



Veeam Cloud Connect

Version 13

Administrator Guide

August, 2026

© 2026 Veeam Software.

All rights reserved. All trademarks are the property of their respective owners.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form by any means, without written permission from Veeam Software (Veeam). The information contained in this document represents the current view of Veeam on the issue discussed as of the date of publication and is subject to change without notice. Veeam shall not be liable for technical or editorial errors or omissions contained herein. Veeam makes no warranties, express or implied, in this document. Veeam may have patents, patent applications, trademark, copyright, or other intellectual property rights covering the subject matter of this document. All other trademarks mentioned herein are the property of their respective owners. Except as expressly provided in any written license agreement from Veeam, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

NOTE

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

Contents

CONTACTING VEEAM SOFTWARE	8
ABOUT THIS DOCUMENT	9
ABOUT VEEAM CLOUD CONNECT	10
Veeam Cloud Connect Infrastructure	11
SP Veeam Backup Server	13
Tenant Veeam Backup Server	18
Cloud Gateway	19
Cloud Gateway Pool	21
Cloud Repository	23
Backup Proxies	26
Hardware Plan	27
Network Extension Appliance	29
WAN Accelerators	34
Service Providers and Tenants	36
Tenant Account Types	38
Tenant Account Credentials	39
Custom Roles on Tenant Side	41
Veeam Cloud Connect Backup	42
Getting Started with Veeam Cloud Connect Backup	43
How Veeam Cloud Connect Backup Works	44
Tasks with Cloud Repository	45
Insider Protection	47
Support for Capacity Tier	52
Support for Archive Tier	53
Backup to Object Storage	54
Backup Copy to Cloud Repository	63
Background Retention for Tenant Backups	65
Access to Tenant Backups	66
Instant Recovery from Tenant Backups	68
Veeam Cloud Connect Replication	70
Getting Started with Veeam Cloud Connect Replication	72
How Veeam Cloud Connect Replication Works	73
Tasks with Cloud Host	74
Cloud Replica Failover and Failback	75
Continuous Data Protection (CDP) with Veeam Cloud Connect	83
Veeam Cloud Connect CDP Scenarios	84
CDP Infrastructure in Veeam Cloud Connect	86

Getting Started with CDP	89
Failover and Failback for CDP	91
VMware Cloud Director Support	92
Getting Started with Replication to VMware Cloud Director	93
VMware Cloud Director Tenant Account	96
Network Resources for VMware Cloud Director Replicas	98
Partial Site Failover for VMware Cloud Director Replicas	100
Full Site Failover for VMware Cloud Director Replicas	102
TLS Certificates	104
Types of TLS Certificates	105
TLS Certificates Handshake	106
TLS Certificate Thumbprint Verification.....	108
Rights and Permissions to Access TLS Certificates	109
Tenant Lease and Quota	110
Subtenants.....	112
Subtenant Account	113
Subtenant Quota.....	115
Data Encryption and Throttling	116
Remote Connection to Tenant Backup Server	118
Network Redirectors	119
Remote Access Console.....	120
Remote Desktop Connection to Tenant	124
Tenant Backup to Tape	127
Getting Started with Tenant Backup to Tape	128
Tenant Backup to Tape Job	129
Data Restore from Tenant Backups on Tape.....	130
IPv6 Support	131
PLANNING AND PREPARATION	133
System Requirements	134
Ports.....	137
Veeam Product Versions	147
Considerations and Limitations	148
Veeam Cloud Connect Backup	149
Veeam Cloud Connect Replication.....	152
Naming Conventions.....	154
LICENSING FOR SERVICE PROVIDERS.....	155
Veeam Cloud Connect License	157
Rental Machines Licensing	159
Rental Veeam Backup & Replication License	160
Installing License	163

Updating License	164
Viewing License Information	166
Reducing Number of Used Points	167
Viewing Tenant Machine Count	168
Resetting Tenant Machine Count	169
License Usage Reporting	170
Automatic License Usage Reporting	171
Manual License Usage Reporting	173
Managing License Usage Reports	174
GUIDE FOR SERVICE PROVIDERS	181
Setting Up SP Veeam Cloud Connect Infrastructure	182
Deploying SP Veeam Backup Server	183
Managing TLS Certificates	184
Adding Cloud Gateways	194
Configuring Cloud Gateway Pools	203
Configuring Cloud Repositories	208
Configuring Hardware Plans	210
Managing VLANs	222
Managing Public IP Addresses	226
Managing Network Extension Appliance Credentials	231
Creating Tenant Accounts	233
Configuring Target WAN Accelerators	263
Managing Tenant Accounts	265
Disabling and Enabling Tenant Accounts	266
Renaming Tenant Accounts	268
Changing Password for Tenant Account on SP Side	270
Changing Resource Allocation for Tenant Account	272
Redeploying Network Extension Appliance	275
Viewing Tenant Account Information	276
Deleting Tenant Accounts	278
Managing Subtenant Accounts on SP Side	280
Creating Subtenant Account for Standalone Tenant	281
Creating Subtenant Account for VMware Cloud Director Tenant	286
Editing Subtenant Account	291
Deleting Subtenant Account	293
Restoring Data from Tenant Backups	295
Performing Entire VM Restore from Tenant Backups	296
Performing Instant Recovery from Tenant Backups	315
Restoring Disks from Tenant Backups	317
Publishing Disks from Tenant Backups	318

Managing Tenant Data	319
Moving Tenant Backups to Another Cloud Repository	320
Migrating Tenant Data Between Performance Tier Extents	331
Switching from Linux Repository to Hardened Repository	332
Switching from Linux Hardened Repository to Linux Repository	336
Downloading Tenant Data from Capacity Tier	339
Retrieving Tenant Data from Archive Tier	340
Managing Tenant VM Replicas	341
Scanning Tenant Backups	348
Managing Tenant Cloud Failover Plans	349
Running Cloud Failover Plan	350
Testing Cloud Failover Plan	351
Retrying Cloud Failover Plan.....	353
Undoing Failover by Cloud Failover Plan	354
Editing Cloud Failover Plan Settings.....	355
Performing Permanent Failover	357
Using Remote Access Console	358
Connecting to Tenant with Remote Access Console	359
Launching Remote Desktop Session to Tenant.....	368
Enabling Access to Cloud Gateway	371
Adjusting Remote Desktop Connection Settings	372
Managing SP Backup Server	374
Switching to Maintenance Mode	375
Creating Custom Maintenance Mode Notification.....	377
Working with Tapes	378
Creating Tenant Backup to Tape Job	379
Restoring Tenant Data from Tape	385
Reporting.....	390
Viewing Veeam Cloud Connect Report	391
Viewing Tenant Job Statistics	395
Support for Veeam Backup for Public Clouds	400
GUIDE FOR TENANTS.....	403
Setting Up Tenant Veeam Cloud Connect Infrastructure	404
Deploying Tenant Veeam Backup Server	405
Connecting Source Virtualization Hosts	406
Finding Service Providers	407
Connecting to Service Providers.....	408
Changing Password for Tenant Account	422
Managing Subtenant Accounts on Tenant Side	424
Managing Network Extension Appliance	436

Managing Default Gateways	439
Configuring Source WAN Accelerators	442
Viewing Cloud Hosts	443
Using Cloud Repositories	444
Performing Backup	445
Performing Restore	478
Managing Backups	508
Copying Backups from Cloud Repositories	511
Using Cloud Hosts	512
Creating Replication Jobs	514
Creating CDP Policies for VMware vSphere	530
Creating Universal CDP Policies	544
Performing Full Site Failover	556
Performing Partial Site Failover	576
Performing Failback	586
Restoring VM Guest OS Files	587
Restoring Application Items	590
Viewing Replicas and Failover Plans	592
Managing Replicas	593

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 13 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.

SPs use their own 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 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.
- The SP can deploy multiple backup proxies in the Veeam Cloud Connect infrastructure. For more information, see [Backup Proxies](#).

Veeam Cloud Connect Backup

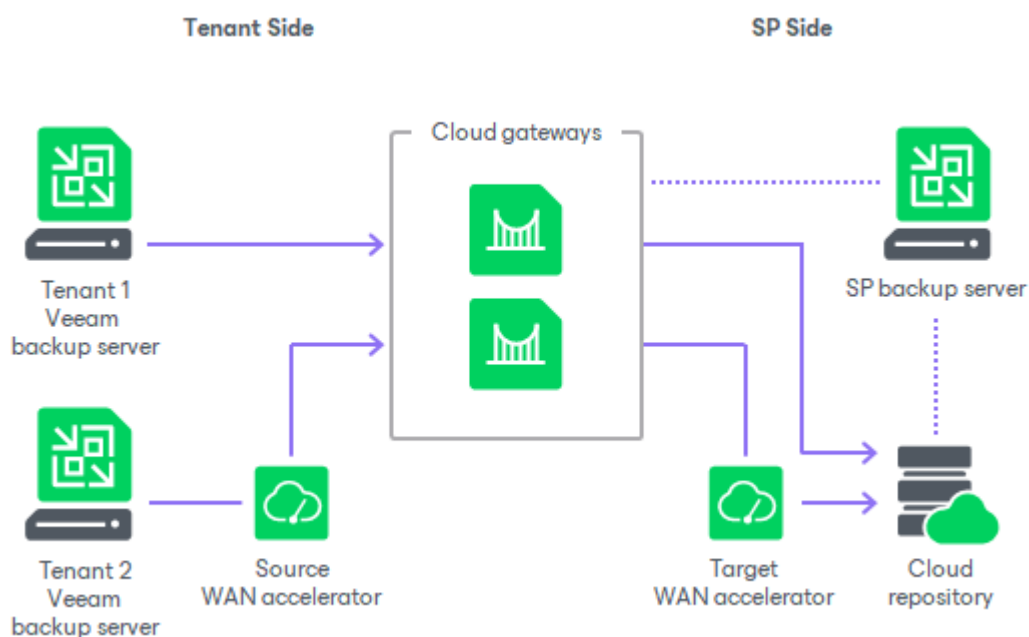
To expose cloud repository resources to tenants, the SP must configure the Veeam Cloud Connect Backup infrastructure. The Veeam Cloud Connect Backup infrastructure comprises the following components:

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

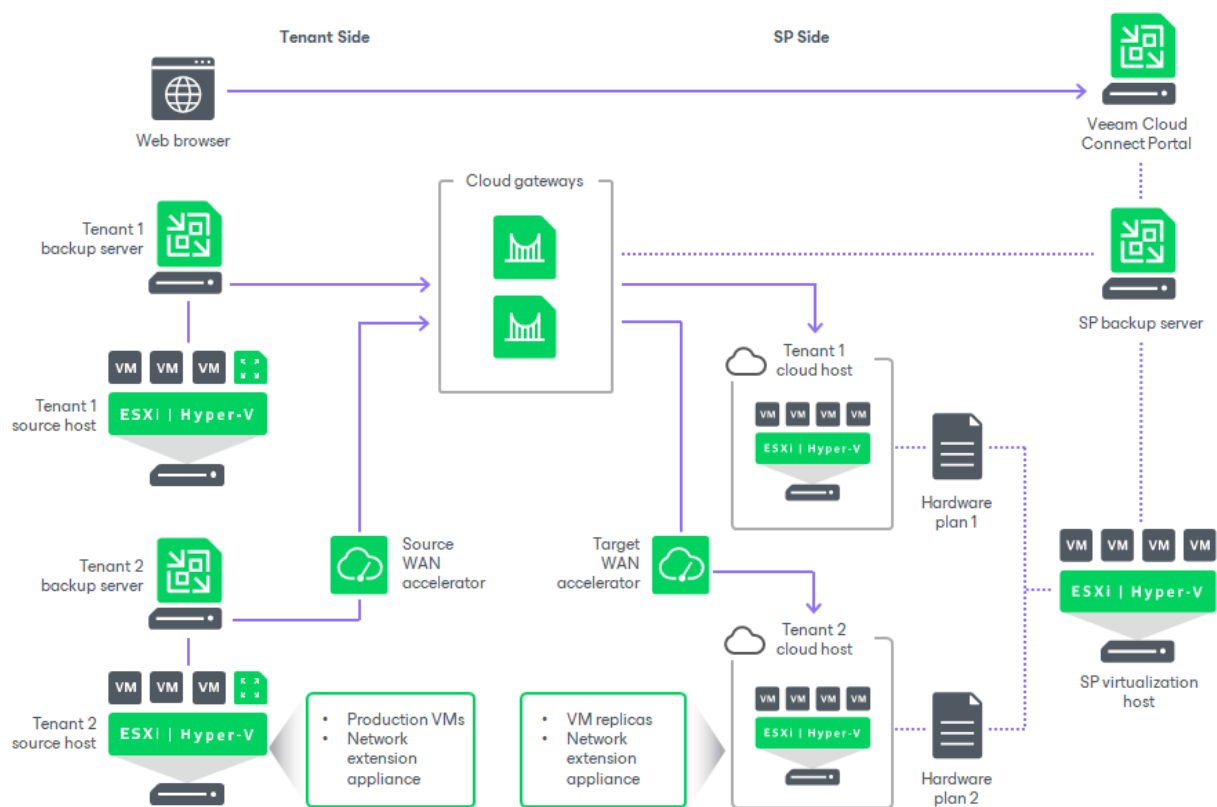
- [SP Veeam backup server](#)
- [One or several cloud gateways](#)
- [One or several hardware plans](#)
- [Optional] [One or several network extension appliances](#)
- [Optional] [One or several target WAN accelerators](#)

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.

NOTE

If the SP uses Veeam Service Provider Console and wants to use multi-factor authentication (MFA) on the SP backup server, they must set up a service account in Veeam Backup & Replication. For details, see [this Veeam KB article](#).

To learn more about MFA support in Veeam Backup & Replication, see the [Multi-Factor Authentication](#) section in the Veeam Backup & Replication User Guide.

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 with tenant backups other than [Instant Recovery](#), [restore to Microsoft Azure](#) and [restore to Amazon EC2](#). Only these three operations are supported with tenant backups on the SP Veeam backup server.

IMPORTANT

The SP must avoid the following operations with the tenant backups, for example, in an attempt to restore data from these backups:

- Import tenant backups on the SP Veeam backup server.
- Decrypt tenant backups on the SP Veeam backup server.

To perform other data restore tasks, the SP must deploy a separate backup server in their backup infrastructure and do either of the following:

- Import tenant backups. In this scenario, the SP must install a separate license key on this backup server. The trial license key works for this scenario.
- Rescan the repository with tenant backups. To learn how to rescan a repository, see the [Rescanning Backup Repositories](#) section in the Veeam Backup & Replication User Guide. In this scenario, the SP can use its existing Veeam Cloud Connect license on the backup server.

IMPORTANT

Do not add the same repository to more than one Veeam Backup & Replication installation. Instead, copy backups to a separate folder and add this folder to a separate Veeam Backup & Replication as a new repository. This approach ensures the safety of the procedure, as it involves working with duplicates of the backups rather than their originals.

If the SP adds the same repository to another Veeam Backup & Replication server and then runs a restore process (or any other procedure related to that backup), the backups may become corrupted.

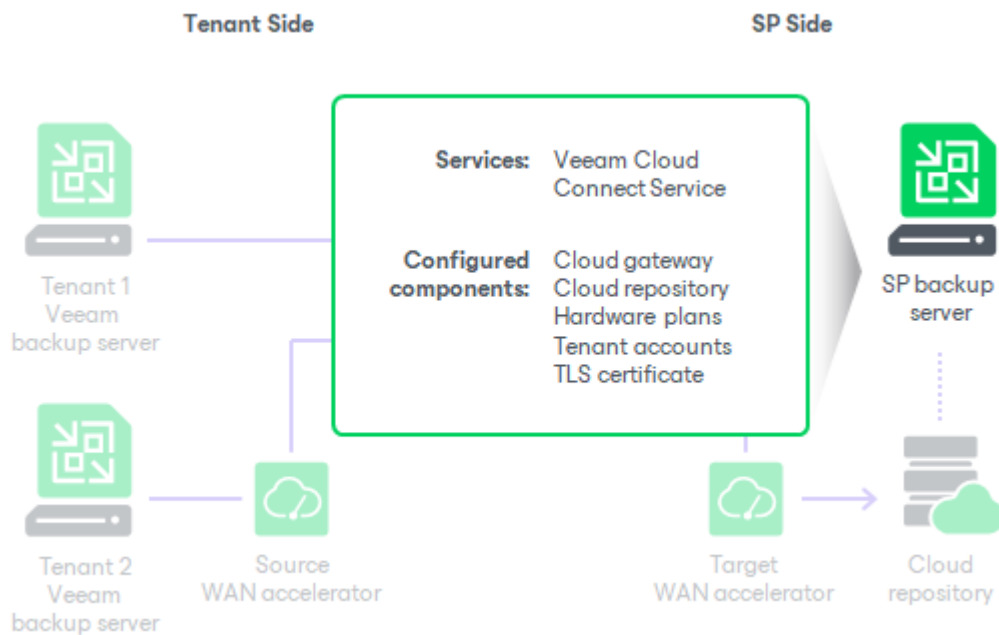
- Add itself as an SP in the Veeam Backup & Replication console, for example, to address specific scenarios that were supported in previous versions of Veeam Backup & Replication. For such scenarios, the SP must deploy a separate backup server in its backup infrastructure. The SP can use their existing 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, or to copy tenant VM backups to a secondary location. 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.

Note that the SP can configure backup copy jobs for backups created by public cloud appliances. To learn more, see [Support for Veeam Backup for Public Clouds](#).

NOTE

The use 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](#).

Note that in this scenario, a configuration where two SPs are added on each other's backup servers is not supported. For example, you have two *Veeam Cloud Connect for the Enterprise* servers: *Server 1* and *Server 2*. If you add *Server 2* as an SP on *Server 1*, you must not add *Server 1* as an SP on *Server 2*.



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 cloud resources of the SP. The following types of jobs are supported:
 - 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, and backup copy jobs for Veeam Agent backups created in the Veeam backup repository
 - VMware vSphere, VMware Cloud Director and Microsoft Hyper-V replication jobs
 - CDP policies

- 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:

- 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.
- 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.
- If there is an active CDP policy at the time when the SP backup server is switched into the Maintenance mode, the CDP policy stops processing of all VMs. The CDP policy itself remains enabled, and Veeam Backup & Replication displays *Syncing* status in the console. This status changes if the CDP policy is manually disabled or deleted.

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.

If a tenant creates a new CDP policy at the time when the SP backup server is in the Maintenance mode, the CDP policy does not start processing of any VMs. The CDP policy itself is enabled, and Veeam Backup & Replication displays *Initial sync* status in the console. This status changes when the Maintenance mode is turned off and the initial synchronization is completed, or when the CDP policy is manually disabled or deleted.

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 [Creating Custom 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:
 - Perform a data restore task with a backup already created in a cloud repository provided by the SP (for example, restore entire VM, VM files, VM disks, or perform file-level restore, and so on).
 - Perform tasks with VM replicas that were in the failover state at the time when the SP backup server was switched to the Maintenance mode (for example, perform failback, commit failback, perform permanent failover, undo failover, 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.

The tenant cannot perform the following tasks targeted at the SP cloud resources at the time when the SP backup server is operating in the Maintenance mode:

- Start new replication jobs targeted at a cloud host provided by the SP.
- Perform file level restore from a CDP replica.
- Perform the Delete from disk operation for snapshot-based replicas and CDP replicas. (This operation is available on the SP side.)
- Perform full site failover and other operations with cloud failover plans (for example, test a cloud failover plan). (This operation is available on the SP side.)
- Perform partial site failover and planned failover.

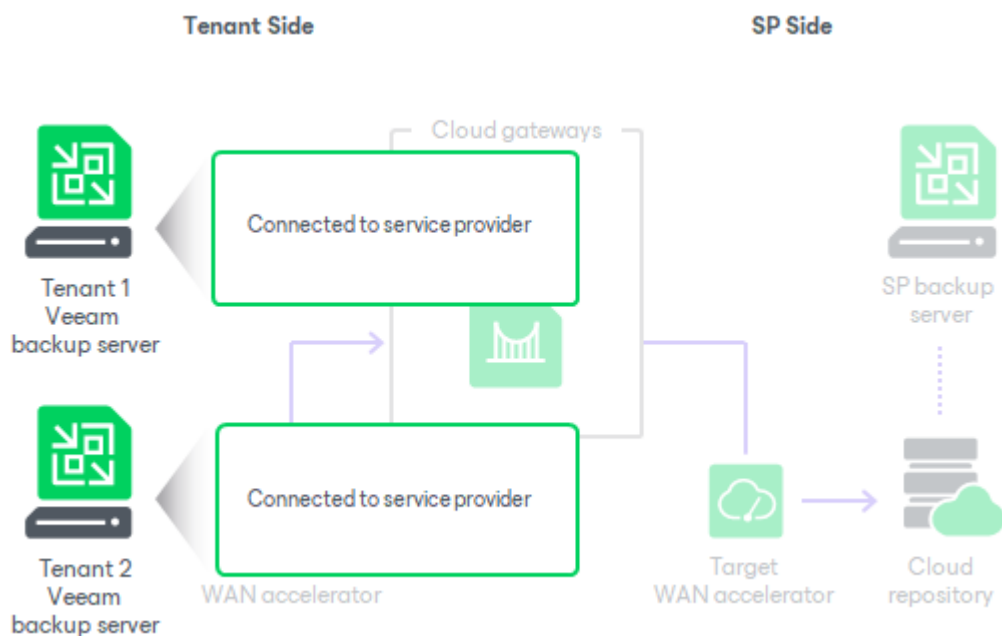
Tenant Veeam Backup Server

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 the tenant 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 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 [Service Providers and Tenants](#).



Cloud Gateway

The Veeam Cloud Connect infrastructure configured at the SP side is hidden from tenants. Tenants know only about cloud repositories and cloud hosts and can work with them as with locally deployed backup repositories and target hosts. Veeam backup servers on the tenant side do not communicate with cloud repositories and cloud hosts directly. Data communication and transfer in the cloud is carried out through cloud gateways.

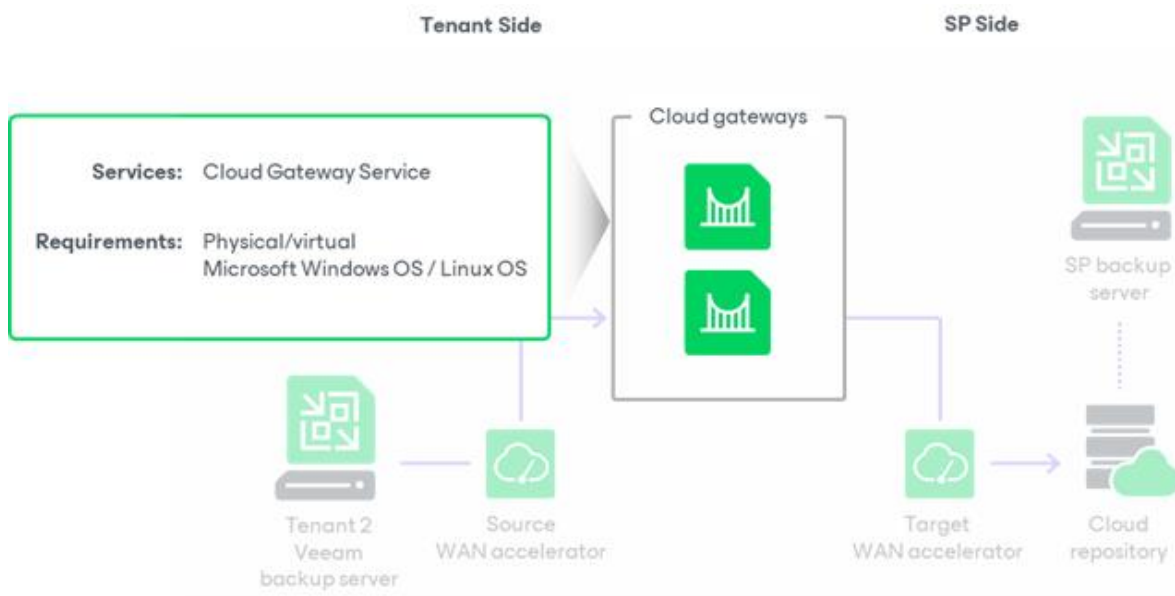
The cloud gateway is a network appliance that resides on the SP side. The cloud gateway acts as a communication point in the cloud: it routes commands and traffic between the tenant Veeam backup server, SP Veeam backup server and other Veeam Cloud Connect infrastructure components.

The cloud gateway is a Microsoft Windows server or a Linux 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:

- The cloud gateway can be a physical or virtual machine.
- The cloud gateway must run Microsoft Windows OS or a Linux 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.

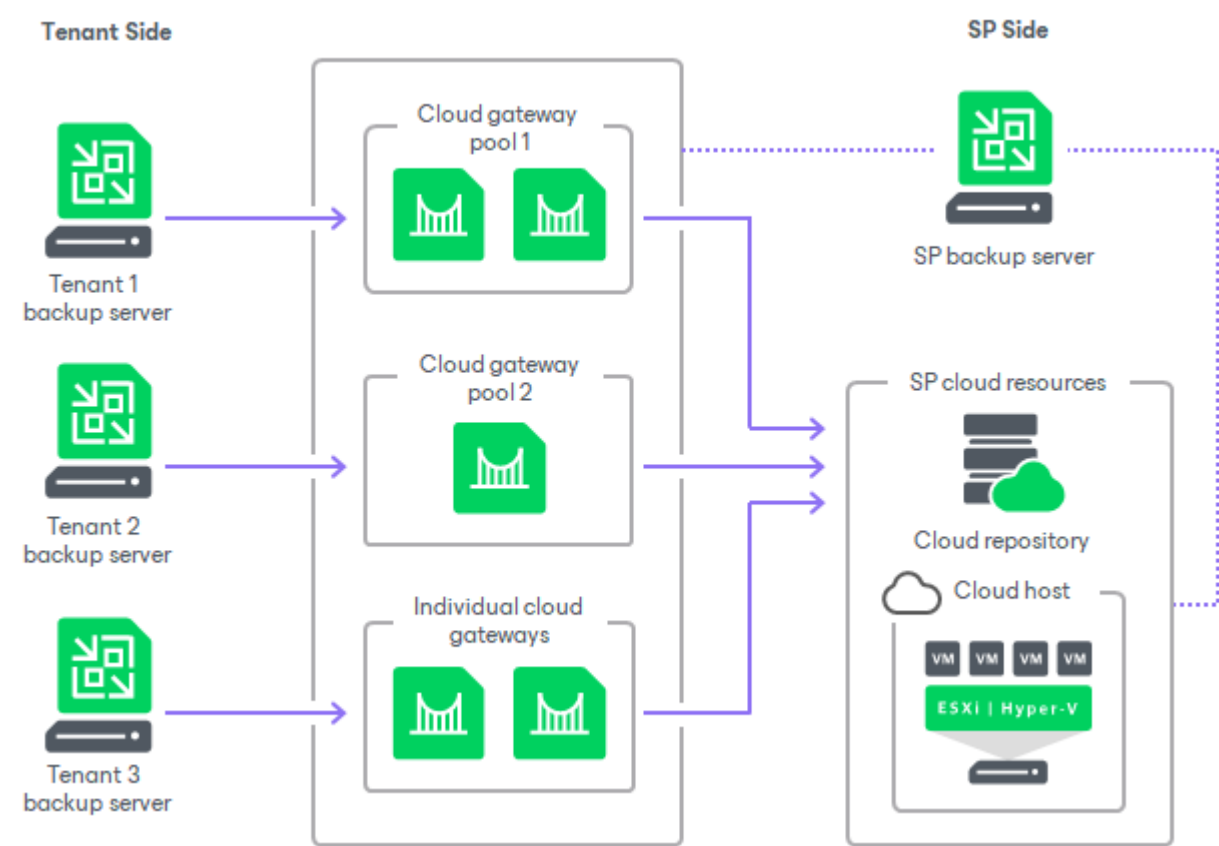
The SP can configure the desired number of cloud gateway pools in the Veeam Cloud Connect infrastructure. Each cloud gateway pool can comprise one or more cloud gateways.

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:

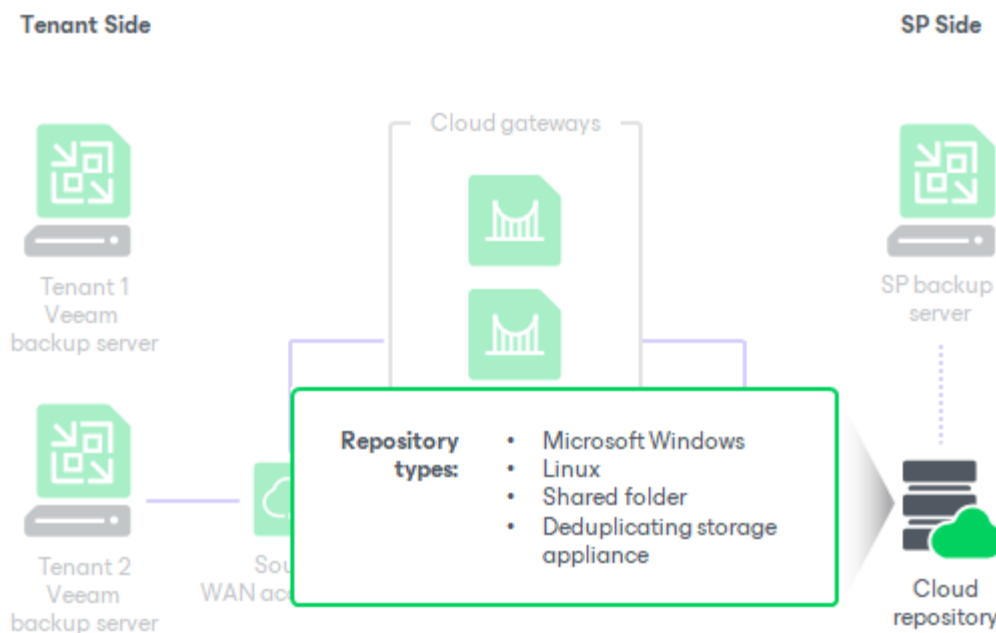
- Microsoft Windows-based server
- Linux-based server, including hardened backup repository
To learn more, see [Support for Hardened \(Immutable\) Backup Repository](#).
- Shared folder
- Deduplicating storage appliance: Dell Data Domain, ExaGrid, Quantum DXi and HPE StoreOnce
- Scale-out backup repository
To learn more, see [Support for Scale-Out Backup Repository](#).
- Object storage, including S3 compatible, Amazon S3, IBM Cloud, Microsoft Azure, Wasabi and Veeam Data Cloud Vault
To learn more, see [Backup to Object Storage](#).

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 Hardened (Immutable) Backup Repository

To protect tenant backup files from loss due to malware activity or unplanned actions, the SP can add a hardened repository based on a Linux server to the backup infrastructure. The hardened repository has an immutability feature that specifies a period of time during which backup files must be immutable. The behavior of the hardened (immutable) backup repository in the Veeam Cloud Connect infrastructure does not differ from the behavior of this component in the regular Veeam backup infrastructure. To learn more, see the [Hardened Repository](#) section in the Veeam Backup & Replication User Guide.

Keep in mind that the immutable time is a per-repository setting and different tenants cannot have different immutable times.

NOTE

The tenant can enable configuration backup in Veeam Backup & Replication and target it at a hardened repository used as a cloud repository. In this case, the configuration backup does not become immutable.

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. A scale-out backup repository is a repository system that supports multi-tier data storage and can comprise following tiers of storage:

- Performance Tier. This functionality allows the SP and the tenant to quickly access the backup data. The SP uses this functionality for tenant backups in a similar way to a simple backup repository. Performance tier extents can be simple backup repositories or object storage repositories. To learn more, see the [Performance Tier](#) section in the Veeam Backup & Replication User Guide.

The SP can migrate tenant data between performance extents within the same scale-out backup repository to balance storage resources. To perform this operation, the SP must use Veeam PowerShell cmdlets. To learn more, see [Migrating Tenant Data Between Performance Tier Extents](#).

- Capacity Tier. The SP uses this functionality to offload tenant backups for long-term storage. Capacity tier is a cloud-based object storage repository. To learn more, see [Support for Capacity Tier](#).
- Archive Tier. The SP uses this functionality to keep backups of rarely accessed tenant data. Archive tier is a cloud-based object storage repository. To learn more, see [Support for Archive Tier](#).

For more information, see the [Scale-Out Backup Repositories](#) section in the Veeam Backup & Replication User Guide.

NOTE

The SP may need to rebalance a scale-out backup repository used as a cloud repository for maintenance purposes. This operation is time consuming and requires careful consideration of its limitations before proceeding. To learn more, see the [Rebalancing Extents of Scale-Out Backup Repositories](#) section in the Veeam Backup & Replication User Guide.

Backup Proxies

A backup proxy is an architecture component that operates as a data mover and transfers data between source and target. Backup proxies in the Veeam Cloud Connect infrastructure run the same services and perform the same roles as backup proxies in the regular backup infrastructure.

In the Veeam Cloud Connect infrastructure, the SP and the tenant can use the following types of backup proxies:

- VMware Backup Proxy is used for backup, recovery and snapshot-based replication of VMware vSphere virtual machines. To learn more, see the [VMware Backup Proxies](#) section in the Veeam Backup & Replication User Guide.
- CDP Proxy is used for continuous data protection of VMware vSphere virtual machines. To learn more about source and target CDP proxies, see [CDP Infrastructure in Veeam Cloud Connect](#).
- Hyper-V Proxy is used for backup, recovery and replication of Hyper-V virtual machines. To learn more about Hyper-V proxies, see the [Backup Infrastructure Components](#) section in the Veeam Backup & Replication User Guide.

By default, the proxy role is assigned to the following components:

- The backup server itself for VMware Backup Proxy.
- The Hyper-V host for Hyper-V Proxy.

For large installations, it is recommended to deploy dedicated VMware proxies and off-host Hyper-V proxies to distribute the backup workload. The SPs and tenants configure backup proxies in the following way:

- The source proxy is configured on the tenant side.
- The target proxy is configured on the SP side.

The number of target backup proxies required in the SP infrastructure varies. At least one proxy must be deployed per hypervisor cluster, so that this proxy can access all available underlying storage and then write the received data to it.

It is recommended to deploy the VMware backup proxy as a virtual machine on the same ESXi host as the VMs to be backed up. In contrast to physical proxies, virtual proxies can use virtual appliance mode (also known as HotAdd mode), which is the most effective transport mode for a target-side proxy, especially in replication scenarios. To learn more, see the [Transport Modes](#) section in the Veeam Backup & Replication User Guide.

Veeam Backup & Replication does not apply the maximum concurrent task limit to backup proxies used in the Veeam Cloud Connect infrastructure. The maximum number of allowed concurrent tasks is defined per tenant in the properties of the tenant account. For optimal performance and to avoid overload, the maximum number of concurrent tasks specified in the tenant settings should not exceed the limits for backup proxies and backup repositories in the SP Veeam Cloud Connect infrastructure.

To ensure that the tenant has sufficient resources, the SP must consider the sizing and capacity of the backup proxies. The recommended ratio of available CPUs on a backup proxy server to the maximum number of concurrent tasks is one-to-one.

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 clusters.

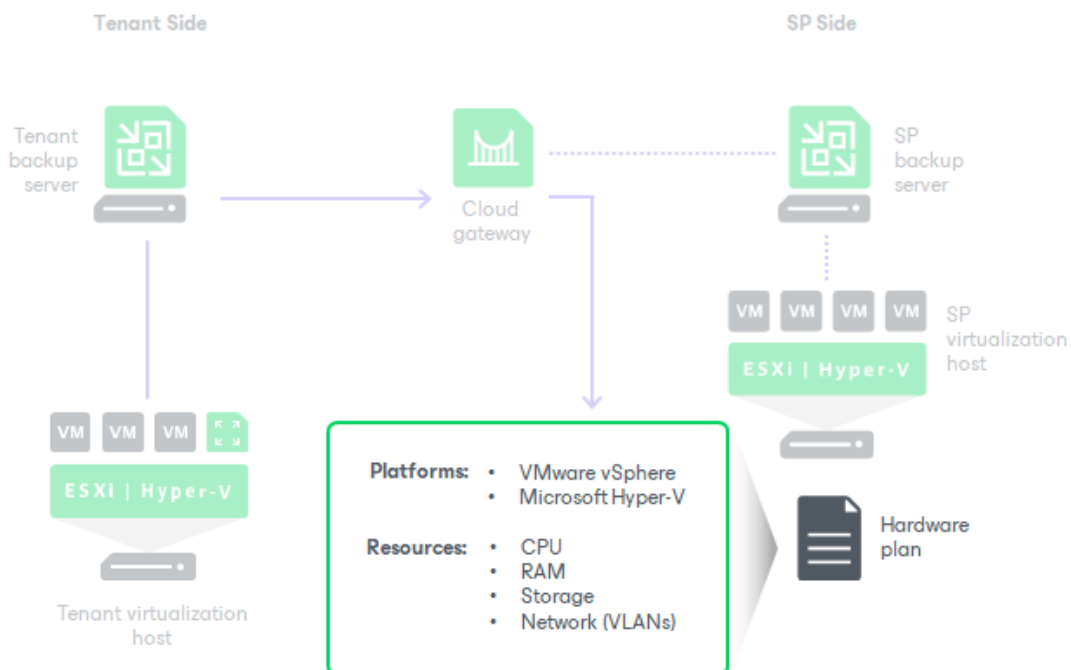
If the SP configures a hardware plan using resources allocated on a cluster, Veeam Backup & Replication automatically distributes the workload between the components of the cluster:

- 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 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 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 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 the tenant 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.

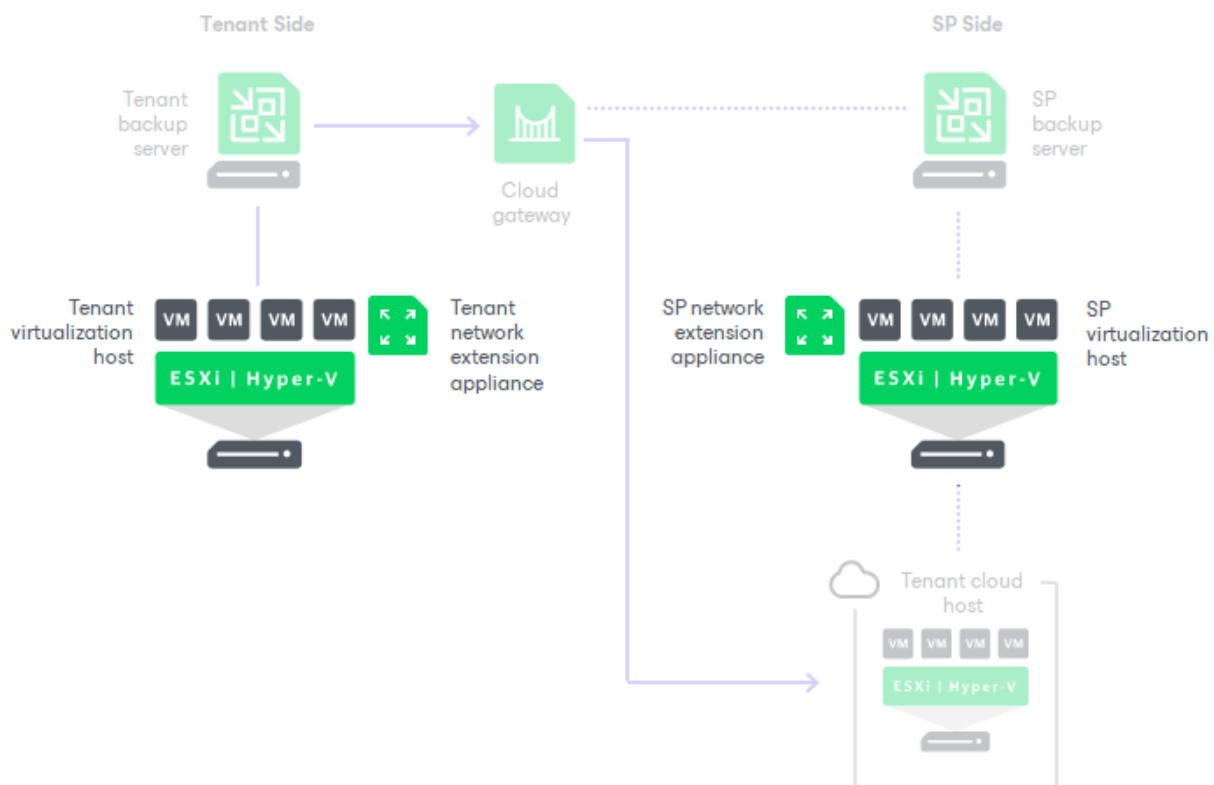
The SP specifies network settings for the provider-side network extension appliance when subscribing a tenant to a hardware plan. To learn more, see [Specify Network Extension Settings](#).

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 Network Extension Appliance

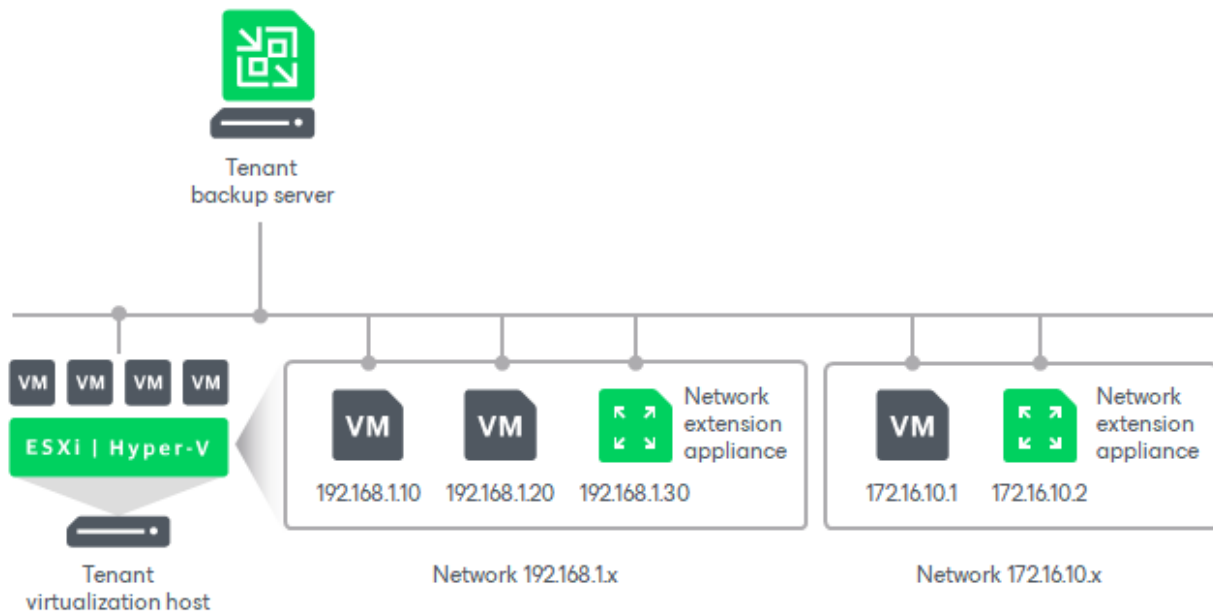
Veeam Backup & Replication uses the network extension appliance on the tenant side to route requests between production VMs on the source host and VM replicas on the cloud host after partial site failover.

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 networks 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 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:
 - VMware Virtual Volumes (VVols)
 - Datastore Cluster

WAN Accelerators

WAN accelerators are optional components in the Veeam Cloud Connect infrastructure. Tenants may use WAN accelerators:

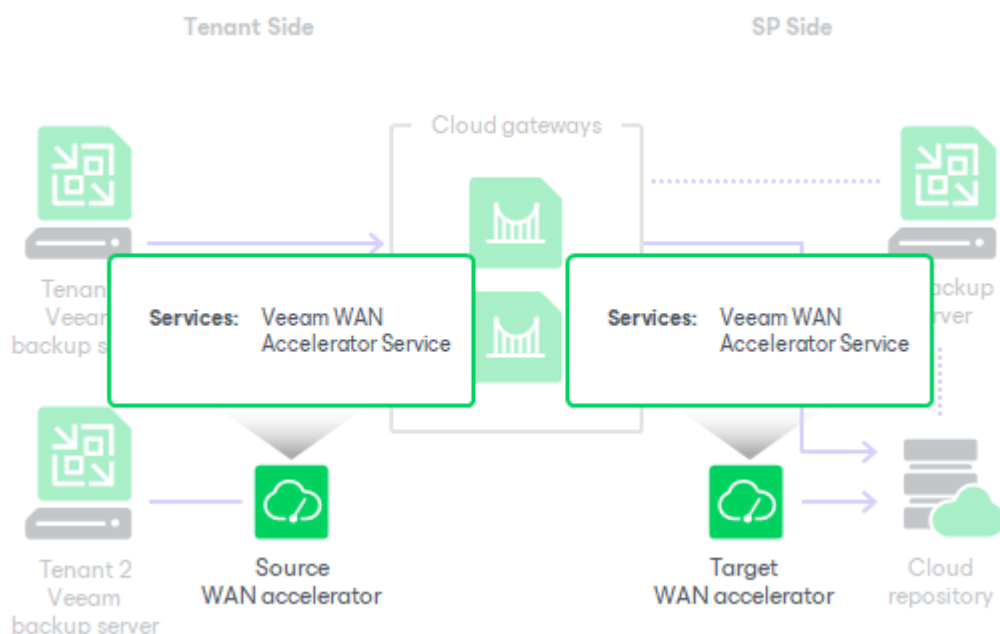
- For backup copy jobs targeted at the cloud repository
- For replication jobs targeted at cloud hosts

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 the tenant quota on the cloud repository and the hardware plan to which the tenant is subscribed (cloud host). This way, tenant 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 the [Manual Population of Global Cache](#) section in the Veeam Backup & Replication User Guide.

Service Providers and Tenants

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.

NOTE

Veeam Cloud Connect does not support Role-Based Access Control (RBAC). Tenants cannot be assigned custom roles to control access to the SP cloud infrastructure. However, tenants can use RBAC on the tenant backup server to control access to cloud backup copies. To learn more, see [Custom Roles on Tenant 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 selected VM restore operations and instant recovery from tenant backups. For details, see [Restoring Data from Tenant Backups](#).

Veeam Cloud Connect Replication Tasks

- Configuring the Veeam Cloud Connect Replication infrastructure — environment needed to expose SP 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 and CDP policies.
- 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 \(MSP Backup\)](#).

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](#).
- *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](#).

NOTE

Starting from Veeam Backup & Replication version 13, SP can no longer create new Active Directory tenant accounts in Veeam Cloud Connect. However, if the SP has previously configured Active Directory tenant accounts, tenants using supported versions of Veeam Agent or Veeam Backup & Replication (version 12 or earlier) may continue to access the cloud repository with these accounts. The SP can still manage existing Active Directory tenant accounts, but creation of new ones is no longer possible.

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.

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 backup policies in Veeam Service Provider Console. To learn more, see [How Secondary Password Works](#).
- Scenario 2. The tenant uses Veeam Backup & Replication version 12 or earlier, and the SP provided users of this tenant with access to a cloud repository through Active Directory tenant accounts. A user can continue to connect to the SP in Veeam Agent using an 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 Secondary Password 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.

Custom Roles on Tenant Side

The tenant can use role-based access control (RBAC) to grant users granular access to Veeam Cloud Connect backup copies. When the tenant assigns a custom role to a user or a group and includes cloud backup copies in the role restore scope, the user can see and restore only the backup copies within the assigned scope. For details on creating custom roles, see [Configuring Roles](#) in the Veeam Backup & Replication User Guide.

NOTE

This capability applies only to custom roles on the tenant backup server. It is unrelated to the Veeam Backup & Replication infrastructure on the SP side, for which Veeam Cloud Connect does not support RBAC.

Within the assigned scope, users with the custom role can perform the following operations with cloud backup copies:

- View and restore data from cloud backups and backup copies within the assigned scope.
- Perform point-in-time restore from transaction logs using the following Veeam Explorers:
 - Veeam Explorer for Microsoft SQL Server
 - Veeam Explorer for Oracle
 - Veeam Explorer for PostgreSQL

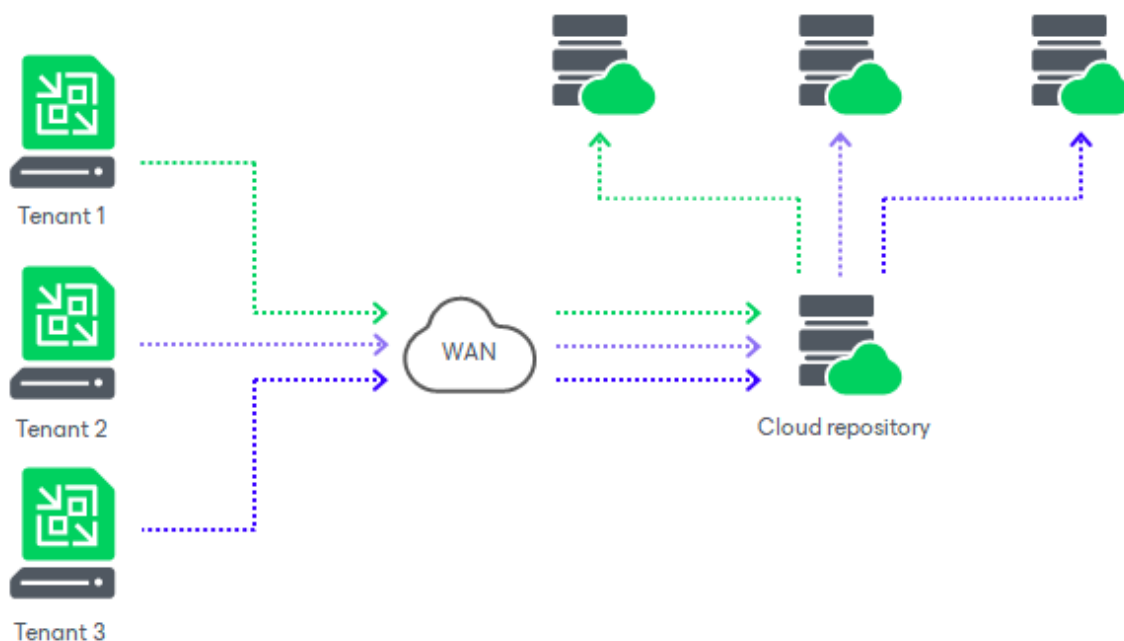
Consider the following limitations:

- A scoped custom role sees only the cloud backup copies included in its scope. Backup copies outside the scope are hidden.
- You can create custom roles only on the tenant backup server. An SP backup server with a Veeam Cloud Connect license installed does not support role-based access control.
- Custom roles can be configured only using the backup console. They are not supported in Veeam Backup Powershell, Veeam Backup & Replication web UI or Veeam Backup Enterprise Manager REST API.
- Users with a custom role can only use credentials that another user with Admin role created.

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. [Create tenant accounts.](#)
7. [Communicate information about the tenant account and gateway to all tenants who plan to connect to the SP.](#)

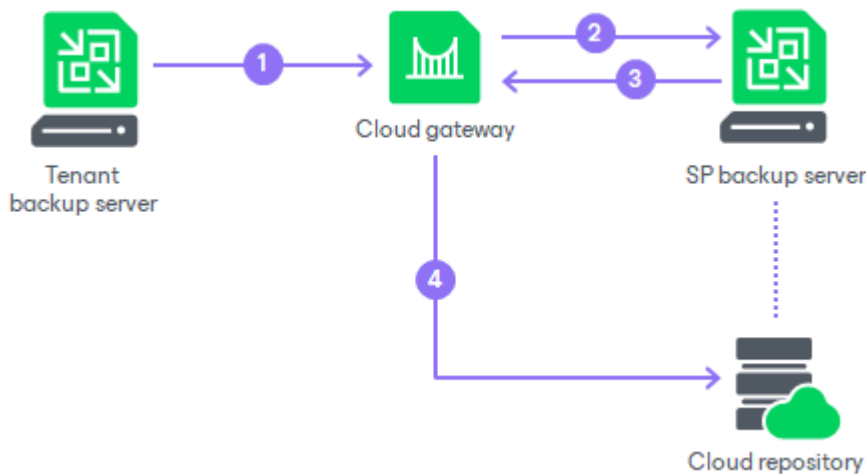
Once the SP has configured necessary components, tenants can add the SP to their Veeam Backup & Replication consoles and use cloud repositories allocated to them in the SP Veeam Cloud Connect infrastructure.

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 the tenant 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 the tenant 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. The tenant 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

VM backup is supported for VMware vSphere and Microsoft Hyper-V platforms only. For other platforms, use backup copy.

- 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)
 - Disk publishing
 - Instant Recovery to [Nutanix AHV](#) (requires an additional plug-in)
- Backup export
- File copy (manual operations)

Tasks on SP Side

In addition to data restore operations performed by the tenant, the SP can perform the following operations:

- Instant Recovery
- Backup restore to Microsoft Azure
- Backup restore to Amazon EC2
- Disk restore (using Veeam PowerShell cmdlets only)
- Disk publishing (using Veeam PowerShell cmdlets only)

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 files. 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 files 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 tenant backups if an object storage repository is assigned to the tenant as a cloud repository. After the SP assigns such a cloud repository to the tenant, backups in other repositories are no longer covered by insider protection.

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

For backups created by backup copy jobs, Veeam Backup & Replication does not move transaction log backup files to the "recycle bin".

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 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 backups 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 files 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 Customer Support](#).

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 files. This operation can be available depending on multiple conditions. For details, consider submitting a support case to the [Veeam Customer Support](#).

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. 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](#).

Support for Archive Tier

Archive tier is a functionality to extend a scale-out backup repository with an additional tier of storage. In the Veeam Cloud Connect infrastructure, the SP can use the archive tier 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 the restore from the archive tier. The tenant cannot restore data from the archive tier without support of the SP. The SP must retrieve the archived data to enable a successful restore from the archive tier. In contrast to the regular backup scenario where SP can retrieve archived data using the Veeam Backup & Replication console, in the Veeam Cloud Connect scenario, this operation is available with a Microsoft PowerShell cmdlet only. For more information, see [Retrieving Tenant Data from Archive Tier](#).

How Restore from Archive Tier Works

In the scenario where the tenant data is stored in the archive tier, the SP and tenant perform restore in the following way:

1. The tenant attempts to perform a restore operation.
2. During the restore process, Veeam Backup & Replication displays the following message: *Unable to restore from the Archive Tier because backup was not retrieved. Ask your service provider to publish restore point with ID '<restore point ID>'.*
3. The tenant collects the message with the restore point ID and sends it to the SP.
4. The SP retrieves the data, publishes the restore point and notifies the tenant that the restore point is ready for a restore.
5. The tenant reattempts to perform the restore operation from the published restore point.

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
- Veeam Data Cloud Vault

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.

To learn more about connection modes, see [How Backup to Object Storage Works](#).

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 [Creating 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:
 - Veeam Backup & Replication 13 (or later)

For Veeam Data Cloud Vault, both the SP and tenant must run Veeam Backup & Replication 12.1.2 (or later).

- Veeam Agent for Microsoft Windows 6.0 (or later)
- Veeam Agent for Linux 6.0 (or later)
- Veeam Agent for Mac 2.0 (or later)

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. In 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:
 - The *Connection through a gateway server* mode is supported without prerequisites and limitations.
 - 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.
- Veeam Data Cloud Vault can only be used as a cloud repository in the *Connection through a gateway server* mode.

- You cannot use S3 compatible repositories with multiple buckets as a cloud repository.
- For backup to Azure object storage, the tenant uses SAS (shared access signature) links. You can configure an expiration policy for SAS on your Azure container. In such case, the SAS expiry interval should be set to at least:
 - 30 days – for repositories using Shared Access Key.
 - 7 days – for repositories using Entra ID credentials.

For more information on how to configure an expiration policy for SAS, see [Microsoft docs](#).

How Backup to Object Storage Works

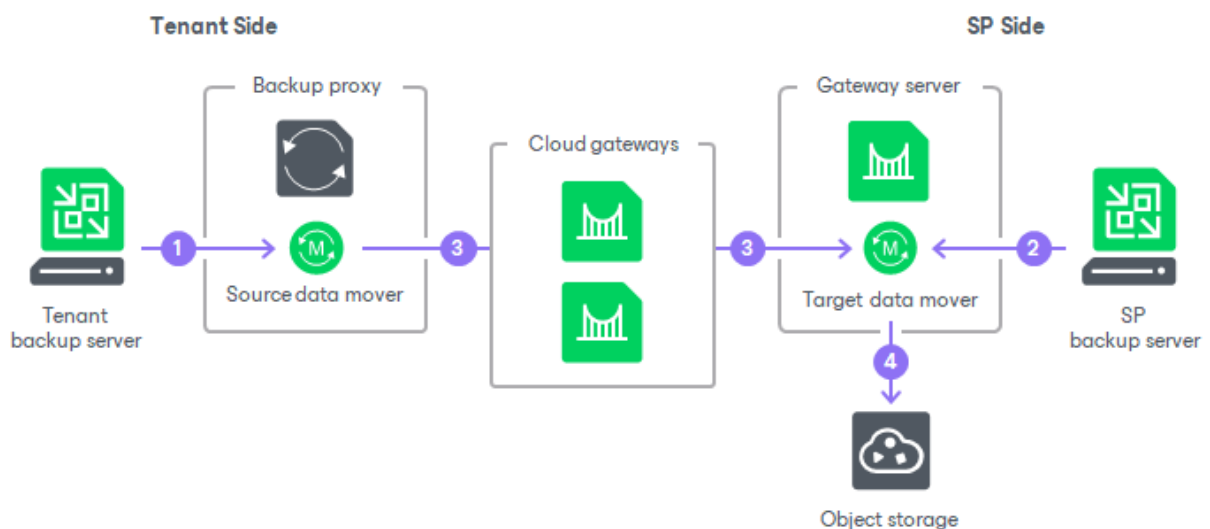
To back up data directly to object storage repository deployed on the SP side, Veeam products on the tenant side communicate with the object storage in one of the following connection modes:

- [Connection through a gateway server](#)
- [Direct connection](#)

Connection Through Gateway Server

In this mode, data traffic passes through a gateway server deployed in the Veeam Backup & Replication infrastructure on the SP side. This gateway server is specified in the object storage repository settings in the SP backup Veeam Backup & Replication console. Backup to the object storage works in the following way:

1. Veeam Backup & Replication on the tenant backup server starts the source Veeam Data Mover on the source backup proxy to access the object storage.
- In case of Veeam Agent backup, the source Veeam Data Mover is started on the Veeam Agent machine.
2. Veeam Backup & Replication on the SP backup server starts the target Veeam Data Mover on the gateway server.
 3. The source Veeam Data Mover sends backup data from Veeam Backup & Replication or Veeam Agent to the target Veeam Data Mover located on the gateway server on the SP side. The data passes through the cloud gateway.
 4. The target Veeam Data Mover transfers backup data from the gateway server to the object storage used as a cloud repository.



Direct Connection

In this mode, the tenant backs up data to the object storage directly. Backup to the object storage works in the following way:

1. Veeam Backup & Replication on the tenant backup server starts the source Veeam Data Mover and the target Veeam Data Mover, both on the source backup proxy.

In case of Veeam Agent backup, the source and the target Veeam Data Movers are started on the Veeam Agent machine.
2. The target Veeam Data Mover starts communication with the SP backup server through the cloud gateway.
3. Veeam Backup & Replication on the SP backup server obtains temporary credentials for the tenant from the object storage system.

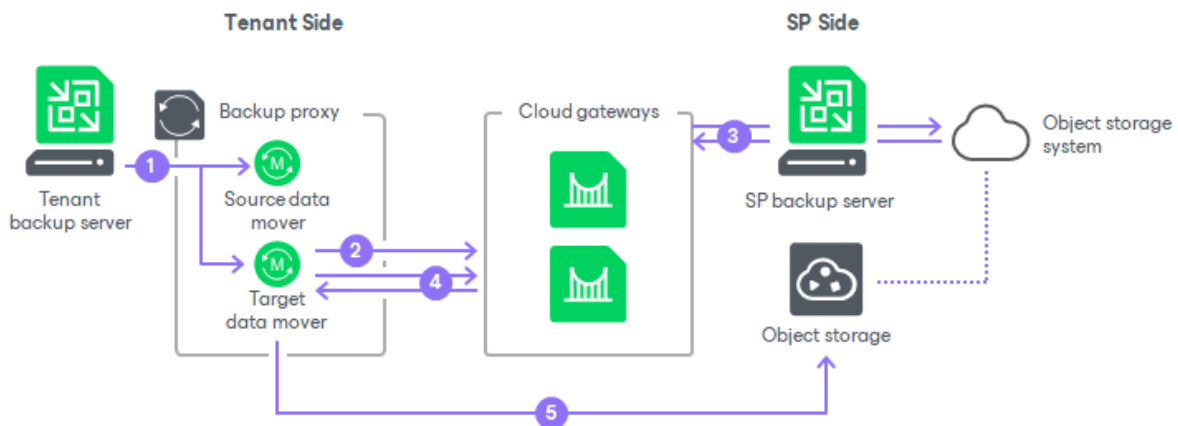
To learn more about temporary credentials, see [Credentials for Direct Connection Mode](#).

4. Veeam Cloud Connect sends credentials to the target Veeam Data Mover along with information about available storage quota. The target Veeam Data Mover uses these credentials to access object storage. The target Veeam Data Mover communicates constantly with the SP backup server to check and update information about available backup storage space.
5. The target Veeam Data Mover transfers backup data directly to the object storage.

During this process, the SP backup server and the tenant backup server keep persistent connection to each other through the cloud gateway to communicate credentials and backup storage space information.

NOTE

Keep in mind that direct backup to the S3 compatible object storage requires an additional action on the SP side. After selecting the *Direct connection* mode in the object storage repository settings, the SP must configure [access permissions](#) to access the object storage. Until the SP specifies access permissions, backup data to the S3 compatible object storage is transferred through the cloud gateway regardless of the *Direct connection* mode in the repository settings.



Credentials for Direct Connection Mode

To access the object storage in the *Direct connection* mode, Veeam products on the tenant side use temporary credentials. The SP obtains credentials from the object storage system and provides them to the tenant. Credentials are used in the following way:

- For backup to Google Cloud and AWS object storage, the tenant uses credentials with a limited access.

An expiration date for temporary credentials is 14 days. When connecting to the cloud gateway, the tenant Veeam Backup & Replication checks how much time is left before the expiration date. If there is less than 24 hours until the expiration date or if credentials have already expired, Veeam Backup & Replication renews them.

The temporary credentials are obtained through object storage APIs and saved in the configuration database on the SP side. On the tenant side, the credentials are kept encrypted in the target Veeam Data Mover runtime process and are not saved in the configuration database.

- For backup to Azure object storage, the tenant uses SAS (shared access signature) links.

By default, the links are valid for 30 days. When the tenant requests credentials, Veeam Backup & Replication checks how much time is left before expiration. If there is less than 15 days or if SAS links have already expired, Veeam Backup & Replication reissues them. The SP can instruct Veeam Backup & Replication to override default time limits with a registry key. For more information, contact [Veeam Customer Support](#).

- For backup to S3 compatible object storage, Veeam Backup & Replication offers three access permission options. Note that these take priority over *Connection through a gateway server* and *Direct connection* modes. The options are following:
 - *Agents share credentials to object storage repository.* If the SP selects this option, the cloud gateway passes the full set of credentials that are used in the repository settings to the tenant.
 - *Provided by the backup server.* If the SP selects this option, Veeam Backup & Replication does not pass credentials to the tenant side, and backup to the object storage is performed in a similar way to the *Connection through a gateway server* mode. With this option selected, backup to the object storage works in the following way:
 - The target Veeam Data Mover starts on the mount server selected in object storage settings.
 - The target Veeam Data Mover on the mount server processes data in the same way as the target Veeam Data Mover on a gateway server in the *Connection through a gateway server* mode.
 - Backup data is transferred between the source Veeam Data Mover and the target Veeam Data Mover through the cloud gateway.

This option is selected by default. For the data traffic to go directly from the tenant side to the object storage, the SP must select another access permission option.

- *Provided by IAM/STS object storage capabilities.* If the SP selects this option, Veeam Cloud Connect creates and provides credentials with limited access for the tenant.

In addition to configuring object storage settings, the SP must specify access permissions for each S3 compatible object storage repository added in the Veeam Cloud Connect infrastructure. For configuration details, see the [Managing Permissions for S3 Compatible Object Storage](#) section in the Veeam Backup & Replication User Guide.

Veeam Backup & Replication on the SP backup server passes temporary credentials to the tenant side only for backup, restore and other necessary operations. Temporary credentials provide tenants and subtenants with the following permissions:

- *Read* access to the backup repository configuration.

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

For details on object storage permissions in the *Direct connection* mode, see [Access Permissions for Direct Connection to Object Storage](#).

Access Permissions for Direct Connection to Object Storage

To back up data to object storage, you must set up access permissions. General permissions are listed in the [Using Object Storage Repositories](#) section in the Veeam Backup & Replication User Guide.

Additional permissions are required for object storage in the Veeam Cloud Connect infrastructure. The list of required permissions differs depending on the selected object storage and the way the SP sets the backup infrastructure. To learn more, see the following subsections:

- [Amazon S3](#)
- [S3 compatible storage \(including IBM Cloud and Wasabi Cloud\)](#)
- [Google Cloud](#)

Amazon S3

Consider the following:

- Make sure the user account you are using has access to Amazon buckets and folders.
- The *ListAllMyBuckets* permission is not required if you specify the bucket name explicitly at the **Bucket** step of the **New Object Repository** wizard.
- If you plan to use Amazon S3 storage with immutability enabled, see permissions required for immutability in the [Using Object Storage Repositories](#) section in the Veeam Backup & Replication User Guide. To learn more about immutability, see the [Backup Immutability](#) section in the Veeam Backup & Replication User Guide.

The list of permissions below is required for the following configuration:

- You plan to back up data to the Amazon S3 storage.
- You selected direct connection in the object storage settings. To learn more, see the [Adding Amazon S3 Object Storage, Amazon S3 Glacier Storage and AWS Snowball Edge](#) section in the Veeam Backup & Replication User Guide.

If you plan to back up data using the configuration above, make sure the user account that you use to connect to the object storage has the following permissions:

```
{
  "iam:AttachUserPolicy",
  "iam:CreateAccessKey",
  "iam:CreatePolicy",
  "iam:CreatePolicyVersion",
  "iam:CreateUser",
  "iam:DeleteAccessKey",
  "iam:DeletePolicy",
  "iam:DeletePolicyVersion",
  "iam:DeleteUser",
  "iam:DeleteUserPolicy",
  "iam:DetachUserPolicy",
  "iam:GetPolicy",
  "iam:GetPolicyVersion",
  "iam:GetUser",
  "iam:GetUserPolicy",
  "iam:ListAccessKeys",
  "iam:ListAttachedUserPolicies",
  "iam:ListPolicyVersions",
  "iam:ListUserPolicies",
  "iam:PutUserPolicy",
  "iam:SetDefaultPolicyVersion",
  "iam:SimulatePrincipalPolicy",
  "iam:TagUser"
}
```

S3 Compatible Storage (Including IBM Cloud, Wasabi Cloud)

Consider the following:

- Make sure the user account you are using has access to Amazon buckets and folders.
- The *ListAllMyBuckets* permission is not required if you specify the bucket name explicitly at the **Bucket** step of the **New Object Repository** wizard.
- If you plan to use S3 Compatible storage with immutability enabled, see permissions required for immutability in the [Using Object Storage Repositories](#) section in the Veeam Backup & Replication User Guide. To learn more about immutability, see the [Backup Immutability](#) section in the Veeam Backup & Replication User Guide.

The list of permissions below is required for the following configuration:

- You plan to back up data to the S3 compatible storage.
- Direct connection is selected in the object storage settings. To learn more, see the [Specify Object Storage Account](#) section in the Veeam Backup & Replication User Guide.
- The **Provided by IAM/STS object storage capabilities** option is selected for the object storage. To learn more, see the [Managing Permissions for S3 Compatible Object Storage](#) section in the Veeam Backup & Replication User Guide.

If you plan to back up data using the configuration above, make sure the user account that you use to connect to the object storage has the following permissions:

```
{
  "iam:AttachUserPolicy",
  "iam:CreateAccessKey",
  "iam:CreatePolicy",
  "iam:CreatePolicyVersion",
  "iam:CreateUser",
  "iam:DeleteAccessKey",
  "iam:DeletePolicy",
  "iam:DeletePolicyVersion",
  "iam:DeleteUser",
  "iam:DeleteUserPolicy",
  "iam:DetachUserPolicy",
  "iam:GetPolicy",
  "iam:GetPolicyVersion",
  "iam:GetUser",
  "iam:GetUserPolicy",
  "iam:ListAccessKeys",
  "iam:ListAttachedUserPolicies",
  "iam:ListPolicyVersions",
  "iam:ListUserPolicies",
  "iam:PutUserPolicy",
  "iam:SetDefaultPolicyVersion",
  "sts:GetCallerIdentity"
}
```

Google Cloud

The list of permissions below is required for the following configuration:

- You plan to back up data to the Google Cloud storage.
- You configured Helper Appliance in the object storage settings. To learn more, see the [Configuring Helper Appliance](#) section in the Veeam Backup & Replication User Guide.
- You selected direct connection in the object storage settings. To learn more, see the [Specify Object Storage Account](#) section in the Veeam Backup & Replication User Guide.

If you plan to back up data using the configuration above, make sure the user account that you specify in the Helper Appliance settings has the following permissions:

```
{
  "iam.serviceAccounts.create",
  "iam.serviceAccounts.delete",
  "iam.serviceAccounts.get",
  "iam.serviceAccounts.list",
  "storage.buckets.get",
  "storage.buckets.getIamPolicy",
  "storage.buckets.list",
  "storage.buckets.setIamPolicy",
  "storage.buckets.update",
  "storage.hmacKeys.create",
  "storage.hmacKeys.delete",
  "storage.hmacKeys.get",
  "storage.hmacKeys.list",
  "storage.objects.create",
  "storage.objects.delete",
  "storage.objects.get",
  "storage.objects.list"
}
```

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.

For more information, see the [Backup Copy](#) section in the Veeam Backup & Replication User Guide.

Supported Backup Types

Veeam Cloud Connect supports backup copy to the cloud repository for backups of the following workloads created by Veeam Backup & Replication:

- [VMware vSphere VMs](#)
- [VMware Cloud Director VMs](#)
- [Microsoft Hyper-V VMs](#)
- [Nutanix AHV VMs](#)
- [Proxmox VE VMs](#)
- [HPE Morpheus VM Essentials VMs](#) (requires installation of the HPE Morpheus plug-in)
- [oVirt KVM VMs](#)
- Backups created by backup copy jobs configured in Veeam Backup & Replication (For details, see [Support for Backup Copy from Backup Copy](#).)

Veeam Cloud Connect supports backup copy to the cloud repository for the following types of backups created by [Veeam Agents](#):

- Microsoft Windows machines
- Linux machines
- Mac machines
- IBM AIX machines
- Oracle Solaris machines (based on the x86 or SPARC architecture)

Veeam Cloud Connect supports backup copy to the cloud repository for backups of the following workloads created by Veeam products for public cloud backup:

- [Amazon EC2 instances](#)
- [Microsoft Azure VMs](#)
- [Google Compute Engine VM instances](#)

Support for Backup Copy from Backup Copy

Veeam Backup & Replication allows you to create a backup copy from another backup copy. For this operation, consider the following specifics and limitations:

- Veeam Cloud Connect supports this operation for copies of the following types of backups:
 - VMware vSphere VMs
 - VMware Cloud Director VMs
 - Microsoft Hyper-V VMs
- Veeam Cloud Connect does not support this operation for copies of the following types of backups:
 - Nutanix AHV VMs
 - Proxmox VE VMs
 - HPE Morpheus VM Essentials VMs (requires installation of the HPE Morpheus plug-in)
 - oVirt KVM VMs
 - Backups created by Veeam Agents
 - Backups of cloud workloads, such as Amazon EC2, Microsoft Azure or Google Cloud, created by Veeam products for public cloud backup

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.

NOTE

The SP can also disable background retention.

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.

Access to Tenant Backups

The SP can restore data from tenant backups stored in the cloud repository. The tenant controls the restore scope which is the group of backups the SP can access for restore. Starting from Veeam Backup & Replication version 13.1, the tenant can grant the SP access to both encrypted and unencrypted backups. As a result, the SP can perform recovery operations on behalf of the tenant directly in the SP infrastructure.

The tenant selects the restore scope when connecting to the SP or later when editing the SP connection. The following options are available:

- **None.** The SP cannot restore data from tenant backups from the cloud repository.
- **Unencrypted backups only.** The SP can only restore data from unencrypted tenant backups.
- **All.** The SP can restore data from both unencrypted and encrypted tenant backups.

To enable data restore from encrypted backups, Veeam Backup & Replication on the tenant side releases the encryption password to the SP, so that the SP can decrypt the backup for the restore operation. For details, see [How Access to Tenant Backups Works](#).

For details on how to set up access to tenant backups, see [Specify Backup Storage Settings](#).

When the tenant allows restore from encrypted backups, Veeam Backup & Replication decrypts the eligible backups on the SP side and stores them in decrypted form in the cloud repository. Backups outside the granted scope, or of unsupported types, remain encrypted. The SP cannot restore these backups.

How Access to Tenant Backups Works

After the tenant grants restore access to the SP, Veeam Backup & Replication on the tenant side performs the following steps:

1. Veeam Backup & Replication synchronizes information about all backups with the SP backup server. Synchronization runs when the feature is first enabled and every 15 minutes after that.
2. Veeam Backup & Replication checks what kind of restore access is granted to the SP.
3. Veeam Backup & Replication checks whether the backup is encrypted.
4. If the backup is encrypted, the tenant has allowed data restore from **All** backups, and the backup type is supported, Veeam Backup & Replication starts the decryption at the end of the synchronization. It releases the encryption password to the SP, which uses it in memory to decrypt the backup data and store it in decrypted form in the cloud repository and configuration database. Otherwise, the backup remains encrypted and is skipped during the SP restore.

Veeam Backup & Replication also starts the decryption when a tenant backup job begins, if a supported encrypted backup on the SP side has not been decrypted yet.

As a result of these operations, the SP has up-to-date information about which tenant backups it can restore, and all eligible encrypted backups are already decrypted on the SP side. Because the backups are already decrypted, the SP can restore them without requesting the encryption password from the tenant. The password is used only in memory during decryption and is never saved to the SP database.

Considerations and Limitations

For restore access to tenant backups, consider the following:

- The restore access settings apply to all backups of the tenant stored in the SP cloud repository.

- If the tenant Veeam backup server runs Veeam Backup & Replication version 13.1 and the SP Veeam backup server runs Veeam Backup & Replication version the Unencrypted backups only and the All option is unavailable. For the tenant to allow the SP to restore data from unencrypted backups, 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 [Specify Cloud Gateway Settings](#).

It is recommended, however, that the SP and tenant both always install latest hotfixes and updates on the backup server. For the SP to see tenant backups in the SP Veeam backup console, the tenant must also

- Any updates to the restore scope or encryption password are not applied immediately. They take effect during the next synchronization cycle, which runs every 15 minutes.
- The feature is not supported if the SP uses tenant backup to tape job functionality for the tenant.

In such cases, the tenant cannot enable access to restore data from encrypted backups. The SP can only restore data from unencrypted tenant backups.

If the tenant has already enabled the option to restore data from both unencrypted and encrypted backups for the SP, tenant backup to tape job cannot be started on the SP side.

- The feature is not supported for backups created by Veeam Agent for Linux, Veeam Agent for Mac, Veeam Agent for Oracle Solaris and Veeam Agent for IBM AIX in any operation mode.
- For backups created by Veeam Agent for Microsoft Windows, the following limitations apply:
 - The feature is not supported for Veeam Agent for Microsoft Windows operating in the standalone mode.
 - The feature is not supported for Veeam Agent for Microsoft Windows version 13.0 or earlier. Only imported or orphaned backups created by these versions are decrypted.
- [For backups encrypted with a KMS key] Only KMS-encrypted backups created after the upgrade to Veeam Backup & Replication version 13.1 are supported. They are sent to the SP in decrypted form. Backups encrypted with a KMS key before the upgrade are skipped, because the tenant has no password to forward to the SP for decryption.
- [For backups encrypted with password loss protection enabled in Veeam Backup Enterprise Manager] The SP cannot decrypt such backups. To make these backups available to the SP, the tenant must map the backup to a backup job, assign a password, and run the job to re-encrypt the backup. After that, the backup works like a regular encrypted backup.
- To use this feature, both the SP and tenant must run Veeam Backup & Replication version 13.1 or later.
- The feature is not supported for backup formats unsupported in Veeam Backup & Replication version 13.0 (or earlier), such as reverse incremental backups or per-VM backups in the legacy (split VM) format.
- If a backup was decrypted on the SP side and then the backup is re-imported into the SP Veeam Backup & Replication configuration database, the backup will be encrypted again. To restore it on the SP side, the tenant must re-release the encryption password.
- If a tenant backup was ever offloaded to the capacity tier or archive tier of a scale-out backup repository, Veeam Backup & Replication skips its decryption on the SP side. This applies even if the backup was later removed from the configuration and re-imported, or if the capacity tier or archive tier was removed from the scale-out backup repository. Once a backup has been offloaded, it is never decrypted.
- Backups that are created after the feature is enabled and are decrypted on the SP side are not offloaded to the capacity tier or archive tier.

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 Veeam Agent users, consider that to display on the SP side backups created by Veeam Agent in the standalone mode, a backup server connected to the SP with the **Allow this Veeam Backup & Replication installation to be managed by the service provider** option enabled is required.

- 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 encrypted tenant backups only if the tenant has granted the SP restore access to all backups. For details, see [Access to Tenant Backups](#).

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.

Considerations and Limitations

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.

Note that Veeam Cloud Connect supports Instant Recovery to VMware vSphere only. Other platforms are not supported as an Instant Recovery target.

- Veeam Cloud Connect supports Instant Recovery from backups that reside in the performance tier, capacity tier or archive tier.
- During Instant Recovery, the tenant account will be in the disabled state.

[For backups in the archive tier] The Instant Recovery operation will be pending until the backed-up data is retrieved from the archive tier. Data retrieval time may take from several minutes to several hours depending on the object storage system and data retrieval method. During this time, the tenant account will be in the disabled state. For more information on data retrieval cost and speed, see the [Data Retrieval](#) section in the Veeam Backup & Replication User Guide.

Note that after Instant Recovery, the tenant account remains in the disabled state. The SP needs to manually enable the tenant account. For details, see [Disabling and Enabling Tenant Accounts](#).

- 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:
 - For Instant Recovery from VM backups, see the [Considerations and Limitations](#) section in the Veeam Backup & Replication User Guide.
 - For Instant Recovery from Veeam Agent backups, see the [Restoring Veeam Agent Backup to vSphere VM](#) section in the Veeam Backup & Replication User Guide.

Tenant Backups in SP Backup Console

In the SP Veeam backup console, tenant backups are displayed under the **Backups** node of the **Home** view. To identify tenant backups available for Instant Recovery, as well as 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 account name in the **Tenant Name** column.
- For Veeam Agent backups created under the subtenant account, Veeam Backup & Replication displays the subtenant account 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.

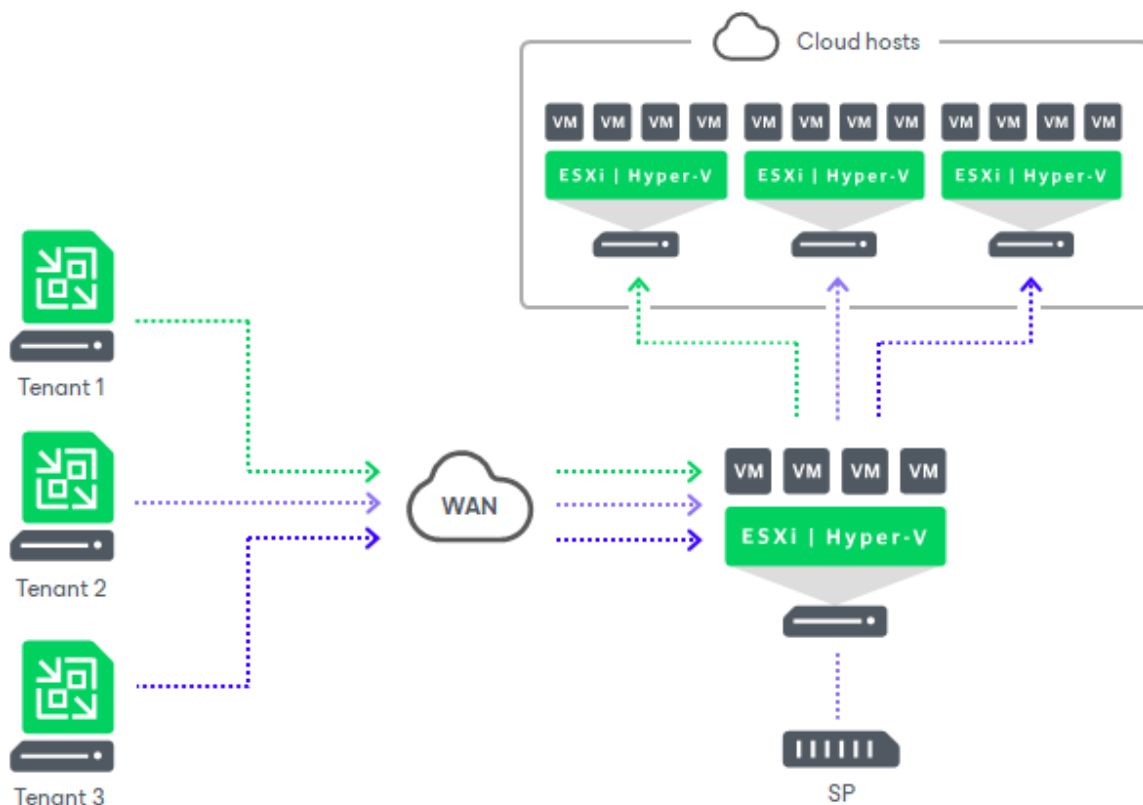
For a tenant, a hardware plan appears as a cloud host that can be used as a regular target host for off-site replication.

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 the tenant production site to the cloud host upon a request from the tenant 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] [Configure target WAN accelerators](#).
9. [Create tenant accounts](#).
10. [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 [VMware Cloud Director Support](#).

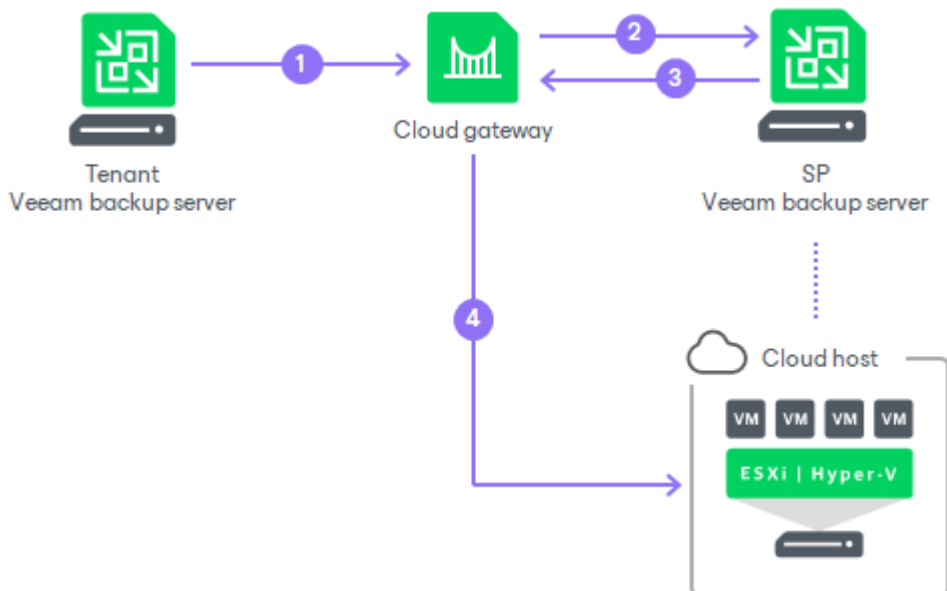
Once the SP has configured necessary components, tenants can add the SP to their Veeam Backup & Replication consoles and use cloud hosts allocated to them in the SP Veeam Cloud Connect infrastructure.

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 the tenant 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 the tenant 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
 - Full site failover (failover by cloud failover plan)
 - Partial site failover
- Failback
- Restore from replica
 - VM guest OS files restore (Microsoft Windows FS only. Multi-OS restore is not supported.)
 - 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:

- [Failover and Failback for Replication](#)
- [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.

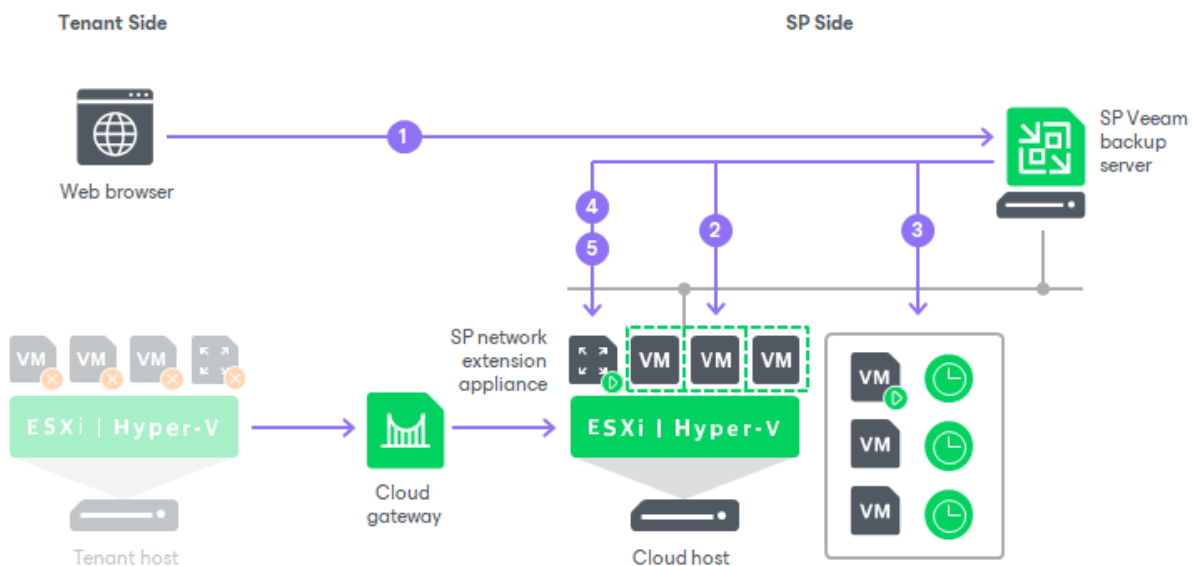
Full site failover is performed in the following way:

1. The tenant 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:

- 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:
 - 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.
 - 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: undo 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

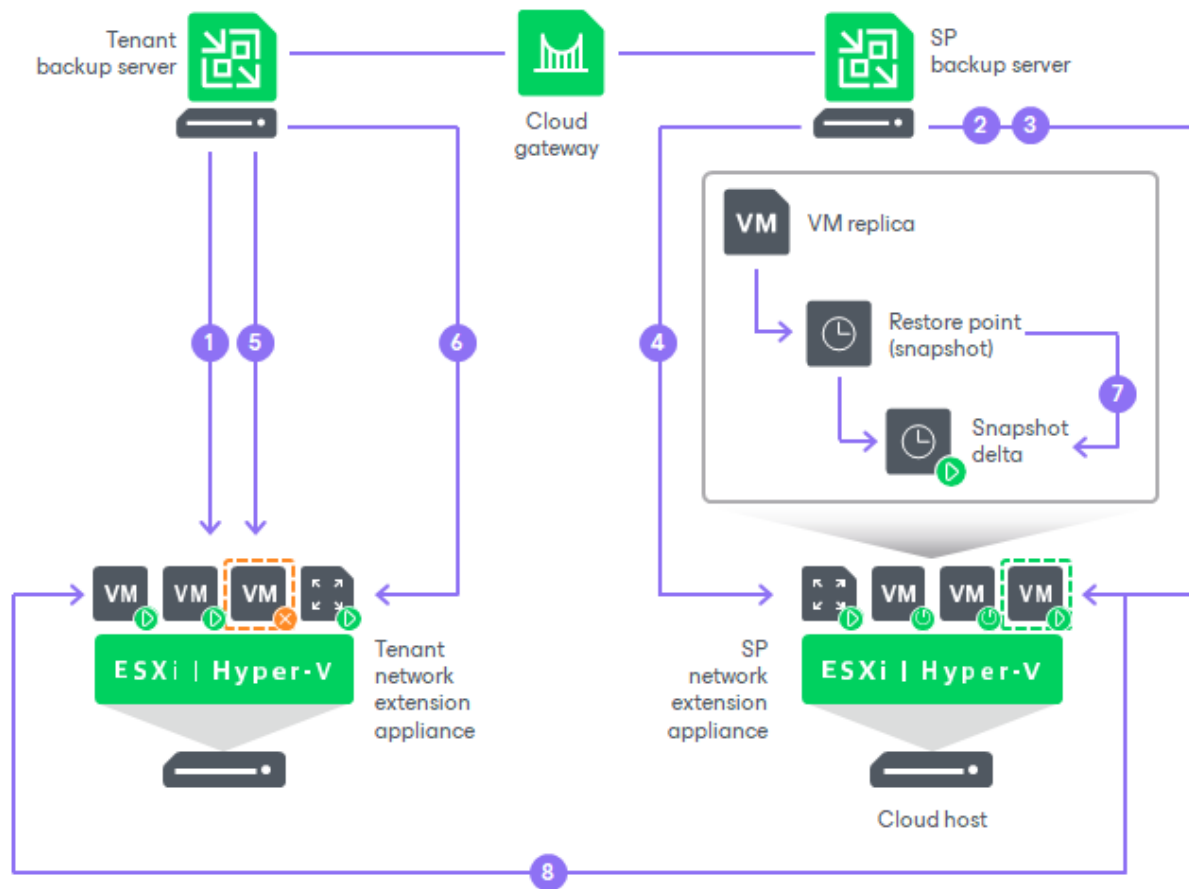
If one or several production VMs become corrupted, but the rest of the production site, including the most critical VMs and Veeam Backup & Replication infrastructure, remain operative, the tenant can perform partial site failover. With partial site failover, the tenant can quickly recover a corrupted 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:
 - 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.
 - 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 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:
 - 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.
 - 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 in the following cases:

- If the cloud host has fewer networks than the number of networks in the production infrastructure.
- 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.
- If IPv6 communication is enabled in the Veeam Cloud Connect infrastructure.

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 [Failover and Failback for Replication: Failback](#) section in the Veeam Backup & Replication User Guide.

- To learn more about failback for CDP replicas, see the [Failover and Failback for CDP: Failback](#) 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 without creating snapshots. This allows the SP to protect mission-critical tenant machines for which data loss is unacceptable: compared to snapshot-based replication, CDP provides near-zero recovery time objective (RTO) because CDP replicas are in a ready-to-start state.

Veeam Cloud Connect supports the following types of the CDP technology offered by Veeam Backup & Replication:

- [CDP for VMware vSphere](#)
- [Universal CDP to VMware vSphere](#)

NOTE

Veeam Cloud Connect does not support VMware Cloud Director as a source for CDP replication. With Veeam Cloud Connect, you can only replicate individual VMware vSphere VMs, not vApps.

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 tenant machines. To learn more about CDP mechanisms in Veeam Backup & Replication, see the [Continuous Data Protection \(CDP\) for VMware vSphere](#) and [Universal CDP to VMware vSphere](#) sections 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 machines or individual machines to CDP replicas on the cloud host.

Veeam Cloud Connect CDP Scenarios

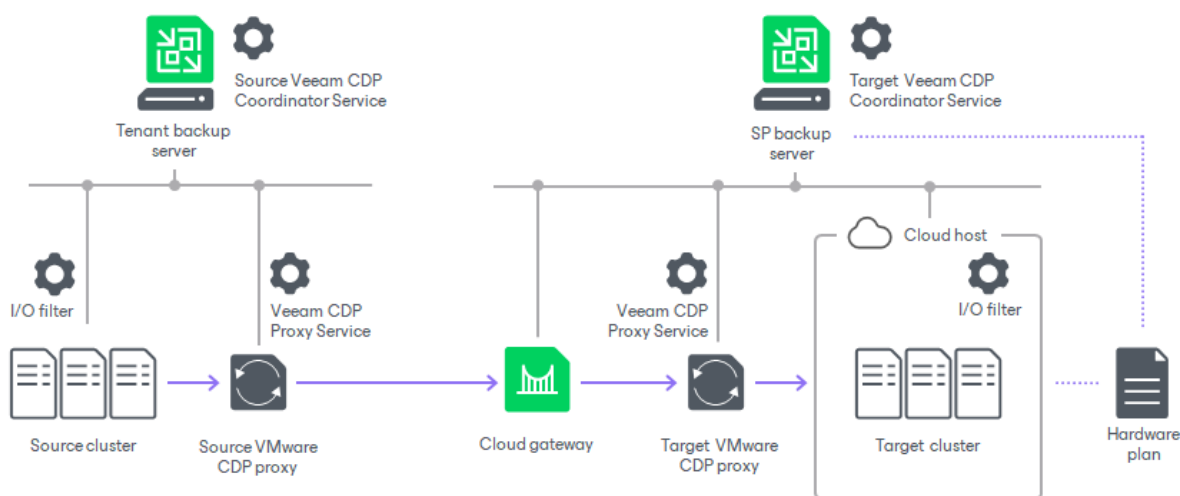
Veeam Cloud Connect offers the following CDP scenarios.

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 or source workload 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.

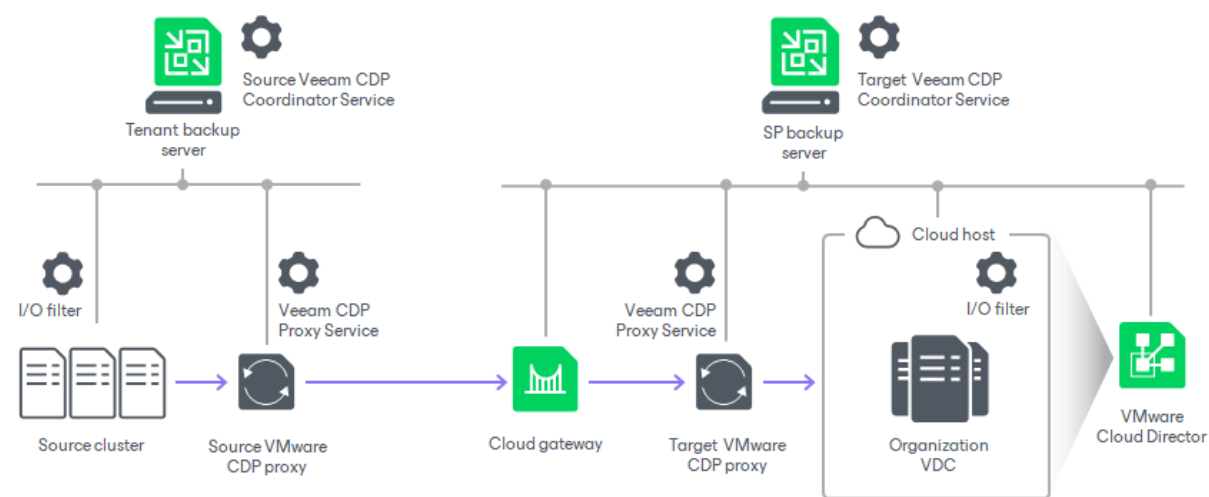


Scenario 2. CDP to VMware Cloud Director

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 or source workload to the cloud host that has VMware Cloud Director resources as a back end.

This scenario is similar to [VMware Cloud Director Support](#).



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 CDP proxies](#)

Components on the tenant side

- [Tenant Veeam backup server](#)
- [One or more source virtualization hosts](#) (in case of CDP for VMware vSphere)
- [One or more source workloads](#) (in case of universal CDP)
- [One or more source 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 a part of the CDP for VMware vSphere infrastructure. 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.

Source Workloads

Source workloads are a part of the universal CDP infrastructure. Source workloads can be of various types, such as physical machines, virtual machines, or cloud instances. However, Veeam Backup & Replication supports specific operation systems. For more information, see the [Supported Platforms, Applications and Workloads](#) section in the Veeam Backup & Replication User Guide.

Veeam CDP Agent Service and Veeam CDP Volume Filter Drive

To protect workloads, the tenant must install the Veeam CDP Agent Service and Veeam CDP Volume Filter Driver on those workloads.

The driver intercepts I/O transactions generated by the operating system and sends them to the CDP agent service. The CDP agent service deploys the drivers, receives the captured data, aggregates it and sends to the CDP proxies. For information on how to install the service and the drivers, see the [Installing CDP Agent Service and Filter Driver](#) section in the Veeam Backup & Replication User Guide.

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.

NOTE

If you add a new organization VDC to the Cloud Director server after the I/O filter is installed on the existing VDCs, you must do the following:

1. Install the I/O filter on the newly added organization VDC. To do this, at the **Organization VDC** step of the **I/O Filter Management** wizard, select check boxes next to the VDC where the I/O filter must be present and finish the wizard. For details, see the [Select VDC Organizations](#) section in the Veeam Backup & Replication User Guide.
2. Create CDP target policy on the new organization VCD and mark it as CDP-ready. To do this, launch the **Edit Tenant** wizard for this tenant, click **Next** at each step of the wizard. At the **Replica Resources** step of the wizard, add new organization VDC as replication resource and then click **Finish** at the **Summary** step of the wizard. For details, see [Allocate Replication Resources](#).

Once the SP completes these steps, the tenant can rescan the SP in the tenant Veeam backup console and start using the newly added VDC as a cloud host.

- [For CDP for VMware vSphere] 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.

NOTE

For universal CDP, Veeam CDP Agent Service and Veeam CDP Volume Filter Driver are used on the tenant side. To learn more, see [Source Workloads](#).

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 underlying datastores.
- Send and receive data to and from 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 CDP Proxies

A 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 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 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 it to the target host.

For more information on CDP proxies, their requirements, limitations and deployment, see the [CDP Proxies](#) 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:
 - [For the CDP to VMware vSphere scenario] If you want to use resources of a VMware vSphere cluster, create 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](#).
 - [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 CDP proxy. For details, see the [Adding 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.
 - [For the CDP to VMware vSphere scenario] Subscribe as the tenant with a standalone tenant account to a hardware plan. For details, see [Configuring Standalone Tenant Account](#).

- [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 CDP proxy. For details, see the [Adding CDP Proxies](#) section in the Veeam Backup & Replication User Guide.
 - b. [For CDP for VMware vSphere] 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.
 - c. [For universal CDP] Install Veeam CDP Agent Service and Veeam CDP Volume Filter Driver on the source workloads, that is, machines for which the tenant wants to create CDP replicas. For details, see the [Installing CDP Agent Service and Filter Driver](#) 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.

