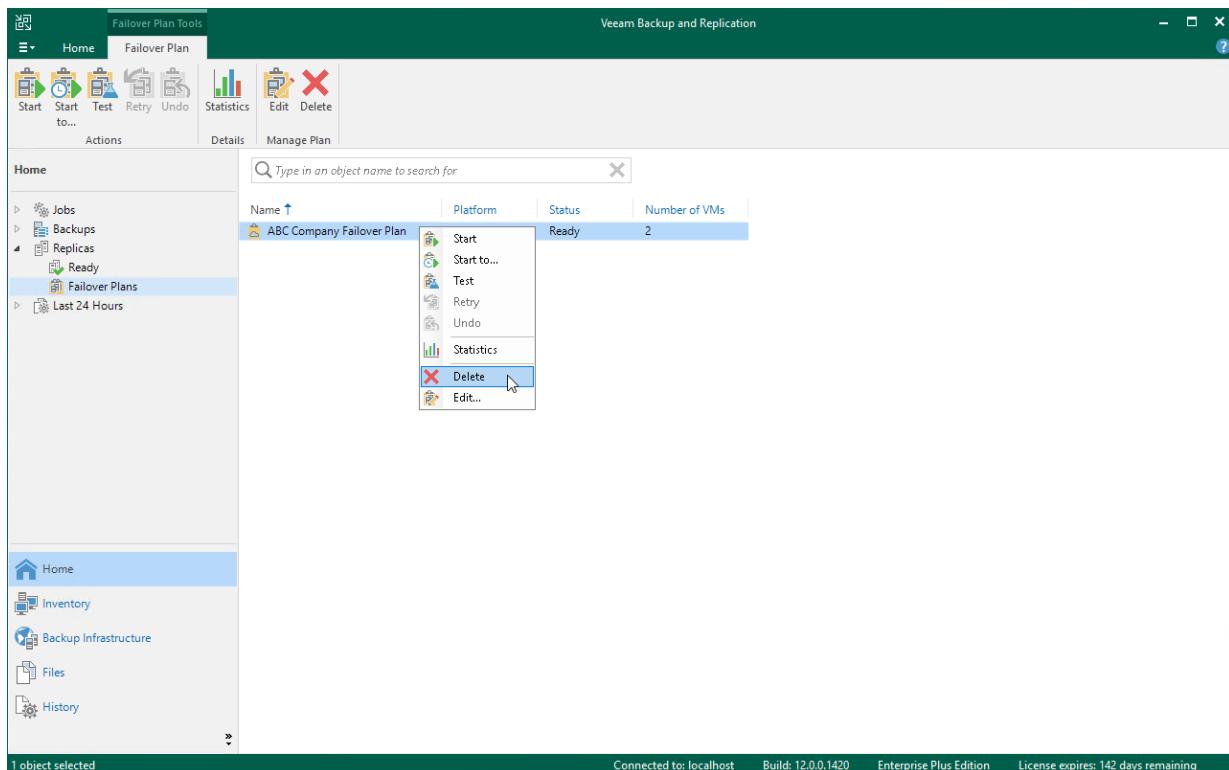
Deleting Cloud Failover Plan

You can delete a cloud failover plan, for example, if you do not plan to use it any longer.

To delete a cloud failover plan:

1. Open the **Home** view.

2. In the inventory pane, expand the **Replicas** node and click **Failover Plans**.

3. In the working area, right-click the necessary cloud failover plan and select **Delete**.

4. In the displayed window, click **Yes** to confirm the operation.

Performing Partial Site Failover

You can quickly recover one or several corrupted VMs by failing over to their replicas on the cloud host.

For regular, snapshot-based replicas on the cloud host, the partial site failover operation is similar to the regular failover for the off-site replication scenario. To learn more, see the following sections of the Veeam Backup & Replication documentation:

- Failover section in the Veeam Backup & Replication User Guide for VMware vSphere

- Failover section in the Veeam Backup & Replication User Guide for Microsoft Hyper-V

For CDP replicas on the cloud host, the partial site failover operation is similar to failover for regular CDP replicas. To learn more, see the Failover section in the Veeam Backup & Replication User Guide:

Performing Failover

If one or several production VMs become corrupted, but the rest of production site, including the most critical VMs and Veeam Backup & Replication infrastructure, remain operative, you can perform partial site failover. With partial site failover, you can quickly recover a corrupted VM by failing over to its replica on the cloud host.

> **IMPORTANT**
>
> You can perform partial site failover only for those VMs that have a static IP address. If a VM receives an IP address from DHCP, the failover operation will succeed but the VM replica will not be accessible over the network.

To perform partial-site failover, do the following:

1. Launch the failover wizard in one of the following ways:

    o Open the **Home** view and select the **Replicas** node. In the working area, select the necessary VM and click **Failover Now** on the ribbon.

    o Open the **Home** view and select the **Replicas** node. In the working area, right-click the necessary VM and select **Failover now**.

    o Open the **Home** view and select **Ready** under the **Replicas** node. In the working area, select the necessary replica and click **Failover Now** on the ribbon or right-click the replica and select **Failover now**.

    > **NOTE**
    >
    > If you have not deployed the network extension appliance for the network to which the corrupted VM is connected, Veeam Backup & Replication will display a warning. You can proceed to the **Network Extension** step of the **Service Provider** wizard to configure and deploy the missing network extension appliance. To learn more, see Configure Network Extension Appliances.
   >
    > After the network extension appliance is deployed, you can launch the **Failover** wizard to start the partial site failover operation.

2. At the **Virtual Machines** step of the wizard, select one or more VMs for which you want to perform failover.

3. By default, Veeam Backup & Replication uses the latest valid restore point of the VM replica. If you want to fail over to an earlier state of the VM, select the VM in the **Virtual machines to failover** list and click **Point**.

4. In the **Restore Points** window, expand the replication job that contains the VM you plan to fail over, select the necessary restore point, and click **OK**.

5. At the **Reason** step of the wizard, specify the reason for failing over to the VM replicas for future reference.

6. At the **Summary** step of the wizard, review details of the failover task and click **Finish** to exit the wizard. When the failover process is complete, the VM replicas will be started on the cloud host.