- 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.
 - 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 for VMware vSphere](#) and [Creating Universal 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

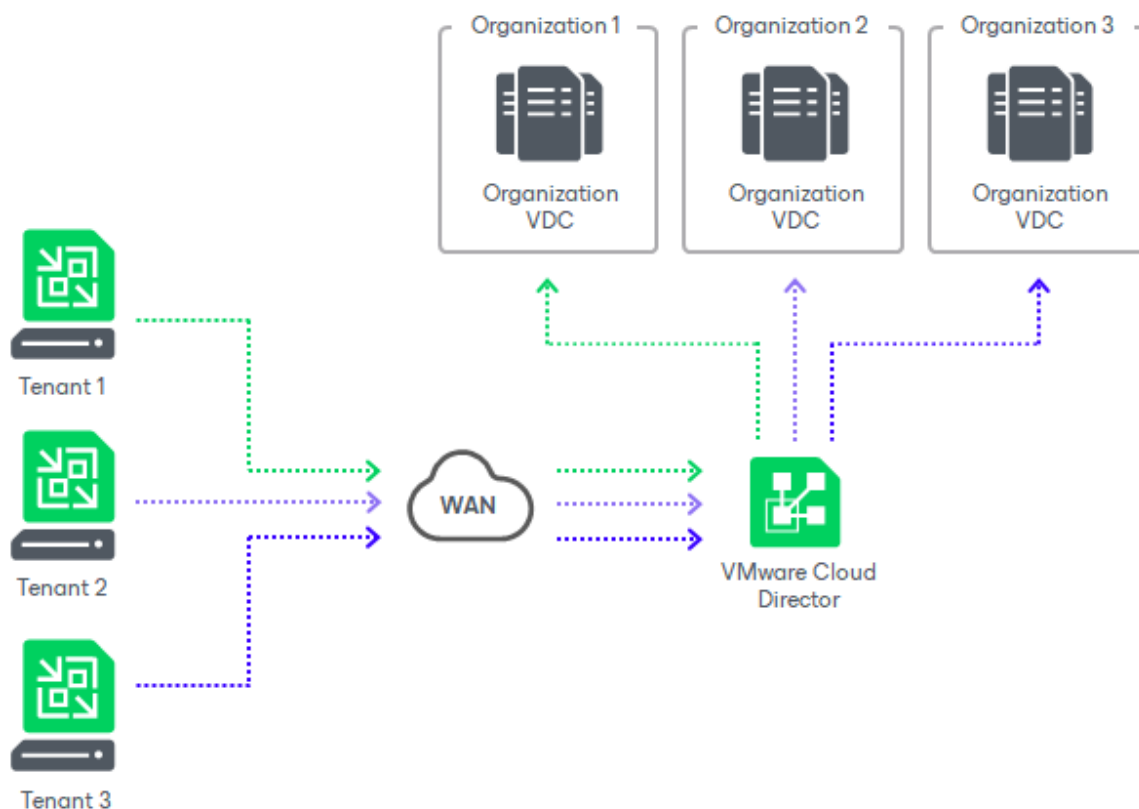
SPs who have VMware Cloud Director deployed in their infrastructure can expose VMware Cloud Director resources as cloud hosts for tenant VM replicas. This allows such SPs to offer Disaster Recovery as a Service (Veeam Cloud Connect Replication) to tenants without the need to deploy additional VMware 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.

NOTE

Veeam Cloud Connect does not support VMware Cloud Director as a source for replication to a VMware Cloud Director target.

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 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 Servers](#) 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 CDP proxies (for CDP). For details, see the [Adding VMware Backup Proxies](#) and [Adding 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.

NOTE

If you add a new organization VDC to the Cloud Director server after the I/O filter is installed on the existing VDCs, you must do the following:

1. Install the I/O filter on the newly added organization VDC. To do this, at the **Organization VDC** step of the **I/O Filter Management** wizard, select check boxes next to the VDC where the I/O filter must be present and finish the wizard. For details, see the [Select VDC Organizations](#) section in the Veeam Backup & Replication User Guide.
2. Update properties of the cloud gateway through which the tenant who will use the newly added VDC connects to the SP. To do this, launch the **Edit Cloud Gateway** wizard for this cloud gateway, click **Next** at each step of the wizard and then click **Finish** at the **Summary** step of the wizard.

Once the SP completes these steps, the tenant can rescan the SP in the tenant Veeam backup console and start using the newly added VDC as a cloud host.

- 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 CDP proxies (for CDP). For details, see the [Adding VMware Backup Proxies](#) and [Adding 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

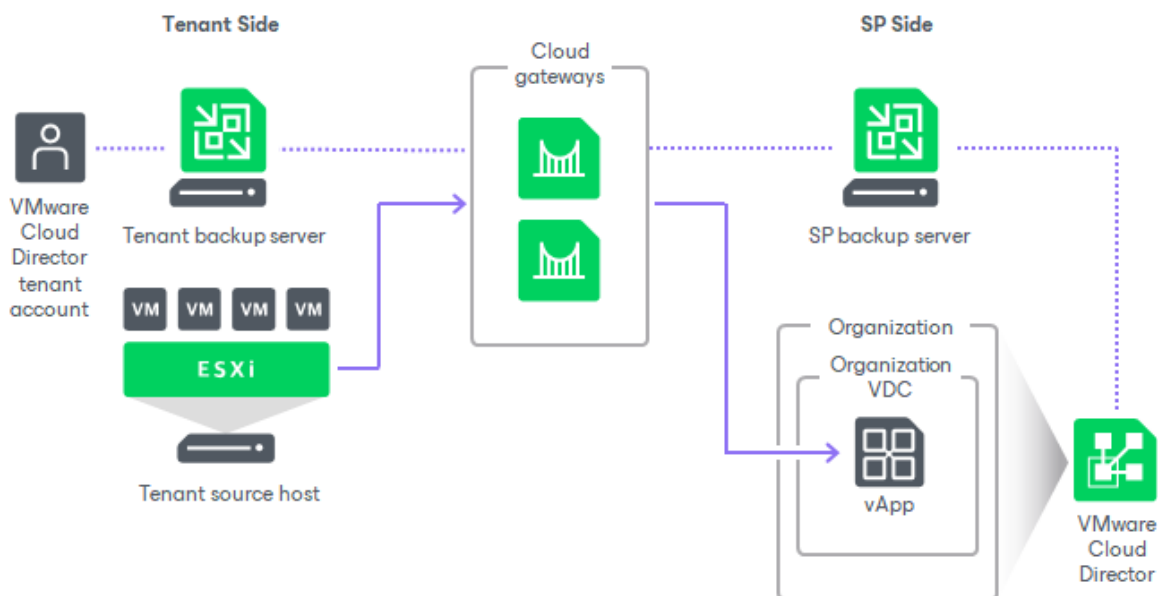
To let the tenant create VM replicas in VMware Cloud Director, the SP must register for this tenant a tenant account of a specific type — a VMware Cloud Director tenant account. When the SP registers a VMware Cloud Director tenant account, the SP permits the tenant to access Cloud Director organization 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:
 - 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](#).

- 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:

- To provide network resources to tenant VM replicas, the SP should use isolated organization VDC networks.
- 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.
- 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.
- 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 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:
 - 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.
 - 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 network extension appliance through the VPN tunnel.

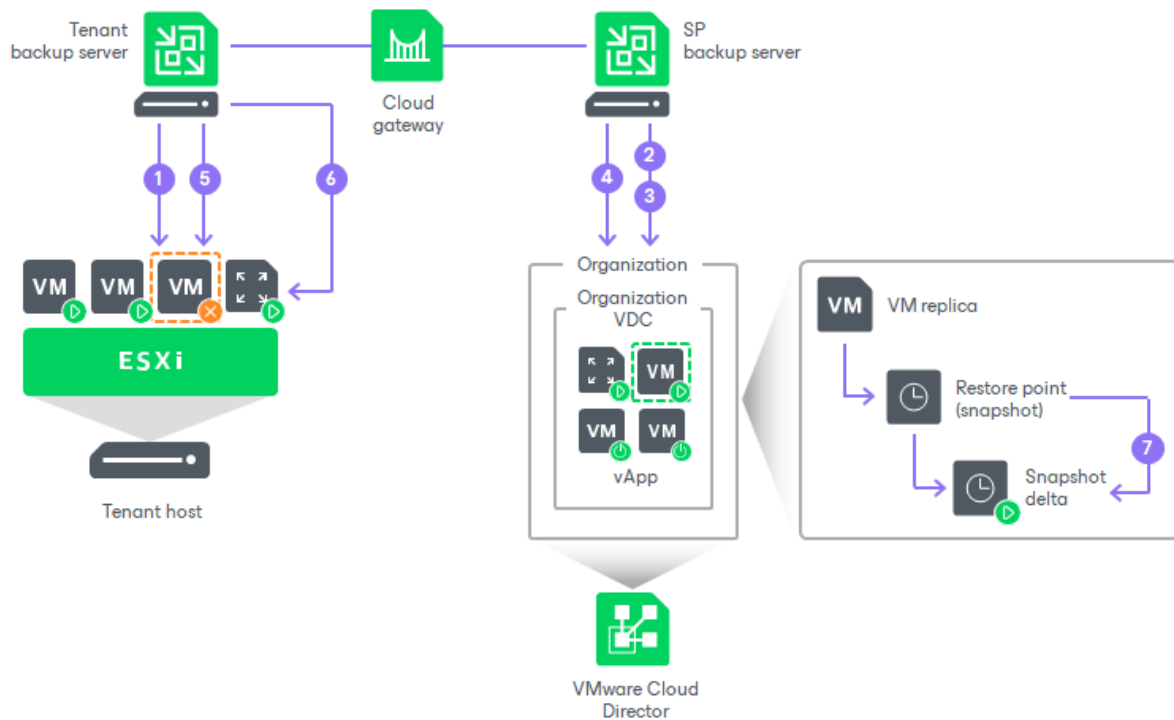
In addition, the SP network extension appliance imports in its vApp all organization VDC networks and connects to these networks. Keep in mind that if the number of organization VDC networks is greater than 9, the failover operation will fail because the number of virtual network adapters for a VMware 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:
 - 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.

- 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.

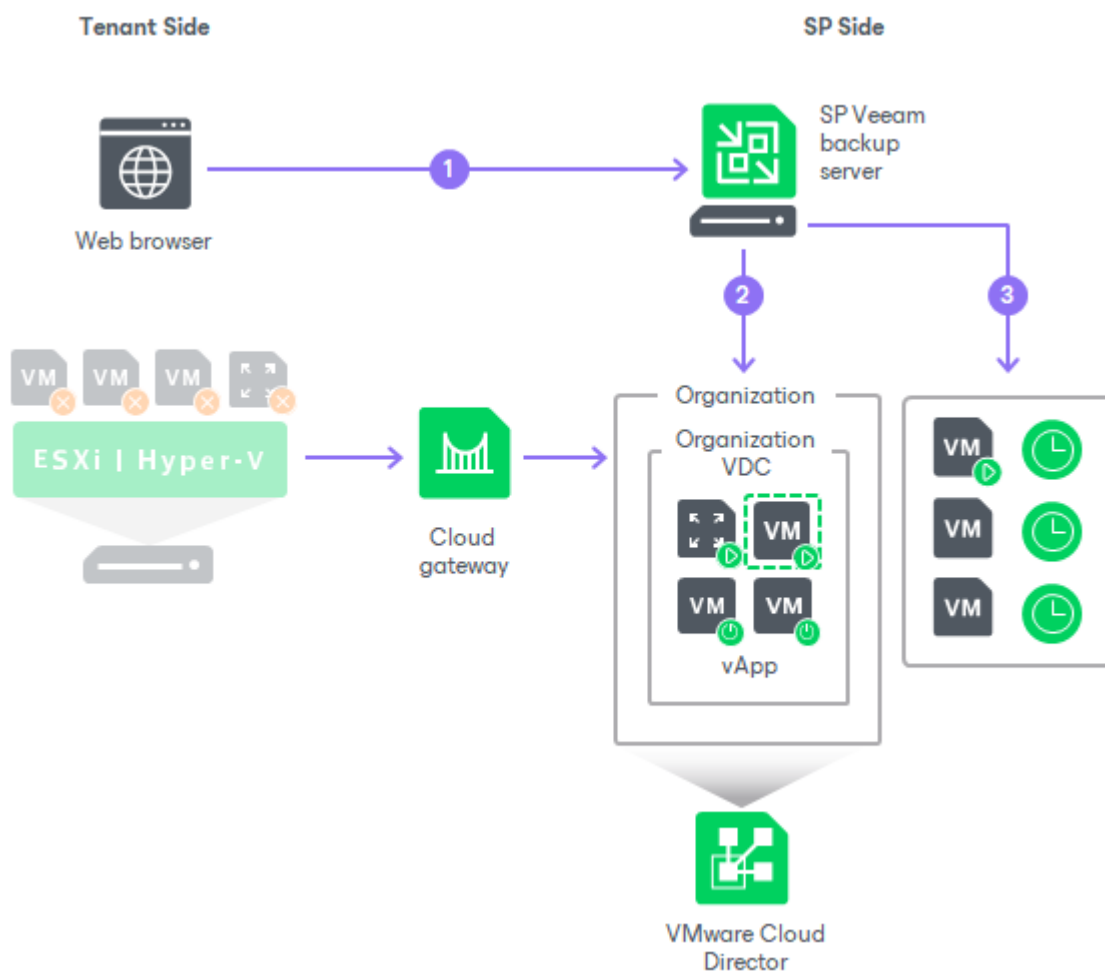
Full site failover for tenant VM replicas in VMware Cloud Director is in many regards similar to full site failover for VM replicas created on a cloud host provided through a hardware plan. To perform full site failover to VM replicas in VMware Cloud Director, the tenant must create a cloud failover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

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 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](#).

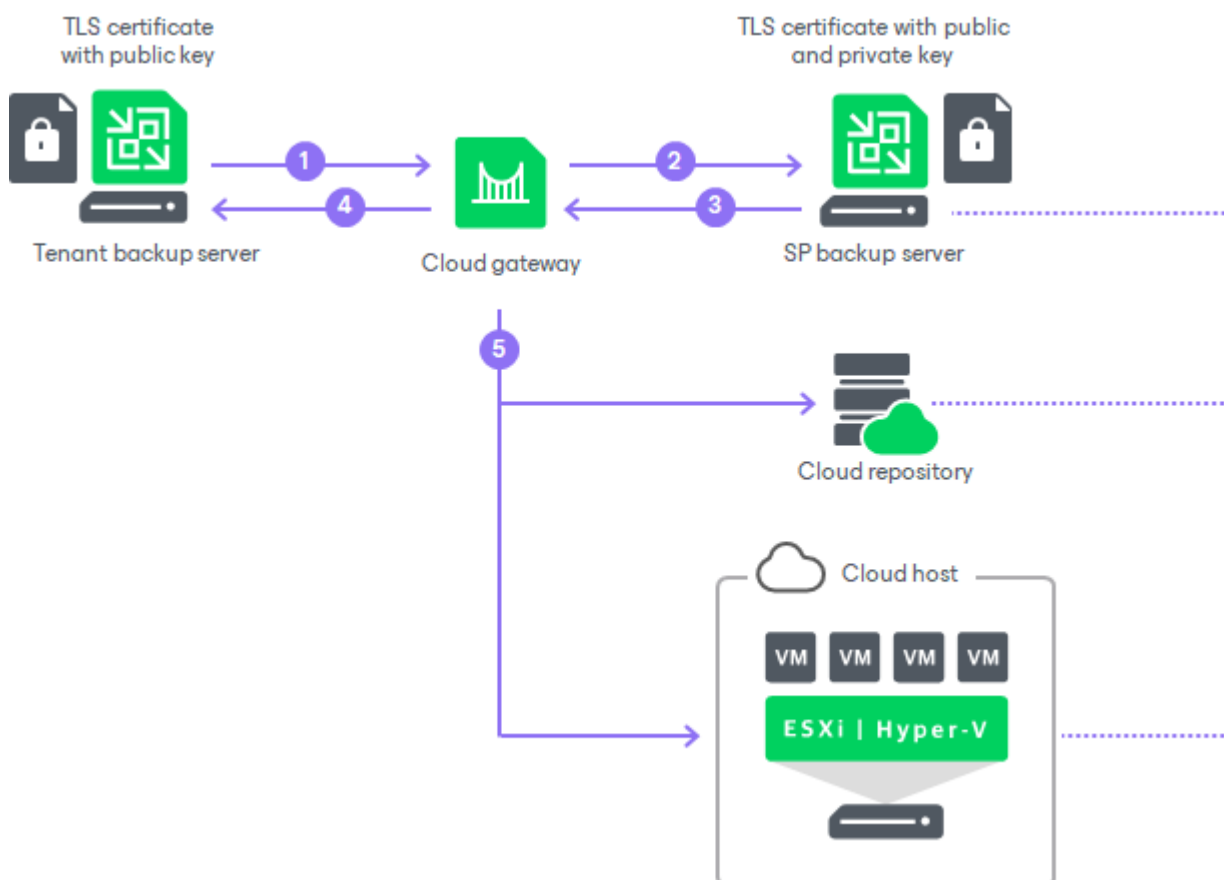
TLS Certificates Handshake

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 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 the tenant 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 documentation](#).

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:

- User who created the TLS certificate
 - LocalSystem Windows account
 - Local Administrators group
3. The Windows account must have access to the TLS certificate itself (stored in the registry) and permissions to the registry folders that contain that certificate.

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 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 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

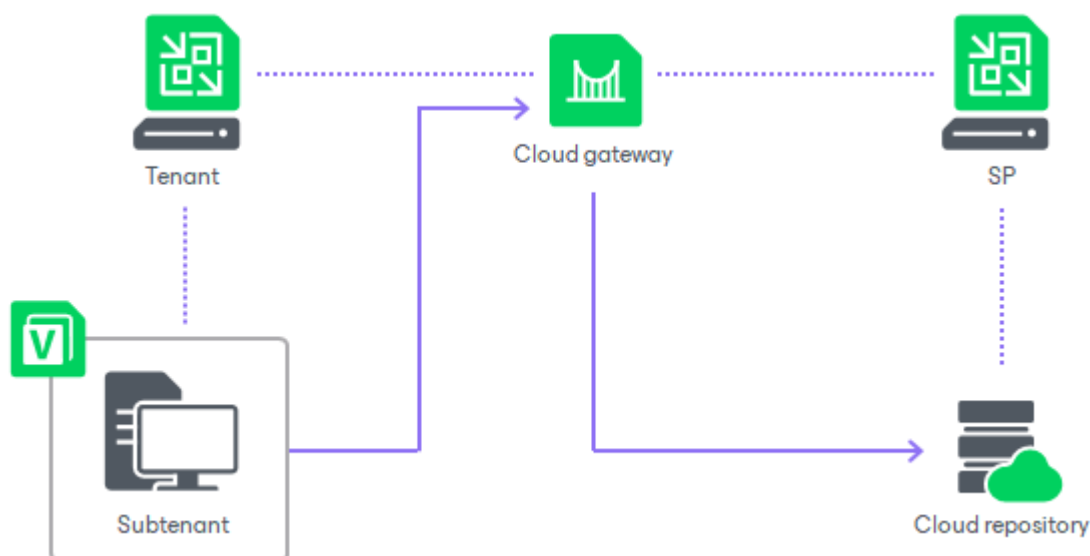
Consider the following:

- 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



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.

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 Backup & Replication User 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.

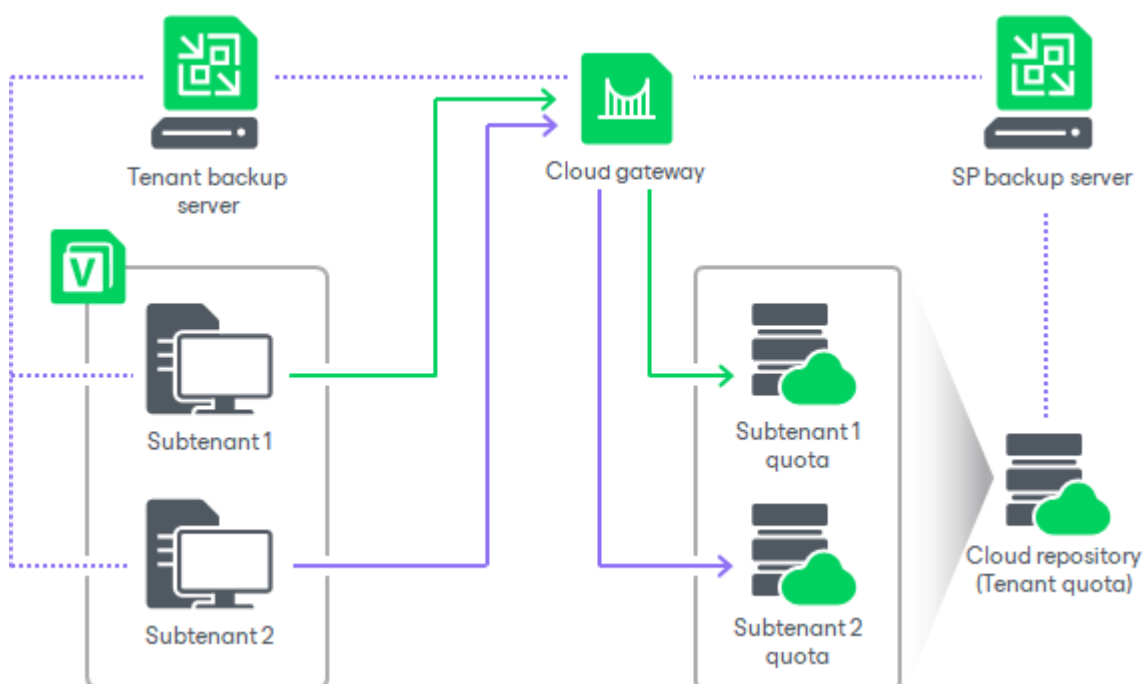
The tenant or SP can allocate only one quota on one cloud repository for each subtenant account. If the tenant or SP wants to provide to a user multiple quotas on the same or different cloud repositories, they must create different subtenant accounts for this user.

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 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 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 you 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 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

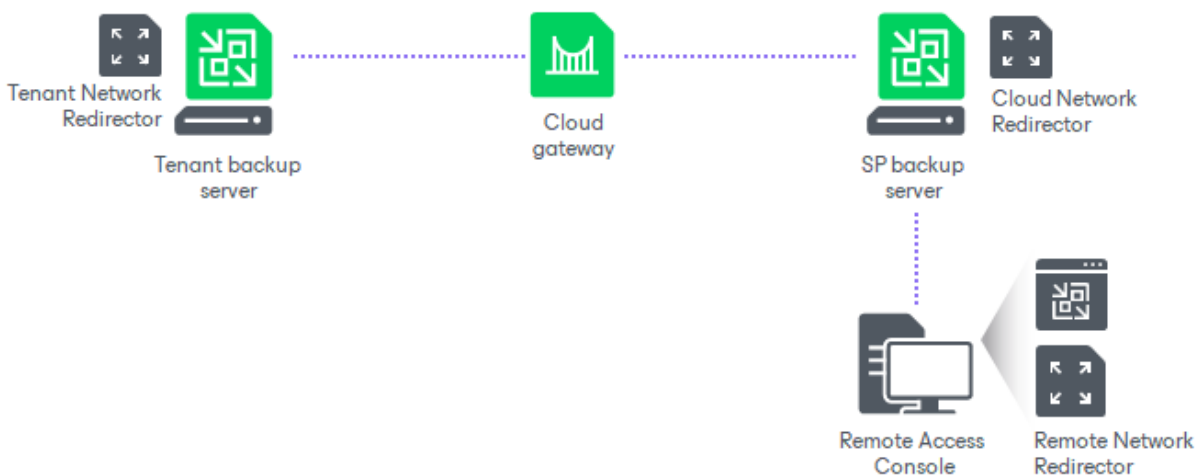
To open and keep a communication channel between the tenant backup server and SP backup infrastructure, Veeam Backup & Replication uses *network redirectors*. Network redirectors route requests between Veeam Backup & Replication components of the two parties allowing Veeam Backup & Replication to pass 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 or 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

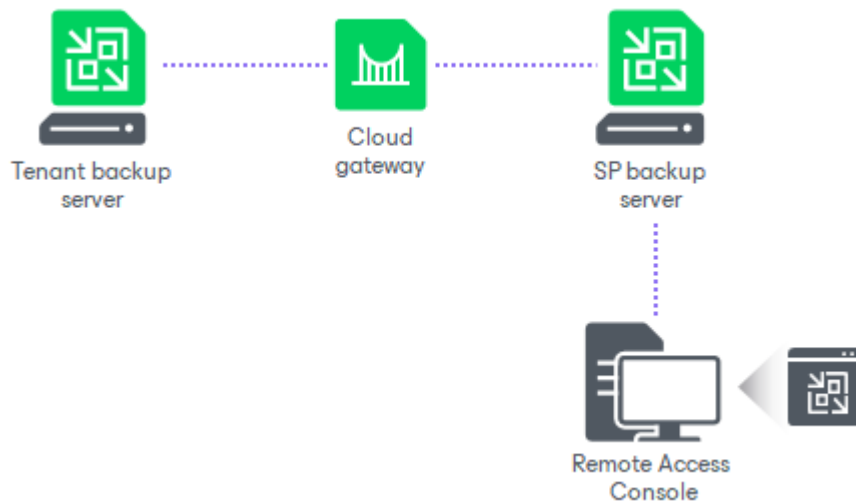
The process of establishing a connection to the SP and tenant backup servers with the Remote Access Console may require longer time depending on the distance between these components and quality of the network connection.

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

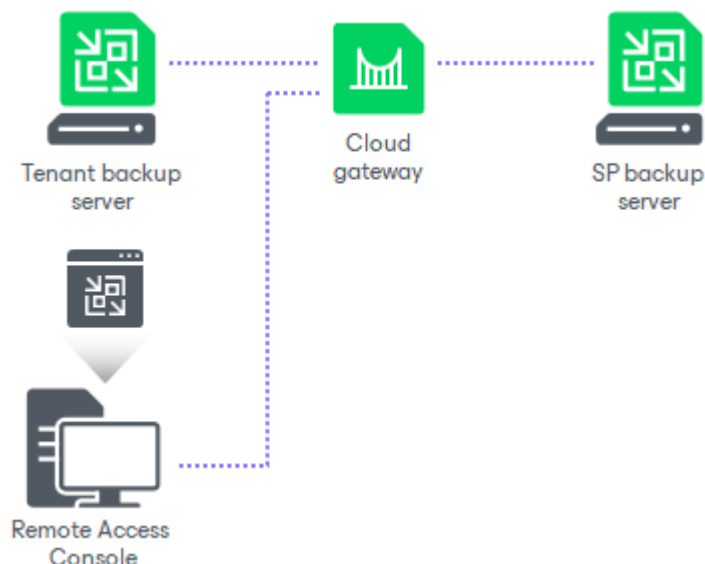
Veeam Backup & Replication offers the following scenarios of the Remote Access Console usage:

- 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 Veeam Backup & Replication settings if necessary. To learn more, see [Enabling Access to Cloud Gateway](#).



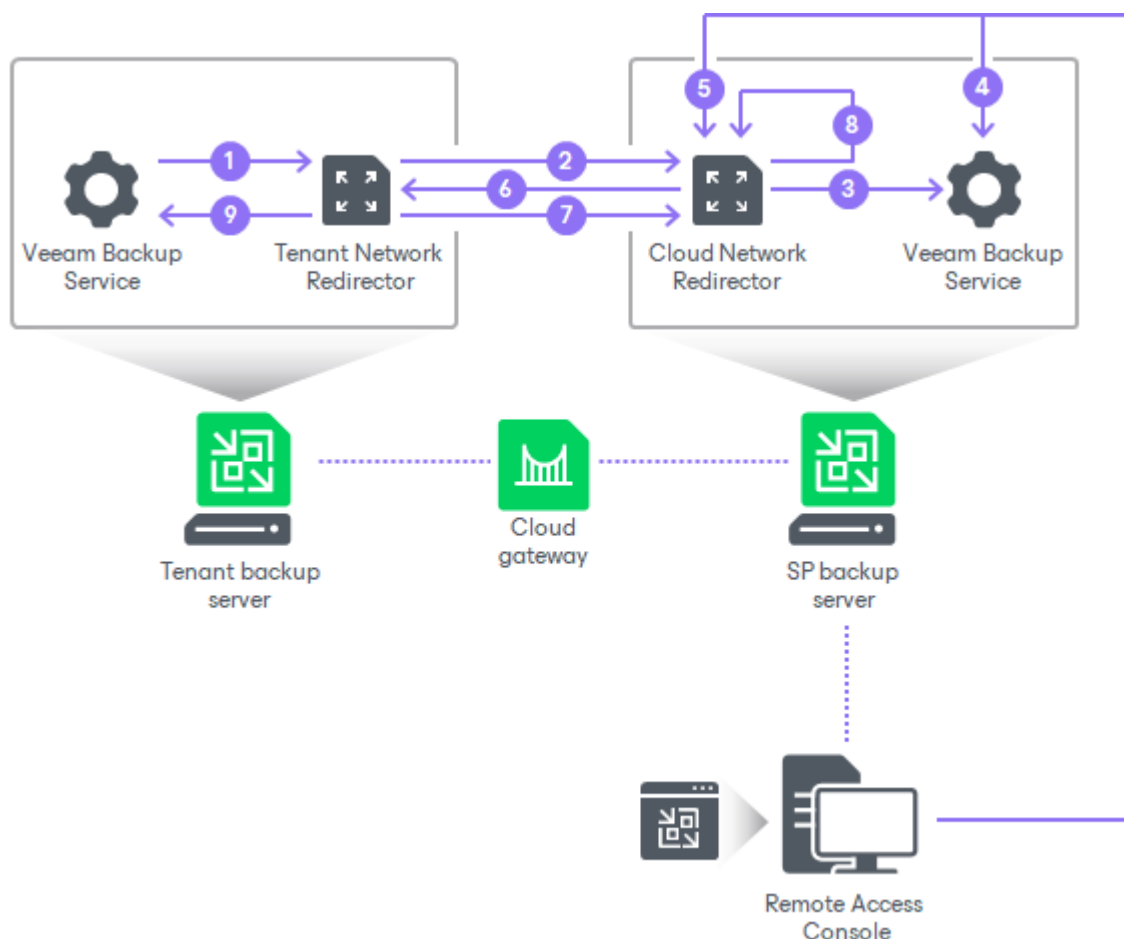
How Remote Access Console Works

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 connection to the tenant backup server with the Remote Access Console is not supported if multi-factor authentication (MFA) is enabled for the user account in the Veeam Backup & Replication console on that backup server.
- The SP cannot perform the following operations with the Remote Access Console:
 - Perform file-level restore
 - Perform application items restore with Veeam Explorers
 - 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 that runs the Microsoft Windows OS over the Remote Desktop Protocol. In this case, the SP can log on to the Microsoft Windows OS 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

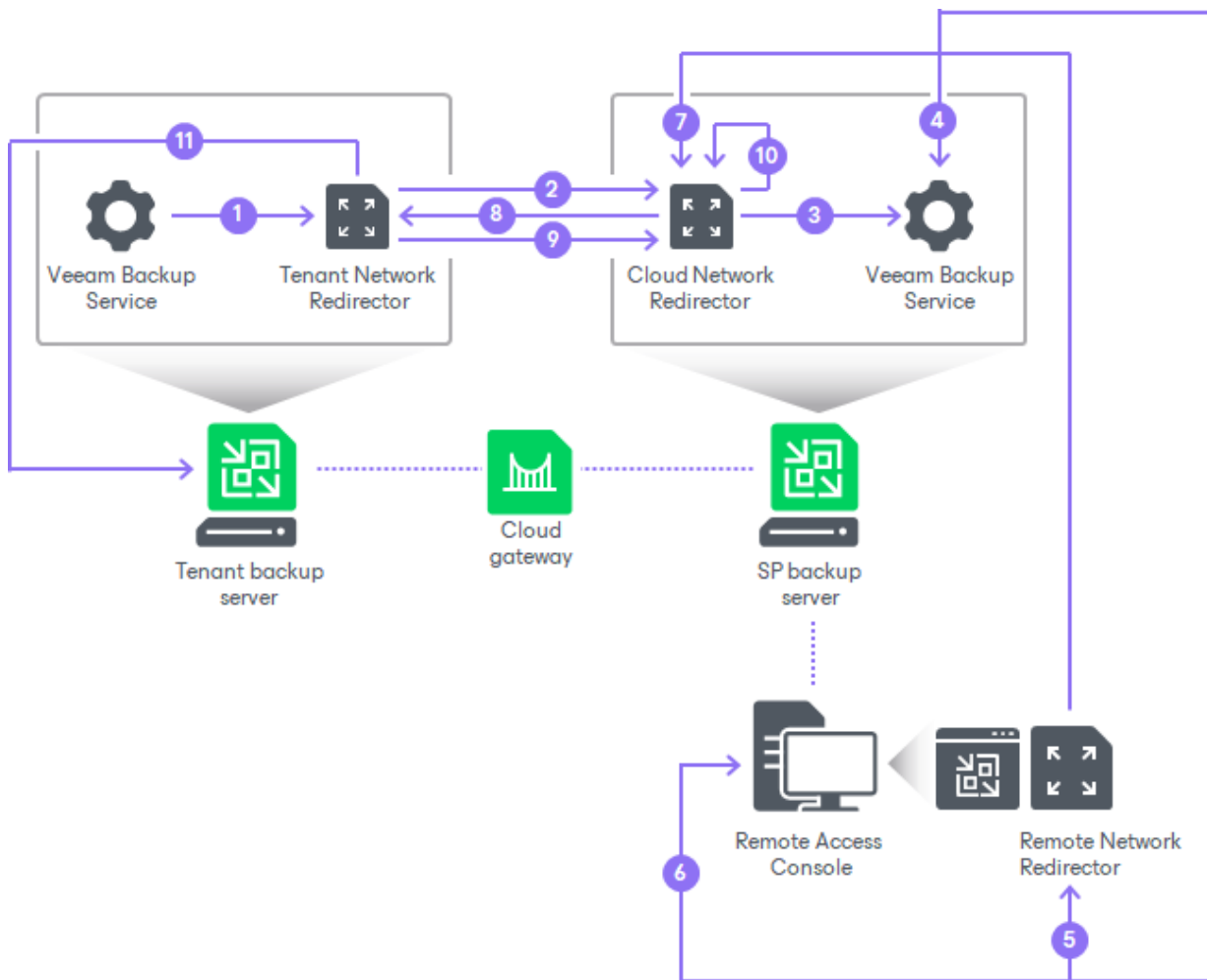
To open and keep a remote connection to the tenant backup server over the Remote Desktop Protocol, Veeam Backup & Replication components communicate in the following way:

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.

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.



Tenant Backup to Tape

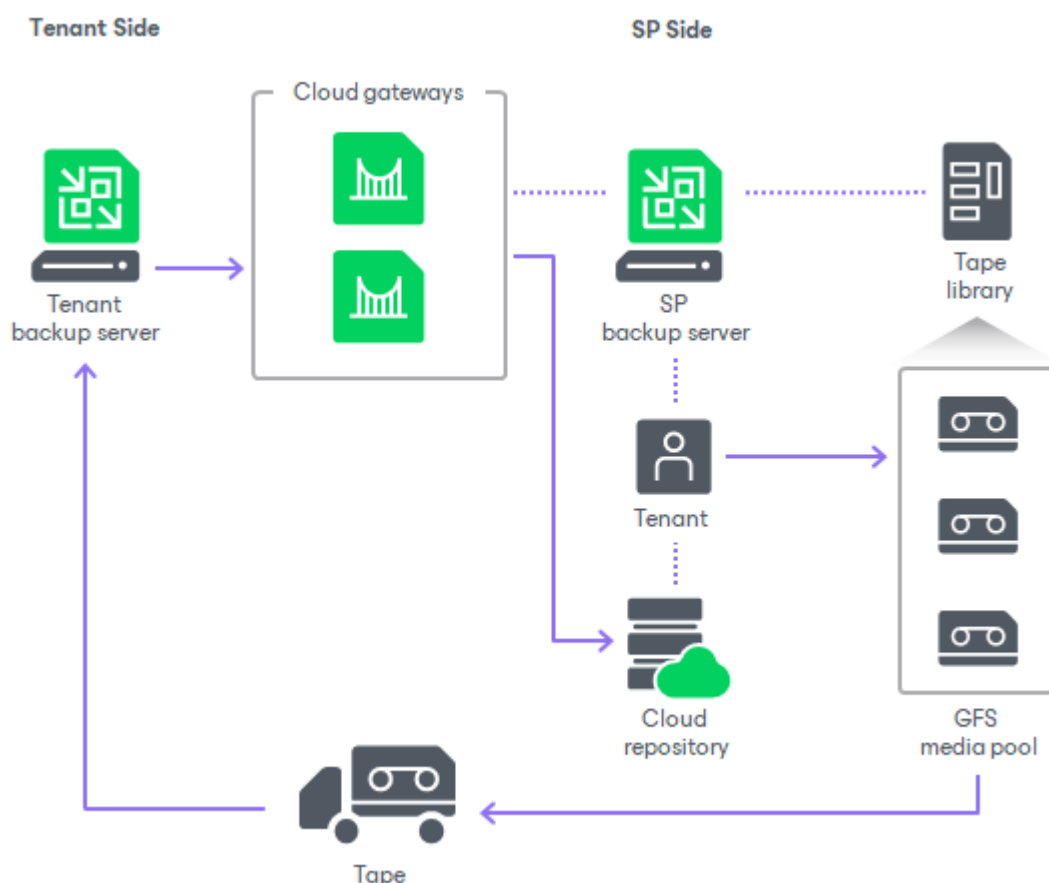
The SP can write backups created by a tenant in a cloud repository to a tape media. This allows the SP to offer additional tier of data protection to their tenants: the tenant will have one copy of the backed-up data in a cloud repository, and another copy of the backed-up on a tape media on the SP side. 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 Servers](#) 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 13. 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](#).

To enable IPv6 communication for previously added cloud gateways, the SP must reconfigure these cloud gateways using the Edit Cloud Gateway wizard.

- The SP and tenant can specify whether to use IPv6 addresses for network extension appliances. The following scenarios for are available:
 - Use an IPv4 interface
 - Use an IPv6 interface
 - 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 [Creating 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](#).

To enable IPv6 communication for previously deployed network extension appliances, the SP and tenant must redeploy network extension appliances on their sides.

NOTE

Only the /64 network mask is supported for failover with network extension appliances over the IPv6 protocol.

- 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.

- If IPv4/IPv6 dual stack networks are present in VMware Cloud Director, Veeam Backup & Replication displays a warning in the replication job or CDP policy session statistics. In this situation, the SP or tenant must manually import all organization VDC networks to all vApps in which the VM replicas and network extension appliance reside. Otherwise, failover to VMs in VMware Cloud Director may fail.

For details on how to add networks to a vApp, see [VMware Docs](#).

Keep in mind that after the networks are added to a vApp, Veeam Backup & Replication will continue displaying the warning. The SP can instruct Veeam Backup & Replication to suppress the warning with a registry key. For more information, contact [Veeam Customer Support](#).

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.

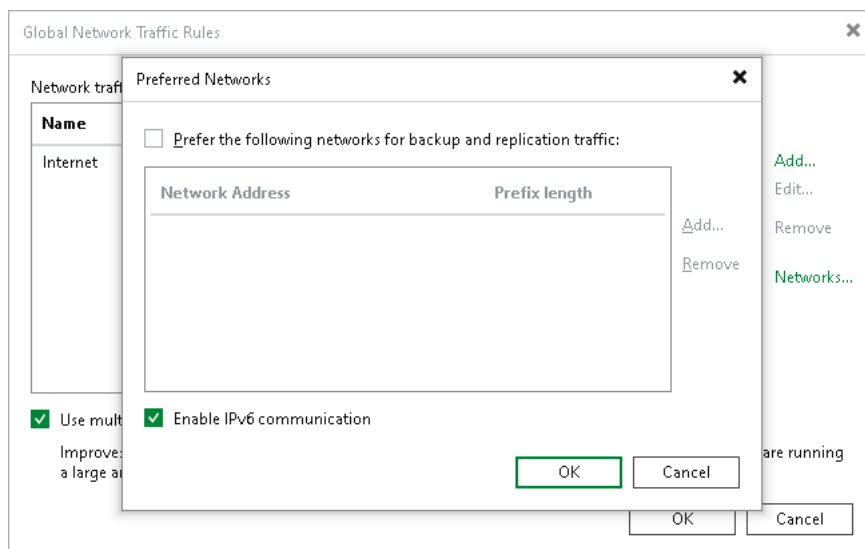
To enable IPv6 communication:

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 in this section.

Cloud Gateway

Specification	Requirement
Hardware	<i>CPU:</i> x86 or x86-64 processor with 8 cores (vCPUs) minimum. <i>Memory:</i> 16 GB RAM for up to 500 concurrent tenant tasks. <i>Disk Space:</i> 300 MB for Cloud Gateway service installation. Note: Disk requirements differ for cloud gateways deployed with the Veeam Infrastructure Appliance. For details, see the Veeam Infrastructure Appliance section in the Veeam Backup & Replication User Guide. <i>Network:</i> 1 Gbps LAN or faster.
OS	64-bit versions of the following Microsoft Windows operating systems are supported, including Core edition: • Microsoft Windows Server 2025 • Microsoft Windows Server 2022 • Microsoft Windows Server 2019 • Microsoft Windows Server 2016 • Microsoft Windows 11 (versions 22H2 - 25H2) • Microsoft Windows 10 (version 22H2) • Microsoft Windows 10 LTS (version LTSC 2021) 64-bit versions of the following Linux distributions are supported: • RHEL 9.6 • Veeam Infrastructure Appliance

SP Veeam Backup Server

To learn about system requirements for Veeam backup servers deployed on the SP 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	<i>Memory:</i> 16 GB RAM minimum.

Specification	Requirement
OS	64-bit versions of the following Microsoft Windows operating systems are supported: • Microsoft Windows Server 2025 • Microsoft Windows Server 2022 • Microsoft Windows Server 2019 • Microsoft Windows Server 2016 • Microsoft Windows 11 (versions 22H2 – 25H2) • Microsoft Windows 10 (version 22H2) • Microsoft Windows 10 LTS (version LTSC 2021)

NOTE

Linux distributions are not supported for the Veeam backup servers deployed on the SP side.

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 17.x (PostgreSQL 17.6 is included in the Veeam Backup & Replication 13 setup, but we strongly recommend to download and install the latest PostgreSQL 17.x version) • PostgreSQL 15.x • PostgreSQL 14.x The following versions of Microsoft SQL Server are supported: • Microsoft SQL Server 2025 Standard or Enterprise Edition • 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 high loads (up to 1,000 parallel tenant tasks), consider performance tuning. To learn more, see [this Veeam KB article](#).

Tenant Veeam Backup Server

To learn about system requirements for Veeam backup servers deployed on the 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 tenant backup server must meet the following requirements:

Specification	Requirement
OS	64-bit versions of the following Microsoft Windows operating systems are supported: • Microsoft Windows Server 2025 • Microsoft Windows Server 2022 • Microsoft Windows Server 2019 • Microsoft Windows Server 2016 • Microsoft Windows 11 (versions 22H2 - 25H2) • Microsoft Windows 10 (version 22H2) • Microsoft Windows 10 LTS (version LTSC 2021) For Linux-based server, Veeam Software Appliance ISO deployment to a virtual machine is supported for all hypervisors for which Veeam offers host-based VM backup functionality. For details, see Supported Platforms, Applications and Workloads.

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.

Backup Proxy

To learn about system requirements for backup proxies used in the Veeam Cloud Connect infrastructure, 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.

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.

In this section, you can also find diagrams illustrating the interaction between Veeam Cloud Connect components and used ports in following scenarios:

- [Ports in Backup Scenarios](#)
- [Ports in Snapshot-Based Replication Scenarios](#)
- [Ports in CDP Replication Scenarios](#)
- [Ports in Universal CDP Replication Scenarios](#)
- [Ports in Remote Access Console Scenarios](#)

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 redirectors 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.
		TCP	6185, 33034, 33035	Ports on the SP backup server used for communication with the Veeam CDP Coordinator Service. For the complete list of ports used in the CDP infrastructure, see the CDP Components section in the Veeam Backup & Replication User Guide.

From	To	Protocol	Port	Notes
	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.
	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.
	SP CDP proxy	TCP	33032, 33033	Default ports used as transmission channels to the target CDP proxy. For the complete list of ports used in the CDP infrastructure, see the CDP Components section in the Veeam Backup & Replication User Guide.

From	To	Protocol	Port	Notes
	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 IP network. For example, a tenant <i>Tenant1</i> replicates VMs that are connected to 3 IP networks. In the Veeam Cloud Connect infrastructure, the SP deployed a network extension appliance for <i>Tenant1</i>. 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.
	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	135, 445	Ports used for deploying Veeam Backup & Replication components.
		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.

From	To	Protocol	Port	Notes
		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.
	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.
	SP backup repository (or gateway server)	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.
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

From	To	Protocol	Port	Notes
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 Veeam Backup & Replication console	Cloud gateway	TCP	6180	Port used by the Veeam Software Appliance (VSA) to connect to the cloud gateway 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 documentation.
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.

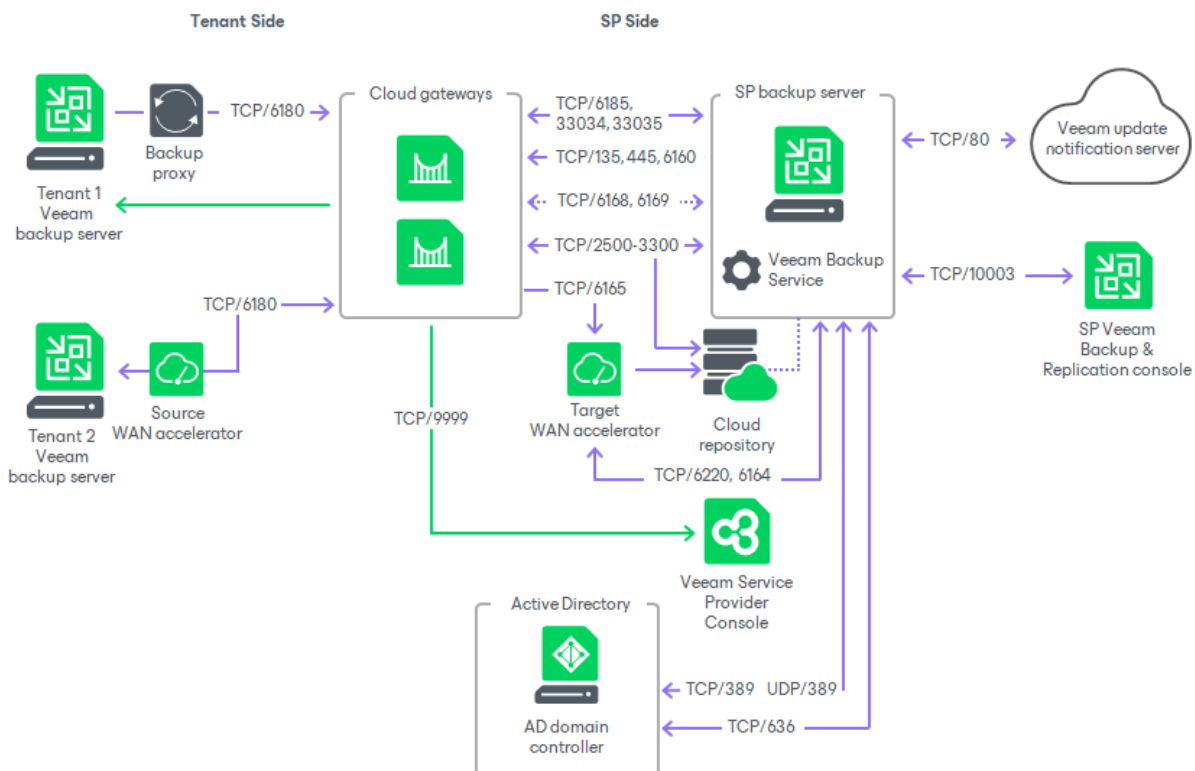
From	To	Protocol	Port	Notes
	Veeam License Update Server (autolk.veeam.com)	TCP	443	Default port used for license auto-update.
	Backup server	TCP	10003	Port used for communication with the Veeam Backup Service (locally on the backup server).
Provider-side network extension appliance	Cloud gateway	UDP	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 IP network. For example, a tenant <i>Tenant1</i> replicates VMs that are connected to 3 IP networks. In the Veeam Cloud Connect infrastructure, the SP deployed a network extension appliance for <i>Tenant1</i>. 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 and replication 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 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 redirectors.
		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 redirectors.
	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.
Tenant Hyper-V server	Cloud gateway	TCP and UDP	6180	Port used for data transport during full VM restore.

From	To	Protocol	Port	Notes
Veeam Agent computer (Microsoft Windows, Linux, macOS)	Cloud gateway	TCP	6180	Port on the cloud gateway used to transport Veeam Agent data to the cloud repository.
	Certificate Revocation Lists	TCP	80 or 443 (most popular)	Veeam Agent computer 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

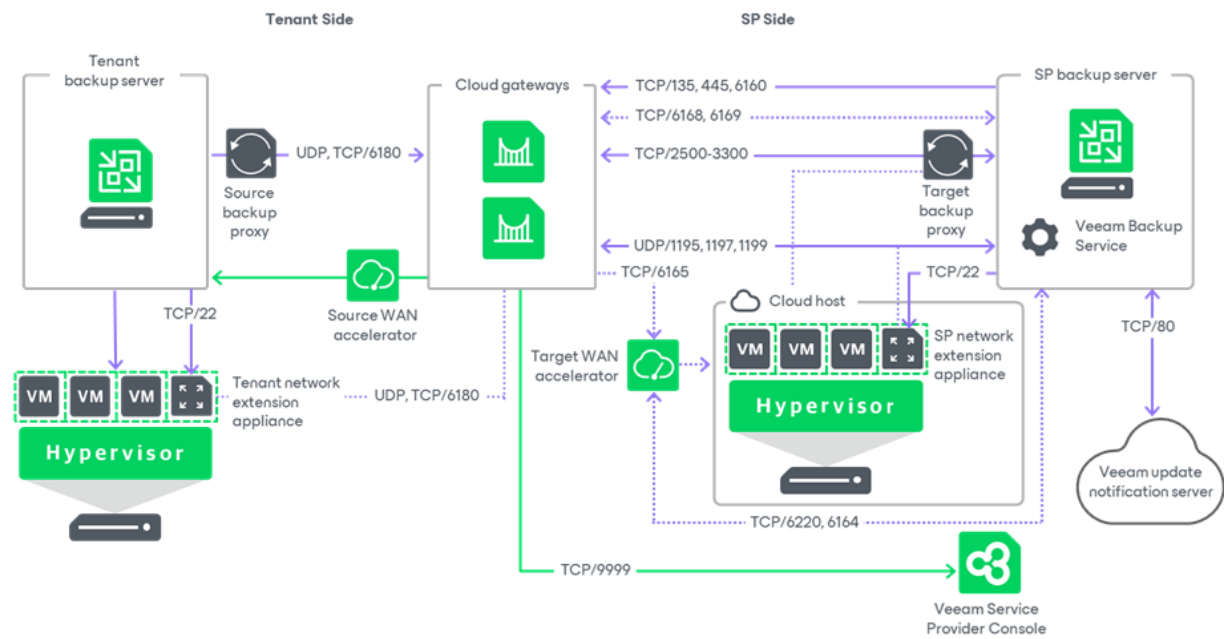
Ports in Backup Scenarios

The following diagram illustrates the interaction between Veeam Cloud Connect components and used ports in backup scenarios.



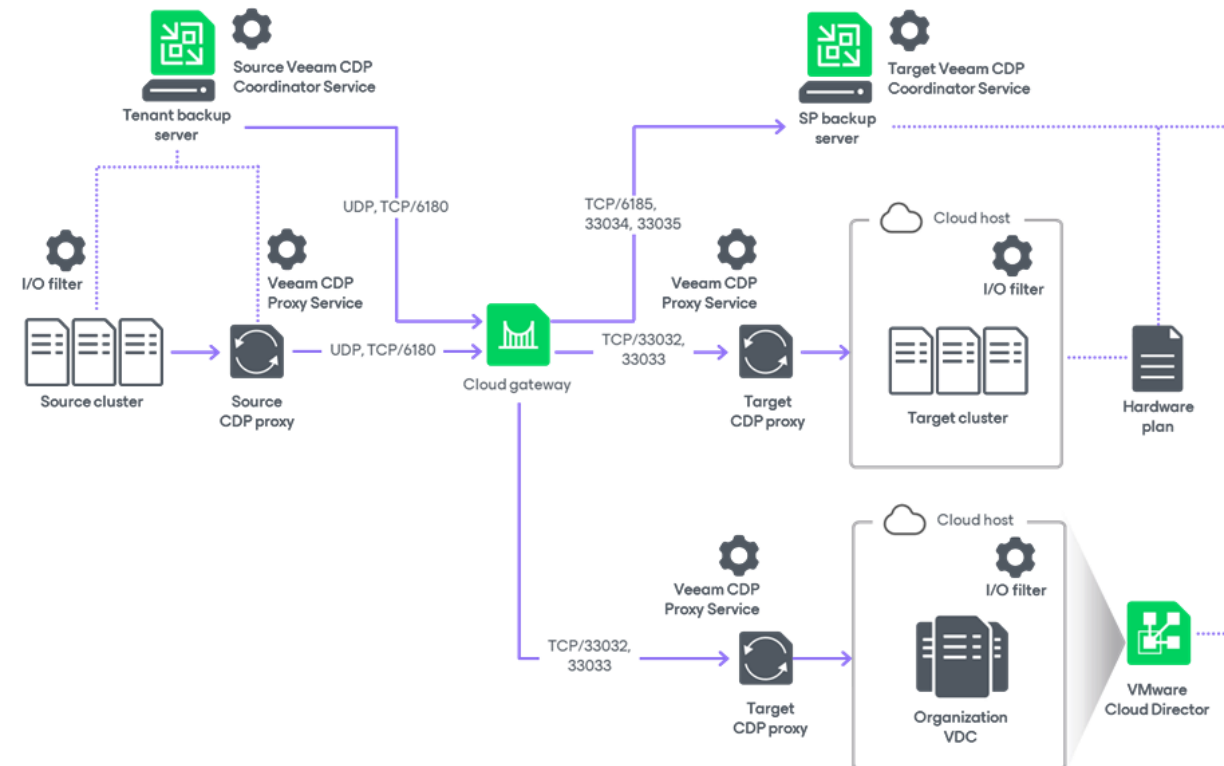
Ports in Snapshot-Based Replication Scenarios

The following diagram illustrates the interaction between Veeam Cloud Connect components and used ports in snapshot-based replication scenarios.



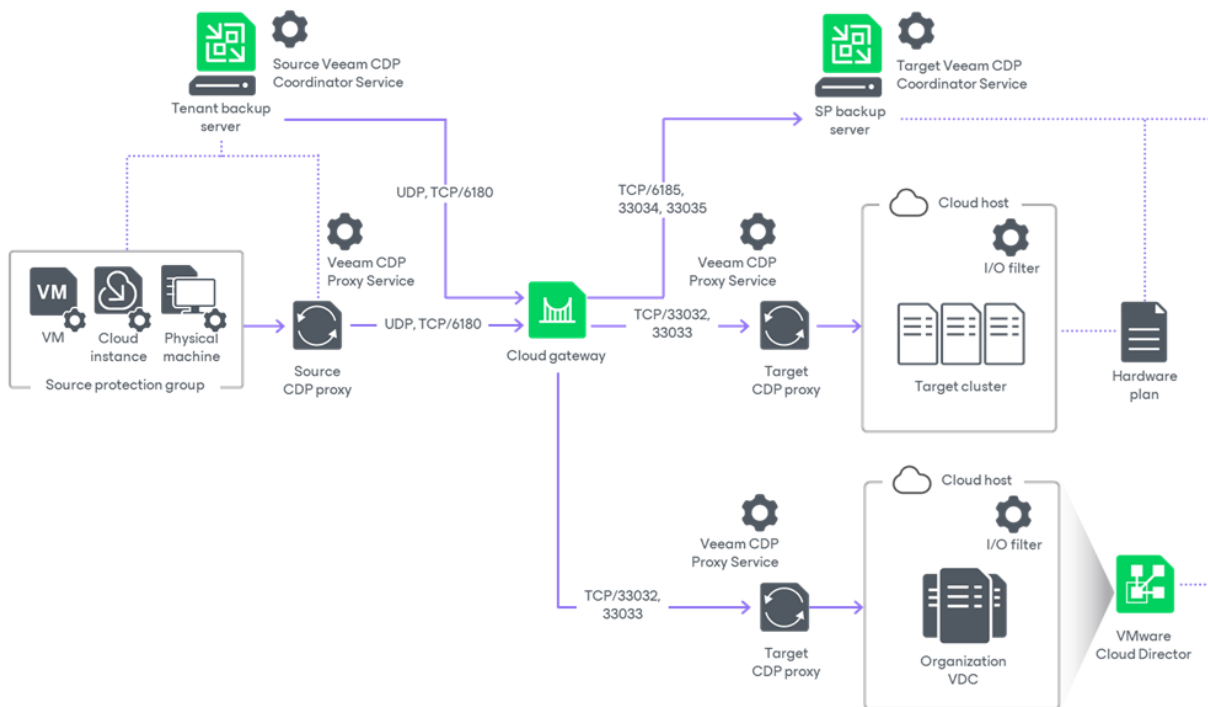
Ports in CDP Scenarios

The following diagram illustrates the interaction between Veeam Cloud Connect components and used ports in CDP replication scenarios.



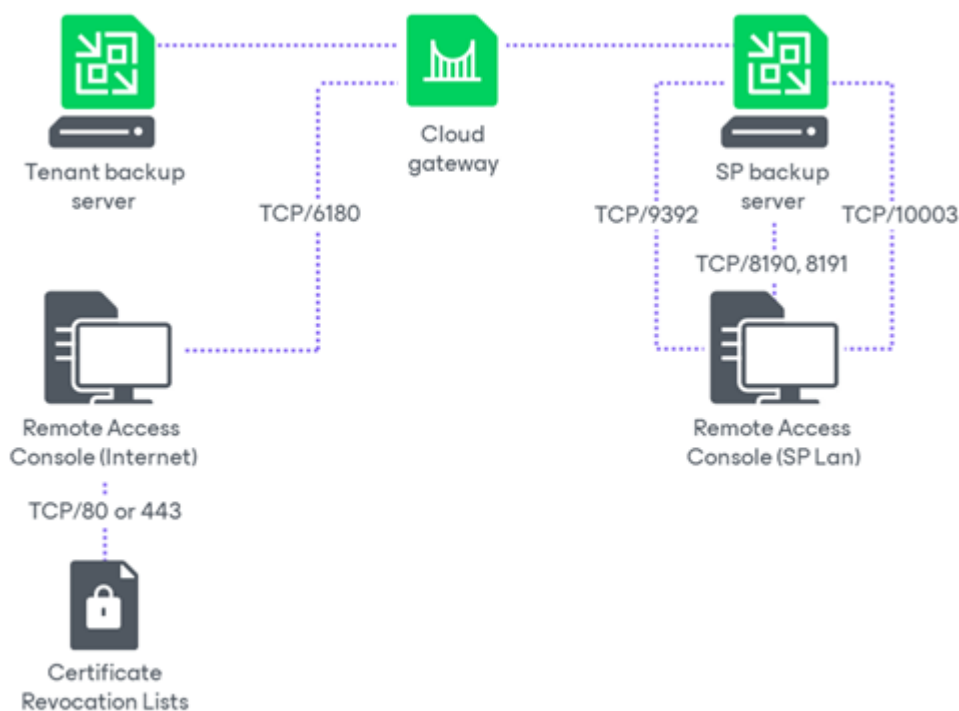
Ports in Universal CDP Scenarios

The following diagram illustrates the interaction between Veeam Cloud Connect components and used ports in Universal CDP replication scenarios.



Ports in Remote Access Console Scenarios

The following diagram illustrates the interaction between Veeam Cloud Connect components and used ports in the Remote Access Console scenarios.



Veeam Product Versions

The 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 can run the same or later version of Veeam Backup & Replication than the tenant Veeam backup server. The SP backup server cannot run an earlier version of Veeam Backup & Replication than the tenant backup server.

This applies to major product versions. Within Veeam Backup & Replication version 13, the SP and tenant can use a product build 13.0.1 or later. Version 13.1 is backward compatible with version 13.0.1. It is recommended, however, that the SP and tenant install latest hotfixes and updates on the backup server.

- Veeam Backup & Replication 13.1 running on the SP backup server is compatible with the following versions of Veeam products running on the tenant side:
 - Veeam Backup & Replication 12.3.2 (starting from 12.3.2.3617) and 13.0.1 or later

NOTE

Veeam Backup & Replication 13.0.0 is not supported.

- Veeam Agent for Microsoft Windows 6.3.2 and later
- Veeam Agent for Linux 6.3.2 and later
- Veeam Agent for Mac 2.3.1 and later

If the SP or tenant plan to upgrade Veeam Backup & Replication to a later major product version, 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 13 on Windows](#) section in the Veeam Backup & Replication User Guide.
2. After Veeam Backup & Replication on the SP side is upgraded, the tenant can perform the upgrade procedure on the tenant backup server.

The sequence required for the upgrade to a later major product version does not apply to bug fixes and cumulative patch updates. In such scenarios, the update process can start on either the SP side or the tenant side.

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.

For installations with high loads (up to 1000 parallel tenant tasks), it is recommended that all tenants run the latest version of Veeam Backup & Replication and Veeam Agents.

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 specifics and 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.
- Veeam Backup & Replication does not support the use of backup repositories with rotated drives as cloud repositories.
- 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 Proxmox VE, restore to oVirt KVM, restore to Microsoft Azure and Amazon EC2 from backups in the cloud repository are not supported on the tenant side.

If Nutanix AHV Plug-in is installed and a Nutanix AHV cluster is added in Veeam Backup & Replication, the tenant can perform instant recovery to Nutanix AHV from backups that reside in the cloud repository. For more information, see the [Instant Recovery](#) section in the Veeam Backup for Nutanix AHV User Guide.

Some restore operations are available on the SP side only, including Instant Recovery from VM backups and Veeam Agent backups, restore to Microsoft Azure and restore to Amazon EC2. To learn more, see [Restoring Data from Tenant Backups](#).

- Removed GFS restore points could remain displayed in the Veeam backup console 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.
- The *Forget* and *Remove from disk* operations for restore points created by tenant backup copy jobs are unavailable in the Veeam backup console. The SP can find and remove missing restore points using Veeam PowerShell cmdlets on the SP side only. For more information, see [this Veeam KB article](#).
- 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.
- A machine that runs the tenant Veeam backup console must have access to the cloud gateway over the network. For example, connection to the cloud gateway is required when the tenant performs file-level restore using the backup console installed on a different machine than the tenant backup server.
- For backup copies of Proxmox VMs, Veeam Cloud Connect supports only File-Level Restore.

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 and associated backup 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 120 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 15-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 120.

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 specifics and 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 10.6.
- 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 [Considerations 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.

- To use the CDP functionality in the Veeam Cloud Connect environment, both the SP and tenant must run Veeam Backup & Replication version 12 or later.
- 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:
 - On the SP side, the minimum required ESXi version is 7.0.
 - On the tenant side, the minimum required ESXi version is 6.5 Update 2.
 - You must not use the same vApp as a target for both a snapshot-based replication job and a CDP policy.
 - 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.

Consider that the *Any* storage policy is not supported for CDP. If Organization VDC has *Any* as its default storage policy, Veeam Backup & Replication will not automatically create a CDP-ready policy based on it. In this case, the SP must create a CDP-ready policy and add it to the Organization VDC manually.

If a CDP-ready policy exists in VMware vSphere, and it has the same settings as the *Default* VDC storage policy, Veeam Backup & Replication will import it to VMware Cloud Director and use it for CDP.

If the SP creates new storage policies, they must make sure to configure a replication provider as well as the tags they need. The provider name is *veecdp*. For details, see [VMware Docs](#). After that, this policy can be used as a CDP replication target.

Keep in mind that Veeam Backup & Replication should not use the existing storage policies that are applied to any VMs because Veeam Backup & Replication installs I/O filters on all VMs on this policy. This includes VMs that are out-of-scope of CDP. This can cause problems when removing I/O filters.

- CDP replication of encrypted VMs is not supported.
- CDP replication to a target datastore under a VM Encryption Policy is supported.

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 documentation](#).

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 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 in 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 SPs to back up and replicate VMs with the jobs configured on the SP Veeam backup server.

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 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

SPs and tenants can use a *Rental Veeam Backup & Replication license* within the Veeam Cloud Connect infrastructure. This section describes the details of this license that apply to Veeam Cloud Connect. To learn more on how Rental licensing works in general, including details for other Veeam products, see [Veeam Rental Licensing and Usage Reporting Guide](#).

In the Veeam Cloud Connect infrastructure, the main usage scenario for the *Rental Veeam Backup & Replication license* is the [MSP Backup](#) scenario. In this scenario, the SP controls the Veeam Backup & Replication infrastructure on the tenant side and manages tenant machines. As part of this process, the SP installs a Rental Veeam Backup & Replication license on the tenant Veeam backup server.

TIP

The SP can also use a *Rental Veeam Backup & Replication license* when using the Veeam Backup & Replication server together with Veeam products for public cloud backup to protect shared or private cloud environments.

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.

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.

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.

For more information on new workloads in the context of Veeam Rental Licensing, see the [Delayed License Consumption for New Workloads and Users](#) in the Veeam Rental Licensing and Usage Reporting Guide.

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).

IMPORTANT

Although it is possible to distribute one rental license to multiple backup servers, this scenario is not recommended. Instead, the SP can issue the necessary number of licenses at any time. For more information, see the [Using Veeam Service Provider Console](#) section and the [Using Veeam Service Provider Console](#) section in the Veeam Rental Licensing and Usage Reporting Guide.

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.

License Information

License

Points

License Information

Status	Valid
Type	Rental
Edition	Enterprise Plus
Package	Backup
Support ID	02067762
Licensed to	Veeam Software Group GmbH
Cloud Connect Provider	Yes

Points

Points	100 (0 used + 22 new)
Expiration date	12.12.2026 (403 days left)

Install

Remove

Update Now

Create Report...

Renew...

☐ Update license automatically (enables usage reporting)

☐ Receive proactive support (enables diagnostic data sharing)

Proactive technical support services require sharing anonymized backup infrastructure telemetry with Veeam. For more information on what is being shared, please refer to the User Guide.

Close

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.

License Information

License

Points

License Information

Status	Valid
Type	Rental
Edition	Enterprise Plus
Package	Backup
Support ID	02067762
Licensed to	Veeam Software Group GmbH
Cloud Connect Provider	Yes

Points

Points	100 (0 used + 22 new)
Expiration date	12.12.2026 (403 days left)

[Install](#)

[Remove](#)

[Update Now](#)

[Create Report...](#)

[Renew...](#)

☒ Update license automatically (enables usage reporting)

☒ Receive proactive support (enables diagnostic data sharing)

Proactive technical support services require sharing anonymized backup infrastructure telemetry with Veeam. For more information on what is being shared, please refer to the User Guide.

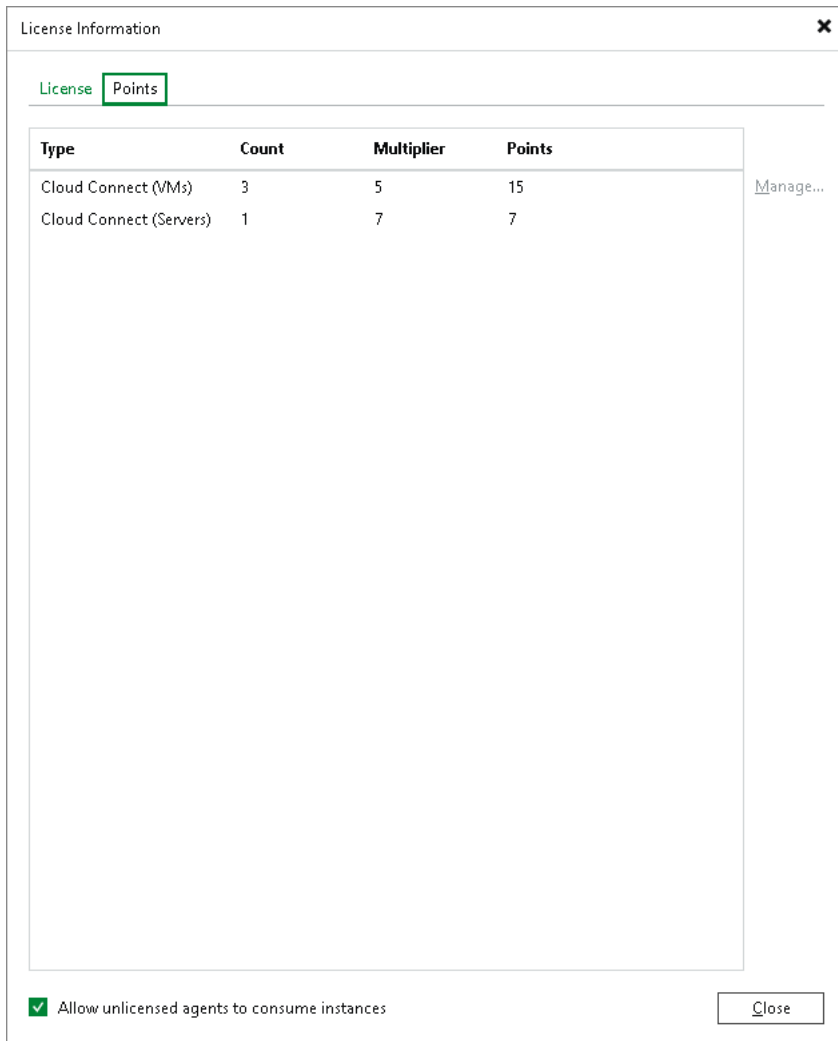
Close

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:
 - *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 in 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 screenshot shows the 'License Information' window with the 'Points' tab selected. It contains a table with the following data:

Type	Count	Multiplier	Points
Cloud Connect (VMs)	3	5	15
Cloud Connect (Servers)	1	7	7

At the bottom of the window, there is a checkbox labeled 'Allow unlicensed agents to consume instances' which is checked, and a 'Close' button.

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 Veeam Backup & Replication User Guide.

Viewing 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:
 - [/cloud/tenants/{ID}](#)
 - [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 v3.6, see the [Get All Companies](#) and [Get License Usage by All Organizations](#) 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 Tenant Account Information](#).

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 Tenant Account Information](#).

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**.

TIP

The SP can also use Veeam PowerShell to reset the tenant machine count. To learn more, see the [Reset-VBRCloudTenant](#) section in the Veeam PowerShell Reference.

License Usage Reporting

The SP must periodically submit a license usage report. There are different mechanisms to do so. 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 on how Rental licensing works for various workloads within Veeam Platform, how to manage licenses using Veeam Service Provider Console and VCSP Pulse, and how to collect and report the license usage, see the [Veeam Rental Licensing and Usage Reporting Guide](#).

Veeam Backup & Replication also allows the SP to submit license usage reports from the Veeam backup console. This section provides a detailed description of reporting mechanisms offered by Veeam Backup & Replication.

The SP submits a license usage report 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 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

If the same *Rental Veeam Backup & Replication license* is installed on multiple tenant backup servers and the SP does not use the Veeam Service Provider Console to manage the Veeam backup infrastructure, the SP must report license usage for all Veeam Backup & Replication servers in one of the following ways:

- The SP must send individual license usage reports from each backup server separately using the Veeam Backup & Replication console.
- For tenant backup servers that are connected to the Veeam Backup Enterprise Manager, a single report containing license usage information from each backup server is generated on the Veeam Backup Enterprise Manager server. In this case, the SP must send information about the license usage information from the Veeam Backup Enterprise Manager.
- Auto-Populate and Auto-Submit (APAS) reports can be used. To do that, the SP must properly manage license keys and review the report before it is submitted. To learn more, see the [Auto-Populate and Auto-Submit Usage Reporting](#) section in the 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*, Veeam Backup & Replication performs license usage reporting 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`.

If the SP configured email notification settings, Veeam Backup & Replication will also send the report to an email address specified there. To learn more, see the [Configuring Global Email Notification Settings](#) section in the Veeam Backup & Replication User Guide.

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.

The notification window appears on the first day of the month.

NOTE

If the SP uses Veeam Service Provider Console to manage the Veeam backup infrastructure, and the Automatic Report Approval option is enabled in Veeam Service Provider Console, Veeam Backup & Replication does not display the notification window. To learn more, see the [Enabling Automatic Report Approval](#) section in the Guide for Service Providers.

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 does not send the report, on the third 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*, Veeam Backup & Replication performs license usage reporting 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`.

If the SP configured email notification settings, Veeam Backup & Replication will also send the report to an email address specified there. To learn more, see the [Configuring Global Email Notification Settings](#) section in the Veeam Backup & Replication User Guide.

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.

NOTE

If the SP uses Veeam Service Provider Console to manage the Veeam backup infrastructure, the notification window in the Veeam Backup & Replication console on the first day of the month will not be displayed.

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](#).

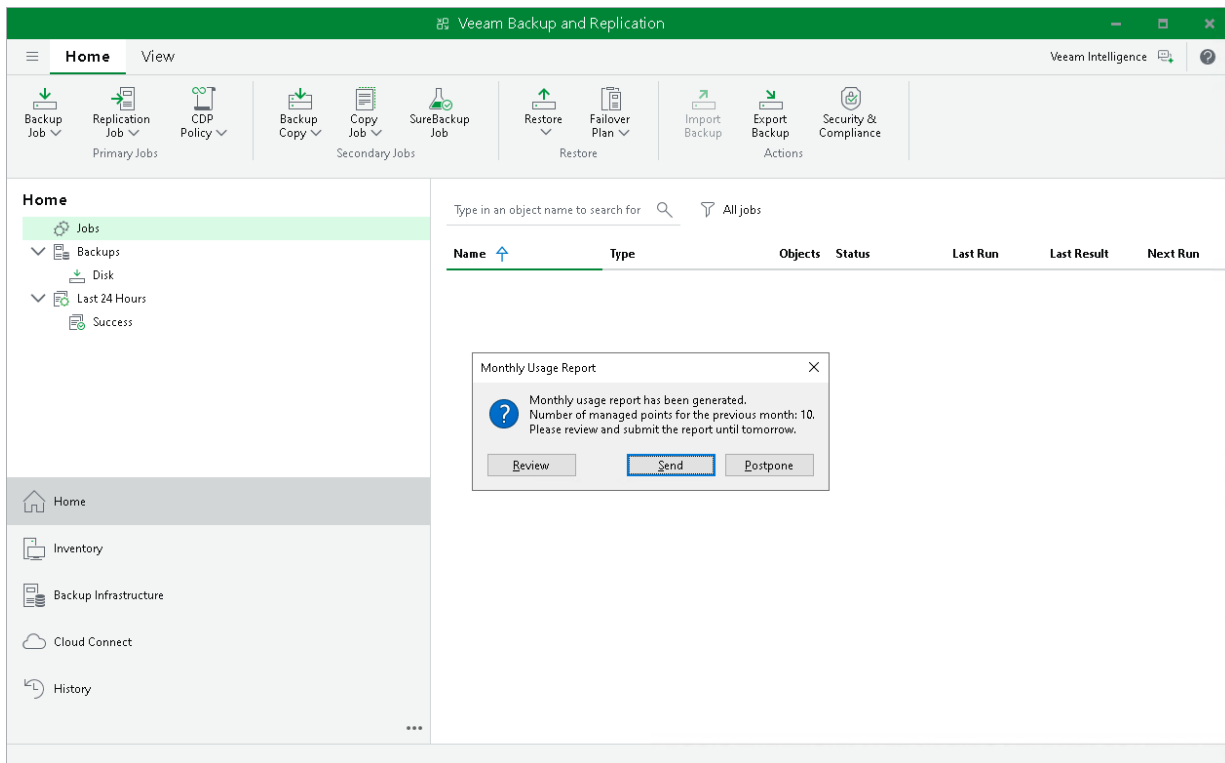
Submitting License Usage Report

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.
- If the SP uses Veeam Service Provider Console to manage the Veeam backup infrastructure, the notification window in the Veeam Backup & Replication console on the first day of the month will not be displayed.



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:
 - [For automatic reporting] In the notification window informing that the report is generated, click **Review**.
 - [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.
 - 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.
 - 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:
 - [For automatic reporting] In the notification window informing that the report is generated, click **Review**.
 - [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.

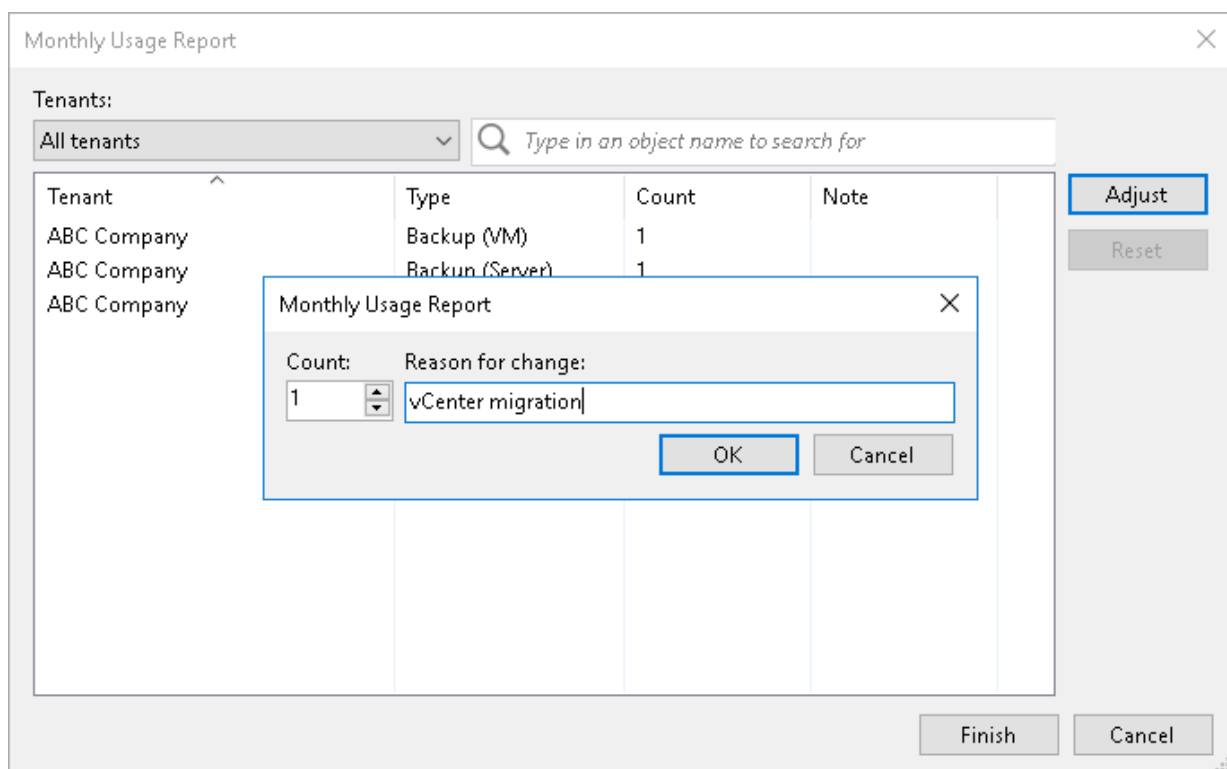
To adjust a report:

1. Open the **Monthly Usage Report** window:
 - [For automatic reporting] In the notification window informing that the report is generated, click **Review**.
 - [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.

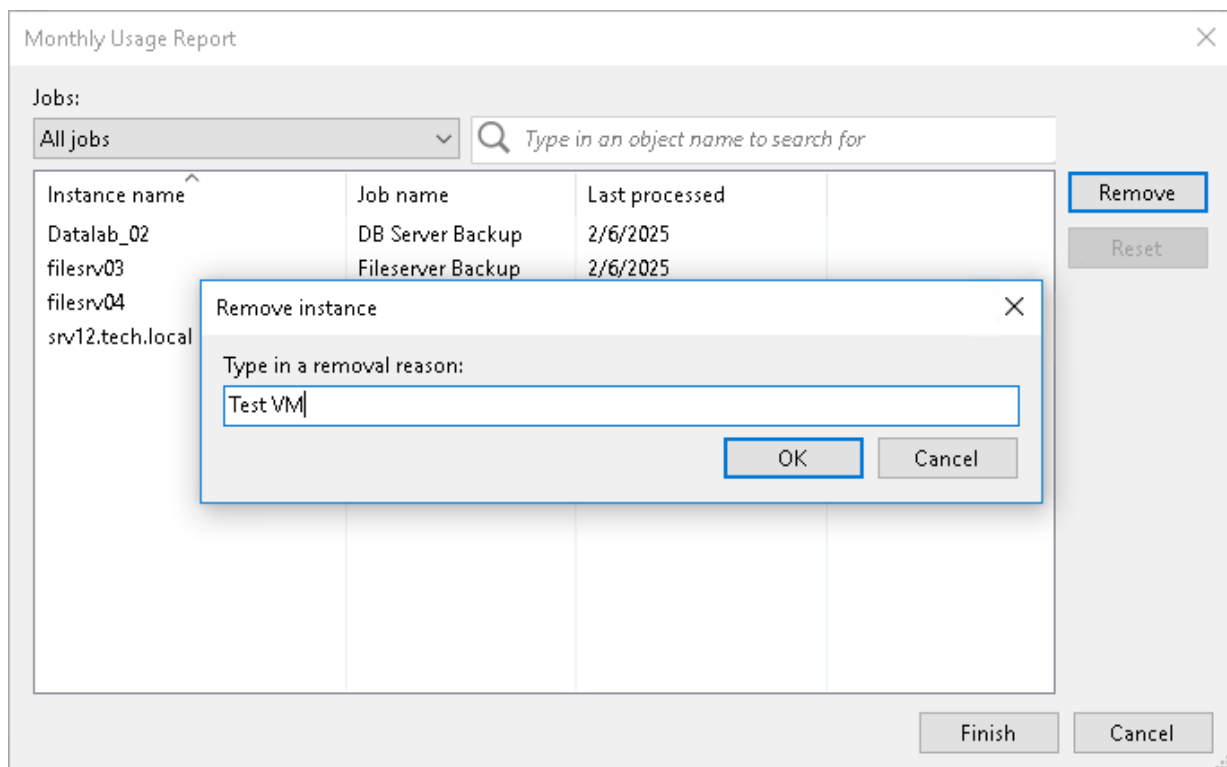
To adjust a report:

1. Open the **Monthly Usage Report** window:
 - [For automatic reporting] In the notification window informing that the report is generated, click **Review**.
 - [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**.



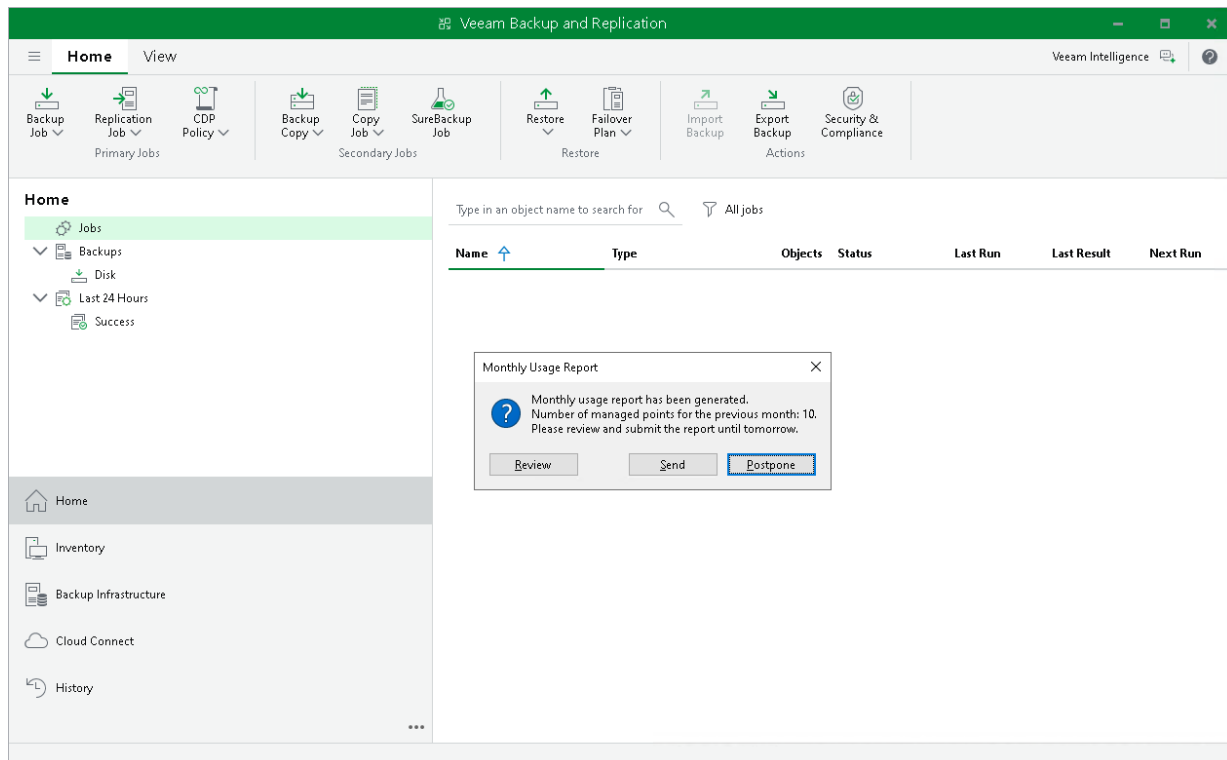
Postponing License Usage Report Review

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 third 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.

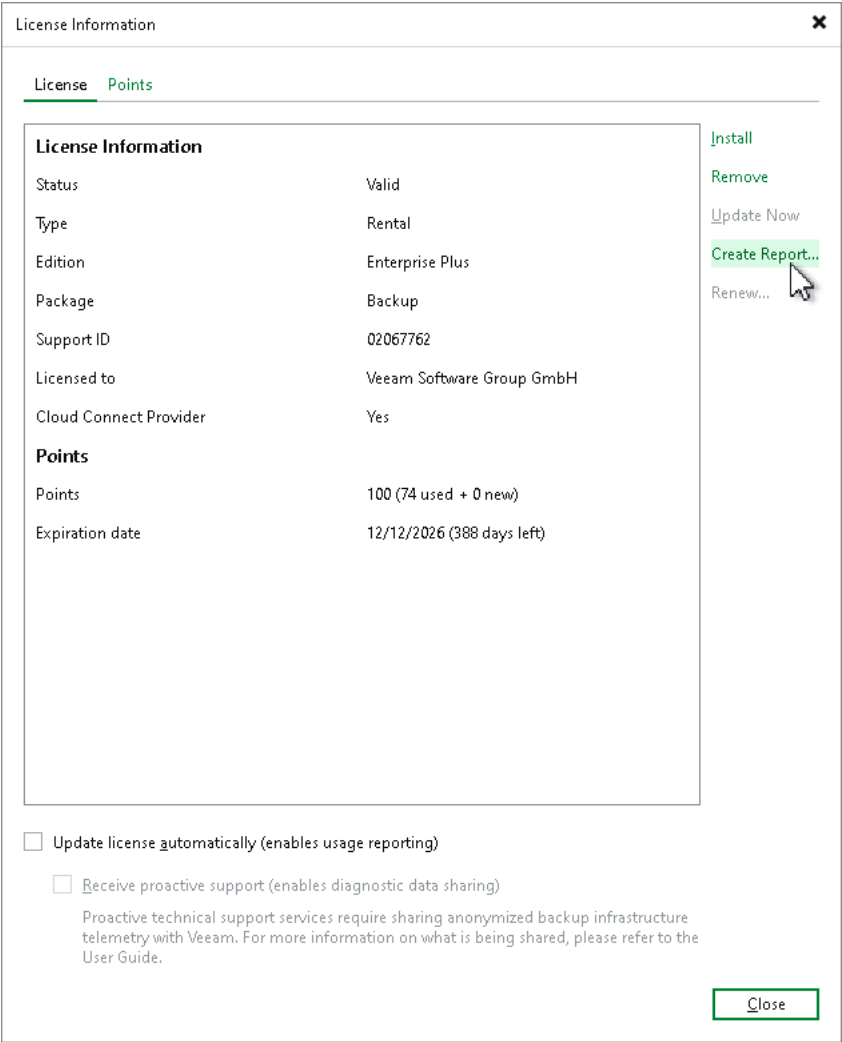
The report displays information about current license usage in the similar way as the monthly usage report. The report contains the following data:

- 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 Guide for Service Providers 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 guide describes main tasks that the SP must take to set up the necessary infrastructure and manage it.

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.](#)
- [Create tenant accounts.](#)
- [Configure target WAN accelerators.](#)

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:
 - Backup repositories that will be used as cloud repositories
 - Managed servers that will be used for configuring replication resources (cloud hosts)
 - Cloud gateways
 - [Optional] Target WAN accelerators
3. If the SP plans to use Veeam Backup for Microsoft 365 to provide Mail Backup as a Service to tenants, the SP must install Veeam Backup for Microsoft 365 on the SP backup server. For further information, see the [For Service Providers](#) section of the Veeam Backup for Microsoft 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 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 the 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

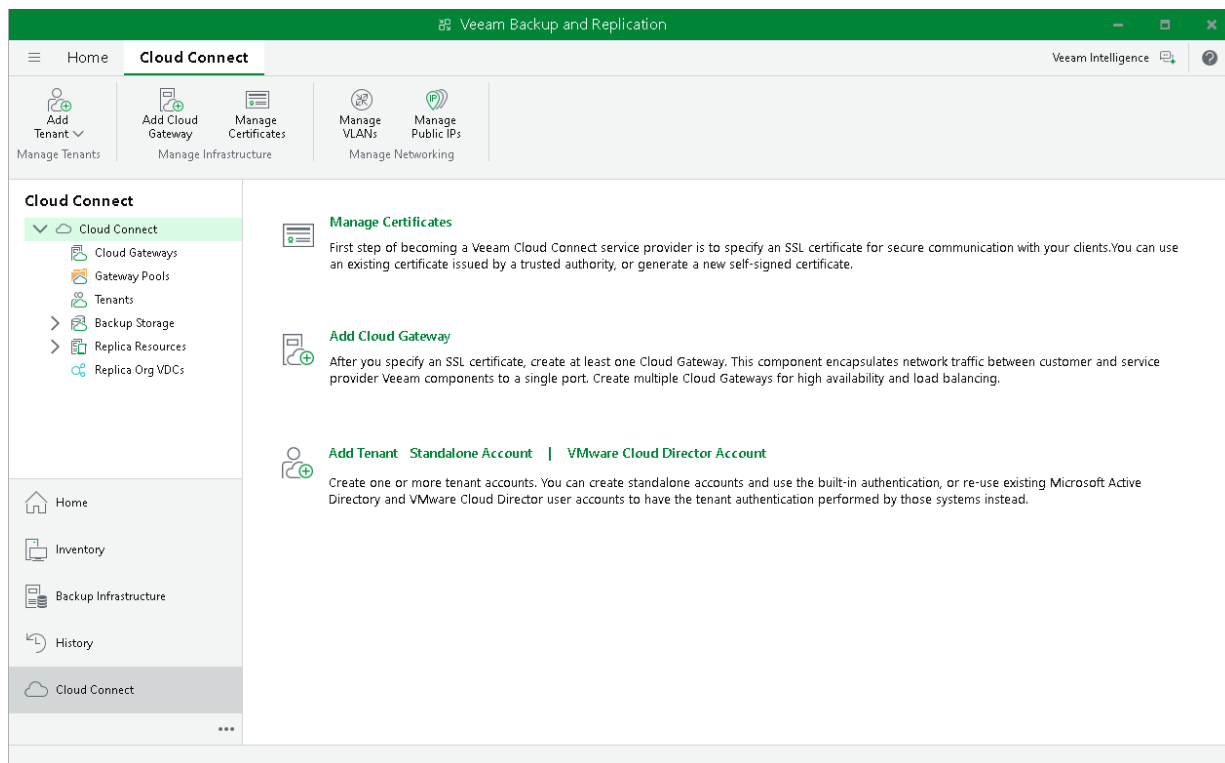
If you use a self-signed TLS certificate generated by Veeam Backup & Replication, you do not need to take any additional actions to deploy the TLS certificate on the tenants side. When the tenant adds the SP to Veeam Backup & Replication, a matching TLS certificate with a public key is installed on the 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 a new certificate**.

The screenshot shows a 'Manage Certificate' dialog box with a sidebar on the left containing 'Certificate Type' (highlighted), 'Generate Certificate', and 'Summary'. The main area is titled 'Certificate Type' and contains the instruction 'Choose certificate to be used for encrypted SSL connection.' Below this, there are three radio button options: 'Generate a new certificate' (selected), 'Select an existing certificate from the certificate store', and 'Import certificate from a file'. Each option has a brief description. At the bottom right, there are four buttons: '< Previous', 'Next >' (highlighted with a green border), 'Finish', and 'Cancel'.

Manage Certificate ✕

Certificate Type

Choose certificate to be used for encrypted SSL connection.

☒ **Generate a new certificate**
Generates a new self-signed certificate that is verifiable with the thumbprint.

☐ **Select an existing certificate from the certificate store**
Pick an existing certificate from the certificate store.

☐ **Import certificate from a file**
Import certificate from a file (PFX, XER, PEM or other).

< Previous **Next >** Finish Cancel

- At the **Generate Certificate** step of the wizard, specify a friendly name for the created self-signed TLS certificate.

The screenshot shows a 'Manage Certificate' dialog box with a sidebar on the left containing 'Certificate Type', 'Generate Certificate' (highlighted in green), and 'Summary'. The main area is titled 'Generate Certificate' and contains the instruction 'Type in friendly name for self-signed certificate.' Below this is a text input field labeled 'Friendly Name:' containing the text 'Veeam Software Group GmbH Cloud Connect Certificate'. A paragraph of text follows: 'The certificate created by this feature will not originate from a trusted certification authority (CA). Cloud Connect users will be notified about this fact when establishing the initial connection to your service, and provided with the ability to verify the certificate with the thumbprint.' At the bottom right are four buttons: '< Previous', 'Next >', 'Finish' (disabled), and 'Cancel'.

Manage Certificate

Certificate Type

Generate Certificate

Summary

Generate Certificate

Type in friendly name for self-signed certificate.

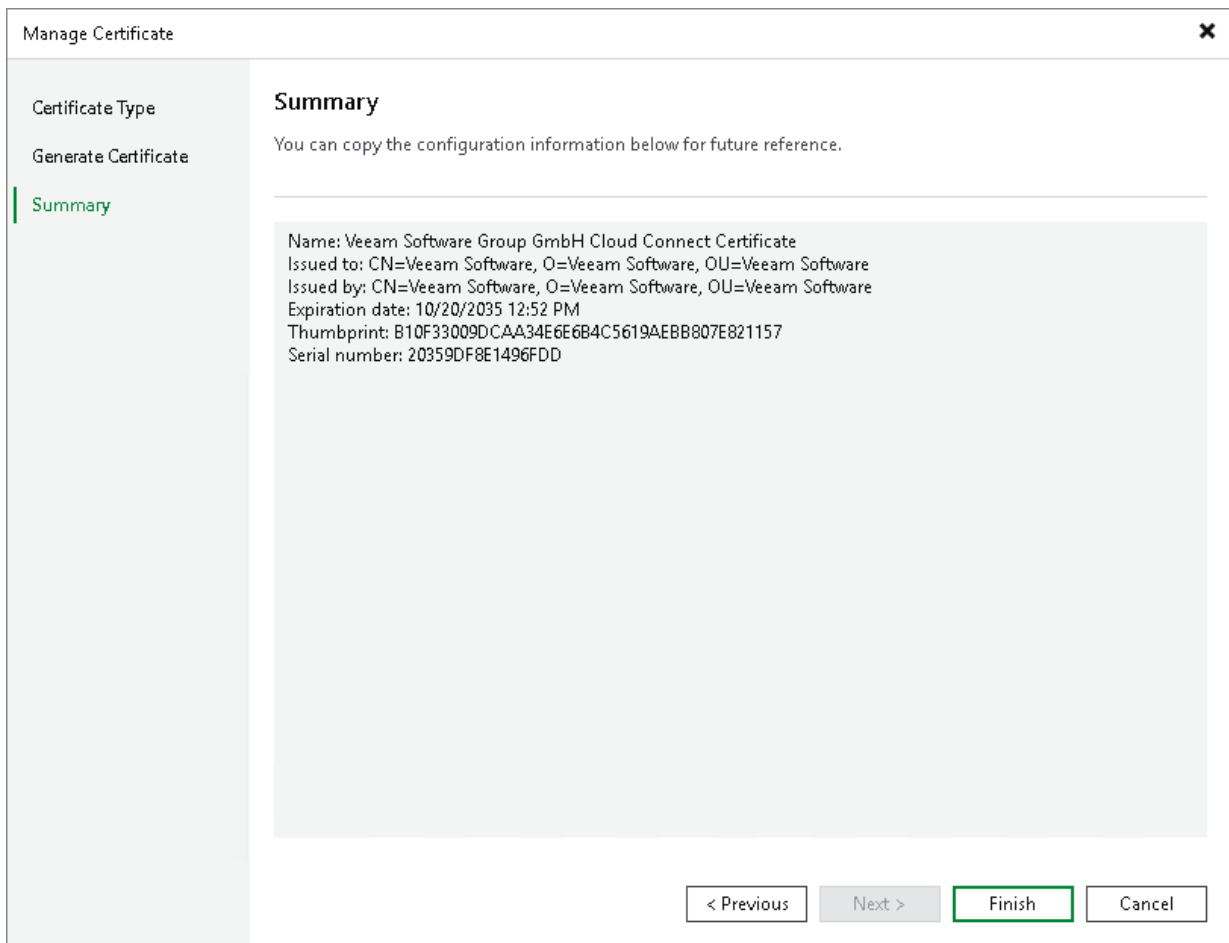
Friendly Name:

The certificate created by this feature will not originate from a trusted certification authority (CA). Cloud Connect users will be notified about this fact when establishing the initial connection to your service, and provided with the ability to verify the certificate with the thumbprint.

< Previous Next > Finish Cancel

- 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.

- Click **Finish**. Veeam Backup & Replication will save the generated certificate in the *Shared* certificate store on the Veeam backup server.



The screenshot shows a 'Manage Certificate' dialog box with a sidebar on the left containing three options: 'Certificate Type', 'Generate Certificate', and 'Summary'. The 'Summary' option is selected and highlighted with a green bar. The main area of the dialog is titled 'Summary' and contains the text: 'You can copy the configuration information below for future reference.' Below this text is a light gray box containing the following certificate details:

- Name: Veeam Software Group GmbH Cloud Connect Certificate
- Issued to: CN=Veeam Software, O=Veeam Software, OU=Veeam Software
- Issued by: CN=Veeam Software, O=Veeam Software, OU=Veeam Software
- Expiration date: 10/20/2035 12:52 PM
- Thumbprint: B10F33009DCAA34E6E6B4C5619AEBB807E821157
- Serial number: 20359DF8E1496FDD

At the bottom right of the dialog, there are four buttons: '< Previous', 'Next >', 'Finish' (which is highlighted with a green border), and 'Cancel'.

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.