Performing Failover for CDP Replicas

If one or several production VMs become corrupted, but the rest of production site, including the most critical VMs and Veeam Backup & Replication infrastructure, remain operative, you can perform partial site failover. With partial site failover, you can quickly recover a corrupted VM by failing over to its CDP replica on the cloud host.

> **IMPORTANT**
>
> You can perform partial site failover only for those VMs that have a static IP address. If a VM receives an IP address from DHCP, the failover operation will succeed but the VM replica will not be accessible over the network.

To perform partial-site failover to a CDP replica, do the following:

1. Launch the failover wizard in one of the following ways:

   o Open the **Home** view and select the **Replicas** node. In the working area, select the necessary VM and click **Failover Now** on the ribbon.

   o Open the **Home** view and select the **Replicas** node. In the working area, right-click the necessary VM and select **Failover now**.

   o Open the **Home** view and select **Ready** under the **Replicas** node. In the working area, select the necessary replica and click **Failover Now** on the ribbon or right-click the replica and select **Failover now**.

   > **NOTE**
   >
   > If you have not deployed the network extension appliance for the network to which the corrupted VM is connected, Veeam Backup & Replication will display a warning. You can proceed to the **Network Extension** step of the **Service Provider** wizard to configure and deploy the missing network extension appliance. To learn more, see Configure Network Extension Appliances.
   >
   > After the network extension appliance is deployed, you can launch the **Failover** wizard to start the partial site failover operation.

2. At the **Virtual Machines** step of the wizard, select one or more VMs for which you want to perform failover.

3. By default, Veeam Backup & Replication uses the latest valid restore point of the VM replica. If you want to fail over to an earlier state of the VM, select the VM in the **Virtual machines to failover** list and click **Point**.

4. In the **Restore Points** window, select whether you want to fail over to the latest available crash-consistent restore point, to the latest long-term application-consistent restore point or to a specific point in time.

   If you fail over to a specific point in time, use the right and left arrows on the keyboard to select the required restore point.

   To quickly find a long-term restore point, in the **Restore point** field click a link that shows a date. In the displayed window, use the calendar to select the necessary day, and then select a long-term restore point created during the selected day.

5. At the **Reason** step of the wizard, specify the reason for failing over to the VM replicas for future reference.
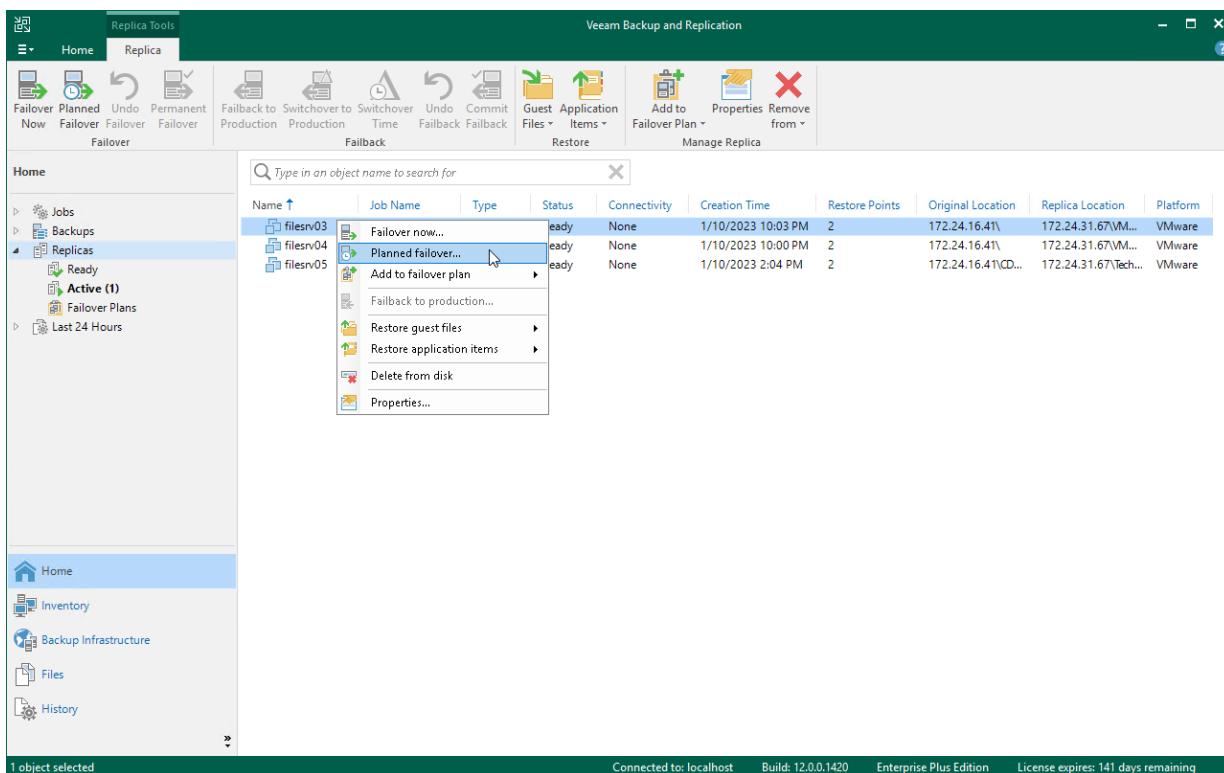
6. At the **Summary** step of the wizard, review details of the failover task and click **Finish** to exit the wizard. When the failover process is complete, the VM replicas will be started on the cloud host.

Performing Planned Failover

Within the partial site failover scenario, you can perform planned failover for snapshot-based replicas on the cloud host. This operation is helpful if you know that your production VMs are about to go offline and you need to proactively switch the workload from source VMs to their replicas on the cloud host. During planned failover, Veeam Backup & Replication triggers the replication job to fully synchronize the replica with the source VM, shuts down the source VM and fails over the VM to its replica. To learn more, see the Planned Failover section in the Veeam Backup & Replication User Guide.

To launch the **Planed Failover** wizard, do one of the following:

- Open the **Home** view and select the **Replicas** node. In the working area, select the necessary VM and click **Planned Failover** on the ribbon.

- Open the **Home** view and select the **Replicas** node. In the working area, right-click the necessary VM and select **Planned failover**.

- Open the **Home** view and select **Ready** under the **Replicas** node. In the working area, select the necessary replica and click **Planned Failover** on the ribbon or right-click the replica and select **Planned failover**.

Re-establishing VPN Tunnel
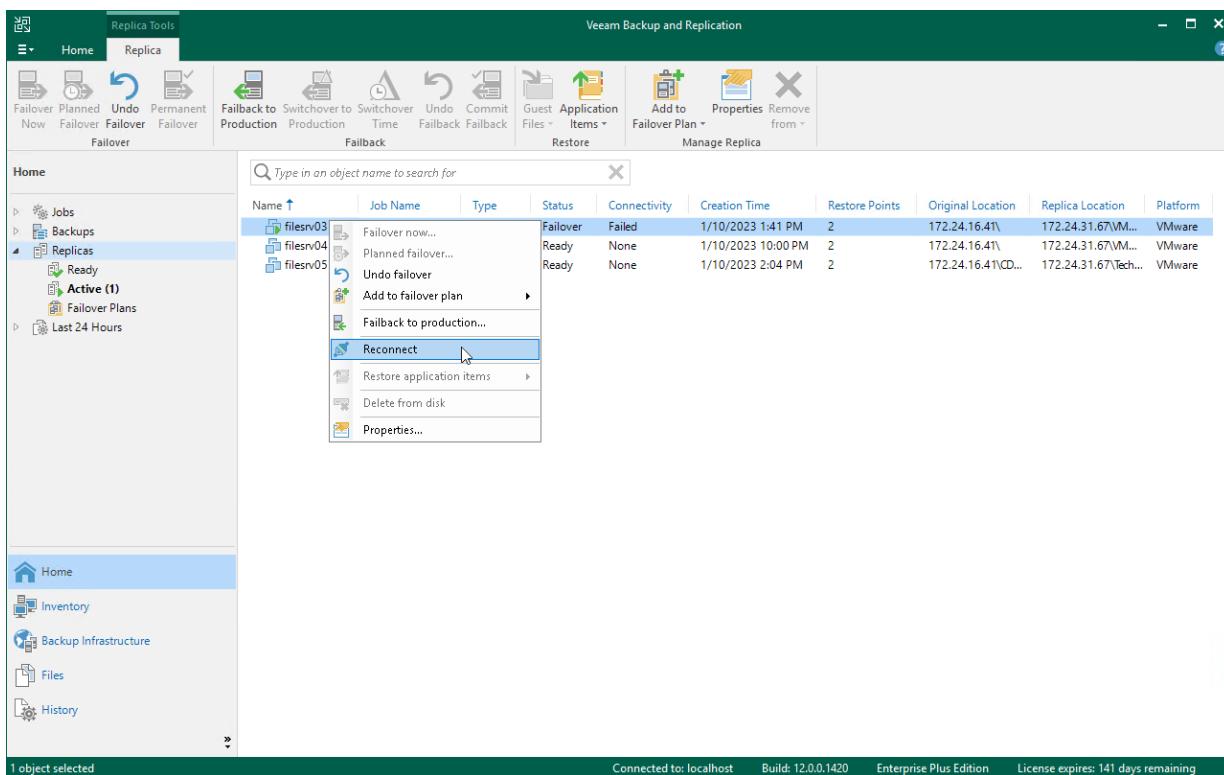
When you perform partial site failover, production VMs and VM replicas on the cloud host communicate through the secure VPN tunnel that is set between the pair of network extension appliances. You can monitor the VPN connection state and re-establish the VPN tunnel in case the VPN connection breaks.

To view the VPN connection state:

1. Open the **Home** view.

2. In the inventory pane, click the **Replicas** node. VPN connection state will be displayed in the **Connectivity** column of the working area.

To re-establish a VPN tunnel:

1. Open the **Home** view.

2. In the inventory pane, click the **Replicas** node.

3. In the working area, right-click the necessary VM replica in the *Failed* connectivity state and select **Reconnect**. Veeam Backup & Replication will restart the VPN daemon on the network extension appliances that are used for connecting production VMs and VM replicas on the cloud host.
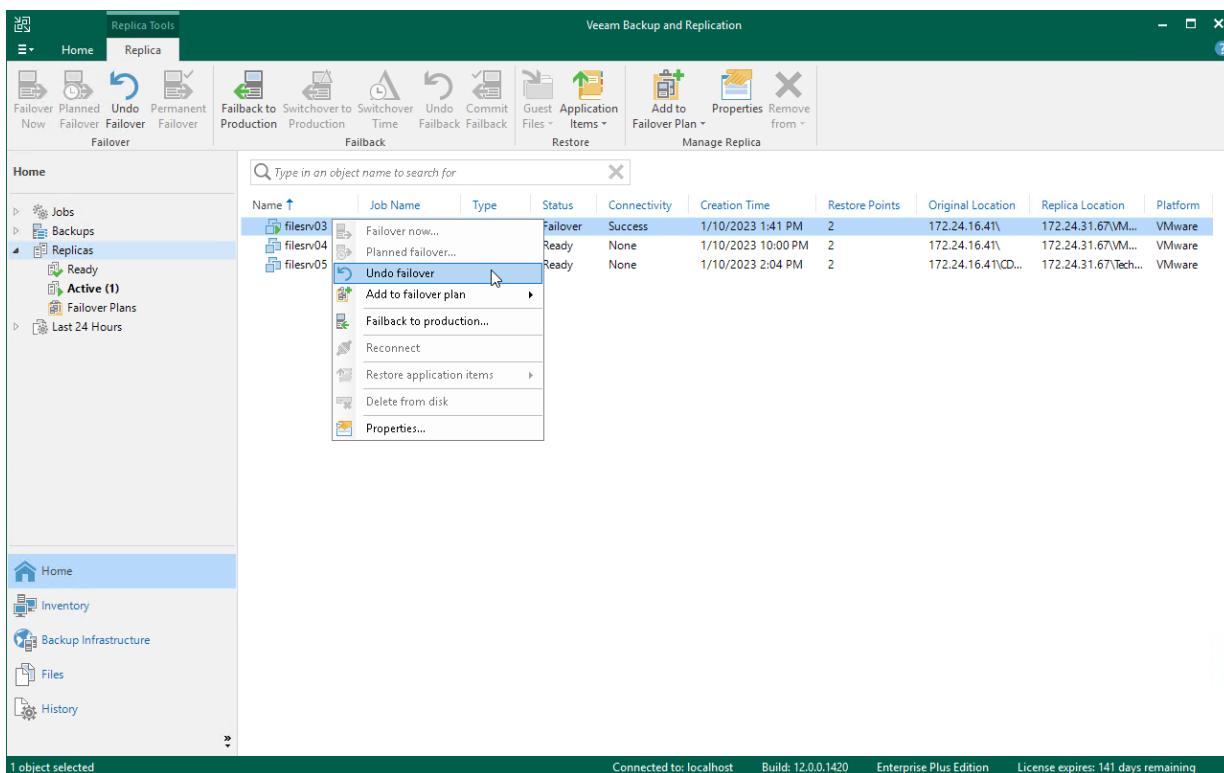
Undoing Partial Site Failover