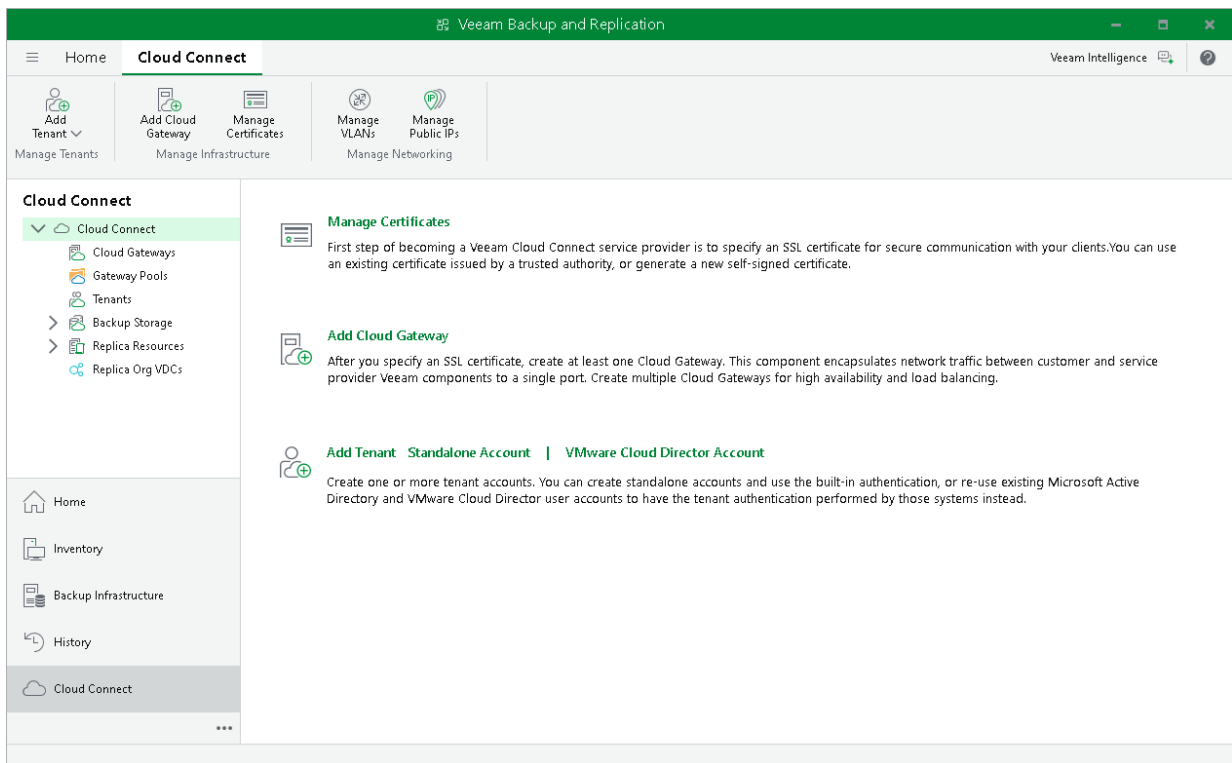
IMPORTANT

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.

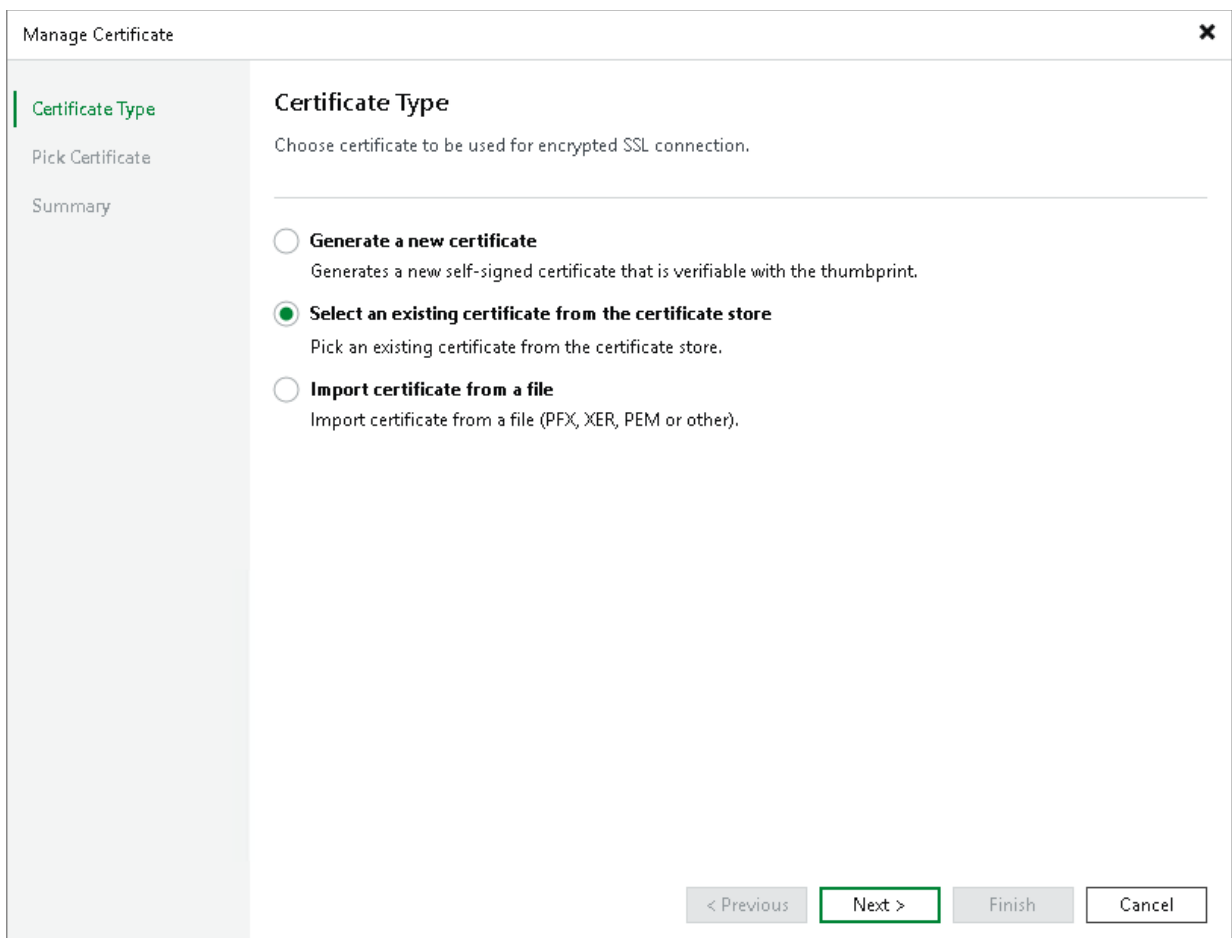
To select a certificate from the Microsoft Windows Certificate store:

- Open the **Cloud Connect** view.

- 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**.



- At the **Certificate Type** step of the wizard, choose **Select an existing certificate from the certificate store**.



- 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.

Manage Certificate

Certificate Type

Pick Certificate

Pick the existing certificate from local Certificate Store of this server.

Certificates:

Issued to	Expiration...	Friendly...	Issued by
CN=Veeam Software, O=Veeam Software, OU=Veeam	10/20/2035 12:5	Veeam Softwar	CN=Veeam Sof
CN=Veeam Software, O=Veeam Software, OU=Veeam	10/13/2035 3:20	Veeam Softwar	CN=Veeam Sof

Type in an object name to search for

< Previous Next > Finish Cancel

- At the **Summary** step of the wizard, review the certificate properties.
- Click **Finish** to apply the certificate.

Importing Certificates from 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.

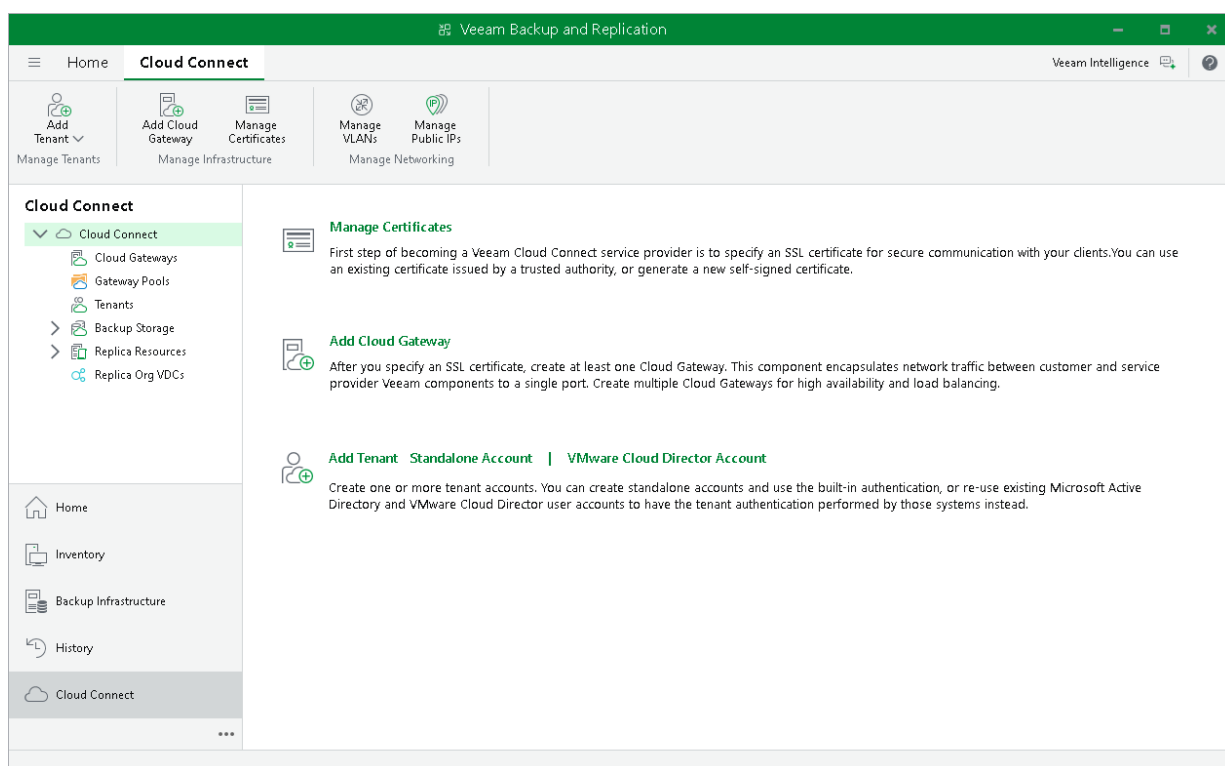
IMPORTANT

Consider the following:

- All certification authorities (CAs) related to the TLS certificate must be trusted by the SP Veeam backup server. Therefore, make sure that they are included in the *Intermediate Certification Authorities* and *Trusted Root Certification Authorities* folders within the Microsoft Windows Certificate store. Otherwise, you will not be able to import the TLS certificate. For more information about certificate and connectivity issues, see [this Veeam KB article](#).
- 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 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**.



- At the **Certificate Type** step of the wizard, choose **Import certificate from a file**.

The screenshot shows a window titled 'Manage Certificate' with a close button (X) in the top right corner. On the left is a sidebar with three items: 'Certificate Type' (highlighted with a green vertical bar), 'Import Certificate', and 'Summary'. The main area is titled 'Certificate Type' and contains the instruction 'Choose certificate to be used for encrypted SSL connection.' Below this is a horizontal line, followed by three radio button options: 1. 'Generate a new certificate' with the description 'Generates a new self-signed certificate that is verifiable with the thumbprint.' 2. 'Select an existing certificate from the certificate store' with the description 'Pick an existing certificate from the certificate store.' 3. 'Import certificate from a file' (selected with a green dot) with the description 'Import certificate from a file (PFX, XER, PEM or other).' At the bottom right are four buttons: '< Previous' (disabled), 'Next >' (active/highlighted with a green border), 'Finish' (disabled), and 'Cancel' (disabled).

- At the **Import Certificate** step of the wizard, specify a path to the PFX file.

5. If the PFX file is protected with a password, specify the password in the **Password** field.

The screenshot shows a 'Manage Certificate' window with a sidebar on the left containing 'Certificate Type', 'Import Certificate' (highlighted with a green bar), and 'Summary'. The main area is titled 'Import Certificate' and contains the following text: 'Specify the PFX file to import certificate from. The certificate will be automatically imported into the local Certificate Store of this server.' Below this, there are two input fields: 'Certificate:' with the value 'C:\cert\ABC_cert.pfx.txt' and a 'Browse...' link to its right; and 'Password:' with a masked input field (dots) and an eye icon to its right. A note below the password field states: 'Password is required only if this certificate was exported with the password protection enabled.' At the bottom right, there are four buttons: '< Previous', 'Next >' (highlighted with a green border), 'Finish', and 'Cancel'.

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 or Linux 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:
 - The cloud gateway can be a physical or virtual machine.
 - The cloud gateway can run Microsoft Windows OS or Linux OS.

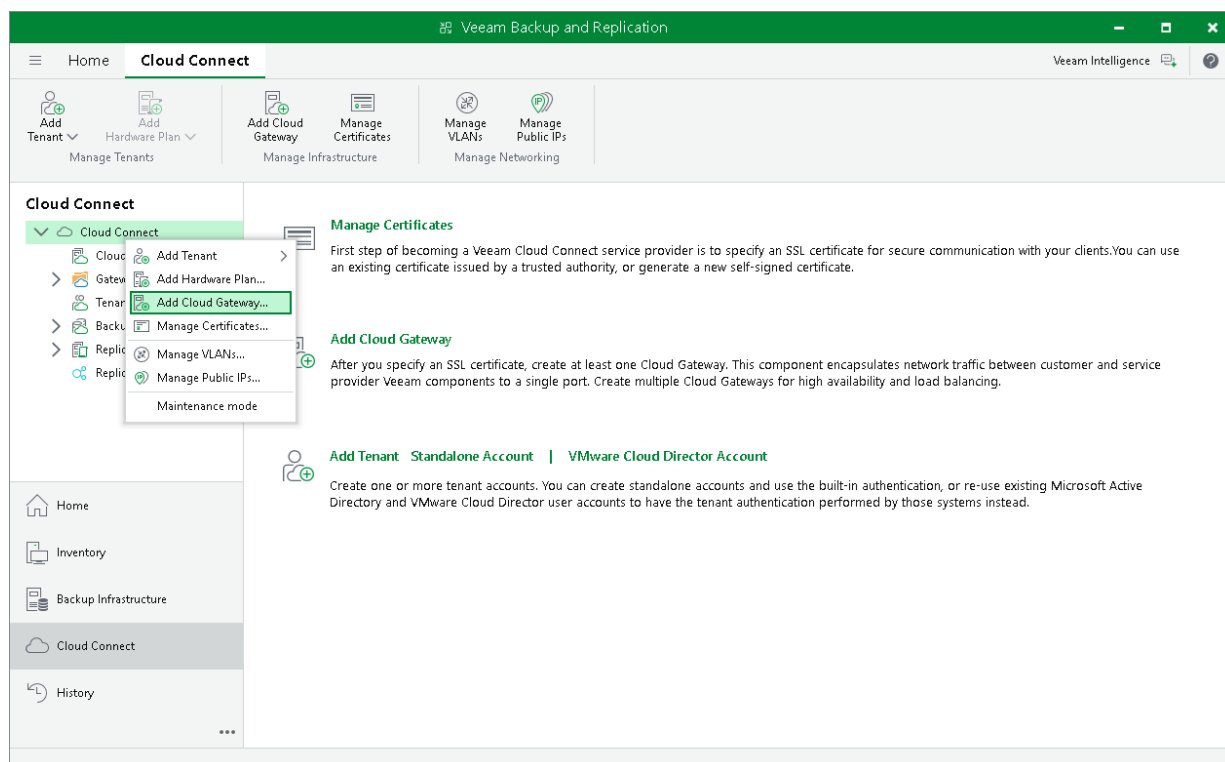
To learn more, see [System Requirements](#).

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 or a Linux 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.

The screenshot shows the 'New Cloud Gateway' wizard window. The left sidebar contains a vertical list of steps: 'Name' (highlighted in green), 'Networking', 'Review', 'Apply', and 'Summary'. The main content area is titled 'Name' and includes the following elements:

- A sub-header: 'Choose a server to set up cloud gateway service on. We recommend that you set up multiple cloud gateways for high availability and automatic load balancing.'
- A 'Choose server:' dropdown menu with the selected value 'srvt1.tech.local (Backup server)' and a green 'Add New...' link to its right.
- A 'Description:' text area containing the text 'My Cloud Gateway'.
- An 'External port:' spinner control set to '6180'.
- A note: 'TCP/UDP port for external connections. All traffic between you and your users will go through this port. Your users will need to specify this port when establishing the initial connection to your service.'
- At the bottom right, four buttons: '< Previous' (disabled), 'Next >' (active/highlighted), 'Finish' (disabled), and 'Cancel'.

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.

NOTE

In a scenario where the tenant connects to the SP over a private network, the DNS name of a cloud gateway available to the tenant can resolve to a private IP address. In this scenario, it is recommended that the cloud gateway operates as part of a cloud gateway pool. Otherwise, information about this cloud gateway will be passed to other tenants, including those who connect to the SP from the internet and may have no access to the cloud gateway.

- 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](#).

New Cloud Gateway

Name

Networking

Review

Apply

Summary

Networking

Specify how this server is connected to the Internet

☒ Located behind NAT or uses external DNS name (recommended)

Type in the external DNS name. Port forwarding rule must be set up on the NAT to forward network traffic from the external port to the internal port specified below.

DNS name: gateway01.tech.com

Internal port: 6180

☐ This server is connected directly to the Internet

Select network adapter (NIC) connected to the Internet:

Ethernet0, (172.24.26.16)

⚠ Direct connection mode cannot be used with IPv6 networking enabled.

< Previous

Next >

Finish

Cancel

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.

New Cloud Gateway

Name

Networking

Review

Apply

Summary

Review

Please review the required actions.

The following components will be processed:

Component name	Status
Cloud Gateway	will be installed

After you click Apply missing components will be installed on the target host.

< Previous

Apply

Finish

Cancel

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.

New Cloud Gateway

Name

Networking

Review

Apply

Summary

Apply

Please wait while required operations are being performed. This may take a few minutes...

Message	Duration
Starting infrastructure item update process	0:00:03
Connecting to Veeam Installer service	
[svt1] Discovering installed packages	
Creating temporary folder	
Package VeeamGateSvc.msi has been uploaded	
Installing package Cloud Gateway	0:00:26
Deleting temporary folder	
Registering client svt1 for package Cloud Gateway	
Discovering installed packages	0:00:05
All required packages have been successfully installed	
Detecting server configuration	
Checking Cloud Gate service state	
Restarting Cloud Gate service	0:00:01
Creating configuration database records for Cloud Gateway	
Creating configuration database records for installed packages	
Cloud Gateway created successfully	

< Previous

Next >

Finish

Cancel

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.

New Cloud Gateway

Name

Networking

Review

Apply

Summary

Summary

You can copy the configuration information below for future reference.

srvt1.tech.local was successfully saved.

Hardware info:

Chassis type: Virtual (VMware)
Cores count: 4

Components:

Cloud Gateway using port 6168
Dell Data Domain Library
Guest Interaction Proxy using port 6190
HPE StoreOnce Library
Installer service using port 6160
Mount service using port 6170
Veeam Backup VSS Integration using port 6210
Veeam Data Mover service using port 6162
Veeam Standby service
Veeam Threat Hunter
Veeam VSS Hardware Snapshot Provider
VMware VDDK
vPower NFS using port 6161

< Previous

Next >

Finish

Cancel

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

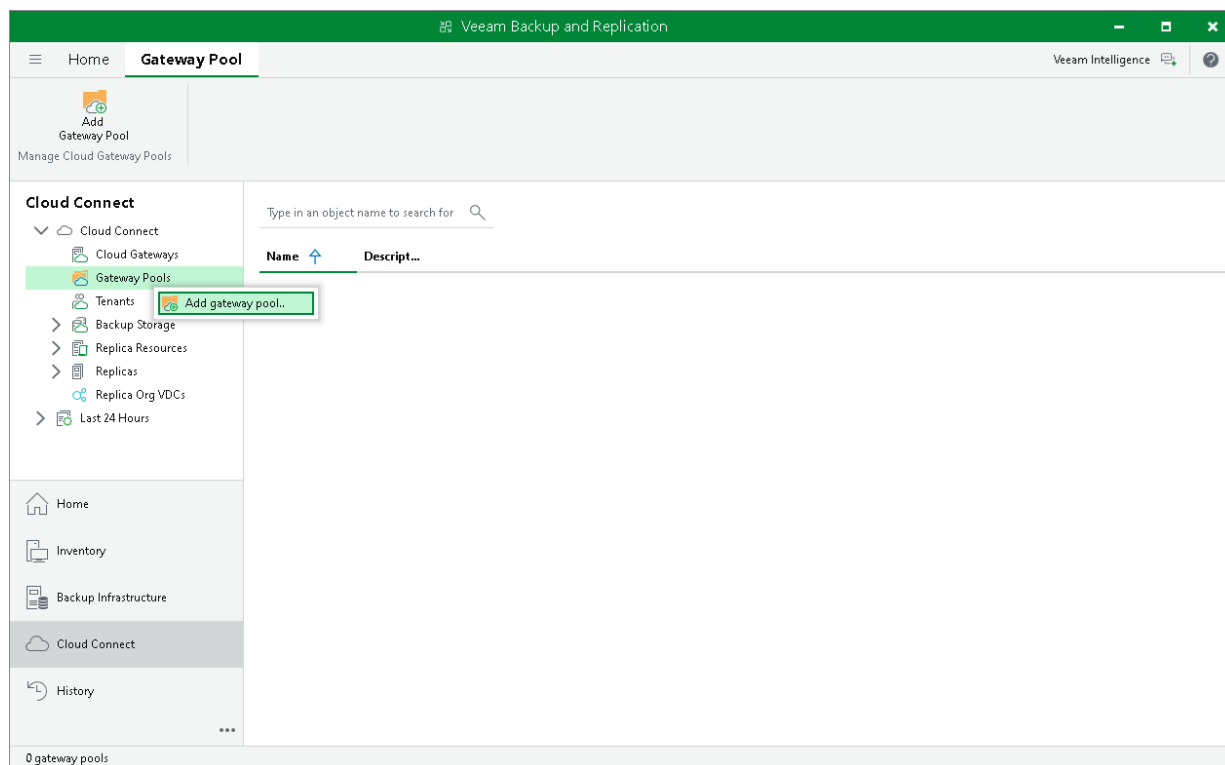
Before you configure a cloud gateway pool, check the following prerequisites:

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.

New Gateway Pool

Name

Cloud Gateways

Summary

Name

Gateway pools allow assigning groups of cloud gateways to tenants. For example, you can have a pool of gateways for Internet connected tenants, and a separate pool for MPLS connected tenants.

Name:

Cloud Gateway Pool

Description:

Cloud gateway pool for TechCompany

< Previous

Next >

Finish

Cancel

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.

New Gateway Pool

Name

Cloud Gateways

Summary

Cloud Gateways

Select cloud gateways to add to the created gateway pool.

Cloud gateways:

Name

☒

srvt1

< Previous

Next >

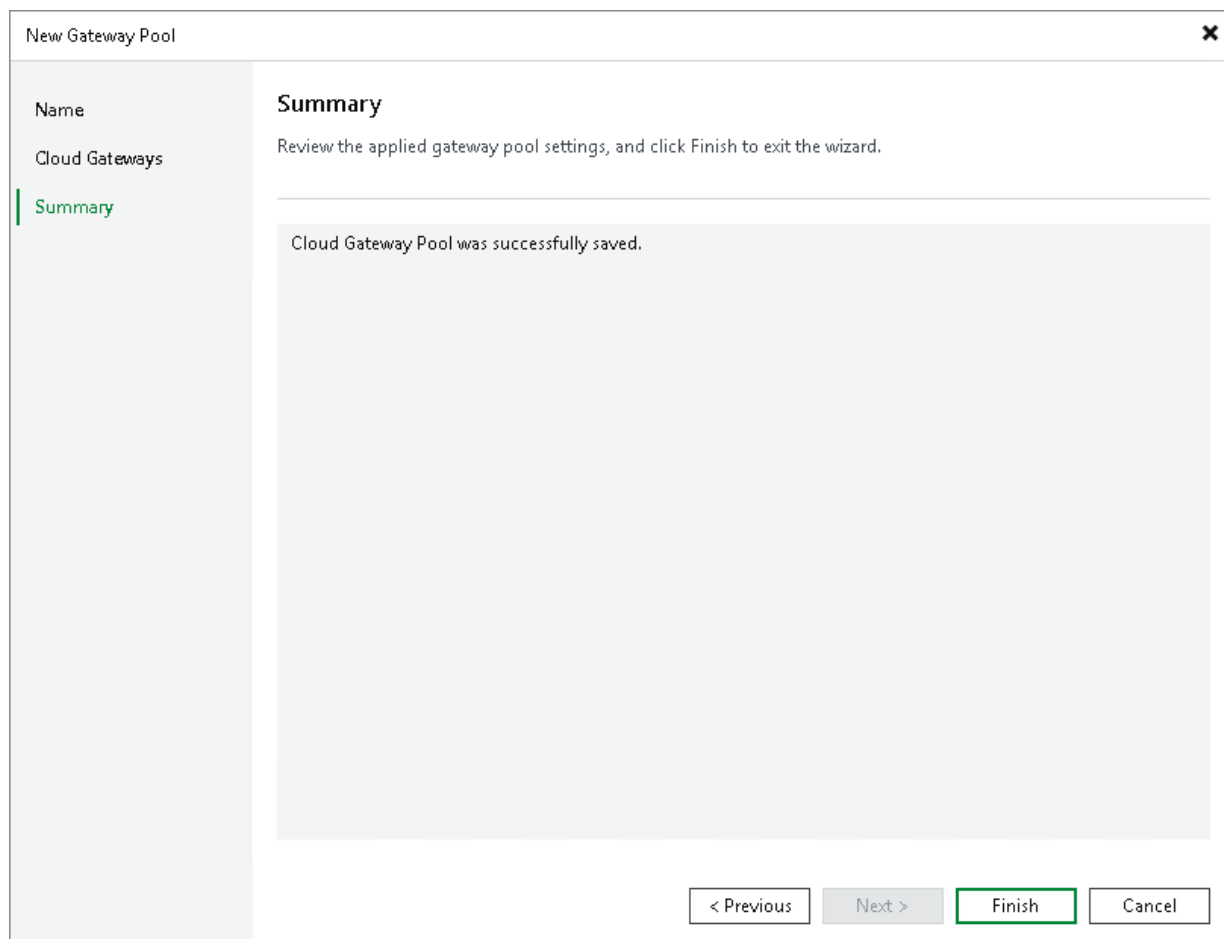
Finish

Cancel

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.



The screenshot shows a window titled "New Gateway Pool" with a close button (X) in the top right corner. On the left is a sidebar with three items: "Name", "Cloud Gateways", and "Summary". "Summary" is selected and highlighted with a green vertical bar. The main area is titled "Summary" and contains the text "Review the applied gateway pool settings, and click Finish to exit the wizard." Below this is a large light gray box with the message "Cloud Gateway Pool was successfully saved." At the bottom right, there are four buttons: "< Previous", "Next >", "Finish" (which is highlighted with a green border), and "Cancel".

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
- Deduplicating storage appliance: Dell Data Domain, ExaGrid, Quantum DXi and HPE StoreOnce
- Scale-out backup repository
- Object storage: S3 compatible, Amazon S3, IBM Cloud, Microsoft Azure and Wasabi

To learn more, see [Backup to Object Storage](#).

The configuration process for backup repositories in the Veeam Cloud Connect infrastructure does not differ from the same process in the regular Veeam backup infrastructure. To learn more, see the following sections in the Veeam Backup & Replication User Guide:

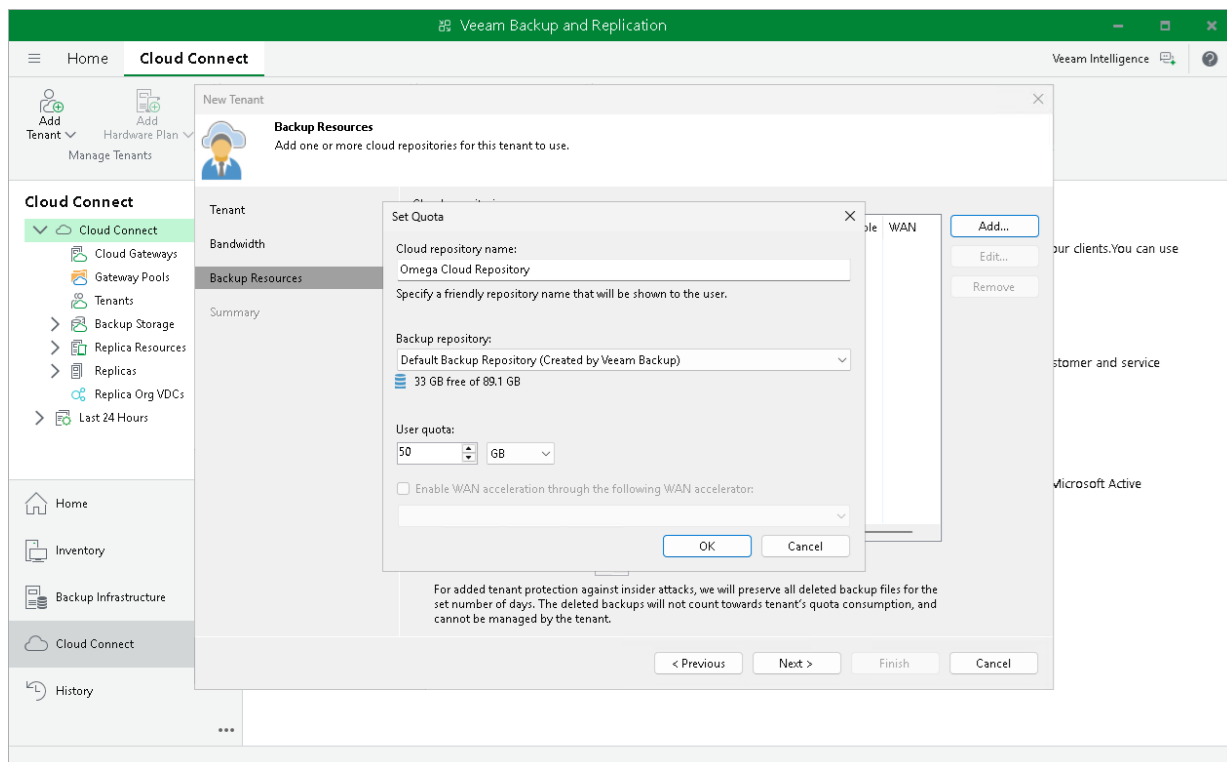
- [Adding Microsoft Windows Repository](#)
- [Adding Scale-Out Backup Repository](#)
- [Adding Object Storage Repositories](#)

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 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:
 - The **New VMware Hardware Plan** wizard — to configure a VMware hardware plan.
 - 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

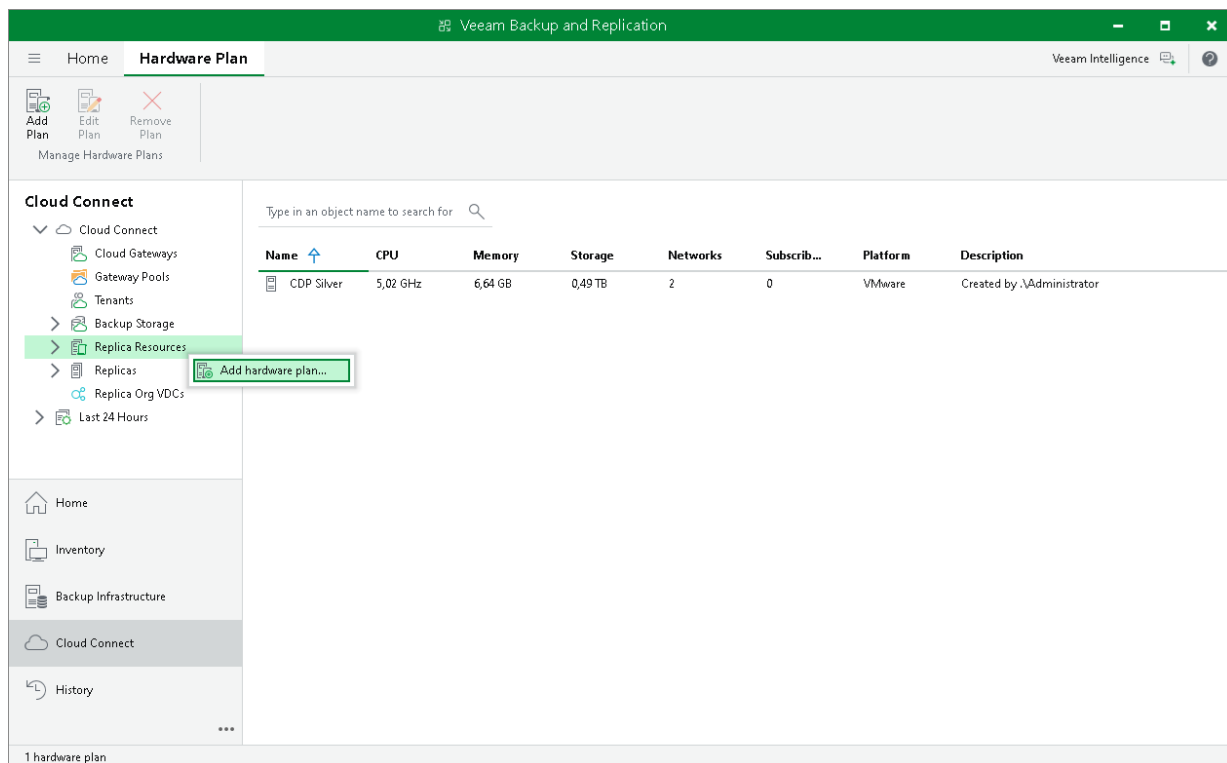
Before you add a new Hyper-V hardware plan, consider the following limitations:

- 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:
 - Clusters with server nodes that run Nano Server installations of the Microsoft Windows Server 2016 OS
 - Clusters with the Cluster Operating System Rolling Upgrade feature enabled
 - 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.

New VMware Hardware Plan

Name
Specify a name and description for this hardware plan.

Name

Host

Storage

Network

Apply

Summary

Name:
VMware Silver

Description:
Hardware plan for VMware vSphere VMs

< Previous Next > Finish Cancel

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.

The screenshot shows the 'New VMware Hardware Plan' wizard, specifically the 'Host' step. The window title is 'New VMware Hardware Plan' with a close button (X) in the top right corner. On the left, there is a sidebar with icons and labels: 'Name', 'Host' (selected), 'Storage', 'Network', 'Apply', and 'Summary'. The main area is titled 'Host' and contains the instruction 'Specify the host or cluster where tenant's replica VMs should be created.' Below this, there is a 'Host or cluster:' label followed by a text input field containing 'prgtwex01.tech.local' and a 'Choose...' button. Further down, there are two sections: 'CPU' and 'Memory'. Each section has a horizontal slider, a numeric input field, and a unit. For CPU, the slider is at 10.0, the input field shows '10,0', and the unit is 'GHz'. For Memory, the slider is at 16.0, the input field shows '16,0', and the unit is 'GB'. Below each slider is an 'Unlimited' checkbox, which is currently unchecked. At the bottom of the window, there are four buttons: '< Previous', 'Next >' (highlighted with a blue border), 'Finish', and 'Cancel'.

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.

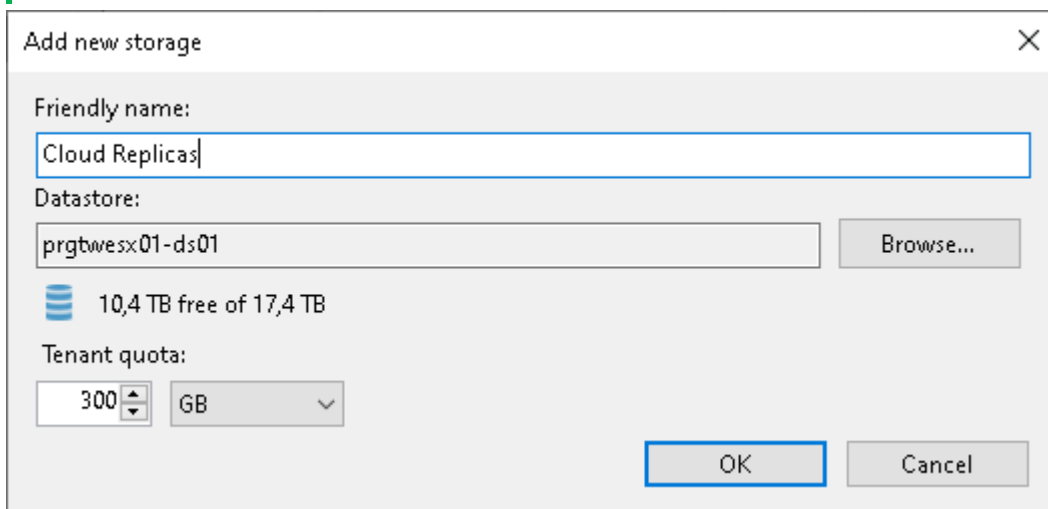
1. In the **Storage** section, click **Add** to open the **Add new storage** window.
2. In the **Friendly name** field, specify a name of the storage that will be displayed to a tenant.
3. [For a VMware hardware plan] In the **Datastore** section, click **Browse** and select a datastore on which to allocate 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.



The screenshot shows the 'Add new storage' dialog box. It has a title bar with a close button. The 'Friendly name' field is filled with 'Cloud Replicas'. The 'Datastore' field contains 'prgtwex01-ds01' and has a 'Browse...' button to its right. Below the datastore field, there is a blue icon and the text '10,4 TB free of 17,4 TB'. The 'Tenant quota' section has a spinner box set to '300' and a dropdown menu set to 'GB'. At the bottom right are 'OK' and 'Cancel' buttons.

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.

Add new storage [X]

Friendly name:

Path:

 8,63 TB free of 17,4 TB

Tenant quota:

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**.

New VMware Hardware Plan [X]

Storage
Specify storage assigned to this hardware plan.

vm

Name

Host

Storage

Network

Apply

Summary

Storage:			
Friendly name	Datastore	Quota	Available
 Cloud Replicas	prgtwex01-ds01	300 GB	17,4 TB

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.

The screenshot shows the 'New VMware Hardware Plan' wizard window, specifically the 'Network' step. The window title is 'New VMware Hardware Plan' with a close button (X) in the top right corner. On the left side, there is a sidebar with a 'vm' icon and a list of steps: 'Name', 'Host', 'Storage', 'Network' (which is highlighted), 'Apply', and 'Summary'. The main area of the window is titled 'Network' and contains the instruction 'Specify network resources to assign to this hardware plan.' Below this, there is a section labeled 'Networks' with two input fields: 'Specify number of networks with Internet access:' with a value of '1', and 'Specify number of internal networks:' with a value of '1'. A note below these fields states 'Total number of networks available to tenant cannot exceed 9.' At the bottom of the main area, there is a blue link that says 'Configure VLAN ID range'. At the very bottom of the window, there are four buttons: '< Previous', 'Apply' (which is highlighted with a blue border), 'Finish', and 'Cancel'.

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.

New VMware Hardware Plan



Apply

Please wait while settings are being saved to the configuration database.

Name

Host

Storage

Network

Apply

Summary

Log:

Message	Duration
✔ Creating hardware plan	0:00:01

< Previous

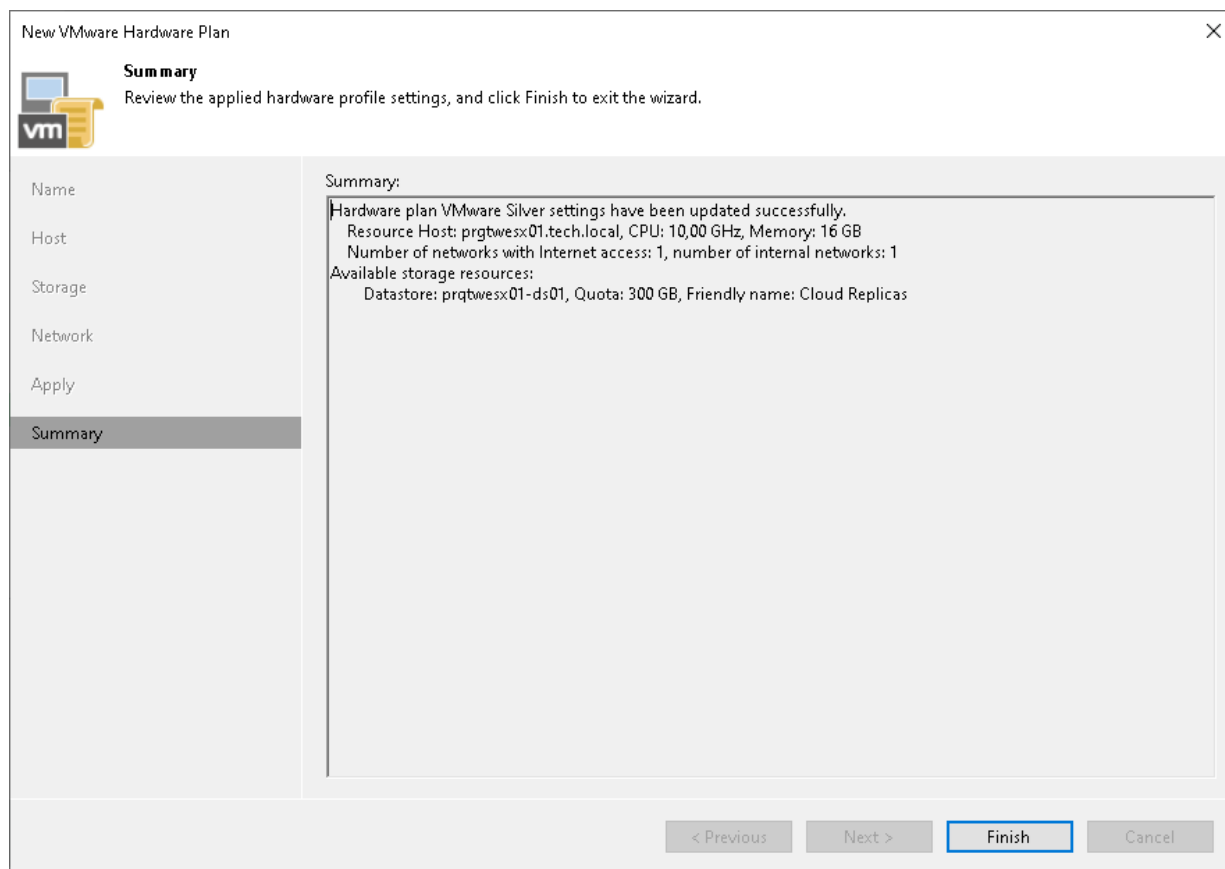
Next >

Finish

Cancel

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.

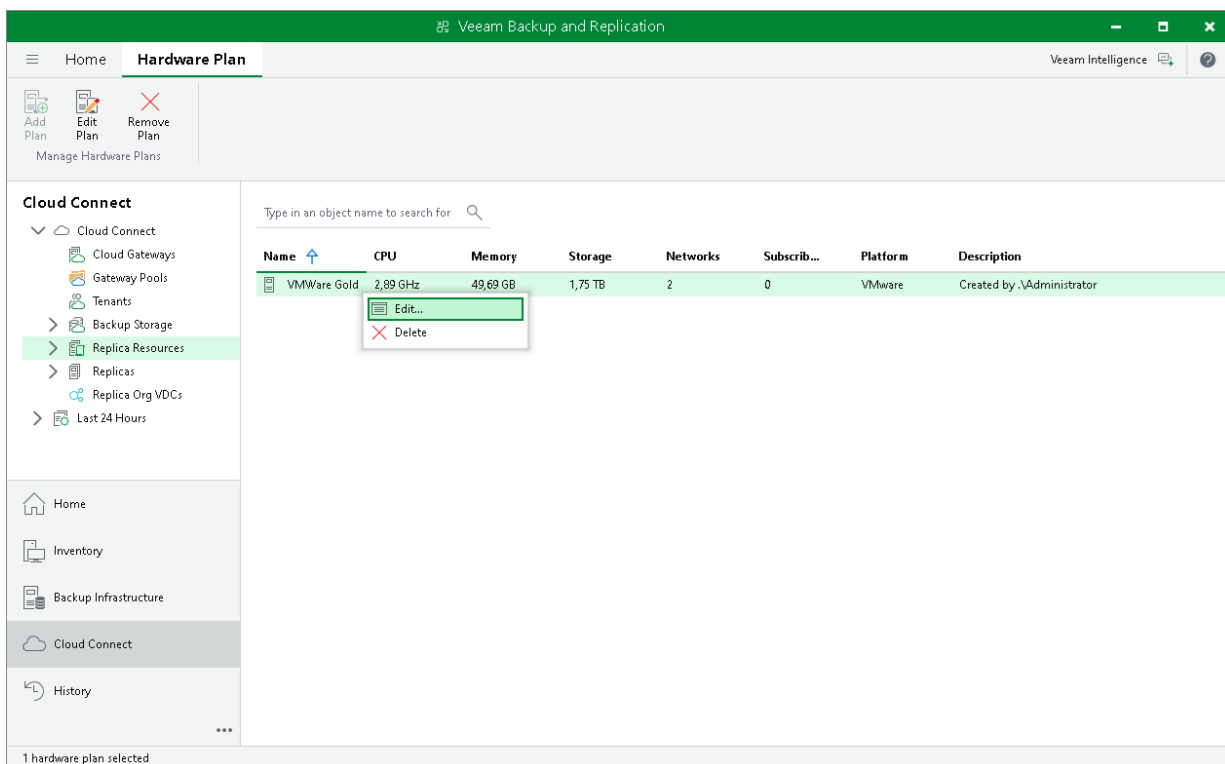
3. Do one of the following:

- 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**.
- 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**.

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:
 - 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 **Delete**.

- 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 **Delete**.

The screenshot shows the Veeam Backup and Replication console. The top ribbon has a 'Hardware Plan' tab. Below the ribbon, there are three buttons: 'Add Plan', 'Edit Plan', and 'Remove Plan'. The left sidebar shows a tree view with 'Cloud Connect' expanded, and 'Replica Resources' selected. The main area displays a table of hardware plans. A context menu is open over the 'VMware Silver' plan, showing 'Edit...' and 'Delete' options.

Name	CPU	Memory	Storage	Networks	Subscrib...	Platform	Description
VMware Silver	2.89 GHz	49.69 GB	1.75 TB	2	0	VMware	Created by .\Administrator

1 hardware plan selected

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.
- The SP must avoid configuration of overlapping VLAN ranges. If one or more VLAN IDs overlap, the tenant creation process will fail.

TIP

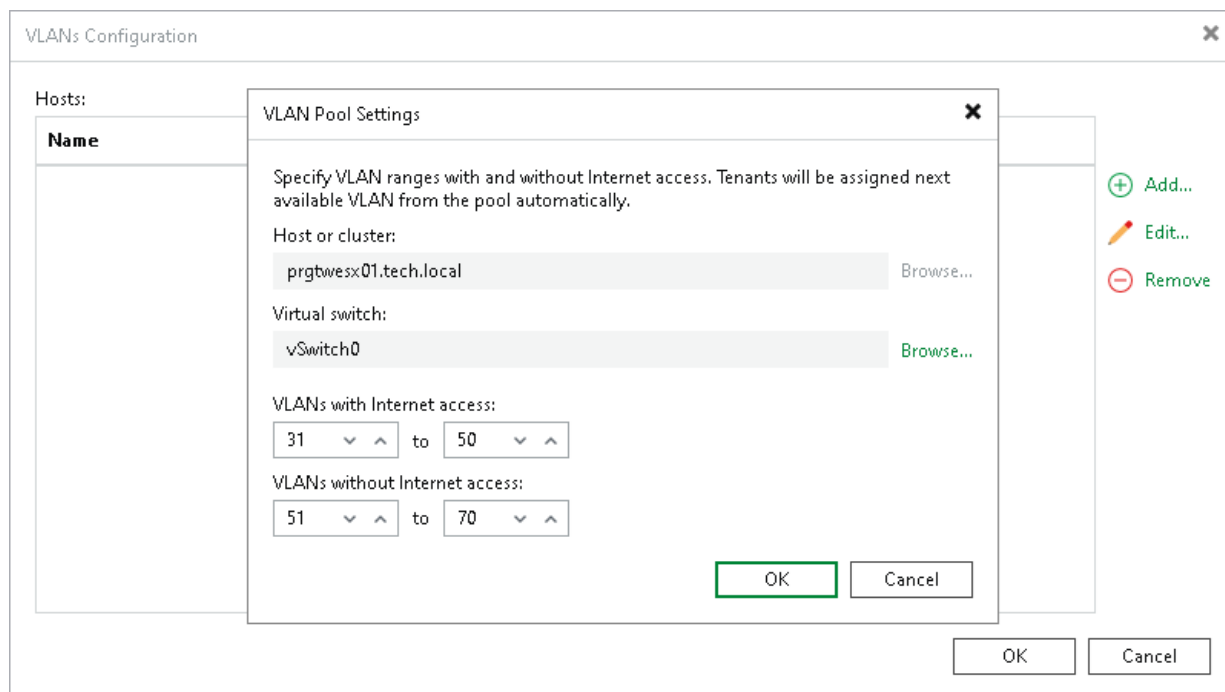
It is recommended that the SP plans network resources allocation and configures VLAN ranges in the Veeam Backup & Replication console in advance, prior to configuring hardware plans. However, the SP can also access the **VLANs Configuration** window when the SP performs the following tasks:

- 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:
 - Open the **Cloud Connect** view, click the **Cloud Connect** node and click **Manage VLANs** on the ribbon.
 - 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**.



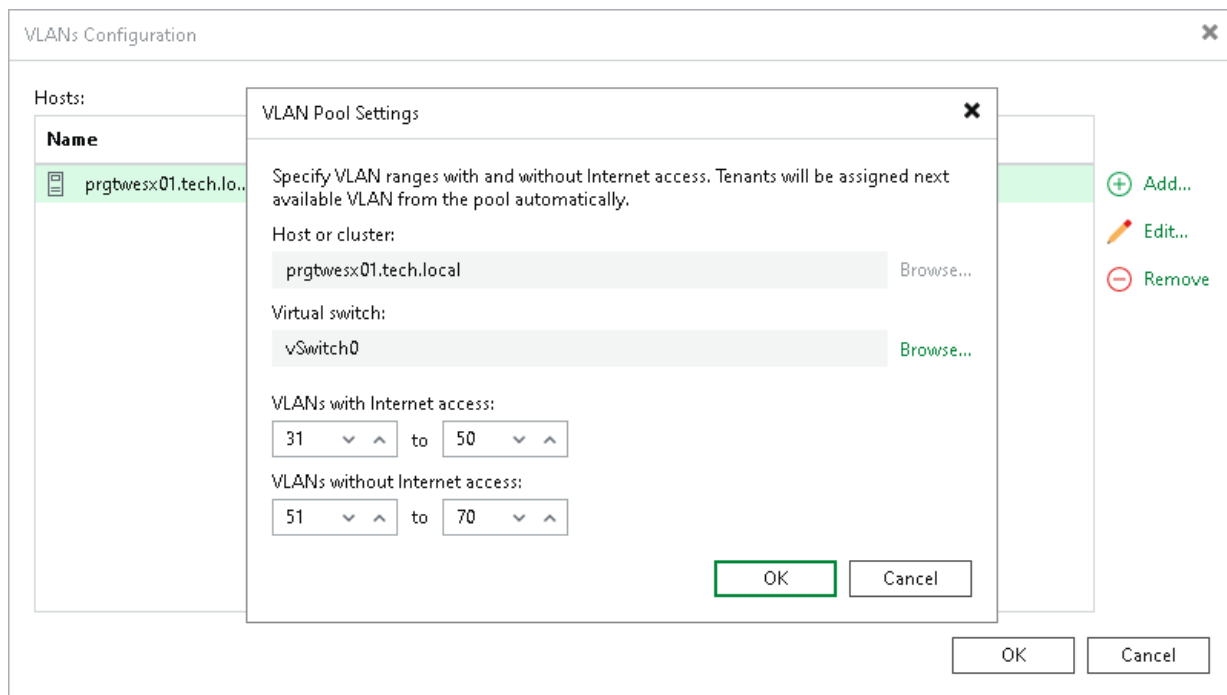
Editing VLAN Ranges

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:
 - Open the **Cloud Connect** view, click the **Cloud Connect** node and click **Manage VLANs** on the ribbon.
 - 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:
 - Open the **Cloud Connect** view, click the **Cloud Connect** node and click **Manage VLANs** on the ribbon.
 - 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**.

VLANs Configuration

Hosts:

Name	Virtual switch	VLANs with Inter...	Internal VLANs
 prgbwesx01.tech.lo...	vSwitch0	10 - 20	21 - 30

 Add...

 Edit...

 Remove

OK

Cancel

Managing Public IP Addresses

It may 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 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:

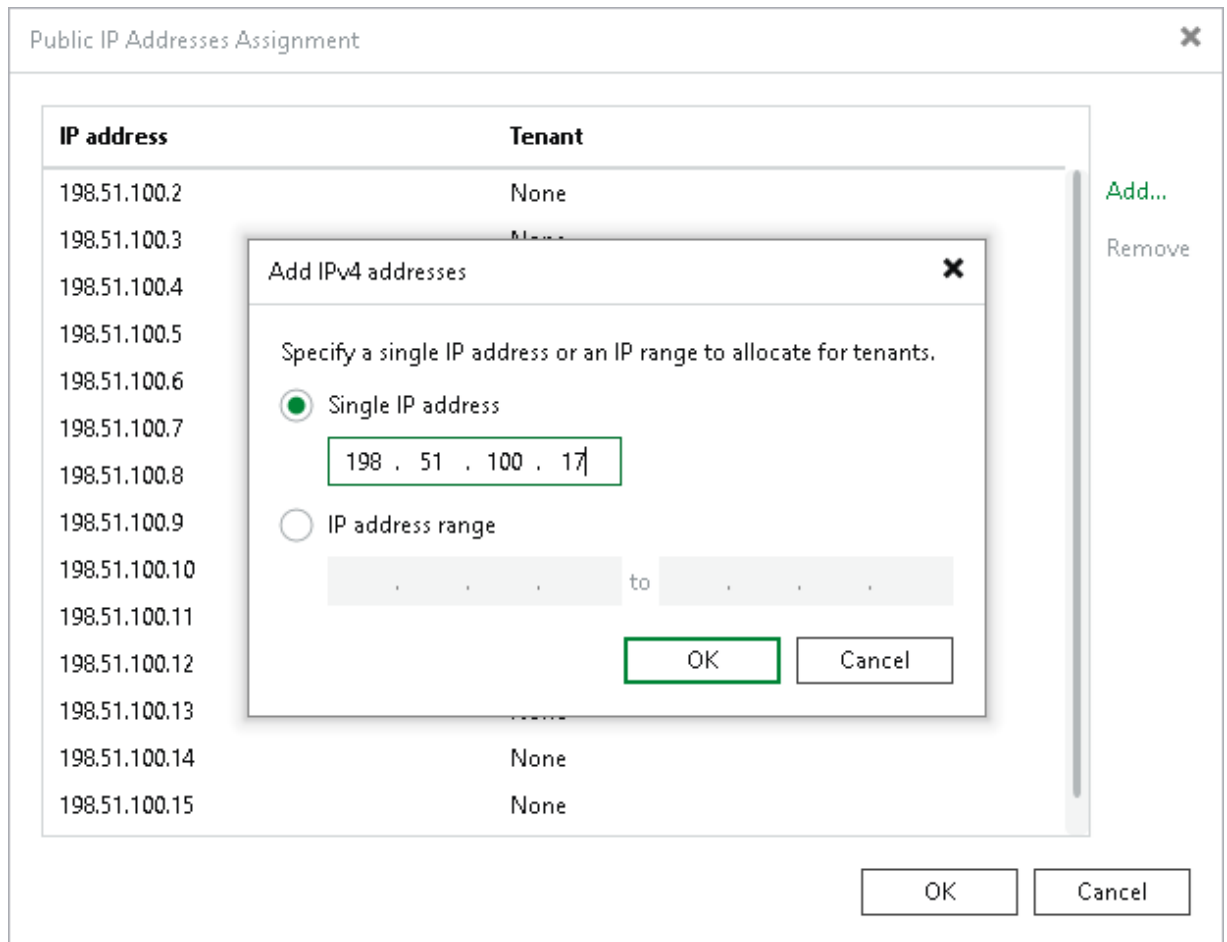
- The SP does not need to allocate public IP addresses in Veeam Backup & Replication if the SP uses VMware Cloud Director to provide replication resources to tenants. Instead, the SP configures the NSX Edge gateway in the properties of the organization VDC that will be used as a cloud host for tenant 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

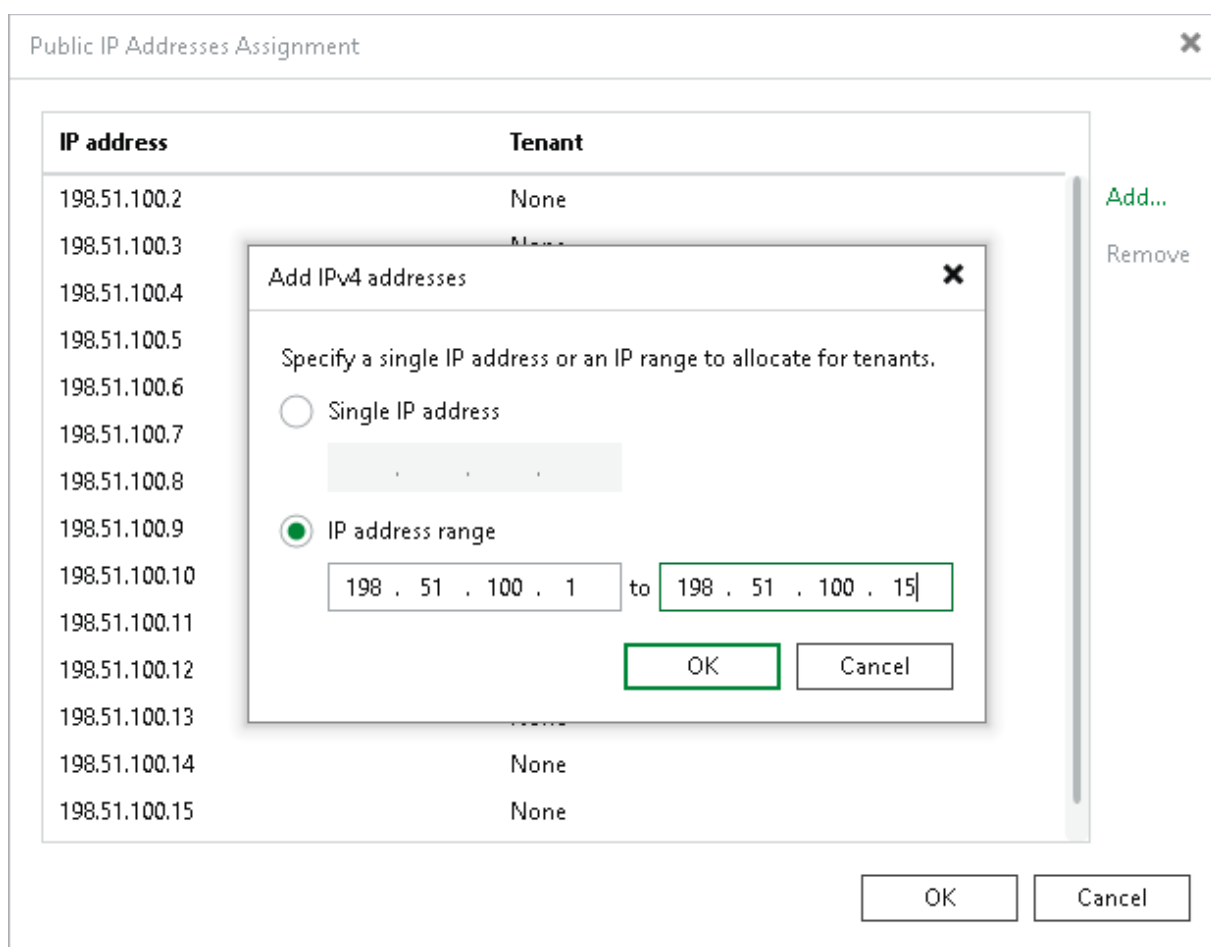
To configure a pool of public IPv4 addresses:

1. Open the **Public IP Addresses Assignment** window in one of the following ways:
 - Open the **Cloud Connect** view, click the **Cloud Connect** node and click **Manage Public IPs** on the ribbon.
 - 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:
- 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.



- 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.



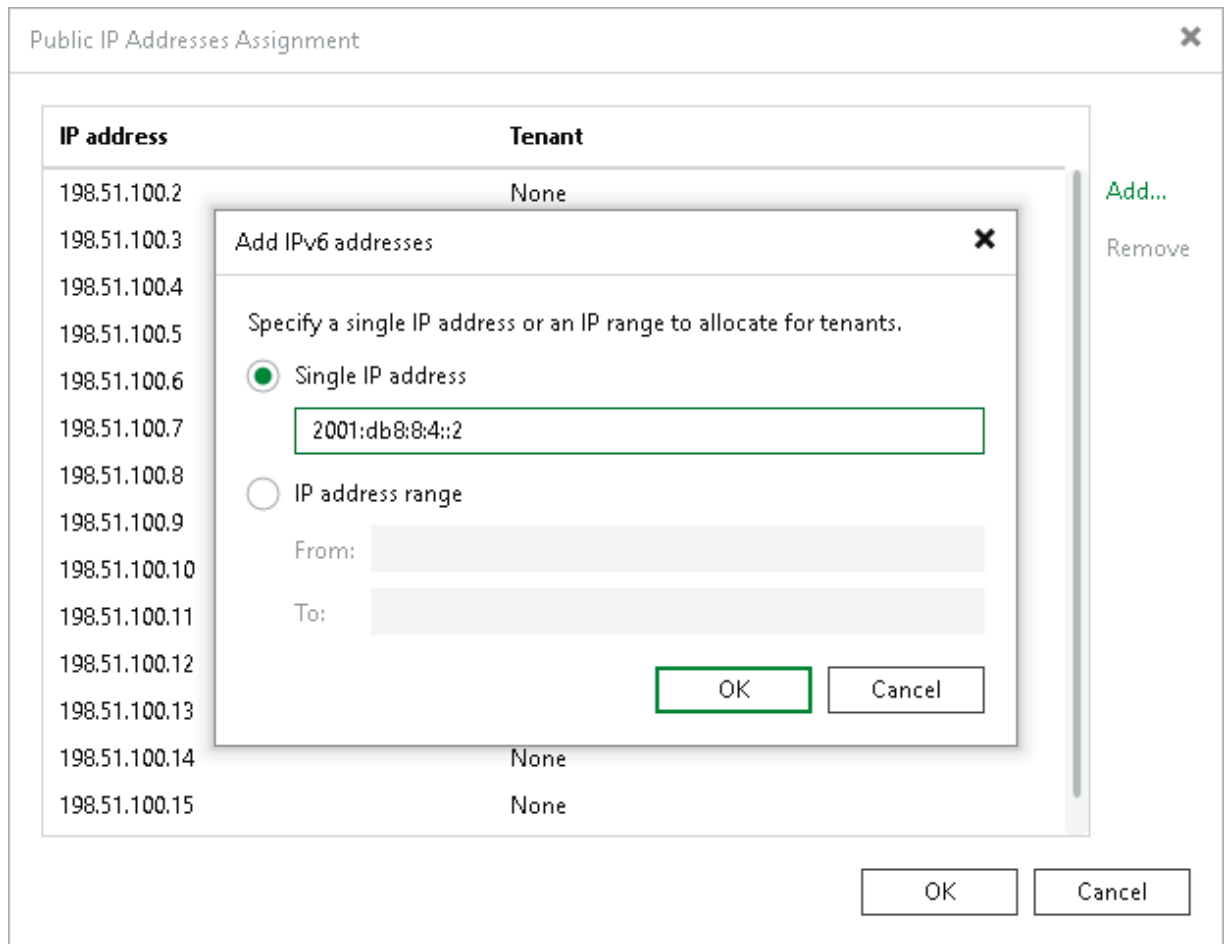
4. Click **OK**.

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:
 - Open the **Cloud Connect** view, click the **Cloud Connect** node and click **Manage Public IPs** on the ribbon.
 - 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:
- 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.



- 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.

Public IP Addresses Assignment

IP address	Tenant
198.51.100.2	None
198.51.100.3	
198.51.100.4	
198.51.100.5	
198.51.100.6	
198.51.100.7	
198.51.100.8	
198.51.100.9	
198.51.100.10	
198.51.100.11	
198.51.100.12	
198.51.100.13	
198.51.100.14	None
198.51.100.15	None

Add...

Remove

Add IPv6 addresses

Specify a single IP address or an IP range to allocate for tenants.

☐ Single IP address

☒ IP address range

From: 2001:db8:8:4::2

To: 2001:db8:8:4::4

OK Cancel

OK Cancel

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](#).

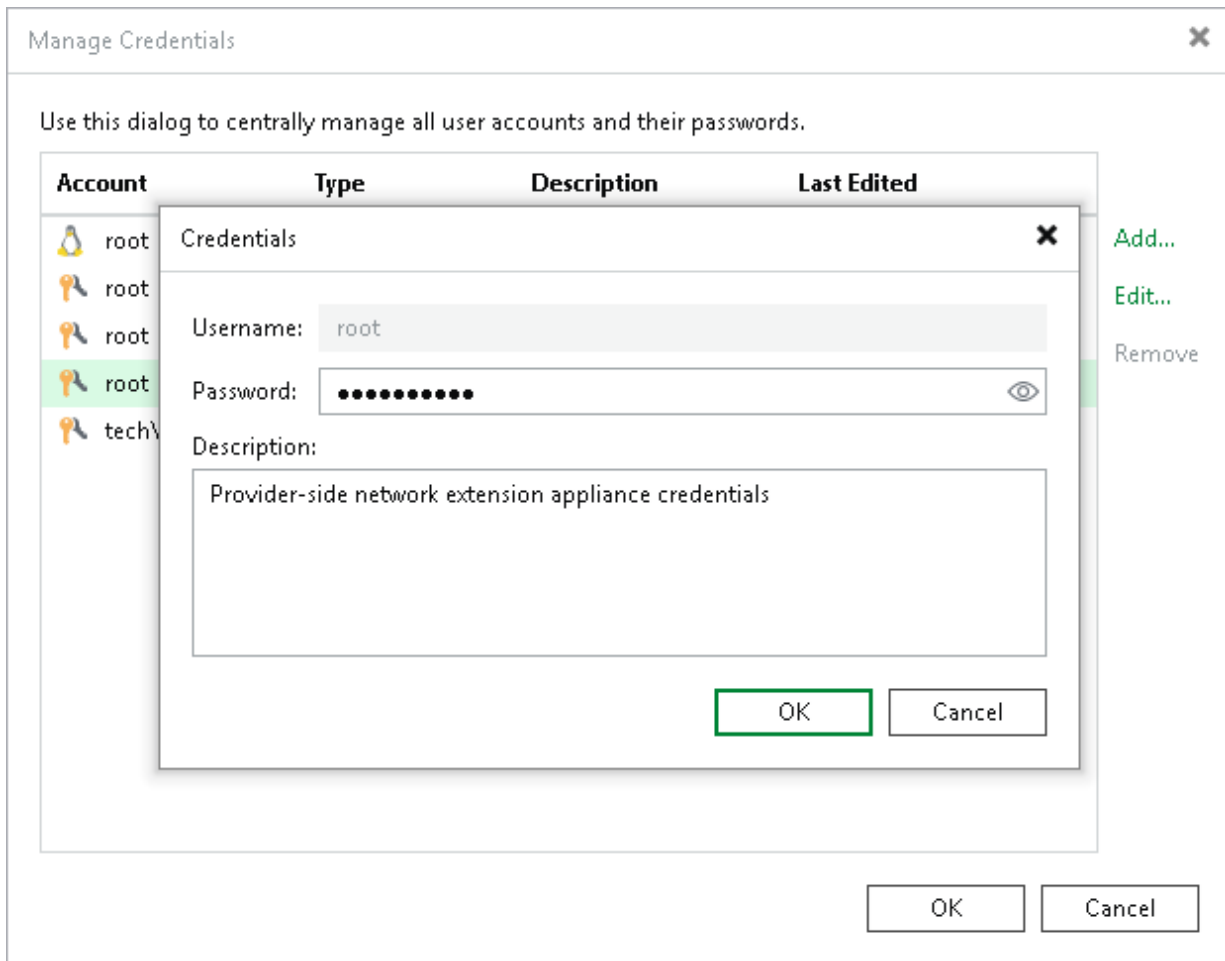
To specify a password for the root account of the network extension appliance VM:

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](#).



Creating 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.
- [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.
- 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:

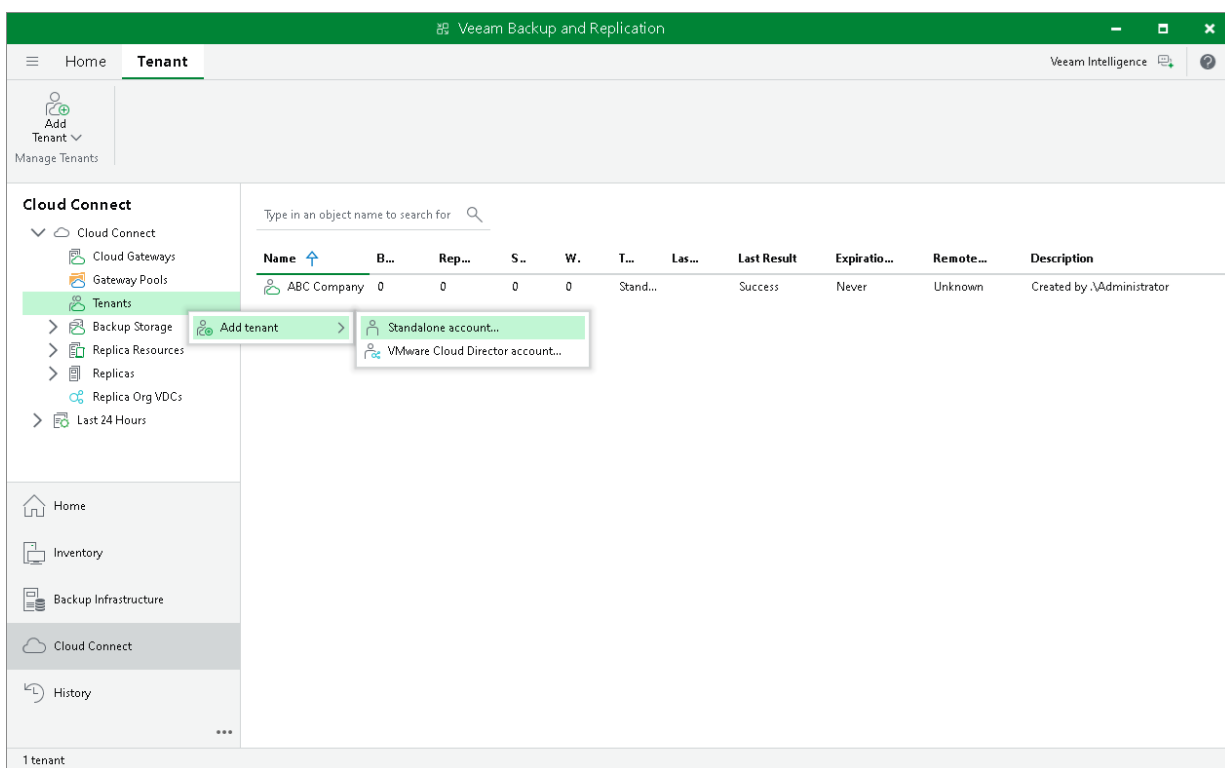
- A TLS certificate must be installed on the SP Veeam backup server.
- At least one cloud gateway must be added in the Veeam Cloud Connect infrastructure on the SP backup server.
- Backup repositories that you plan to use as cloud repositories must be added to your backup infrastructure. When you create 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 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:
 - The maximum length of the user name is 128 characters. To avoid problems with long paths to backup files on the cloud repository, it is recommended to create user names not longer than 50 characters.
 - The user name may contain space characters.
 - The user name must not contain the following characters: +][, \: *? \ " < > | = ; @ as well as ASCII symbols.
 - 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:
 - **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](#).
 - **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 Replication 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.

New Tenant [Close]

Tenant
Specify tenant name, password, assigned cloud resource types and optional contract expiration date.

Tenant (selected)
Bandwidth
Backup Resources
Replica Resources
Network Extension
Apply
Summary

Username: Omega Company

Password: [Masked] [Generate new](#)

Description: Tenant account for Omega Company

Assigned resources

- ☒ Backup storage (cloud backup repository)
- ☒ Replication resources (cloud host)

Automatic expiration

- ☒ Contract expires: Never [Calendar](#)

< Previous **Next >** Finish Cancel

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](#).

New Tenant

Bandwidth
Specify maximum number of task slots available to this tenant and if desired, limit incoming network traffic from this tenant.

Tenant

Bandwidth

Backup Resources

Replica Resources

Network Extension

Apply

Summary

Max concurrent tasks:
2

Each task slot allows processing of a single disk, so tenants with one slot assigned will not be able to leverage parallel processing, or run multiple jobs concurrently. This setting applies to direct mode transfers only (WAN accelerators process disks sequentially).

☒ Limit network traffic from this tenant to:
10 MB/s

Defines maximum allowed incoming network traffic rate for the tenant. If the tenant exceeds the assigned limit, the traffic will be throttled to the specified value.

Gateway pool:
Cloud Gateway Pool

Choose...

< Previous Next > Finish Cancel

Assigning Cloud Gateway Pools

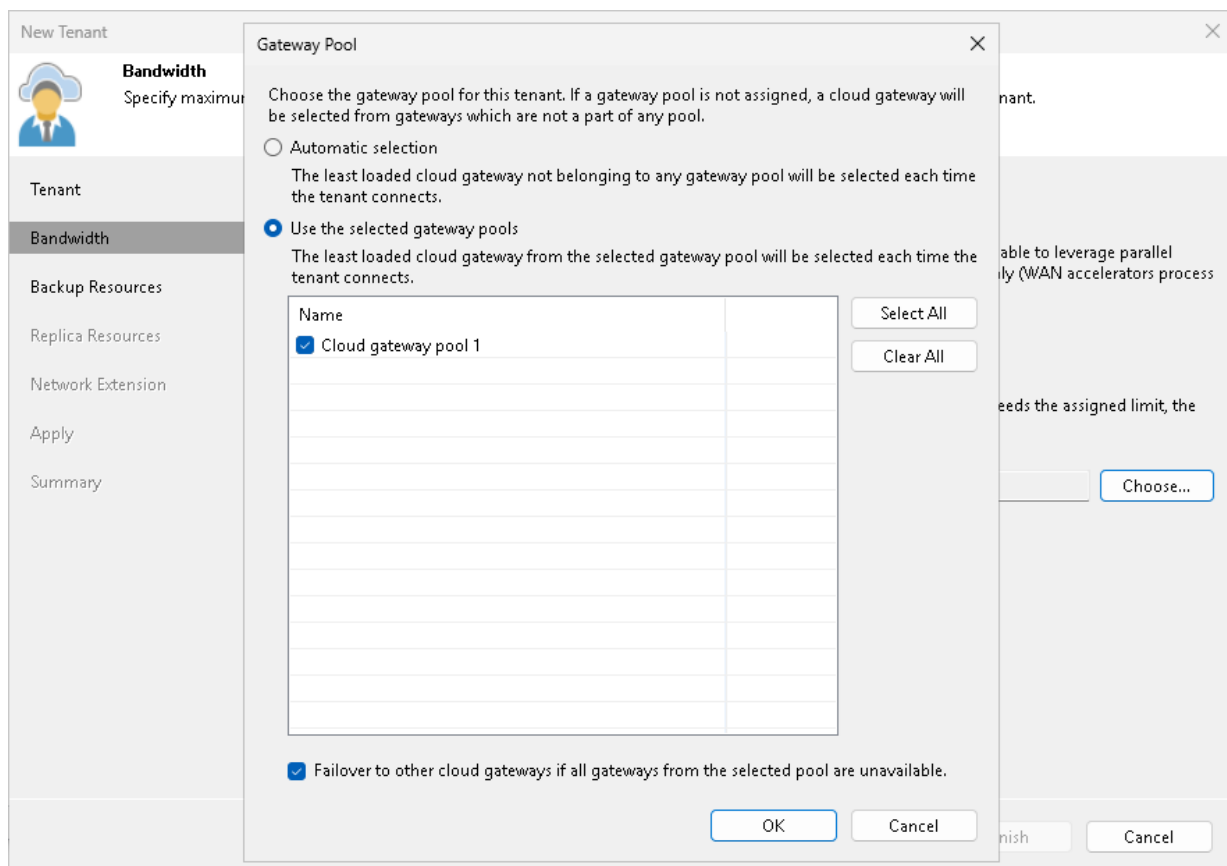
You can assign to the tenant one or more cloud gateway pools configured in the Veeam Cloud Connect infrastructure. After you assign a cloud gateway pool to the tenant, communication between the tenant backup server and Veeam Cloud Connect infrastructure components in the SP side will be possible only 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 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. [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.

New Tenant

**Backup Resources**
Add one or more cloud repositories for this tenant to use.

Tenant

Bandwidth

Backup Resources

Replica Resources

Network Extension

Apply

Summary

Set Quota

Cloud repository name:
Omega Company Cloud Repository

Specify a friendly repository name that will be shown to the user.

Backup repository:
Default Backup Repository (Created by Veeam Backup)

9.8 GB free of 89.1 GB

User quota:
100 GB

☒ Enable WAN acceleration through the following WAN accelerator:
172.24.31.66 (Target WAN Accelerator for Veeam Cloud Connect)

OKCancel

ole WAN

Add...

Edit...

Remove

For added tenant protection against insider attacks, we will preserve all deleted backup files for the set number of days. The deleted backups will not count towards tenant's quota consumption, and cannot be managed by the tenant.

< Previous

Next >

Finish

Cancel

241 | Veeam CloudConnect | Administrator Guide | 13.1.0.411

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](#).

New Tenant

Replica Resources
Add one or more hardware plans for this tenant to use.

Tenant

Bandwidth

Backup Resources

Replica Resources

Network Extension

Apply

Summary

Hardware plans:

Name	CPU	Memory	Storage	Networks	WAN

Add...

Edit...

Remove

Add replication resource

Select hardware plan:

VMware Silver

☒ Enable WAN acceleration through the following WAN accelerator:

srvt1.tech.local

OK

Cancel

Manage network settings

☒ Use Veeam network extension capabilities during partial and full site failover

The network extension appliance will be deployed to the tenant environment. Skip this if you are already using a 3rd party solution like VMware NSX Edge to manage networking during failover.

< Previous

Next >

Finish

Cancel

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:
 - 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.
 - 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](#).

New Tenant

Network Extension
Specify network settings to be used during failover.

Tenant

Bandwidth

Backup Resources

Replica Resources

Network Extension

Apply

Summary

Network extension appliances:

Name	IP address
▶ Network Extension Appliance Omega Company(...	

Edit

☒ Allocate 1 public IPv4 addresses

☒ Allocate 1 public IPv6 addresses

Public IP addresses are required for tenants to be able to perform full site failover.

[Manage...](#)

< Previous Apply Finish Cancel

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**.

New Tenant

Network Extension
Specify network settings to be used during failover.

Tenant
Bandwidth
Backup Resources
Replica Resources
Network Extension
Apply
Summary

Network extension appliances:

Name	IP address

Network Settings

IPv4 IPv6

☒ Enable IPv4 interface

☐ Obtain an IP address automatically

☒ Use the following IP address

IP address: 172 . 17 . 52 . 11

Subnet mask: 255 . 255 . 254 . 0

Default gateway: 172 . 17 . 52 . 1

OK Cancel

☒ Allocate 1 public IPv4 addresses

☒ Allocate 1 public IPv6 addresses

Public IP addresses are required for tenants to be able to perform full site failover. [Manage...](#)

< Previous Apply Finish Cancel

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.

New Tenant



Apply
Please wait while settings are being saved to the configuration database, and required changes are being made to the virtual infrastructure.

Tenant

Bandwidth

Backup Resources

Replica Resources

Network Extension

Apply

Summary

Log:

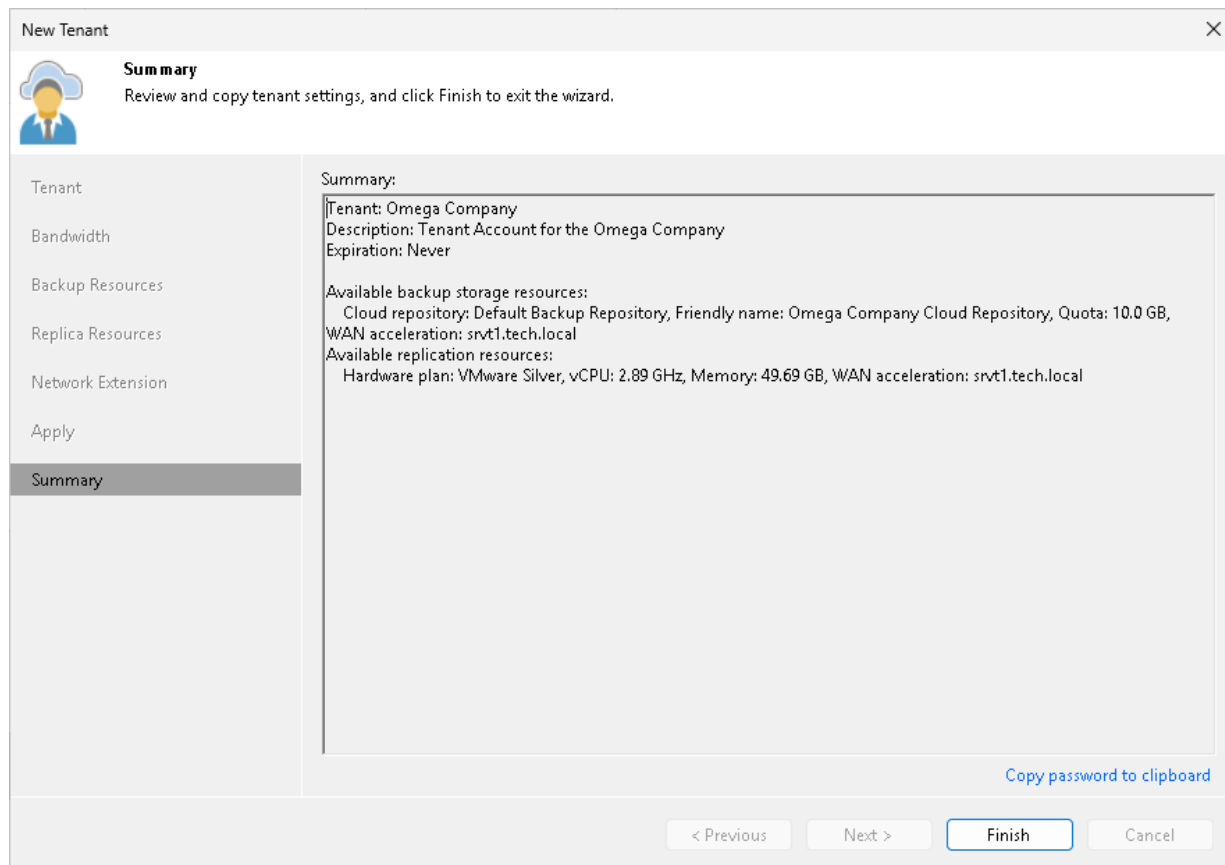
Message	Duration
✓ Hardware quotas processing for tenant Omega Company started at 10...	
✓ Subscribing tenant to hardware plan VMware Silver	0:00:08
✓ Tenant resource pool and VM folder for hardware plan VMware Silver ...	0:00:04
✓ Tenant storage created for plan VMware Silver	0:00:03
✓ 2 tenant networks added to hardware plan VMware Silver	
✓ Hardware quotas processing for tenant Omega Company finished at 1...	
✓ Deploying network extension appliance for plan VMware Silver	0:02:10

< Previous Next > Finish Cancel

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:
 - 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.
 - 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 120 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 15-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 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

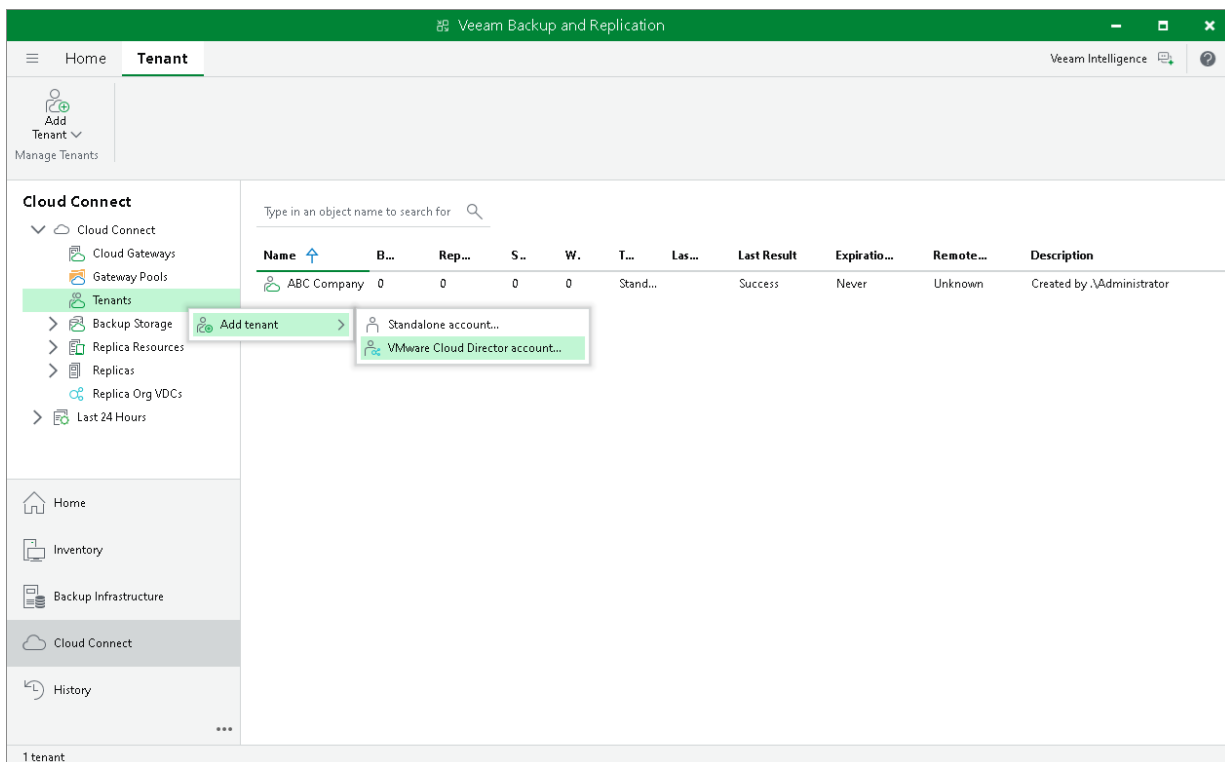
Before you add a new VMware Cloud Director tenant account, check the following prerequisites and limitations:

- 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 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 Replication 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.

The screenshot shows the 'New Tenant' wizard window with the 'Organization' step selected. The window has a title bar 'New Tenant' and a close button 'X'. Below the title bar is a header section with a user icon and the title 'Organization' followed by the instruction 'Specify VMware Cloud Director organization, assigned cloud resource types.'.

The main content area is divided into two parts. On the left is a sidebar with a list of steps: 'Organization' (highlighted), 'Bandwidth', 'Backup Resources', 'Replica Resources', 'Apply', and 'Summary'. On the right is the configuration area for the 'Organization' step. It contains two fields: 'Organization:' with the value 'TechCompanyOrg' and a 'Choose...' button, and 'Description:' with a text area containing 'Created by .\Administrator at 10/27/2025 10:45 AM.'.

Below these fields is the 'Assigned resources' section, which contains two checked checkboxes: 'Backup storage (cloud repository for off-site backup)' and 'Replica resources (cloud infrastructure for disaster recovery)'.

At the bottom of the window are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

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](#).

New Tenant

Bandwidth
Specify maximum number of task slots available to this tenant and if desired, limit incoming network traffic from this tenant.

Organization

Bandwidth

Backup Resources

Replica Resources

Apply

Summary

Max concurrent tasks:
2

Each task slot allows processing of a single disk, so tenants with one slot assigned will not be able to leverage parallel processing, or run multiple jobs concurrently. This setting applies to direct mode transfers only (WAN accelerators process disks sequentially).

☒ Limit network traffic from this tenant to:
10 MB/s

Defines maximum allowed incoming network traffic rate for the tenant. If the tenant exceeds the assigned limit, the traffic will be throttled to the specified value.

Gateway pool:
Cloud gateway pool 1

Choose...

< Previous Next > Finish Cancel

Assigning Cloud Gateway Pools

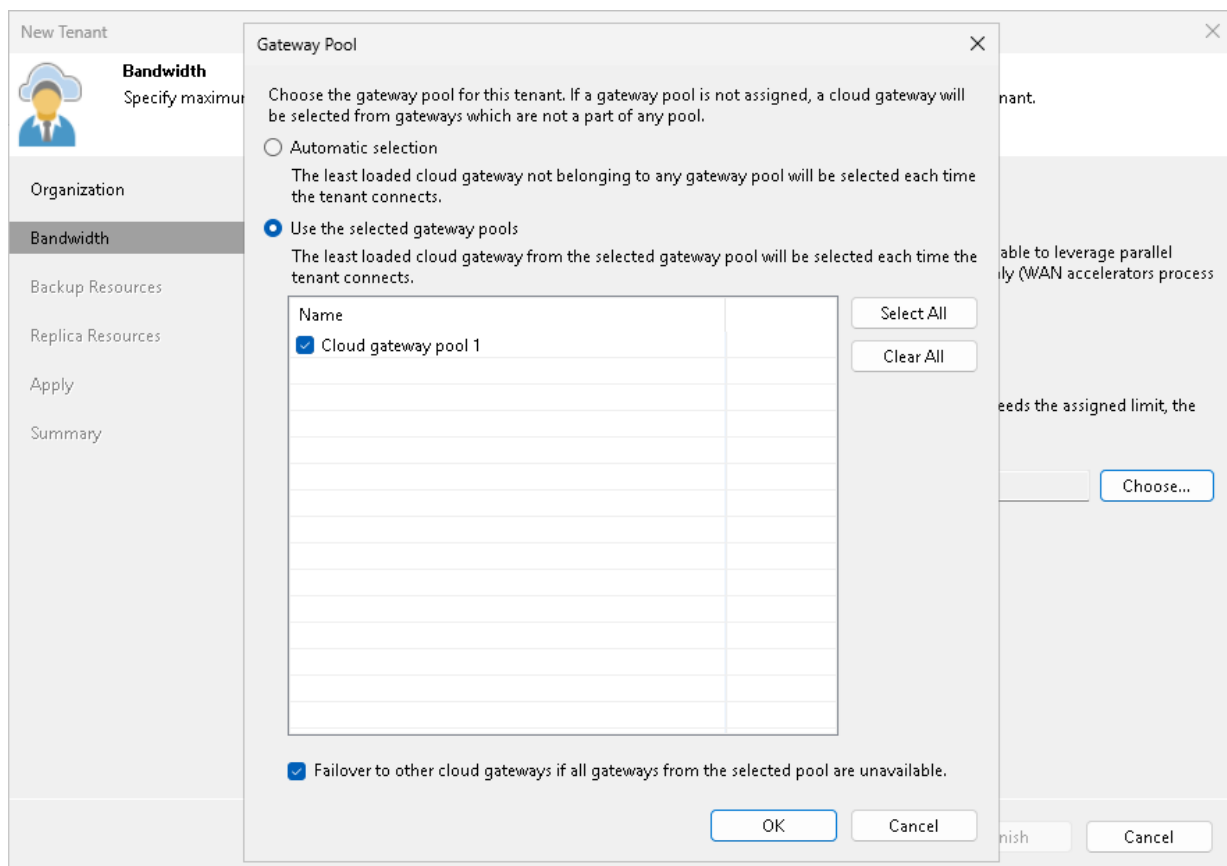
You can assign to the tenant one or more cloud gateway pools configured in the Veeam Cloud Connect infrastructure. After you assign a cloud gateway pool to the tenant, communication between the tenant backup server and Veeam Cloud Connect infrastructure components in the SP side will be possible only 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 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. [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.

New Tenant



Backup Resources
Add one or more cloud repositories for this tenant to use.

Organization

Bandwidth

Backup Resources

Replica Resources

Apply

Summary

Cloud repository name:
TechCompany Cloud Vol

Specify a friendly repository name that will be shown to the user.

Backup repository:
Default Backup Repository (Created by Veeam Backup)

160.1 GB free of 250 GB

User quota:
100 GB

☐ Enable WAN acceleration through the following WAN accelerator:

OK

Cancel

able WAN

Add...

Edit...

Remove

For added tenant protection against insider attacks, we will preserve all deleted backup files for the set number of days. The deleted backups will not count towards tenant's quota consumption, and cannot be managed by the tenant.

< Previous

Next >

Finish

Cancel

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 the tenant 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.

New Tenant

Replica Resources
Specify organization VDC for this tenant to use.

Organization

Bandwidth

Backup Resources

Replica Resources

Network Extension

Apply

Summary

Organization VDC:

Name	WAN
TechCompanyOrgVDC	Not set

Add...

Edit...

Remove

☒ Use Veeam network extension capabilities during partial and full site failover
The network extension appliance will be deployed to the tenant environment. Skip this if you are already using a 3rd party solution like VMware NSX Edge to manage networking during failover.

< Previous

Next >

Finish

Cancel

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.

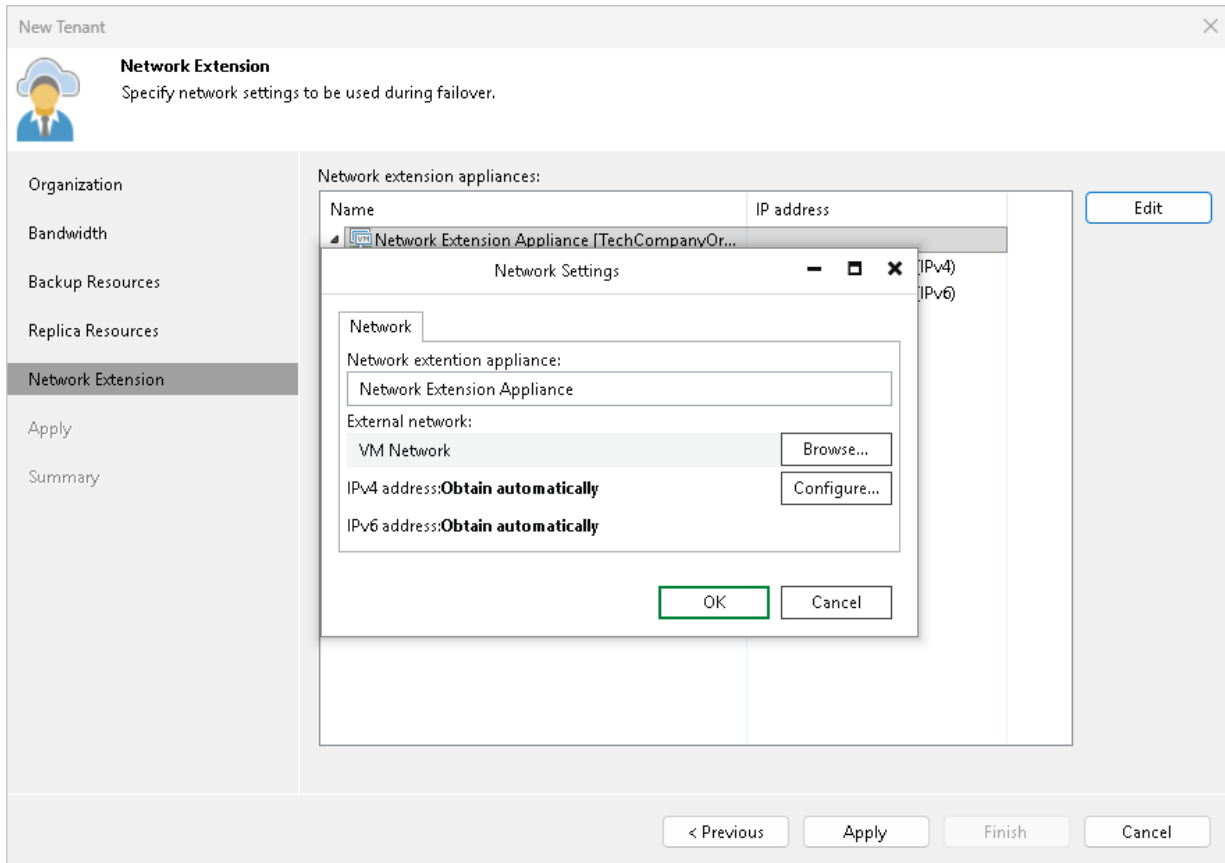
Veeam Backup & Replication deploys the SP network extension appliance in the organization VDC specified as a target for tenant VM replicas. VM replicas on the cloud host will use the SP network extension appliance to communicate to VMs in the production site after partial site failover.

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:
 - 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.
 - 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.

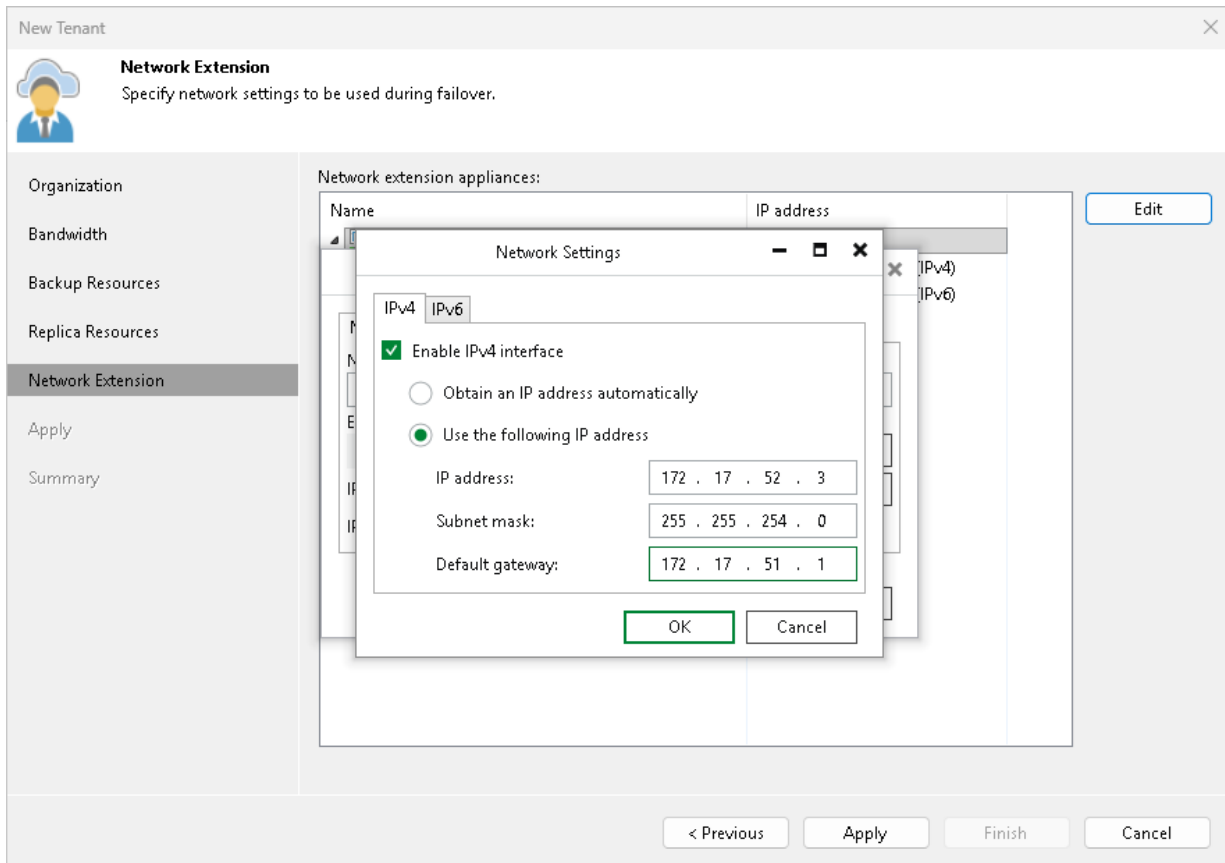
3. If you want to assign an IPv6 address to the appliance, do the following:
 - a. Click the **IPv6** tab.
 - b. Make sure that the **Enable IPv6 interface** check box is selected.
 - c. Select the **Use the following IP address** option and specify the following network settings:

- 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.