To switch back to a production VM and revert a VM replica on the cloud host to its pre-failover state, you can undo partial site failover. When you undo the failover operation, Veeam Backup & Replication powers off a running VM replica on the cloud host and rolls back to initial state of a VM replica.

To undo partial site failover, do either of the following:

- Open the **Home** view and select the **Replicas** node. In the working area, select the necessary VM and click **Undo Failover** on the ribbon.

- Open the **Home** view and select the **Replicas** node. In the working area, right-click the necessary VM and select **Undo failover**.

- Open the **Home** view and select **Active** under the **Replicas** node. In the working area, select the necessary replica and click **Undo Failover** on the ribbon or right-click the replica and select **Undo failover**.

In the displayed dialog box, click **Yes** to confirm the operation.
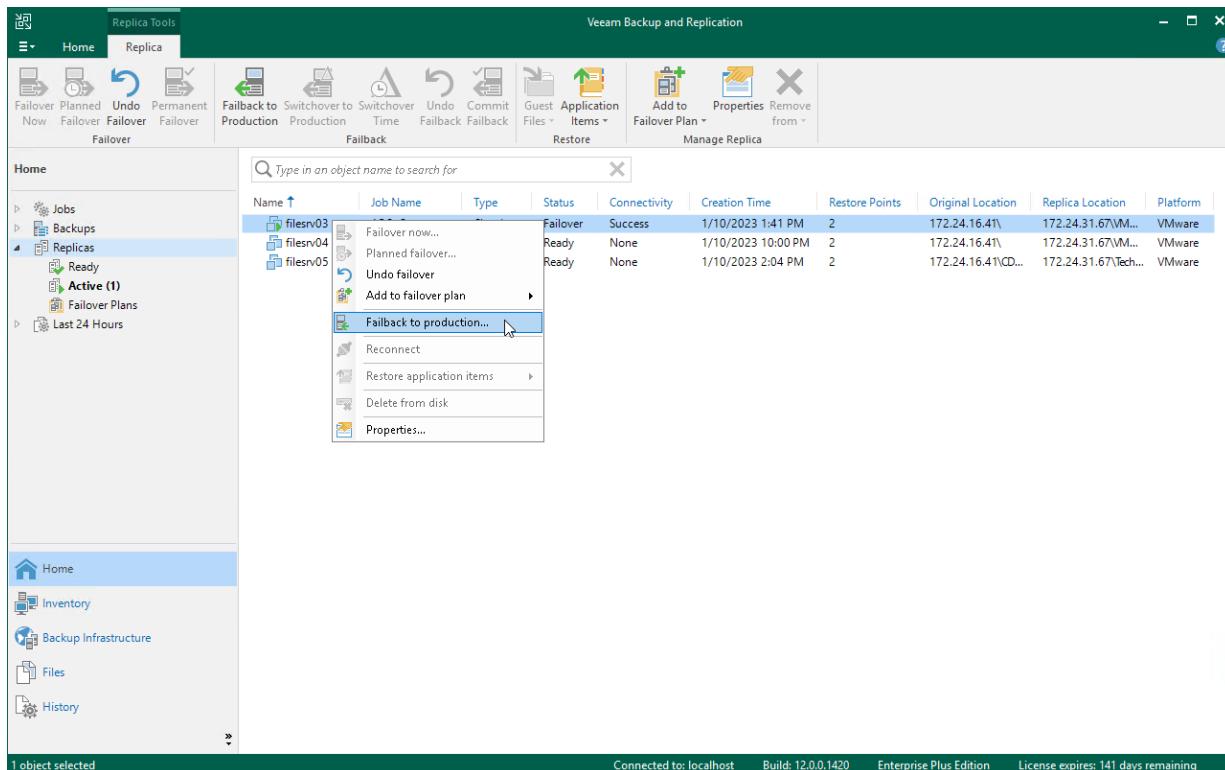
Performing Failback

You can resume operation of a production VM by failing back to it from a VM replica on the cloud host. Performing failback for VM replicas on the cloud host is similar to performing failback for regular VM replicas. To learn more, see the Performing Failback section in the Veeam Backup & Replication User Guide.

To launch the **Failback** wizard, do one of the following:

- Open the **Home** view and select the **Replicas** node. In the working area, select the necessary VM and click **Failback to Production** on the ribbon.

- Open the **Home** view and select the **Replicas** node. In the working area, right-click the necessary VM and select **Failback to production**.

Committing Failback

The **Commit failback** operation finalizes failback from the VM replica to the original VM.

To commit failback, do one of the following:

- Open the **Home** view, in the inventory pane select **Replicas**. In the working area, select the necessary replica and click **Commit Failback** on the ribbon.

- Open the **Home** view, in the inventory pane select **Replicas**. In the working area, right-click the necessary replica and select **Commit failback**.

- On the **Home** tab, click **Restore**. In the **Restore from replica** section, select **Commit failback**.

In the displayed window, click **Yes** to confirm the operation.

Restoring VM Guest OS Files

You can restore individual Microsoft Windows guest OS files from snapshot-based replicas of Microsoft Windows VMs on the cloud host.
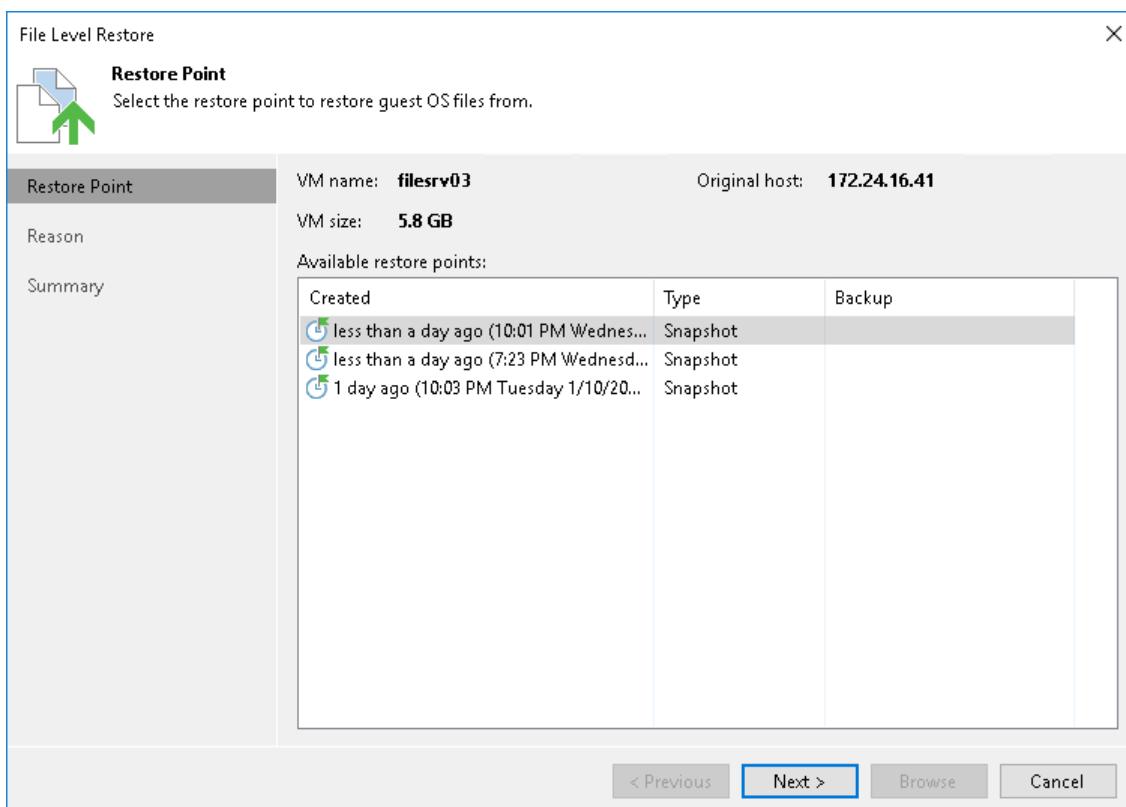
During file-level recovery, Veeam Backup & Replication publishes VM replica virtual disk files directly into the Veeam backup server file system with the help of Veeam's proprietary driver. After VM disks are mounted, you can use the Veeam Backup Browser or Microsoft Windows Explorer to copy necessary files and folders to the local machine drive, save them in a network shared folder or point any applications to restored files and work with them as usual.

> **NOTE**
>
> This section describes only basic steps that you must take to restore VM guest OS files. To get a detailed description of all settings of the restore process, see the Guest OS File Recovery section in the Veeam Backup & Replication User Guide.

To restore VM guest OS files of a Microsoft Windows VM replica:

1. Open the **Home** view.

2. Click the **Replicas** node in the inventory pane. Right-click the necessary VM replica and select **Restore guest files** > **Microsoft Windows**.

3. At the **Restore Point** step of the wizard, select the necessary restore point.
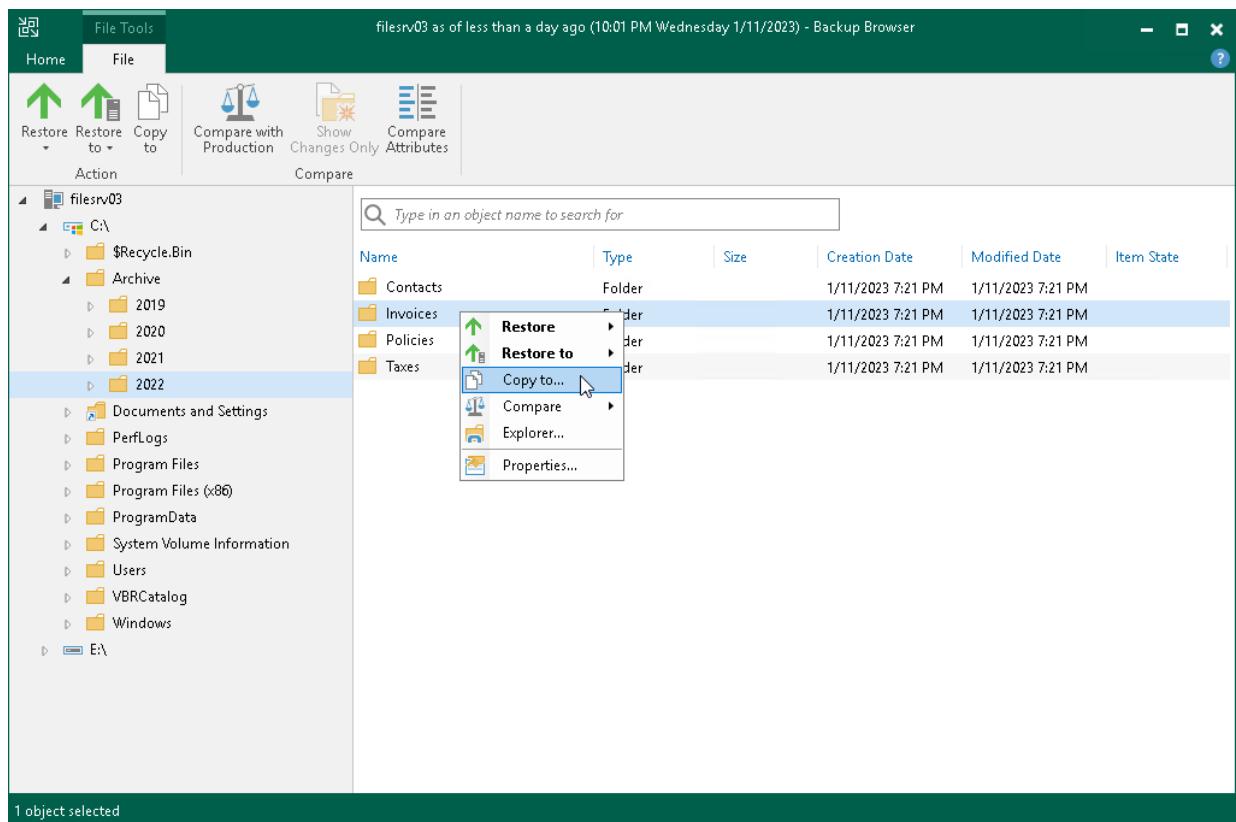
4. At the **Reason** step of the wizard, specify the reason for future reference.