New Tenant



Apply

Please wait while settings are being saved to the configuration database, and required changes are being made to the virtual infrastructure.

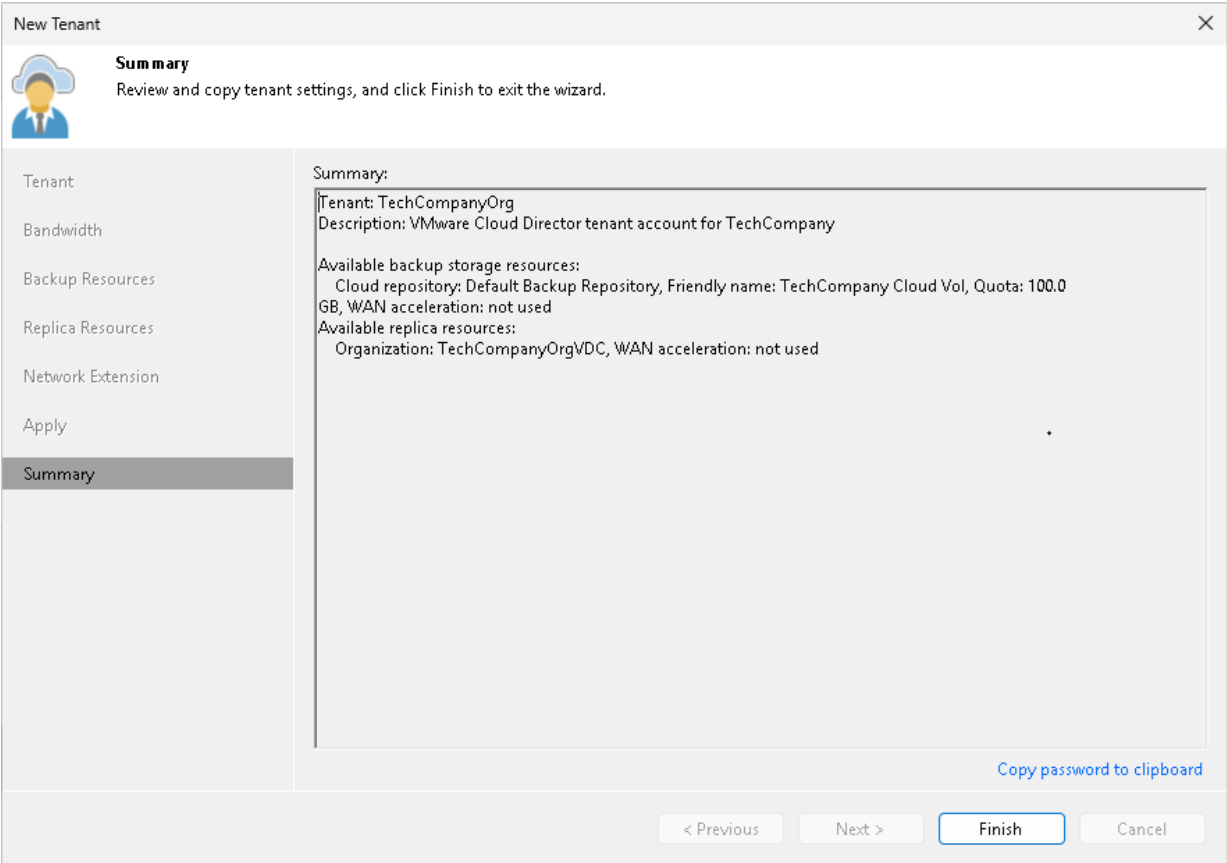
Organization	Bandwidth	Backup Resources	Replica Resources	Network Extension	Apply	Summary	
Log:							
					Message	Duration	
					✓ Hardware quotas processing for tenant TechCompanyOrg started at 1...		
					✓ Preparing tenant's subscription to VDC TechCompanyOrgVDC	0:00:09	
					✓ VDC TechCompanyOrgVDC has been prepared successfully	0:00:08	
					✓ Storage policies for VDC TechCompanyOrgVDC have been saved succ...		
					✓ Networks for VDC TechCompanyOrgVDC have been saved successfully		
					✓ Hardware quotas processing for tenant TechCompanyOrg finished at ...		
					✓ Deploying network extension appliance for datacenter TechCompany...	0:05:01	

< Previous Next > Finish Cancel

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.



The screenshot shows the 'New Tenant' wizard window, specifically the 'Summary' step. The window has a title bar 'New Tenant' and a close button. Below the title bar is a 'Summary' section with a wizard icon and the text 'Review and copy tenant settings, and click Finish to exit the wizard.' On the left is a sidebar with navigation links: 'Tenant', 'Bandwidth', 'Backup Resources', 'Replica Resources', 'Network Extension', 'Apply', and 'Summary' (which is highlighted). The main area displays the following summary information:

Summary:

- Tenant: TechCompanyOrg
- Description: VMware Cloud Director tenant account for TechCompany
- Available backup storage resources:
 - Cloud repository: Default Backup Repository, Friendly name: TechCompany Cloud Vol, Quota: 100.0 GB, WAN acceleration: not used
- Available replica resources:
 - Organization: TechCompanyOrgVDC, WAN acceleration: not used

At the bottom right of the main area is a link 'Copy password to clipboard'. At the bottom of the window are four buttons: '< Previous', 'Next >', 'Finish' (highlighted with a blue border), and 'Cancel'.

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.
 - 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.

- 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 120 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 15-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

The screenshot shows the 'New Tenant' wizard in Veeam Cloud Connect. The 'Backup Resources' step is active, showing a list of resources on the left: Tenant, Bandwidth, Backup Resources (selected), Replica Resources, Network Extension, Apply, and Summary. The main area displays 'Backup Resources' with the instruction 'Add one or more cloud repositories for this tenant to use.' A 'Set Quota' dialog box is open, showing the following fields:

- Cloud repository name:** ABC Company Cloud Repository
- Specify a friendly repository name that will be shown to the user.**
- Backup repository:** Default Backup Repository (Created by Veeam Backup)
- 27.6 GB free of 89.1 GB**
- User quota:** 10 GB
- ☒ **Enable WAN acceleration through the following WAN accelerator:** srvt1.tech.local (Target WAN Accelerator for Veeam Cloud Connect)

Buttons for 'OK' and 'Cancel' are at the bottom of the dialog. Below the dialog, a note states: 'For added tenant protection against insider attacks, we will preserve all deleted backup files for the set number of days. The deleted backups will not count towards tenant's quota consumption, and cannot be managed by the tenant.'

At the bottom of the wizard, there are buttons for '< Previous', 'Next >', 'Finish', and 'Cancel'.

- For replication jobs targeted at the cloud host

New Tenant

Replica Resources
Add one or more hardware plans for this tenant to use.

Tenant

Bandwidth

Backup Resources

Replica Resources

Network Extension

Apply

Summary

Hardware plans:

Name	CPU	Memory	Storage	Networks	WAN

Add...

Edit...

Remove

Add replication resource

Select hardware plan:

VMware Silver

☒ Enable WAN acceleration through the following WAN accelerator:

srx11.tech.local

OK Cancel

[Manage network settings](#)

☒ Use Veeam network extension capabilities during partial and full site failover
The network extension appliance will be deployed to the tenant environment. Skip this if you are already using a 3rd party solution like VMware NSX Edge to manage networking during failover.

< Previous Next > Finish Cancel

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 cloud host can use WAN acceleration, the tenant can configure a source WAN accelerator on the tenant side and create backup copy and 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.

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.

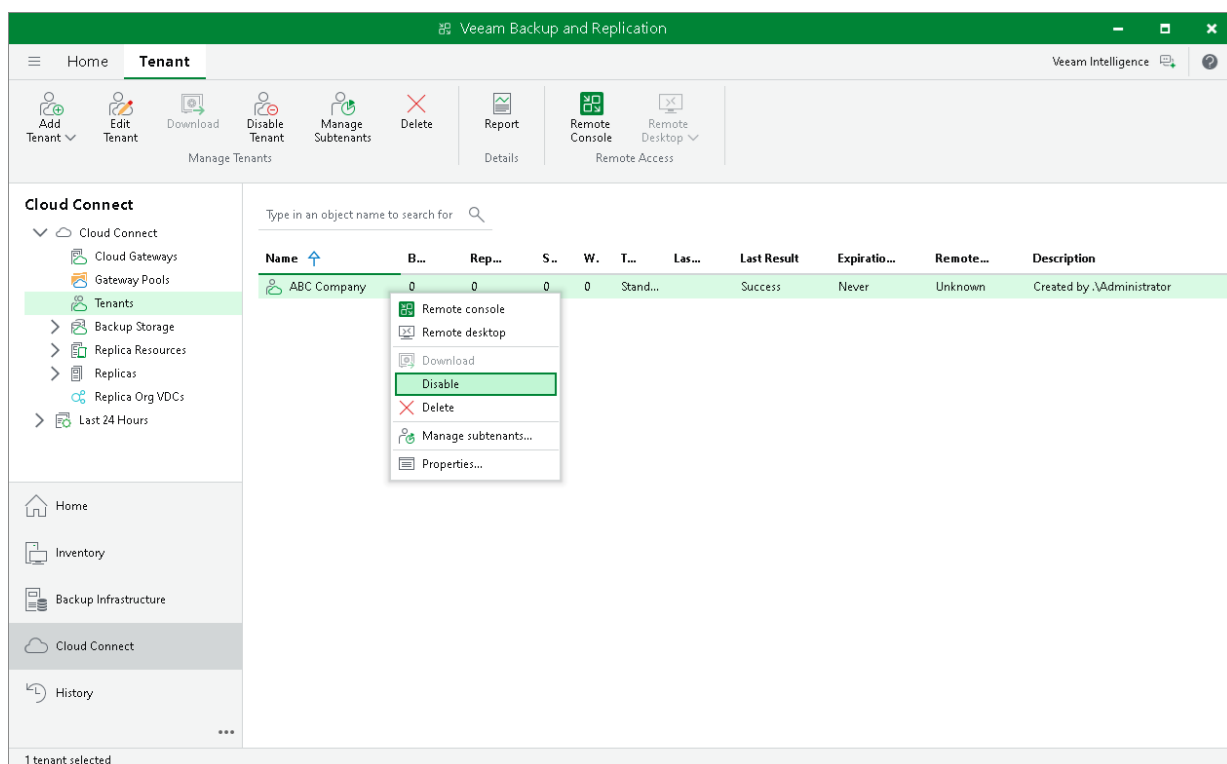
When the SP disables a tenant account, the tenant can no longer perform the following operations:

- 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 tenant account that you want to disable 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 tenant account that you want to enable and click **Disable Tenant** on the ribbon once again. You can also right-click the account in the working area and select **Disable**.

The screenshot shows the Veeam Backup and Replication interface with the 'Tenant' ribbon selected. The ribbon contains buttons for 'Add Tenant', 'Edit Tenant', 'Download', 'Disable Tenant', 'Manage Subtenants', 'Delete', 'Report', 'Remote Console', and 'Remote Desktop'. The 'Disable Tenant' button is highlighted. Below the ribbon, the 'Cloud Connect' section is visible, showing a list of tenants. The 'Tenants' section is expanded, and a context menu is open over the 'ABC Company' tenant, with the 'Disable' option highlighted.

Name	B...	Rep...	S...	W...	T...	Las...	Last Result	Expiratio...	Remote...	Description
ABC Company	0	0	0	0	Stand...		Success	Never	Unknown	Created by \Administrator

1 tenant selected

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.

The maximum length of the user name is 128 characters. To avoid problems with long paths to backup files on the cloud repository, it is recommended to create user names not longer than 50 characters.
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.

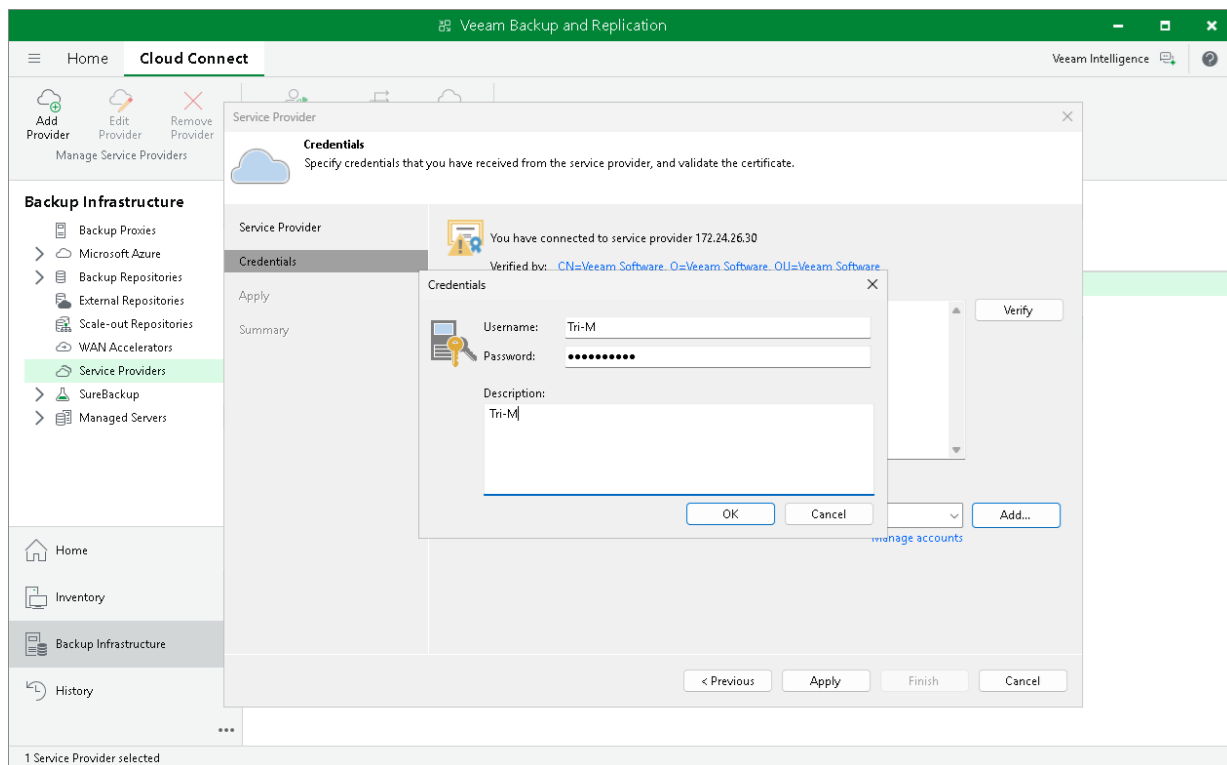
7. Inform the tenant about the user name change and make sure that the tenant reconnects to the SP under this name.

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.

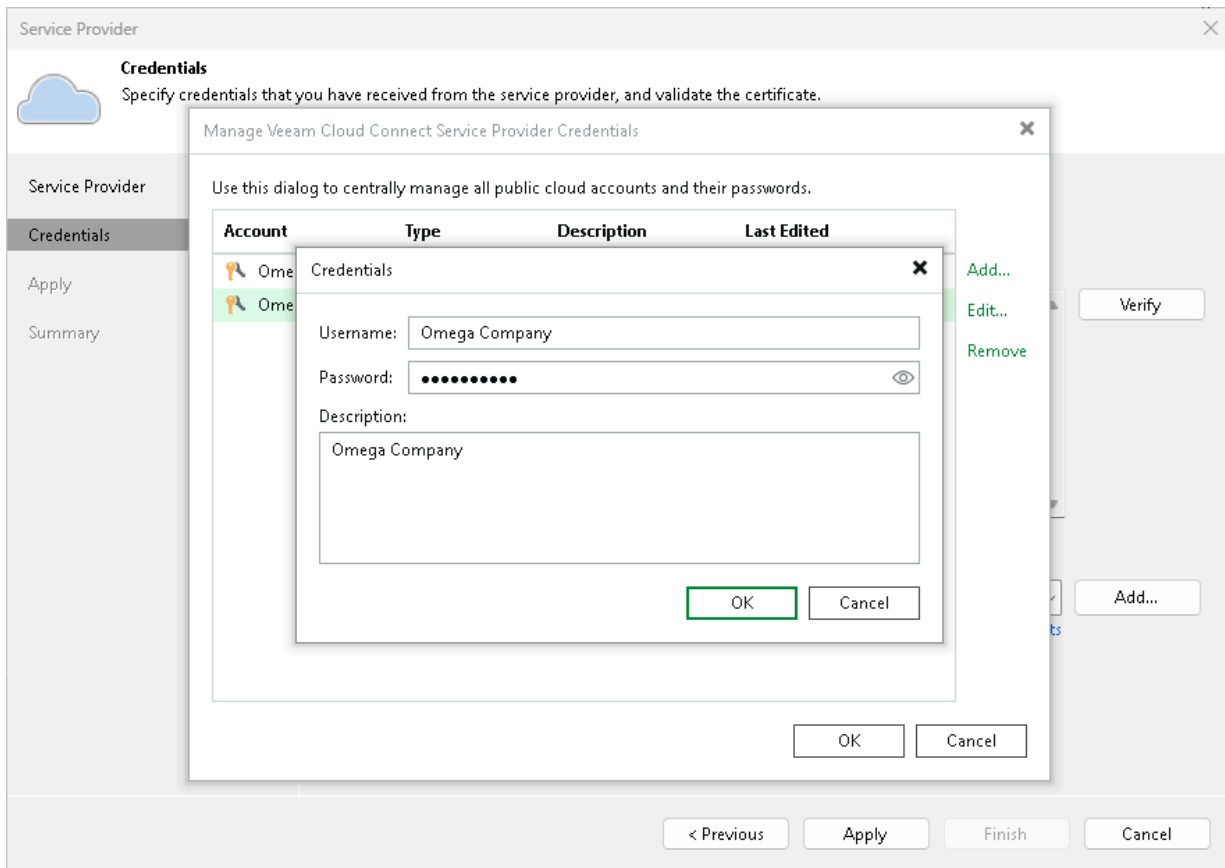
To change a password for the tenant account (performed by the SP on the SP Veeam backup server):

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:
 - **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](#).
 - **Replication resources** – with this option enabled, you can subscribe the tenant to a hardware plan. To learn more, see [Allocate Replication 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.

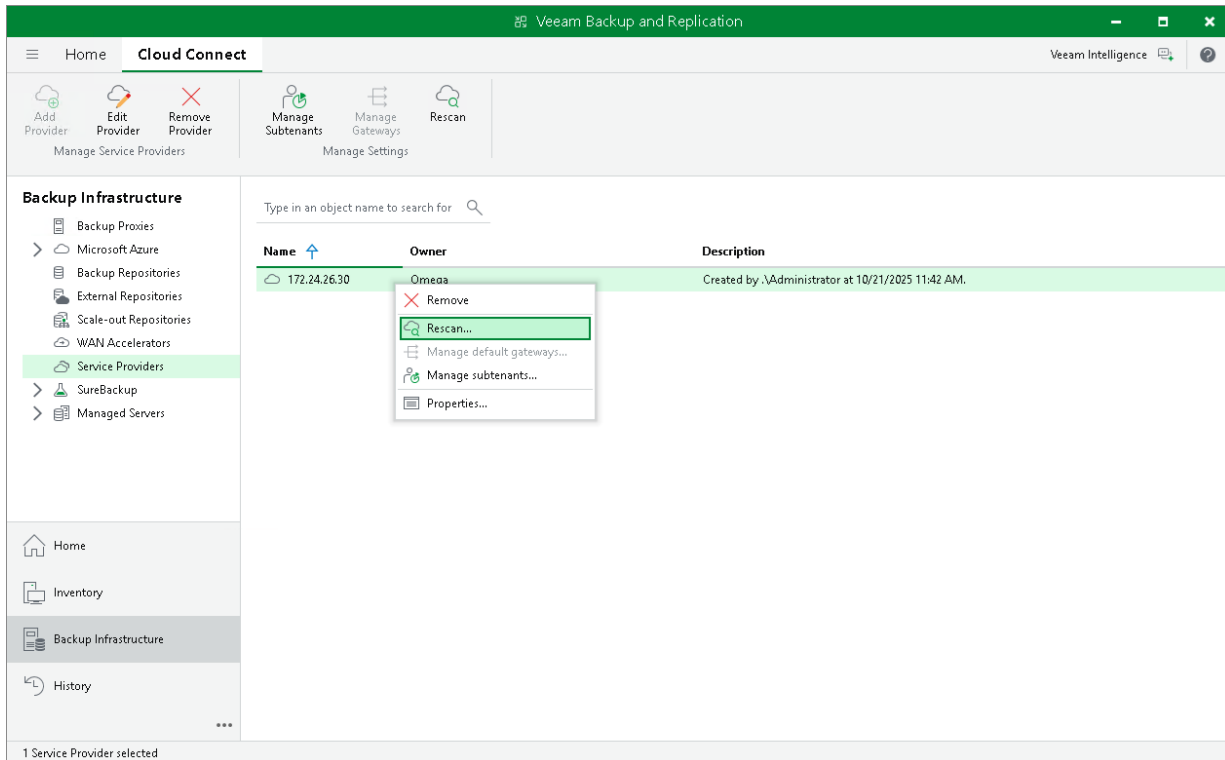
This operation is also required in case the SP assigned replication resources to the tenant, and the tenant wants to configure and deploy the network extension appliance. Alternatively, the tenant can rescan the SP. In this case, Veeam Backup & Replication will prompt to deploy the network extension 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**.

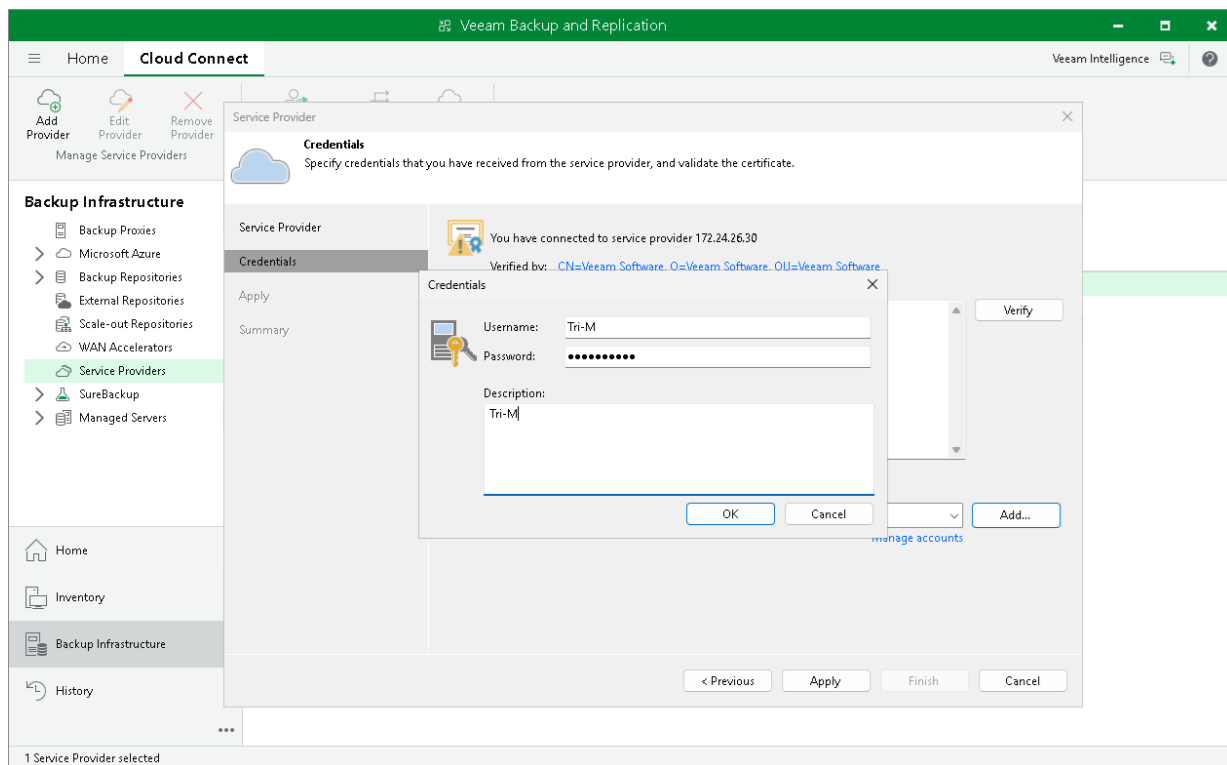


To reconnect to the SP (performed by the tenant on the tenant Veeam backup server):

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](#).

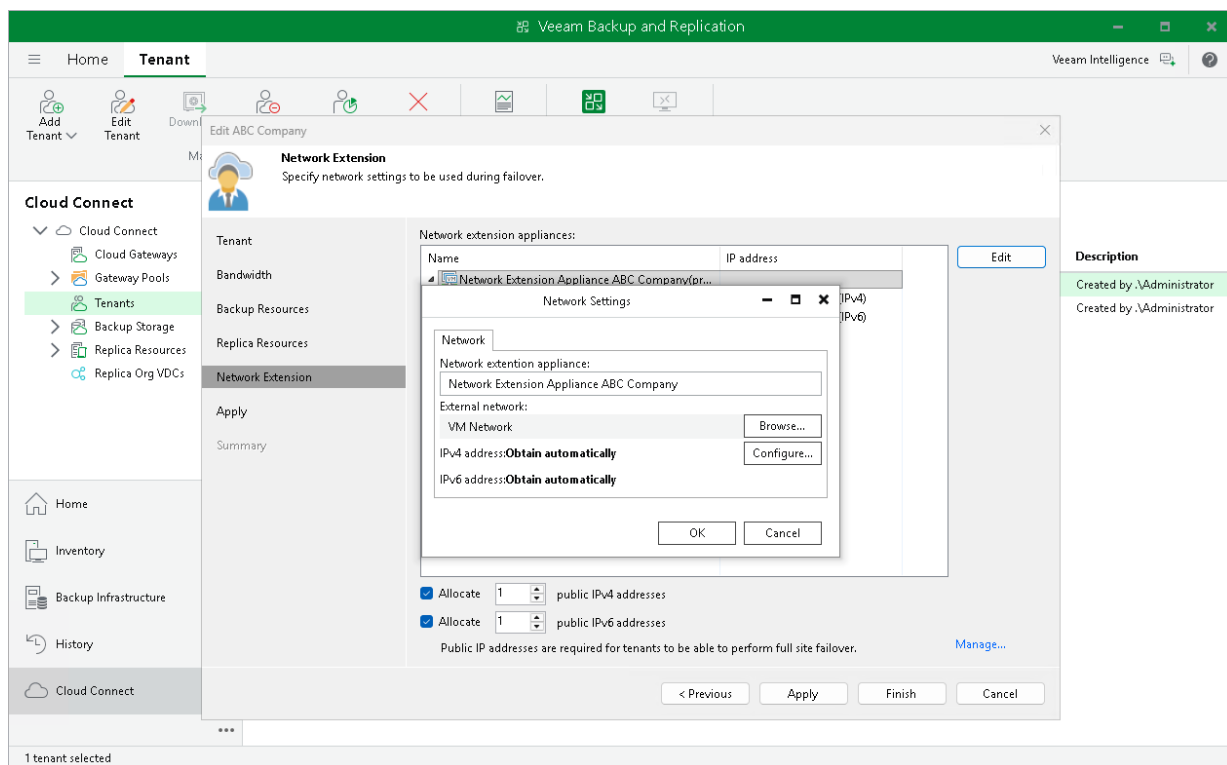


Redeploying Network Extension Appliance

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* 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.
- **Last Active** – time since the latest backup job session, replication job session or restore session was completed.
- **Last Result** – information about the result of the latest session: *Success*, *Warning* or *Failed*.

- **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.

Name	Backups	Replicas	Servers	Worksta...	Type	Last A...	Last R...	Expira...	Rem...	Description
ABC Company	0	0	0	0	Standalone		Success	Never	Unknown	Created by .\Administrator
Omega	0	0	0	0	Standalone		Success	Never	Unknown	Created by .\Administrator

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 **Delete 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 Machine Count](#).

Veeam Backup and Replication

HomeTenantVeeam Intelligence

Add Tenant

Edit Tenant

Download

Disable Tenant

Manage Subtenants

Delete

Report

Remote Console

Remote Desktop

Manage Tenants

Details

Remote Access

Cloud Connect

Cloud Connect

Cloud Gateways

Gateway Pools

Tenants

Backup Storage

Replica Resources

Replicas

Replica Org VDCs

Last 24 Hours

Home

Inventory

Backup Infrastructure

Cloud Connect

History

Type in an object name to search for

Name	B...	Rep...	S...	W...	T...	Las...	Last Result	Expiratio...	Remote...	Description
ABC Company	0	0	0	0	Stand...		Success	Never	Unknown	Created by \Administrator
Omega				0	VMw...	1 day a...	Success	Never	Unknown	Created by \Administrator

Remote console

Remote desktop

Download

Disable

Delete

Manage subtenants...

Properties...

1 tenant selected

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.](#)

Creating Subtenant Account for Standalone Tenant

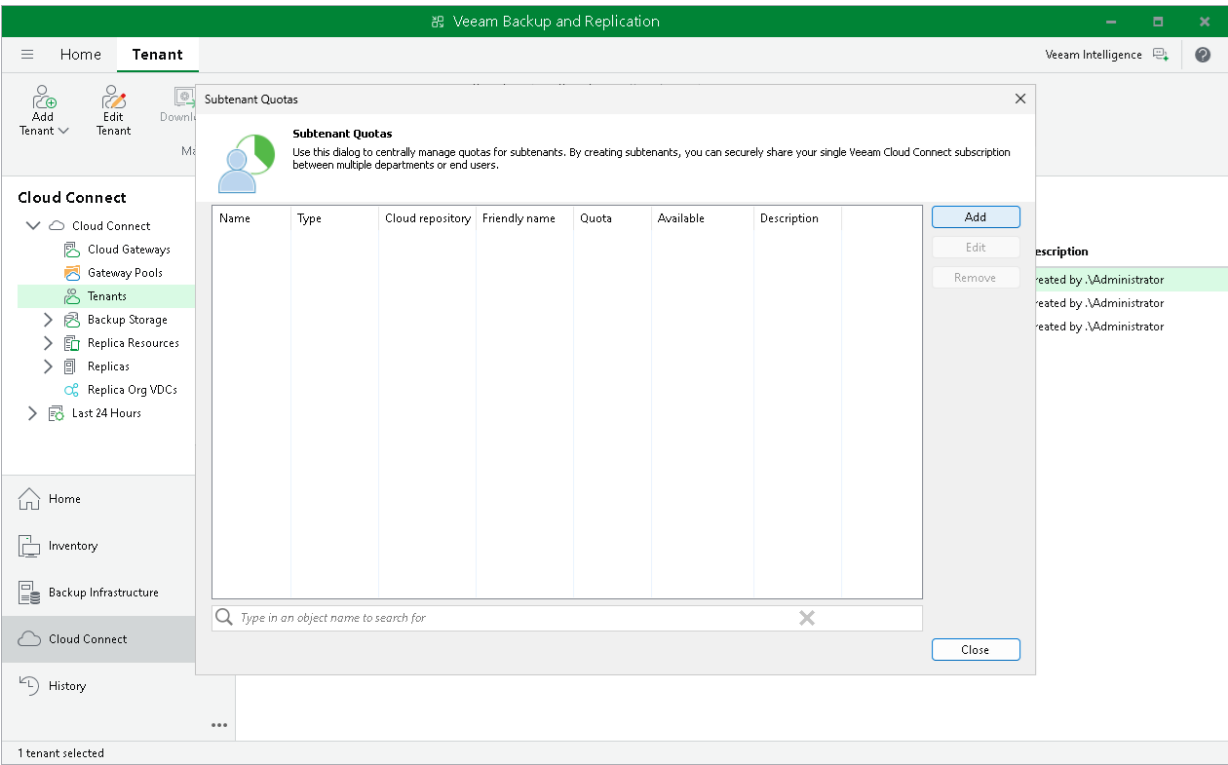
The procedure of subtenant accounts registration can be performed by the SP on the SP Veeam backup server.

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:

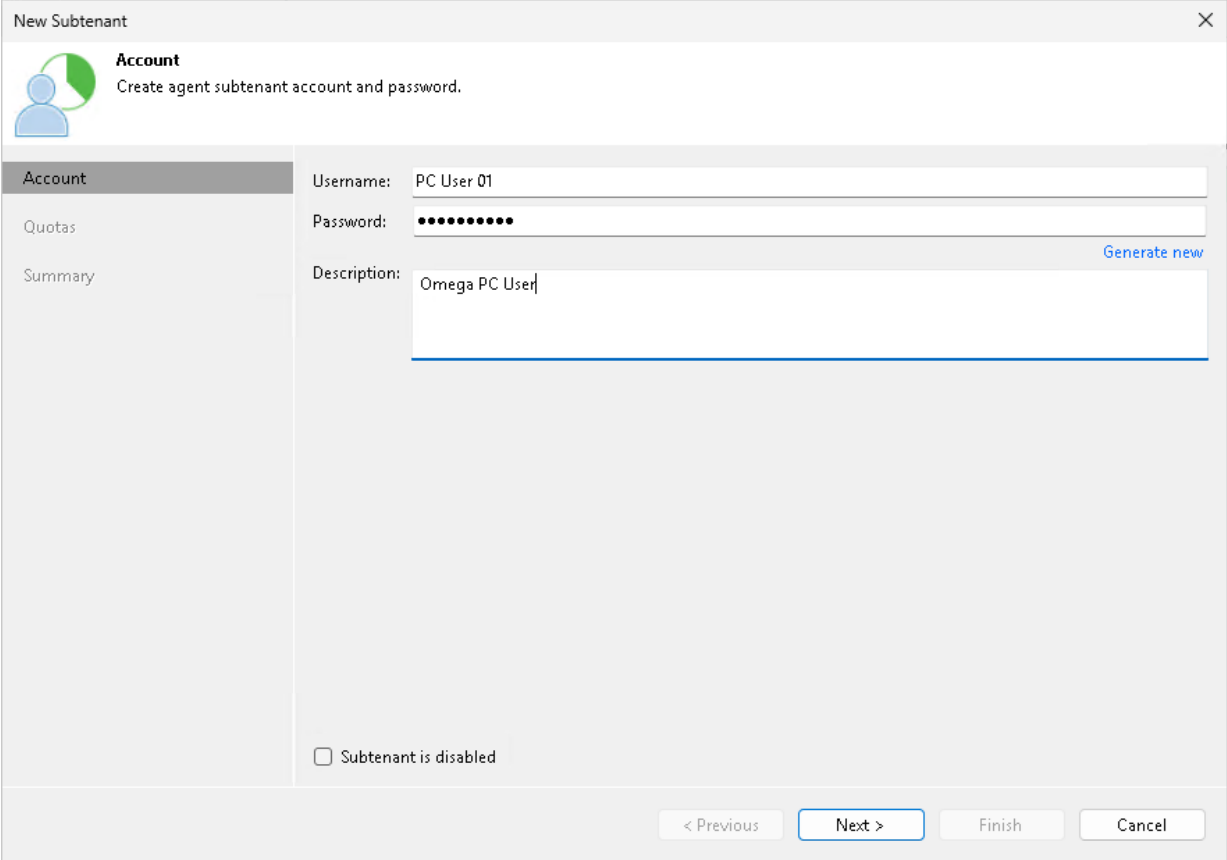
- 1. Open the **Cloud Connect** view.
- 2. In the inventory pane, click the **Tenants** node.
- 3. In the working area, select the necessary tenant and click **Manage Subtenants** on the ribbon or right-click the tenant and select **Manage subtenants**.
- 4. In the **Subtenant Quotas** window, click **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. To avoid problems with long paths to backup files on the cloud repository, it is recommended to create user names not longer than 50 characters.
 - 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.



The screenshot shows the 'New Subtenant' wizard window, specifically the 'Account' step. The window title is 'New Subtenant' with a close button (X) in the top right corner. Below the title bar, there is a header section with a user icon and the text 'Account' and 'Create agent subtenant account and password.' Below this, there is a sidebar with three items: 'Account' (selected), 'Quotas', and 'Summary'. The main area contains three input fields: 'Username' with the value 'PC User 01', 'Password' with masked characters and a 'Generate new' link to its right, and 'Description' with the value 'Omega PC User'. At the bottom left of the main area, there is a checkbox labeled 'Subtenant is disabled'. At the bottom right, there are four buttons: '< Previous', 'Next >' (highlighted with a blue border), 'Finish', and 'Cancel'.

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 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**.

The screenshot shows the 'New Subtenant' wizard at the 'Quotas' step. The main window has a sidebar with 'Account', 'Quotas', and 'Summary'. The 'Quotas' section is active, showing a list of 'Available user quotas' with an 'Add' button. A 'Subtenant Quota' dialog is open, displaying the following fields:

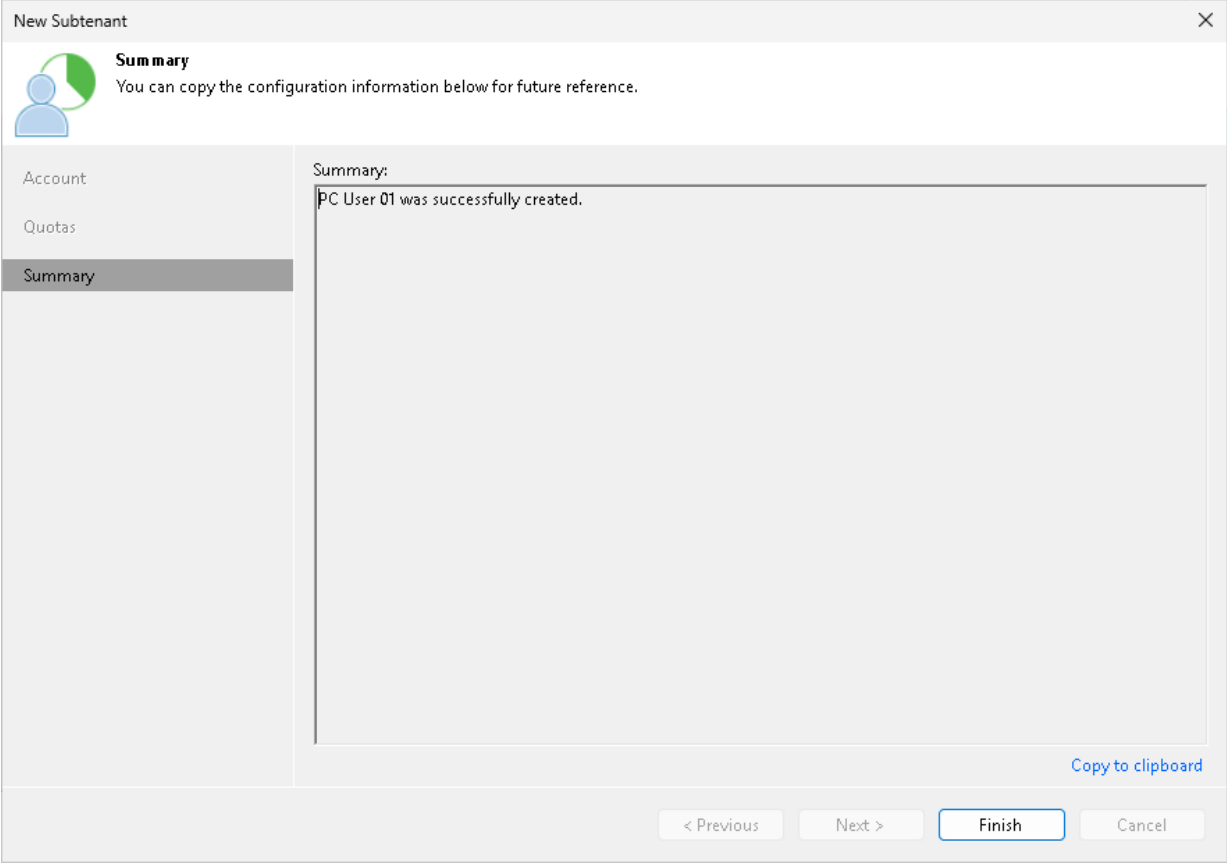
- Name:** Cloud Backup Storage
- Repository:** Omega Cloud Repository (Tenant's quota)
- Quota:** ☒ Limit size to: 5 GB

The dialog also shows '10 GB free of 10 GB' and buttons for 'OK' and 'Cancel'. The background window has buttons for '< Previous', 'Next >', 'Finish', and 'Cancel'.

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.



The screenshot shows a window titled "New Subtenant" with a close button (X) in the top right corner. On the left is a sidebar with three items: "Account", "Quotas", and "Summary", with "Summary" selected and highlighted. The main area has a header with a green circular progress indicator and the title "Summary". Below the title is the text: "You can copy the configuration information below for future reference." The main content area contains a text box with the text "Summary:" followed by "PC User 01 was successfully created." In the bottom right of the main area is a blue link that says "Copy to clipboard". At the bottom of the window is a navigation bar with four buttons: "< Previous", "Next >", "Finish" (which is highlighted with a blue border), and "Cancel".

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.

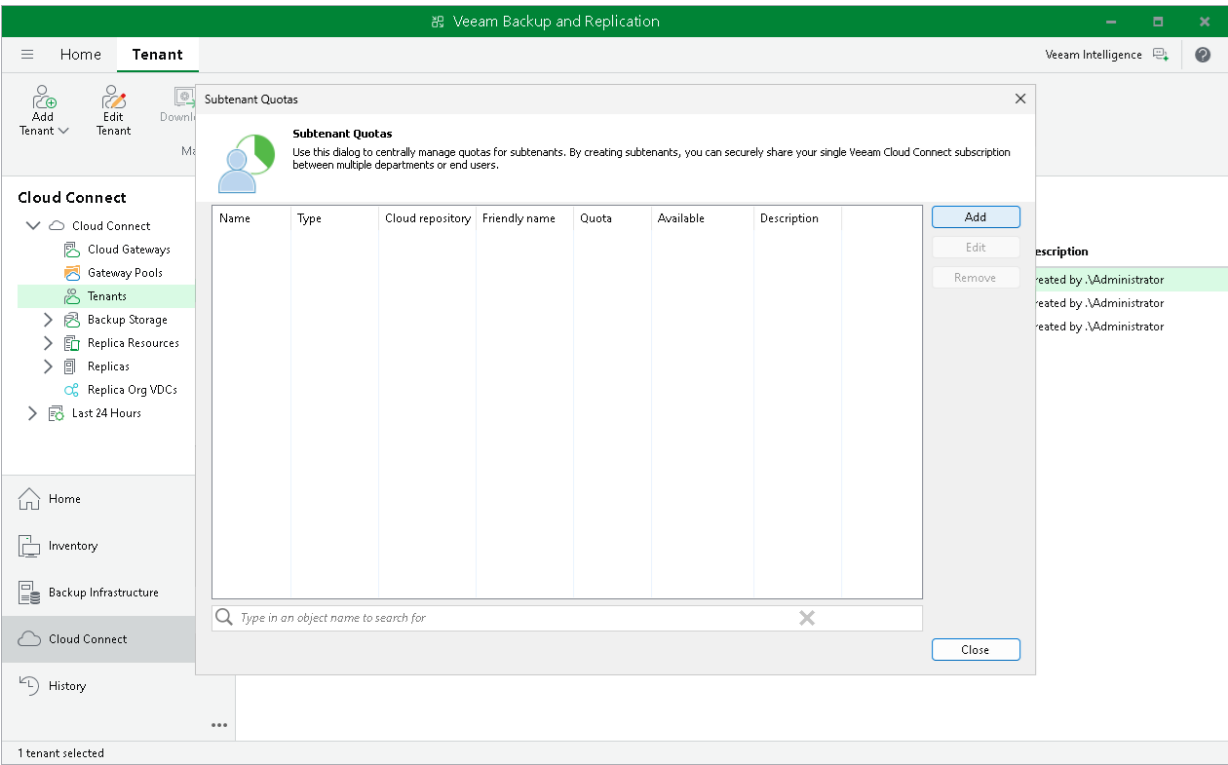
Before You Begin

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:

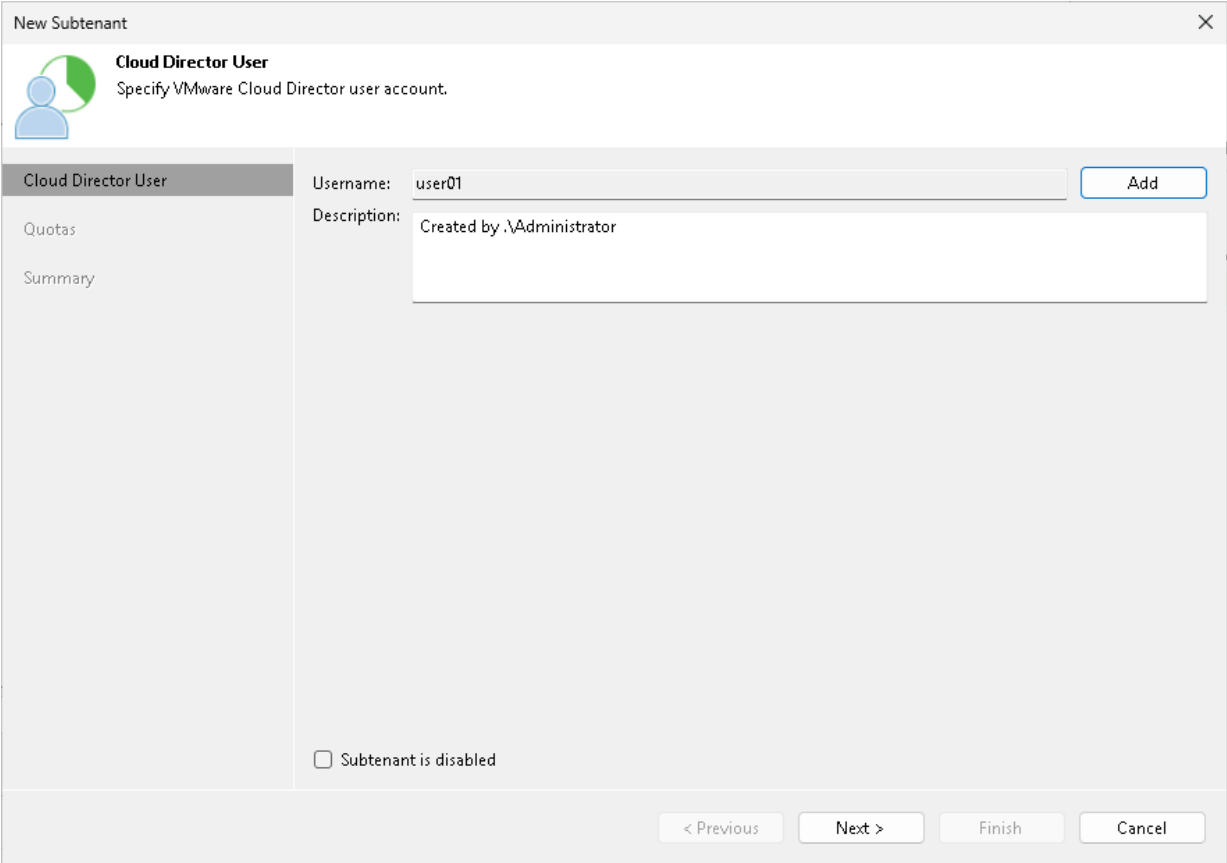
- 1. Open the **Cloud Connect** view.
- 2. In the inventory pane, click the **Tenants** node.
- 3. In the working area, select the necessary tenant and click **Manage Subtenants** on the ribbon or right-click the tenant and select **Manage subtenants**.
- 4. In the **Subtenant Quotas** window, click **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.



The screenshot shows the 'New Subtenant' wizard window. The title bar says 'New Subtenant' with a close button. The main header area has a green and blue icon, the title 'Cloud Director User', and the subtitle 'Specify VMware Cloud Director user account.' Below this is a sidebar with 'Cloud Director User' (selected), 'Quotas', and 'Summary'. The main content area has a 'Username:' field with 'user01' and an 'Add' button. Below it is a 'Description:' field with the text 'Created by .\Administrator'. At the bottom left, there is a checkbox labeled 'Subtenant is disabled'. At the bottom right, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

New Subtenant

Cloud Director User
Specify VMware Cloud Director user account.

Cloud Director User

Username: user01 **Add**

Description: Created by .\Administrator

☐ Subtenant is disabled

< Previous Next > Finish Cancel

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 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**.

The screenshot shows the 'New Subtenant' wizard at the 'Quotas' step. The main window has a sidebar with 'Cloud Director User', 'Quotas', and 'Summary'. The 'Quotas' section is active, showing a list of available quotas and an 'Add' button. A 'Subtenant Quota' dialog box is open, allowing configuration of a new quota. The dialog has the following fields and options:

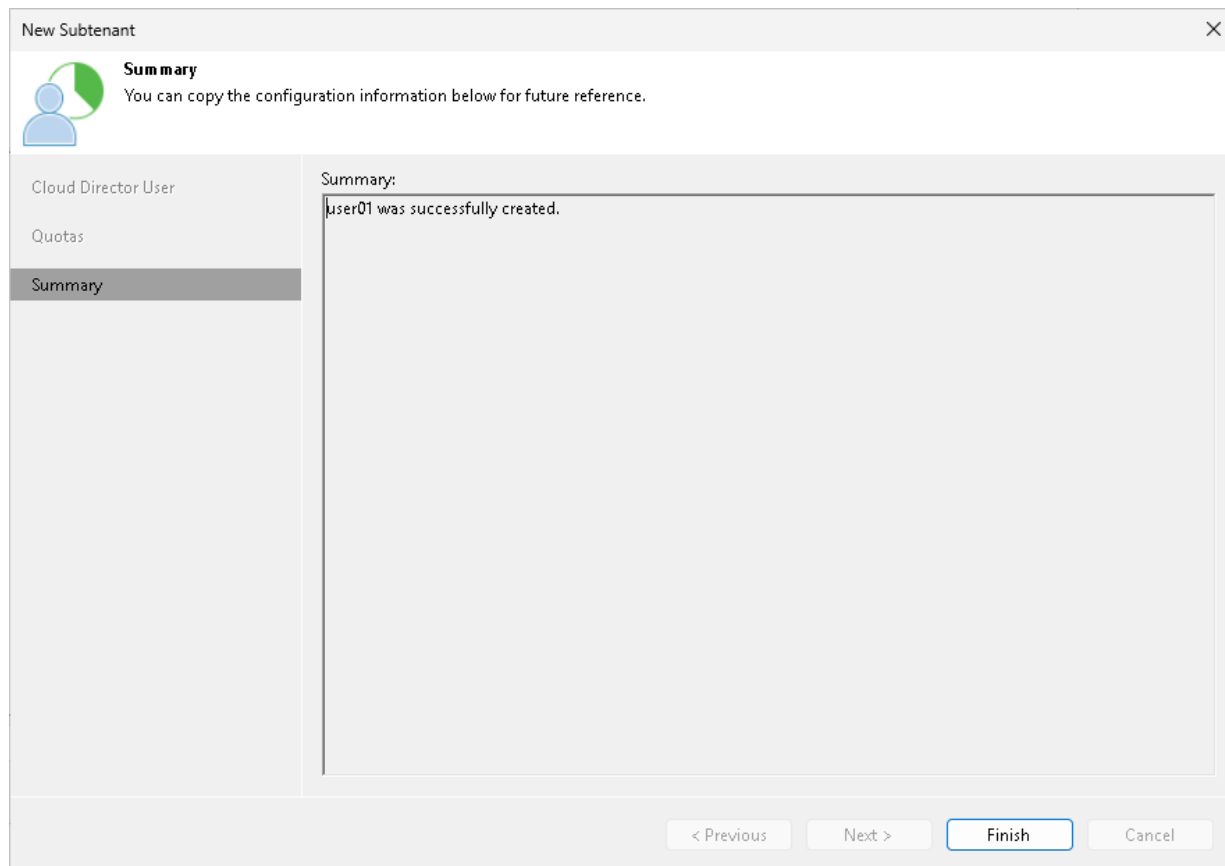
- User quota** section:
 - Name:** Cloud Backup Storage
 - Repository:** TechCompany Cloud Vol (Tenant's quota)
 - 100 GB free of 100 GB**
- Quota:** section with two radio buttons:
 - ☐ Unlimited
 - ☒ Limit size to: 50 GB
- Buttons:** OK and Cancel

The background window shows the 'Add' button and a list of available quotas. At the bottom of the wizard, there are navigation buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

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.

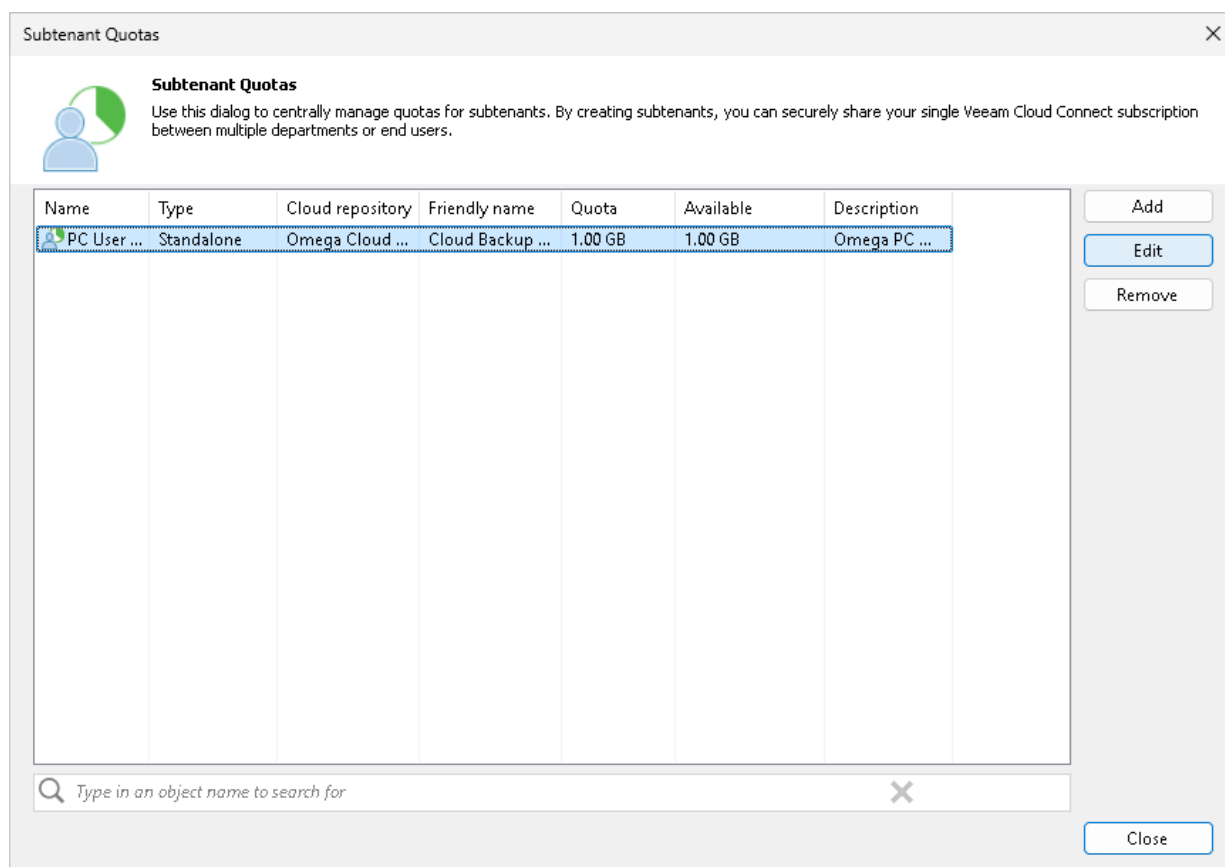
To edit settings of a subtenant account:

1. Open the **Subtenant Quotas** window in one of the following ways:
 - 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.
 - 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 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.

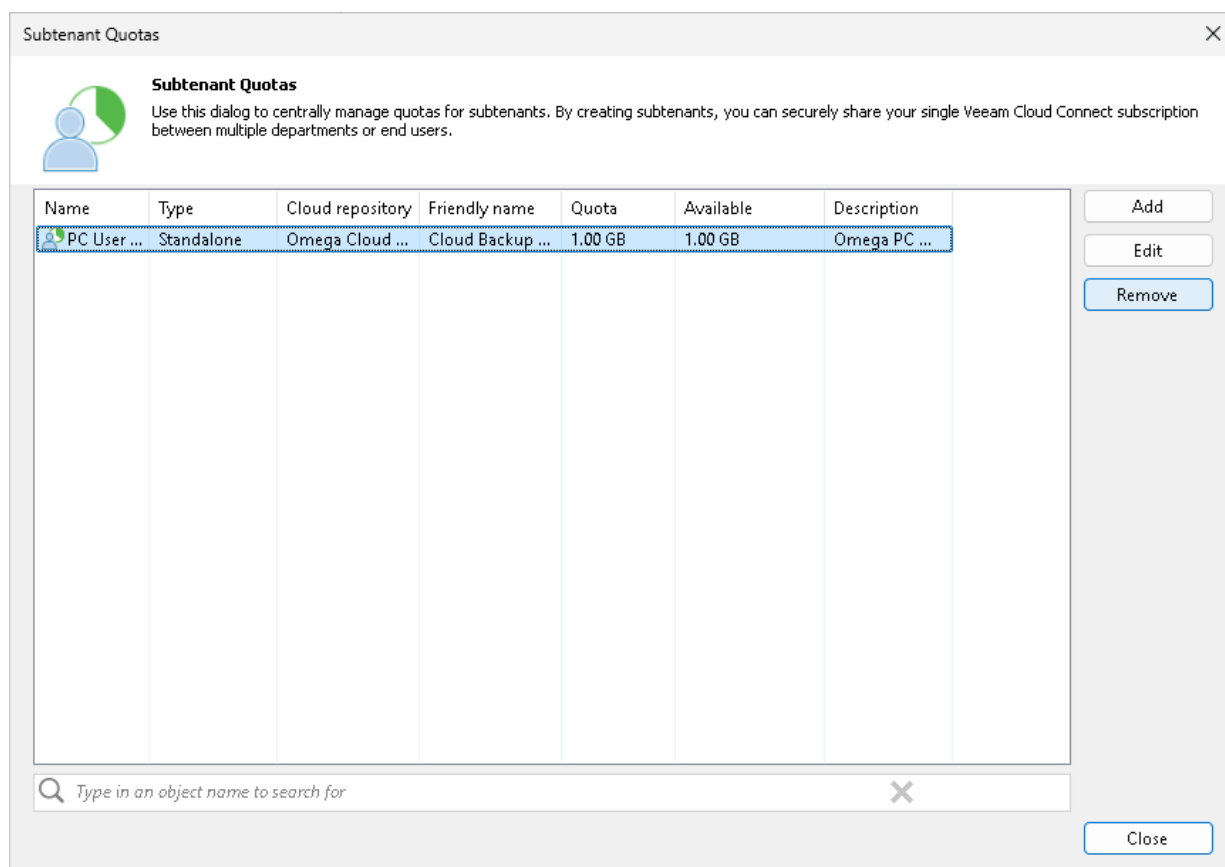
To delete a subtenant account:

1. Open the **Subtenant Quotas** window in one of the following ways:
 - 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.
 - 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]**.



Restoring Data from Tenant Backups

The SP can restore data from tenant backups that reside in the cloud repository. To use this functionality, the SP must have access to tenant backups on the SP side.

- For standalone tenant accounts, tenant backups are available on the SP side if the tenant selected 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](#).
- For data restore from backups created by Veeam Agent in the standalone mode, a tenant backup server connected to the SP with the **Allow this Veeam Backup & Replication installation to be managed by the service provider** option enabled is required.

NOTE

By default, the SP Veeam Backup & Replication console does not display encrypted tenant backups. The SP can restore encrypted tenant backups only if the tenant grants the SP restore access to all backups. For details, see [Access to Tenant Backups](#).

The set of data restore operations available on the SP side differs from the one on the tenant side. The SP can perform the following tasks:

- [Performing Entire VM Restore from Tenant Backups](#):
 - Restoring to Nutanix AHV
 - Restoring to Proxmox VE
 - Restoring to oVirt KVM
 - Restoring to Scale Computing HyperCore
 - Restoring to HPE Morpheus VM Essentials
 - [Restoring to Amazon EC2](#)
 - [Restoring to Microsoft Azure](#)
- [Performing Instant Recovery from Tenant Backups](#)
- [Disk restore](#) (using Veeam PowerShell cmdlets only)
- [Disk publishing](#) (using Veeam PowerShell cmdlets only)

Performing Entire VM Restore from Tenant Backups

The SP can restore machines from tenant backups stored in a cloud repository.

Veeam Cloud Connect supports entire VM restore from tenant backups stored in a cloud repository to the following virtualization platforms:

- Restoring to Nutanix AHV
- Restoring to Proxmox VE
- Restoring to oVirt KVM
- Restoring to Scale Computing HyperCore
- Restoring to HPE Morpheus VM Essentials

The SP can also restore machines from tenant backups stored in a cloud repository to the following public cloud environments:

- Restoring to Amazon EC2
- Restoring to Microsoft Azure

The SP can restore one VM or several VMs from the backup. A VM can be recovered to the latest state or to any valid restore point.

To restore a VM from the backup, do the following:

1. Open the **Home** view.
2. Select the **Backups** node in the inventory pane.
3. Expand the backup job in the working area, select **Entire VM** on the ribbon or right-click the necessary VM in the backup job and select **Restore entire VM**. Then select the target platform.
4. Follow the procedure steps described in the user guide.

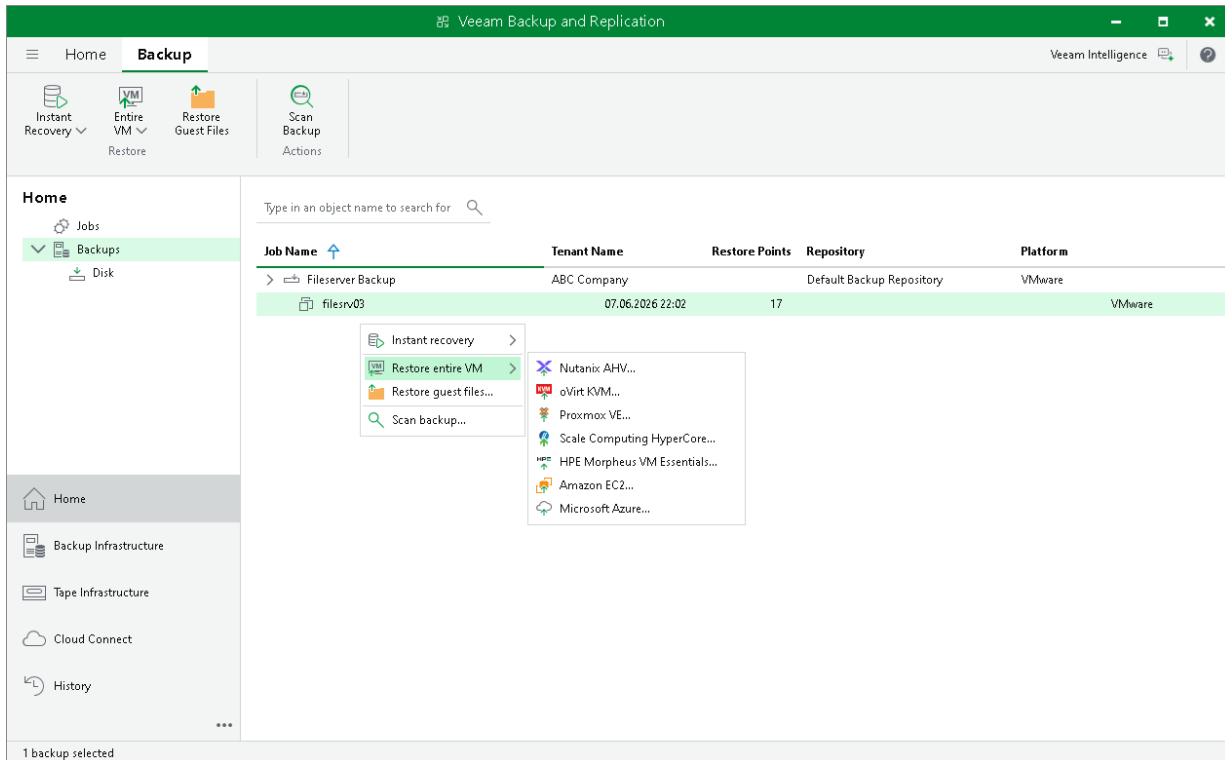
[*For virtualization platforms*] The operation does not differ from the same scenario in the regular Veeam Backup & Replication infrastructure. For details, see the following sections in the Veeam Backup & Replication User Guide:

- [Restoring to Nutanix AHV](#)
- [Restoring to Proxmox VE](#)
- [Restoring to oVirt KVM](#)
- [Restoring to Scale Computing HyperCore](#)
- [Restoring to HPE Morpheus VM Essentials](#)

[*For public cloud environments*] For details, see the following sections of this user guide:

- [Restoring to Amazon EC2](#)

- [Restoring to Microsoft Azure](#)



Restoring to Amazon EC2

The SP can restore machines from tenant backups stored in a cloud repository to a public cloud environment. This capability allows the SP to use tenant backups to recover workloads directly in Amazon Elastic Compute Cloud (Amazon EC2), rather than to the original on-premises location. As a result, the SP can offer additional data protection scenarios, such as migration if the tenant decides to permanently move from an on-premises environment to a public cloud environment.

To use this functionality, the SP 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 Veeam Agent users, consider that to display on the SP side backups created by Veeam Agent in the standalone mode, a backup server connected to the SP with the **Allow this Veeam Backup & Replication installation to be managed by the service provider** option enabled is required.

- Veeam Cloud Connect supports restore to Amazon EC2 from encrypted tenant backups only if the tenant has granted the SP restore access to all backups. Otherwise, restore to Amazon EC2 is supported from unencrypted backups only. For details, see [Access to Tenant Backups](#).
- Veeam Cloud Connect supports restore to Amazon EC2 for the following workloads:
 - Backups of VMware Cloud Director VMs created by Veeam Backup & Replication.
 - Backups of Microsoft Windows and Linux VMs created by Veeam Backup & Replication.
 - Backups of Microsoft Hyper-V virtual machines 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 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](#).
- Backups of Nutanix AHV VMs created by [Veeam Backup for Nutanix AHV](#).
- Backups of oVirt VMs created by [Veeam Backup for OLVM and RHV](#).
- Backups of Proxmox VE VMs created by [Veeam Backup for Proxmox VE](#).

This procedure description is specific for the Veeam Cloud Connect environment. This section describes only basic steps that you must take to restore a tenant backup to Amazon EC2. For details on how restore to the Amazon EC2 works, description of all options and limitations within the Veeam Backup & Replication infrastructure, see the [Restore to Amazon EC2](#) section in the Veeam Backup & Replication User Guide.

Before starting the restore to Amazon EC2 operation, the SP must first disable the tenant account. To do that, complete the following steps:

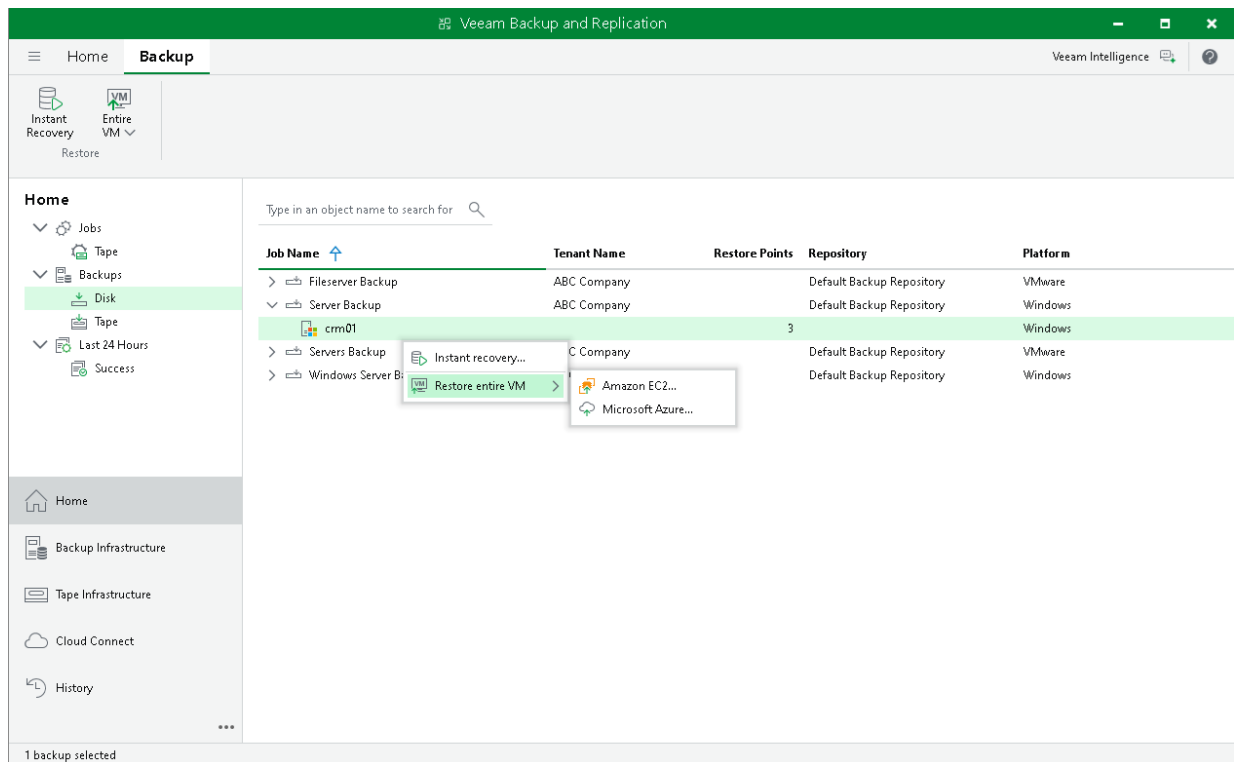
1. In Veeam Backup & Replication on the SP backup server, open the **Cloud Connect** view.
2. In the inventory pane, click **Tenants**.
3. In the working area, right-click the tenant account and select **Disable**.

To learn more about this operation, see [Disabling and Enabling Tenant Accounts](#).

To restore tenant backup to Amazon EC2, do the following:

1. In Veeam Backup & Replication on the SP backup server, open the **Home** view.

2. Select the **Backups** node in the inventory pane. Expand the backup in the working area, select the necessary VM, select **Entire VM** and click **Amazon EC2** on the ribbon or right-click the backup and select **Restore entire VM** and click **Amazon EC2**.



- At the **Machine** step of the **Restore to Amazon EC2** wizard, select the VM in the list, click **Point** on the right and select the necessary restore point.

Restore to Amazon EC2

Machine

Account

Name

Instance Type

Network

Secure Restore

Helper Appliance

Reason

Summary

Machine

Select a machine to restore to Amazon EC2 VM. If multiple restore points are available for selected machines, click Point to pick the desired one.

Machine

Type in a VM name for instant lookup

Name	Size	Restore point
 srv12.tech.local	57,1 GB	less than a day ago (2:05 čtvrtk...

+ Add...

⌚ Point...

⊖ Remove

< Previous

Next >

Finish

Cancel

300 | Veeam Cloud Connect | Administrator Guide | 13.1.0.411

- At the **Account** step of the wizard, specify credentials of a user account that will be used to connect to AWS, region and a target data center.

Restore to Amazon EC2

Machine

Account

Name

Instance Type

Network

Secure Restore

Helper Appliance

Reason

Summary

Account

Specify AWS account and data center to restore to.

AWS account:

AKIAY4ZWOU4WHWXYMI5X (last edited: less than a day ago)

Add...

Manage accounts

AWS region:

Global

Select an AWS region based on your regulatory and compliance requirements.

Data center:

Africa (Cape Town) (af-south-1)

Select an Amazon data center based on the geographical proximity or pricing.

< Previous

Next >

Finish

Cancel

- At the **Name** step of the wizard, specify names and manage AWS tags for the restored workloads.

Restore to Amazon EC2

Machine

Account

Name

Instance Type

Network

Secure Restore

Helper Appliance

Reason

Summary

Name

Specify a name for the created Amazon EC2 VM.

Original name	VM name	VM Tags
 srv12.tech.local	srv12.tech.local	Original name, Rest...

VM Name...

Tags...

< Previous

Next >

Finish

Cancel

6. At the **Instance Type** step of the wizard, configure the instance for the restored workload, select which disks to restore and if necessary change their type.

Restore to Amazon EC2

Machine

Account

Name

Instance Type

Network

Secure Restore

Helper Appliance

Reason

Summary

Instance Type

Specify an instance size and a disk type for the created Amazon EC2 VM.

Original Name	Instance Type	License	Estimated Price per Month
 srv12.tech.local	<Select VM size>	Provided by AWS	N/A

srv12.tech.local Instance Type

EC2 instance type:
c5.12xlarge (48 vCPUs, 96,00 GB memory)

vCPUs: 48
Memory: 96,00 GB

OS license:
Provided by AWS

OKCancel

Edit...
Disks...

< Previous

Next >

Finish

Cancel

- At the **Network** step of the wizard, select to which Amazon Virtual Private Cloud (Amazon VPC) the restored workload must be connected. You can also specify a subnet and a security group - a virtual firewall for the restored EC2 instance.

Restore to Amazon EC2

Machine

Account

Name

Instance Type

Network

Secure Restore

Helper Appliance

Reason

Summary

Network

Specify the virtual private cloud (VPC) to connect the created Amazon EC2 VM to.

Name	Amazon VPC	Security group	IP
 srv12.tech.local	<Select AWS VPC>	Select AWS security group.	Pr

 VPC...

 IP address...

< Previous

Next >

Finish

Cancel

8. At the **Secure Restore** step of the wizard, configure Veeam Backup & Replication to scan machine data with antivirus software and YARA rules before restoring the machine to the production environment.

Restore to Amazon EC2

Machine

Account

Name

Instance Type

Network

Secure Restore

Helper Appliance

Reason

Summary

Secure Restore

Scan the selected backup for malware, such as computer viruses or ransomware, prior to performing the restore. This requires a compatible antivirus installed on the mount server specified for the corresponding backup repository.

Content scan

☐ Scan the backup content with Veeam Threat Hunter prior to performing a recovery

☐ Scan the backup with the following YARA rule:

Select a YARA rule to use

Copy YARA rules location to clipboard

Scan options:

If malware is found

☒ Proceed with recovery but disable network adapters

Security group: not selected Click to change

☐ Abort recovery

☐ Continue scanning remaining files after the first malware has been found.

< Previous

Next >

Finish

Cancel

- At the **Helper Appliance** step of the wizard, specify helper appliance settings. A helper appliance is an auxiliary Linux-based instance used to upload disks of a backed-up workload to Amazon EC2.

For details on the helper appliance settings configuration, see the [Configure Helper Appliance](#) section in the Veeam Backup & Replication User Guide.

The screenshot shows a wizard window titled "Restore to Amazon EC2". On the left is a sidebar with steps: Machine, Account, Name, Instance Type, Network, Secure Restore, **Helper Appliance** (highlighted), Reason, and Summary. The main area is titled "Helper Appliance" and contains the following text: "Choose whether to use a helper appliance for improved restore performance." Below this is a horizontal line, followed by a paragraph: "The helper appliance is required when restoring backups of Amazon EC2 instances. For backups of other platforms it is optional but improves the restore performance significantly. We will provision the helper appliance in Amazon EC2 automatically." Another paragraph follows: "The appliance takes about a minute to be created and to boot up." Below these paragraphs is a checkbox labeled "Use the helper appliance (recommended)" which is checked, with a "Customize..." link next to it. At the bottom right are four buttons: "< Previous", "Next >", "Finish", and "Cancel".

- At the **Reason** step of the wizard, specify the reason for future reference.
- At the **Summary** step of the wizard, check the specified settings and click **Finish**.

After completing the restore operation, the SP must enable the tenant account. To do that, complete the following steps:

- In Veeam Backup & Replication on the SP backup server, open the **Cloud Connect** view.
- In the inventory pane, click **Tenants**.
- In the working area, right-click the tenant account and select **Disable**.

To learn more about this operation, see [Disabling and Enabling Tenant Accounts](#).

Restoring to Microsoft Azure

The SP can restore machines from tenant backups stored in a cloud repository to a public cloud environment. This capability allows the SP to use tenant backups to recover workloads directly in Microsoft Azure, rather than to the original on-premises location. As a result, the SP can offer additional data protection scenarios, such as migration if the tenant decides to permanently move from an on-premises environment to a public cloud environment.

To use this functionality, the SP 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 Veeam Agent users, consider that to display on the SP side backups created by Veeam Agent in the standalone mode, a backup server connected to the SP with the **Allow this Veeam Backup & Replication installation to be managed by the service provider** option enabled is required.

- Veeam Cloud Connect supports restore to Microsoft Azure from encrypted tenant backups only if the tenant has granted the SP restore access to all backups. Otherwise, restore to Microsoft Azure is supported from unencrypted backups only. For details, see [Access to Tenant Backups](#).
- Veeam Cloud Connect supports restore to Microsoft Azure for the following workloads:
 - Backups of VMware Cloud Director VMs created by Veeam Backup & Replication.
 - Backups of Microsoft Windows and Linux VMs created by Veeam Backup & Replication.
 - Backups of Microsoft Hyper-V virtual machines 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 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](#).
 - Backups of Nutanix AHV VMs created by [Veeam Backup for Nutanix AHV](#).
 - Backups of oVirt VMs created by [Veeam Backup for OLVM and RHV](#).
 - Backups of Proxmox VE VMs created by [Veeam Backup for Proxmox VE](#).

This procedure description is specific for the Veeam Cloud Connect environment. This section describes only basic steps that you must take to restore a tenant backup to Microsoft Azure. For details on how restore to the Microsoft Azure works, description of all options and limitations within the Veeam Backup & Replication infrastructure, see the [Restore to Microsoft Azure](#) section in the Veeam Backup & Replication User Guide.

Before starting the restore to Microsoft Azure operation, the SP must first disable the tenant account. To do that, complete the following steps:

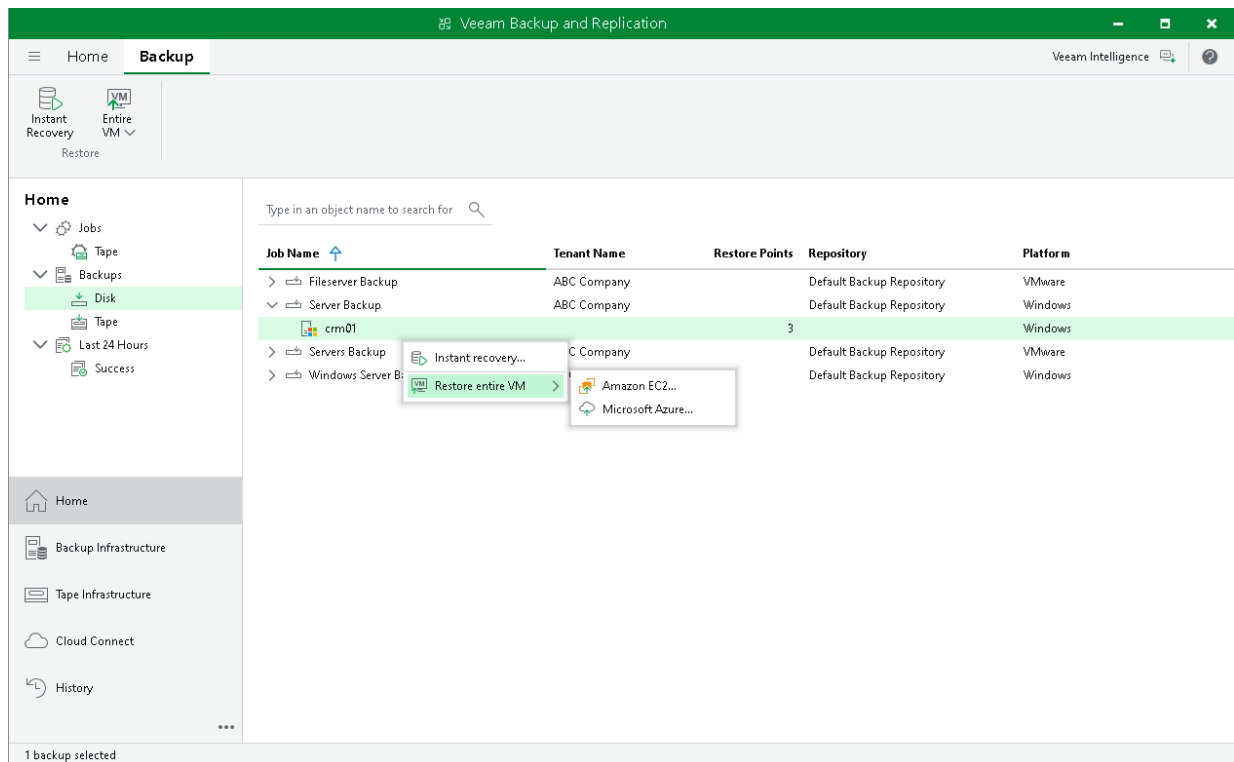
1. In Veeam Backup & Replication on the SP backup server, open the **Cloud Connect** view.
2. In the inventory pane, click **Tenants**.
3. In the working area, right-click the tenant account and select **Disable**.

To learn more about this operation, see [Disabling and Enabling Tenant Accounts](#).

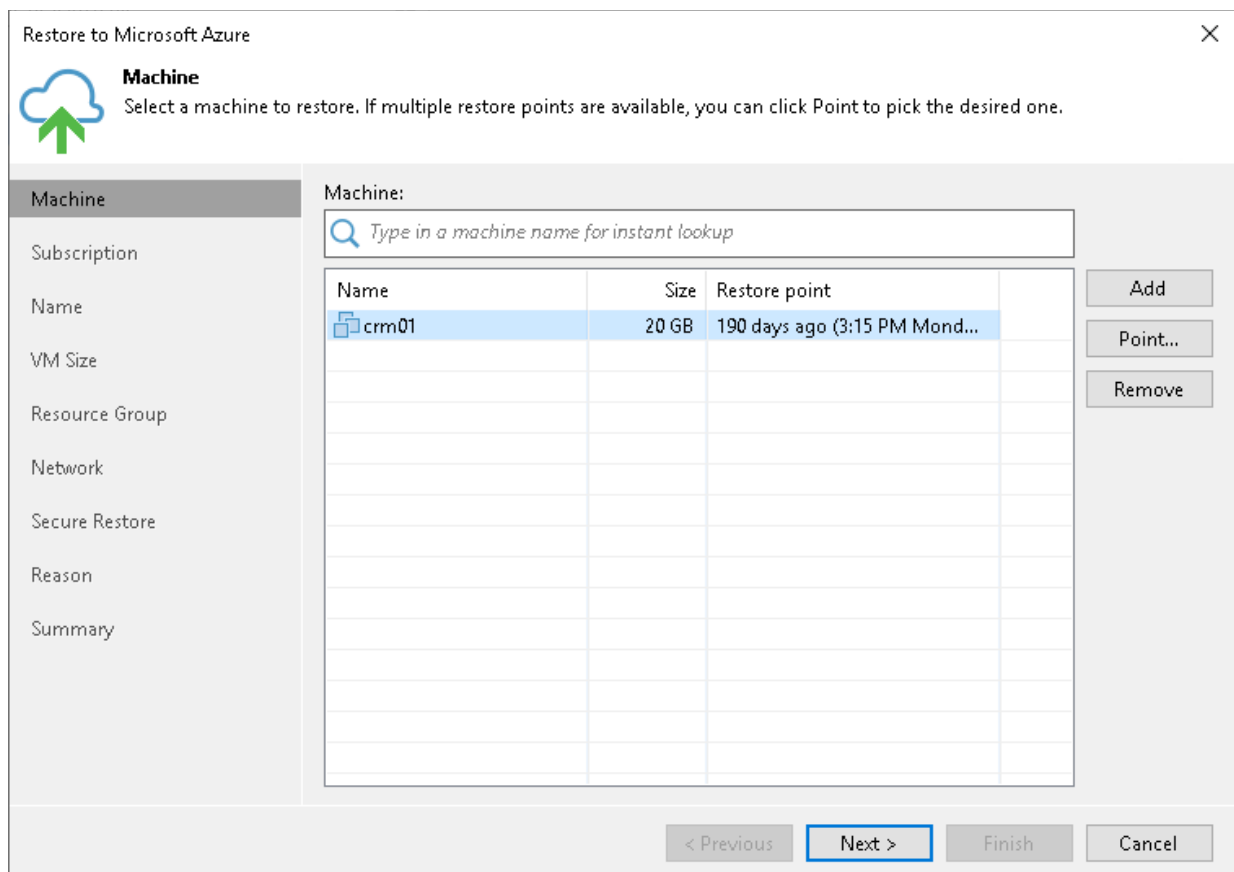
To restore tenant backup to Microsoft Azure, do the following:

1. In Veeam Backup & Replication on the SP backup server, open the **Home** view.

2. Select the **Backups** node in the inventory pane. Expand the backup in the working area, select the necessary VM, select **Entire VM** and click **Microsoft Azure** on the ribbon or right-click the backup and select **Restore entire VM** and click **Microsoft Azure**.



3. At the **Machine** step of the **Restore to Microsoft Azure** wizard, select the VM in the list, click **Point** on the right and select the necessary restore point.



4. At the **Subscription** step of the wizard, select a subscription, location for the restored workloads and define how workload data must be transported to Microsoft Azure.

If you are restoring the workloads to a distant location and want to speed up the restore process, select the **Use a proxy appliance** check box. From the drop-down list, select an Azure restore proxy appliance.

The screenshot shows the 'Restore to Microsoft Azure' wizard window. The title bar says 'Restore to Microsoft Azure' with a close button. Below the title bar is a blue cloud icon with a green arrow pointing up, followed by the heading 'Subscription' and the instruction 'Specify Azure subscription and data center region to restore to.' On the left is a sidebar with a list of steps: Machine, Subscription (highlighted), Name, VM Size, Resource Group, Network, Secure Restore, Reason, and Summary. The main area contains two dropdown menus: 'Subscription:' with 'Enterprise - QA (MS Azure Account)' selected, and 'Location:' with 'Australia Central' selected. Below these is a checkbox labeled 'Use a proxy appliance (recommended)' which is unchecked. Under the checkbox is a dropdown menu showing 'srv444.tech.local'. A note below the dropdown states 'Using a proxy appliance improves the restore performance significantly.' At the bottom right are four buttons: '< Previous', 'Next >' (highlighted with a blue border), 'Finish', and 'Cancel'.

Restore to Microsoft Azure

Subscription
Specify Azure subscription and data center region to restore to.

Machine

Subscription

Name

VM Size

Resource Group

Network

Secure Restore

Reason

Summary

Subscription:
Enterprise - QA (MS Azure Account)

Specify Azure subscription and data center region to restore to.

Location:
Australia Central

Choose the Azure data center region where the VMs should be restored to.

☐ Use a proxy appliance (recommended)

srv444.tech.local

Using a proxy appliance improves the restore performance significantly.

< Previous Next > Finish Cancel

- At the **Name** step of the wizard, specify names and manage tags for the restored workloads.

Restore to Microsoft Azure

 **Name**
Specify names to assign to the newly created Microsoft Azure VMs.

Machine

Subscription

Name

VM Size

Resource Group

Network

Secure Restore

Reason

Summary

Machines to restore:

Original name	VM name	VM Tags
 crm01	crm01	

VM Name... Tags...

< Previous Next > Finish Cancel

- At the **VM Size** step of the wizard, select VM sizes, storage accounts where to store disks of the restored workloads, select disks to restore and change their type.

Restore to Microsoft Azure

**VM Size**
Specify the storage account and disk type for the restored VM.

Machine

Subscription

Name

VM Size

Resource Group

Network

Secure Restore

Reason

Summary

Azure VM configuration:

Name	VM size	Storage account
 crm01	Standard_B2ls_v2 (2 cores, 4.00...	Managed storage type

Edit...

Disks...

< Previous

Next >

Finish

Cancel

- At the **Resource Group** step of the wizard, select resource groups for the restored workloads for them. By default, Veeam Backup & Replication creates a new resource group for the restored workloads and places them to it.

Restore to Microsoft Azure

**Resource Group**
Specify the resource group to place the restored VM into.

Machine

Subscription

Name

VM Size

Resource Group

Network

Secure Restore

Reason

Summary

Resource group:

Name	Resource group
 crm01	crm01

Group...

< Previous

Next >

Finish

Cancel

8. At the **Network** step of the wizard, select to which networks and subnets the restored workloads will be connected. By default, Veeam Backup & Replication creates a new security group for the restored workloads.

Restore to Microsoft Azure

**Network**
Specify the virtual network to connect the restored VM to.

Machine

Subscription

Name

VM Size

Resource Group

Network

Secure Restore

Reason

Summary

Virtual network:

Name	Virtual network	Network security group
 crm01	<--> <Select network>	Empty

Network...

Group...

< Previous

Next >

Finish

Cancel

- At the **Secure Restore** step of the wizard, configure Veeam Backup & Replication to scan machine data with antivirus software and YARA rules before restoring the machine to the production environment.

The screenshot shows the 'Restore to Microsoft Azure' wizard window. The title bar reads 'Restore to Microsoft Azure'. The main heading is 'Secure Restore' with a cloud and green arrow icon. Below the heading is a description: 'Scan the selected backup for malware, such as computer viruses or ransomware, prior to performing the restore. This requires a compatible antivirus installed on the mount server specified for the corresponding backup repository.' On the left is a sidebar with a list of steps: Machine, Subscription, Name, VM Size, Resource Group, Network, Secure Restore (highlighted), Reason, and Summary. The main area is titled 'Content scan' and contains several options: 'Scan restore points with Veeam Threat Hunter' (unchecked), 'Scan the restore point with the following YARA rule:' (unchecked), a text box for the YARA rule, a 'Copy YARA rules location to clipboard' button, 'Scan options:' with a radio button selected for 'Proceed with recovery but connect the VM to a different network' (showing 'Target network: <not configured> Click to change'), a radio button for 'Abort VM recovery', and a checkbox for 'Continue scanning all remaining files after the first occurrence' (unchecked). At the bottom right are four buttons: '< Previous', 'Next >' (highlighted with a blue border), 'Finish', and 'Cancel'.

- At the **Reason** step of the wizard, specify the reason for future reference.
- At the **Summary** step of the wizard, check the specified settings and click **Finish**.

After completing the restore operation, the SP must enable the tenant account. To do that, complete the following steps:

- In Veeam Backup & Replication on the SP backup server, open the **Cloud Connect** view.
- In the inventory pane, click **Tenants**.
- In the working area, right-click the tenant account and select **Disable**.

To learn more about this operation, see [Disabling and Enabling Tenant Accounts](#).

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 to the following platforms:

- VMware vSphere
- Microsoft Hyper-V

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** 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 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.
 - d. Then select the target platform.
2. Follow the steps of the **Instant Recovery** 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.

- [For *Instant Recovery to VMware vSphere*] 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 Using Console](#) section in the Veeam Backup & Replication User Guide.

- [For *Instant Recovery to Microsoft Hyper-V*] Instant Recovery in the Veeam Cloud Connect infrastructure is performed to a Microsoft Hyper-V VM on the SP virtualization host. Thus, in this scenario the **Instant Recovery to Microsoft Hyper-V** wizard does not include the **Recovery Mode** step.

To get a detailed description of all Instant Recovery options, see the [Performing Instant Recovery to Microsoft Hyper-V Using Console](#) section in the Veeam Backup & Replication User Guide.

The screenshot shows the Veeam Backup & Replication console interface. The top bar is green with the title 'Veeam Backup & Replication'. Below it, the 'Backup' tab is selected. The left sidebar contains navigation options: Home, Jobs, Backups, Last 24 Hours, Inventory, Backup Infrastructure, Cloud Connect, and History. The main area displays a table of backup jobs. A context menu is open for the selected job 'filesrv03', showing options: 'Instant recovery', 'Restore entire VM', 'Restore guest files...', and 'Scan backup...'. The 'Instant recovery' option is highlighted, and a sub-menu is visible showing 'VMware vSphere...' and 'Microsoft Hyper-V...'.

Job Name	Tenant Name	Creation Time	Restore Points	Repository	Platform
Backup Job 2	Omega Company	20.05.2026 12:06		Default Backup Reposit...	VMware
filesrv03		11.06.2026 22:02	21		VMware

Restoring Disks from Tenant Backups

The SP can restore disks from tenant backups and attach them to a VM that runs on a virtualization host in the SP infrastructure. To perform the disk restore operation, the SP must use Veeam PowerShell cmdlets – this operation is not available in the SP Veeam backup console.

Prerequisites and limitations for disk restore on the SP side are the same as in the regular Veeam backup infrastructure. For details, see the [Performing Instant Disk Recovery: Before You Begin](#) section in the Veeam Backup & Replication User Guide.

In addition, for disk restore from tenant backups on the SP side consider the following:

- Tenant backups must be available on the SP side. For details, see [Restoring Data from Tenant Backups](#).
- The target virtualization host and VM where the SP plans to restore disks must be added to the Veeam Backup & Replication infrastructure on the SP backup server.
- Veeam Cloud Connect supports disk restore from encrypted tenant backups only if the tenant has granted the SP restore access to all backups. Otherwise, disk restore is supported from unencrypted backups only. For details, see [Access to Tenant Backups](#).

To restore disks from a tenant backup, complete the following steps:

1. Disable the tenant account. For more information, see [Disabling and Enabling Tenant Accounts](#).
2. Run the `Get-VBRCloudTenantBackup` cmdlet to specify the backup from which you want to restore disks. For details, see the [Get-VBRCloudTenantBackup](#) section in the Veeam PowerShell Reference.
3. Run the `Get-VBRCloudTenantRestorePoint` cmdlet to specify the necessary restore point in the backup. For details, see the [Get-VBRCloudTenantRestorePoint](#) section in the Veeam PowerShell Reference.
4. Run the `Get-VBRServer` and `Find-VBRViEntity` cmdlets to specify the target host and VM where you want to restore disks from the backup.
5. Run the `Get-VBRViVirtualDevice` cmdlet to specify the disks that you want to restore.
6. Run the `Start-VBRViInstantVMDiskRecovery` cmdlet to restore disks.

For example:

```
$backup = Get-VBRCloudTenantBackup -Name "Fileserver Backup to Cloud"
$restorepoint = Get-VBRCloudTenantRestorePoint
$server = Get-VBRServer -Name "esx01"
$vm = Find-VBRViEntity -Server $server -Name "filesrv05"
$device = Get-VBRViVirtualDevice -RestorePoint $restorepoint
Start-VBRViInstantVMDiskRecovery -RestorePoint $restorepoint[3] -TargetVM $vm -
TargetVirtualDevice $device
```

For details, see the [Start-VBRViInstantVMDiskRecovery](#) section in the Veeam PowerShell Reference.

After Veeam Backup & Replication mounts the restored disk to the target VM, you must finalize the process. For details, see the [Finalizing Instant Disk Recovery](#) section in the Veeam Backup & Replication Guide and [Start-VBRViInstantRecoveryDiskMigration](#) section in the Veeam PowerShell Reference.

Once you finalize the disk restore operation, you can enable the tenant account.

Publishing Disks from Tenant Backups

The SP can publish disks from tenant backups and mount them to a server added to the SP Veeam Backup & Replication infrastructure. To perform the disk publishing operation, the SP must use Veeam PowerShell cmdlets — this operation is not available in the SP Veeam backup console.

TIP

The disk publishing operation is also available on the tenant side. To publish disks, the tenant can use the Veeam backup console. To learn more, see [Publishing Disks](#).

Prerequisites and limitations for disk publishing on the SP side are the same as in the regular Veeam backup infrastructure. For details, see the [Disk Publishing \(Data Integration API\)](#) section in the Veeam Backup & Replication User Guide.

Also keep in mind that Veeam Cloud Connect supports disk publishing from encrypted tenant backups only if the tenant has granted the SP restore access to all backups. Otherwise, disk publishing is supported from unencrypted backups only. For details, see [Access to Tenant Backups](#).

To publish disks from a tenant backup, complete the following steps:

1. Disable the tenant account. For more information, see [Disabling and Enabling Tenant Accounts](#).
2. Run the `Get-VBRCloudTenantBackup` cmdlet to get the backup from which you want to restore disks. For details, see the [Get-VBRCloudTenantBackup](#) section in the Veeam PowerShell Reference.
3. Run the `Get-VBRCloudTenantRestorePoint` cmdlet to get the necessary restore point in the backup. For details, see the [Get-VBRCloudTenantRestorePoint](#) section in the Veeam PowerShell Reference.
4. Run the `Publish-VBRBackupContent` cmdlet to publish disks.

For example:

```
$backup = Get-VBRCloudTenantBackup -Name "Fileserver Backup to Cloud"
$point = Get-VBRCloudTenantRestorePoint -Backup $backup -Name "filesrv04" | Sort-Object -Property CreationTime | Select -Last 1
$creds = Get-VBRCredentials -Name "tech\william.fox"
Publish-VBRBackupContent -RestorePoint $point -TargetServerName "srv18.tech.local" -TargetServerCredentials $creds
```

For more information, see the [Publish-VBRBackupContent](#) section in the Veeam PowerShell Reference.

The disk content will become available in the `C:\VeeamFLR\` folder on the target server. For disks of Microsoft Windows machines, the disk content is available in the read-only state. You can perform the necessary operations with the published disk data, for example, find specific documents, copy files or perform antivirus scan of the backed-up data.

After you finish working with the disk content, you can stop the disk publishing session. For details, see the [Managing Published Disks](#) section in the Veeam Backup & Replication Guide and [Unpublish-VBRBackupContent](#) section in the Veeam PowerShell Reference.

Once the disk publishing session is stopped, you can enable the tenant account.

Managing Tenant Data

The SP can perform the following actions with tenant data:

- [Move tenant backups to another cloud repository](#)
- [Migrate tenant data between performance tier extents](#)
- [Switching from a Linux repository to a hardened \(immutable\) backup 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.