5. Click **Next**. Then click **Browse**.

6. Veeam Backup & Replication will display a file browser with the file system tree of the VM. Right-click the necessary file or folder and select the necessary option.

   o To restore a file or folder to its original location on the original VM:

      ▪ Select **Restore > Overwrite** if you want to overwrite the original file or folder on the VM guest OS with the file or folder restored from the replica.

      ▪ Select **Restore > Keep** if you want to save a file or folder restored from the replica next to the original file or folder. Veeam Backup & Replication will add the _RESTORED_YYYYMMDD_HHMMSS_ postfix to the original file or folder name and save the restored file or folder in the same location where the original file or folder resides.

   o To restore a file or folder to another VM in the Veeam backup infrastructure:

      ▪ Select **Restore to > Overwrite** if you want to overwrite the file or folder on the VM guest OS with the file or folder restored from the replica in case the file or folder with the same name resides on the target VM.

      ▪ Select **Restore to > Keep** if you want to save a file or folder restored from the replica next to the file or folder on the VM guest OS in case the file or folder with the same name resides on the target VM. Veeam Backup & Replication will add the _RESTORED_YYYYMMDD_HHMMSS_ postfix to the original file or folder name and save the restored file or folder in the specified location.

   If you select one of this options, select the target VM and target path for the restored file or folder, and click **OK**.

o To restore to the original location only those files or folders that have changed on the original VM since the restore point for the replica was created, select **Compare** > **Compare**. Then right-click the file or folder and select one of the following options:

- Select **Restore changed only** > **Overwrite** if you want to overwrite the original file or folder on the VM guest OS with the file or folder restored from the replica.

- Select **Restore changed only** > **Keep** if you want to save a file or folder restored from the replica next to the original file or folder. Veeam Backup & Replication will add the *_RESTORED_YYYYMMDD_HHMMSS* postfix to the original file or folder name and save the restored file or folder in the same location where the original file or folder resides.

o To save a file or folder on the local machine or in a network shared folder, select **Copy to**, specify a path to the destination location and click **OK**.

To learn more, see the Finalize Restore section in the Veeam Backup & Replication User Guide.

Restoring Application Items

You can use Veeam Explorers to restore application items from snapshot-based replicas on the cloud host.

Veeam Backup & Replication lets you restore items of the following applications:

- Microsoft Active Directory
- Microsoft Exchange
- Microsoft SharePoint
- Microsoft SQL Server
- Microsoft OneDrive for Business
- Microsoft Teams
- Oracle
- PostgreSQL

For replicas on the cloud host created by replication jobs with guest processing options enabled, the procedure of application-item restore does not differ from the regular one. To perform application-item restore, do either of the following:

- Open the **Home** view, in the inventory pane select **Replicas**. In the working area, select the necessary VM and click **Application Items** > *<Application>* on the ribbon.

- Open the **Home** view, in the inventory pane select **Replicas**. In the working area, right-click the necessary VM and select **Restore application items** > *<Application>.*

Then follow instructions in the procedure for the required application. For details, see the Application Item Restore section in the Veeam Backup & Replication User Guide.

The list of available data recovery operations differs depending on what Veeam Explorer you use. To learn more, see the Veeam Explorers User Guide.

Viewing Replicas and Failover Plans

After replication job targeted at the cloud host or a cloud failover operation completes, it takes some time for Veeam Backup & Replication to retrieve changes from the database and display those changes in the Veeam Backup & Replication console on the tenant side. For example, when you perform a failover operation, VM replicas and cloud failover plans may be not displayed or displayed with a wrong status.

To refresh the view in the Veeam Backup & Replication console:

1. Open the **Home** view.

2. Expand the **Replicas** node and press **[F5]** to refresh the view.

Managing Replicas

The tenant can perform the following operations with VM replicas created with replication jobs and CDP policies targeted at the cloud host:

- View properties
- Delete from disk

> **NOTE**
>
> The tenant cannot perform the *Remove from configuration* operation with VM replicas on the cloud host. Such VM replicas are actually stored on the remote DR site in the SP virtualization environment. As a result, they would become permanently inaccessible for a tenant. The tenant would also be unable to delete replica files from the cloud host.
>
> The *Remove from configuration* operation is available only for the SP in the SP Veeam Backup & Replication console. To learn more, see Removing from Configuration.
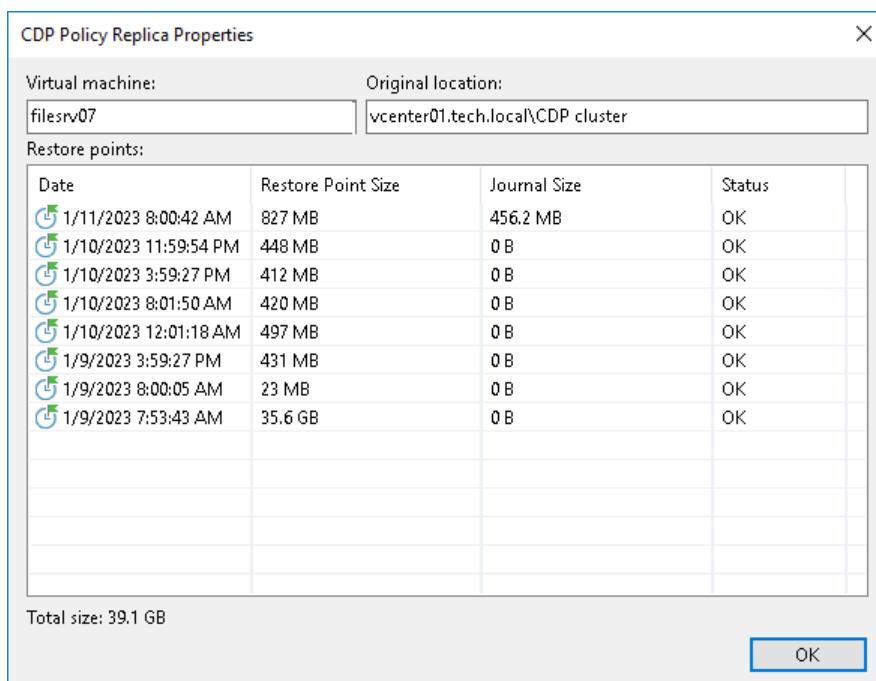
Viewing Properties

You can view summary information about created VM replicas. The summary information provides the following data: available restore points, date of restore points creation, data size, restore point size and replica status. For CDP replicas, Veeam Backup & Replication additionally displays the journal size.

To view summary information for replicas:

1. Open the **Home** view.

2. In the inventory pane, click the **Replicas** node.

3. Right-click the necessary VM replica in the working area and select **Properties**.

Deleting from Disk
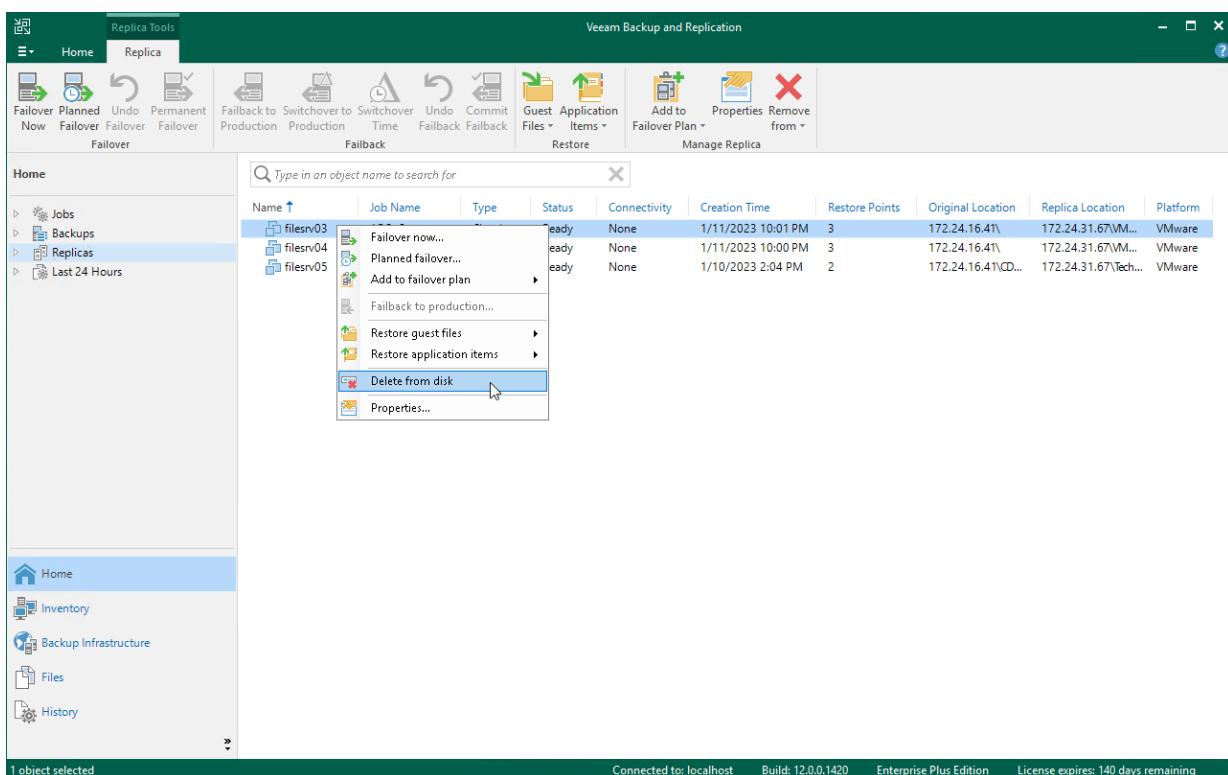
You can use the **Delete from disk** operation if you want to delete records about VM replicas from the Veeam Backup & Replication console and database and, additionally, delete actual replica files from the cloud host.

> **NOTE**
>
> The *Delete from disk* option is the only way for a tenant to delete replica files from the cloud host. The *Remove from configuration* operation is not available in the tenant Veeam Backup & Replication console.

To delete replica files from the cloud host:

1. Open the **Home** view.

2. In the inventory pane, click the **Replicas** node.

3. Right-click the necessary VM replica and select **Delete from disk**.

Using Veeam Cloud Connect Portal

In case of a disaster in the production site when all critical VMs go offline and Veeam backup server becomes inaccessible, you can perform full site failover using Veeam Cloud Connect Portal. Veeam Cloud Connect Portal is a standalone web tool that allows a tenant to run a cloud failover plan remotely from a web browser on a desktop computer or a portable device.

Before You Begin

Consider the following prerequisites and limitations:

- You can access Veeam Cloud Connect Portal with a web browser on a desktop computer or a portable device. To ensure successful usage of Veeam Cloud Connect Portal, use the following supported web browsers:

  - For desktop computers:

    - Microsoft Internet Explorer 11 or later

    - Microsoft Edge

    - Latest versions of Mozilla Firefox and Google Chrome

  - For portable devices (tablets): latest versions of Apple Safari for iOS and Google Chrome for Android

- You cannot use Veeam Cloud Connect Portal to perform full site failover to CDP replicas.

Accessing Veeam Cloud Connect Portal

You can access Veeam Cloud Connect Portal with a web browser using URL address and credentials of the tenant account provided to you by the SP.

To access Veeam Cloud Connect Portal, open your web browser and enter the following address to the address bar:

```
https://hostname:6443
```

where `hostname` is a DNS name or IP address of Veeam Cloud Connect Portal provided to you by the SP.

For example:

```
https://sp01:6443
```

After the Veeam Cloud Connect Portal has loaded, you will be prompted to log in. For that, enter credentials of the tenant account that was provided to you by the SP. To learn more, see Logging In To Veeam Cloud Connect Portal.

Logging In to Veeam Cloud Connect Portal

To perform full site failover by remotely starting a cloud failover plan, you need to log in to Veeam Cloud Connect Portal.