Consider the following:

- This section describes procedures of moving tenant data between regular, or simple, backup repositories used as cloud repositories. To operations that involve scale-out backup repositories, the following limitations apply:
 - You can move tenant backups to a cloud repository that has a scale-out backup repository as a back end with Microsoft PowerShell cmdlet only. To learn more, see the [Switch-VBRCloudTenantsQuotaRepositoryToSOBR](#) section in the Veeam PowerShell Reference.

This contrasts with the same scenario in previous versions of Veeam Backup & Replication, which required you to contact [Veeam Customer Support](#).

 - You cannot move tenant data to a cloud repository that has a scale-out backup repository as a back end if this repository has object storage added as a performance tier extent.
 - If you want to move tenant data from a scale-out backup repository used as a cloud repository, follow instructions for the [Scenario 2](#). You cannot use the Scenario 1 to move data from a scale-out backup repository.

TIP

You can also migrate tenant backups between performance extents within the same scale-out backup repository. To learn more, see [Migrating Tenant Data Between Performance Tier Extents](#).

- You cannot move tenant data from a cloud repository that has object storage as a back end.

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.

IMPORTANT

Do not rescan the backup repository to which you copied tenant backup files before you replace the cloud repository as described in the step 4 of this procedure.

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**.

To learn more about this operation, see [Disabling and Enabling Tenant Accounts](#).

Edit ABC Company

Backup Resources
Add one or more cloud repositories for this tenant to use.

Tenant

Bandwidth

Backup Resources

Replica Resources

Network Extension

Apply

Summary

Edit Quota

Cloud repository name:
ABC Company Cloud Repository

Specify a friendly repository name that will be shown to the user.

Backup repository:
ABC Company Cloud Repository (New cloud repository)

649.5 MB free of 89.1 GB ⚠️ Allocated: 130 GB

User quota:
10 GB

☒ Enable WAN acceleration through the following WAN accelerator:
srvt1.tech.local (Created by .\Administrator at 10/20/2025 1:47 PM.)

OK Cancel

For added tenant protection against insider attacks, we will preserve all deleted backup files for the set number of days. The deleted backups will not count towards tenant's quota consumption, and cannot be managed by the tenant.

< Previous Next > Finish Cancel

After the SP completes their tasks, the tenant may need to rescan the cloud repository in the tenant Veeam Backup & Replication console in one of the following cases:

- If the SP moved tenant data between backup repositories based on servers with different operating systems, the tenant must rescan the cloud repository.
- If the SP changed the tenant quota, the new quota becomes visible to the tenant after the next job run. Alternatively, the tenant can perform the rescan operation for the service provider or cloud repository.

To rescan the cloud repository on the tenant side:

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**.

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.

The screenshot shows the 'Edit ABC Company' wizard in the 'Backup Resources' step. A 'Set Quota' dialog box is open, allowing configuration for a new cloud repository. The dialog includes the following fields and options:

- Cloud repository name:** A text field containing 'ABC Company Cloud Repository 2'.
- Specify a friendly repository name that will be shown to the user.** (Instructional text)
- Backup repository:** A dropdown menu showing 'ABC Company Cloud Repository (New cloud repository)'.
- User quota:** A numeric field set to '10' and a unit dropdown set to 'GB'.
- Enable WAN acceleration through the following WAN accelerator:** An unchecked checkbox with an empty dropdown menu below it.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom of the dialog.

In the background, the 'Backup Resources' step of the wizard is visible, showing a list of resources with columns for 'Name', 'Type', and 'WAN'. The 'Add...' button is highlighted. At the bottom of the wizard, navigation buttons '< Previous', 'Next >', 'Finish', and 'Cancel' are present.

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.

New File Copy Job

Name

Source

Destination

Schedule

Summary

Source

Select items to be copied with this job.

Objects to process:

File or folder	Server
 D:\Backup\ABC Company	srv12

+ Add...

- Remove

< Previous

Next >

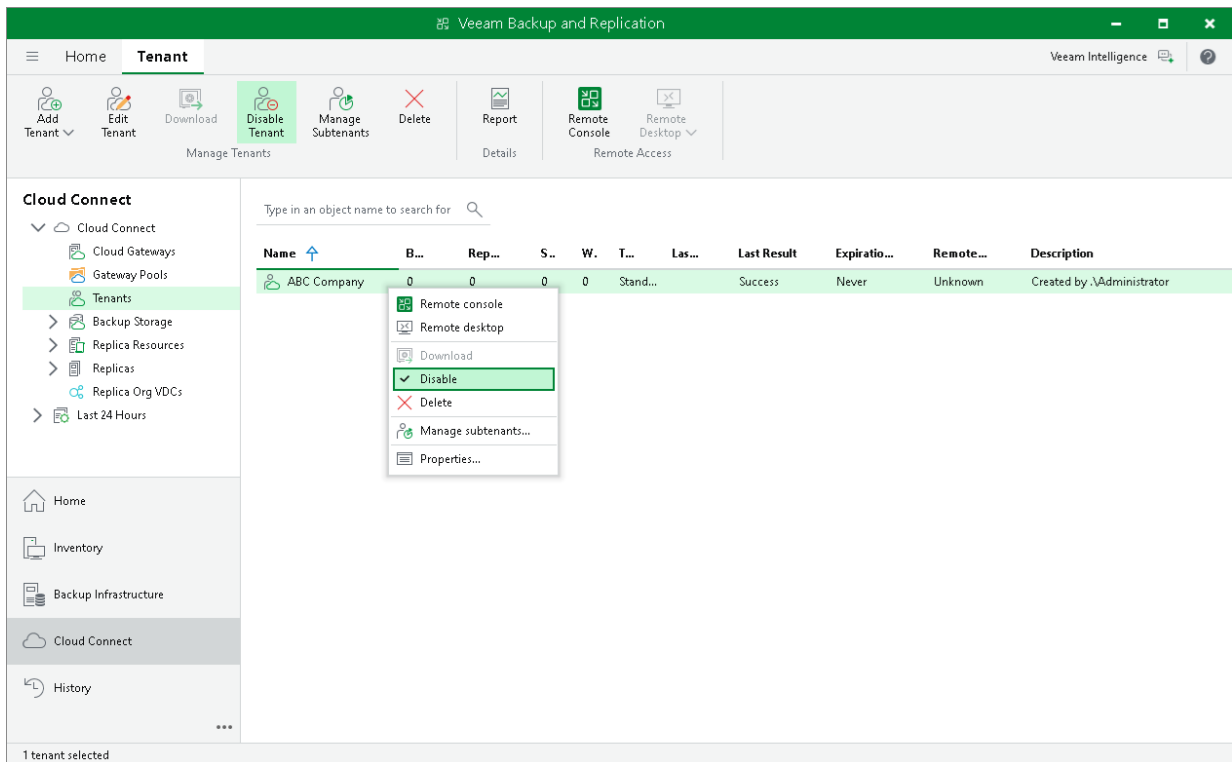
Finish

Cancel

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**.

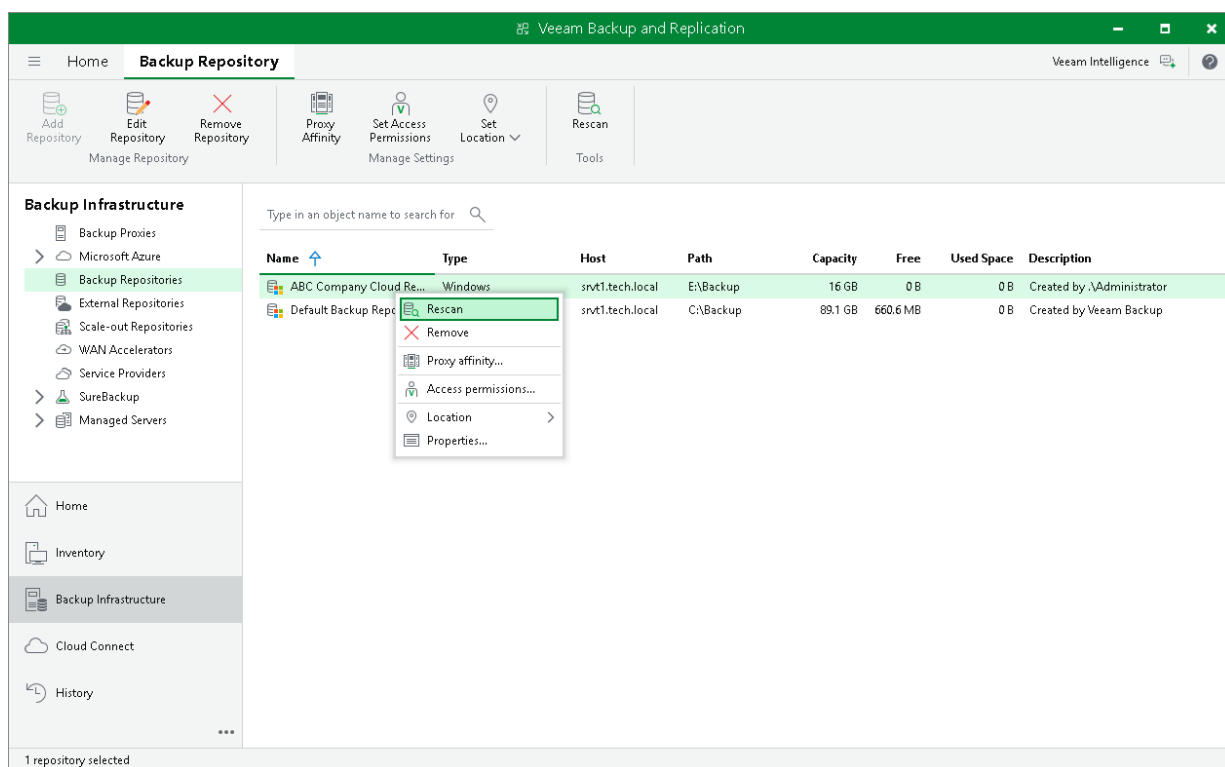
To learn more about this operation, see [Disabling and Enabling Tenant Accounts](#).



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**.



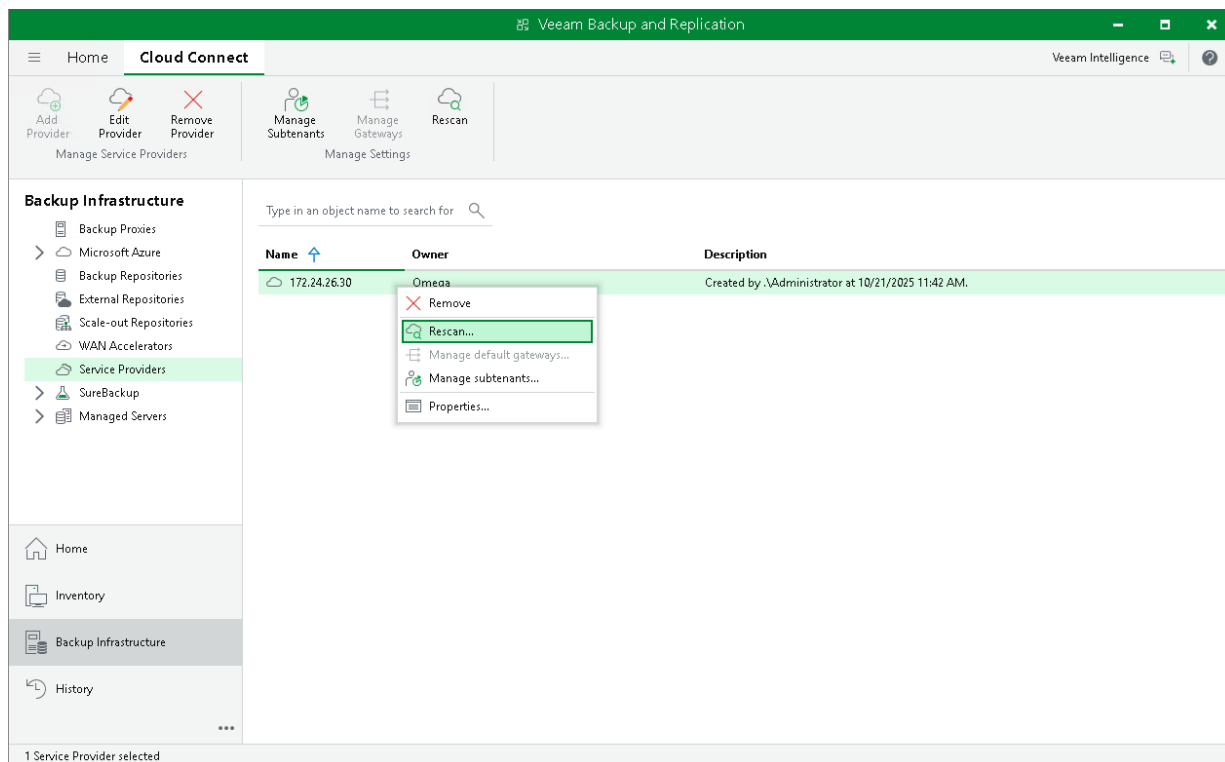
IMPORTANT

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.

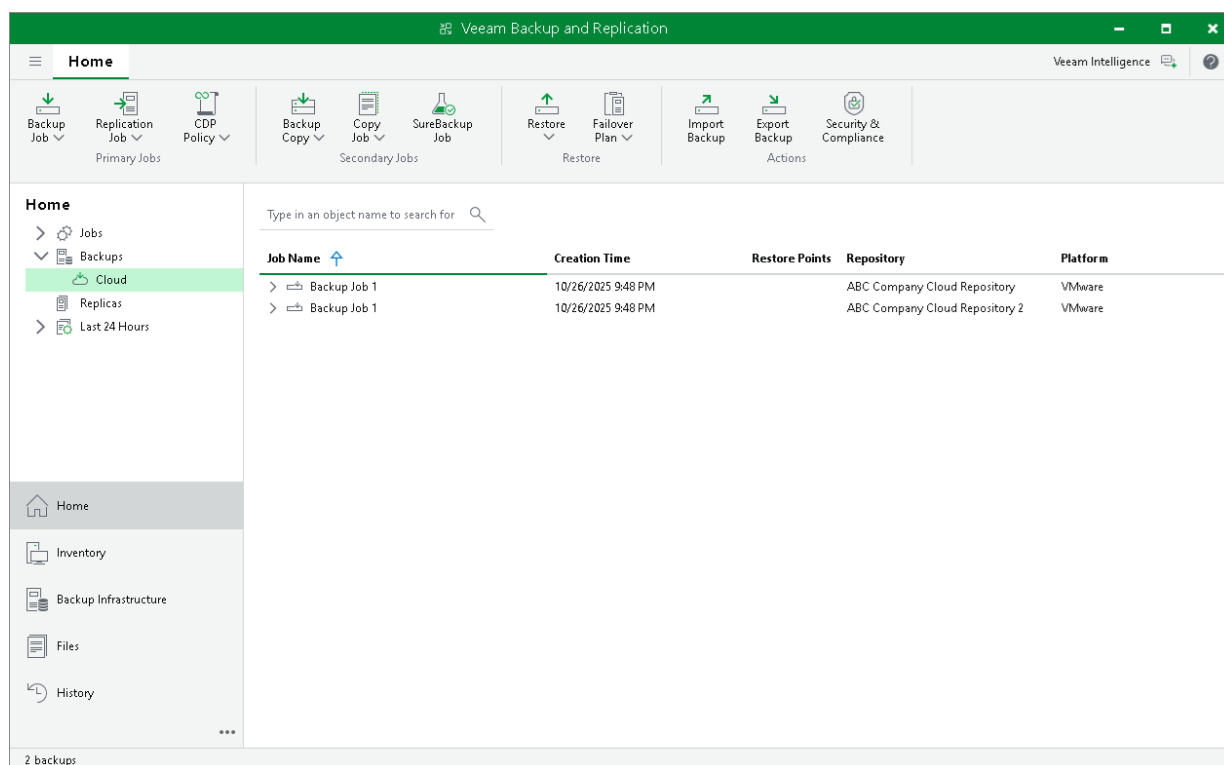
Backups that reside in the new cloud repository will appear in the **Home** view next to backups that were created in the initial cloud repository.

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**.

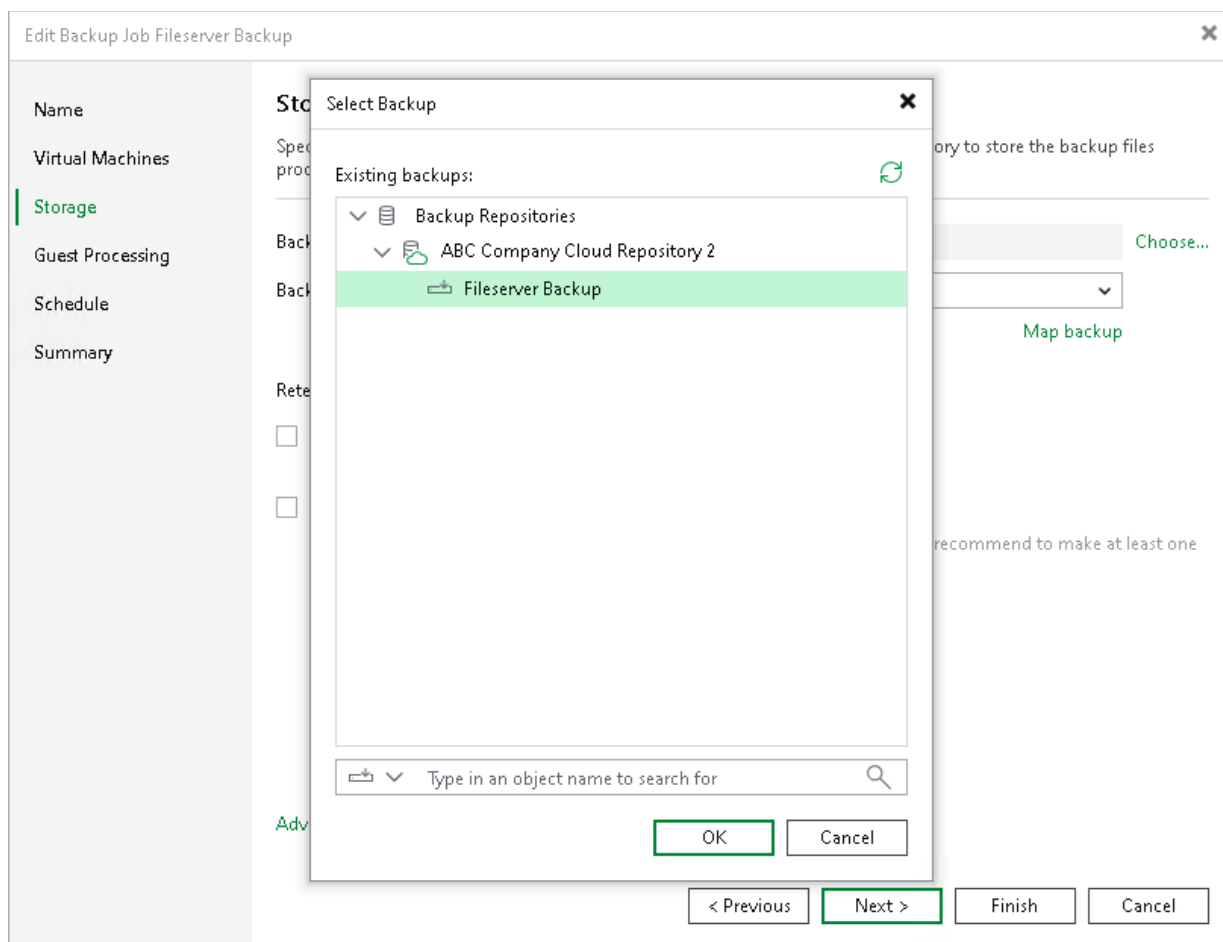
b. In the **Specify Password** window, type in the password for the backup.

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 have been moved.

IMPORTANT

Make sure that you do not delete backup files from the new cloud repository instead of the initial cloud repository.

Veeam Backup and Replication

Home

Veeam Intelligence

Backup Job

Replication Job

CDP Policy

Primary Jobs

Backup Copy

Copy Job

SureBackup Job

Secondary Jobs

Restore

Failover Plan

Restore

Import Backup

Export Backup

Security & Compliance

Actions

Home

> Jobs

> Backups

> Cloud

> Replicas

> Last 24 Hours

Home

Inventory

Backup Infrastructure

Files

History

...

Type in an object name to search for

Job Name	Creation Time	Restore Points	Repository	Platform
> Backup Job 1	10/26/2025 9:48 PM		ABC Company Cloud Repository	VMware
> Backup Job 1			ABC Company Cloud Repository 2	VMware

Remove from

Properties

Job

Disk

1 backup selected

Migrating Tenant Data Between Performance Tier Extents

The SP can migrate tenant data between performance extents within the same scale-out backup repository to balance storage resources, for example, after the SP adds a new extent to a scale-out backup repository. To perform this operation, the SP must use Veeam PowerShell cmdlets.

NOTE

If the source extent contains encrypted backups, Veeam Cloud Connect does not apply [Fast Clone](#) to these backups during migration between extents.

To migrate tenant data between performance extents, follow these steps:

1. The SP specifies the source performance extent and the target performance extent for the operation, along with the tenant account whose data the SP wants to migrate. The migration process has no effect on other tenants.
2. The SP runs the `Start-VBRCLOUDTenantBackupEvacuation` cmdlet.

The cmdlet performs following steps:

- a. Disables the tenant account.
- b. Migrates following items from the source performance extent to the target performance extent:
 - Tenant backups
 - Subtenant backups
 - Backup metadata files
 - Backup files in the "recycle bin" used for insider protection
 - Archive tier indexes for tenants running Veeam Backup & Replication version 11

Note that backup data offloaded to the capacity tier is not downloaded back to the performance tier during the migration process.

- c. Enables the tenant account.

For detailed instructions, see the [Start-VBRCLOUDTenantBackupEvacuation](#) section in the Veeam PowerShell Reference.

NOTE

Veeam Backup & Replication supports migration of tenant backups from a scale-out backup repository to a hardened (immutable) backup repository. For details, see [Switching from Linux Repository to Hardened Repository](#).

Switching from Linux Repository to Hardened Repository

The SP can enable immutability for a Linux repository with tenant data. This allows the SP to increase the level of data protection for tenant backups. This operation is available for simple backup repositories and backup repositories used as a performance extent of a scale-out backup repository.

To enable immutability for tenant backups, the SP changes the type of the backup repository from the Linux repository to the hardened (immutable) repository. To achieve this, the SP must add the same server again under a different name:

- If the Linux repository server was added using an IP address, add the server using a hostname.
- If the Linux repository server was added using a hostname, add the server using a different hostname or using the IP address of the server.

For more information, see [Prerequisites](#).

IMPORTANT

This operation does not apply to repositories deployed with the JeOS (Just Enough Operating System) ISO file for Veeam Infrastructure Appliance.

To learn more about hardened repositories, see the [Hardened Repository](#) section in the Veeam Backup & Replication User Guide.

Prerequisites

Before changing the repository type, complete the following prerequisites:

- If the Linux repository server was added using an IP address, ensure the local hosts file has a hostname set up that points to that IP address (for example `/etc/hosts` on Linux, `C:\Windows\System32\drivers\etc\hosts` on Windows) or in DNS.
- If the Linux repository server was added using a hostname, ensure there is either another hostname that points to the same IP address (use hosts file or DNS), or that the IP address of the server is known.
- Make sure that the Linux server you want to use as a hardened repository does not have other roles assigned. For example, the server must not be configured as a mount server, and mount server components must not be installed on the server.

IMPORTANT

The hardened repository role cannot be assigned to a Linux server that has optional server roles installed. Before proceeding, use the `Uninstall-VBRServerComponent` cmdlet to remove any installed optional components, such as `dell-ddboost-sdk`, `hpe-catalyst-client`, `veeam-mount` or `veeam-mount-server-dependencies`. For details, see the [Uninstall-VBRServerComponent](#) section in the Veeam PowerShell Reference.

To check which components are installed, open **Backup Infrastructure > Managed Servers**. In the working area, select the Linux server and click **Edit Server** on the ribbon or right-click the server and select **Properties**. Navigate to the **Access** step, and click **Optional components and advanced connection settings**. To learn more, see the [Specify Credentials and SSH Settings](#) section in the Veeam Backup & Replication User Guide.

- On the Linux server, change permissions for the directory where backups are stored. Specify the account with non-root permissions that you use to connect to the Linux server as the owner of this directory, and the group to which this account belongs.

```
chown -R owner:group
```

For detailed requirements and limitations for a hardened repository, see the [Requirements and Limitations](#) section in the Veeam Backup & Replication User Guide.

- For backup jobs targeting the Linux repository used as a cloud repository, ensure that tenants use forward incremental backup mode with periodic full backups enabled in the job settings.
- For backup copy jobs, ensure that the tenant has a GFS retention policy enabled and configured.
- In the Veeam Backup & Replication console, disable all tenants whose data resides in the Linux repository used as a cloud repository. Make sure related sessions are finalized.

For details, see [Disabling and Enabling Tenant Accounts](#).

- [For a scale-out backup repository] In the Veeam Backup & Replication console, put the Linux backup repository used as a performance extent of a scale-out backup repository to the Maintenance mode.

For details, see the [Switching to Maintenance Mode](#) section in the Veeam Backup & Replication User Guide.

Switching from Linux Repository to Hardened Repository

To change the repository type from a Linux repository to a hardened repository, do the following:

1. Prepare the Linux server:
 - a. Open the **Backup Infrastructure** view. In the inventory pane, right-click the **Managed Servers** node and select **Add Server**. Alternatively, you can click **Add Server** on the ribbon.
 - b. In the **Add Server** window, select **Linux**.
 - c. At the **Name** step of the wizard, enter a full DNS name or IP address of the Linux server.

Make sure to use a different value than the one used when adding the Linux repository server, for example, if you used an IP address before, enter a hostname now.

NOTE

Note that you can use IPv6 addresses only if IPv6 communication is enabled. For details, see the [IPv6 Support](#) section in the Veeam Backup & Replication User Guide.

- d. Complete the remaining steps of the wizard.

For detailed instructions, see the [Adding Linux Servers Using Console](#) section in the Veeam Backup & Replication User Guide.

- e. At the **SSH Connection** step of the wizard, specify the account permissions you want to use to connect to the Linux server. Select **Single-use credentials for hardened repository**.

For detailed instructions, see the [Specify Credentials and SSH Settings](#) section in the Veeam Backup & Replication User Guide.

2. Use the **New Backup Repository** wizard to add the hardened repository as a backup repository:
 - a. Open the **Backup Infrastructure** view. Click **Add Repository** on the ribbon.

- b. In the **Add Backup Repository** window, select **Direct attached storage > Linux (Hardened Repository)**.
- c. At the **Server** step of the wizard, select the same Linux server where tenant backups are stored.
- d. At the **Repository** step of the wizard, select the same directory where tenant backups are stored.
- e. At the **Review** step of the wizard, make sure that the **Search the repository for existing backups and import them automatically** check box is not selected.
- f. Proceed to the **Summary** step of the wizard and click **Finish** to exit the wizard.

For detailed instructions, see the [Adding Hardened Repositories](#) section in the Veeam Backup & Replication User Guide.

IMPORTANT

Do not rescan the initial Linux repository after adding the new hardened repository to the SP Veeam Backup & Replication infrastructure.

3. Point Veeam Backup & Replication at the newly added hardened repository with tenant data. This step differs depending on whether you want to switch a simple backup repository or a performance extent of a scale-out backup repository to a hardened repository.
 - [For a simple Linux backup repository] Change backup resource allocation settings in the properties of the tenant account.
 - i. Open the **Cloud Connect** view. In the inventory pane, select **Tenants**.
 - ii. In the working area, right-click the tenant account and select **Properties**.
 - iii. At the **Backup Resources** step of the wizard, select the initial cloud repository in the list and click **Edit**.
 - iv. In the **Edit Quota** window, select the new hardened repository from the **Backup repository** list.

NOTE

Do not change the **Cloud repository name**.

- v. Proceed to the **Summary** step of the wizard and click **Finish** to exit the wizard.
 - [For a scale-out backup repository] Change settings of the scale-out backup repository.
 - i. Open the **Backup Infrastructure** view. In the inventory pane, click **Scale-out Repositories**.
 - ii. In the working area, select the scale-out repository and click **Edit Scale-out Repository** on the ribbon or right-click the scale-out backup repository and select **Properties**.
 - iii. At the **Performance Tier** step of the wizard, click **Remove** to remove the initial Linux repository, and then click **Add** to add the new hardened repository.
 - iv. Proceed to the **Summary** step of the wizard and click **Finish** to exit the wizard.
4. Remove the initial Linux repository from the SP infrastructure.

For details, see the [Removing Backup Repositories](#) section in the Veeam Backup & Replication User Guide.

5. [For a scale-out backup repository] Rescan the backup repository.

For details, see the [Rescanning Backup Repositories](#) section in the Veeam Backup & Replication User Guide.

6. Enable the tenant account.

For details, see [Disabling and Enabling Tenant Accounts](#).

After you switch repositories, the existing backups will become immutable on the next backup job run.

What You Do Next

[For a simple Linux backup repository] After you switch from a Linux repository to a hardened repository, tenants must clone existing jobs and map the cloned jobs to the existing cloud backups to continue using the same backup chains. Otherwise, only newly created jobs will run successfully, and existing jobs will fail.

To map the existing backup chain, do the following:

1. In the Veeam Backup & Replication console, select the existing backup job and click **Clone**. For details, see the [Cloning Jobs](#) section in the Veeam Backup & Replication User Guide.
2. Select the cloned backup job and click **Edit**. For details, see the [Editing Job Settings](#) section in the Veeam Backup & Replication User Guide.
3. At the **Storage** step of the wizard, click **Map backup** and select the existing backup chain to which you want to map the cloned backup job.
4. When prompted that the selected backup is already used by another job, confirm the warning.
5. Delete the original job. For details, see the [Deleting Backup Jobs](#) section in the Veeam Backup & Replication User Guide.

Switching from Linux Hardened Repository to Linux Repository

The SP can enable governance mode immutability for a Linux hardened repository with tenant data. This operation is available for simple backup repositories and backup repositories used as a performance extent of a scale-out backup repository.

To enable governance mode immutability for tenant backups, the SP changes the type of the backup repository from the Linux hardened repository to the Linux repository. To achieve this, the SP must add the same server again under a different name:

- If the Linux hardened repository server was added using an IP address, add the server using a hostname.
- If the Linux hardened repository server was added using a hostname, add the server using a different hostname or using the IP address of the server.

For more information, see [Prerequisites](#).

Prerequisites

Before changing the repository type, complete the following prerequisites:

- If the Linux hardened repository server was added using an IP address, ensure the local hosts file has a hostname set up that points to that IP address (for example `/etc/hosts` on Linux, `C:\Windows\System32\drivers\etc\hosts` on Windows) or in DNS.
- If the Linux hardened repository server was added using a hostname, ensure there is either another hostname that points to the same IP address (use hosts file or DNS), or that the IP address of the server is known.
- In the Veeam Backup & Replication console, disable all tenants whose data resides in the Linux hardened repository used as a cloud repository. Make sure related sessions are finalized.

For details, see [Disabling and Enabling Tenant Accounts](#).

- [For a scale-out backup repository] In the Veeam Backup & Replication console, put the Linux hardened backup repository used as a performance extent of a scale-out backup repository to the Maintenance mode.

For details, see the [Switching to Maintenance Mode](#) section in the Veeam Backup & Replication User Guide.

Switching from Linux Hardened Repository to Linux Repository

To change the repository type from a Linux hardened repository to a Linux repository, do the following:

1. Prepare the Linux server:
 - a. Open the **Backup Infrastructure** view. In the inventory pane, right-click the **Managed Servers** node and select **Add Server**. Alternatively, you can click **Add Server** on the ribbon.
 - b. In the **Add Server** window, select **Linux**.
 - c. At the **Name** step of the wizard, enter a full DNS name or IP address of the Linux server.

Make sure to use a different value than the one used when adding the hardened repository server, for example, if you used an IP address before, enter a hostname now.

NOTE

Note that you can use IPv6 addresses only if IPv6 communication is enabled. For details, see the [IPv6 Support](#) section in the Veeam Backup & Replication User Guide.

- d. Complete the remaining steps of the wizard.

For detailed instructions, see the [Adding Linux Servers Using Console](#) section in the Veeam Backup & Replication User Guide.

- e. At the **SSH Connection** step of the wizard, specify the account permissions you want to use to connect to the Linux server.

For detailed instructions, see the [Specify Credentials and SSH Settings](#) section in the Veeam Backup & Replication User Guide.

2. Use the **New Backup Repository** wizard to add the hardened repository as a backup repository:

- a. Open the **Backup Infrastructure** view. Click **Add Repository** on the ribbon.
- b. In the **Add Backup Repository** window, select **Direct attached storage > Linux**.
- c. At the **Server** step of the wizard, select the Linux server you added in step 1.
- d. At the **Repository** step of the wizard, select the same directory where tenant backups are stored.
- e. At the **Review** step of the wizard, make sure that the **Search the repository for existing backups and import them automatically** check box is not selected. Note that the option to import backups is not available for service providers.
- f. Proceed to the **Summary** step of the wizard and click **Finish** to exit the wizard.

For detailed instructions, see the [Adding Hardened Repositories](#) section in the Veeam Backup & Replication User Guide.

IMPORTANT

Do not rescan the initial Linux hardened repository after adding the new non-hardened repository to the SP Veeam Backup & Replication infrastructure.

3. Point Veeam Backup & Replication at the newly added Linux repository with tenant data. This step differs depending on whether you want to switch a simple backup repository or a performance extent of a scale-out backup repository to a hardened repository.
 - o [For a simple Linux backup repository] Change backup resource allocation settings in the properties of the tenant account.
 - i. Open the **Cloud Connect** view. In the inventory pane, select **Tenants**.
 - ii. In the working area, right-click the tenant account and select **Properties**.
 - iii. At the **Backup Resources** step of the wizard, select the initial cloud hardened repository in the list and click **Edit**.
 - iv. In the **Edit Quota** window, select the new non-hardened repository from the **Backup repository** list.

NOTE

Do not change the **Cloud repository** name.

- v. Proceed to the **Summary** step of the wizard and click **Finish** to exit the wizard.
- o [For a scale-out backup repository] Change settings of the scale-out backup repository.
 - i. Open the **Backup Infrastructure** view. In the inventory pane, click **Scale-out Repositories**.
 - ii. In the working area, select the scale-out repository and click **Edit Scale-out Repository** on the ribbon or right-click the scale-out backup repository and select **Properties**.
 - iii. At the **Performance Tier** step of the wizard, click **Remove** to remove the initial Linux hardened repository, and then click **Add** to add the new Linux repository.
 - iv. Proceed to the **Summary** step of the wizard and click **Finish** to exit the wizard.
- 4. Remove the initial Linux hardened repository from the SP infrastructure.

For details, see the [Removing Backup Repositories](#) section in the Veeam Backup & Replication User Guide.
- 5. [For a scale-out backup repository] Rescan the backup repository.

For details, see the [Rescanning Backup Repositories](#) section in the Veeam Backup & Replication User Guide.
- 6. Enable the tenant account.

For details, see [Disabling and Enabling Tenant Accounts](#).

Downloading Tenant Data from Capacity Tier

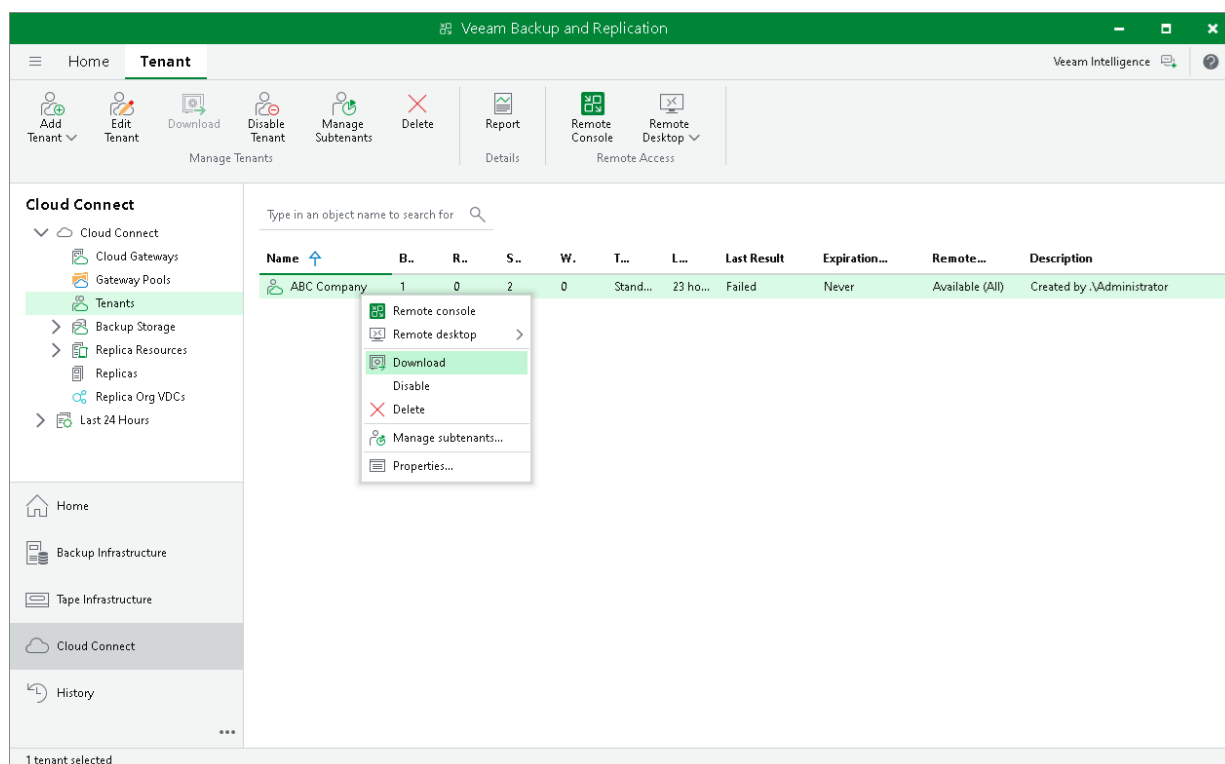
The SP can download tenant data that was offloaded to an object storage repository back to the on-premises extents of a scale-out backup repository. Veeam Backup & Replication lets the SP download all offloaded tenant backups at once. Downloaded backups remain in the performance tier and cannot be moved back to the capacity tier.

NOTE

The procedure to download tenant backup files from the capacity tier is supported only for unencrypted backups.

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 on-premises extents:
 - Click **All Backups** to download all tenant backup files.
 - 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 retrieve tenant data from the archive tier. This operation is required if the tenant needs to restore data from a restore point that was offloaded to the archive tier: it is not possible to restore data from such restore points immediately. To perform the retrieve operation, the SP must use Veeam PowerShell cmdlets.

To retrieve the tenant data, follow these steps:

1. Obtain the restore point ID from the tenant.

If the tenant is unsure which restore point to use, or if you manage the tenant Veeam Backup & Replication environment, ask the tenant to provide you with information about the point in time to which the tenant wants to restore data. Then, you can use the `Get-VBRCloudArchiveRestorePoint` PowerShell cmdlet to get a list of restore points located in the archive tier and obtain the restore point ID. For detailed instructions, see the [Get-VBRCloudArchiveRestorePoint](#) section in the Veeam PowerShell Reference.

2. Run the `Publish-VBRCloudArchiveRestorePoint` PowerShell cmdlet. This cmdlet retrieves tenant data from archive storage and places them in the capacity tier of the scale-out backup repository.

Use the restore point ID as a parameter value when performing the operation. For detailed instructions, see the [Publish-VBRCloudArchiveRestorePoint](#) section in the Veeam PowerShell Reference.

3. After the data is retrieved, notify the tenant that the data is ready. The tenant can then restore the data from the specified restore point.

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**.

Servers Replication Replica Properties

Virtual machine:

Original location:

filesrv03

vcenter01.tech.local\

Files:

Date	Restore Point Size	Status
 2 days ago (22:26 pondělí 03.11.2025)	270,9 KB	OK
 3 days ago (22:26 neděle 02.11.2025)	270,9 KB	OK

Total size: 270,9 KB

OK

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.

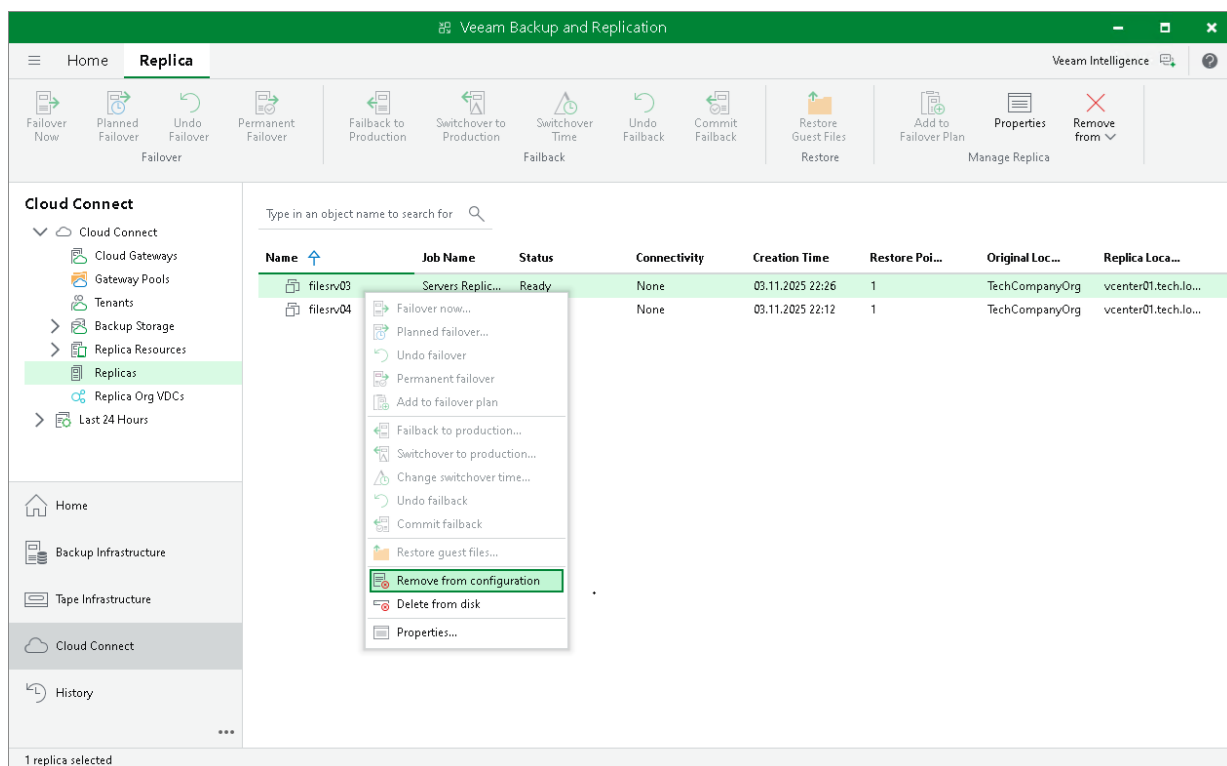
IMPORTANT

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**.



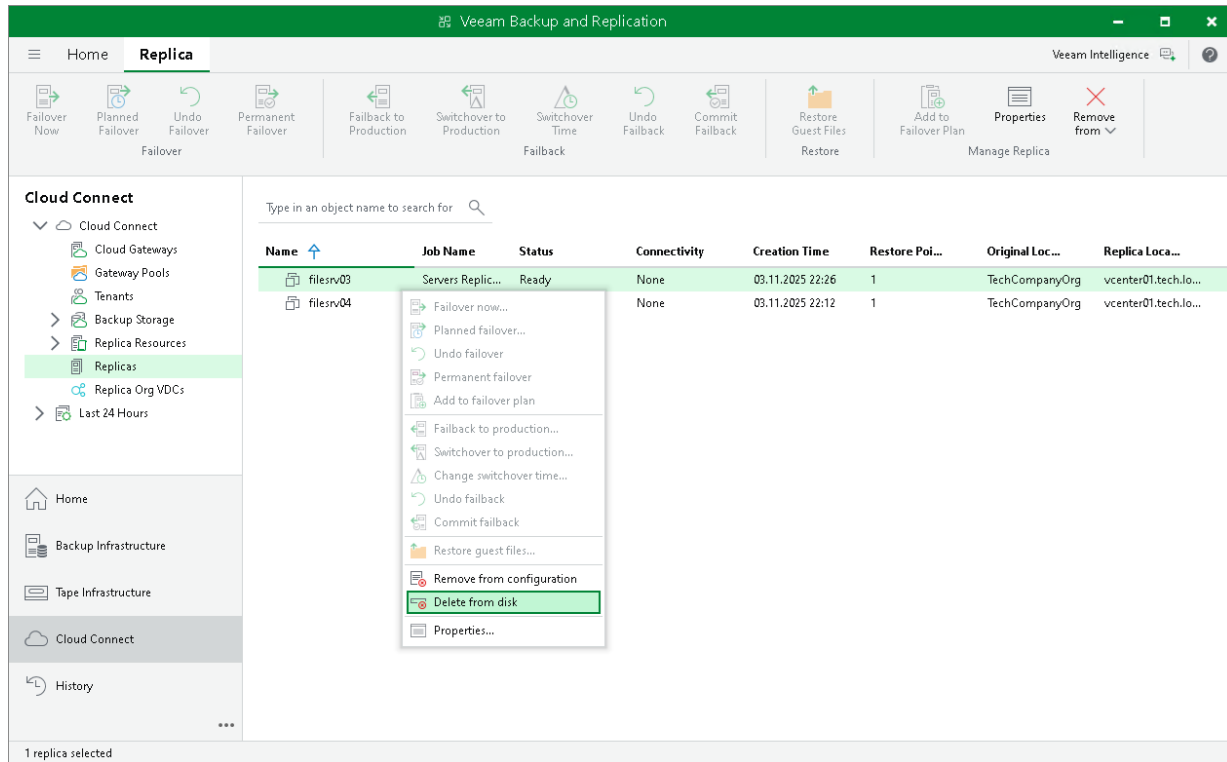
Deleting from Disk

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 appliances 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.

Edit ABC Company

Backup Resources
Add one or more cloud repositories for this tenant to use.

Tenant

Bandwidth

Backup Resources

Apply

Summary

Cloud repositories:

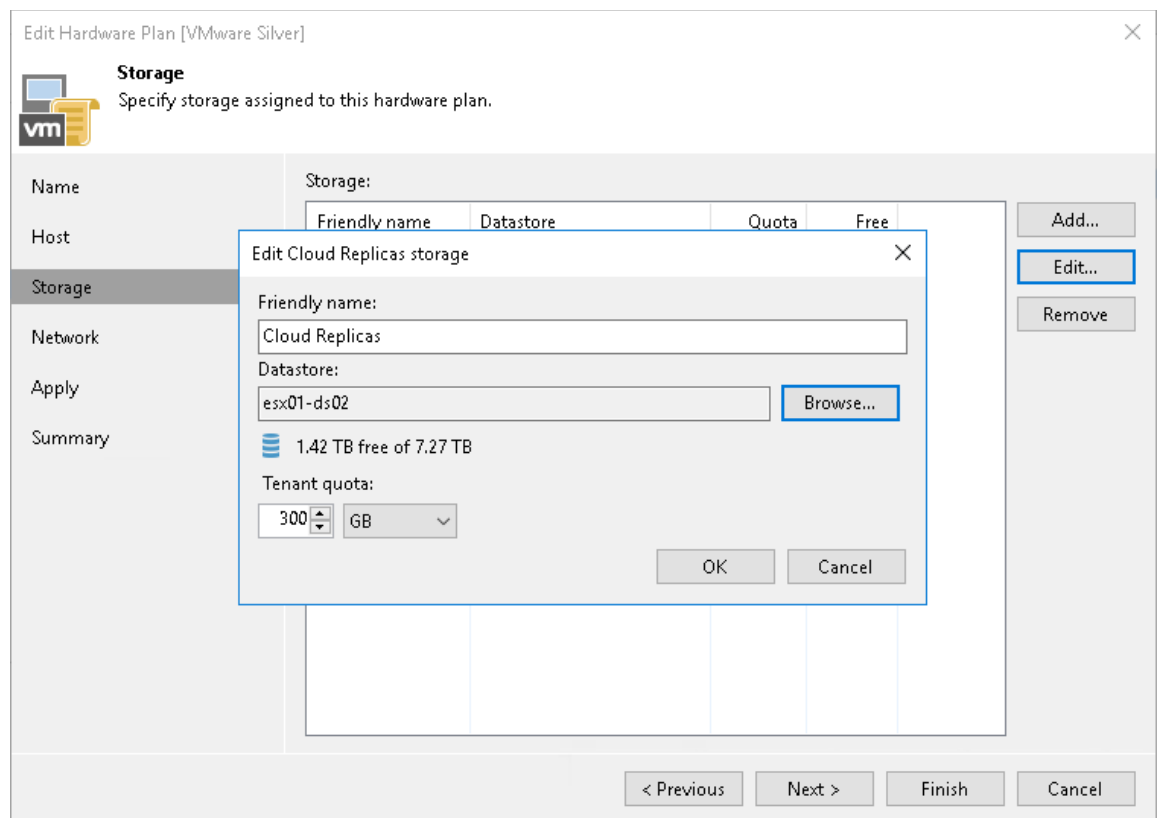
Repository	Friendly name	Quota	Available	WAN
Default Backup Repository	Cloud Vol 01	100,0 GB	351,2 MB free of 8...	Not set

☐ Keep deleted backup files for days

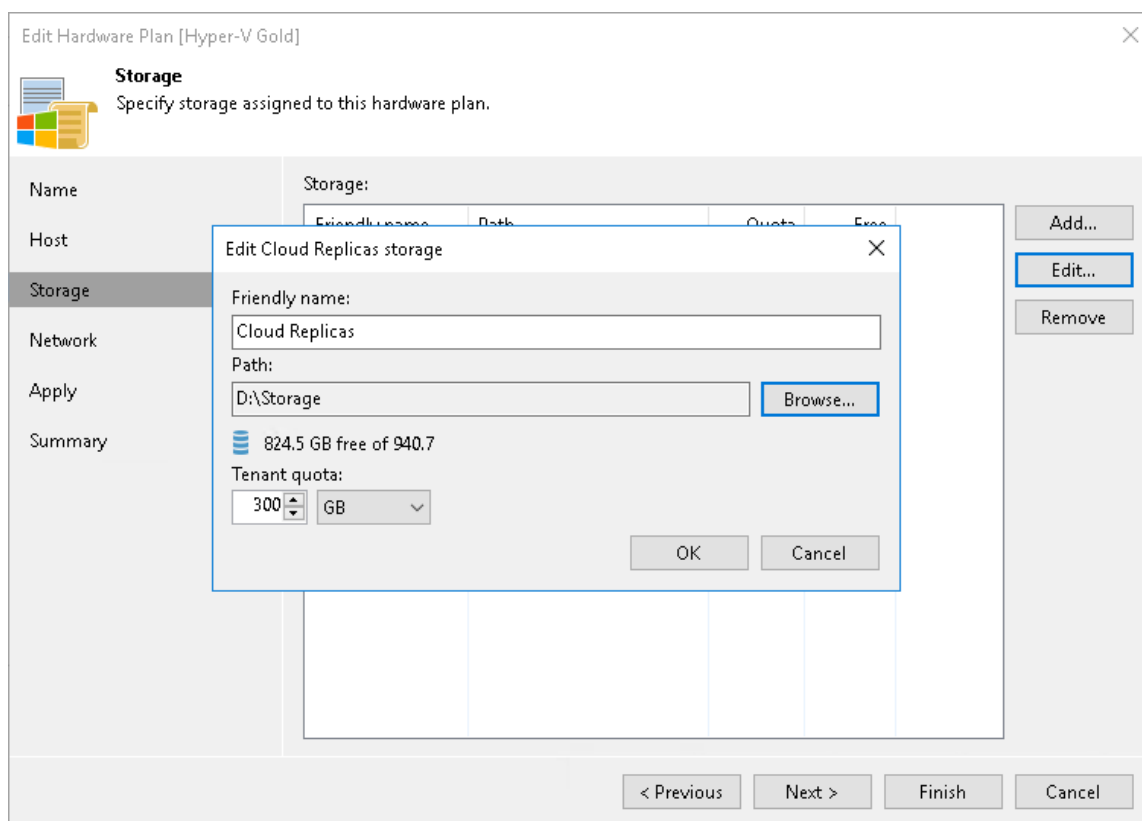
For added tenant protection against insider attacks, we will preserve all deleted backup files for the set number of days. The deleted backups will not count towards tenant's quota consumption, and cannot be managed by the tenant.

< Previous **Next >** Finish Cancel

2. Move tenant data from the initial location to the new location:
 - [For VMware vSphere] Use Storage vMotion to move tenant VM replicas to the new datastore.
 - [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.



- Click **OK**.
 - At the **Apply** step of the wizard, wait until Veeam Backup & Replication updates the hardware plan settings. Then click **Finish**.
- Deploy the new SP-side network extension appliances in the new location where you have moved tenant VM replicas.
 - Open the **Cloud Connect** view.
 - In the inventory pane, click **Tenants**.
 - In the working area, right-click the necessary tenant and select **Properties**.
 - At the **Replica Resources** step of the wizard, select the **Use built-in network management capabilities during failover** check box.
 - 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](#).
 - 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.

Edit ABC Company

Network Extension
Specify network settings to be used during failover.

Tenant

Bandwidth

Backup Resources

Replica Resources

Network Extension

Apply

Summary

Network extension appliances:

Network Settings

Network extension appliance:
Network Extension Appliance ABC Company(esx01)

External network:
VM Network

IPv4 address: **Obtain automatically**

IPv6 address: **Obtain automatically**

OK Cancel

☒ Allocate 1 public IPv4 addresses

☒ Allocate 1 public IPv6 addresses

Public IP addresses are required for tenants to be able to perform full site failover. [Manage...](#)

< Previous Apply Finish Cancel

Veeam Backup & Replication will deploy the new SP-side network extension appliances 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.

Scanning Tenant Backups

The scan backup functionality allows the SP to scan tenant backups stored in cloud repositories for malware. The SP can use this functionality to check tenant backups for infected restore points and to identify the last clean restore point that can be used for recovery. As a result, the SP can detect which restore points are infected and which are safe to use for recovery.

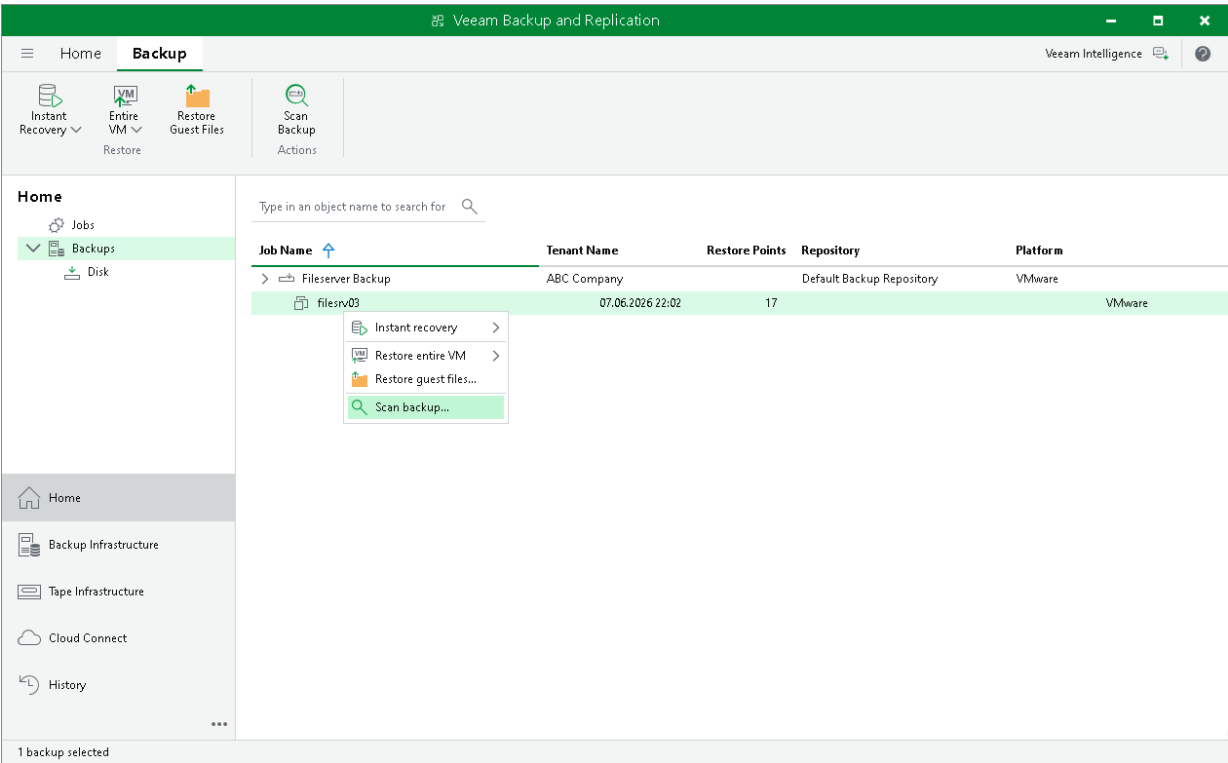
The SP scans tenant backups on the SP backup server with an antivirus software, YARA rules, or both. The scan can be performed for backups created by tenant backup jobs and backup copy jobs that target cloud repositories.

For details, see the [Scan Backup](#) section in the Veeam Backup & Replication User Guide.

To scan a tenant backup, do the following:

1. Open the **Home** view.
2. Select the **Backups** node in the inventory pane.
3. Expand the backup job in the working area, click **Scan Backup** on the ribbon or right-click the necessary VM in the backup job and select **Scan backup**.

To get a detailed description of the scan backup configuration, see the [Configuring Scan Backup Session](#) section in the Veeam Backup & Replication User Guide.



Managing Tenant Cloud Failover Plans

A cloud failover plan created by a tenant is stored in the database on the SP 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 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.

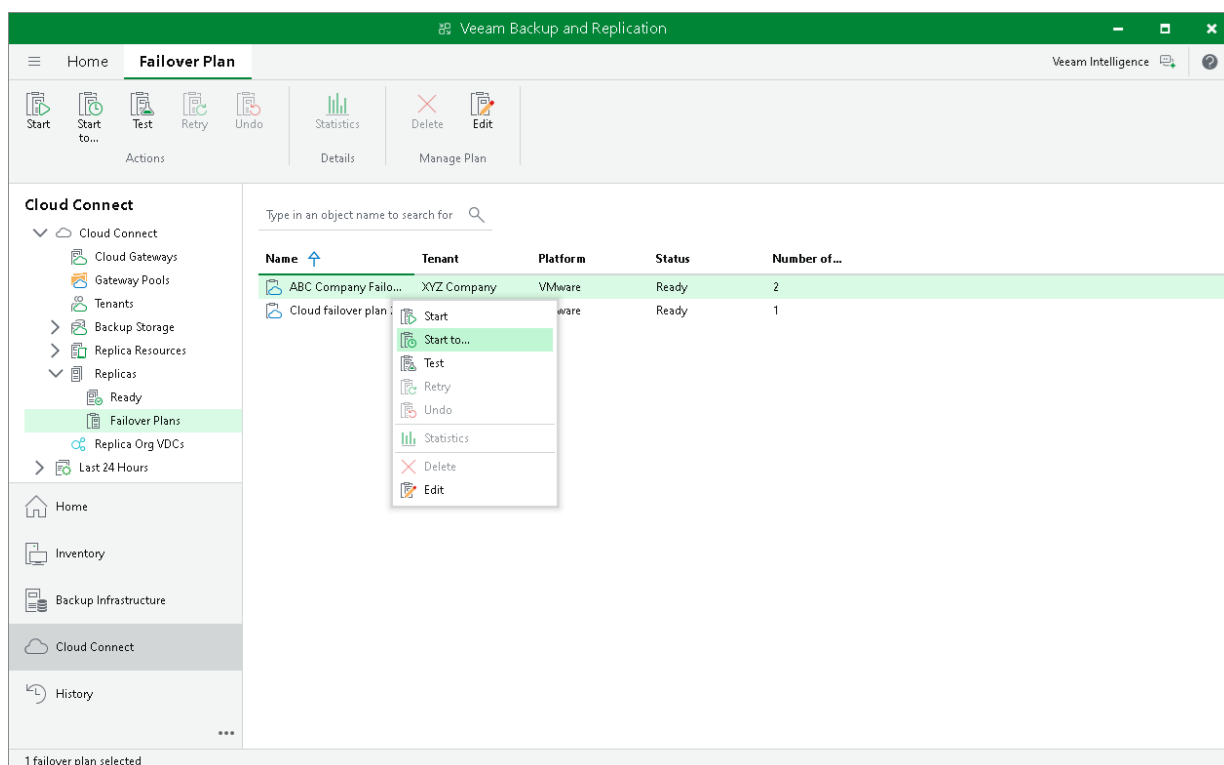
The SP can run a tenant cloud failover plan from the Veeam Backup & Replication console on the SP Veeam backup server.

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 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.

This operation is supported for cloud failover plans that contain snapshot-based replicas and failover plans that contain CDP replicas.

NOTE

Consider the following limitations:

- Veeam Backup & Replication does not support this operation for failover plans that contain CDP replicas with I/O filters older than version 12.1 installed on the cluster where the VMs that you plan to protect reside and where replicas will reside. To learn more about updating I/O filters, see the [Updating and Uninstalling I/O Filter](#) section in the Veeam Backup & Replication User Guide.
- If the SP starts the cloud failover plan test for CDP replicas created with Veeam Backup & Replication version 12.2 (or earlier), long-term retention policy creation will be stopped while testing.

TIP

To keep CDP replica VMs running, for example, to reach data from the VM or from an application installed on the VM, you can use Veeam PowerShell cmdlets. To perform the operation, use the *KeepAlive* parameter. For detailed instructions, see the [Start-VBRFailoverPlan](#) section in the Veeam PowerShell Reference.

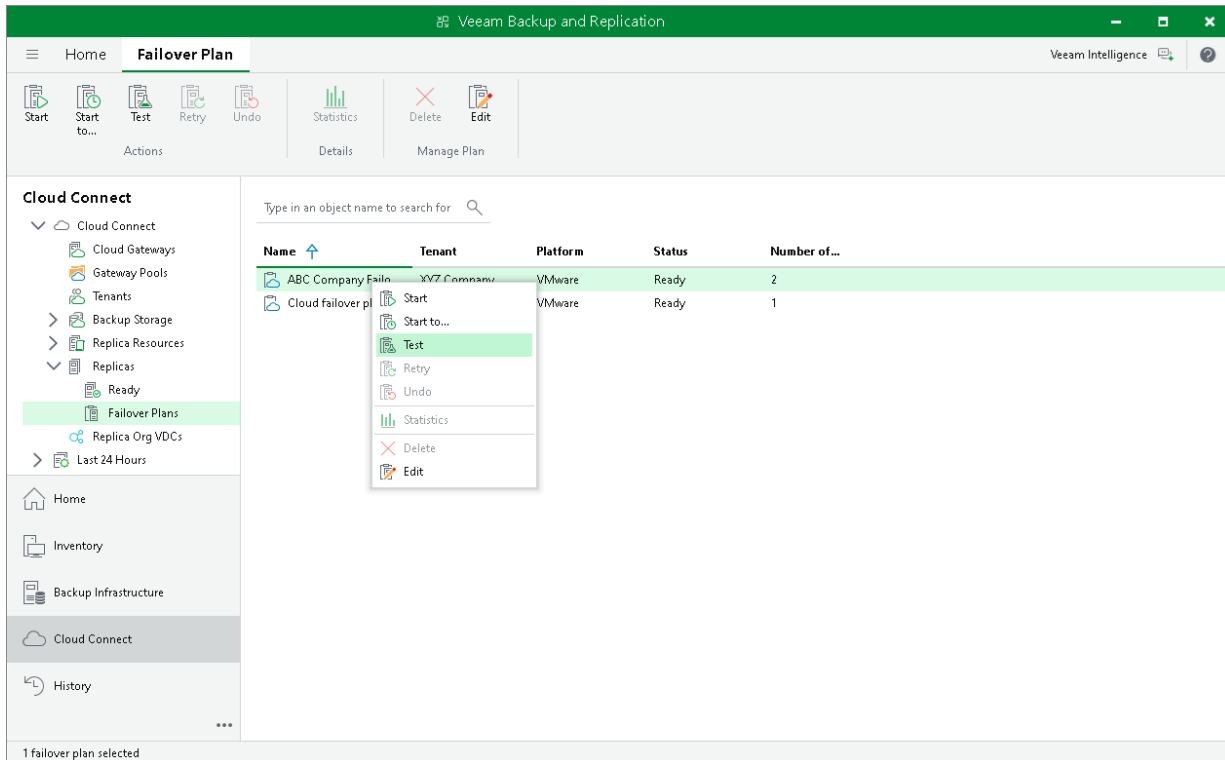
The following limitations apply to the operation:

- You can use the keep alive mode only for cloud failover plans that contain CDP replicas. This operation is not supported for cloud failover plans that contain snapshot-based replicas.
- By default, this operation is available only for the SP. The SP can use the `CdpTenantTestFailoverKeepAliveDurationLimitMin` registry key to allow this operation to tenants. The key also defines the allowed keep alive time for tenant CDP replicas. For details, see [Allowing Tenants to Keep CDP Replicas Running](#).

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**.



Allowing Tenants to Keep CDP Replicas Running

The SP can use a registry key to let tenants keep CDP replica VMs running while testing cloud failover plans. The registry key allows the tenant to keep CDP replicas running and limits the allowed duration of the keep alive mode.

To use the registry key, complete the following steps:

1. On the SP Veeam backup server, launch the Registry Editor.
2. Create the key `HKEY_LOCAL_MACHINE\SOFTWARE\Veeam\Veeam Backup and Replication\CdpTenantTestFailoverKeepAliveDurationLimitMin (REG_SZ)`.
3. As a registry value, enter the number of minutes to set the keep alive time for CDP replicas.

You can set CDP replicas to run in the keep alive mode for a maximum of 24 hours.

Retrying Cloud Failover Plan

The SP can retry failover by a tenant 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**.

The screenshot shows the Veeam Backup and Replication console with the 'Failover Plan' tab selected. The left sidebar shows the 'Cloud Connect' view expanded, with 'Replicas' > 'Failover Plans' selected. The main area displays a table of failover plans. A context menu is open over the 'Cloud failover plan' row, with 'Retry' highlighted.

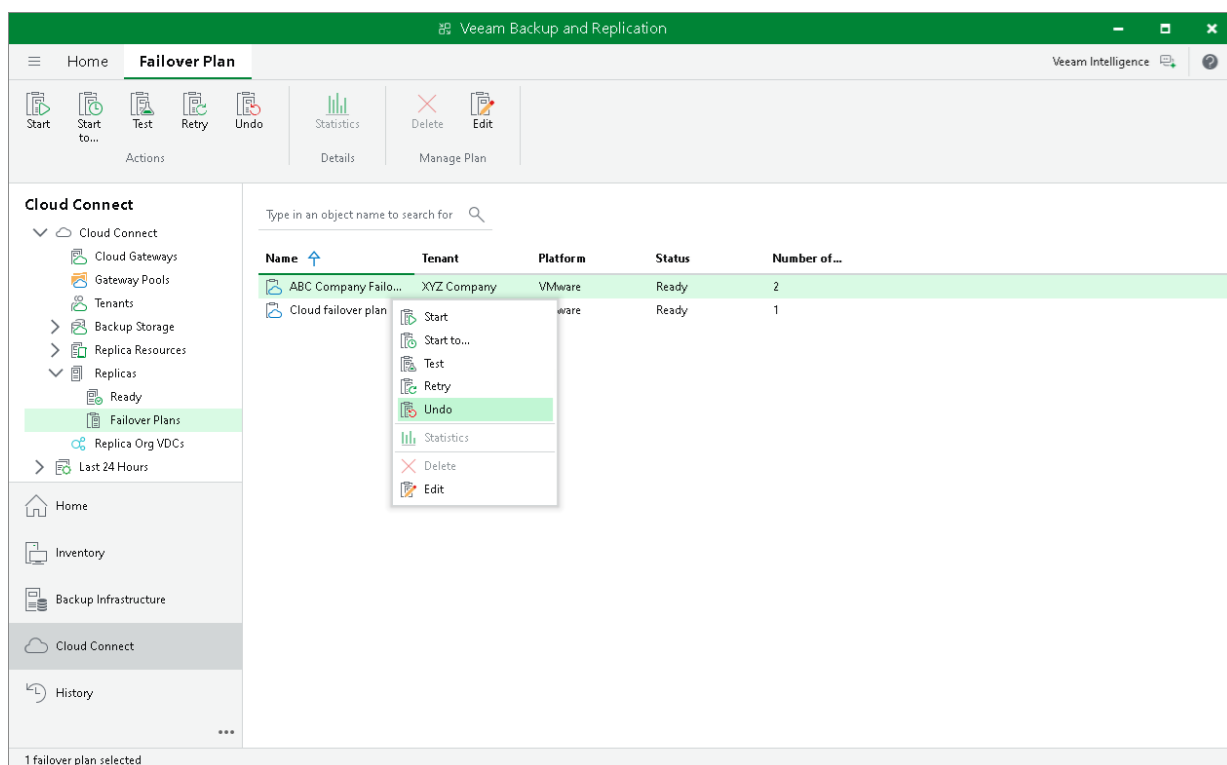
Name	Tenant	Platform	Status	Number of...
ABC Company Failo...	XYZ Company	VMware	Ready	2
Cloud failover plan		ware	Ready	1

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 after the tenant 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 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 files.

The screenshot shows the 'Edit Cloud Failover Plan' wizard for 'ABC Company Failover Plan'. The 'Failover Plan' step is active, showing a left sidebar with 'Failover Plan', 'Machines', and 'Summary'. The main area contains fields for 'Name' (ABC Company Failover Plan) and 'Description' (Cloud failover plan for ABC Company full site failover). Below these are two checked checkboxes: 'Pre-failover script' and 'Post-failover script'. Each has a text field with a file path (C:\scripts\pre-failover.bat and C:\scripts\post-failover.bat respectively) and a 'Browse...' button. At the bottom are navigation buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

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.

The screenshot shows the Veeam Backup and Replication console. The 'Replica' view is active. The 'Cloud Connect' pane on the left shows the 'Replicas' folder selected. The main pane displays a table of replicas. A context menu is open over the first replica, showing the 'Permanent failover...' option highlighted.

Name	Job Name	T...	S...	C...	Creation Time	R...	Original Loc...	Replica Loca...	Platform
filesrv04	XYZ Replicati...	Regul...	Ready	None	18.11.2025 22:11	2	XYZ Company	vcenter01.tech.lo...	VMware
filesrv03	Failover now...			None	18.11.2025 22:11	2	XYZ Company	vcenter01.tech.lo...	VMware
websrv03.tech.local	Planned failover...			N/A	19.11.2025 8:05	3	XYZ Company	vcenter01.tech.lo...	Server
websrv04.tech.local	Undo failover			N/A	19.11.2025 8:05	3	XYZ Company	vcenter01.tech.lo...	Server

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 \(over the internet\).](#)
- [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 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:

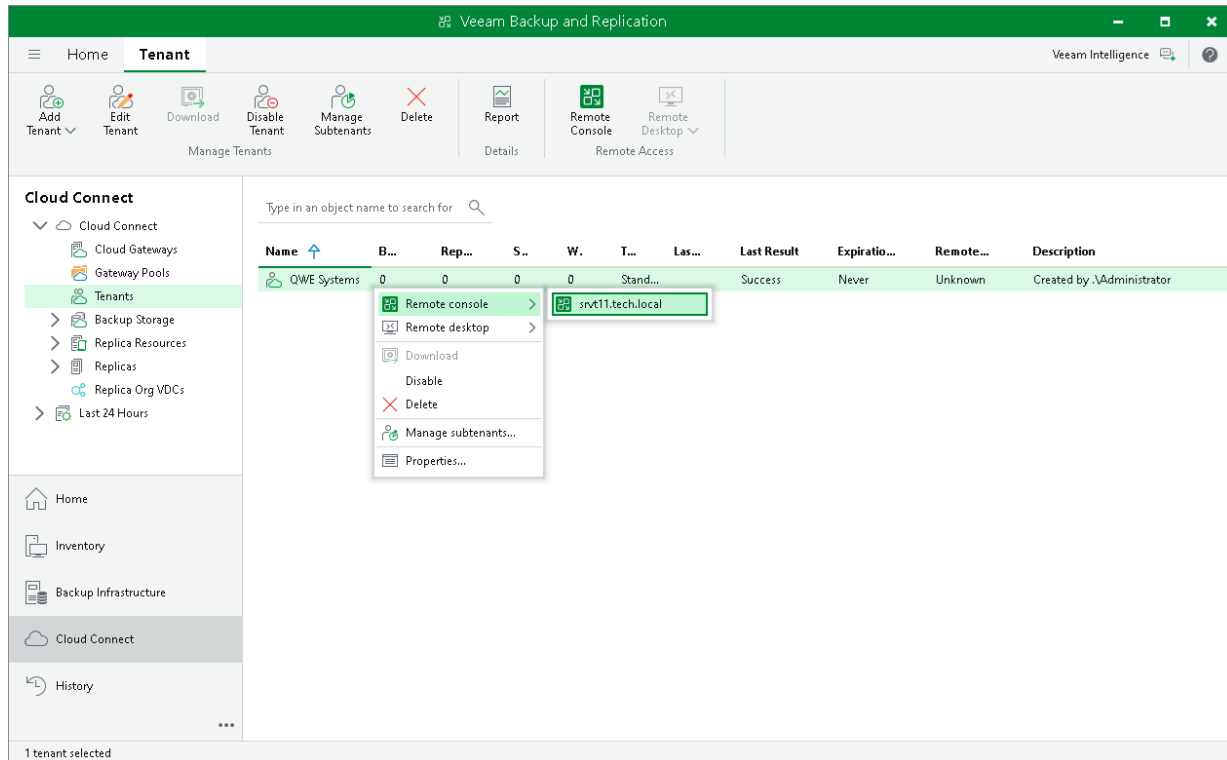
- Double-click the **Veeam Backup & Replication Remote Access Console** icon on the desktop (you can use this option only if you want to open the Remote Access Console on the SP backup server).
- Run the following command:

```
"%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. Connect to SP Backup Server

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:

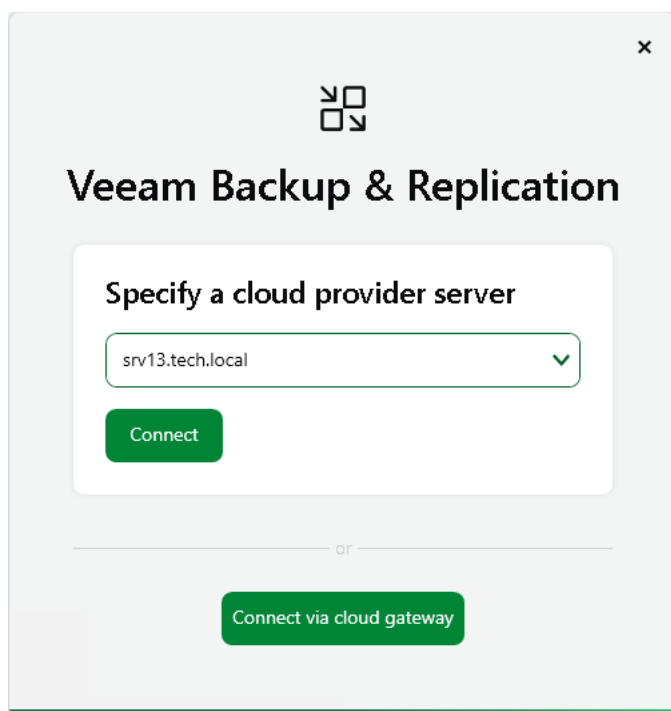
- If the Remote Access Console is deployed in the SP Veeam Cloud Connect infrastructure, you must specify settings to connect directly to the SP backup server. To learn more, see [Direct Connection](#).
- If the Remote Access Console is deployed on a remote machine in an external network, you must specify settings to connect to the SP backup server through a cloud gateway. To learn more, see [Connection Through Cloud Gateway](#).

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 connect to the SP backup server:

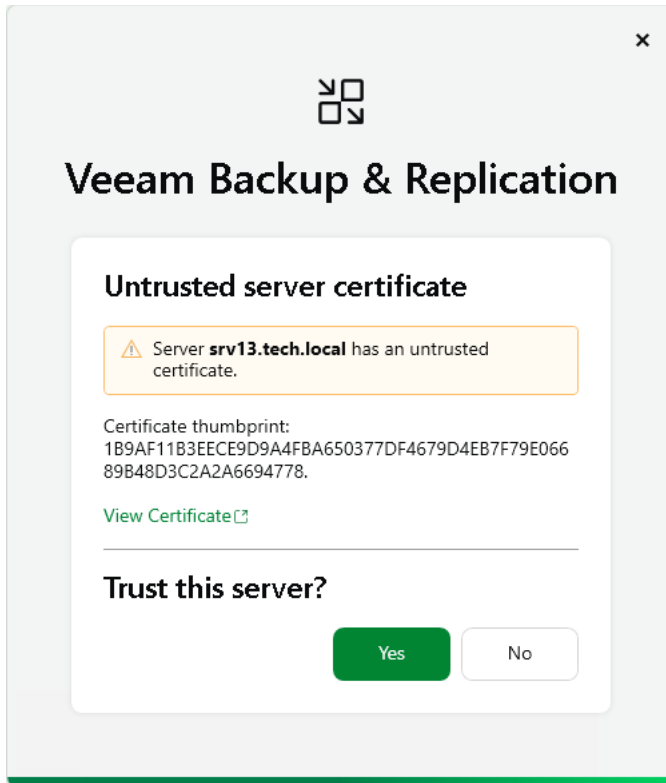
1. At the **Specify a cloud provider server** step, type the name or IP address of the SP backup server or select it from the list of recent connections. Then click **Connect**.

If you open the Remote Access Console on the SP backup server, by default, the backup server field contains the name of this backup server — *localhost*.

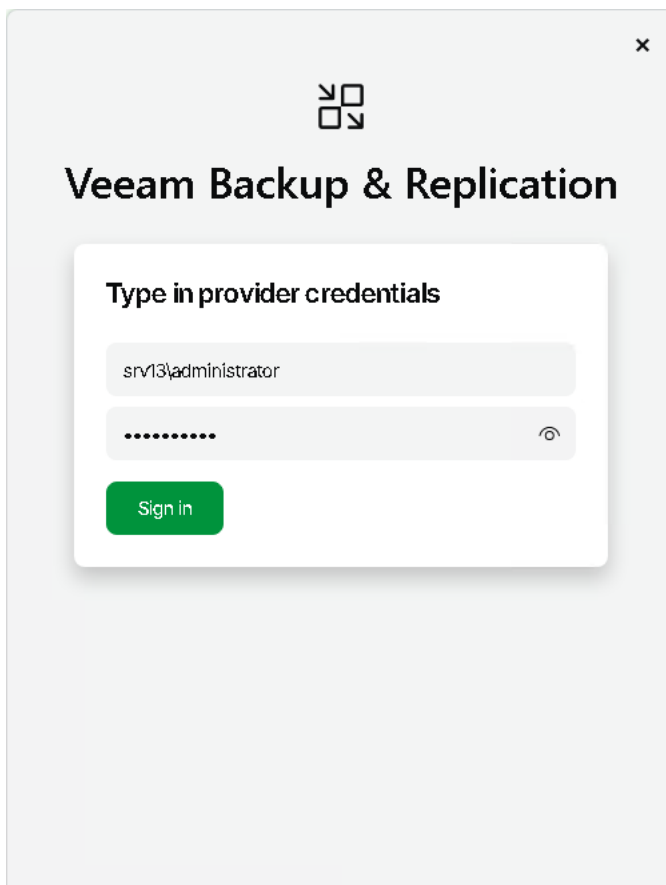


The screenshot shows a dialog box titled "Veeam Backup & Replication" with a close button (X) in the top right corner. Inside the dialog, there is a section titled "Specify a cloud provider server". Below this title is a text input field containing "srv13.tech.local" and a green checkmark icon on the right. Below the input field is a green button labeled "Connect". Below this section, there is a horizontal line with the word "or" in the center. Below the line is another green button labeled "Connect via cloud gateway".

- At the **Server certificate** step, select if you trust the server certificate. Click **Yes**.



- At the **Type in provider credentials** step, enter the user name and password of the 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.



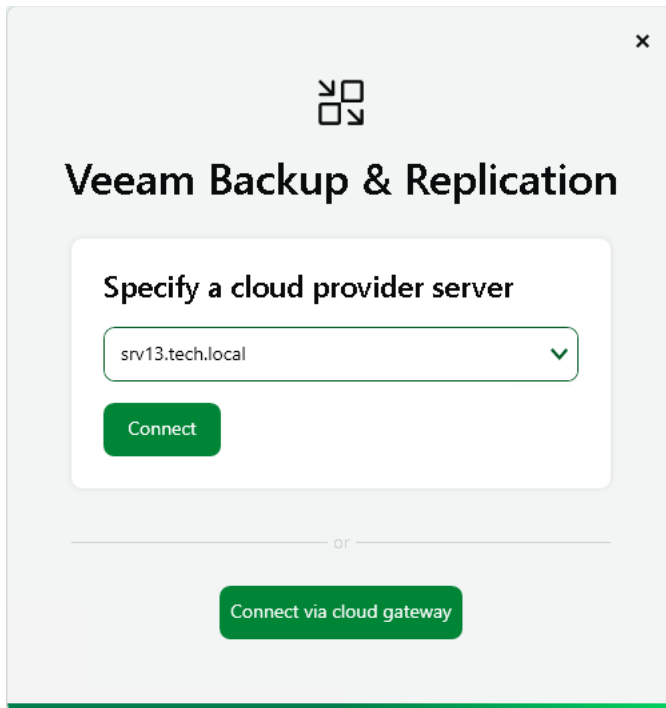
4. Click **Sign in**.

You will proceed to the steps to connect to the tenant backup server. For details, see [Connect to Tenant Backup Server](#).

Connection Through Cloud Gateway

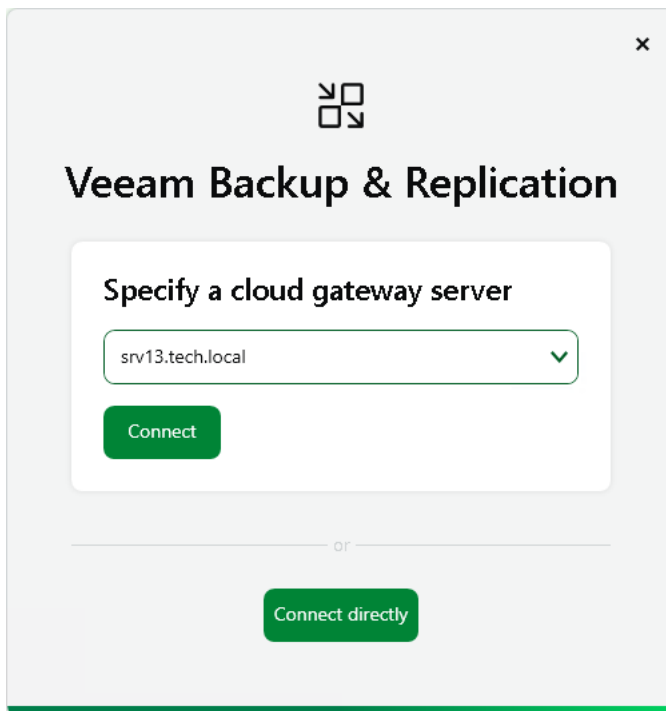
If the Remote Access Console is deployed on a remote machine connected to an external network, you must specify settings to connect to the SP backup server from the internet through a cloud gateway. To specify connection settings:

1. At the **Specify a cloud provider server** step, click **Connect via cloud gateway**.



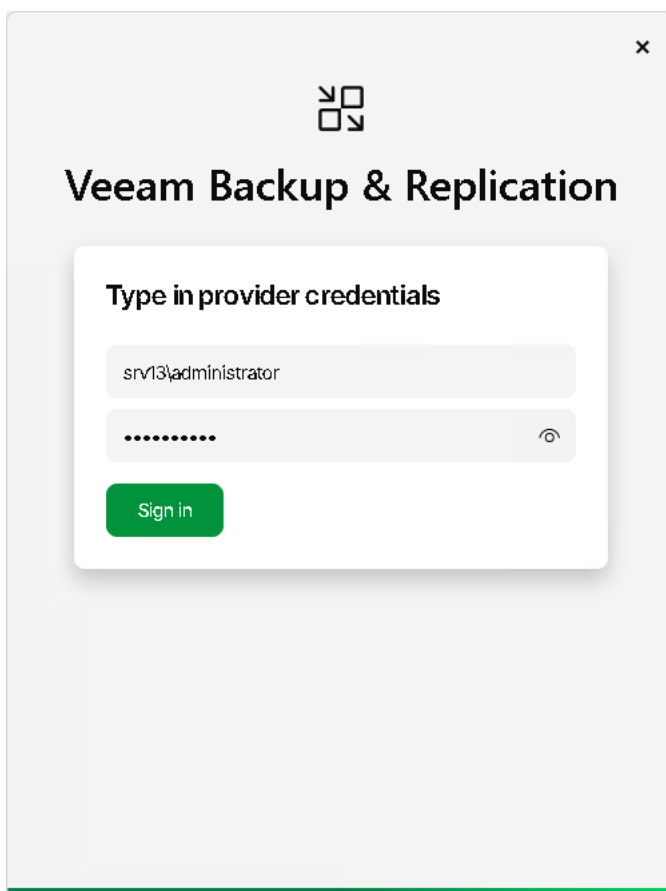
The screenshot shows a web interface for Veeam Backup & Replication. At the top, there is a logo consisting of four squares arranged in a larger square, with the text "Veeam Backup & Replication" below it. The main content area is titled "Specify a cloud provider server". Below this title, there is a text input field containing "srv13.tech.local" and a green checkmark icon to its right. Below the input field is a green button labeled "Connect". Below the "Connect" button is a horizontal line with the word "or" in the center. Below the line is a green button labeled "Connect via cloud gateway". The entire interface is enclosed in a light gray box with a close button (X) in the top right corner.

2. At the **Specify a cloud gateway server** step, type the name or IP address of the cloud gateway or select it from the list of recent connections. Then click **Connect**.



The dialog box is titled "Veeam Backup & Replication" and features a close button (X) in the top right corner. Below the title bar is a Veeam logo. The main heading is "Specify a cloud gateway server". There is a text input field containing "srv13.tech.local" with a green checkmark icon on the right. Below the input field is a green "Connect" button. A horizontal line with the word "or" in the center separates this section from the bottom section, which contains a green "Connect directly" button.

3. At the **Type in provider credentials** step, enter the user name and password of the 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.



The dialog box is titled "Veeam Backup & Replication" and features a close button (X) in the top right corner. Below the title bar is a Veeam logo. The main heading is "Type in provider credentials". There are two input fields: the first contains "srv13\administrator" and the second contains a masked password "....." with an eye icon on the right. Below the input fields is a green "Sign in" button.

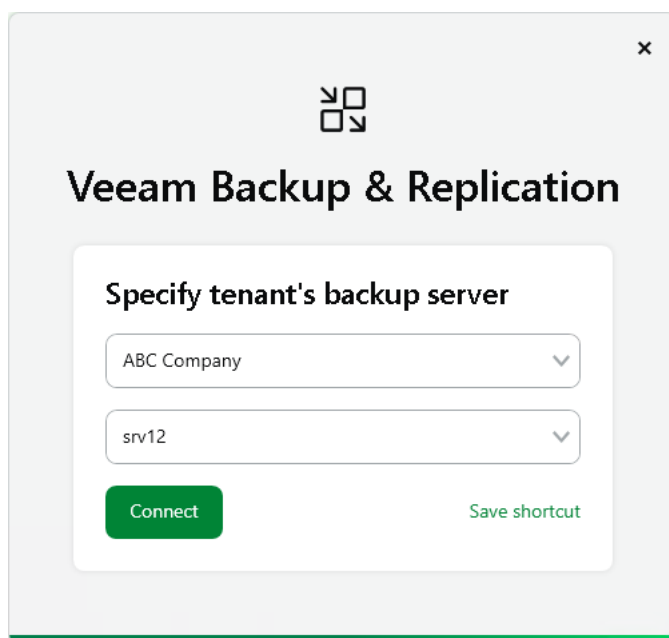
4. Click **Sign in**.

You will proceed to the steps to connect to the tenant backup server. For details, see [Connect to Tenant Backup Server](#).

Step 3. Connect to Tenant Backup Server

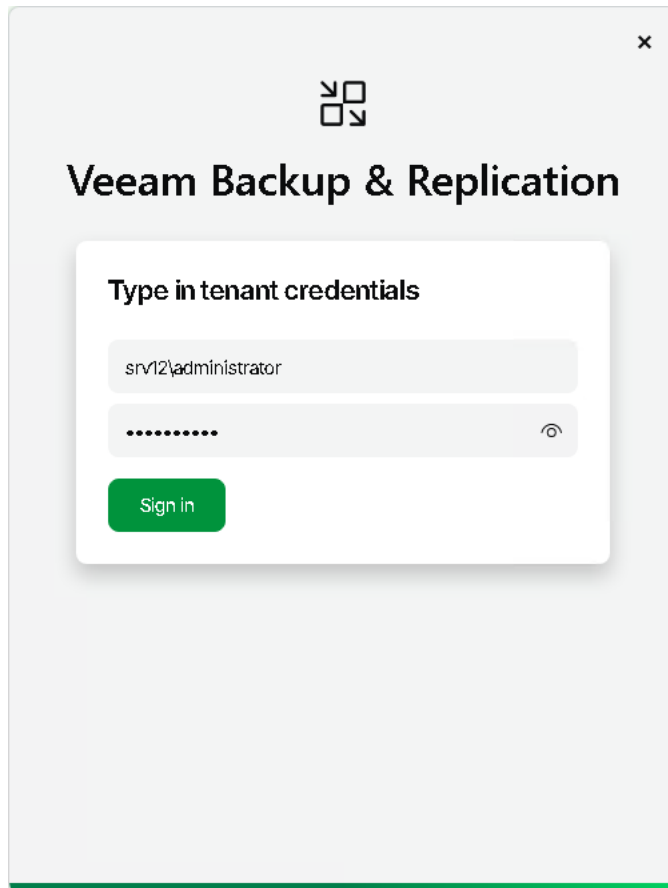
To log on to Veeam Backup & Replication on the tenant side, you must specify connection settings to access the tenant backup server.

1. At the **Specify tenant's backup server** step, do the following:
 - a. From the drop-down list, select 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.
 - b. From the drop-down list, select 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.
 - c. To create a shortcut for the connection, click **Save shortcut**. You can create as many shortcuts as you need.
 - d. Click **Connect**.



The screenshot shows a dialog box titled "Veeam Backup & Replication" with a close button (X) in the top right corner. Inside the dialog, there is a section titled "Specify tenant's backup server". This section contains two drop-down menus. The first menu is labeled "ABC Company" and the second menu is labeled "srv12". Below these menus are two buttons: a green "Connect" button and a green "Save shortcut" button.

2. At the **Type in tenant credentials** step, 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).

A screenshot of the Veeam Backup & Replication login dialog. The dialog has a light gray background with a dark gray border. At the top center is the Veeam logo, consisting of four squares arranged in a 2x2 grid. Below the logo is the title "Veeam Backup & Replication" in a bold, black font. In the center is a white rectangular box with a subtle shadow. Inside this box, the text "Type in tenant credentials" is displayed in a bold, black font. Below this text are two input fields. The first field contains the text "srv12\administrator". The second field contains a series of dots, indicating a password, and has a small eye icon to its right. Below the input fields is a green button with the text "Sign in" in white. The dialog has a close button (an 'x' icon) in the top right corner.

3. Click **Sign in**.

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:

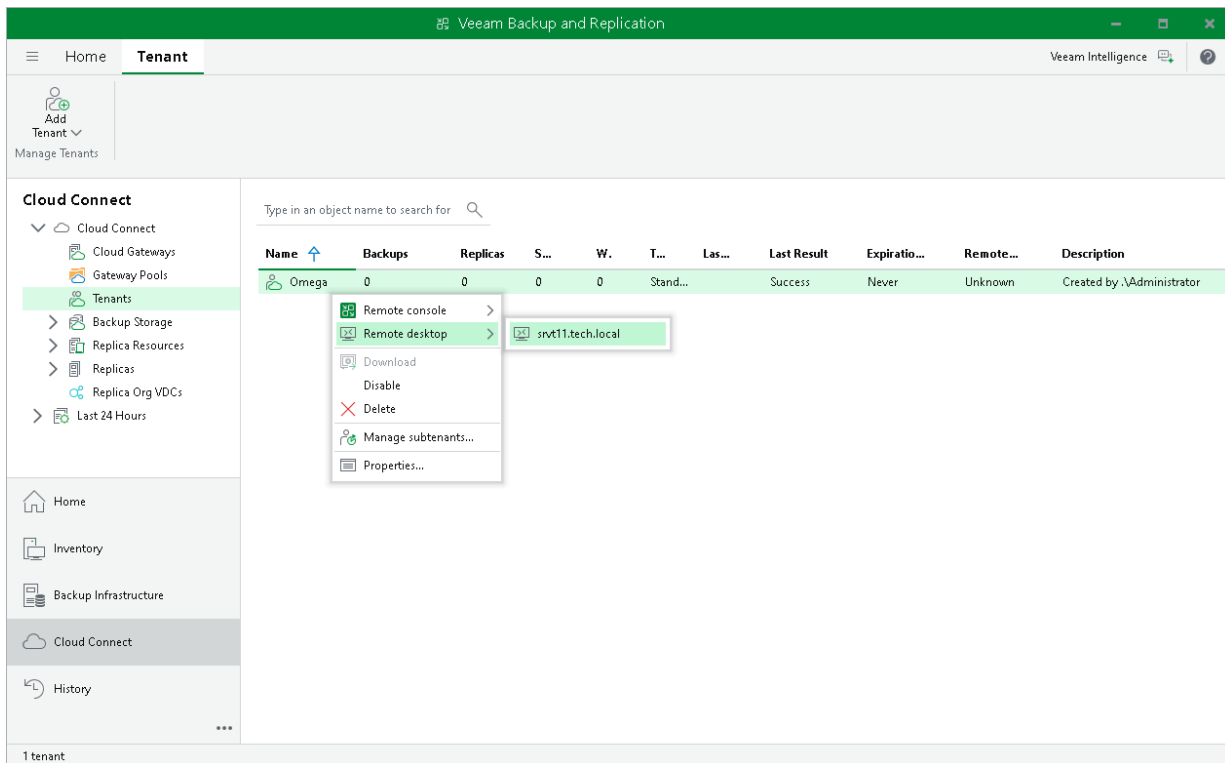
- The tenant backup server must run the Microsoft Windows OS.
- The OS running on the tenant backup server must be set up to accept remote desktop connections.

To launch a remote desktop session:

1. Do either of the following:
 - 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.
 - 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.
 - 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.
2. 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](#).

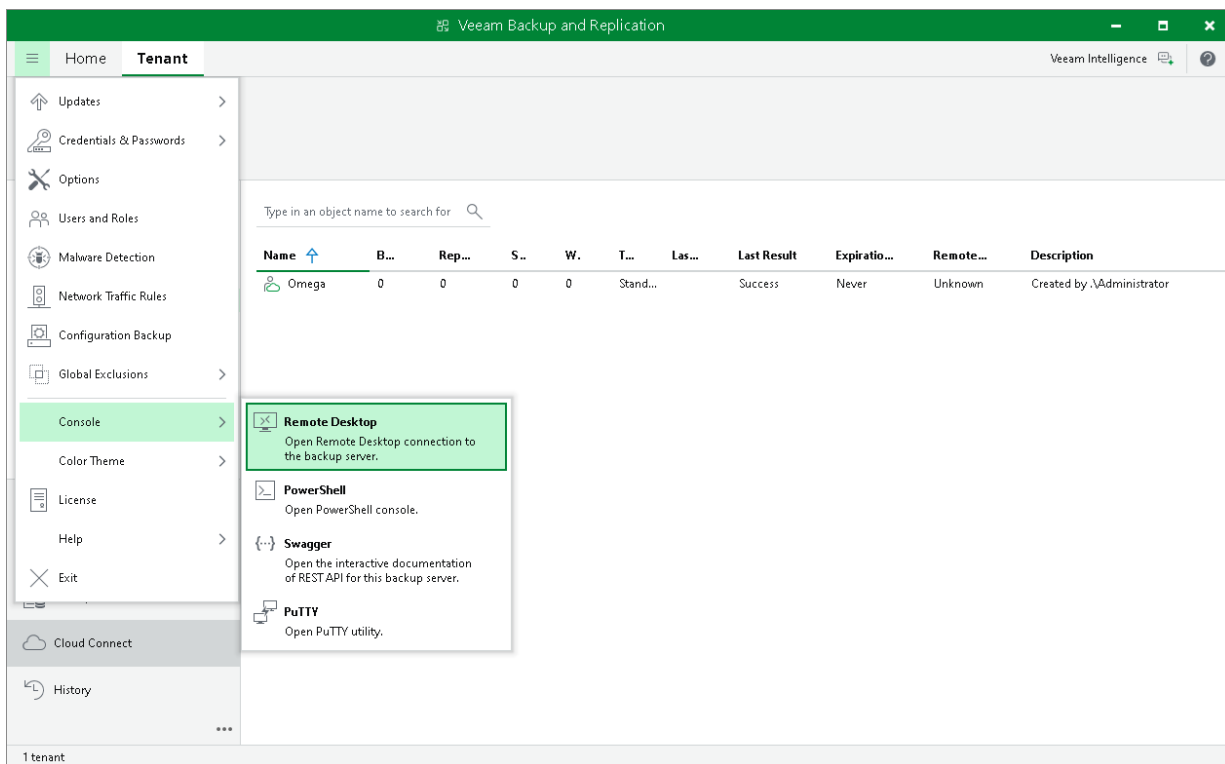


Establishing Remote Desktop Connection to Backup Server

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 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 **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.

The screenshot shows the 'Options' dialog box with the 'Security' tab selected. The 'Cloud Connect' section is expanded, showing the checkbox 'Accept remote console connection requests originating from the Internet' which is checked. Other sections visible include 'Backup server certificate', 'Host authentication', 'FIPS compliance', and 'Audit logs location'.

Veeam Intelligence	Notifications	History
I/O Control	Security	Email Settings
		Event Forwarding

Backup server certificate

Self-signed
CN=srv13 [Install...](#)

Host authentication

Trusted hosts: 3 [Export...](#)

Trusted hosts list:

☒ Add all discovered hosts to the list automatically

☐ Add unknown hosts to the list manually (more secure) [Import...](#)

Cloud Connect

☒ Accept remote console connection requests originating from the Internet

FIPS compliance

☐ Force strict FIPS compliance mode

Terminate connections to all external data sources, hosts and API endpoints that do not implement FIPS compliant encryption. Veeam's own encryption modules operate exclusively in FIPS compliant mode and are not affected by this setting.

Audit logs location

C:\ProgramData\Veeam\Backup\Audit [Browse...](#)

☒ Compress older audit logs automatically (saves disk space)

Consider disabling this option when using a WORM storage for audit logs.

[OK](#) [Cancel](#) [Apply](#)

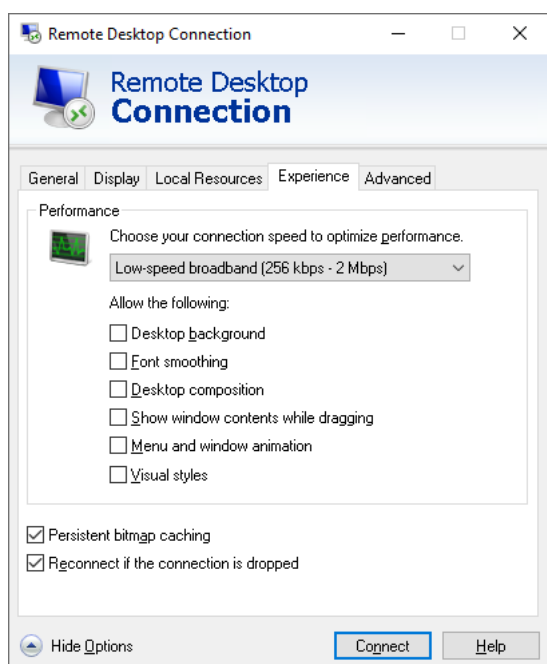
Adjusting Remote Desktop Connection Settings

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 may 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.](#)

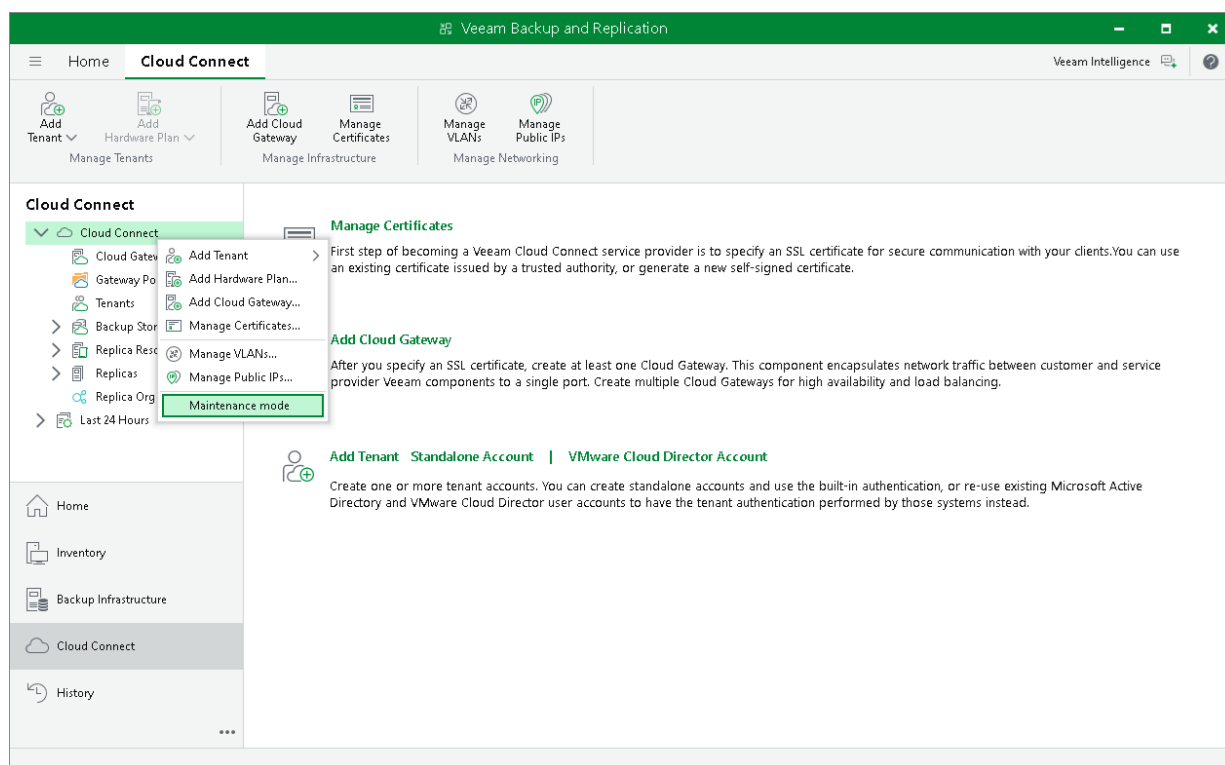
Switching to Maintenance Mode

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 backup copy jobs that the SP backup server is under maintenance and cloud resources are temporary unavailable.

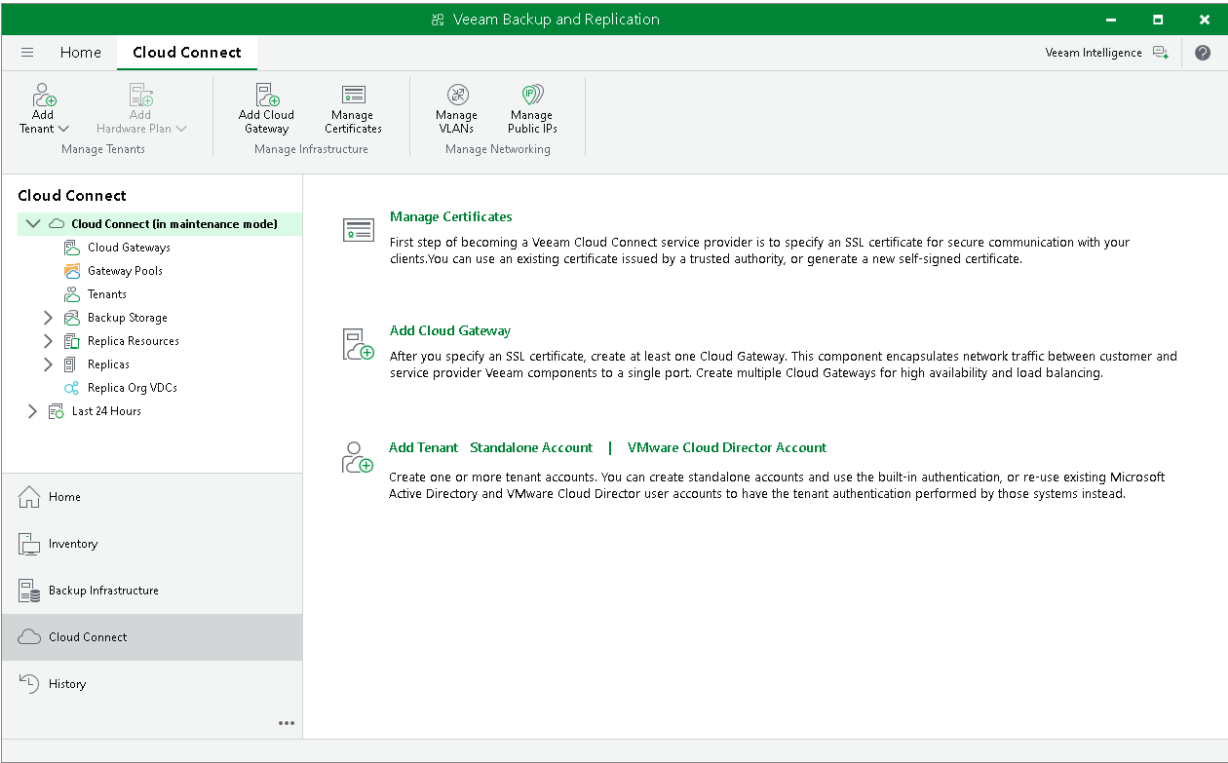
To switch the SP backup server to the Maintenance mode:

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, Veeam Backup & Replication informs you about the impact of maintenance mode on tenant jobs. Click **Yes**.
4. If there are any replicas in the *Failover* or *Failback* state, Veeam Backup & Replication displays a window informing you about the impact of maintenance mode on active replication tasks. 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**.

- At the **Name** step of the wizard, specify a name and description for the backup to tape job.
To avoid problems with long paths, it is recommended to create job names not longer than 50 characters.

The screenshot shows the 'New Backup to Tape Job' wizard at the 'Name' step. The left sidebar contains a vertical list of steps: Name (highlighted in green), Backups, Media Pool, Incremental Backup, Options, Schedule, and Summary. The main area is titled 'Name' and contains the instruction 'Type in a name and description for this tape job.' Below this, there are two input fields: 'Name:' with the text 'Tenants Backup to Tape' and 'Description:' with the text 'Backup job to write tenant backups to tape'. At the bottom right, there are four buttons: '< Previous' (disabled), 'Next >' (active/highlighted), 'Finish' (disabled), and 'Cancel'.

- At the **Backups** step of the wizard, click **Add > Tenants** and select tenants or cloud repositories whose data you want to write to tape.

The screenshot shows the 'New Backup to Tape Job' wizard at the 'Backups' step. The left sidebar contains a vertical list of steps: Name, Backups (highlighted in green), Media Pool, Incremental Backup, Options, Schedule, and Summary. The main area is titled 'Backups' and contains the instruction 'Specify objects to be processed by this tape job.' Below this, there is a table with the following data:

Name	Type	Size
ABC Company	Tenant	11,7 GB
TechCompanyOrg\Cloud Vol 01	Quota	3,2 MB

To the right of the table, there are three buttons: '+ Add...' (green), '- Remove' (red), and 'Up' (blue) and 'Down' (blue) arrows. At the bottom right, there is a summary of the backup sizes: 'Full: 11,6 GB' and 'Incremental: 0 B'. At the bottom, there are four buttons: '< Previous' (disabled), 'Next >' (active/highlighted), 'Finish' (disabled), and 'Cancel'.

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](#).

The screenshot shows the 'New Backup to Tape Job' wizard window. The 'Media Pool' step is selected in the left sidebar. The main area displays the 'Media Pool' configuration. A dropdown menu for 'Media pool:' is open, showing 'GFS Media Pool 2 (HP MSL G3 Series 9,50)' and an 'Add new...' link. Below the dropdown, various settings are listed: Tapes (2), Free space (79,9 GB), Daily (14 days; use any available media; append; do not export), Weekly (4 weeks; use any available media; do not append; do not export), Monthly (12 months; use any available media; do not append; do not export), Quarterly (4 quarters; use any available media; do not append; do not export), Yearly (1 years; use any available media; do not append; do not export), Parallel processing (2 drives, multiple backup chains), Encryption (Disabled), and WORM (False). At the bottom, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

Media Pool	
Specify the media pool to perform backup to.	
Media pool:	GFS Media Pool 2 (HP MSL G3 Series 9,50) Add new...
Tapes:	2
Free space:	79,9 GB
Daily:	14 days; use any available media; append; do not export;
Weekly:	4 weeks; use any available media; do not append; do not export;
Monthly:	12 months; use any available media; do not append; do not export;
Quarterly:	4 quarters; use any available media; do not append; do not export;
Yearly:	1 years; use any available media; do not append; do not export;
Parallel processing:	2 drives, multiple backup chains
Encryption:	Disabled
WORM:	False

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.

The screenshot shows the 'New Backup to Tape Job' dialog box with the 'Options' tab selected. The left sidebar contains links for Name, Backups, Media Pool, Options (highlighted), Schedule, and Summary. The main area is titled 'Options' and contains the following settings:

- Media automation**
 - ☒ **Eject tape media upon job completion**
This option makes the job automatically eject tape from drives upon completion, so that tape does not stay in the drive, which is a best practice.
 - ☒ **Export the following media sets upon job completion** [Media Sets...](#)
This option makes the job automatically close and export selected GFS media sets.
- Drive usage**
 - ☐ Limit the number of drives this job can use to: tape drives

At the bottom, there is a link for [Advanced tape job settings](#) and four buttons: '< Previous', 'Next >' (highlighted), 'Finish', and 'Cancel'.

6. Click **Advanced** and specify the necessary settings for the tape job.

- 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.

The screenshot shows the 'New Backup to Tape Job' wizard at the 'Schedule' step. The left sidebar contains a vertical list of steps: Name, Backups, Media Pool, Options, Schedule (highlighted in green), and Summary. The main content area is titled 'Schedule' and includes a description: 'Specify the job scheduling options. You can only set schedule for those media pools which have the corresponding media set enabled in GFS media pool's properties.' Below this is a 'Schedule' section with a text box stating: 'This Backup to Tape job will synthesize a full backup file to archive to tape using the latest restore point available in the source backup repository at the specified time.' A dropdown menu for 'Start daily scan for GFS restore points at:' is set to '00:00'. Below this are five rows of backup frequency options: 'Daily backup: Every day', 'Weekly backup: Saturday', 'Monthly backup: First Sunday of the month', 'Quarterly backup: First Sunday of the quarter', and 'Yearly backup: First Sunday of the year'. A green 'Schedule...' link is to the right of the daily backup option. At the bottom right are four buttons: '< Previous', 'Apply' (highlighted with a green border), 'Finish', and 'Cancel'.

- 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.

The screenshot shows the 'New Backup to Tape Job' wizard at the 'Summary' step. The left sidebar shows the same list of steps as the previous screenshot, with 'Summary' now highlighted in green. The main content area is titled 'Summary' and includes the text: 'You can copy the configuration information below for future reference.' Below this is a large text box containing the following information: 'Name: Tenants Backup to Tape', 'Media pool for full backups: GFS Media Pool 2', and 'PowerShell cmdlet for starting the job: Get-VBRTapeJob -Name "Tenants Backup to Tape" | Start-VBRJob'. At the bottom left of the main area is a checkbox labeled 'Run the job when I click Finish', which is checked with a green checkmark. At the bottom right are four buttons: '< Previous', 'Next >' (disabled), 'Finish' (highlighted with a green border), and 'Cancel'.

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.

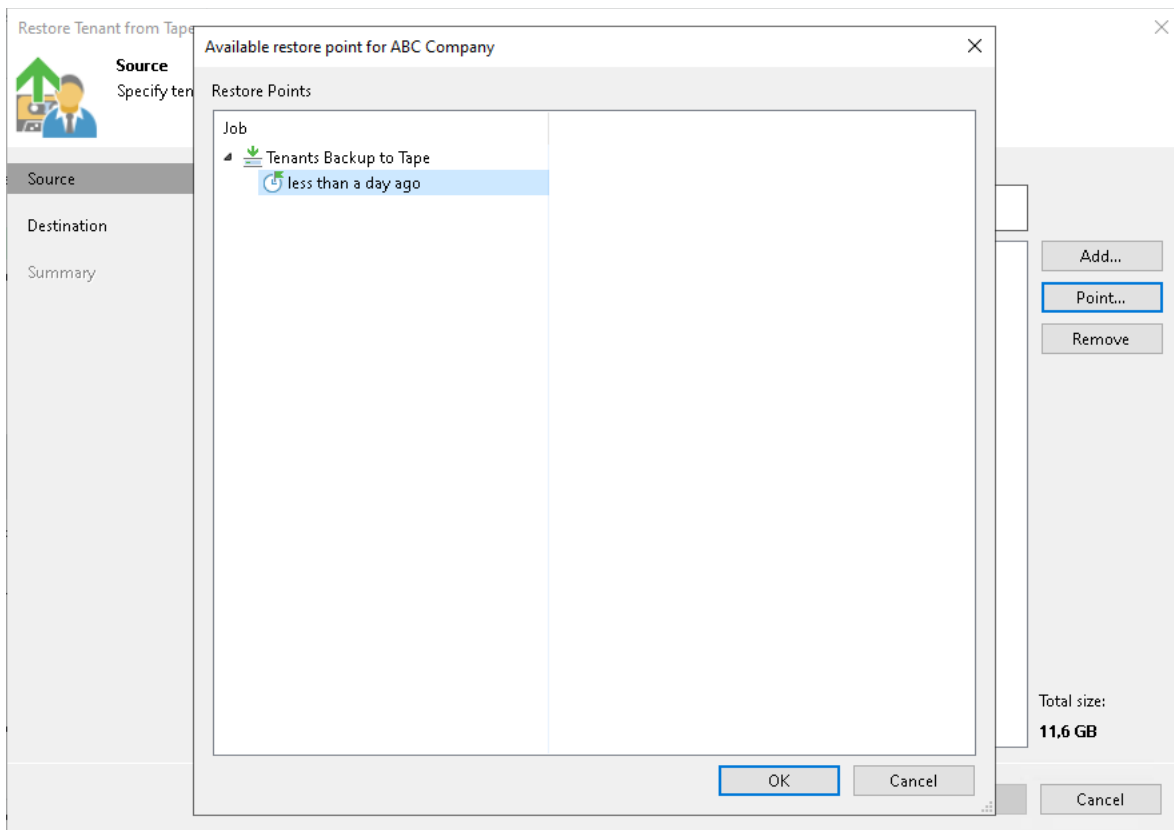
To add one or more tenants to the list, click **Add** and select more tenants. For data restore, you can select the tenant itself, specific cloud repository or backup job.

The screenshot shows the 'Restore Tenant from Tape' wizard in the 'Source' step. The window title is 'Restore Tenant from Tape'. The 'Source' step is selected in the left sidebar, with 'Destination' and 'Summary' also visible. The main area is titled 'Specify tenant, quota or backup job to restore the corresponding backup files from tape.' Below this, there is a search bar with the placeholder text 'Type in a object name for instant lookup'. A table titled 'Objects to restore:' lists three items:

Name	Date
ABC Company	less than a day ago
ABC Company\Cloud Vol 01	less than a day ago
ABC Company\Cloud Vol 01\Fileserver Backup	less than a day ago

To the right of the table are three buttons: 'Add...', 'Point...', and 'Remove'. At the bottom right, the 'Total size:' is displayed as '11,6 GB'. At the bottom of the window are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

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:

- **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.

- **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.

- **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.

The screenshot shows the 'Restore Tenant from Tape' wizard window. The title bar says 'Restore Tenant from Tape' with a close button. Inside, there's a green arrow icon and a person icon. The main heading is 'Destination' with the subtitle 'Select where to restore backup files to.' On the left, there's a sidebar with four tabs: 'Source', 'Destination' (which is selected and highlighted), 'Quota', and 'Summary'. The main area is titled 'Specify restore location:' and contains three radio button options: 1. 'Restore to the original location' with the description 'Restores selected backup files and to the original cloud repository, and maps them to the tenant's quota.' 2. 'Restore to a new location' (which is selected) with the description 'Restores selected backup files to a different cloud repository. Tenant will have to map their backup jobs to the restored backup files manually.' 3. 'Export backup files to disk' with the description 'Restores selected backup files to a server. This option is useful when you want to provide the tenants with their backup files on a removable storage.' At the bottom right, there are four buttons: '< Previous', 'Next >' (which is highlighted with a blue border), 'Finish', and 'Cancel'.

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 [Creating 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**.

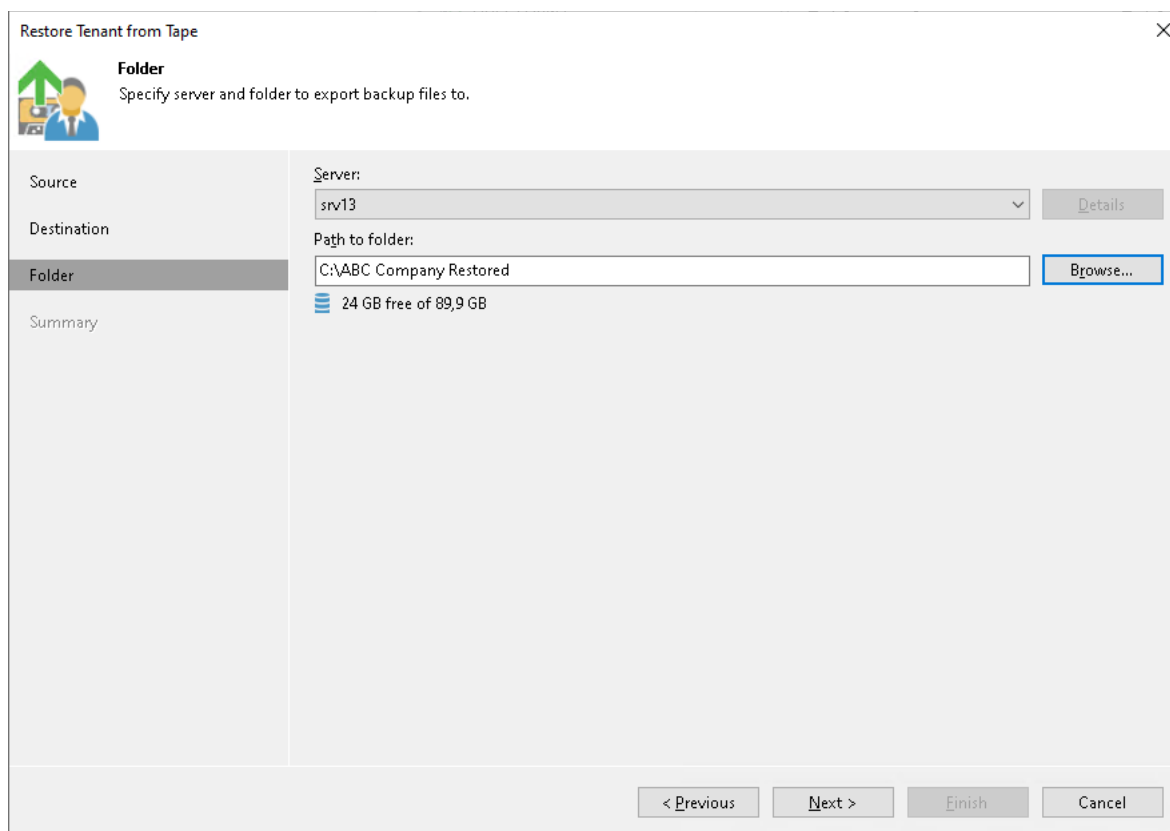
- To save tenant data restored from tape next to original tenant data, in the prompt window, click **Keep**.

The screenshot shows the 'Restore Tenant from Tape' wizard window. The title bar reads 'Restore Tenant from Tape' with a close button (X). Below the title bar is a green arrow icon pointing up and a person icon. The main heading is 'Quota' with the instruction 'Specify the tenant and quota to restore backup files to.' On the left is a sidebar with tabs: 'Source', 'Destination', 'Quota' (selected), and 'Summary'. The main area is titled 'Backup locations:' and contains a table with two columns: 'Original repository' and 'New repository'. Both columns have a single entry: 'ABC Company\Cloud Vol 01'. To the right of the table are 'Add' and 'Edit' buttons. At the bottom of the window are four buttons: '< Previous', 'Next >' (highlighted with a blue border), 'Finish', and 'Cancel'.

Original repository	New repository
ABC Company\Cloud Vol 01	ABC Company\Cloud Vol 01

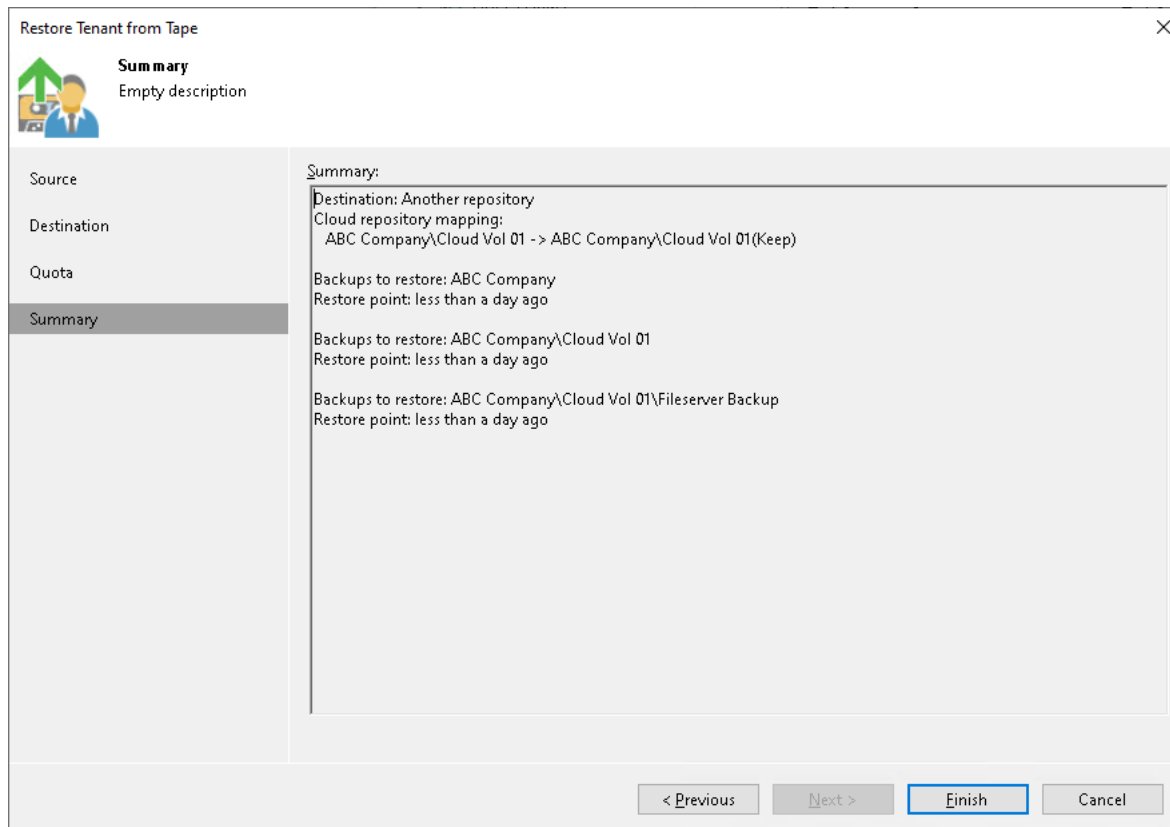
7. If you chose to restore tenant data to a folder, at the **Folder** step of the wizard, specify the server and the folder where you want to restore tenant backup files.
 - a. In the **Server** field, select the server from the list of servers added to the Veeam backup infrastructure.

b. In the **Path to folder** field, specify the folder where you want to place the restored backups.



The screenshot shows the 'Restore Tenant from Tape' wizard at the 'Folder' step. The left sidebar has tabs for Source, Destination, Folder (selected), and Summary. The main area is titled 'Folder' with the instruction 'Specify server and folder to export backup files to.' It contains a 'Server:' dropdown menu set to 'srv13', a 'Path to folder:' text box with 'C:\ABC Company Restored', and a 'Browse...' button. Below the text box, it shows '24 GB free of 89,9 GB'. At the bottom are navigation buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

8. At the **Summary** step of the wizard, review the restore settings.



The screenshot shows the 'Restore Tenant from Tape' wizard at the 'Summary' step. The left sidebar has tabs for Source, Destination, Quota, and Summary (selected). The main area is titled 'Summary' with the instruction 'Empty description'. It displays a 'Summary:' section with the following details: 'Destination: Another repository', 'Cloud repository mapping: ABC Company\Cloud Vol 01 -> ABC Company\Cloud Vol 01(Keep)', 'Backups to restore: ABC Company', 'Restore point: less than a day ago', 'Backups to restore: ABC Company\Cloud Vol 01', 'Restore point: less than a day ago', and 'Backups to restore: ABC Company\Cloud Vol 01\Fileserver Backup', 'Restore point: less than a day ago'. At the bottom are navigation buttons: '< Previous', 'Next >', 'Finish' (highlighted), and '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:
 - *OK.*
 - *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.
 - *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.

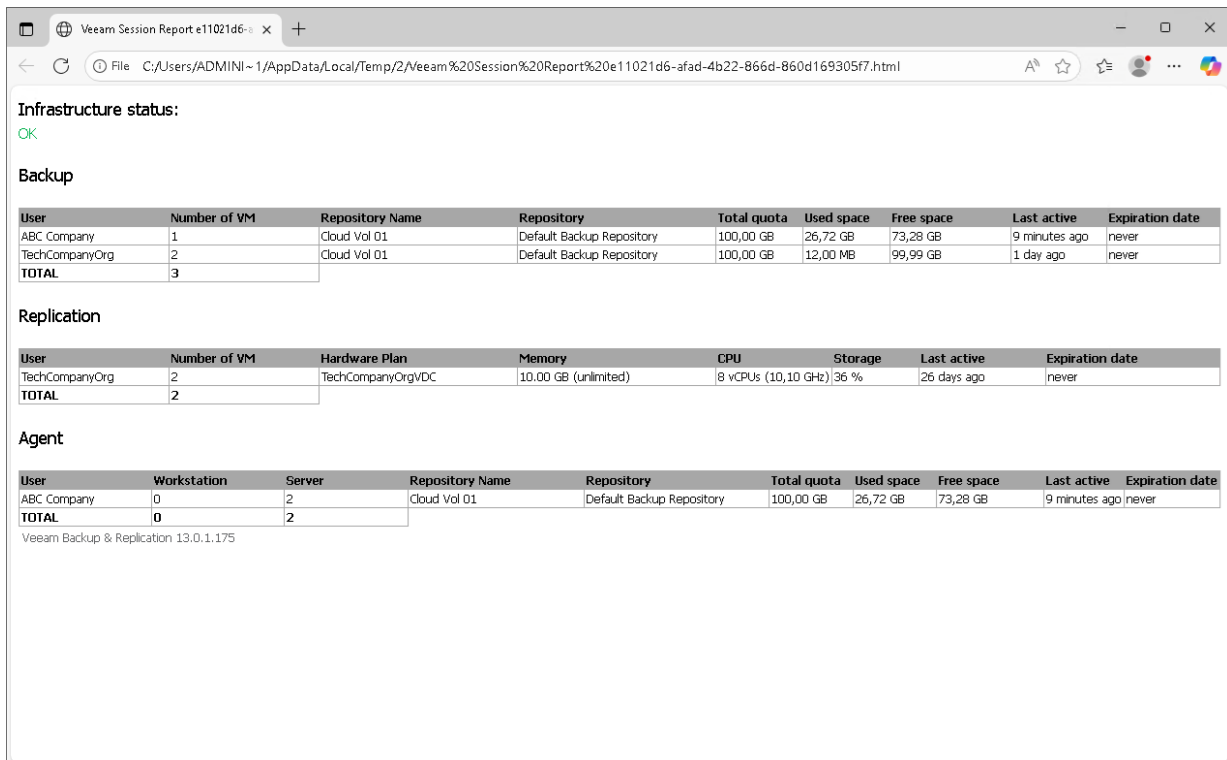
- The **Backup** section shows information about consumption of cloud repository resources by tenants: the user name of the tenant account, the number of VMs in backups stored on the cloud repository, the name of the cloud repository and the name of the backup repository whose resources the SP exposes 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 tenants: 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 tenants: 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.



The screenshot shows a web browser window displaying a Veeam Session Report. The report is titled "Veeam Session Report e11021d6-..." and shows the following sections:

Infrastructure status: OK

Backup

User	Number of VM	Repository Name	Repository	Total quota	Used space	Free space	Last active	Expiration date
ABC Company	1	Cloud Vol 01	Default Backup Repository	100,00 GB	26,72 GB	73,28 GB	9 minutes ago	never
TechCompanyOrg	2	Cloud Vol 01	Default Backup Repository	100,00 GB	12,00 MB	99,99 GB	1 day ago	never
TOTAL	3							

Replication

User	Number of VM	Hardware Plan	Memory	CPU	Storage	Last active	Expiration date
TechCompanyOrg	2	TechCompanyOrgVDC	10.00 GB (unlimited)	8 vCPUs (10,10 GHz)	36 %	26 days ago	never
TOTAL	2						

Agent

User	Workstation	Server	Repository Name	Repository	Total quota	Used space	Free space	Last active	Expiration date
ABC Company	0	2	Cloud Vol 01	Default Backup Repository	100,00 GB	26,72 GB	73,28 GB	9 minutes ago	never
TOTAL	0	2							

Veeam Backup & Replication 13.0.1.175

Generating Report

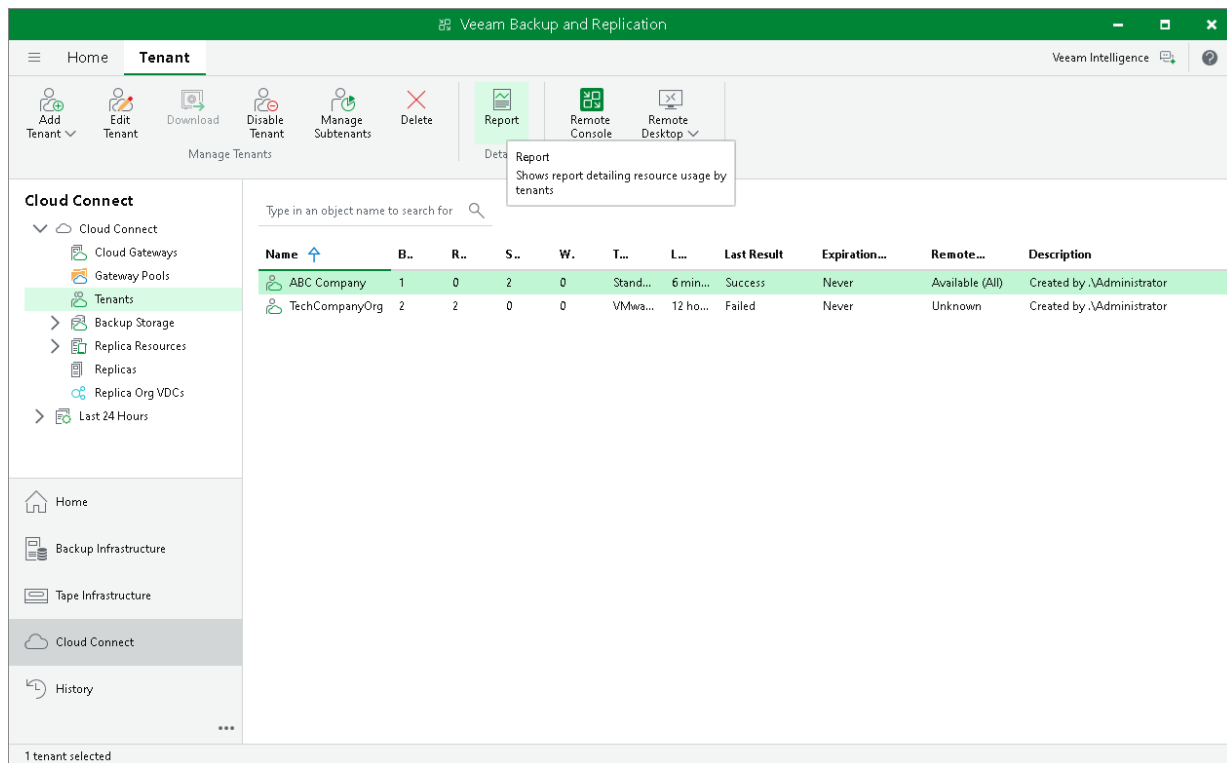
To view the Veeam Cloud Connect report that displays information about a specific tenant:

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.

TIP

The SP can generate a Veeam Cloud Connect report that displays information about multiple tenants. To view the report, use one of the following ways:

- To select multiple tenants, press and hold the **[CTRL]** key and click necessary tenants, then click **Report** on the ribbon.
- To select all tenants, press **[CTRL + A]** to highlight all tenants, then 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. The following rules apply to daily email reporting:

1. The first report is sent immediately after the SP enables the global email notification settings in Veeam Backup & Replication.

2. The second report is sent after 24 hours, plus the time required for the infrastructure check that elapsed since the first report was sent.
3. The third report and subsequent reports are sent using the same rules.

As a result, the time at which a report is sent is shifted forward with each subsequent report. Each day, the report is sent several seconds later than the day before. Keep in mind that the resulting time shift can become significant over time.

TIP

The SP can specify the time at which the daily report is sent. To do this, the SP must create the registry key `HKEY_LOCAL_MACHINE\SOFTWARE\Veeam\Veeam Backup and Replication\CloudConnectReportTime` (REG_SZ) and enter the selected time as a registry value. Use the 24-hour clock and the time zone of the cloud service. For example, 21:30.

Viewing Tenant Job Statistics

When a tenant runs a backup, backup copy, replication job and CDP policy sessions 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 the 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 job, backup copy job, replication job and CDP policy 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

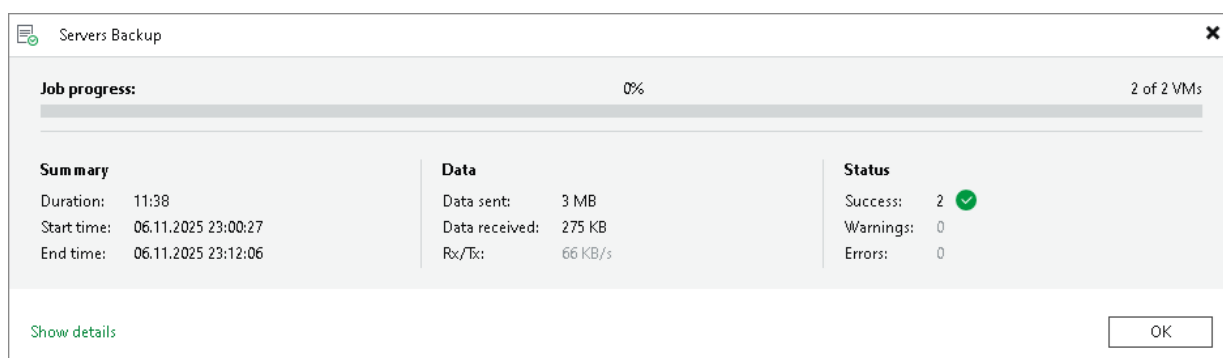
The **Statistics** option is unavailable for Veeam Agent backup jobs. To learn more, see [Veeam Agent Backup Job Statistics](#).

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:
 - **Duration** – time from the job start till the current moment or job end.
 - **Start time** – time of the job start.
 - **End time** – time of the job end.
- The **Data** box shows information about processed VM data:
 - **Data sent** – amount of data sent from the SP side to the tenant side.
 - **Data received** – amount of data transferred from the tenant side to the SP side.
 - **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:
 - 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.
 - 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.

Servers Backup

Job progress: 0% 2 of 2 VMs

Summary
Duration: 11:38
Start time: 06.11.2025 23:00:27
End time: 06.11.2025 23:12:06

Data
Data sent: 3 MB
Data received: 275 KB
Rx/Tx: 66 KB/s

Status
Success: 2
Warnings: 0
Errors: 0

Host	Last Backup	Action	Duration
filesrv031	Success	Job finished at 06.11.2025 23:12:06	
filesrv041	Success		

[Hide details](#)

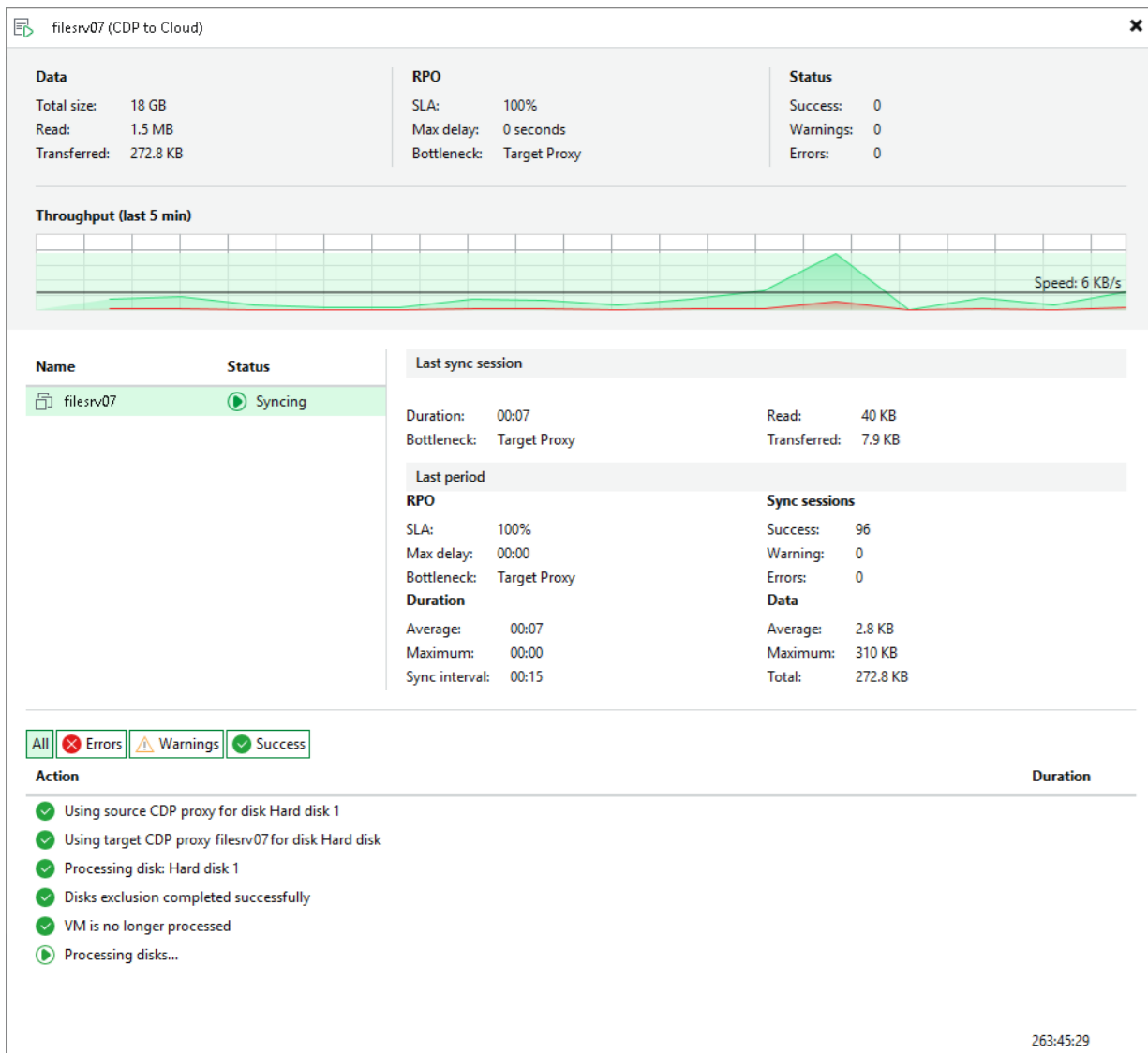
OK

Statistics Counters for CDP Policy Sessions

The SP can view detailed statistics on CDP policy sessions performed by tenants within last 24 hours. Veeam Backup & Replication displays session statistics for the following counters:

- The **Data** box shows general information about the job:
 - **Total size** – total size of the processed data.
 - **Read** – amount of data read from the datastore prior to applying compression and deduplication. The value of this counter is typically lower than the value of the **Total size** counter. Veeam Backup & Replication reads only data blocks that have changed since the last policy session, processes and copies these data blocks to the target.
 - **Transferred** – amount of data transferred from the source CDP proxy to the target CDP proxy. The data is transferred after compression and deduplication.
- The **RPO** box shows information about processed VM data:
 - **SLA** – percentage of sessions completed within the desired RPO.
 - **Max delay** – difference between the configured RPO and time required to transfer and save data.
 - **Bottleneck** – bottleneck in the data transmission process.

- The **Status** box shows information about the job results. This box informs how many tasks have completed with the *Success*, *Warning* and *Error* statuses.



Viewing Job Session Results

The SP can view detailed statistics on VM backup job, backup copy job, replication job and CDP policy 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 that tenant jobs only display a *Failed* status on the SP backup server if the issue is on the SP backup server side. For example, this includes the following cases:

- All cloud gateways are unavailable.

- Disk space is insufficient.
- Connection was forcibly closed by the remote host.
- Storage quota of the cloud repository is exceeded.

For tenant jobs that failed because of an issue on the tenant backup server, the SP backup server displays a *Success* status.

NOTE

The **Statistics** option is unavailable for Veeam Agent backup jobs. To learn more, see [Veeam Agent Backup Job Statistics](#).

Servers Backup

Job progress:

0%

2 of 2 VMs

Summary	Data	Status
Duration: 11:38	Data sent: 3 MB	Success: 2
Start time: 06.11.2025 23:00:27	Data received: 275 KB	Warnings: 0
End time: 06.11.2025 23:12:06	Rx/Tx: 66 KB/s	Errors: 0

Host	Last Backup	Action	Duration
filesrv031	Success	Job finished at 06.11.2025 23:12:06	
filesrv041	Success		

Hide details

OK

Support for Veeam Backup for Public Clouds

The SP can configure backup copy jobs for backups of public cloud appliances.

This feature allows the SP to copy backups of cloud appliances to regular backup repositories in the regular Veeam Backup & Replication backup file format. To learn more, see the [Backup Copy](#) section in the Veeam Backup & Replication User Guide.

The SP can configure backup copy jobs for backups created by the following Veeam products:

- [Veeam Backup for AWS](#)
- [Veeam Backup for Microsoft Azure](#)

To start working with those backups, the SP must add the repository that contains backups of Amazon EC2 instances or Azure VMs to the Veeam Backup & Replication infrastructure as an external repository. Then, they can use this external repository as a source backup repository and use a repository on the SP side as a target backup repository for backup copy.

To work with backup copy jobs for Amazon EC2 or Microsoft Azure data, the SP must be able to manage the backup server with Veeam Service Provider Console. For more information, see the [Connect Veeam Cloud Connect Servers to Veeam Service Provider Console](#) section in the Deployment Guide.

NOTE

The public cloud appliance must be deployed in the SP backup infrastructure. To do this the SP must use the Veeam Service Provider Console. For details see the following sections:

- For Microsoft Azure, see details in the [Adding Veeam Backup for Microsoft Azure Appliances](#) section in the Guide for Service Providers.
- For AWS, see details in the [Adding Veeam Backup for Amazon Web Services Appliances](#) section in the Guide for Service Providers.

You can restore data from backups created by both backup jobs and backup copy jobs. Restore operations are available directly from the SP Veeam Backup & Replication console. For the complete list of the available operations, see the following sections:

1. [Performing Restore](#) in the Veeam Backup for Microsoft Azure User Guide
2. [Performing Restore](#) in the Veeam Backup for AWS User Guide

Getting Started with Backup Copy for Public Cloud Backups

To start working with backup copy jobs for public cloud backups, you must complete the following tasks:

1. In Veeam Service Provider Console, configure connection to the backup server and the public cloud appliance that contains backups of Amazon EC2 instances or Azure VMs.
 - For details on how to connect to the backup server, see the [Connecting Veeam Backup & Replication Servers](#) section in the Guide for Service Providers.
 - For details on how to connect to the public cloud appliance, see the [Managing Veeam Backup for Public Clouds Appliances](#) section in the Guide for Service Providers.

2. In the Veeam Backup & Replication console, set up credentials for repositories available on the appliance.
 - a. Launch the wizard to edit a public cloud appliance.

For detailed instructions, see the following sections:

 - [For Microsoft Azure] The [Editing Appliance Settings](#) section in the Veeam Backup for Microsoft Azure User Guide
 - [For AWS] The [Editing Appliance Settings](#) section in the Veeam Backup for AWS User Guide
 - b. Specify credentials for repositories available on the appliance.

For detailed instructions, see the following sections:

 - [For Microsoft Azure] The [Configure Repository Settings](#) section in the Veeam Backup for Microsoft Azure User Guide
 - [For AWS] The [Configure Repository Settings](#) section in the Veeam Backup for AWS User Guide
3. Backups created for this appliance become available in the SP Veeam Backup & Replication console. To view the backups, do the following:
 - a. Open the **Backup Infrastructure** view.
 - b. In the inventory pane, click **External Repositories**.
 - c. In the working area, right-click the cloud repository and select **Rescan**.
4. Create a backup copy job:
 - a. Open the **Home** view.
 - b. In the inventory pane, click **External Repository** and select **Backup Copy**.

- c. At the **Objects** step of the wizard, click **Add** and select **From backups**. There you can select any root backup that resides in the external repository.

New Backup Copy Job

Objects

Add objects which backups should be mirrored to the target repository. Immediate backup copy job will process image-level and transaction log backups.

Objects to process:

Name	Type	Size
Fileserver Backup	Backup	9.18 GB

Add...

- From jobs...
- From repositories...
- From backups...**

Recalculate

Total size: **9.18 GB**

☐ Include database transaction log backups (increases bandwidth usage)

< Previous **Next >** Finish Cancel

- d. Follow the steps of the new backup copy job wizard and finish it in the same way as regular backup copy job.

To learn more, see [Creating Backup Copy Jobs](#).

Guide for Tenants

The Guide for Tenants 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 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

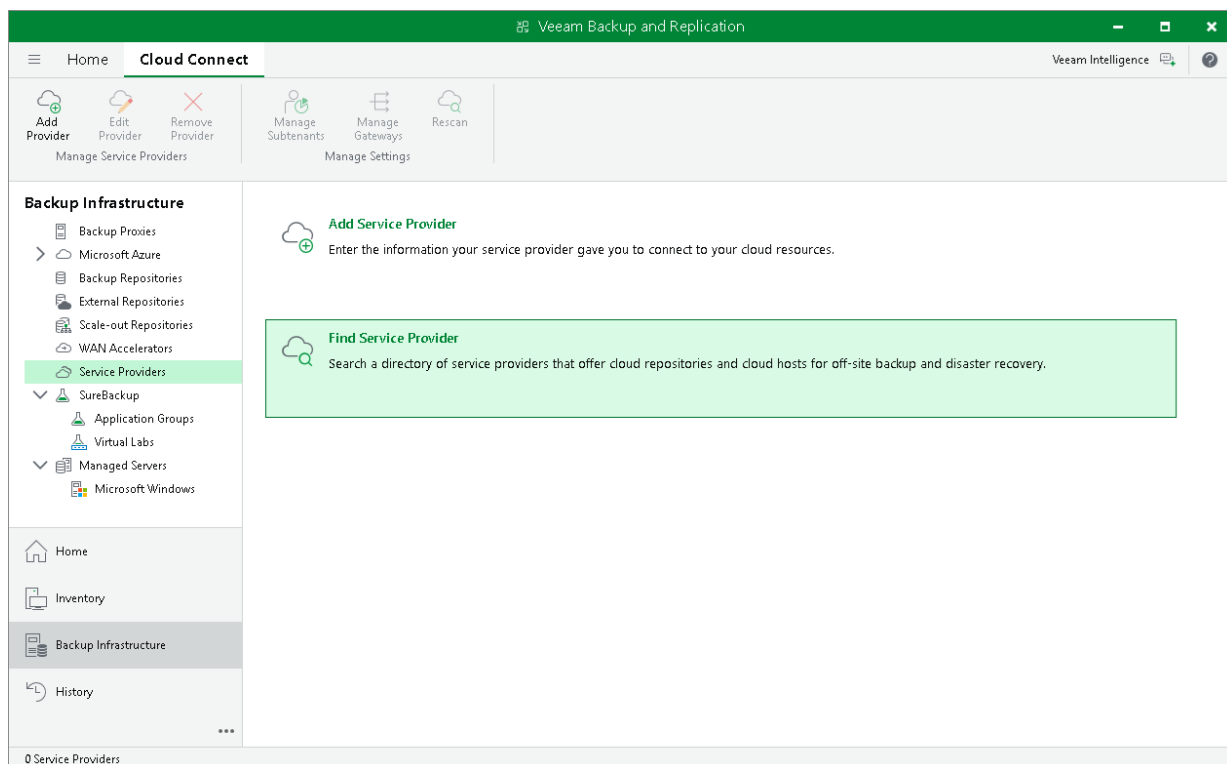
You can look for SPs who offer Backup as a Service and Disaster Recovery as a Service using Veeam Backup & Replication. The list of SPs is published on the Veeam website and constantly updated. You can select the necessary SP from the list and contact this SP to get the cloud repository service.

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 the tenant 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:

- Make sure that the SP has provided you with the following information:
 - You have a user name and password for your tenant account registered at the SP Veeam backup server.
 - You have a full DNS name or IP address of the cloud gateway over which you will communicate with the Veeam Cloud Connect infrastructure.
 - You have a port over which to connect to the cloud gateway (if the SP specified a non-default port).
 - [Optional] You have a TLS certificate thumbprint that you can use for TLS certificates verification.
- [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 Credentials](#).
- The tenant can add the SP on more than one backup server using the same tenant account credentials. This may be useful, for example, if the tenant wants to restore data from a cloud backup after the original tenant backup server becomes unavailable. In this scenario, backups created by the tenant on any of the backup servers connected to the SP become available on each backup server.

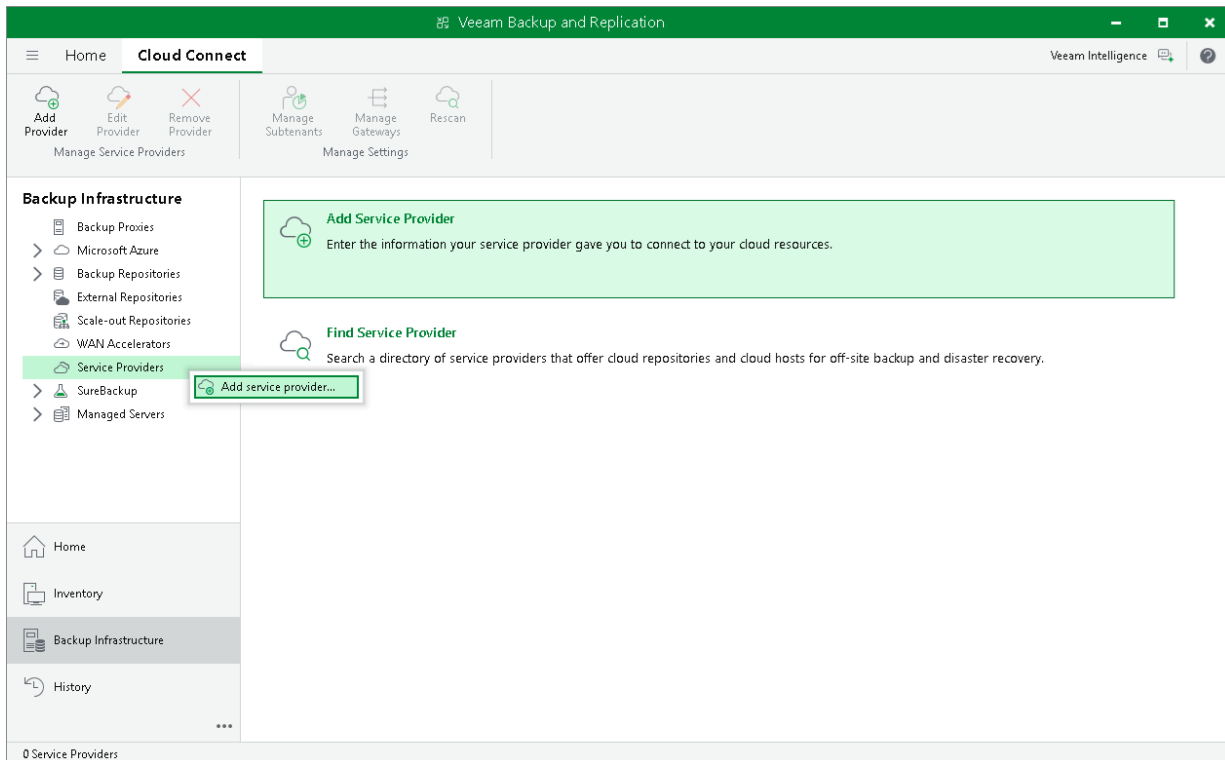
For this scenario, consider the following:

- All backup servers where the tenant plans to add the SP must run the same Veeam Backup & Replication version.
- When you delete a cloud backup in Veeam Backup & Replication, the backup is removed from the cloud repository and becomes unavailable on all backup servers connected to the SP. To learn more, see [Deleting from Disk](#).
- Keep in mind that adding the same SP on multiple backup servers and creating backups under the same tenant account may complicate management of cloud backups in Veeam Backup & Replication.

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 cloud host.

The screenshot shows the 'Service Provider' configuration window. It has a title bar with a close button. Inside, there's a cloud icon and the title 'Service Provider'. Below the title, a subtitle reads: 'Type in DNS name or IP address and a port number received from the service provider. If you are using more than one service provider, add a custom description to more easily distinguish between them.' On the left, there's a sidebar with four items: 'Service Provider' (selected), 'Credentials', 'Apply', and 'Summary'. The main area contains the following fields: 'DNS name or IP address' with the value '172.24.26.107', 'Port' with a dropdown menu showing '6180', and a 'Description' text box containing 'Created by SRVSP11\Administrator'. At the bottom, there's a checked checkbox labeled 'Allow this Veeam Backup & Replication installation to be managed by the service provider' with a subtext: 'Select this check box if you have managed backup contract with the service provider you are adding, and want to allow it to manage your installation remotely.' At the very bottom, there are four buttons: '< Previous', 'Next >' (highlighted with a blue border), 'Finish', and 'Cancel'.

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.
 - To view the TLS certificate, click the certificate link.
 - 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 **Thumbprint** 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*.

Service Provider

Credentials
Specify credentials that you have received from the service provider, and validate the certificate.

Service Provider

Credentials

Apply

Summary

This certificate has been validated.

Verified by: CN=Veeam Software, O=Veeam Software, OU=Veeam Software

Add or select credentials issued to you by the service provider

Credentials:

ABC Company (ABC Company, last edited: less than a day ago)

Add...

Manage accounts

< Previous Apply Finish Cancel

Step 4. Specify Backup Storage Settings

At the **Backup Storage** step of the wizard, Veeam Backup & Replication automatically enumerates the cloud repository resources allocated to you. Then you specify the restore scope of backups that the SP can restore.

1. Wait for Veeam Backup & Replication to enumerate and display cloud repository resources allocated to the you. This may take some time.
2. In the **Allow the service provider to restore backups stored in cloud repositories** field, click the **Unencrypted backups only** link.
3. Select one of the following options:
 - **None**. The SP cannot restore tenant backups from the cloud repository. This is the default option.
 - **Unencrypted backups only**. The SP can restore only unencrypted tenant backups.
 - **All**. The SP can restore both unencrypted and encrypted tenant backups.

To enable restore from encrypted backups, Veeam Backup & Replication on the tenant side releases the encryption password to the SP, so that the SP can decrypt the backup data for the restore operation.

IMPORTANT

This setting is permanent. Once you allow the SP to restore data from encrypted backups, you cannot revert it.

For more information about this feature, see [Access to Tenant Backups](#).

Service Provider

Backup Storage
The following are off-site backup repositories assigned to you by your service provider.

Service Provider
Credentials
Backup Storage
Replica Resources
Network Extension
Apply
Summary

Available Repositories

Service Provider Restore Access

Choose what your service provider can restore from backups stored in cloud repositories.

☐ None
The service provider cannot restore any backups.

☒ **Unencrypted backups only**
The service provider can restore only unencrypted backups.

☐ All
The service provider can restore all backups, including encrypted ones.

OK Cancel

Allow the service provider to restore backups stored in cloud repositories: [Unencrypted backups only](#)

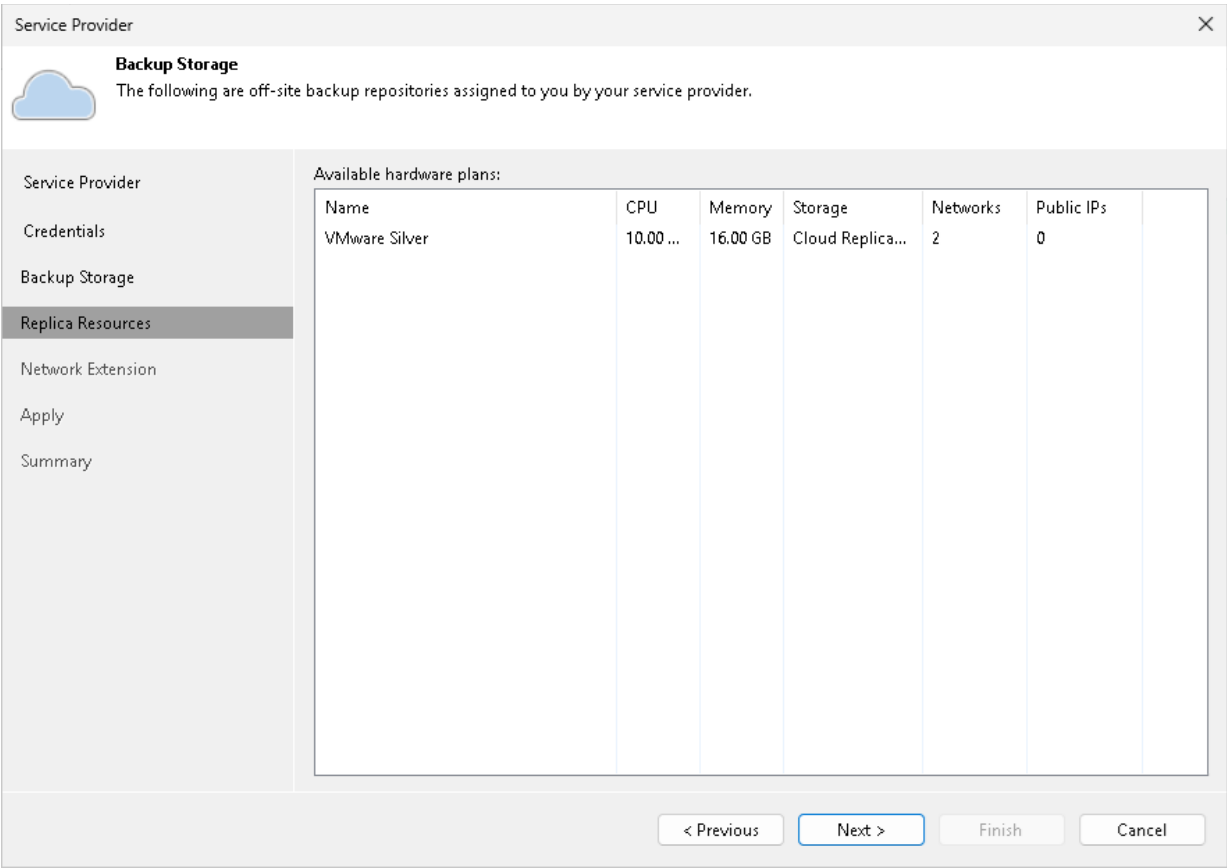
< Previous Next > Finish Cancel

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.

Service Provider

**Replica Resources**
The following is the list of VDC organizations assigned to you by your service provider.

Service Provider

Credentials

Backup Storage

Replica Resources

Network Extension

Apply

Summary

Available organization VDC

Name	CPU	Memory	Storage	WAN
TechCompanyOrgVDC	10,10 GHz	6,70 GB	Veeam CDP Replication (300,...	Disabled

< Previous

Apply

Finish

Cancel

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

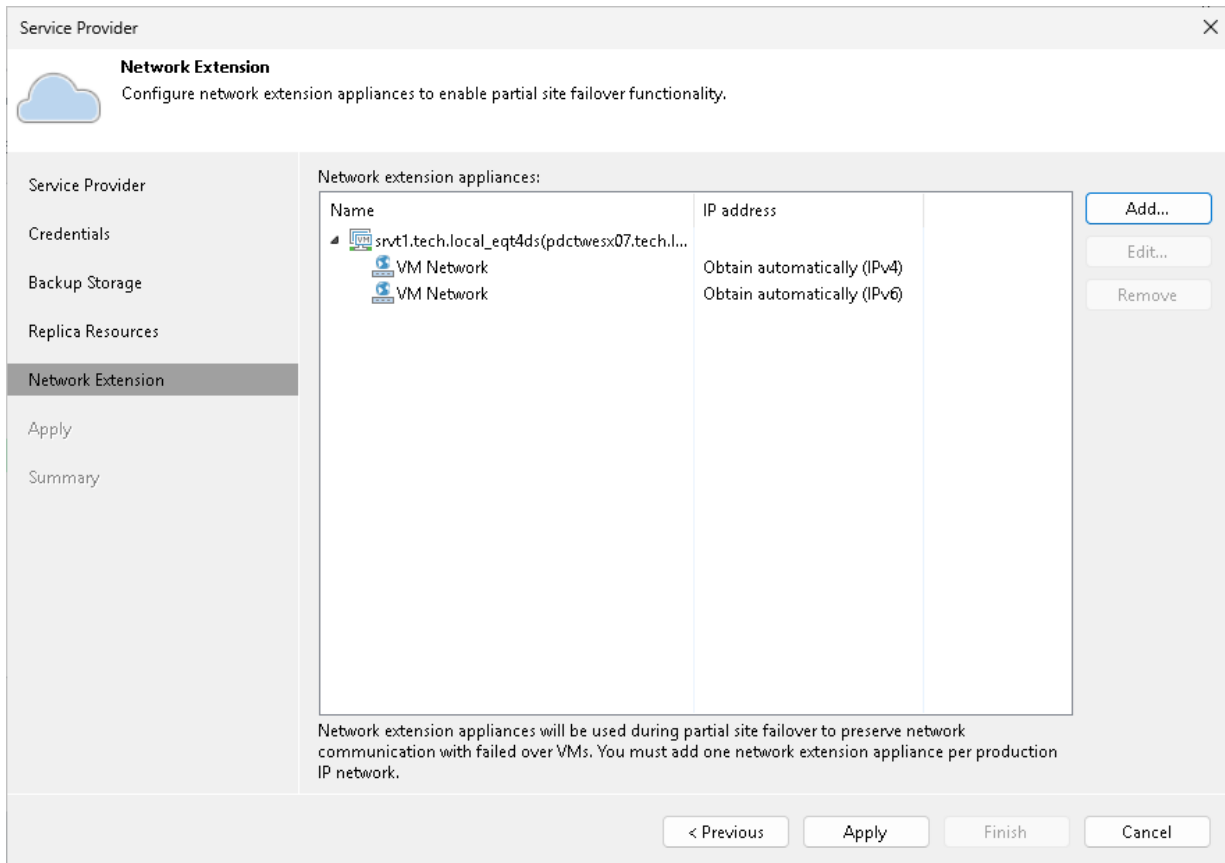
Consider the following:

- 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 be deployed on the source VMware vSphere host:

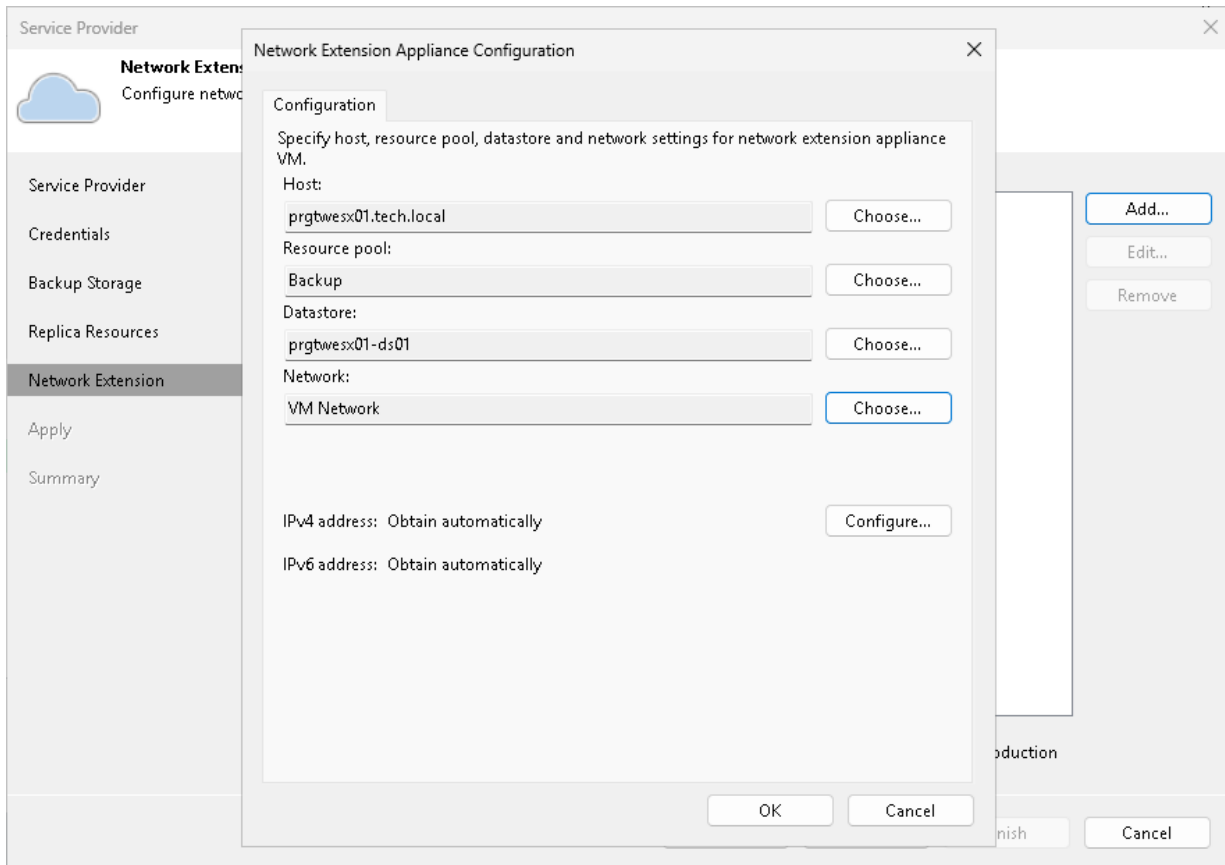
1. Open the **Network Extension Appliance Configuration** window. To do this, do one of the following:
 - To configure a new network extension appliance, click **Add**.
 - To edit settings of the extension appliance that is already in the **Network extension appliances** list, select that network extension 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.
 - 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.
 - 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**.

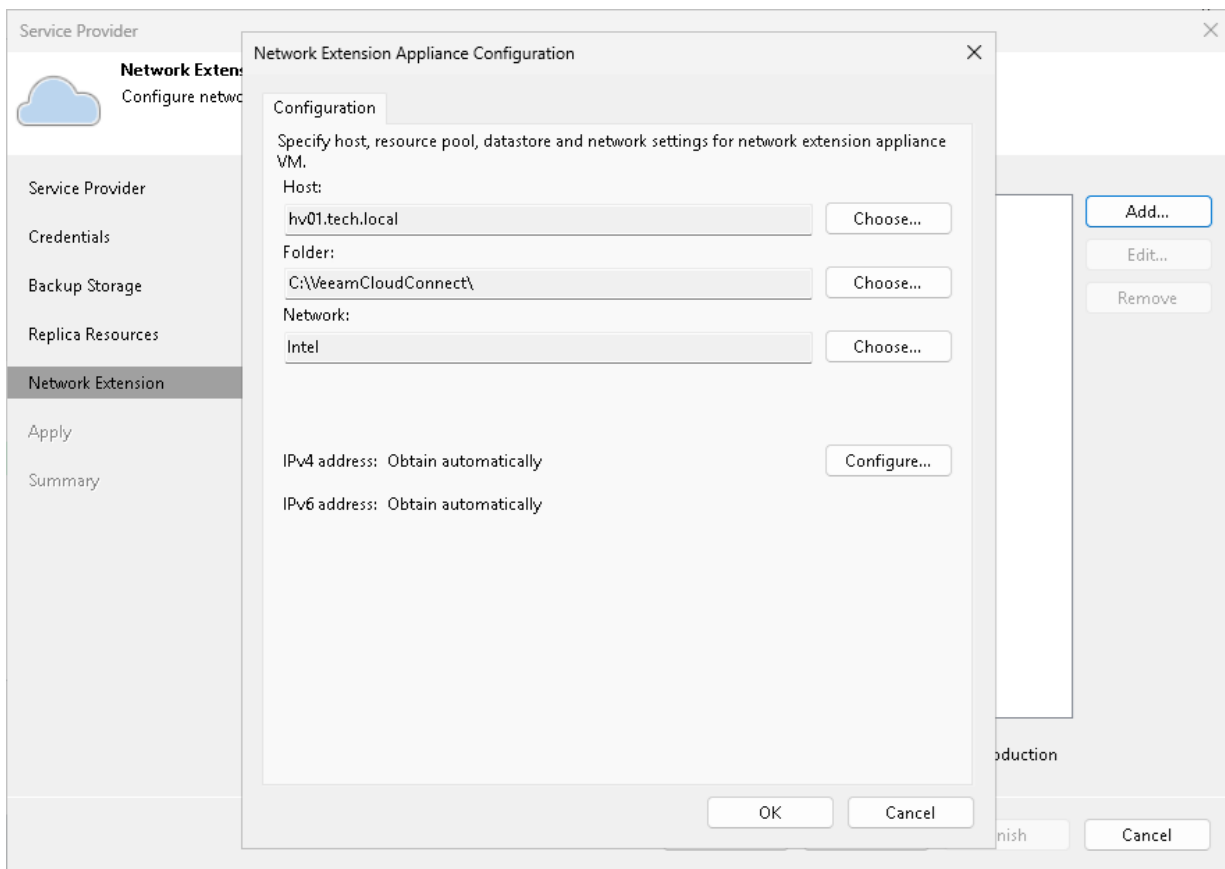


Configuring Network Extension Appliance for Microsoft Hyper-V

To configure the network extension appliance that will be deployed on the source Microsoft Hyper-V host:

1. Open the **Network Extension Appliance Configuration** window. To do this, do one of the following:
 - To configure a new network extension appliance, click **Add**.
 - 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.
 - 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.
 - 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.

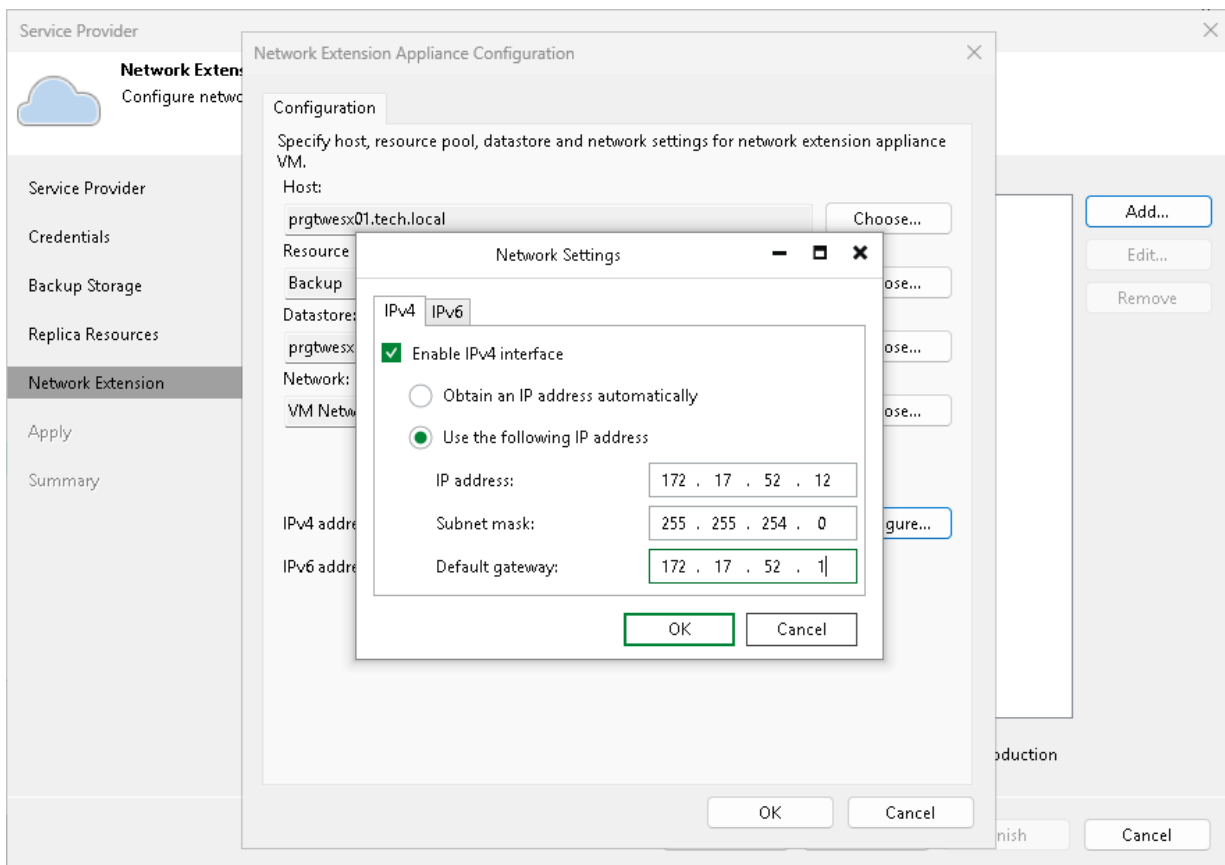
If you do not want the network extension appliance to use an IPv4 address, clear the **Enable IPv4 interface** check box.

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.

Service Provider

Credentials

Backup Storage

Replica Resources

Network Extension

Apply

Summary

Log:

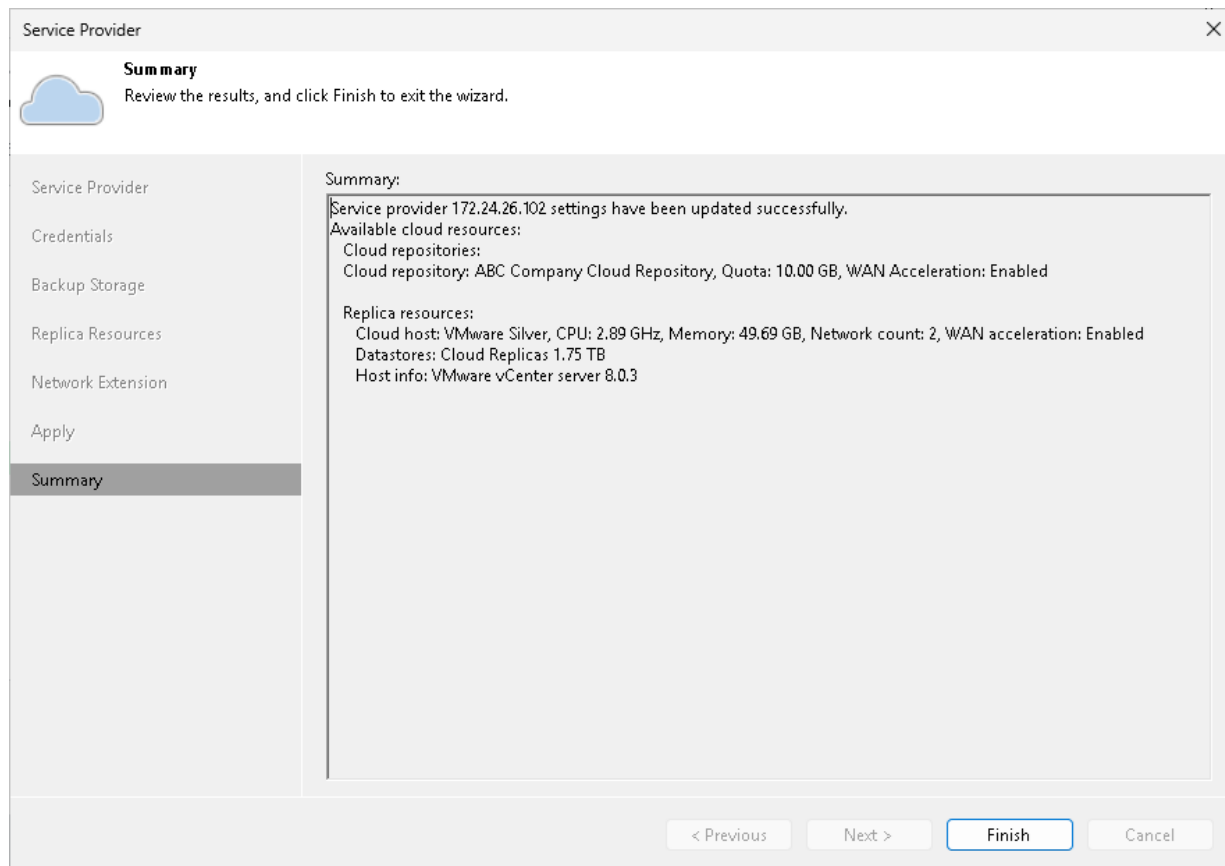
Message	Duration
✓ Saving service provider	0:02:35
✓ Saving cloud resources	0:00:02
✓ Saving network extension appliances	0:02:19
✓ Deploying appliance 172.24.26.107_xoqx2s	0:02:12
✓ Processing network settings for 172.24.26.107_xoqx2s	0:01:14

< PreviousNext >FinishCancel

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**.

The screenshot shows the 'Manage Cloud Credentials' window. At the top, it says 'Use this dialog to centrally manage all user accounts and their passwords.' Below this is a table with four columns: 'Account', 'Type', 'Description', and 'Last Edited'. The first row is highlighted with a green background and contains a key icon, the text 'ABC', and empty cells for 'Type', 'Description', and 'Last Edited'. To the right of the table are three green buttons: 'Add...', 'Edit...', and 'Remove'. Overlaid on top of the table is a 'Credentials' sub-dialog box. This sub-dialog has a title bar with a close button. It contains three input fields: 'Username:' with the text 'ABC Company' and a 'Browse...' button to its right; 'Password:' with a masked password of ten dots and a toggle visibility icon; and 'Description:' with a text area containing 'ABC Company'. At the bottom of the sub-dialog are 'OK' and 'Cancel' buttons. The main 'Manage Cloud Credentials' window also has 'OK' and 'Cancel' buttons at the bottom right.

Account	Type	Description	Last Edited
ABC			

Use this dialog to centrally manage all user accounts and their passwords.

Account Type Description Last Edited

ABC

Username: ABC Company Browse...

Password: eye icon

Description: ABC Company

OK Cancel

OK Cancel

Add... Edit... Remove

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

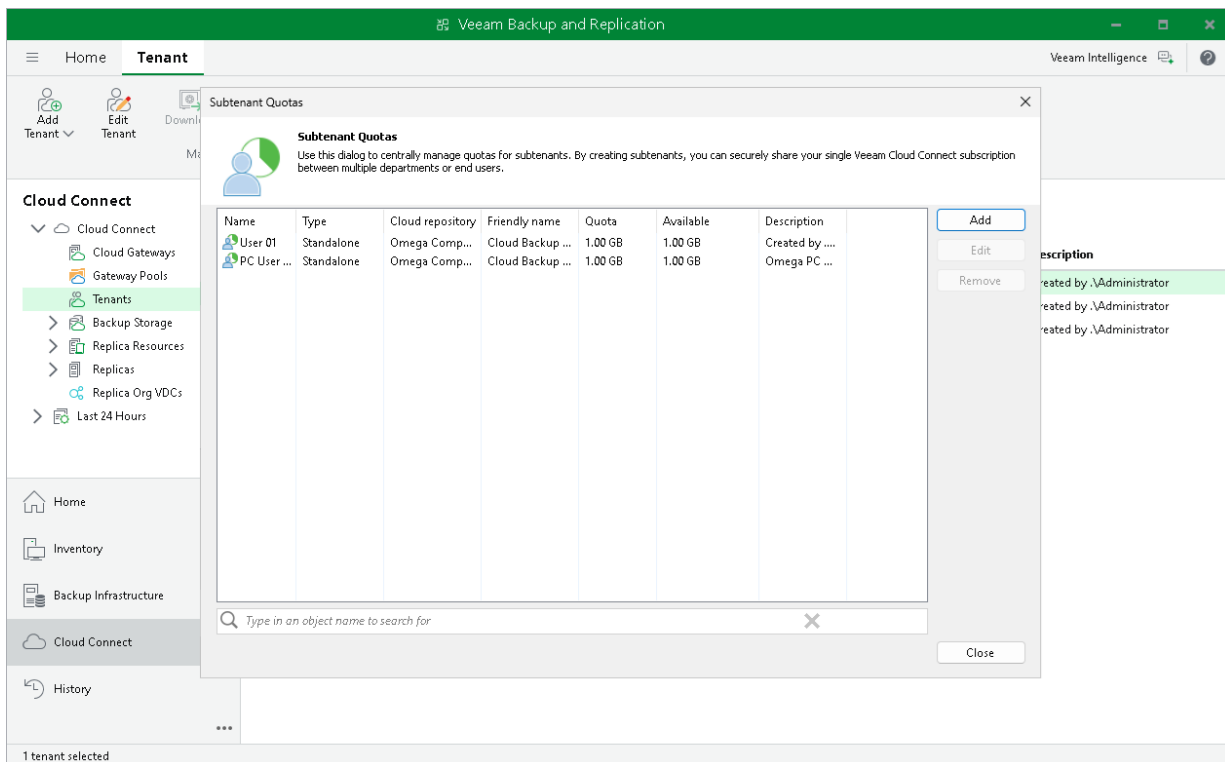
Before you add a new subtenant account, check the following prerequisites:

- 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:

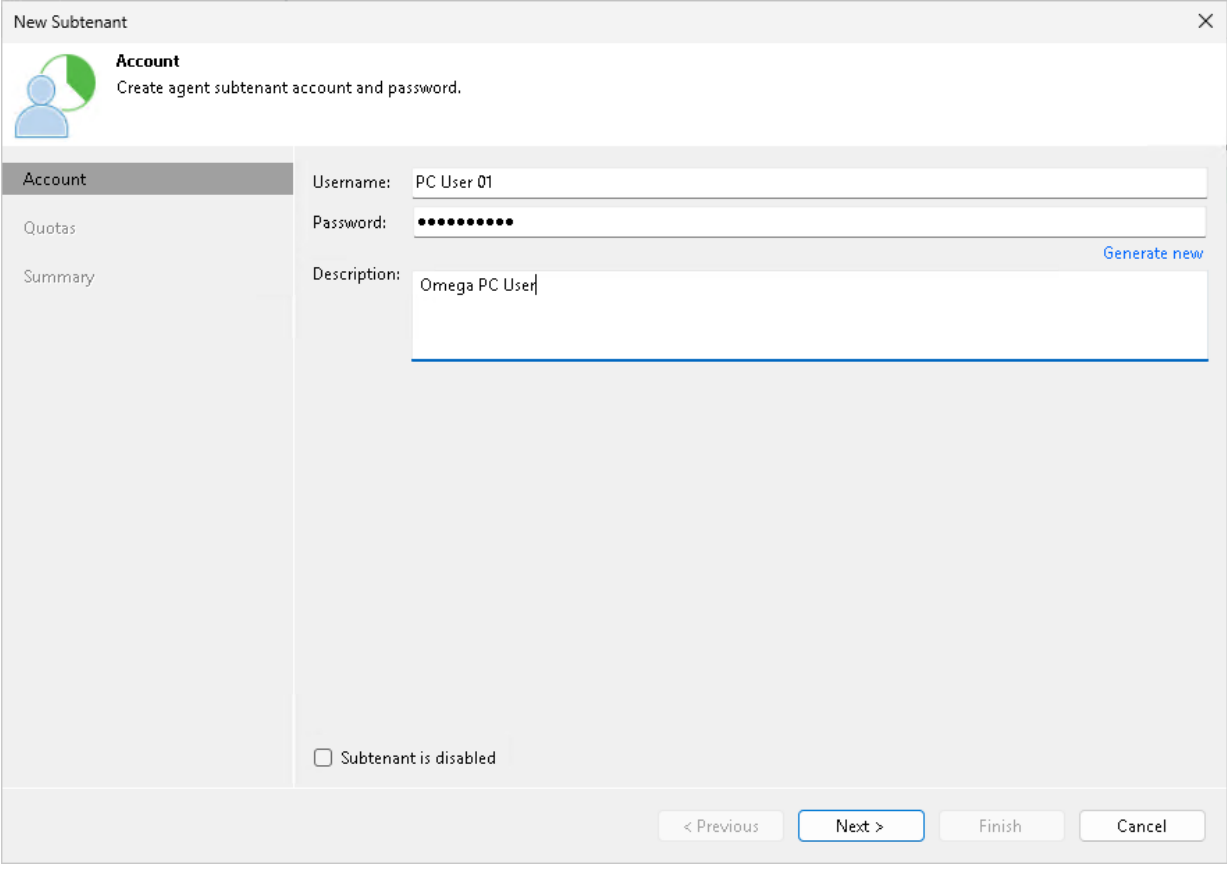
1. Open the **Subtenant Quotas** window in one of the following ways:
 - Open the **Backup Infrastructure** view, click the **Backup Repositories** node in the inventory pane, select the cloud repository in the working area and click **Manage Subtenants** on the ribbon.
 - Open the **Backup Infrastructure** 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, 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. To avoid problems with long paths to backup files on the cloud repository, it is recommended to create user names not longer than 50 characters.
 - 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.



The screenshot shows the 'New Subtenant' wizard window, specifically the 'Account' step. The window has a title bar 'New Subtenant' with a close button. Below the title bar is a header section with a user icon and the text 'Account' and 'Create agent subtenant account and password.' The main area is divided into a left sidebar and a right content area. The sidebar has three items: 'Account' (selected), 'Quotas', and 'Summary'. The content area has three fields: 'Username:' with the value 'PC User 01', 'Password:' with masked characters and a 'Generate new' link, and 'Description:' with the value 'Omega PC User'. At the bottom of the content area is a checkbox labeled 'Subtenant is disabled'. The bottom of the window has four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

New Subtenant

Account
Create agent subtenant account and password.

Account

Quotas

Summary

Username: PC User 01

Password: [Generate new](#)

Description: Omega PC User

☐ Subtenant is disabled

< Previous Next > Finish Cancel

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 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**.