To log in to Veeam Cloud Connect Portal:

1. Access Veeam Cloud Connect Portal.

2. In the **User** field, type the user name of the tenant account provided to you by the SP.

3. In the **Password** field, type the password of the tenant account provided to you by the SP.

4. Select the **Remember me** option to save the specified credentials in the browser cookie. With this option enabled, you will not need to type the username and password every time you access Veeam Cloud Connect Portal.

5. Click **Login**.

Running Cloud Failover Plan

With a cloud failover plan, you can perform full site failover at any time. During the full site failover process the group of critical production VMs fail over to their replicas on the cloud host. You can fail over to the most recent VM state or select the necessary restore point for VMs in the cloud failover plan.

To fail over to the VM replicas latest restore point:

1. Log in to Veeam Cloud Connect Portal. The **Failover Plans** view will automatically open.

2. In the working area, select the necessary cloud failover plan and click **Start**.

   To quickly find the necessary cloud failover plan, you can use the search field at the top-right of the working area.

3. In the displayed dialog box, select the **Start now** option and click **Start**.

4. Monitor the cloud failover process and view results.
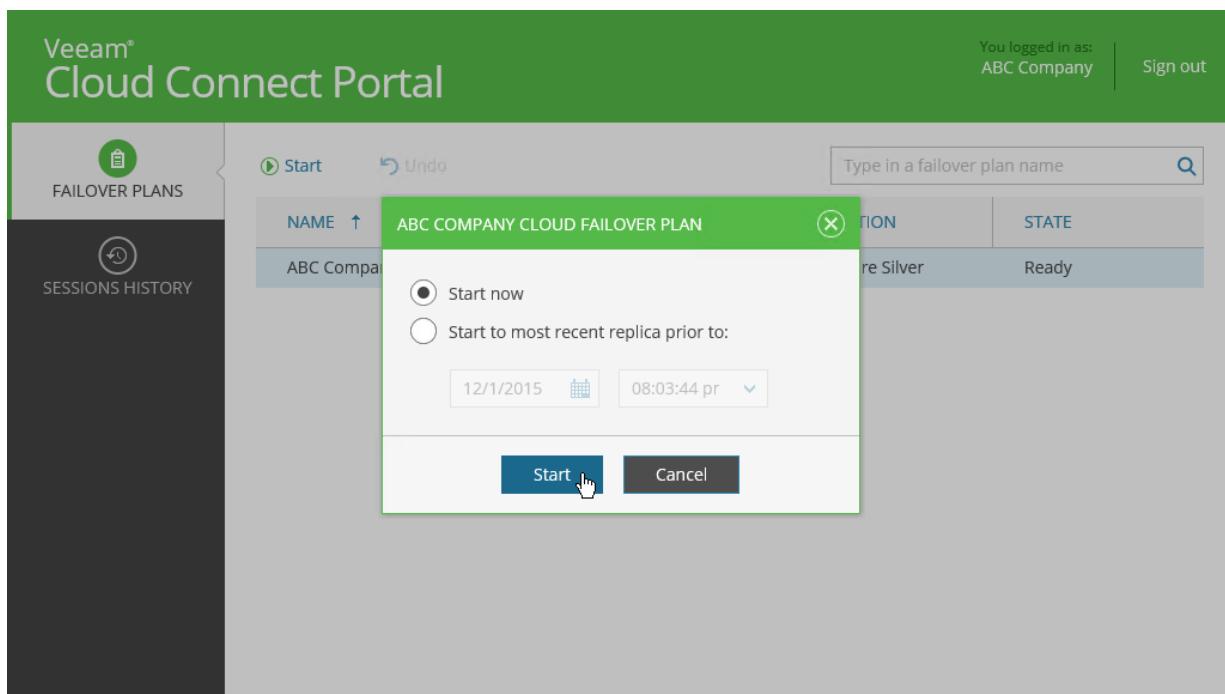
To fail over to a certain restore point:

1. Log in to Veeam Cloud Connect Portal. The **Failover plans** view will automatically open.

2. In the working area, select the necessary cloud failover plan and click **Start**.

   To quickly find the necessary cloud failover plan, you can use the search field at the top-right of the working area.

3. In the displayed dialog box, select the **Start to most recent replica prior to** option, select the replication date and time and click **Start**. Veeam Backup & Replication will find the closest restore point prior to the entered value for each VM and fail over to it.

4. Monitor the cloud failover process and view results.

Retrying Failover by Cloud Failover Plan

You can retry a cloud failover plan if one or several VMs fail to failover properly. Veeam Backup & Replication retries the failover operation only for those VMs that do not succeed to failover to their replicas on the cloud host.

To retry a cloud failover plan:

1. Log in to Veeam Cloud Connect Portal. The **Failover Plans** view will automatically open.

2. In the working area, select the necessary cloud failover plan and click **Retry**.

   To quickly find the necessary cloud failover plan, you can use the search field at the top-right of the working area.

3. Monitor the cloud failover process and view results.

Undoing Failover by Cloud Failover Plan

You can undo failover for all VMs added to the cloud failover plan at once. When you undo failover, you switch the workload back to original VMs and discard all changes that were made to VM replicas during failover.

To undo failover by a cloud failover plan:

1. Log in to Veeam Cloud Connect Portal. The **Failover Plans** view will automatically open.

2. In the working area, select the necessary cloud failover plan and click **Undo**.

   To quickly find the necessary cloud failover plan, you can use the search field at the top-right of the working area.

3. Monitor the undo failover process and view results.

Monitoring Failover Process and Results

With Veeam Cloud Connect Portal, you can monitor the failover plan execution process as well as view results for finished failover tasks. Every run of a cloud failover operation and VM processing initiates a new session. When you start or undo a cloud failover plan, the **Sessions History** section automatically opens. You can also access the **Sessions History** section manually at any time.

The summary information in the **Sessions History** section provides the following data: cloud failover plan and VM replica status, date of failover task start and finish. You can also view detailed information on every VM processing and cloud failover plan session.

To view details on sessions:

1. Log in to Veeam Cloud Connect Portal and open the **Sessions History** view.

2. In the working area, double-click the necessary cloud failover plan and/or VM processing session.

    To quickly find the necessary session, you can sort sessions by name, status, creation or finish date. To sort sessions, click the necessary column heading at the top of the working area.