The screenshot shows the 'New Subtenant' wizard in the 'Quotas' step. The main window has a sidebar with 'Account', 'Quotas', and 'Summary'. The 'Quotas' section is active, showing a list of 'Available user quotas' and an 'Add' button. A 'Subtenant Quota' dialog box is open, displaying the following fields:

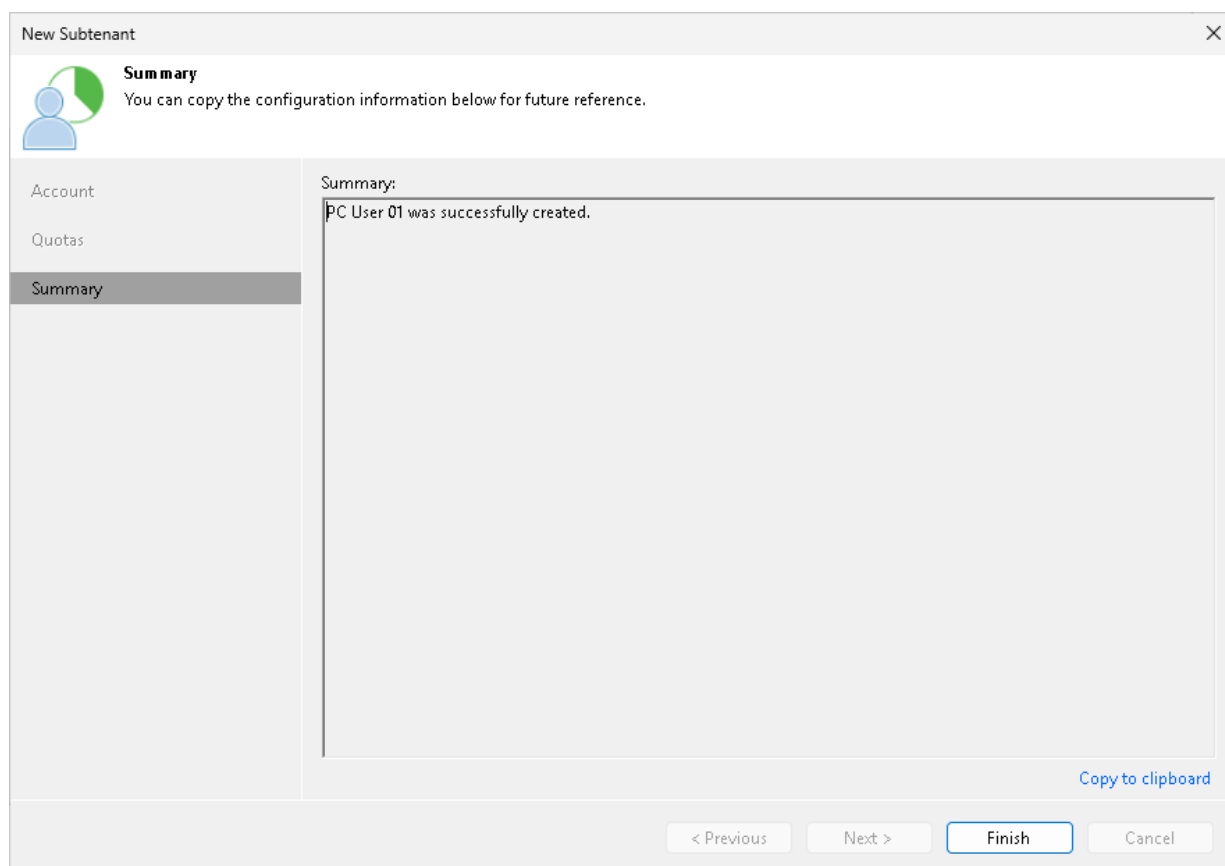
- Name:** Cloud Backup Storage
- Repository:** Omega Cloud Repository (Tenant's quota)
- Quota:** ☒ Limit size to: 5 GB

The dialog also shows '10 GB free of 10 GB' and buttons for 'OK' and 'Cancel'. The main window has buttons for '< Previous', 'Next >', 'Finish', and 'Cancel' at the bottom.

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:

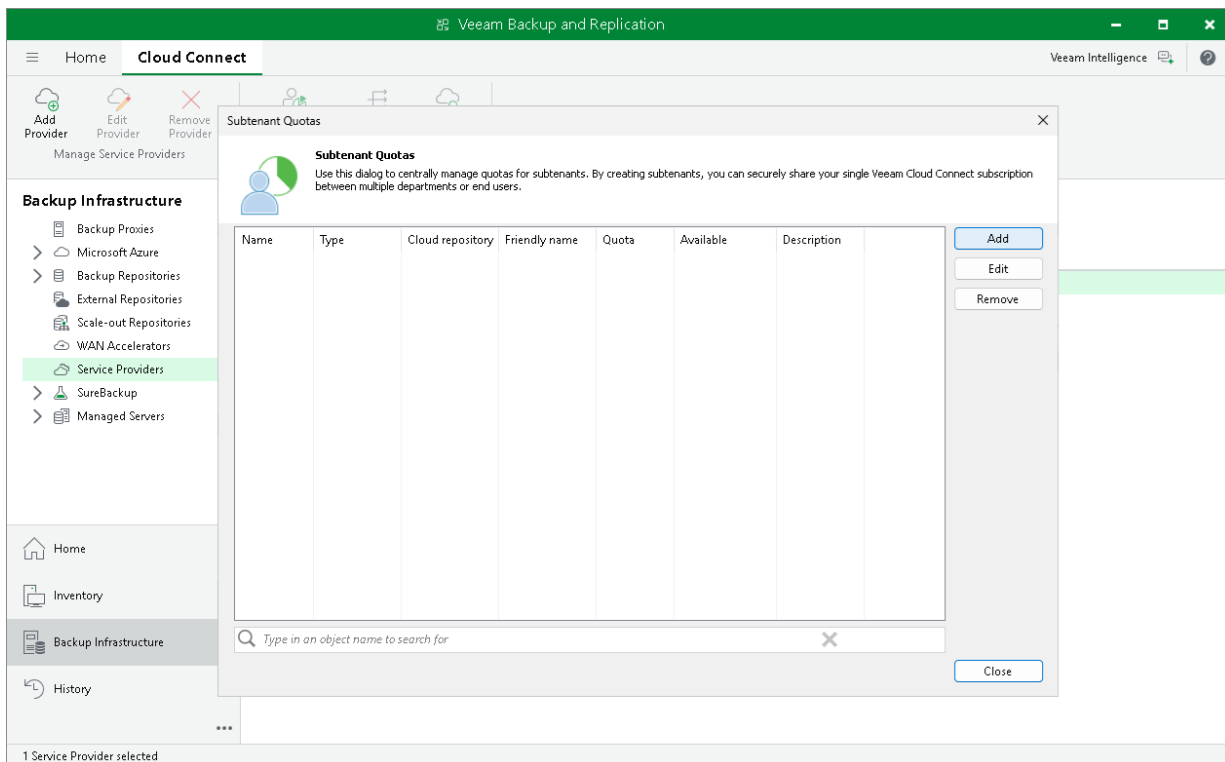
- You must be connected to the SP whose cloud repository you want to expose to subtenants. When you create a subtenant account, you can allocate storage quota only on those cloud repositories that are provided to your tenant account by the SP.

- 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:
 - 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, 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.

The screenshot shows the 'New Subtenant' wizard window. The title bar says 'New Subtenant' with a close button. Inside, there's a header section with a user icon and the text 'Cloud Director User' and 'Specify VMware Cloud Director user account.' Below this is a sidebar with 'Cloud Director User' (selected), 'Quotas', and 'Summary'. The main area has a 'Username:' field with 'user01' and an 'Add' button. Below it is a 'Description:' text area containing 'Created by .\Administrator'. At the bottom left, there is a checkbox labeled 'Subtenant is disabled'. At the bottom right, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

New Subtenant	
Cloud Director User Specify VMware Cloud Director user account.	
Cloud Director User	Username: user01 <button>Add</button>
Quotas	Description: Created by .\Administrator
Summary	
☐ Subtenant is disabled	
< Previous Next > Finish Cancel	

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 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**.

The screenshot shows the 'New Subtenant' wizard in the Veeam Backup & Replication console, specifically the 'Quotas' step. The main window has a sidebar with 'Cloud Director User', 'Quotas', and 'Summary'. The 'Quotas' section is active, showing a list of available user quotas. A 'Subtenant Quota' dialog box is open, allowing the user to configure a new quota. The dialog box contains the following fields and options:

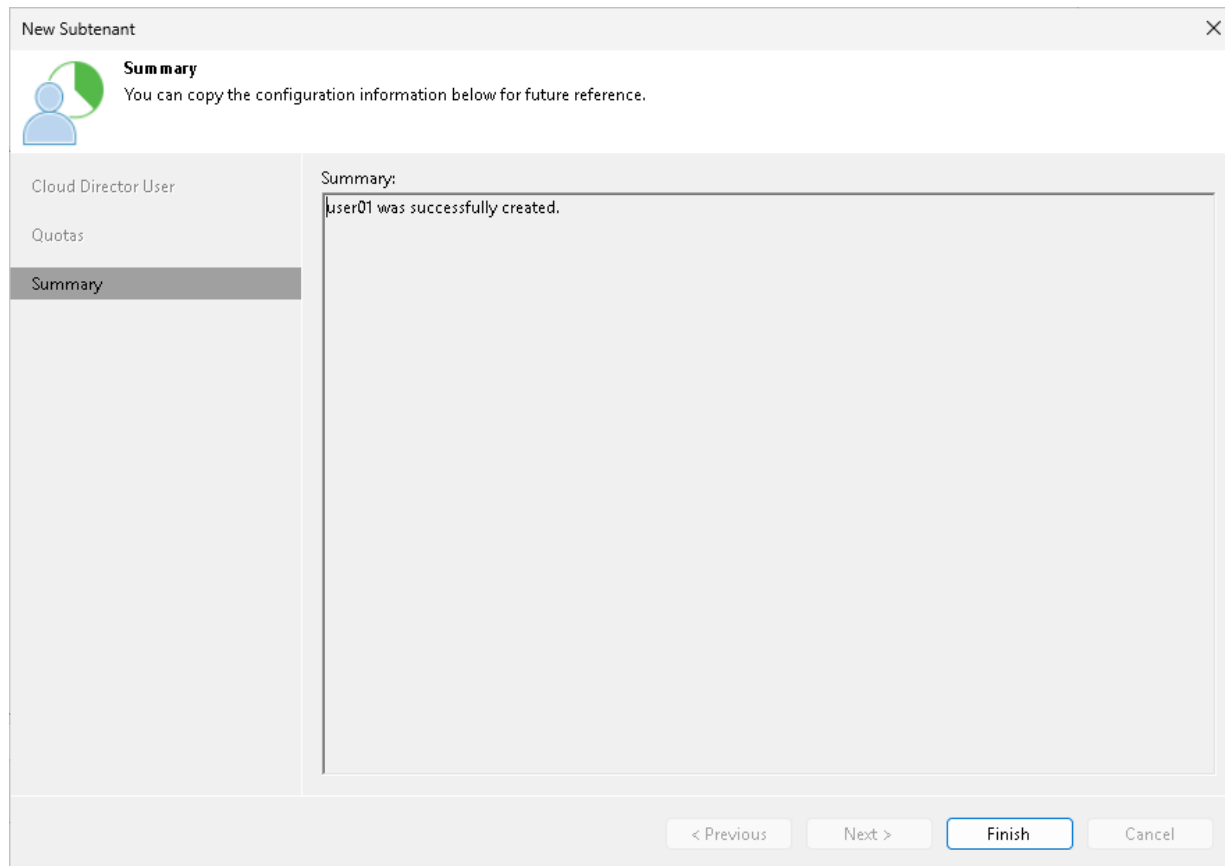
- Name:** Cloud Backup Storage
- Repository:** TechCompany Cloud Vol (Tenant's quota)
- Quota:**
 - ☐ Unlimited
 - ☒ Limit size to: 50 GB

The dialog box also shows '100 GB free of 100 GB' and 'OK' and 'Cancel' buttons. The main window has 'Add', 'Edit', and 'Remove' buttons on the right, and '< Previous', 'Next >', 'Finish', and 'Cancel' buttons at the bottom.

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

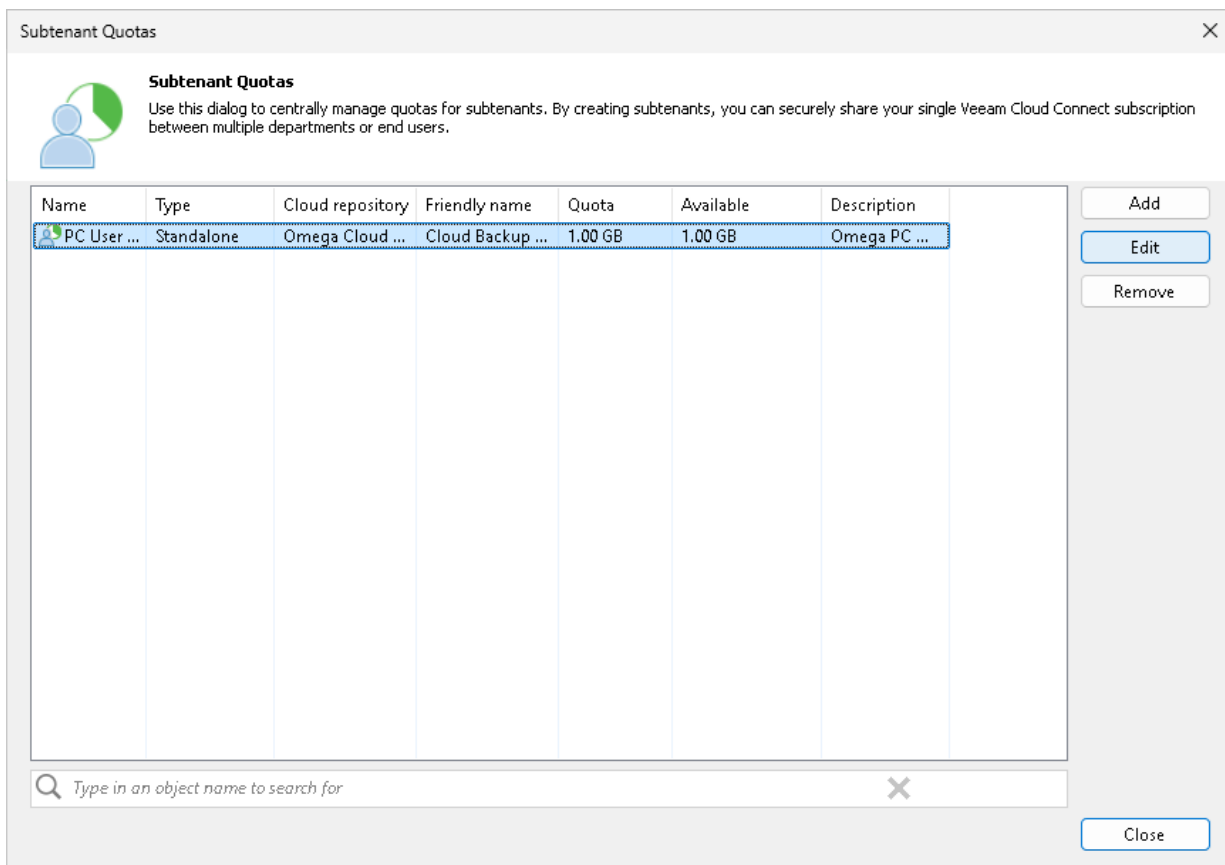
Consider the following:

- You cannot change a user name for the subtenant account.
- 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 backup data remain intact on the cloud repository. You can delete subtenant backup data manually later if needed.

NOTE

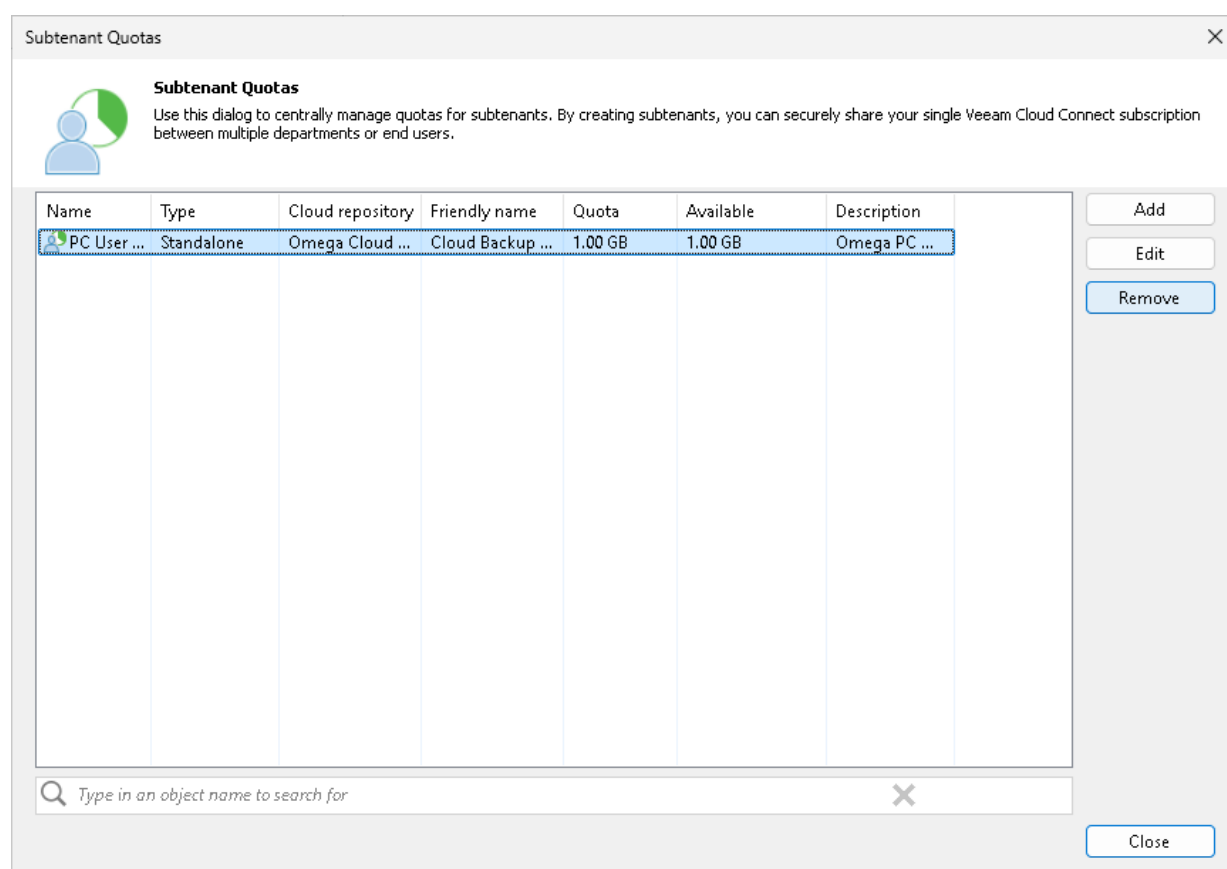
You cannot delete managed subtenant accounts — subtenant accounts created automatically by Veeam Backup & Replication in the Veeam Agent management scenario.

To delete a subtenant account:

1. Open the **Subtenant Quotas** window in one of the following ways:
 - 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 **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](#).

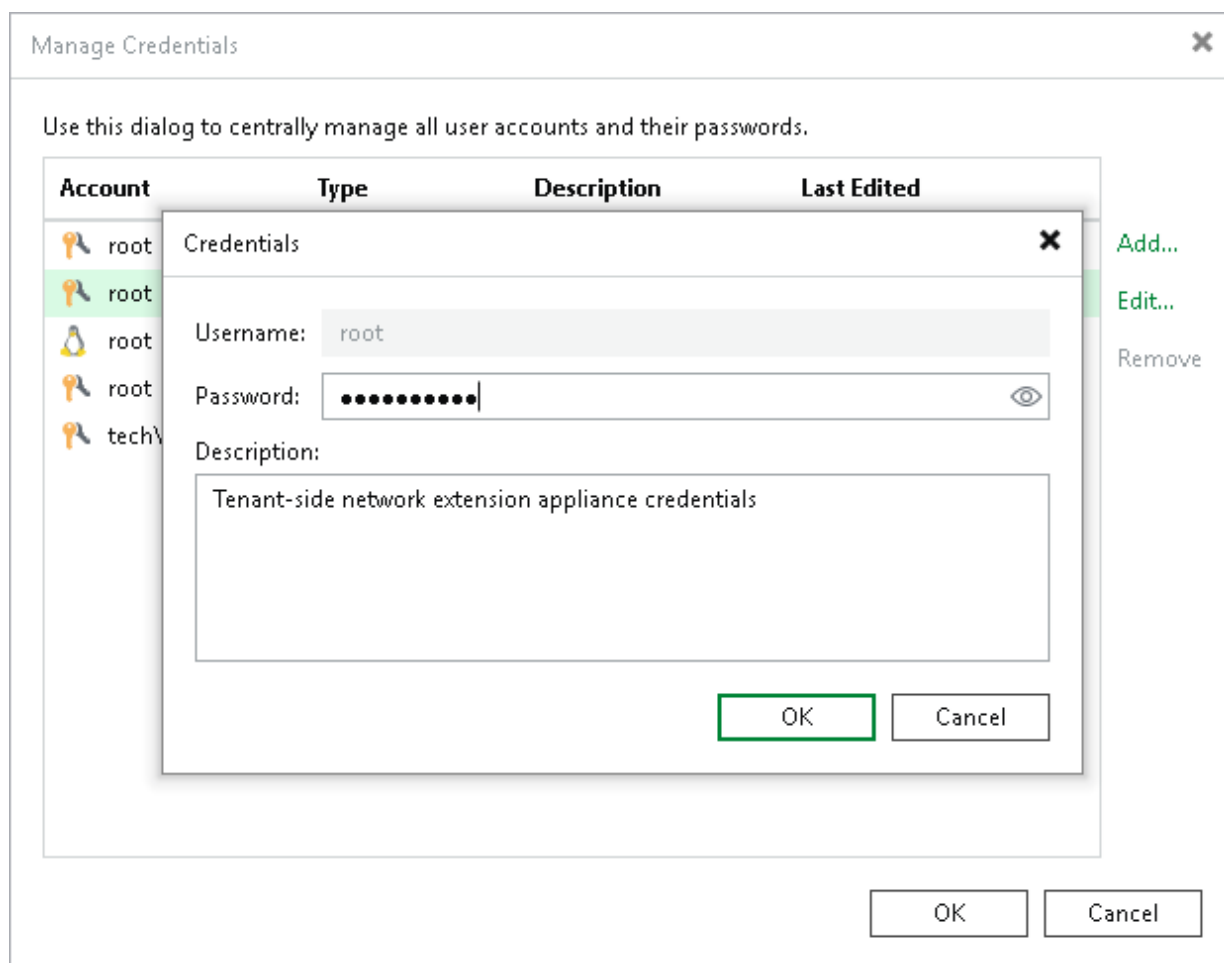
To change a password for the root account of network extension appliance VMs:

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.

- Click **OK** to save the specified password.



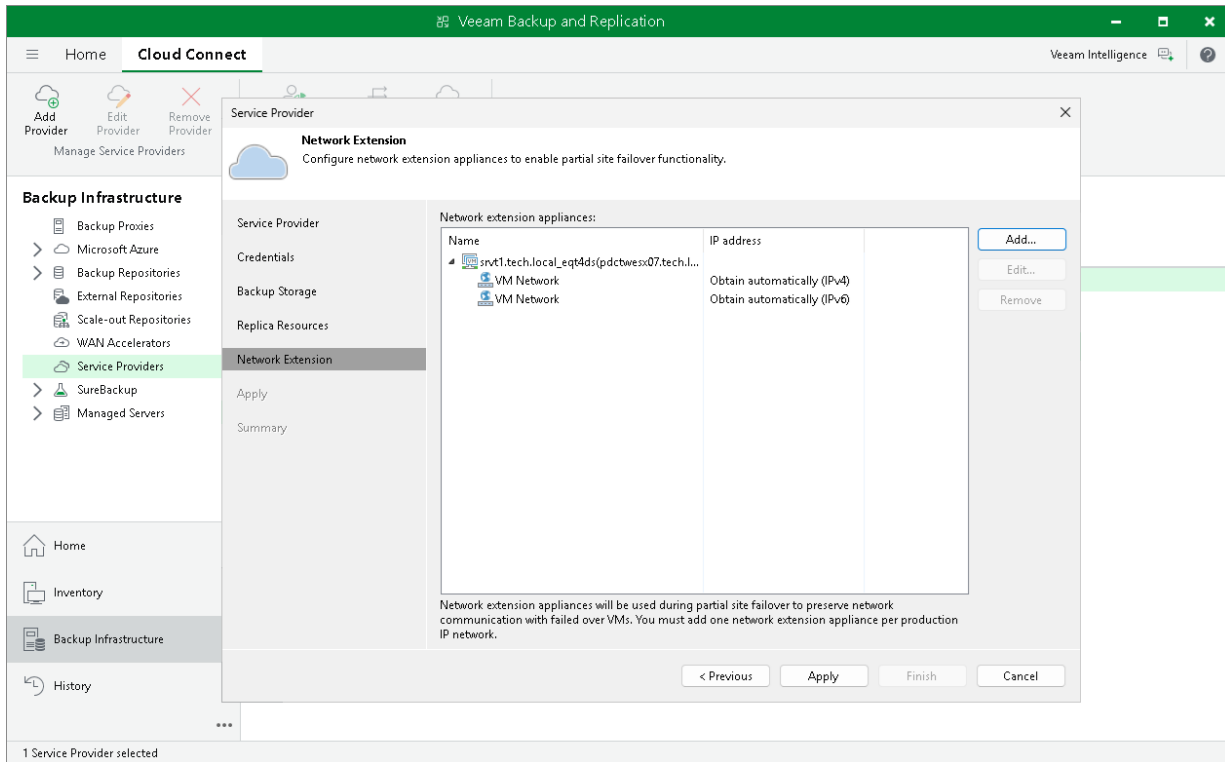
Redeploying Network Extension Appliance

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:

- Open the **Backup Infrastructure** view.
- In the inventory pane, click **Service Providers**.
- In the working area, right-click the necessary service provider and select **Properties**.
- At the **Network extension** step of the **Service Provider** wizard, in the **Network extension appliances** section, select the network extension appliance and click **Remove**.
- 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.
- 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.

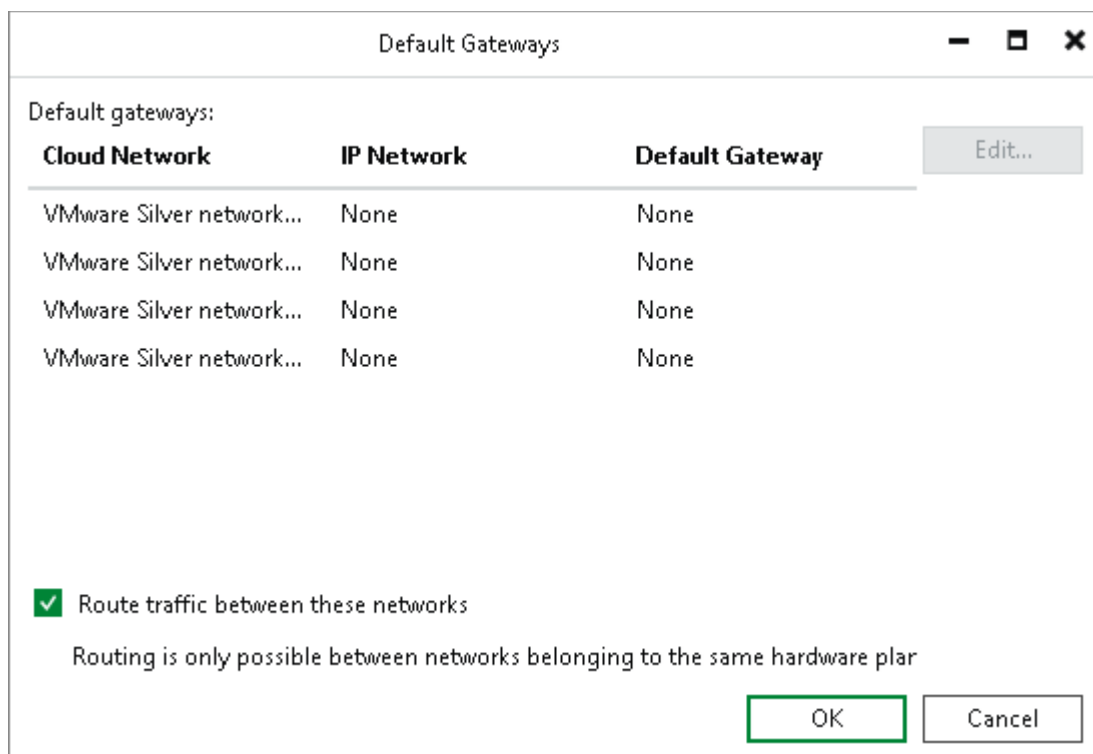
During the first run of the replication job targeted at the cloud host, Veeam Backup & Replication [detects network settings](#) of replicated VMs and automatically saves information about default gateways that are used in every detected production network. You can check and, if necessary, edit default 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.

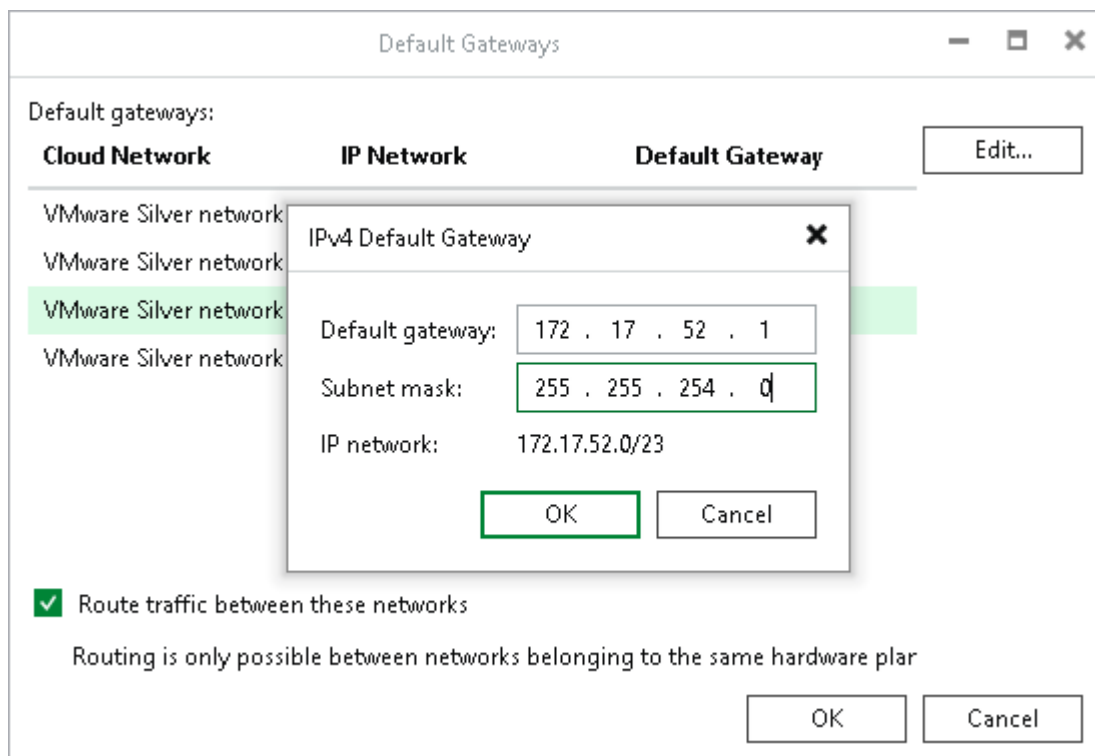
Network extension appliance can also route traffic between several networks provided for VM replicas through the same hardware plan.

To manage default gateways:

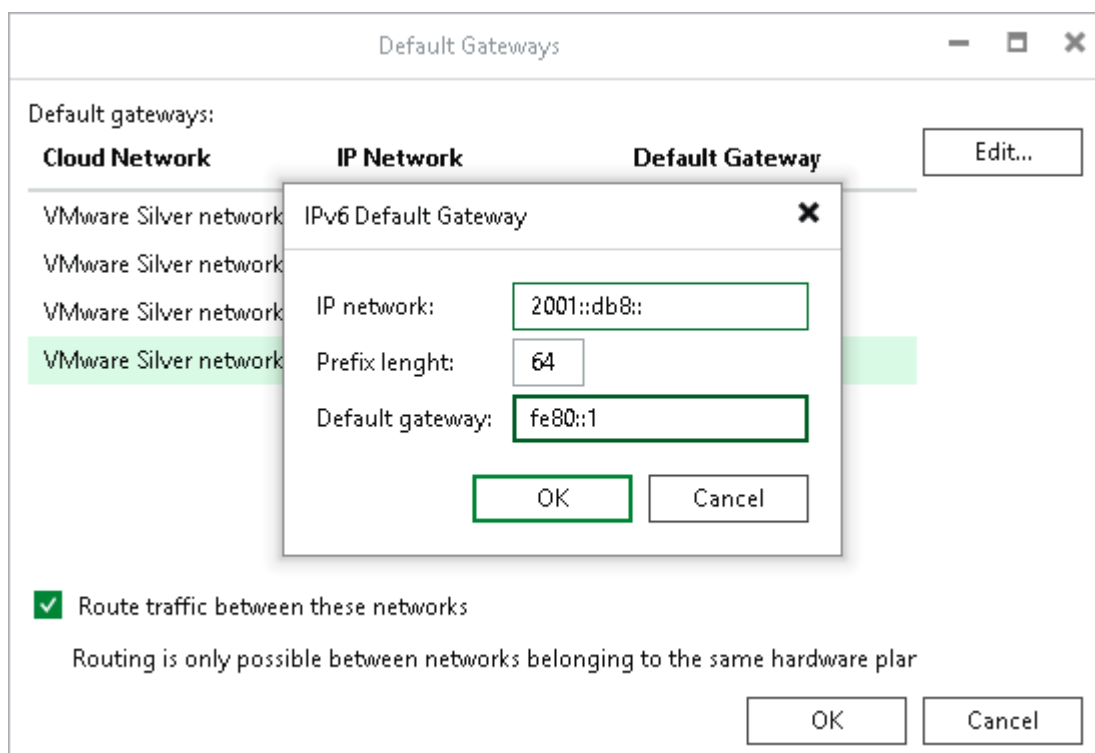
1. Open the **Backup Infrastructure** view.
2. In the inventory pane, click the **Service Providers** node.
3. In the working area, select the service provider and click **Manage Gateways** on the ribbon or right-click the service provider and select **Manage default gateways**.
4. In the **Default Gateways** 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 cloud host can use WAN acceleration, you can configure a source WAN accelerator on your side and create backup copy and replication jobs that will work using WAN accelerators.

The screenshot shows the 'New Replication Job' wizard in Veeam Backup & Replication, specifically the 'Data Transfer' step. The left sidebar contains a list of steps: Name, Virtual Machines, Destination, Network, Job Settings, Data Transfer (highlighted), Seeding, Guest Processing, Schedule, and Summary. The main area is titled 'Data Transfer' and contains the following text: 'Choose how VM data should be transferred to the target site.' Below this, a note states: 'When replicating between remote sites, we highly recommended that you deploy at least one backup proxy server locally in both sites to allow for direct access to storage.' The 'Source proxy:' section has a dropdown menu set to 'Automatic selection' with a 'Choose...' link. The 'Target proxy:' section has a dropdown menu set to 'Service provider's proxy' with a 'Choose...' link. Below these, there are two radio button options: 'Direct' (unselected) and 'Through built-in WAN accelerators' (selected). The 'Through built-in WAN accelerators' option has a description: 'Best for off-site replication over slow links due to significant bandwidth savings.' Under this option, there are two dropdown menus: 'Source WAN accelerator:' set to 'srv12 (ABC Company WAN Accelerator)' and 'Target WAN accelerator:' set to 'Service Provider's WAN Accelerator (Available)'. At the bottom right, there are four buttons: '< Previous', 'Next >' (highlighted), 'Finish', and 'Cancel'.

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

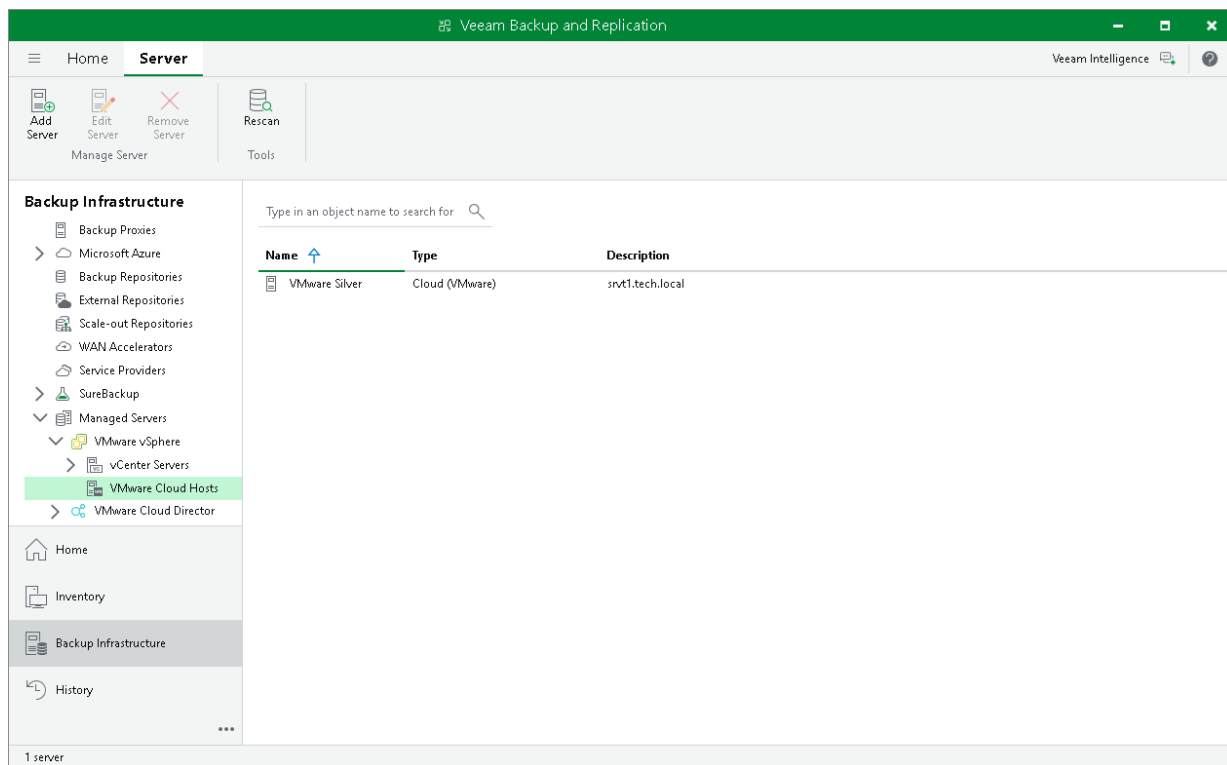
After tenant connects to the SP, cloud hosts provided to the tenant appear in the tenant Veeam backup console.

To view the available cloud hosts:

1. Open the **Backup Infrastructure** view.
2. In the inventory panel, expand the **Managed Servers** node.
 - Cloud hosts provided to the tenant through a VMware vSphere hardware plan are displayed under the **VMware vSphere > VMware Cloud Hosts** node.
 - 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.
 - 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.



The screenshot shows the Veeam Backup and Replication console interface. The top navigation bar is green with the title "Veeam Backup and Replication". Below it, the "Server" tab is selected. The left sidebar contains a "Backup Infrastructure" section with a tree view. The "Managed Servers" node is expanded, and the "VMware Cloud Hosts" node is selected and highlighted in green. The main area displays a table of cloud hosts.

Name	Type	Description
VMware Silver	Cloud (VMware)	srv11.tech.local

At the bottom of the console, a status bar indicates "1 server".

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](#) (for VMware vSphere and Microsoft Hyper-V platforms)
- [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.

To avoid problems with long paths, it is recommended to create job names not longer than 50 characters.

The screenshot shows the 'New Backup Job' wizard window. The left sidebar contains a list of steps: Name, Virtual Machines, Storage, Guest Processing, Schedule, and Summary. The 'Name' step is currently selected and highlighted in green. The main area of the wizard is titled 'Name' and contains the instruction 'Type in a name and description for this backup job.' Below this instruction, there are two input fields. The first is labeled 'Name:' and contains the text 'Fileserver Backup'. The second is labeled 'Description:' and contains the text 'Daily job for fileserver'. At the bottom of the main area, there is a checkbox labeled 'High priority' which is currently unchecked. Below the checkbox, there is a small text block that reads: 'Backup infrastructure resources are offered to high priority jobs first. Use this option for jobs sensitive to the start time, or jobs with strict RPO requirements.' At the bottom right of the wizard, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

New Backup Job

Name

Type in a name and description for this backup job.

Name:

Fileserver Backup

Description:

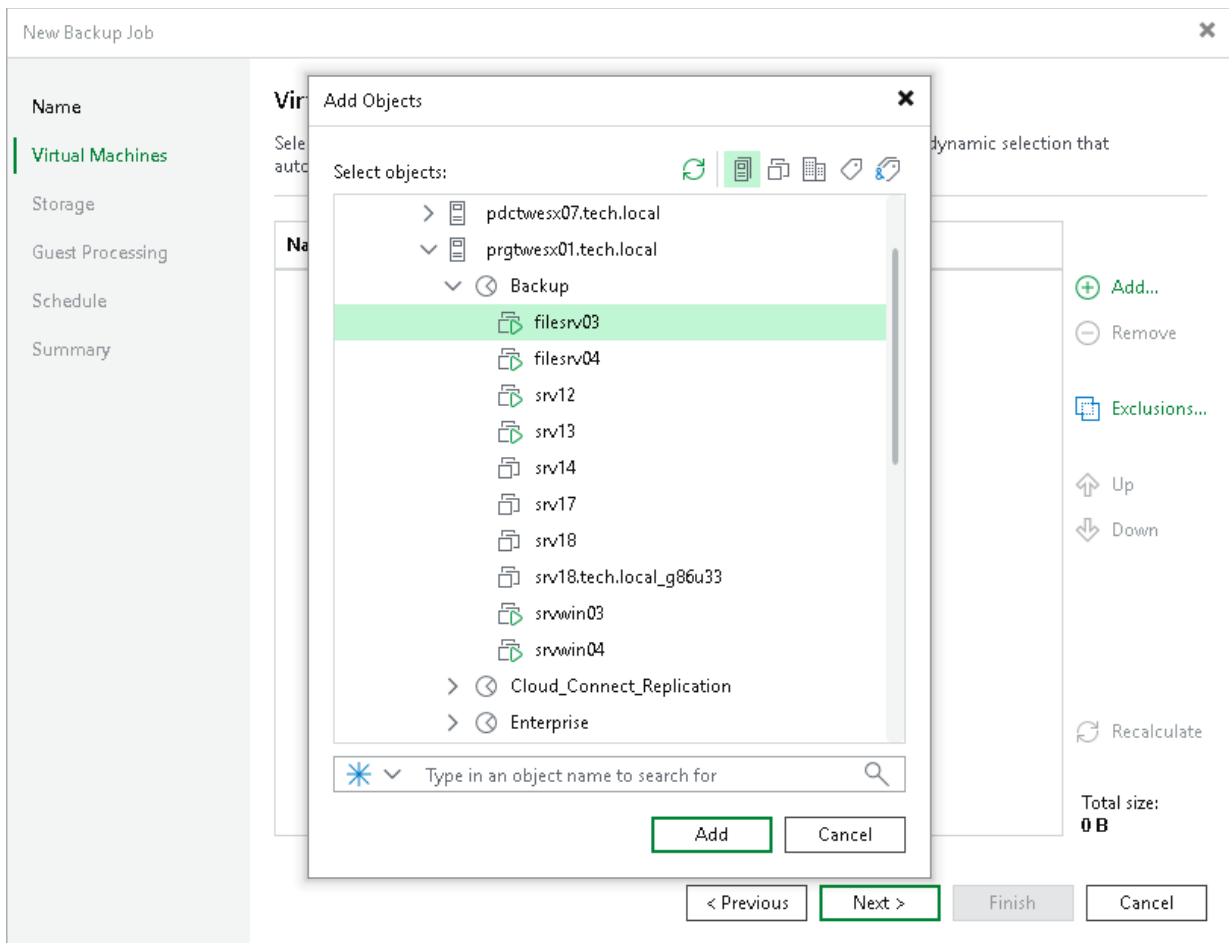
Daily job for fileserver

☐ High priority

Backup infrastructure resources are offered to high priority jobs first. Use this option for jobs sensitive to the start time, or jobs with strict RPO requirements.

< Previous Next > Finish Cancel

- 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.



- 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.
- 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 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.

New Backup Job

Name

Virtual Machines

Storage

Guest Processing

Schedule

Summary

Storage

Specify processing proxy server to be used for source data retrieval, backup repository to store the backup files produced by this job and customize advanced job settings if required.

Backup proxy:

Automatic selection

Choose...

Backup repository:

Omega Company Cloud Repository (Cloud repository)

10.0 GB free of 10.0 GB

Map backup

Retention policy:

7

days

Keep certain full backups longer for archival purposes

Configure...

GFS retention policy is not configured

Configure secondary destinations for this job

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.

Advanced job settings...

< Previous

Next >

Finish

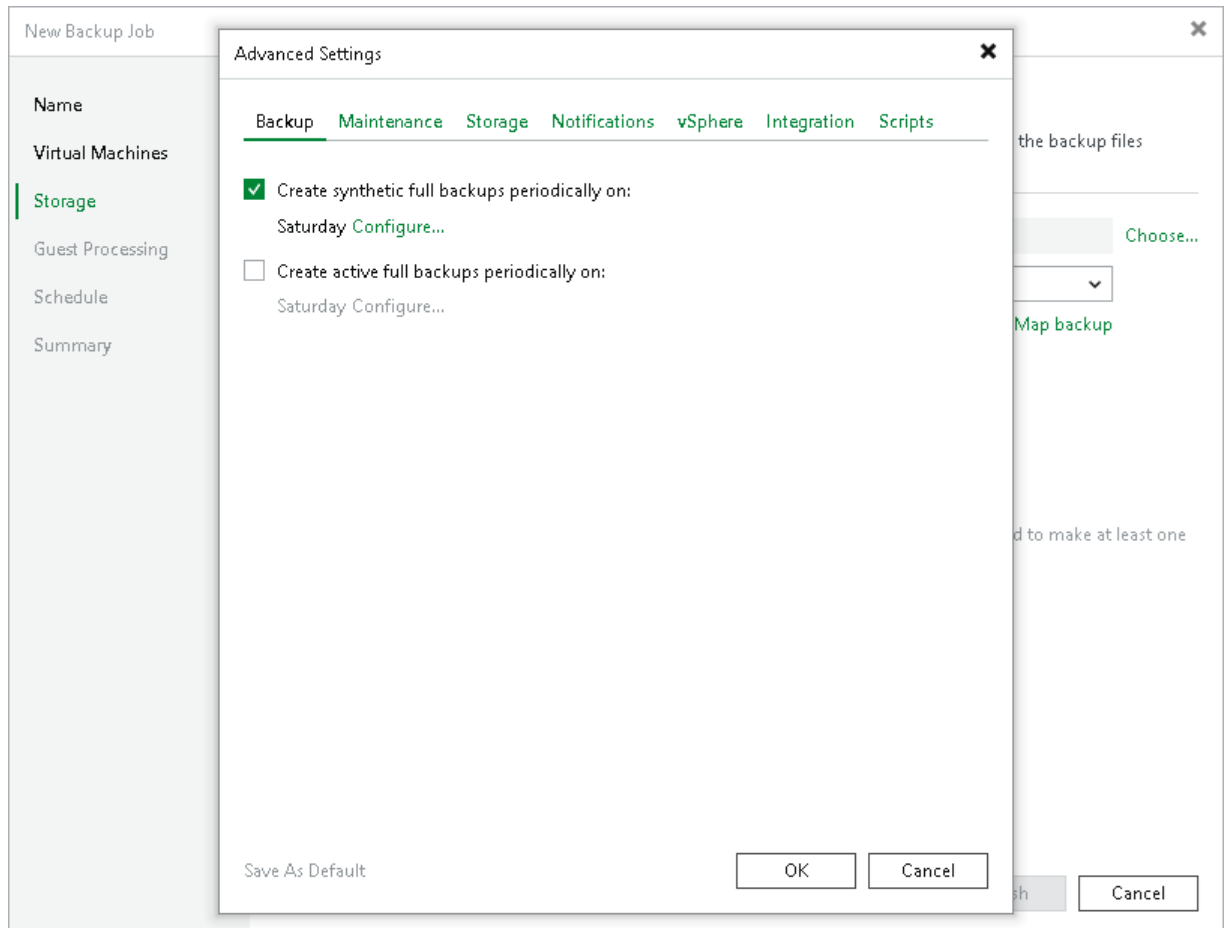
Cancel

7. Click **Advanced job settings**.

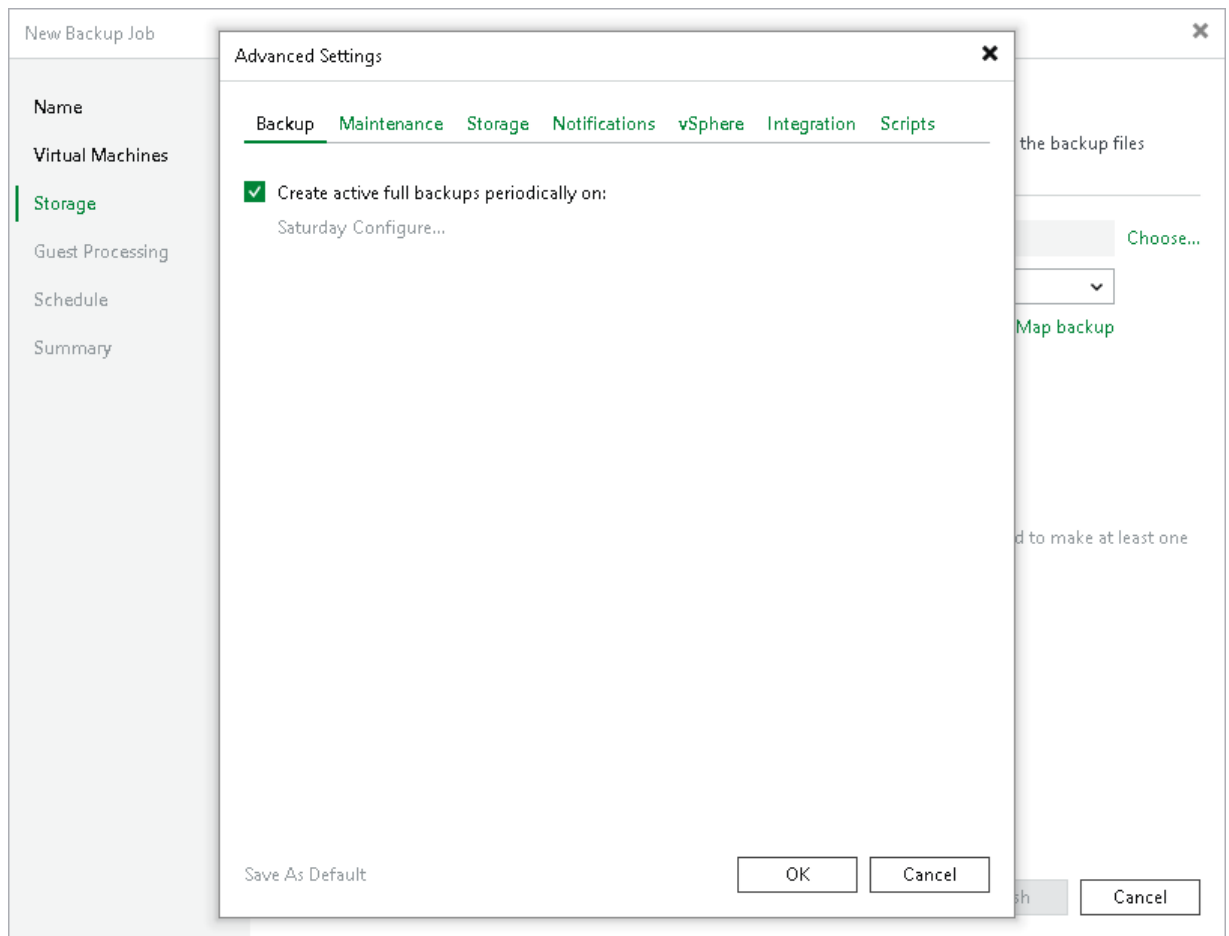
448 | VeeamCloudConnect | Administrator Guide | 13.1.0.411

8. On the **Backup** tab, specify advanced backup settings.

- [If a simple backup repository is used as the cloud repository] Veeam Backup & Replication uses forward incremental backup method for backup chain creation. You can choose to periodically create synthetic full backups and active full backups. To create synthetic full backups periodically, select the **Create synthetic full backups periodically on** check box and specify when you want to create synthetic full backups. To create active full backups periodically, select the **Create active full backups periodically on** check box and specify when you want to create active full backups.

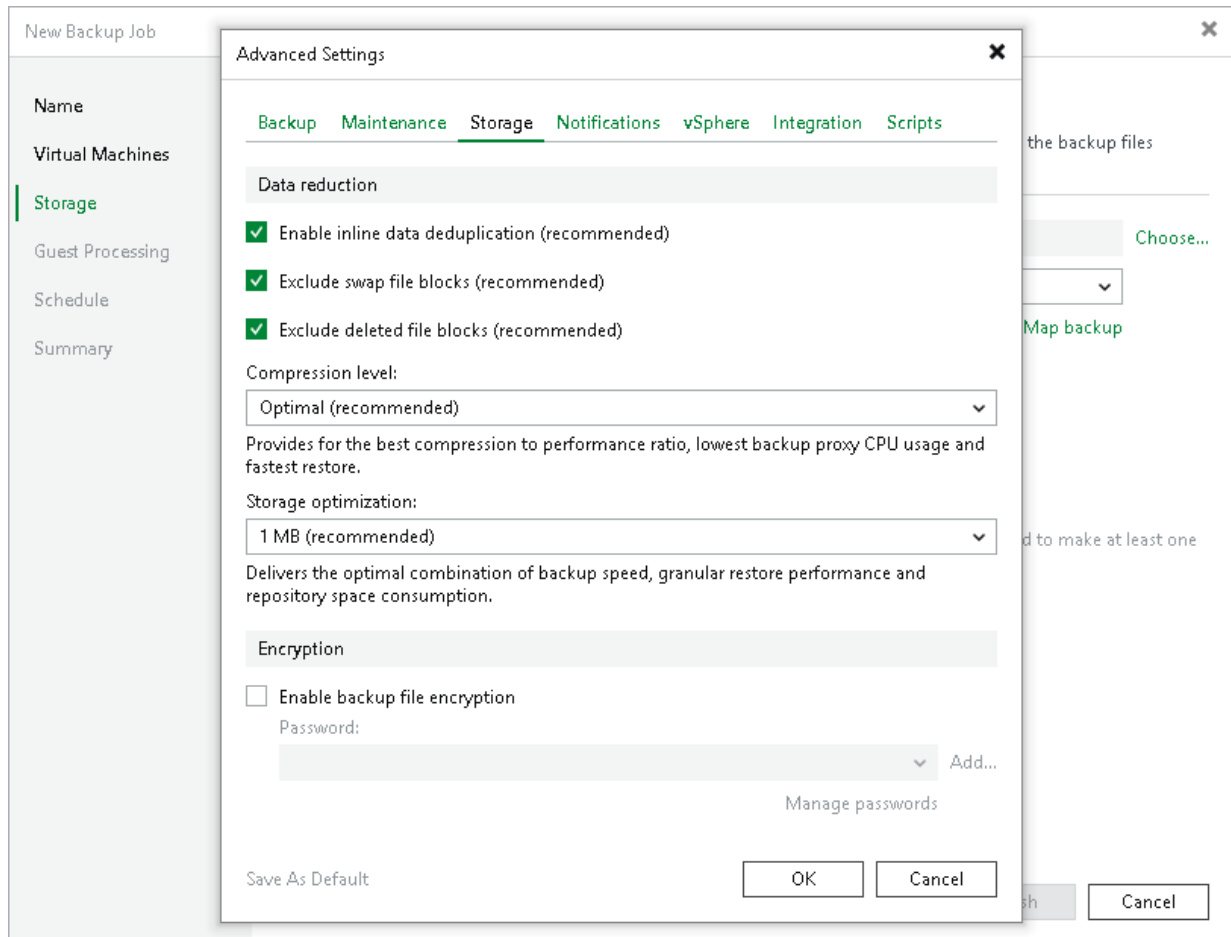


- [If an object storage repository is used as the cloud repository] Veeam Backup & Replication uses forward incremental backup method for backup chain creation. You can select the **Create active full backups periodically on** check box and specify when you want to create active full backups.



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.

You can select a Key Management System (KMS) server in the **Password** field. The KMS server must be added to Veeam Backup & Replication in advance. If you choose to use KMS keys for backup file encryption at this step of the wizard, Veeam Backup & Replication immediately starts communication with the KMS server to retrieve the encryption keys. To learn more, see the [Key Management System Keys](#) section in the Veeam Backup & Replication User Guide.



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 **Guest OS credentials for individual machines** and enter custom credentials for the necessary VM.

Edit Backup Job Fileserver Backup

Guest Processing

Choose guest OS processing options available for running VMs.

☒ **Enable application-aware processing**
 Detects and prepares applications for consistent backup, performs transaction logs processing, and configures the OS to perform required application restore steps upon first boot.
[Application handling options for individual machines](#)

☒ **Enable guest file system indexing and malware detection**
 Indexing enables global file search functionality, automatic detection of suspicious file system activity and known malware files.
[Indexing options for individual machines](#)

Guest interaction proxy:
 Automatic selection [Choose...](#)

Guest OS credentials:
 tech\susan.r.james (tech\susan.r.james, last edited: 5 days ago) [Add...](#)
[Manage accounts](#)

[Guest OS credentials for individual machines](#)

[Verify network connectivity and credentials](#)

< Previous **Next >** Finish Cancel

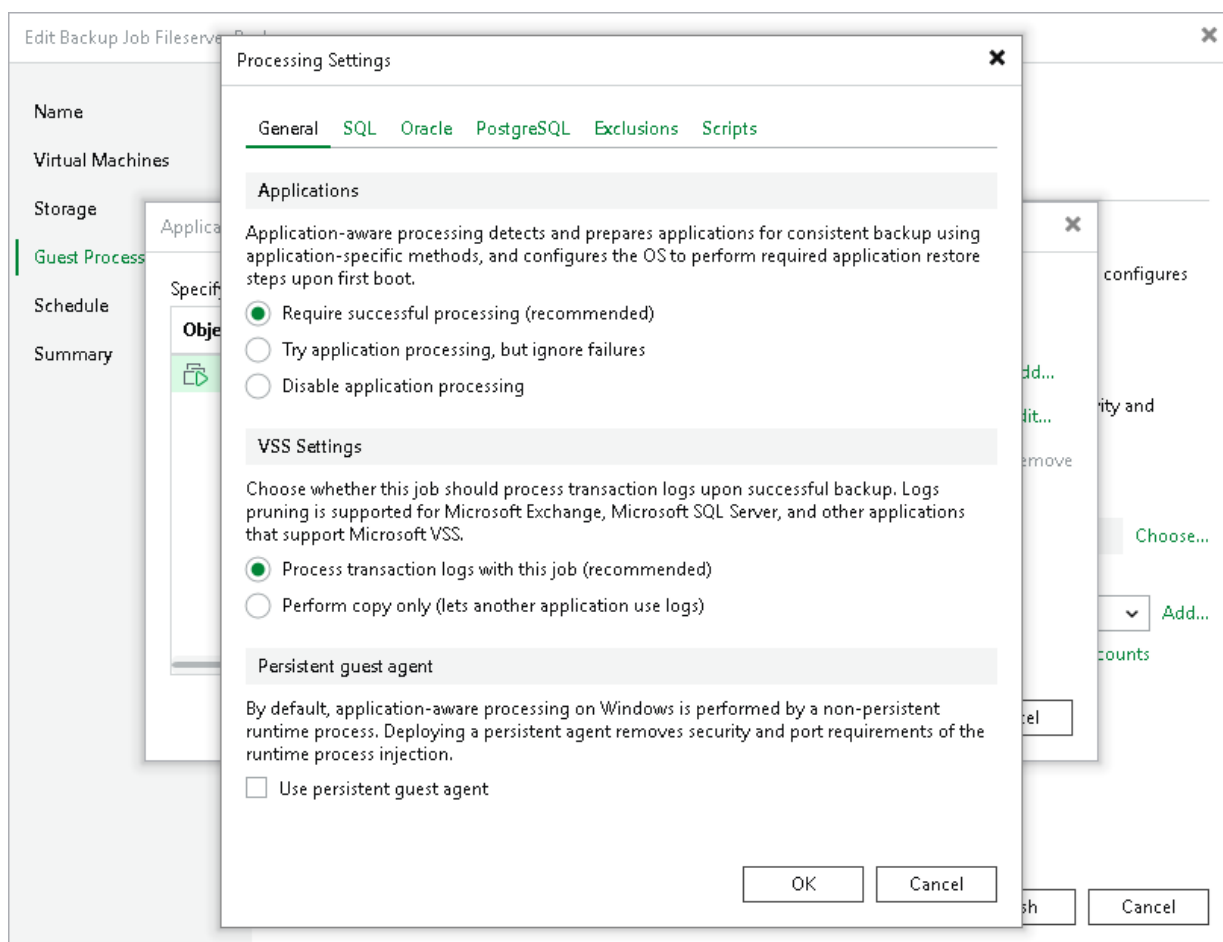
12. Click **Application handling options for individual machines**, select the necessary VM and click **Edit**. On the **General** tab, in the **Applications** section, specify the VSS behavior scenario:
 - Select **Require successful processing** if you want Veeam Backup & Replication to stop the backup process if any VSS errors occur.
 - 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.
 - 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:
 - 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.
 - 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 documentation](#).

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.

Edit Backup Job Fileserver Backup

Name

Virtual Machines

Storage

Guest Processing

Schedule

Summary

Schedule

Specify the job scheduling options. If you do not set the schedule, the job will need to be controlled manually.

☒ Run the job automatically

☒ Daily at this time: 10:00 PM ▼ ▲ Everyday ▼ Days...

☐ Monthly at this time: 10:00 PM ▼ ▲ Fourth ▼ Saturday ▼ Months...

☐ Periodically every: 1 ▼ Hours ▼ Schedule...

☐ After this job: Backup Job 1 (Created by .\Administrator at 10/21/2025 9:19 AM.) ▼

Automatic retry

☒ Retry failed items processing: 3 ▼ ▲ times

Wait before each retry attempt for: 10 ▼ ▲ minutes

Backup window

☐ Terminate the job outside of the allowed backup window

Long running or accidentally started jobs will be terminated to prevent impact on your production infrastructure during busy hours.

Window...

< Previous Apply Finish Cancel

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 Backup & Replication User 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 Backup & Replication User 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 Backup & Replication User 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*.

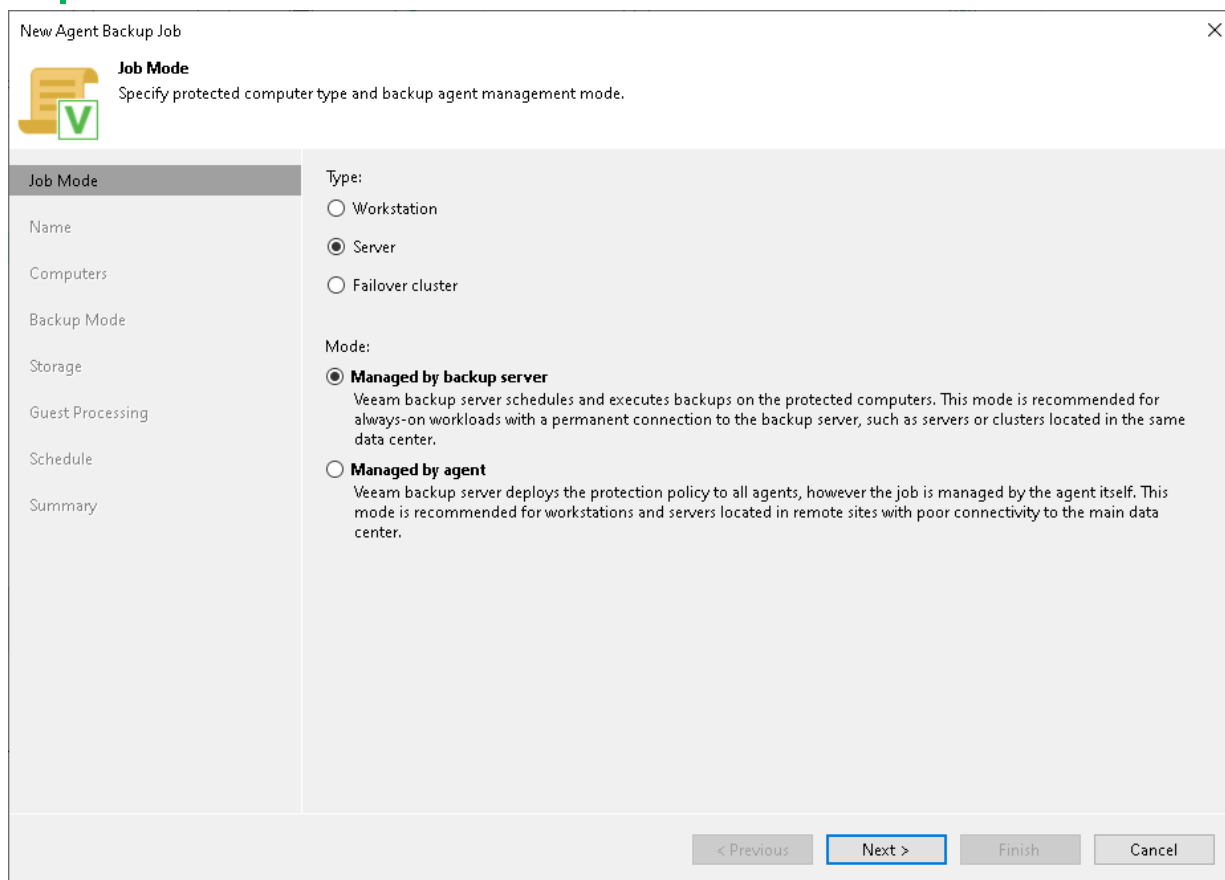
NOTE

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.



The screenshot shows the 'New Agent Backup Job' wizard window. The title bar reads 'New Agent Backup Job' with a close button (X) on the right. Below the title bar is a yellow document icon with a green checkmark and the text 'Job Mode' and 'Specify protected computer type and backup agent management mode.'.

On the left is a vertical sidebar with the following items: 'Job Mode' (highlighted), 'Name', 'Computers', 'Backup Mode', 'Storage', 'Guest Processing', 'Schedule', and 'Summary'.

The main area is divided into two sections:

- Type:**
 - ☐ Workstation
 - ☒ Server
 - ☐ Failover cluster
- Mode:**
 - ☒ **Managed by backup server**
Veeam backup server schedules and executes backups on the protected computers. This mode is recommended for always-on workloads with a permanent connection to the backup server, such as servers or clusters located in the same data center.
 - ☐ **Managed by agent**
Veeam backup server deploys the protection policy to all agents, however the job is managed by the agent itself. This mode is recommended for workstations and servers located in remote sites with poor connectivity to the main data center.

At the bottom right are four buttons: '< Previous' (disabled), 'Next >' (active/highlighted), 'Finish' (disabled), and 'Cancel' (disabled).

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

To avoid problems with long paths, it is recommended to create job names not longer than 50 characters.

The screenshot shows the 'New Agent Backup Job' wizard window. The 'Name' step is selected in the left sidebar. The main area contains a 'Name' field with the text 'Windows Server Backup' and a 'Description' field with the text 'Backup job for Microsoft Windows servers'. There is a 'High priority' checkbox which is unchecked. Below the checkbox, a note states: 'Backup infrastructure resources are offered to high priority jobs first. Use this option for jobs sensitive to the start time, or jobs with strict RPO requirements.' At the bottom right, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'. The 'Next >' button is highlighted with a blue border.

New Agent Backup Job

Name
Type in a name and description for this agent backup job.

Job Mode

Name

Computers

Backup Mode

Storage

Guest Processing

Schedule

Summary

Name:
Windows Server Backup

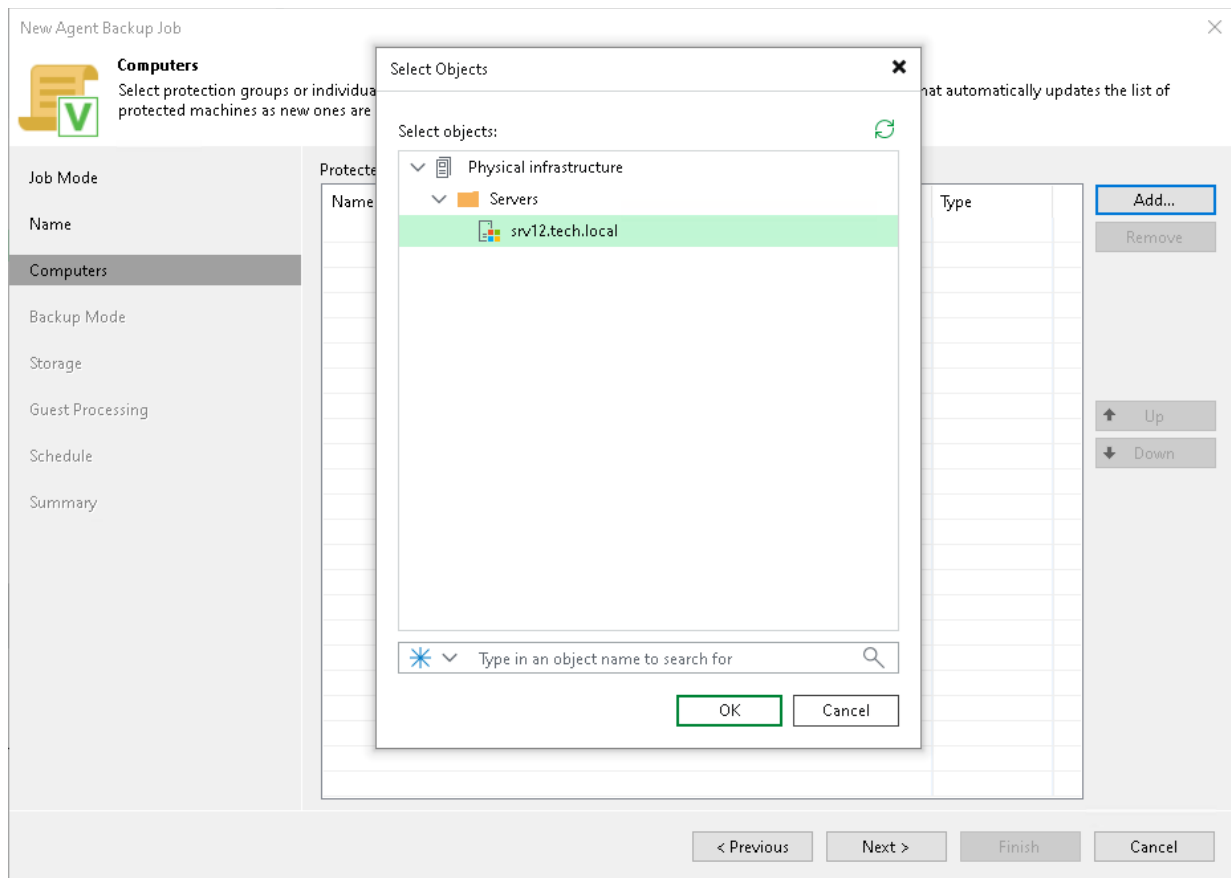
Description:
Backup job for Microsoft Windows servers

☐ High priority

Backup infrastructure resources are offered to high priority jobs first. Use this option for jobs sensitive to the start time, or jobs with strict RPO requirements.

< Previous Next > Finish Cancel

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:
- **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.
 - **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.

- **File level backup** – select this option if you want to create a backup of individual folders on your computer.

New Agent Backup Job ✕

 **Backup Mode**
Choose what data you want to back up from selected computers.

Job Mode	☐ Entire computer Back up entire computer image for fast recovery on any level. Deleted, temporary and page files are automatically excluded from the image to reduce the backup size. ☐ Include external USB drives
Name	
Computers	
Backup Mode	☒ Volume level backup Back up images of specified volumes, for example only data volumes. Deleted, temporary and page files are automatically excluded from the image to reduce the backup size.
Objects	
Storage	
Guest Processing	
Schedule	
Summary	

< Previous **Next >** Finish Cancel

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.
- 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.

New Agent Backup Job

Objects
Specify objects to include in the backup.

Job Mode

Name

Computers

Backup Mode

Objects

Storage

Guest Processing

Schedule

Summary

☒ Backup the following volumes only:

Object	
D:\	
OS volume	

Add... Edit... Remove

☐ Backup all volumes except the following:

Object	

Add... Edit... Remove

< Previous Next > Finish Cancel

- 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.

[illegible]

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.

New Agent Backup Job X

Destination

Choose where you want to backup data to.

Job Mode Name Computers Backup Mode Objects Destination Storage Backup Cache Guest Processing Schedule Summary	☐ Local storage Choose this option to back up to a locally attached storage device such as USB, Firewire or eSATA external hard drive. Backing up to internal hard drives is not recommended. ☐ Shared folder Choose this option to back up to an SMB (CIFS) share on a Network Attached Storage (NAS) device, or on a regular file server. ☐ Veeam backup repository Choose this option to back up to a backup repository managed by Veeam Backup & Replication server. ☒ Veeam Cloud Connect repository Choose this option to back up to a cloud repository managed by Veeam Cloud Connect service provider.

< Previous
Next >
Finish
Cancel

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. In the **Retention policy** field, specify 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.
- For a backup job managed by the backup server:

The screenshot shows the 'New Agent Backup Job' wizard in the 'Storage' step. The left sidebar contains a list of steps: Job Mode, Name, Computers, Backup Mode, Objects, Storage (selected), Guest Processing, Schedule, and Summary. The main area is titled 'Storage' with a subtitle 'Specify a backup repository to store the backup files produced by the backup job and customize advanced job settings if required.' Below this, there is a 'Backup repository:' dropdown menu showing 'Cloud Vol 01 (Cloud repository)' with a 'Map backup' link. A storage icon indicates '87,2 GB free of 100 GB'. The 'Keep backups for:' is set to '7 days'. There are two checkboxes: 'Keep certain full backups longer for archival purposes' (unchecked) with a 'Configure...' button, and 'Configure secondary destinations for this job' (unchecked). Below the second checkbox is a note: '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.' At the bottom of the main area, there is a note about advanced job settings and an 'Advanced...' button. The bottom navigation bar includes '< Previous', 'Next >' (highlighted), 'Finish', and 'Cancel'.

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

Name

Computers

Backup Mode

Objects

Storage

Guest Processing

Schedule

Summary

Backup repository:
Cloud Vol 01 (Cloud repository)

87,2 GB free of 100 GB [Map backup](#)

Keep backups for: 7 days

☐ Keep certain full backups longer for archival purposes [Configure...](#)
GFS retention policy is not configured

☐ Configure secondary destinations for this job
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.

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

- For a backup policy:

The screenshot shows the 'New Agent Backup Job' wizard in the 'Storage' step. The left sidebar contains a list of steps: Job Mode, Name, Computers, Backup Mode, Objects, Storage (highlighted), Backup Cache, Guest Processing, Schedule, and Summary. The main area is titled 'Storage' with a subtitle 'Specify a backup repository to store the backup files produced by the backup job and customize advanced job settings if required.' Below this, there is a 'Backup repository:' dropdown menu showing 'Cloud Vol 01 (Cloud repository)' with a status bar indicating '87,2 GB free of 100 GB'. A 'Keep backups for:' spinner is set to '7' days. There is an unchecked checkbox for 'Keep certain full backups longer for archival purposes' with a 'Configure...' button next to it. At the bottom of the main area, there is a note about advanced job settings and an 'Advanced...' button. The bottom of the wizard has four buttons: '< Previous', 'Next >' (highlighted with a blue border), 'Finish', and 'Cancel'.

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

Name

Computers

Backup Mode

Objects

Storage

Backup Cache

Guest Processing

Schedule

Summary

Backup repository:
Cloud Vol 01 (Cloud repository)
87,2 GB free of 100 GB

Keep backups for: 7 days

☐ Keep certain full backups longer for archival purposes
GFS retention policy is not configured

Configure...

Advanced job settings include backup mode, compression and deduplication, block size, notification settings, automated post-job activity and other settings.

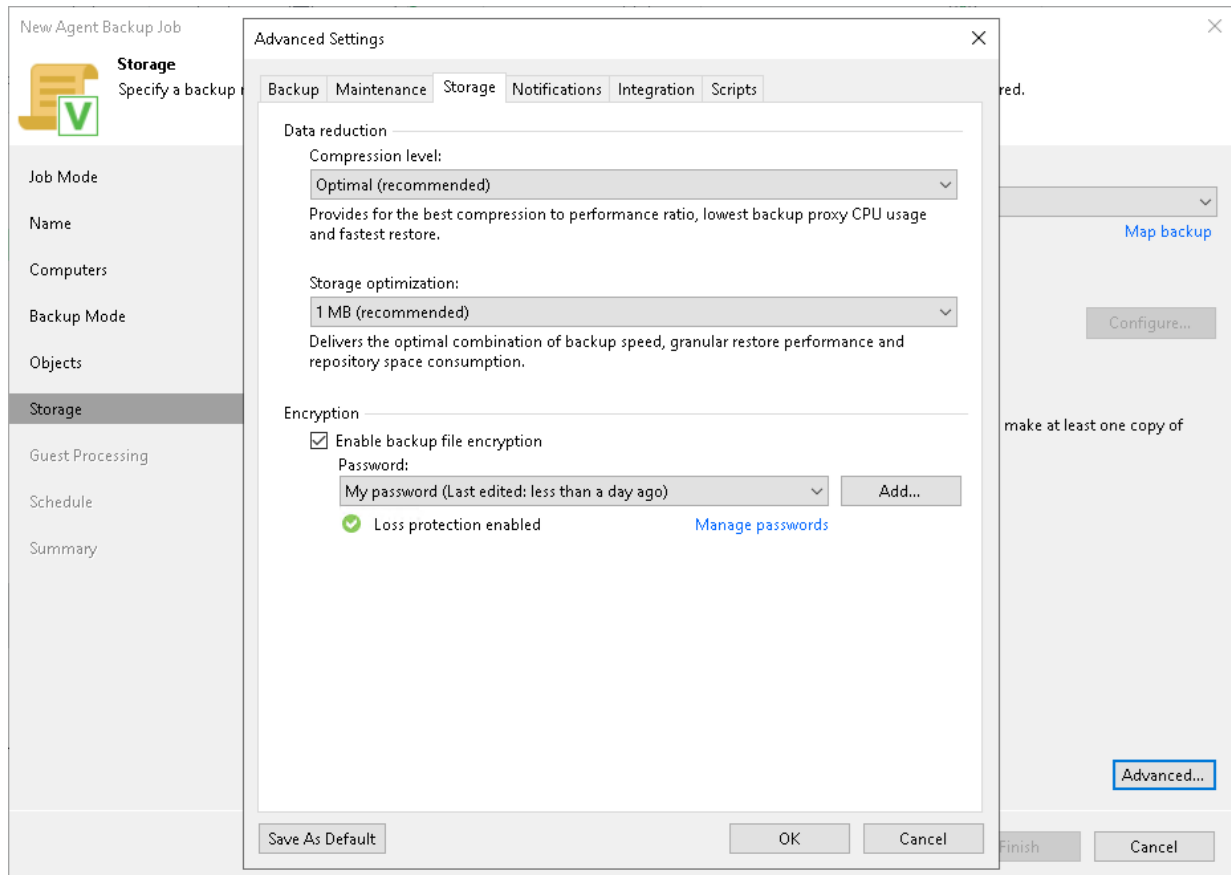
Advanced...

< 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.

[For a backup job managed by the backup server] You can select a Key Management System (KMS) server in the **Password** field. The KMS server must be added to Veeam Backup & Replication in advance. If you choose to use KMS keys for backup file encryption at this step of the wizard, Veeam Backup & Replication immediately starts communication with the KMS server to retrieve the encryption keys. To learn more, see the [Key Management System Keys](#) section in the Veeam Backup & Replication User Guide.



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.

New Agent Backup Job

×



Backup Cache
Local backup cache allows backups to continue on schedule even if remote backup target is temporarily unavailable.

Job Mode

Name

Computers

Backup Mode

Destination

Storage

Backup Cache

Guest Processing

Schedule

Summary

☒ Enable backup cache
Whenever a connection to the backup target cannot be established, the cache folder will be used instead. Cached backups are uploaded to the target as soon as it becomes reachable.
Maximum size:
Location:
☒ Automatic selection (recommended)
We will pick a suitable volume with most free disk space available on every protected machine.
☐ Manual selection (specified volume must exist on every machine)
Folder:

< Previous

Next >

Finish

Cancel

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.

The screenshot shows the 'New Agent Backup Job' wizard window. The title bar reads 'New Agent Backup Job' with a close button (X) on the right. Below the title bar, there is a yellow folder icon with a green checkmark and the text 'Guest Processing' and 'Choose application processing options.'.

On the left side, there is a vertical list of steps: 'Job Mode', 'Name', 'Computers', 'Backup Mode', 'Objects', 'Storage', 'Guest Processing' (which is highlighted with a dark grey background), 'Schedule', and 'Summary'.

The main area of the wizard contains two checked options:

- ☒ **Enable application-aware processing**
Detects and prepares applications for consistent backup, performs transaction logs processing, and configures the OS to perform required application restore steps upon first boot.
Application handling options for individual machines and applications... [Applications...](#)
- ☒ **Enable guest file system indexing and malware detection**
Indexing enables global file search functionality, automatic detection of suspicious file system activity and known malware files.
Advanced guest file system indexing options for individual machines... [Indexing...](#)

At the bottom of the window, there are four buttons: '< Previous', 'Next >' (which is highlighted with a blue border), 'Finish', and 'Cancel'.

14. At the **Schedule** step of the wizard, specify the schedule according to which you want to perform backup:
- 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.

The screenshot shows the 'New Agent Backup Job' wizard, specifically the 'Schedule' step. The window title is 'New Agent Backup Job' with a close button (X) in the top right corner. On the left is a sidebar with a tree view containing: Job Mode, Name, Computers, Backup Mode, Objects, Storage, Guest Processing, **Schedule** (highlighted), and Summary. The main area has a header with a folder icon and a green checkmark, followed by the title 'Schedule' and the instruction 'Specify the scheduling options to distribute to backup agents on hosts under this policy.' Below this, there are several sections: 1. 'Run the job automatically' (checked): Includes radio buttons for 'Daily at this time:', 'Monthly at this time:', 'Periodically every:', and 'After this job:'. 'Daily at this time:' is selected, showing a time of 22:00 and a frequency of 'Everyday'. Other options show '22:00' for monthly, '1' for periodic, and a dropdown for 'After this job' currently set to 'Fileserver Backup (Created by .\Administrator)'. 2. 'Automatic retry': Includes a checked checkbox 'Retry failed items processing:' with a value of 3 times, and 'Wait before each retry attempt for: 10 minutes'. 3. 'Backup window': Includes an unchecked checkbox 'Terminate job outside of the backup window' and a 'Window...' button. At the bottom are buttons: '< Previous', 'Apply' (highlighted with a blue border), 'Finish', and 'Cancel'.

New Agent Backup Job

Schedule
Specify the scheduling options to distribute to backup agents on hosts under this policy.

Job Mode

Name

Computers

Backup Mode

Objects

Storage

Guest Processing

Schedule

Summary

☒ Run the job automatically

☒ Daily at this time: 22:00 Everyday Days...

☐ Monthly at this time: 22:00 Fourth Saturday Months...

☐ Periodically every: 1 Hours Schedule...

☐ After this job: Fileserver Backup (Created by .\Administrator)

Automatic retry

☒ Retry failed items processing: 3 times

Wait before each retry attempt for: 10 minutes

Backup window

☐ Terminate job outside of the backup window Window...

Prevent long-running or accidentally started job from impacting your production infrastructure during the busy hours.

< Previous Apply Finish Cancel

- 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.

New Agent Backup Job [X]

Schedule
Specify the scheduling options. If you do not set the schedule, the job will need to be controlled manually.

Job Mode

Name

Computers

Backup Mode

Objects

Destination

Storage

Backup Cache

Schedule

Summary

Periodically
We will wake your computers from sleep to take a backup unless the connected standby power model is enabled. Normally, this model is only enabled on mobile devices, such as tablets.

☒ Daily at 22:00 Everyday Days...

If computer is powered off at this time Skip backup

Once backup is taken, computer should Keep running

At the following events

☐ Lock

☐ Log off

☐ When backup target is connected

☐ Eject removable storage once backup is completed (ransomware protection)

Back up no more often than every 2 hours

< Previous Apply Finish Cancel

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 for VMs and Physical Machines Using Console](#) section in the Veeam Backup & Replication User Guide.

To create a backup copy job:

1. On the **Home** tab, click **Backup Copy > Image-level backup**.

2. At the **Name** step of the wizard, specify a name and description for the backup copy job and select the backup copy mode:
 - Select the **Immediate copy** option to copy new restore points and, if required, database log backups as soon as they appear in the source backup repository.
 - Select the **Periodic copy** option to copy the most recent restore points according to a specified schedule.

To avoid problems with long paths, it is recommended to create job names not longer than 50 characters.

The screenshot shows the 'New Backup Copy Job' wizard with the 'Name' step selected in the left sidebar. The main area contains the following fields and options:

- Name:** A text input field containing 'DB Backup Copy'.
- Description:** A text area containing 'Daily backup copy job for DB backup'.
- Copy mode:** Two radio button options:
 - ☒ **Immediate copy (mirroring)**: Copies every restore point as soon as it appears in the primary backup repository. This mode will copy all backups created by selected backup jobs, including transaction log backups.
 - ☐ **Periodic copy (pruning)**: Periodically copies the latest available restore point only. This mode also allows for selecting which backups to process, enabling you to further reduce bandwidth usage.

At the bottom right, there are four buttons: '< Previous' (disabled), 'Next >' (active), 'Finish' (disabled), and 'Cancel'.

3. At the **Objects** step of the wizard, specify what data Veeam Backup & Replication will copy to the cloud repository.
 - 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.
 - 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.

New Backup Copy Job

Objects

Add objects which backups should be mirrored to the target repository. Immediate backup copy job will process image-level and transaction log backups.

Objects to process:

Name	Type	Size
DB Backup	VMware Backup Job	20.0 GB

☒ Include database transaction log backups (increases bandwidth usage)

Total size: 20.0 GB

< Previous **Next >** Finish Cancel

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 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.

New Backup Copy Job

Name

Objects

Target

Data Transfer

Schedule

Summary

Target

Specify the target backup repository, number of recent restore points to keep, and the retention policy for full backups. You can use map backup functionality to seed backup files.

Backup repository: Omega Company Cloud Repository (Cloud repository) 29,9 GB free of 30,0 GB Map backup

Retention policy: 7 days

☒ Keep certain full backups longer for archival purposes Configure...

GFS retention policy is not configured

☐ Read the entire restore point from source backup instead of synthesizing it from increments

Advanced job settings

< Previous

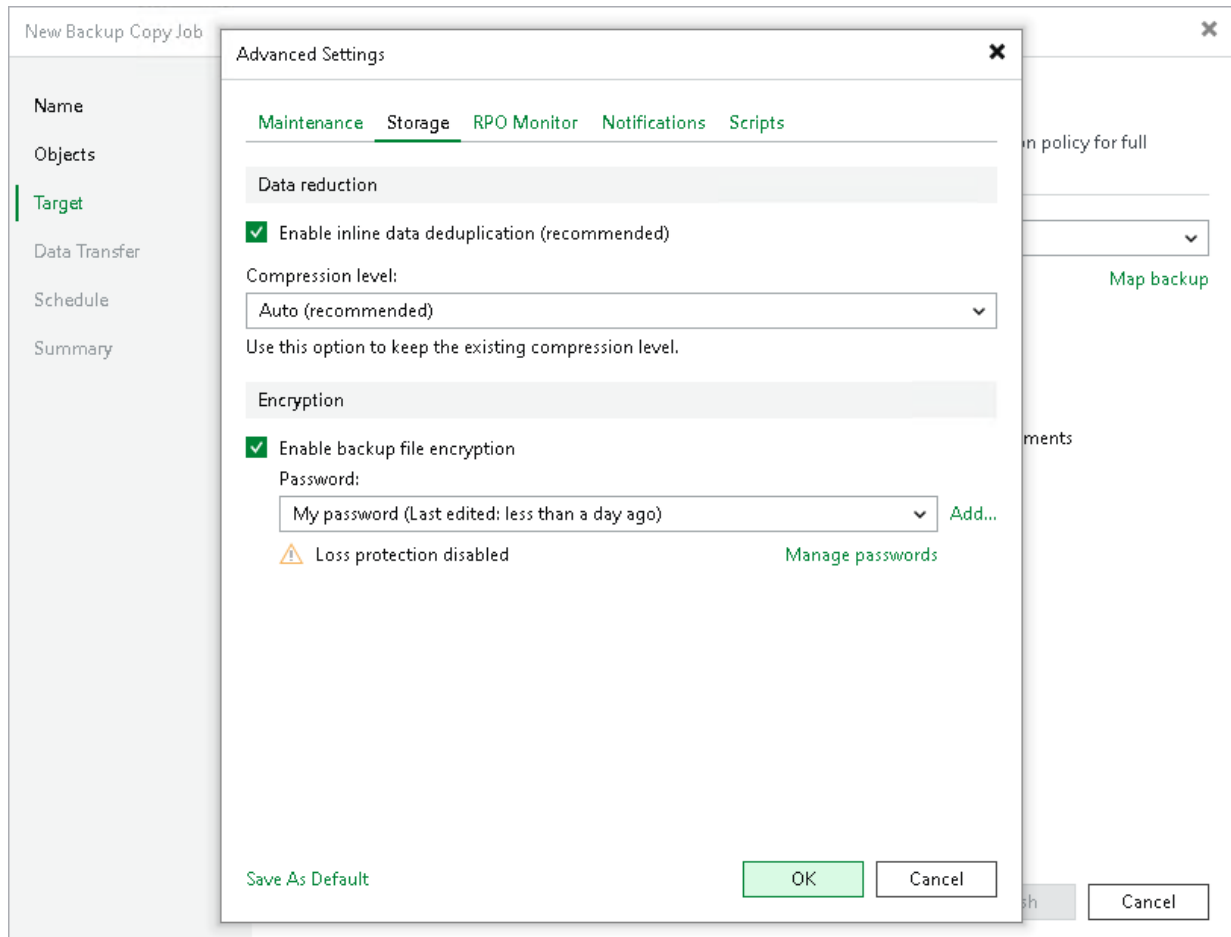
Next >

Finish

Cancel

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.

You can select a Key Management System (KMS) server in the **Password** field. The KMS server must be added to Veeam Backup & Replication in advance. If you choose to use KMS keys for backup file encryption at this step of the wizard, Veeam Backup & Replication immediately starts communication with the KMS server to retrieve the encryption keys. To learn more, see the [Key Management System Keys](#) section in the Veeam Backup & Replication User Guide.



9. At the **Data Transfer** step of the wizard, specify a data transfer path for the backup copy job:
 - If the cloud repository does not use WAN accelerators, select **Direct**.

- 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.

New Backup Copy Job

Name

Objects

Target

Data Transfer

Schedule

Summary

Data Transfer

Choose how object data should be transferred from source to target backup repository.

Direct

Object data will be sent directly from source to target repository. This mode is recommended for copying backups on-site, and off-site over a fast connection.

Through built-in WAN accelerators

Object data will be sent to target repository through WAN accelerators that must be deployed in both source and target sites. This mode provides for significant bandwidth savings.

Source WAN accelerator:

srv12 (ABC Company WAN Accelerator)

Target WAN accelerator:

Service Provider's WAN Accelerator (Available)

< Previous

Next >

Finish

Cancel

- [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.

New Backup Copy Job

Name

Objects

Target

Data Transfer

Schedule

Summary

Schedule

Specify the backup copy job schedule.

This job can transfer data:

Any time (continuously)

During the following time periods only:

AllNone

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Monday	■	■	■	■																		■	■	■
Tuesday	■	■	■	■																		■	■	■
Wednesday	■	■	■	■																		■	■	■
Thursday	■	■	■	■																		■	■	■
Friday	■	■	■	■																		■	■	■
Saturday	■	■	■	■																		■	■	■
Sunday	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■

EnabledDisabled

< PreviousApplyFinishCancel

- [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.

New Backup Copy Job

Name

Objects

Target

Data Transfer

Schedule

Summary

Schedule

Specify the backup copy job schedule.

☒ Run the job automatically

☒ Daily at this time: 22:00 Everyday Days...

☐ Monthly at this time: 22:00 Fourth Saturday Months...

☐ Periodically every: 1 Hours Schedule...

☐ After this job: Backup Job 1 (Created by .\Administrator)

Automatic retry

☒ Retry failed items processing: 3 times

Wait before each retry attempt for: 10 minutes

Backup window

☐ Terminate the job outside of the allowed backup window

Long running or accidentally started jobs will be terminated to prevent impact on your production infrastructure during busy hours.

Window...

< Previous

Apply

Finish

Cancel

- 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.
- Click **Finish**.

Performing Restore

You can perform the following data recovery tasks with backups that reside in 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)
 - [Disk publishing](#)
- [Backup export](#)
- [File copy](#) (manual operations)

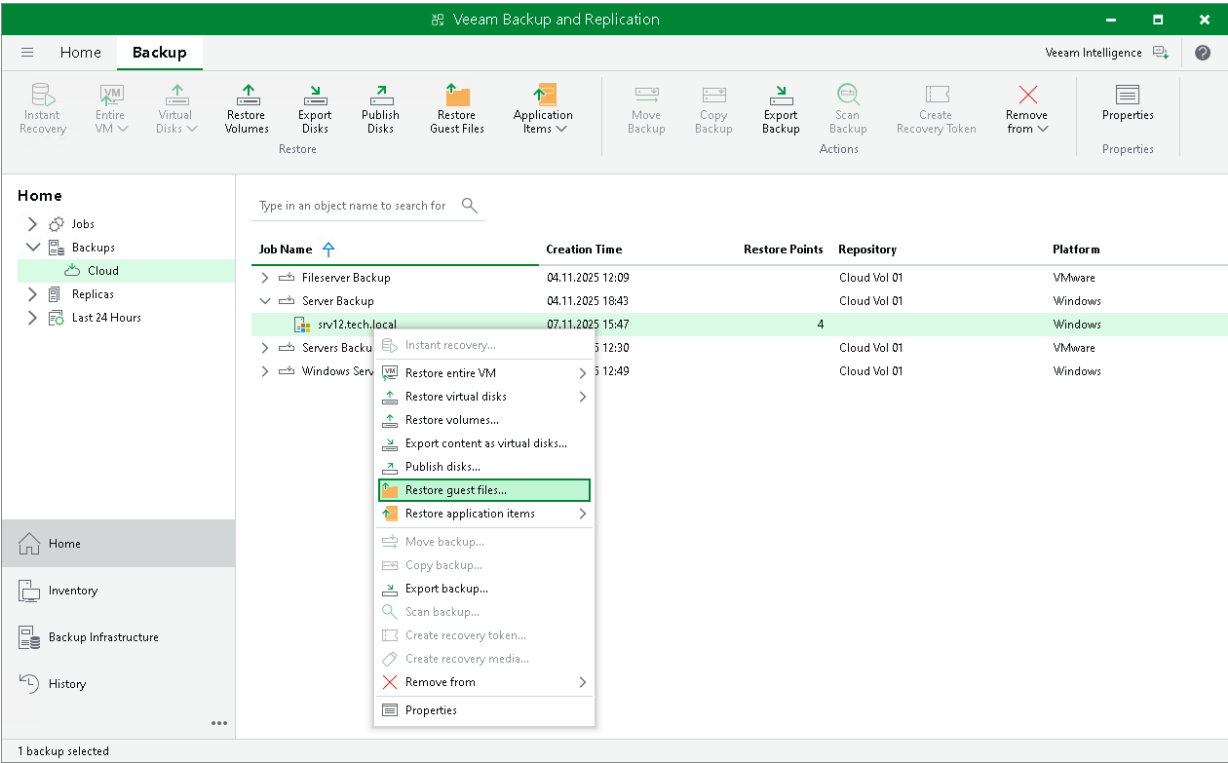
NOTE

Consider the following:

- If you allowed the SP to manage the tenant backup server, the SP can use the SP backup console to perform selected data recovery operations from tenant backups. To learn more, see [Restoring Data 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](#).
- If Nutanix AHV Plug-in is installed and a Nutanix AHV cluster is added in Veeam Backup & Replication, you can perform instant recovery to Nutanix AHV from backups that reside in the cloud repository. For more information, see the [Instant Recovery](#) section in the Veeam Backup for Nutanix AHV 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 VMs Using Console](#) 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**.

- [illegible]

- 480 | Veeam Cloud Connect | Administrator Guide | 13.1.0.411

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.

The screenshot shows the 'Entire VM Restore' wizard window. The title bar says 'Entire VM Restore' with a close button. Inside, there's a 'Restore Mode' section with a sub-header 'Specify whether selected VMs should be restored back to the original location, or to a new location or with different settings.' Below this is a list of steps on the left: 'Virtual Machines', 'Restore Mode' (selected), 'Host', 'Resource Pool', 'Datastore', 'Folder', 'Network', 'Secure Restore', 'Reason', and 'Summary'. The main area has two radio buttons: 'Restore to the original location' (unselected) and 'Restore to a new location, or with different settings' (selected). The selected option has a description: 'Customize the restored VM location, and change its settings. The wizard will automatically populate all controls with the original VM settings as the defaults.' Below this is a link 'Pick proxy to use'. At the bottom, there's a checkbox for 'Quick rollback (restore changed blocks only)' with a description: 'Allows for quick VM recovery in case of guest OS software problem, or user error. Do not use this option when recovering from disaster caused by hardware or storage issue, or power loss.' At the bottom right are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

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 networks 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.

You can instruct Veeam Backup & Replication to scan machine data with YARA rules before restoring the machine to the production environment.

For details on secure restore settings for this operation, see the [Specify Secure Restore Settings](#) section in the Veeam Backup & Replication User Guide.

The screenshot shows the 'Entire VM Restore' wizard window. The left sidebar contains a list of steps: Virtual Machines, Restore Mode, Host, Resource Pool, Datastore, Folder, Network, Secure Restore (highlighted), Reason, and Summary. The main area is titled 'Secure Restore' and includes a description: 'Scan the selected backup for malware, such as computer viruses or ransomware, prior to performing the restore. This requires a compatible antivirus installed on the mount server specified for the corresponding backup repository.' Below this, the 'Content scan' section has two checked options: 'Scan restore point with your existing antivirus software' (with a 'Change...' link) and 'Scan the restore point with the following YARA rule:'. A dropdown menu for 'Select a YARA rule to use' is shown with the text 'Copy YARA rules location to clipboard'. Under 'Scan options: If malware is found', there are three radio buttons: 'Proceed with recovery but disable network adapters' (selected), 'Abort VM recovery', and 'Continue scanning all remaining files after the first occurrence' (unchecked). At the bottom right are buttons for '< Previous', 'Next >', 'Finish', and 'Cancel'.

8. At the **Reason** step of the wizard, specify the reason for restoring the VM.

The screenshot shows the 'Entire VM Restore' wizard window at the 'Reason' step. The left sidebar is the same as the previous step, but 'Reason' is now highlighted. The main area is titled 'Reason' and includes the instruction: 'Type in the reason for performing this restore operation. This information will be logged in the restore sessions history for later reference.' Below this, the 'Restore reason:' label is followed by a large text area containing the text 'Restoring a failed server'. At the bottom left, there is a checkbox labeled 'Do not show me this page again' which is unchecked. At the bottom right are buttons for '< Previous', 'Next >', 'Finish', and 'Cancel'.

- At the **Summary** step of the wizard, select the **Power on target VM after restoring** check box if necessary.
- 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 of 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:

- Open the **Home** view.
- 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**.

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

Virtual Machine Files Restore

Virtual Machine

Restore point

Destination

Reason

Summary

Restore point

Select the restore point to restore VM from.

VM name: **crm01**Original host: **vcenter01.tech.local**

VM size: **20.0 GB**

Available restore points:

Created	Type	Backup
 less than a day ago (10:09 PM Sunday 10/26/20...	Full	Backup Job 1

< Previous

Next >

Finish

Cancel

- At the **Destination** step of the wizard, select the server to which you want to restore the VM files.
- 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.

The screenshot shows the 'Virtual Machine Files Restore' wizard in the 'Destination' step. The left sidebar contains a vertical list of steps: 'Virtual Machine', 'Restore point', 'Destination' (highlighted in green), 'Reason', and 'Summary'. The main area is titled 'Destination' and contains the following fields and controls:

- Server:** A dropdown menu showing 'prgtwex01.tech.local' with a 'Details' link to its right.
- Path to folder:** A text field showing 'C:\backup\restored' with a 'Browse...' link to its right.
- VM files to restore:** A table with two columns: 'Name' and 'Size'. It lists four files, each with a checked checkbox in the first column.

	Name	Size	
☒	crm01.vmx	2.60 KB	☒ Select All
☒	crm01.nvram	8.48 KB	☒ Select All
☒	crm01_1.vmdk	529 B	☒ Select All
☒	crm01_1-flat.vmdk	20.0 GB	☒ Select All

At the bottom right of the main area are two links: 'Select All' (with a green checkmark icon) and 'Clear All' (with a red X icon). At the very bottom of the wizard are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

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**.

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

The screenshot shows the 'Virtual Disk Restore' wizard window. On the left is a sidebar with navigation links: 'Virtual Machine', 'Restore point' (highlighted with a green bar), 'Disk Mapping', 'Secure Restore', 'Reason', and 'Summary'. The main area is titled 'Restore point' and contains the instruction 'Select the desired restore point.' Below this, it displays 'VM name: **crm01**' and 'Original host: **vcenter01.tech.local**'. Further down, it shows 'VM size: **20.0 GB**'. A section titled 'Available restore points:' contains a table with the following data:

Created	Type	Backup
 less than a day ago (10:09 PM Sunday 10/26/20...	Full	Backup Job 1

At the bottom right of the window are four buttons: '< Previous', 'Next >' (highlighted with a green border), 'Finish', and 'Cancel'.

- At the **Disk Mapping** step of the wizard, click **Browse** and select the VM to which the restored hard disks must be attached.
- Select check boxes next to the virtual hard disks that you want to restore.
- 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.
- 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.
 - If you want to replace an existing virtual disk, select an occupied virtual node.
 - 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.

Virtual Machine

Restore point

Disk Mapping

Secure Restore

Reason

Summary

Virtual Disk Restore

✕

Disk Mapping

Map virtual disks from backup to virtual device nodes on target VM.

Virtual machine name:

crm01

Choose...

Disk mapping:

Virtual disk	Virtual Device Node	Datastore
☒ crm01_1.vmdk	SCSI 0:1	prgbwex03-ds01

Change...

Restored disk type:

Same as source

☒ Quick rollback (restore changed blocks only)

Allows for quick VM recovery in case of guest OS software problem, or user error. Do not use this option when recovering from disaster caused by hardware or storage issue, or power loss.

Pick proxy to use...

< Previous

Next >

Finish

Cancel

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.

You can instruct Veeam Backup & Replication to scan machine data with YARA rules before restoring the machine to the production environment.

For details on secure restore settings for this operation, see the [Specify Secure Restore Settings](#) section in the Veeam Backup & Replication User Guide.

The screenshot shows the 'Virtual Disk Restore' wizard window. On the left is a sidebar with steps: Virtual Machine, Restore point, Disk Mapping, Secure Restore (highlighted in green), Reason, and Summary. The main area is titled 'Secure Restore' and contains the following content:

- Instruction: 'Scan the selected backup for malware prior to performing the restore.'
- Section: 'Content scan'
- Checkboxes:
 - ☒ Scan the backup content with your antivirus software prior to performing a recovery [Change...](#)
 - ☒ Scan the backup with the following YARA rule:
 - Dropdown menu: 'Select a YARA rule to use'
 - [Copy YARA rules location to clipboard](#)
- Section: 'Scan options'
- Text: 'The disk you are about to restore will be scanned by antivirus software installed on the mount server to prevent the risk of bringing malware into your environment.'
- Text: 'If malware is detected:'
- Radio buttons:
 - ☒ Proceed with recovery but do not attach infected disks to the target VM
 - ☐ Abort disk recovery
- Checkbox:
 - ☐ Scan the entire image
 - Text: 'Continue scanning all remaining files after the first occurrence.'

At the bottom right are four buttons: '< Previous', 'Next >' (highlighted with a green border), 'Finish', and 'Cancel'.

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 Restore](#) 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.

File Level Restore

Restore point

Select the restore point to restore guest OS files from.

VM name: srv12 Original host: vcenter01.tech.local
 VM size: 20.0 GB Mount server: Automatic selection (Windows)

Available restore points:

Created	Type	Backup
less than a day ago (10:09 PM Sunday 10/26/20...	Full	Backup Job 1

< Previous **Next >** Browse Cancel

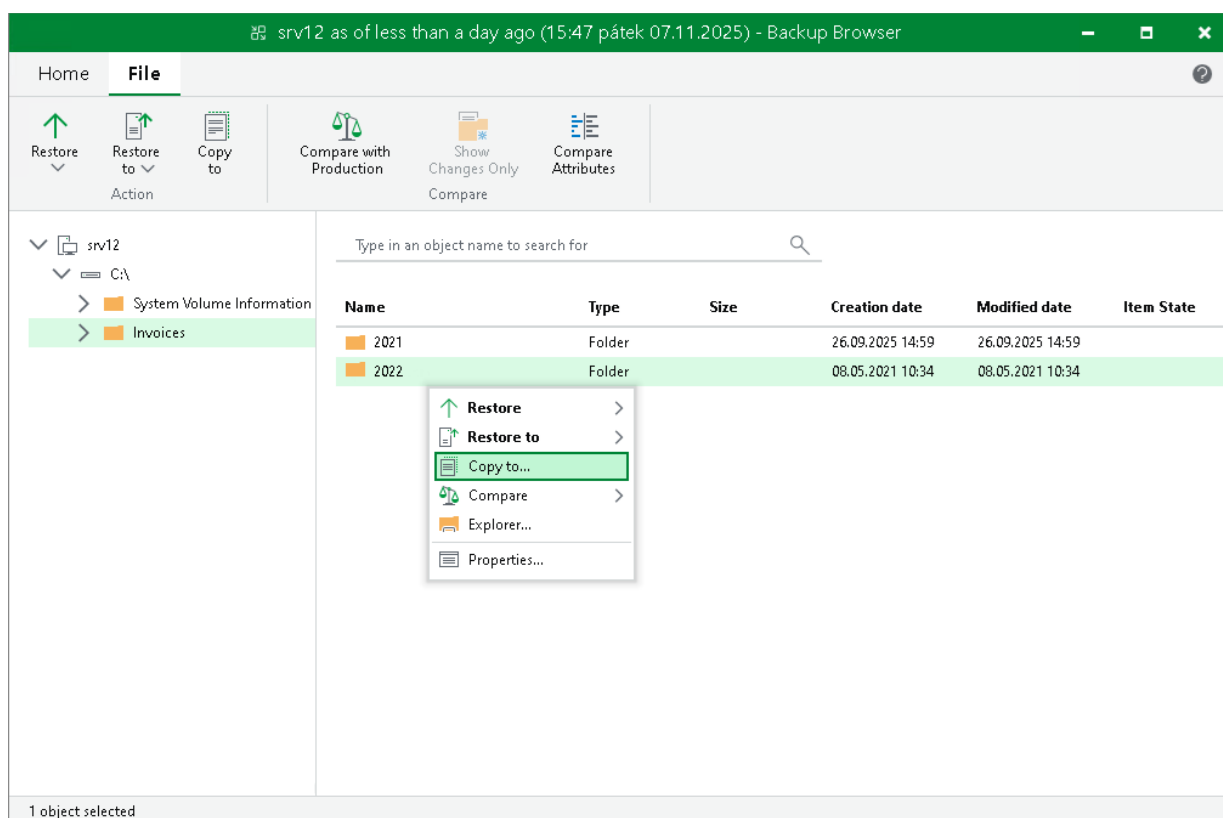
4. At the **Reason** step of the wizard, specify the reason for future reference.
5. Click **Next** and then click **Browse** to finish working with the **File Level Restore** wizard. Veeam Backup & Replication will mount VM disks from the backup to the backup server file system, and display the Veeam 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.
 - 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.
 - 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**.

- 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.
- 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

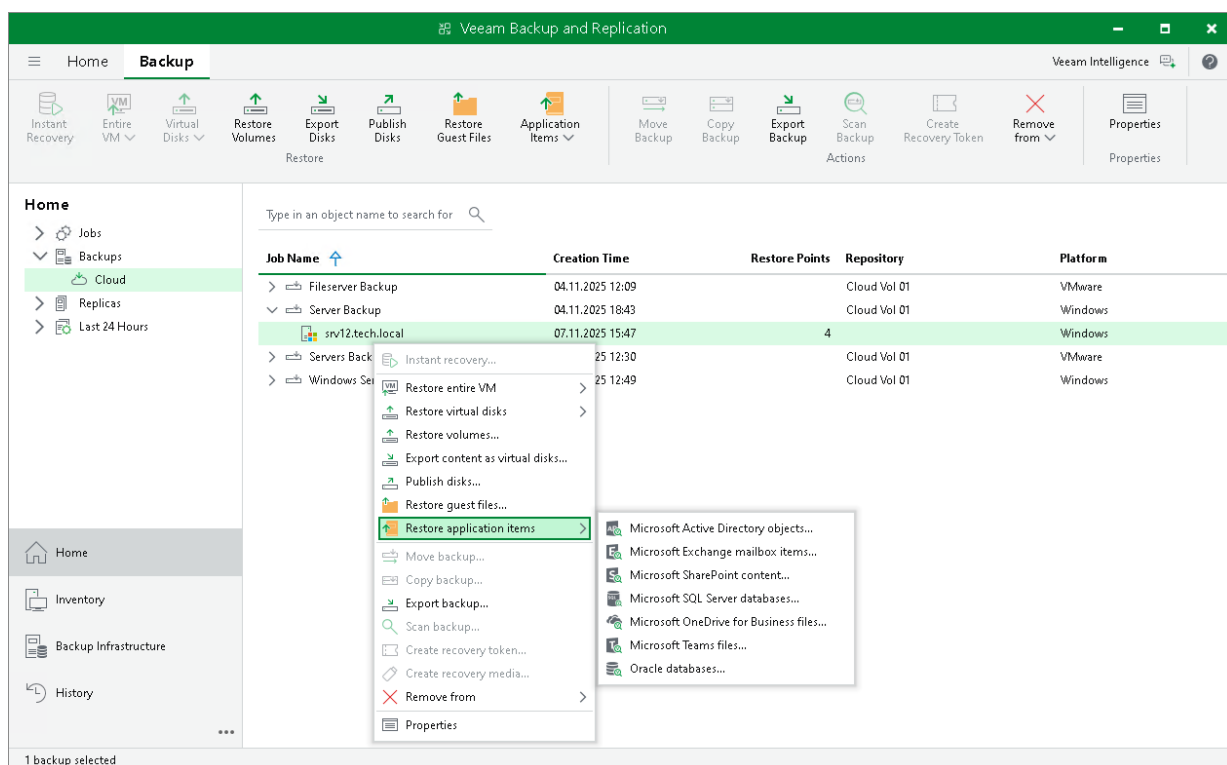
- Microsoft Exchange
- Microsoft SharePoint
- Microsoft SQL Server
- Microsoft OneDrive for Business
- Microsoft Teams
- Oracle
- PostgreSQL

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 Overview](#) section in the Veeam Backup & Replication 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 Backup & Replication User 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.

Volume Restore

Backup

Restore point

Disk Mapping

Secure Restore

Reason

Summary

Restore point

Select the desired restore point

Computer name: **srv12.tech.local**

Data size: **57,2 GB**

Available restore points:

Created	Type	Backup
 less than a day ago (15:47 pátek 07.11.2025)	Increment	Server Backup
 1 day ago (2:05 čtvrtek 06.11.2025)	Increment	Server Backup
 2 days ago (2:04 středa 05.11.2025)	Increment	Server Backup
 2 days ago (18:44 úterý 04.11.2025)	Full	Server Backup

< Previous

Next >

Finish

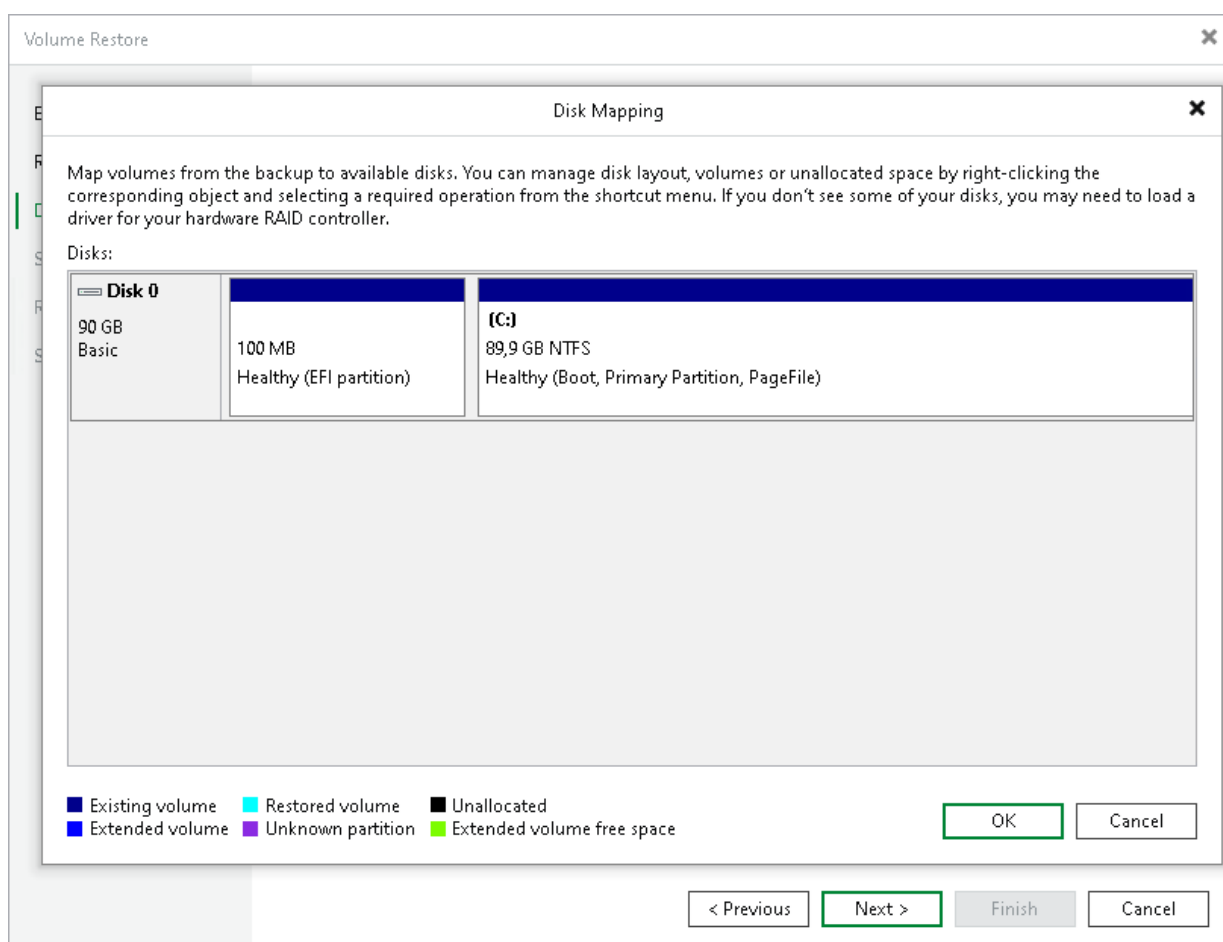
Cancel

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 Backup & Replication User Guide.

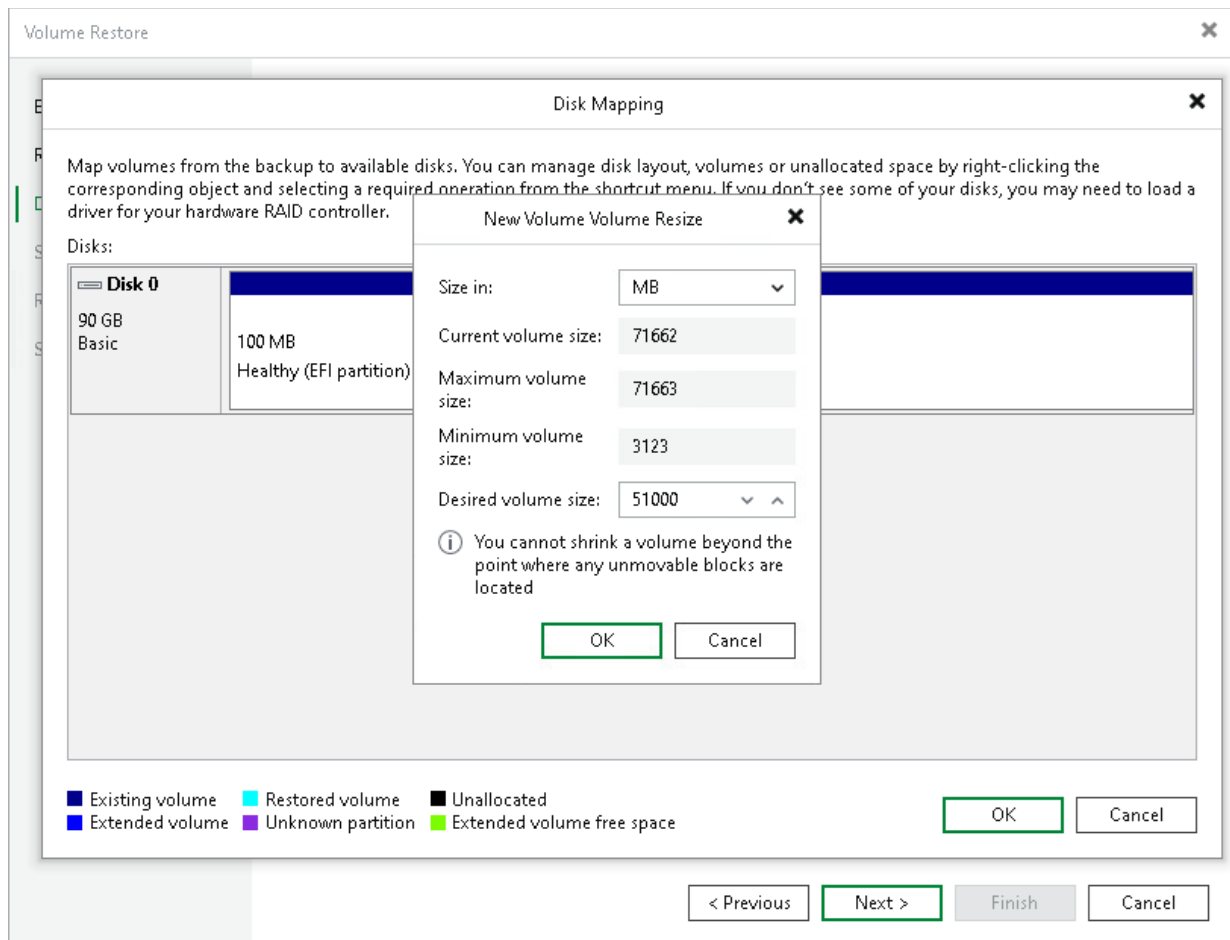
- b. In the **Disk mapping** section, select check boxes next to volumes that you want to restore from the backup. By default, Veeam Backup & Replication restores volumes to their initial location and maps the restored volumes automatically. If the initial location is unavailable, Veeam Backup & Replication 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.
 - To use antivirus software as a scan engine, select the **Scan the restore point with an antivirus engine** check box. For more information on antivirus scan, see [Secure Restore](#).
 - You can instruct Veeam Backup & Replication to scan machine data with YARA rules before restoring the machine to the production environment. For a YARA rule to appear in the drop-down list, it must be placed in the `YaraRules` folder in the Veeam Backup & Replication product folder. The default path is `C:\Program Files\Veeam\Backup and Replication\Backup\YaraRules`. For more information on how to create a YARA rule, see [YARA Documentation](#).

TIP

To copy the path to the folder with YARA rules, click **Copy YARA rules location to clipboard**.

- Select the **Continue scanning all remaining files after the first occurrence** (Scan the entire image – for version Veeam Backup & Replication 12.1 (build 12.1.0.2131) or later) check box if you want to continue the virtual disk scan after a virus threat is detected. For information on how to view results of the malware scan, see the [Viewing Antivirus Scan Results](#) section in the Veeam Backup & Replication User Guide.

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 content as virtual disks**.
3. At the **Restore Point** step of the wizard, select the necessary restore point.

Export Disks

Backup

Restore point

Disks

Target

Secure Restore

Reason

Summary

Restore point

Select the restore point to export disks from.

Computer name: **srv12.tech.local**

Data size: **57,9 GB**

Available restore points:

Created	Type
 less than a day ago (2:03 sobota 08.11.2025)	Full
 less than a day ago (15:47 pátek 07.11.2025)	Increment
 2 days ago (2:05 čtvrtek 06.11.2025)	Increment
 3 days ago (2:04 středa 05.11.2025)	Increment
 3 days ago (18:44 úterý 04.11.2025)	Full

< Previous

Next >

Finish

Cancel

4. At the **Disks** step of the wizard, select check boxes next to the disks that you want to export.

Export Disks

Backup

Restore point

Disks

Target

Secure Restore

Reason

Summary

Select one or more disks to export.

Disk name	Size
☒ Volume 1	90 GB

☒ Select All

☐ Clear All

< Previous Next > Finish Cancel

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:
- 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.
 - In the **Path to folder** field, specify a folder on the server or datastore where the virtual disks must be placed.
 - 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).
 - [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.

Export Disks

Backup

Restore point

Disks

Target

Secure Restore

Reason

Summary

Target

Specify the destination server and folder, and a virtual disk format to export disk content to.

Server:

prgtwesx01.tech.local

Path to folder:

[prgtwesx01-ds01] ABC Company

Browse...

Export format:

☒ VMDK

This virtual disk type is used by VMware products such as VMware Workstation or VMware vSphere. Maximum VMDK disk size is 62 TB.

Pick proxy to use...

☐ VHD

This virtual disk type is used by Microsoft products such as Microsoft Hyper-V or Microsoft Azure. Maximum VHD disk size is 2 TB.

☐ VHDX

This virtual disk type is used by more recent versions of Microsoft products such as Microsoft Hyper-V. Maximum VHDX disk size is 64 TB.

Disk type:

Thick (lazy zeroed)

< Previous

Next >

Finish

Cancel

498 | Veeam Cloud Connect | Administrator Guide | 13.1.0.411

- 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.

The screenshot shows the 'Export Disks' wizard window with the 'Secure Restore' step selected in the left sidebar. The main area is titled 'Secure Restore' and contains the following elements:

- A description: 'Scan the selected backup for malware prior to performing the restore.'
- A section header 'Content scan'.
- Two checked checkboxes:
 - 'Scan the backup content with Veeam Threat Hunter prior to performing a recovery'
 - 'Scan the backup with the following YARA rule:' followed by a dropdown menu labeled 'Select a YARA rule to use'.
- A link: 'Copy YARA rules location to clipboard'
- A section header 'Scan options'.
- A paragraph: 'The disk you are about to restore will be scanned by antivirus software installed on the mount server to prevent the risk of bringing malware into your environment.'
- A label: 'If malware is detected:'
- Three options:
 - 'Proceed with recovery' (selected with a radio button)
 - 'Abort disk recovery' (radio button)
 - 'Scan the entire image' (checkbox), with a sub-note: 'Continue scanning all remaining files after the first occurrence.'
- Navigation buttons at the bottom: '< Previous', 'Next >' (highlighted with a green border), 'Finish', and 'Cancel'.

- At the **Reason** step of the wizard, specify the reason for future reference.
- 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 [Recovering Guest OS Files Using Console](#) section in the Veeam Backup & Replication User Guide.

To restore Microsoft Windows guest OS files from a Veeam Agent backup:

- Open the **Home** view.

2. Click the **Backups > Cloud** node in the inventory pane and do either of the following:
 - 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**.
 - 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.

File Level Restore

Restore point

Reason

Summary

Restore point

Select the restore point to restore guest OS files from.

Computer name: srv12.tech.local

Mount server: Automatic selection (Windows)

Data size: 57,9 GB

Available restore points:

Created	Type	Backup
 less than a day ago (2:03 sobota 08.11.2025)	Full	Server Backup
 less than a day ago (15:47 pátek 07.11.2025)	Increment	Server Backup
 2 days ago (2:05 čtvrtek 06.11.2025)	Increment	Server Backup
 3 days ago (2:04 středa 05.11.2025)	Increment	Server Backup
 3 days ago (18:44 úterý 04.11.2025)	Full	Server Backup

< Previous

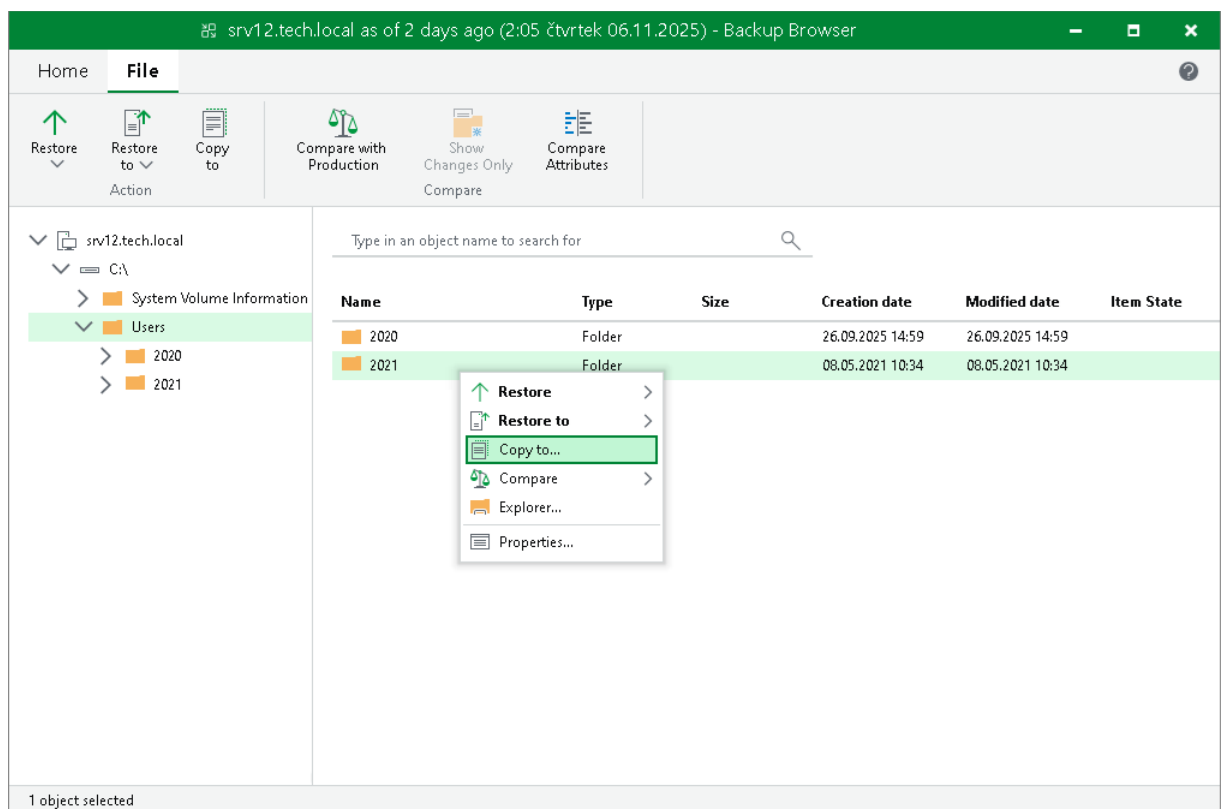
Next >

Browse

Cancel

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:
 - 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.

- 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.
- 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 Recovery](#) 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.

Publishing Disks

You can publish disks to get the backup contents of one or more disks instead of all disks in a backup.

NOTE

This section describes only basic steps that you must take to publish disks. To get a detailed description of all settings of the disk publishing process, see the [Publishing Disks](#) section in the Veeam Backup & Replication User Guide.

In Veeam Cloud Connect, disk publishing is supported for the following types of backups in cloud repositories.

- Backups of VMware vSphere 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

This operation is not supported for VM replicas and backups of Linux, Mac or Unix machines.

In Veeam Cloud Connect, disk publishing operation for backups in the cloud repository is similar to disk publishing within regular backup repositories. To learn more about disk publishing in the regular Veeam Backup & Replication environment, see the [Disk Publishing \(Data Integration API\)](#) section in the Veeam Backup & Replication User Guide.

To publish disks, complete the following steps:

1. Open the **Home** view.
2. Select the **Backups** node in the inventory pane. Expand the necessary backup in the working area, select a backup whose disks you want to publish and click **Publish Disks** on the ribbon.

Alternatively, you can right-click the backup and select **Publish disks**.

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

Publish Disks

Machine

Restore point

Disks

Target

Reason

Summary

Restore point

Select a restore point to publish disks from.

VM name: **crm01**Original host: **vcenter01.tech.local**

VM size: **20.0 GB**

Available restore points:

Created	Type	Backup
 less than a day ago (10:09 PM Sunday 10/26/20...	Full	Backup Job 1

< Previous

Next >

Finish

Cancel

4. At the **Disks** step of the wizard, select check boxes next to the disks that you want to publish.
 - For VM backups, you can see **Disk name** and **Size**.

- For Veeam Agent backups, **Volumes** are displayed as well as **Disk name** and **Size**.

Publish Disks

Machine

Restore point

Disks

Target

Reason

Summary

Disks

Select one or more disks to publish.

Disk name	Size	Volumes
☒ crm01_1-flat.vmdk	20.0 GB	

☒ Select All
 ☐ Clear All

< Previous

Next >

Finish

Cancel

- At the **Target** step of the wizard, select a server to which the disk content will be published. You can select one of the following types of servers:
 - A server added to the backup infrastructure.
 - A temporary server. In this case, select *Specify a different host* from the drop-down list. In the **Target Server** window, specify a server name or IP and credentials to the server.

- The original server if you publish disks from a backup created by Veeam Agent for Microsoft Windows. In this case, select *Original server* from the drop-down list.

If prompted, specify credentials of the user account to connect to.

The screenshot shows the 'Publish Disks' wizard window with the 'Target' step selected in the left sidebar. The main area is titled 'Target' and contains the instruction 'Select a target server to mount disks to.' Below this is a 'Target server:' label and a dropdown menu showing 'srvt44.tech.local (Backup server)' with a downward arrow. To the right of the dropdown is an 'Add...' link. At the bottom of the window are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'. The 'Next >' button is highlighted with a green border.

6. At the **Reason** step of the wizard, enter a reason for publishing disks for future reference.

TIP

If you do not want to show this step of the wizard, select the **Do not show me this page again** check box. If you further will want to return this page, follow the instructions described in [this Veeam KB article](#).

7. At the **Summary** step of the wizard, review the configured settings and click **Finish**.

What You Do Next

The disk content will become available in the `C:\VeeamFLR\` folder on the target server. For disks of Microsoft Windows machines, the disk content is available in the read-only state. You can perform the necessary operations with the published disk data, for example, find specific documents, copy files or perform antivirus scan of the backed-up data.

When you are finished, you can stop the disk publish session.

For details, see the [Managing Published Disks](#) section in the Veeam Backup & Replication Guide.

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.

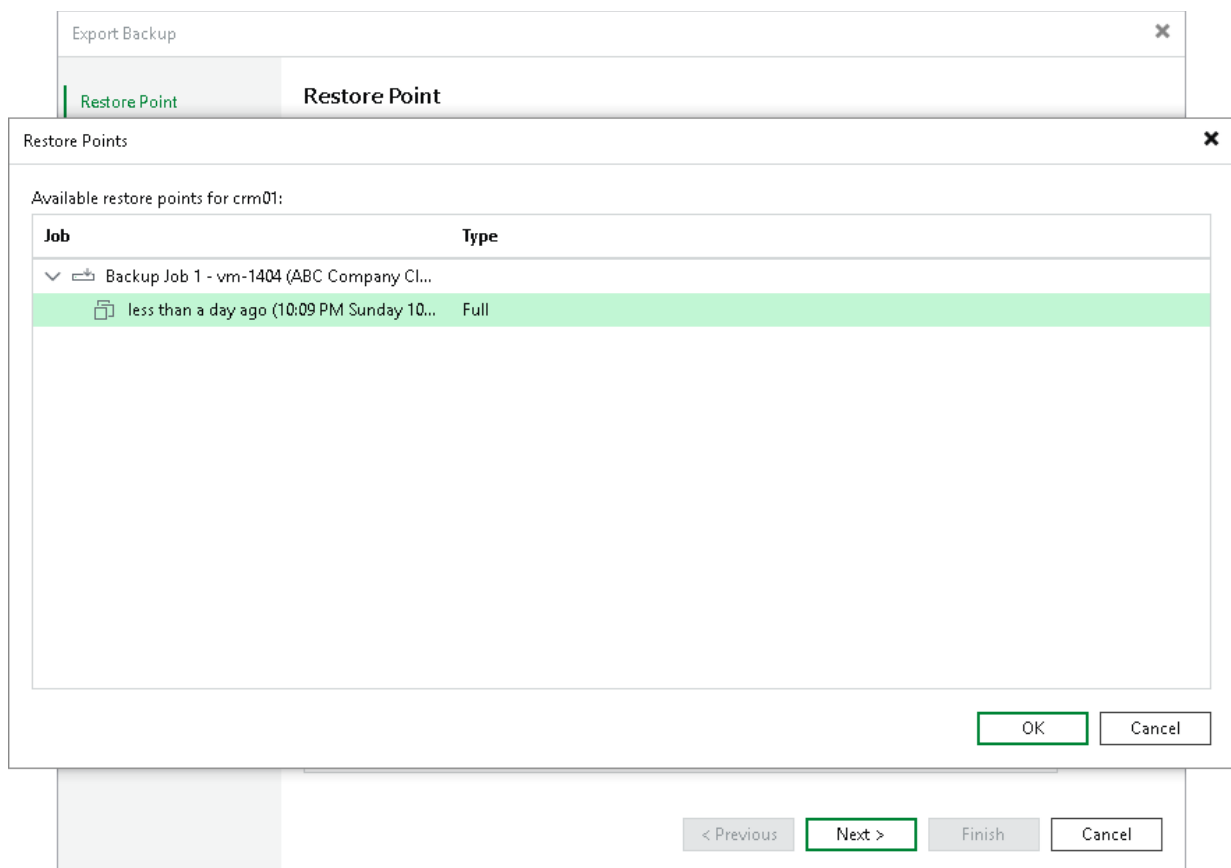
After you export a restore point to a full backup, the resulting full backup becomes available in the tenant Veeam backup console. The tenant can perform the same operations with the standalone full backup as with a regular backup created in a cloud repository.

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**.

Performing Instant Recovery of Workloads to Nutanix AHV

You can immediately restore virtual or physical machines into a Nutanix AHV cluster by running it directly from a compressed and deduplicated backup file.

NOTE

This section describes only basic steps that you must take to perform instant recovery to Nutanix AHV. To get a detailed description of all prerequisites and settings of the instant recovery process, see the [Performing Instant Recovery of Workloads to Nutanix AHV](#) 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 **Instant recovery**.
3. At the **Machines** step of the wizard, select the necessary restore point in the list, click **Point** on the right and select the necessary restore point.
4. At the **Restore Mode** step of the wizard, choose whether you want to restore the selected VM to the original or to a custom location.
5. At the **Cluster** step of the wizard, choose the cluster to which the recovered VM will belong. In the Prism Central deployment, you can also choose whether you want the recovered VM to be assigned the same categories as the original VM.
6. At the **Storage Container** step of the wizard, choose the storage container where virtual disks of the recovered VM will be stored.
7. At the **Name** step of the wizard, you can specify a new name for the recovered VM.
8. At the **Network** step of the wizard, choose a network to which the recovered VM will be connected. If you do not want to connect the VM to any virtual network, select the VM and click **Disconnect**.
9. At the **Reason** step of the wizard, specify the reason for restoring the VM.
10. At the **Summary** step of the wizard, select the **Power on target VM after restoring** check box if necessary.
11. Click **Finish**.

After the VM has been recovered, you can choose whether you want to migrate the VM to the production environment or cancel the recovery operation. When migrating VMs, Veeam Plug-in for Nutanix AHV transfers VM disk data to the production storage that you have selected as a destination for the recovered VM.

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:

Backup Properties Backup Job 1 (ABC Company Cloud Repository)

Type in an object name to search for

Copy path Malware

Show issues only

Name	Original Size
crm01	20.0 GB

Total size: 20.0 GB

File Name	Data Size	Backup Size	Data Reduction	Date
vm-1404.80c8D2025-10-26T214818...	20.0 GB	1.58 MB	3.8 x	10/2

Backup size: 1.58 MB Restore points: 1

Close

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:

Agent Backup Properties Server Backup - srv12.tech.local

Object:
srv12.tech.local

Repository:
Cloud Vol 01

Owner:
VeeamAgentUser47a42542-1b8f-2b99-832f-effdc8

Folder:
srv12.tech.local

Files:

Name	Data Size	Backup Size	Date
Server Backup - srv12.tech.localD2025-11-08T020...	90,0 GB	2,69 MB	08.11.2025 2:03:11
Server Backup - srv12.tech.localD2025-11-07T154...	4,03 MB	2,08 MB	07.11.2025 15:47:19
Server Backup - srv12.tech.localD2025-11-06T020...	3,03 MB	2,00 MB	06.11.2025 2:05:09
Server Backup - srv12.tech.localD2025-11-05T020...	4,03 MB	2,00 MB	05.11.2025 2:04:40
Server Backup - srv12.tech.localD2025-11-04T184...	90,0 GB	2,77 MB	04.11.2025 18:44:27

Backup size: 11,5 MB

Malware

OK

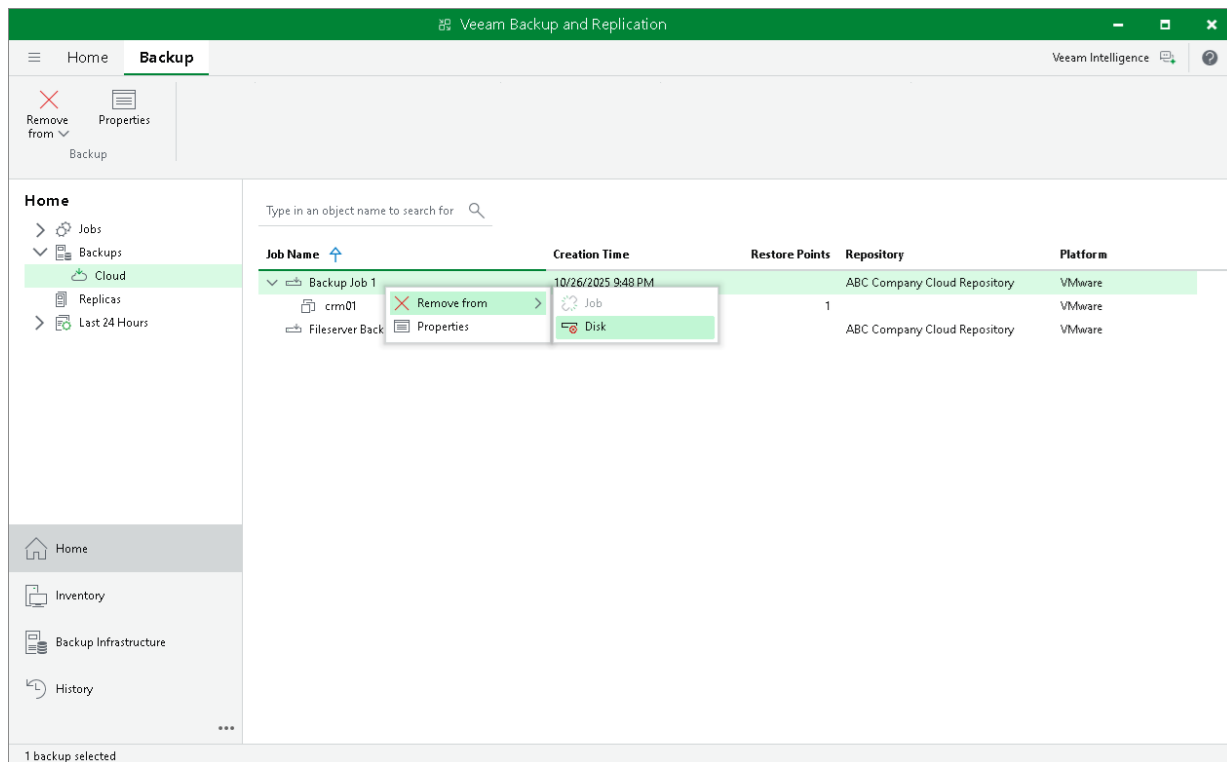
Deleting from Disk

You can remove backups from the disk 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 this 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), click **Remove from** and select **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.

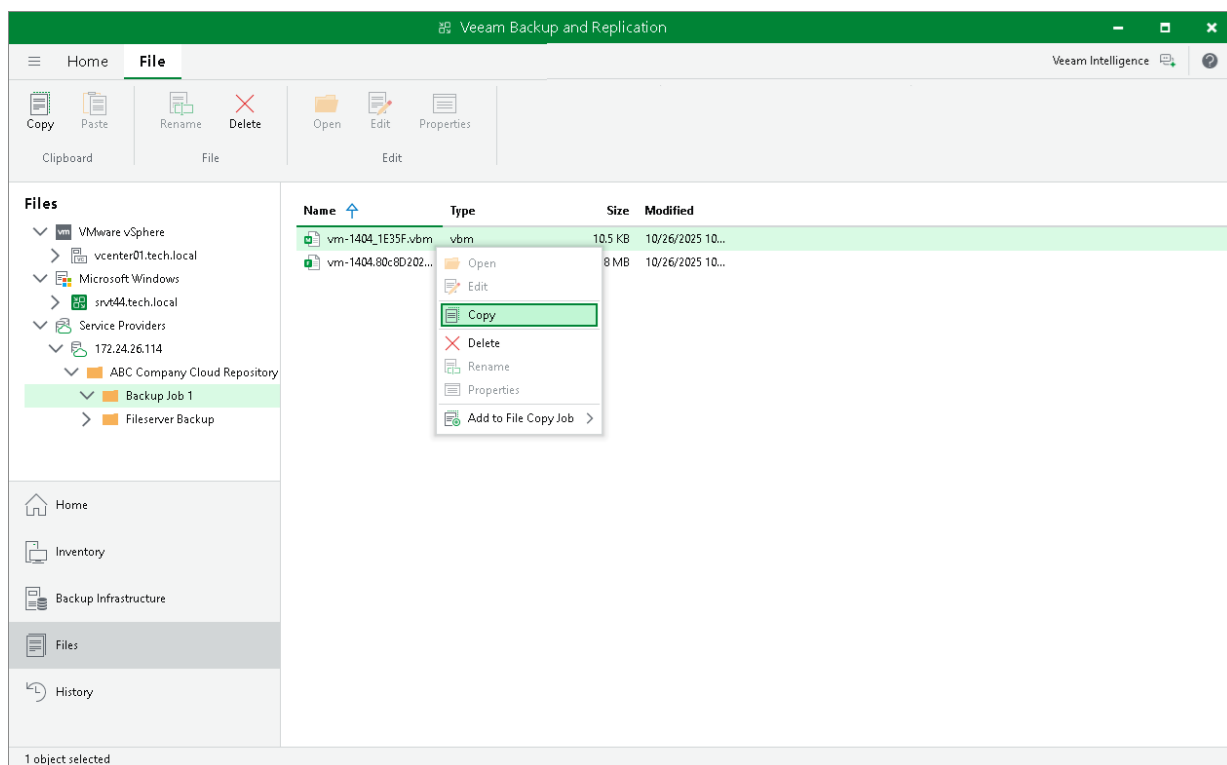
To copy backup files:

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 [Scale-Out Backup Repositories Used as Cloud Repositories](#).



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 CDP policy for VMware vSphere](#)
- [Create a universal CDP policy](#)
- Perform failover:
 - [Full site failover](#)
 - [Partial site failover](#)
- [Perform failback](#)
- Perform data restore:
 - [VM guest OS files restore](#) (Microsoft Windows file system only. Multi-OS restore is not supported.)

This operation is supported for both snapshot-based replicas and CDP replicas. In previous versions of Veeam Backup & Replication, this operation was supported only for snapshot-based replicas.
 - [Application items restore](#)

This operation is supported for snapshot-based replicas only.

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.

The screenshot shows the Veeam Backup & Replication console. The top bar is green with the Veeam logo and title. Below it is a navigation bar with icons for Backup Job, Replication Job, CDP Policy, Backup Copy, Copy Job, SureBackup Job, Restore, Failover Plan, Import Backup, Export Backup, and Security & Compliance. The left sidebar shows a tree view with 'Replicas' selected. The main area displays a table of replicas.

Name	Job Name	T...	S...	Creation Time	R...	Original Loc...	Replica Location	Platform
filesrv03	XYZ Replication to Cloud	Cloud	Ready	11/18/2025 10:11...	2	vcenter01.tech.lo...	srv121.tech.local\CDP...	VMware
filesrv04	XYZ Replication to Cloud	Cloud	Ready	11/18/2025 10:11...	2	vcenter01.tech.lo...	srv121.tech.local\CDP...	VMware
websrv03....	Universal CDP to Cloud	CDP	Ready	11/19/2025 8:05 AM	3	websrv03.tech.local	srv121.tech.local\CDP...	Server
websrv04....	Universal CDP to Cloud	CDP	Ready	11/19/2025 8:05 AM	3	websrv04.tech.local	srv121.tech.local\CDP...	Server
winsrv22....	Universal CDP Policy	CDP	Ready	11/19/2025 8:00 AM	14	winsrv22.tech.local	vcenter01.tech.local\pr...	Server

At the bottom of the console, it says '5 replicas'.

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.
It is recommended to create job names not longer than 50 characters.
3. If you want to use advanced settings for the job:
 - Select the **Replica seeding** check box to enable the **Seeding** step in the wizard.
 - 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.

- 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.

New Replication Job

Name

Virtual Machines

Destination

Network

Job Settings

Data Transfer

Seeding

Guest Processing

Schedule

Summary

Name

Specify the name and description for this policy, and provide information on your DR site.

Name:

ABC Company Servers Replication

Description:

Job for ABC Company servers replication to the cloud

Show advanced controls:

☒ Replica seeding (for low bandwidth DR sites)

☒ Network remapping (for DR sites with different virtual networks)

☐ Replica re-IP (for DR sites with different IP addressing scheme)

☐ High priority

Backup infrastructure resources are offered to high priority jobs first. Use this option for jobs sensitive to the start time, or jobs with strict RPO requirements.

< Previous

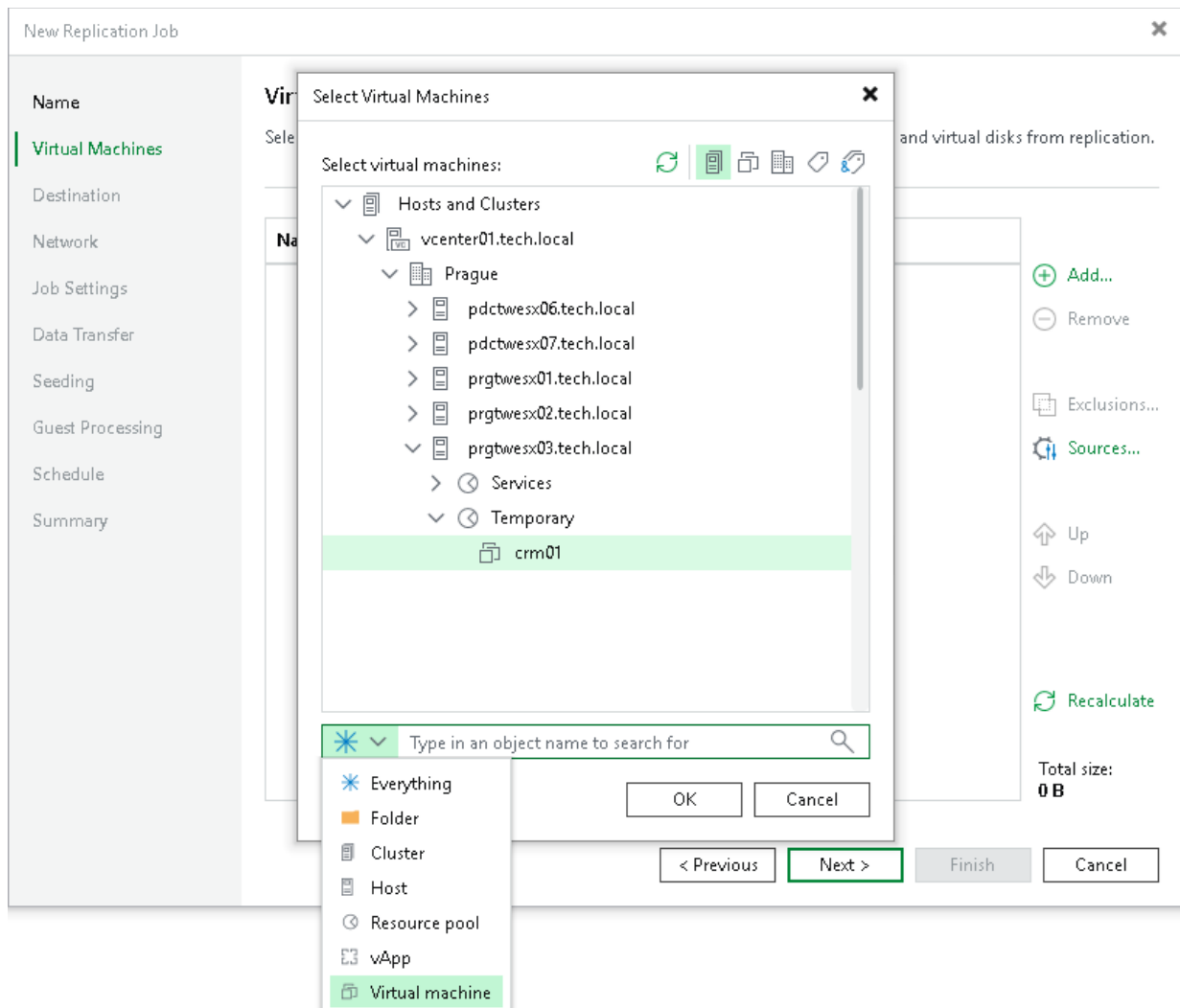
Next >

Finish

Cancel

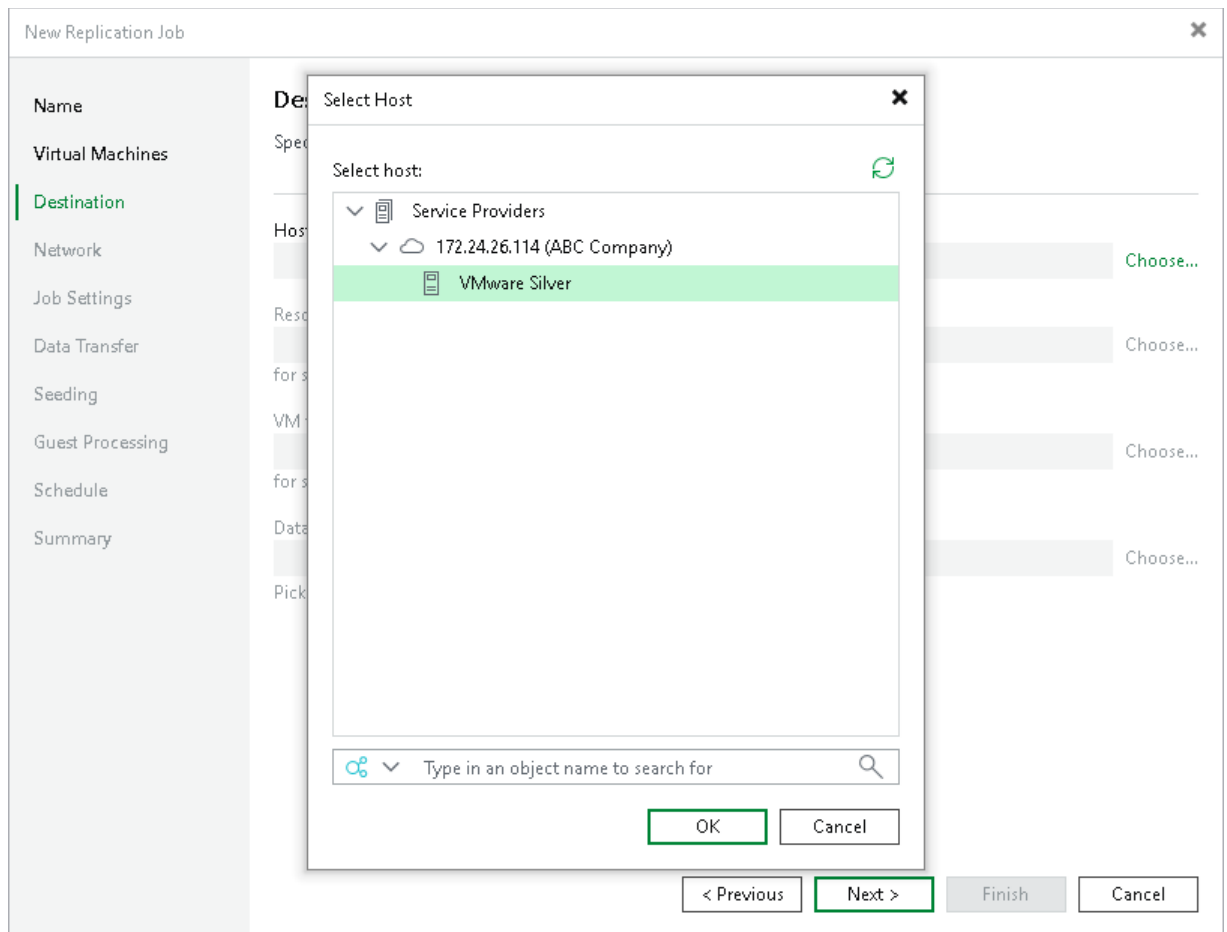
515 | Veeam Cloud Connect | Administrator Guide | 13.1.0.411

- 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.



- If you want to specify the source from which VM data must be read, click **Sources** and select one of the following options:
 - From production storage.** In this case, Veeam Backup & Replication will retrieve VM data from the production storage connected to the source virtualization host.
 - 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.
- 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.
- 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.

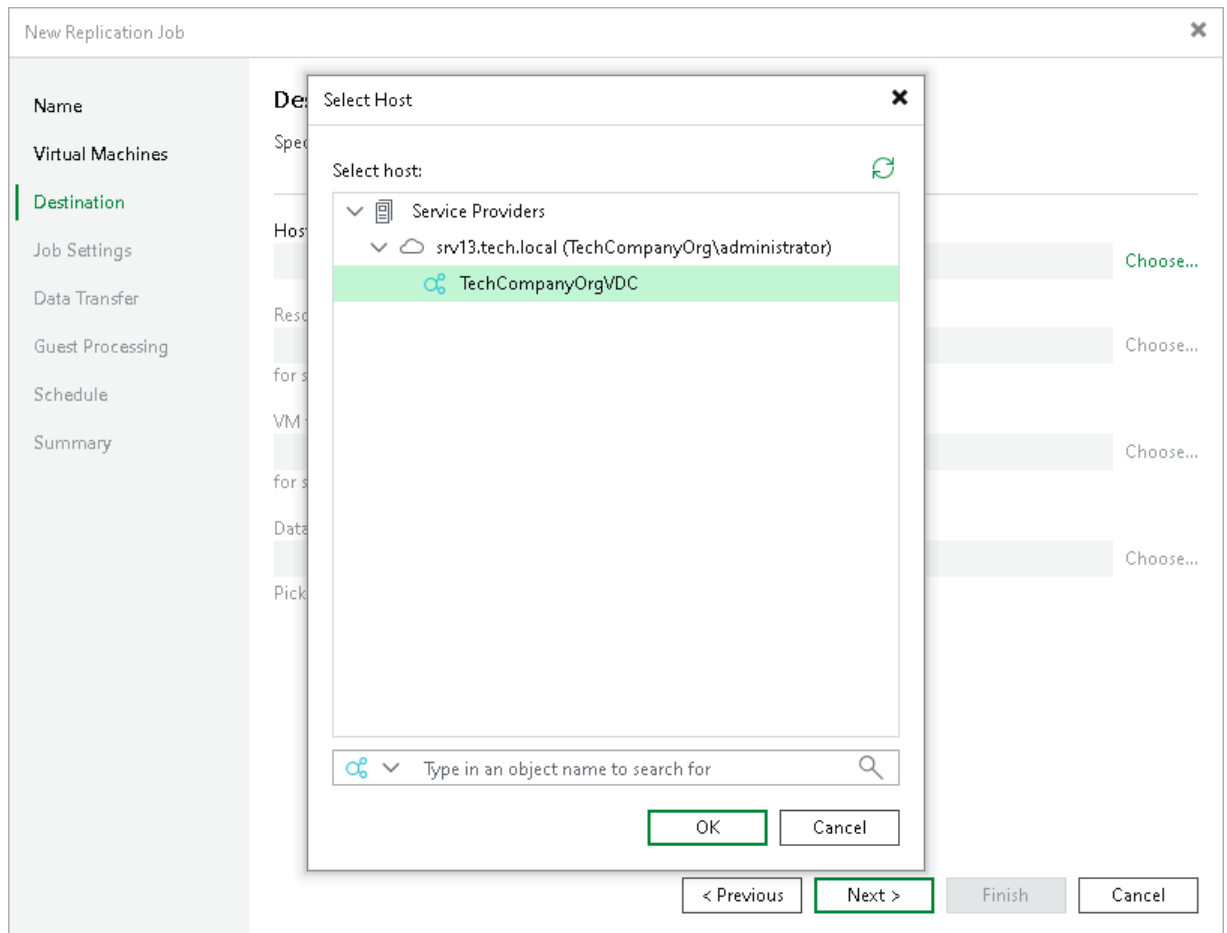
8. At the **Destination** step of the wizard, in the **Host or cluster** section, click **Choose** and select **Cloud host**. Then select the cloud host allocated to you by the SP:
- If the SP allocated to you replication resources on a VMware vSphere or Microsoft Hyper-V host, select the cloud host provided to you through a hardware plan.



- 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:
- [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.

New Replication Job

Name

Virtual Machines

Destination

Network

Job Settings

Data Transfer

Seeding

Guest Processing

Schedule

Summary

Destination

Specify where replicas should be created in the DR site.

Host or cluster:
VMware Silver

Datastore:
Cloud Replicas [300 GB free]

for selected virtual disks

< Previous

Next >

Finish

Cancel

- [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.

The screenshot shows the 'New Replication Job' wizard with the 'Destination' step selected in the left-hand navigation pane. The main area is titled 'Destination' and contains the instruction 'Specify where replicas should be created in the DR site.' Below this, there are two sections: 'Host or cluster:' and 'Path:'. The 'Host or cluster:' section has a dropdown menu showing 'Hyper-V Bronze' and a 'Choose...' link. The 'Path:' section has a dropdown menu showing 'Cloud Replicas [300 GB free]' and a 'Choose...' link. At the bottom right, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

- [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.

The screenshot shows the 'New Replication Job' wizard with the 'Destination' step selected in the left-hand navigation pane. The main area is titled 'Destination' and contains the following fields:

- Organization VDC:** A dropdown menu showing 'TechCompanyOrgVDC' with a 'Choose...' link to its right.
- vApp:** A dropdown menu showing 'Cloud Connect 22 (Default)' with a 'Choose...' link to its right.
- Storage policy:** A dropdown menu showing '*(Any) [193 GB free]' with a 'Choose...' link to its right.

Below these fields, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

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

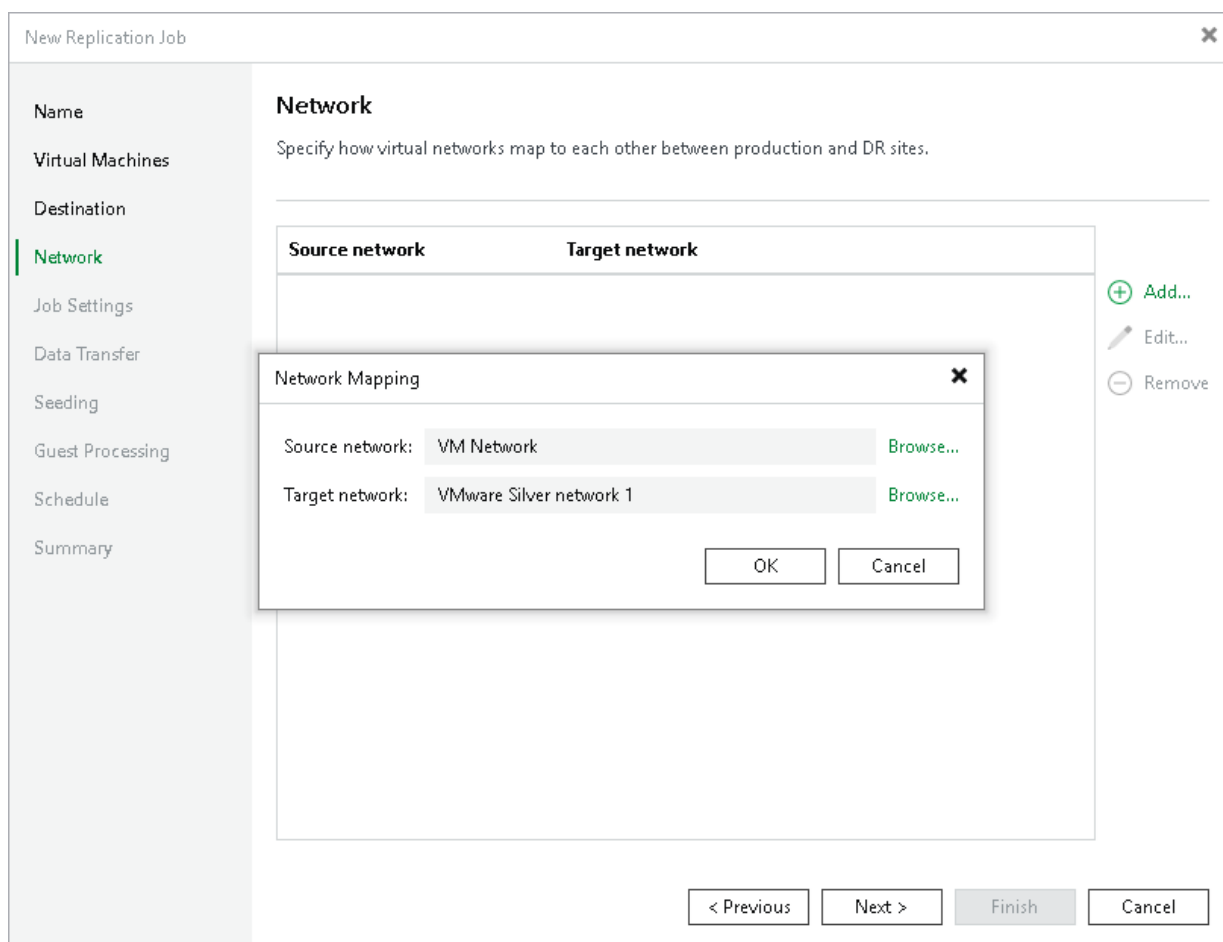
Because Veeam Cloud Connect Replication does not support automatic network mapping for non-Windows VMs, during the job performance, in the list of operations for such VMs included in the job, Veeam Backup & Replication will display a warning that no static IP addresses are detected for the VM. If in 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.



- 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.

New Replication Job

Job Settings

Specify backup repository located in the source site to host metadata in, replica suffix and retention policy, and customize advanced job settings if required.

Repository for replica metadata:

Default Backup Repository (Created by Veeam Backup)

35.9 GB free of 89.1 GB

Replica settings

Replica name suffix:

Restore points to keep:

Advanced job settings...

< Previous Next > Finish Cancel

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:
 - 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.

 - To transport VM data directly through one or more backup proxies to the cloud host, select **Direct**.

- 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.

The screenshot shows the 'New Replication Job' wizard with the 'Data Transfer' step selected in the left sidebar. The main area is titled 'Data Transfer' and contains the following content:

Data Transfer
Choose how VM data should be transferred to the target site.

When replicating between remote sites, we highly recommended that you deploy at least one backup proxy server locally in both sites to allow for direct access to storage.

Source proxy:
Automatic selection Choose...

Target proxy:
Service provider's proxy Choose...

☐ **Direct**
Best for local and off-site replication over fast links.

☒ **Through built-in WAN accelerators**
Best for off-site replication over slow links due to significant bandwidth savings.

Source WAN accelerator:
srv12 (ABC Company WAN Accelerator) ▼

Target WAN accelerator:
Service Provider's WAN Accelerator (Available) ▼

At the bottom right, there are four buttons: '< Previous' (disabled), 'Next >' (active/highlighted), 'Finish' (disabled), and 'Cancel'.

- At the **Seeding** step of the wizard, configure replica seeding and mapping for the replication job.
 - 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.

- 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.

New Replication Job

Name

Virtual Machines

Destination

Network

Job Settings

Data Transfer

Seeding

Guest Processing

Schedule

Summary

Seeding

Specify the backup repository with backup files of production VMs. The backup repository must be located in the DR site.

Initial seeding

☒ Get seed from the following backup repository:

Default Backup Repository (Created by Veeam Backup)

35.9 GB free of 89.1 GB

Replica mapping

☐ Map replica to existing VMs

Original VM	Replica VM	
crm01	no mapping	Edit... Remove Detect

If you already have replicas in the target site, replication job can reuse them. This way, only differences will be transferred over WAN by the first job run.

< Previous

Next >

Finish

Cancel

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](#).

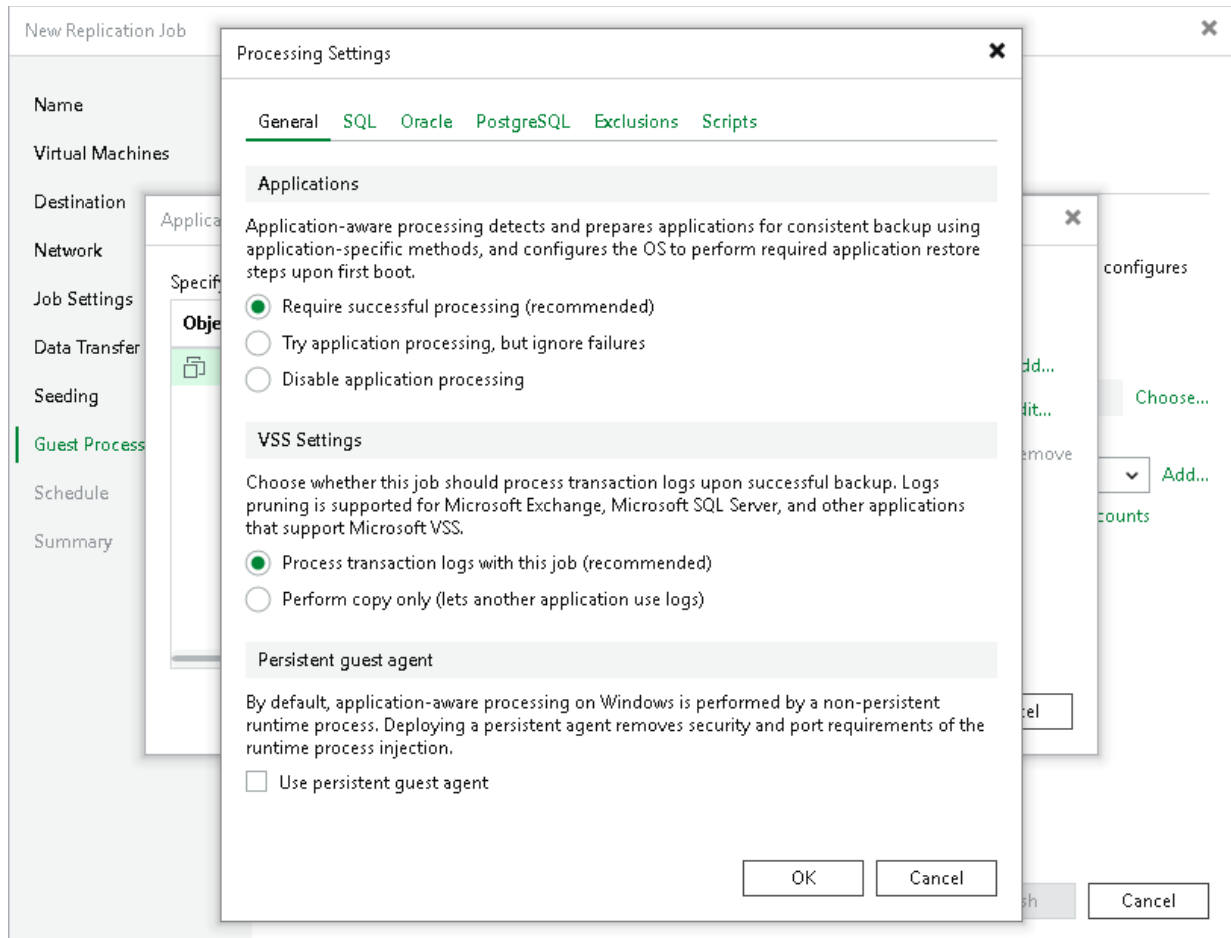
The screenshot shows the 'New Replication Job' wizard with the 'Guest Processing' step selected in the left-hand navigation pane. The main area is titled 'Guest Processing' and contains the following options:

- ☒ **Enable application-aware processing**
Detects and prepares applications for consistent backup, performs transaction logs processing, and configures the OS to perform required application restore steps upon first boot.
[Application handling options for individual machines](#)
- Guest interaction proxy:
Automatic selection [Choose...](#)
- Guest OS credentials:
tech\susan.r.james (tech\susan.r.james, last edited: less than a day ago) [Add...](#)
[Manage accounts](#)
- [Guest OS credentials for individual machines](#)
- [Verify network connectivity and credentials](#)

At the bottom right, there are four buttons: '< Previous', 'Next >' (highlighted with a green border), 'Finish', and 'Cancel'.

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 **Guest OS credentials for individual machines** and enter custom credentials for the necessary VM.
18. Click **Application handling options for individual machines**, select the necessary VM and click **Edit**. On the **General** tab, in the **Applications** section, specify the VSS behavior scenario:
- Select **Require successful processing** if you want Veeam Backup & Replication to stop the backup process if any VSS errors occur.
 - 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.
 - 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.
- 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.

- 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 documentation](#).



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.

The screenshot shows the 'New Replication Job' wizard with the 'Schedule' step selected in the left sidebar. The main area is titled 'Schedule' and contains the following options:

- Run the job automatically** (checked):
 - Daily at this time:** 10:00 PM, Everyday (Days...)
 - Monthly at this time:** 10:00 PM, Fourth, Saturday (Months...)
 - Periodically every:** 1, Hours (Schedule...)
 - After this job:** Backup Job 1 (Created by .\Administrator at 10/26/2025 9:36 PM.)
- Automatic retry**
 - Retry failed items processing:** 3 times
 - Wait before each retry attempt for:** 10 minutes
- Backup window**
 - ☐ **Terminate the job outside of the allowed backup window**
Long running or accidentally started jobs will be terminated to prevent impact on your production infrastructure during busy hours.
Window...

At the bottom right, there are four buttons: '< Previous', 'Next >' (highlighted with a green border), 'Finish', and 'Cancel'.

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 for VMware vSphere

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.

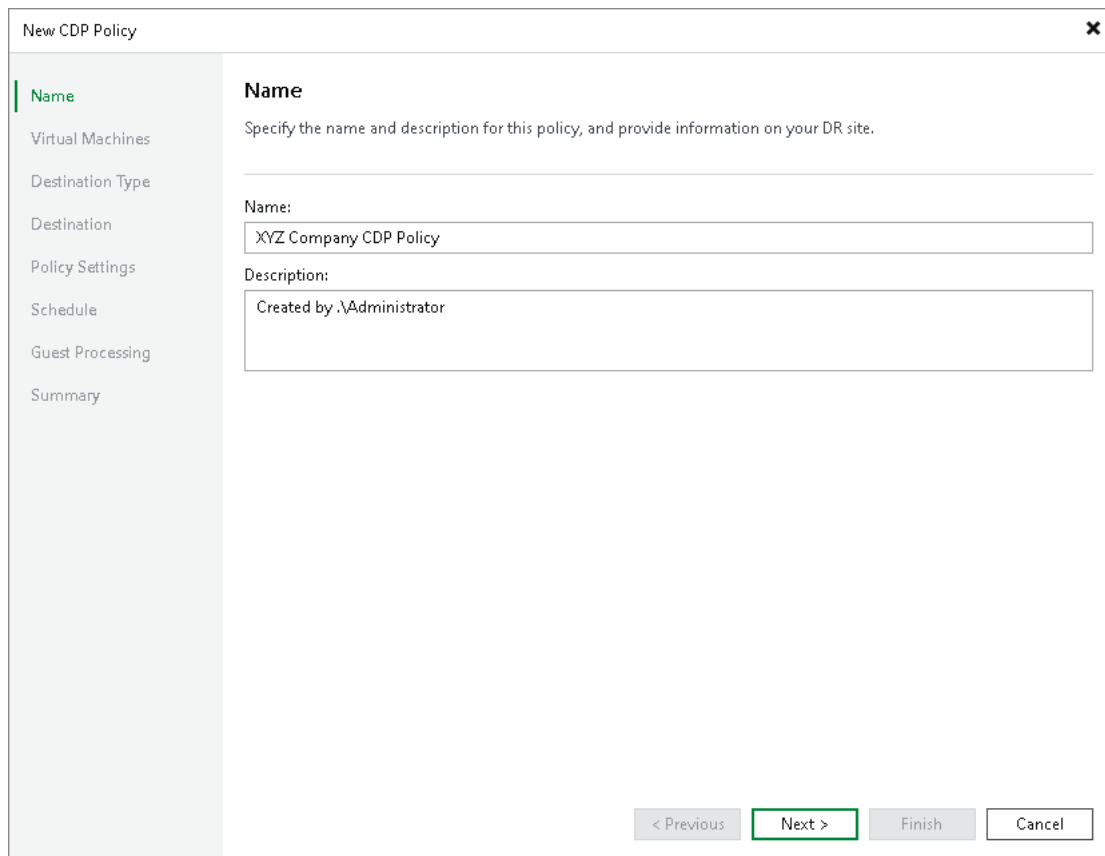
NOTE

This section describes only basic steps that you must take to create a CDP policy for VMware vSphere targeted at the cloud host. To get a detailed description of all CDP for VMware vSphere 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.

To avoid problems with long paths, it is recommended to create policy names not longer than 50 characters.



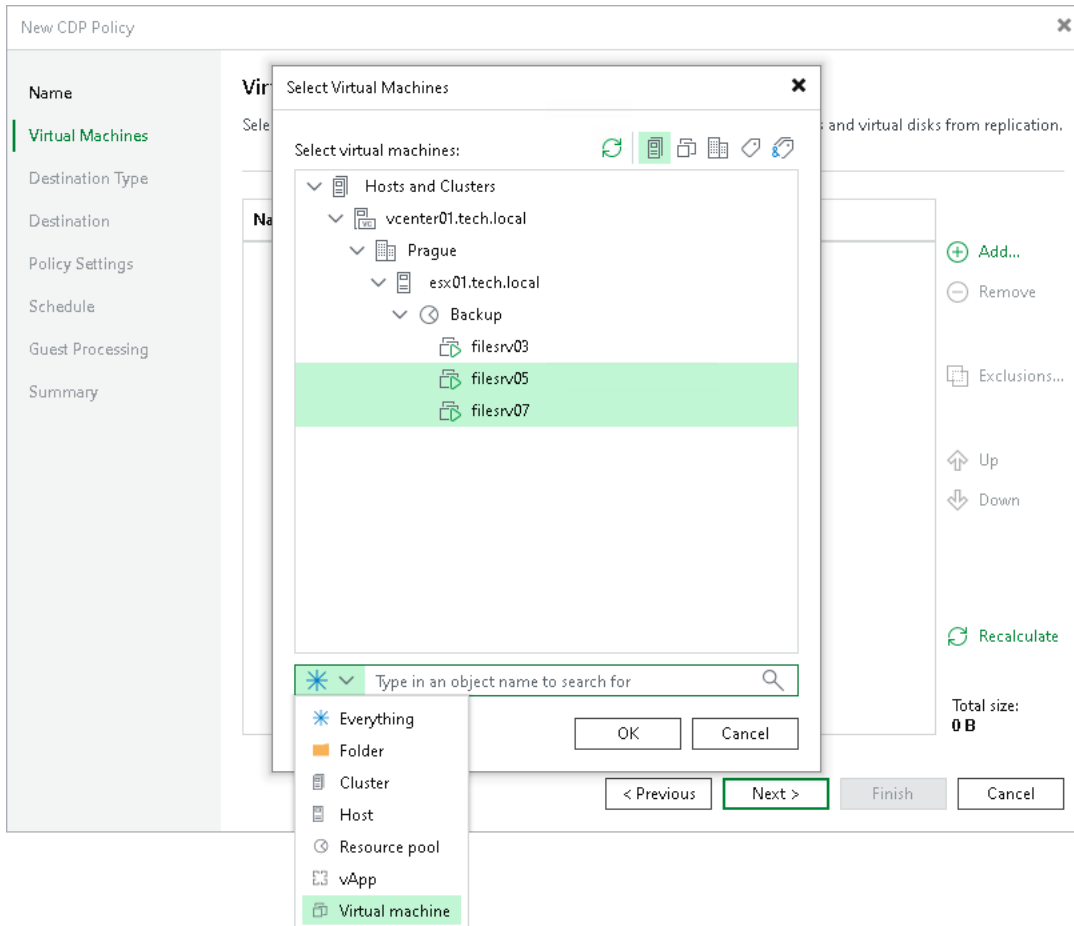
The screenshot shows the 'New CDP Policy' wizard window. On the left is a sidebar with steps: Name (highlighted), Virtual Machines, Destination Type, Destination, Policy Settings, Schedule, Guest Processing, and Summary. The main area is titled 'Name' and contains the instruction 'Specify the name and description for this policy, and provide information on your DR site.' Below this are two text input fields. The 'Name:' field contains 'XYZ Company CDP Policy'. The 'Description:' field contains 'Created by .\Administrator'. At the bottom right are four buttons: '< Previous' (disabled), 'Next >' (active/highlighted), 'Finish' (disabled), and 'Cancel'.

3. 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

Consider 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.



4. 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.
5. 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.
6. At the **Destination Type** step of the wizard, select **Cloud Host**. If you want to use advanced settings for the CDP policy:
 - Select the **Replica seeding** check box to enable the **Seeding** step in the wizard.
 - 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.

- 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.

New CDP Policy

Name

Virtual Machines

Destination Type

Destination

Network

Seeding

Policy Settings

Schedule

Guest Processing

Summary

Destination Type

Choose where the replicated VMs should be created. Additional steps will appear based on your selection.

☐ VMware vSphere

Replicate to a VMware vSphere host or cluster in the DR site.

☒ Cloud Host

Replicate to a cloud host allocated to you by a service provider.

Show advanced controls:

☒ Replica seeding (for low bandwidth DR sites)

☒ Network remapping (for DR sites with different virtual networks)

☐ Replica re-IP (for DR sites with different IP addressing scheme)

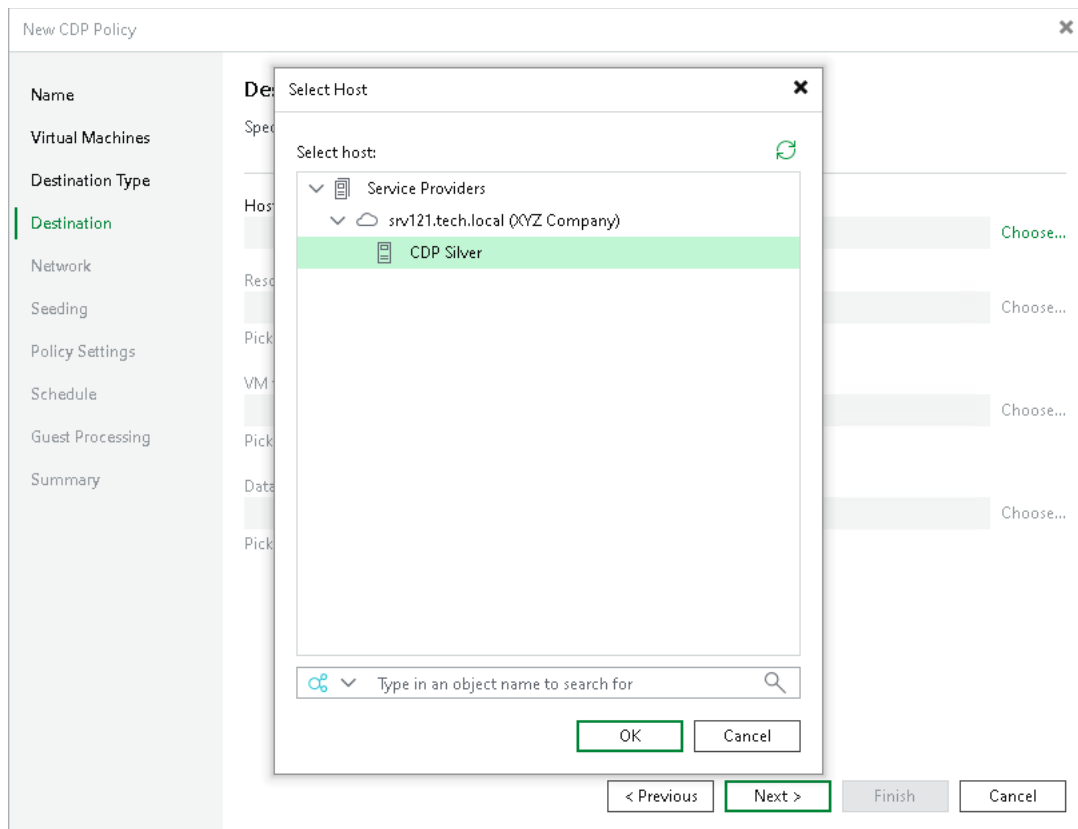
< Previous

Next >

Finish

Cancel

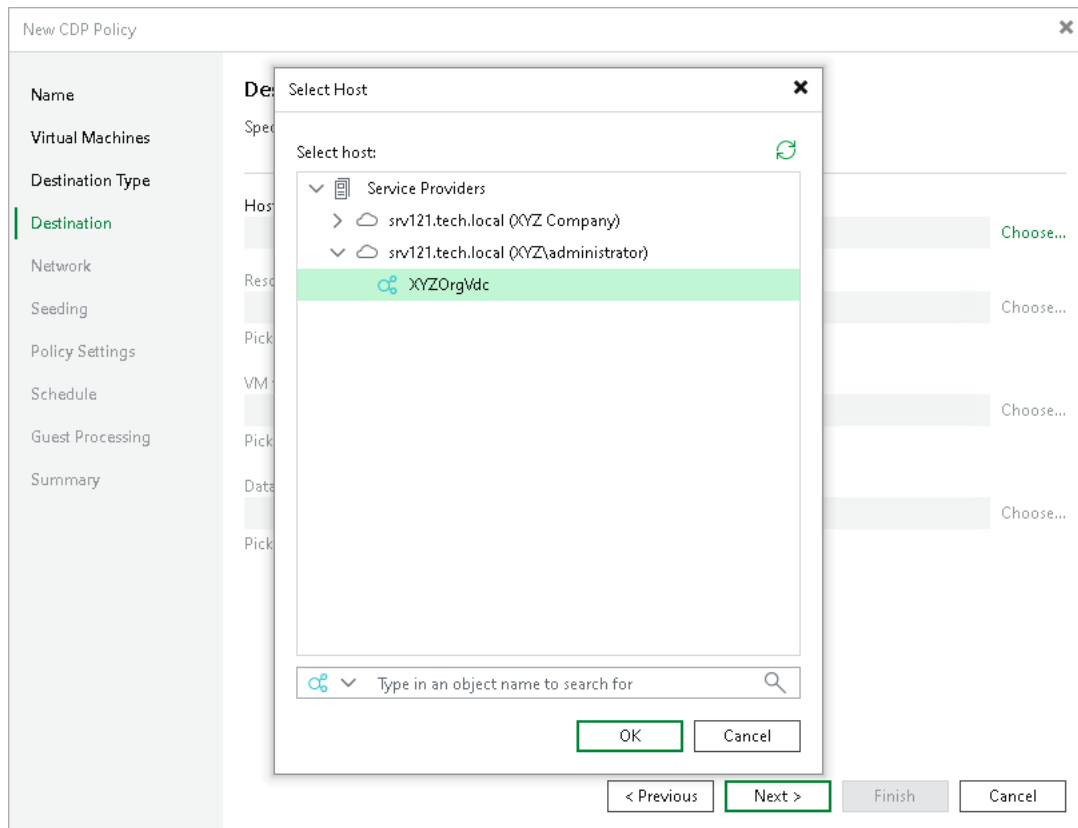
7. At the **Destination** step of the wizard, in the **Host or cluster** section, click **Choose** and select **Cloud host**. Then select the cloud host allocated to you by the SP:
- If the SP allocated to you replication resources on a VMware vSphere host, select the cloud host provided to you through a hardware plan.



- 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:
- [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.

The screenshot shows the 'New CDP Policy' wizard with the 'Destination' step selected in the left-hand navigation pane. The main area is titled 'Destination' and contains the instruction 'Specify where replicas should be created in the DR site.' Below this, there are two sections: 'Host or cluster:' and 'Datastore:'. The 'Host or cluster:' section shows 'CDP Silver' selected with a 'Choose...' link to its right. The 'Datastore:' section shows 'CDP Replicas [500 GB free]' selected with a 'Choose...' link to its right. At the bottom of the wizard, there are four buttons: '< Previous', 'Next >' (which is highlighted with a green border), 'Finish', and 'Cancel'.

- [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.

The screenshot shows the 'New CDP Policy' wizard with the 'Destination' step selected in the left sidebar. The main area is titled 'Destination' and contains the following fields:

- Organization VDC:** XYZOrgVdc (with a 'Choose...' link)
- vApp:** Cloud Connect (Default) (with a 'Choose...' link) for selected replicas
- Storage policy:** Veeam CDP Replication (Default) [300 GB free] (with a 'Choose...' link) for selected virtual disks

At the bottom right, there are four buttons: '< Previous', 'Next >' (highlighted with a green border), 'Finish', and 'Cancel'.

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:

- 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.
- 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.
- If the cloud host has fewer networks than the number of networks in the production infrastructure.

It is also recommended to specify network mapping settings if IPv6 communication is enabled in the Veeam Cloud Connect infrastructure.

To learn more, see [Network Mapping for Cloud Replicas](#).

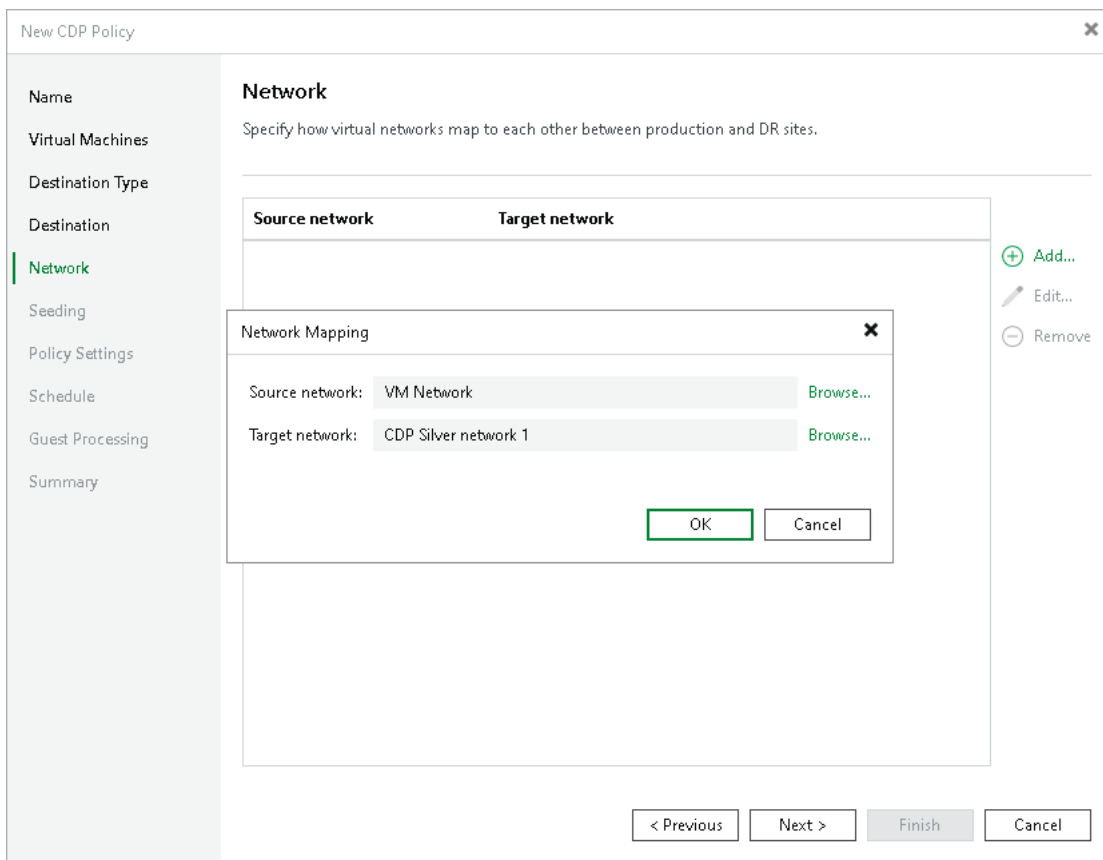
NOTE

[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.

- 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.

- 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.

Keep in mind that only CDP replicas can be used for replica mapping.

New CDP Policy

Seeding

Specify the backup repository with backup files of production VMs. The backup repository must be located in the DR site.

Initial seeding

☒ Get seed from the following backup repository:

Default Backup Repository (Created by Veeam Backup)

18.6 GB free of 89.8 GB

Replica mapping

☐ Map replica to existing VMs

Original VM	Replica VM
filesrv05	no mapping
filesrv07	no mapping

Edit... Remove Detect

If you already have replicas in the target site, replication job can reuse them. This way, only differences will be transferred over WAN by the first job run.

< Previous Next > Finish Cancel

11. At the **Policy Settings** step of the wizard, click **Choose** next to the **Source proxy** field to select a source 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. To test whether CDP proxies available in the source backup infrastructure can handle replication, click **Verify whether currently available resource can handle CDP activity**.

Veeam Backup & Replication will analyze available CPU on all source CDP proxies, the maximum disk write speed during the last hour, and will calculate approximate requirements for CDP proxies. In the **CDP Infrastructure Assessment** window, you will see the calculated values:

- The **Proxy CPU** rows show CPU cores available on all source proxies.
- The **Proxy RAM** rows show RAM required for CDP and, in parenthesis, RAM available on all source proxies. If values in the parentheses and near the parenthesis are the same, you need to upgrade proxies for which values coincide to provide more resources. For example, you can double up the amount of RAM.

- The **Proxy Bandwidth** rows show the maximum disk write speed during the last hour and, in parenthesis, available bandwidth based on available cores of source or target proxies.

CDP Infrastructure Assessment

CDP proxy requirements:

Name	Required
Source Proxy CPU	1 vCPU (4 vCPU available)
Source Proxy RAM	7 MB (6 GB available)
Source Proxy Bandwidth	242 KB/s (800 MB/s available)
Target Proxy CPU	N/A
Target Proxy RAM	N/A (N/A)
Target Proxy Bandwidth	N/A (N/A)

Bandwidth requirements:

VM Name	Required
filesrv05	163 KB/s
filesrv07	79 KB/s

Background window: New CDP Policy

- Name
- Virtual Machines
- Destination Type
- Destination
- Network
- Seeding
- Policy Settings**
- Schedule
- Guest Processing
- Summary

Buttons: Finish, Cancel

13. 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.

The screenshot shows the 'New CDP Policy' wizard with the 'Policy Settings' step selected in the left sidebar. The main area is titled 'Policy Settings' and contains the following elements:

- Name:** A field for naming the policy.
- Virtual Machines:** A section for selecting VMs to back up.
- Destination Type:** A dropdown menu.
- Destination:** A field for the target destination.
- Network:** A section for network-related settings.
- Seeding:** A section for seeding settings.
- Policy Settings:** The current step, containing:
 - Data transfer:** A section for data transfer settings.
 - Source proxy:** A dropdown menu with 'Automatic selection' selected and a 'Choose...' link.
 - Target proxy:** A dropdown menu with 'Service provider's proxy' selected and a 'Choose...' link.
 - Verify whether currently available resource can handle CDP activity:** A green link.
 - Replica settings:** A section for replica settings.
 - Replica name suffix:** A text input field containing '_replica'.
- Schedule:** A section for scheduling settings.
- Guest Processing:** A section for guest processing settings.
- Summary:** A section for a summary of the policy.

At the bottom right, there are four buttons: '< Previous', 'Next >' (highlighted with a green border), 'Finish', and 'Cancel'.

14. At the **Schedule** step of the wizard, configure schedule and retention policy settings for the CDP policy:
- 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.
 - 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 **RPO 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.
 - In the **Short-term retention** section, configure the short-term retention policy, that is, specify for how long to store short-term restore points.
 - 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.

New CDP Policy

Name

Virtual Machines

Destination Type

Destination

Network

Seeding

Policy Settings

Schedule

Guest Processing

Summary

Schedule

Specify policy scheduling and retention options.

Recovery Point Objective (RPO):

15

Seconds

Schedule...

RPO reporting...

Short-term retention

Enable point-in-time recovery within:

4

Hours

Defines how far back you can go from the latest state for a point-in-time recovery. The bigger this interval is, the more disk space is required on the target datastore to store the I/O journal.

Long-term retention

Create additional restore points every:

8

hours

Schedule...

Keep these restore points for:

7

days

Defines how granular and how far back you can roll your replica VM state.

< Previous

Next >

Finish

Cancel

541 | Veeam CloudConnect | Administrator Guide | 13.1.0.411

15. 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](#).

The screenshot shows the 'New CDP Policy' wizard window. The left sidebar contains a list of steps: Name, Virtual Machines, Destination Type, Destination, Network, Seeding, Policy Settings, Schedule, **Guest Processing** (highlighted in green), and Summary. The main area is titled 'Guest Processing' and contains the following elements:

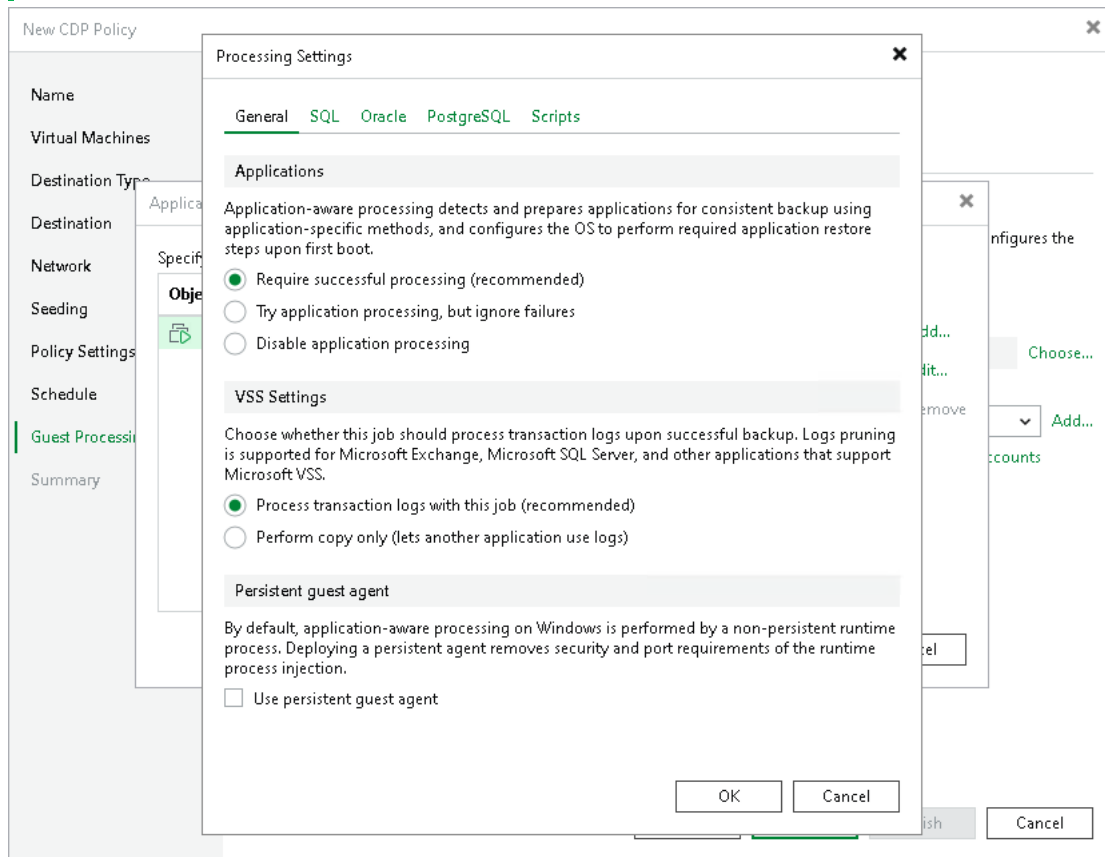
- A description: 'Choose guest OS processing options available for running VMs.'
- A checked checkbox labeled 'Enable application-aware processing' with a sub-description: 'Detects and prepares applications for consistent backup, performs transaction logs processing, and configures the OS to perform required application restore steps upon first boot.' Below this is a link: 'Application handling options for individual machines'.
- A section for 'Guest interaction proxy:' with a dropdown menu set to 'Automatic selection' and a 'Choose...' button.
- A section for 'Guest OS credentials:' with a dropdown menu showing 'tech\william.fox (tech\william.fox, last edited: less than a day ago)' and an 'Add...' button. A 'Manage accounts' link is also present.
- Two icons with links: 'Guest OS credentials for individual machines' and 'Verify network connectivity and credentials'.
- At the bottom, four buttons: '< Previous', 'Next >' (highlighted in green), 'Finish', and 'Cancel'.

16. 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.
17. Click **Applications**, select the necessary VM and click **Edit**. On the **General** tab, in the **Applications** section, specify the VSS behavior scenario:
- Select **Require successful processing** if you want Veeam Backup & Replication to stop the backup process if any VSS errors occur.
 - 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.
 - Select **Disable application processing** if you do not want to enable quiescence for the VM at all.
18. [For Microsoft SQL and Oracle VMs] In the **VSS Settings** section, specify how Veeam Backup & Replication must handle transaction logs.
- 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.

- 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 documentation](#).

NOTE

CDP policies targeted at the cloud host do not support application-aware processing of PostgreSQL VMs.



19. 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.

20. Click **Finish**.

Creating Universal CDP Policies

To protect workloads with universal CDP, you must configure a CDP policy. The CDP policy defines which workloads to protect, where to store replicas, how often create short-term and long-term restore points, and so on. One CDP policy can process one or multiple workloads.

With universal CDP, you can protect Microsoft Windows workloads and Linux-based machines.

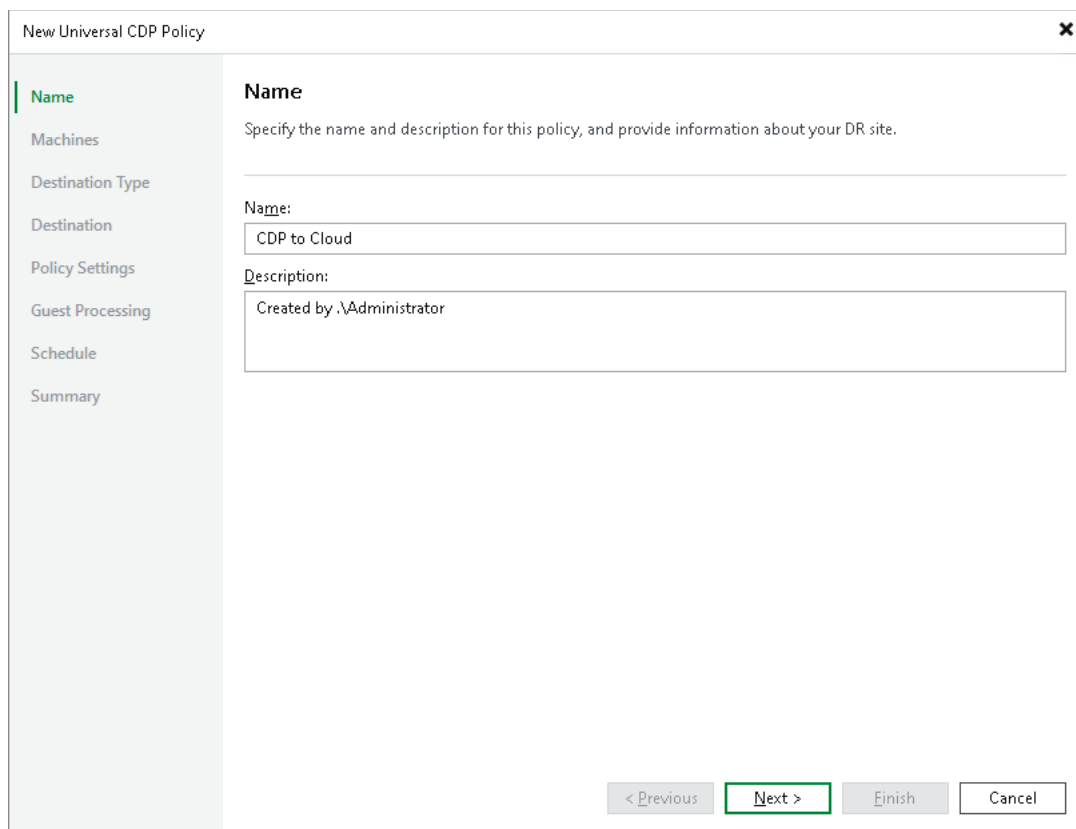
NOTE

This section describes only basic steps that you must take to create a universal CDP policy targeted at the cloud host. To get a detailed description of all universal CDP policy settings, see the [Creating Universal CDP Policies](#) section in the Veeam Backup & Replication User Guide.

To create a universal CDP policy:

1. On the **Home** tab, click **CDP Policy** and select **Universal CDP**.
2. At the **Name** step of the wizard, specify a name and description for the CDP policy.

To avoid problems with long paths, it is recommended to create policy names not longer than 50 characters.



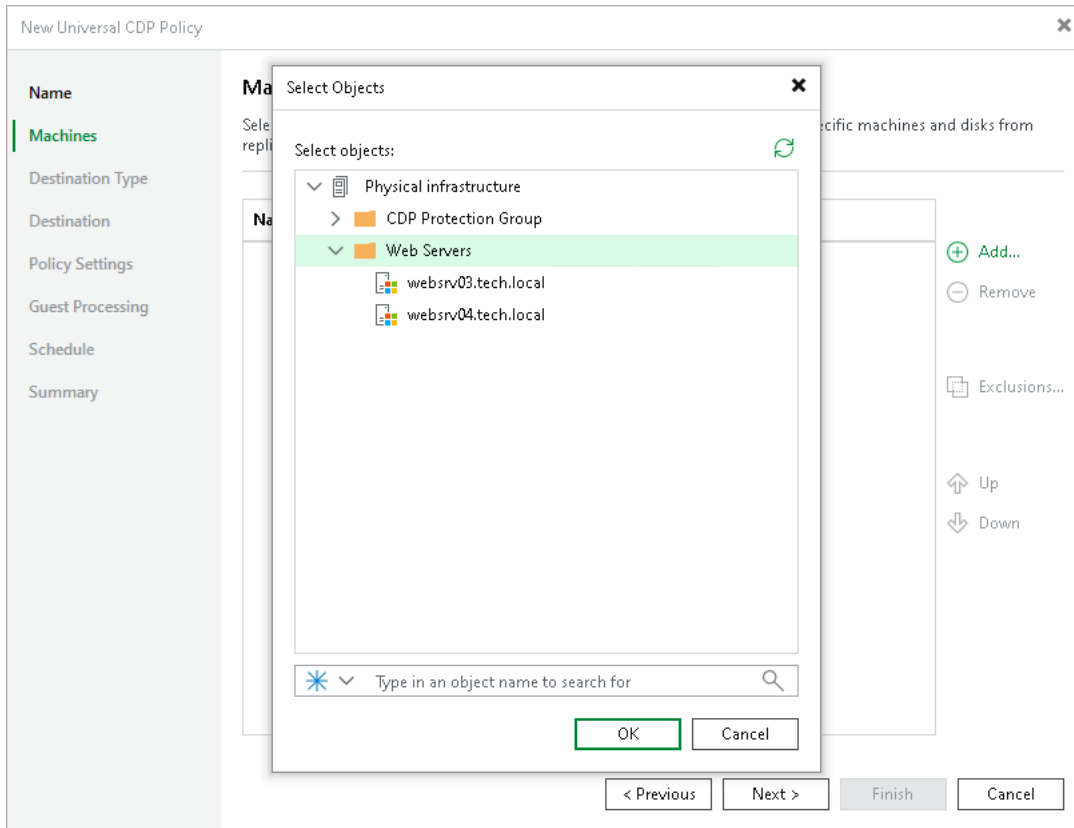
The screenshot shows the 'New Universal CDP Policy' wizard window. On the left is a sidebar with steps: Name (highlighted), Machines, Destination Type, Destination, Policy Settings, Guest Processing, Schedule, and Summary. The main area is titled 'Name' and contains the instruction: 'Specify the name and description for this policy, and provide information about your DR site.' Below this are two text input fields. The first is labeled 'Name:' and contains the text 'CDP to Cloud'. The second is labeled 'Description:' and contains the text 'Created by .\Administrator'. At the bottom right are four buttons: '< Previous' (disabled), 'Next >' (active/highlighted), 'Finish' (disabled), and 'Cancel'.

3. At the **Machines** step of the wizard, click **Add** and select workloads or protection groups that contain workloads you want to replicate. To quickly find the necessary object, use the search field at the bottom of the **Select Objects** window.

IMPORTANT

Consider the following:

- You can replicate only workloads that are turned on, the turned off workloads will be skipped from processing.
- You cannot add to a universal CDP policy workloads that were already added to other universal CDP policies created on the same backup server.



4. If you want to exclude workloads from the CDP policy, click **Exclusions** and specify what objects you want to exclude.
5. If you want to define the order in which the CDP policy must process workloads or protection groups, select a workload or protection group added to the policy and use the **Up** and **Down** buttons on the right to move the object up or down in the list.
6. At the **Destination Type** step of the wizard, select **Cloud Host**. If you want to use advanced settings for the CDP policy:
 - Select the **Replica seeding** check box to enable the **Seeding** step in the wizard.
 - 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.

- 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.

The screenshot shows the 'New Universal CDP Policy' wizard window. The left sidebar contains a list of steps: Name, Machines, Destination Type (highlighted in green), Destination, Network, Seeding, Policy Settings, Guest Processing, Schedule, and Summary. The main area is titled 'Destination Type' and includes the instruction: 'Choose where the replicated VMs should be created. Additional steps will appear based on your selection.' There are two radio button options: 'VMware vSphere' (unselected) and 'Cloud Host' (selected). Below these, under 'Show advanced controls:', there are three checkboxes: 'Replica seeding (for low bandwidth DR sites)' (checked), 'Network remapping (for DR sites with different virtual networks)' (checked), and 'Replica re-IP (for DR sites with different IP addressing scheme)' (unchecked). At the bottom right, there are four buttons: '< Previous', 'Next >', 'Finish' (disabled), and 'Cancel'.

New Universal CDP Policy

Name

Machines

Destination Type

Destination

Network

Seeding

Policy Settings

Guest Processing

Schedule

Summary

Destination Type

Choose where the replicated VMs should be created. Additional steps will appear based on your selection.

☐ **VMware vSphere**
Replicate to a VMware vSphere host or cluster in the DR site.

☒ **Cloud Host**
Replicate to a cloud host allocated to you by a service provider.

Show advanced controls:

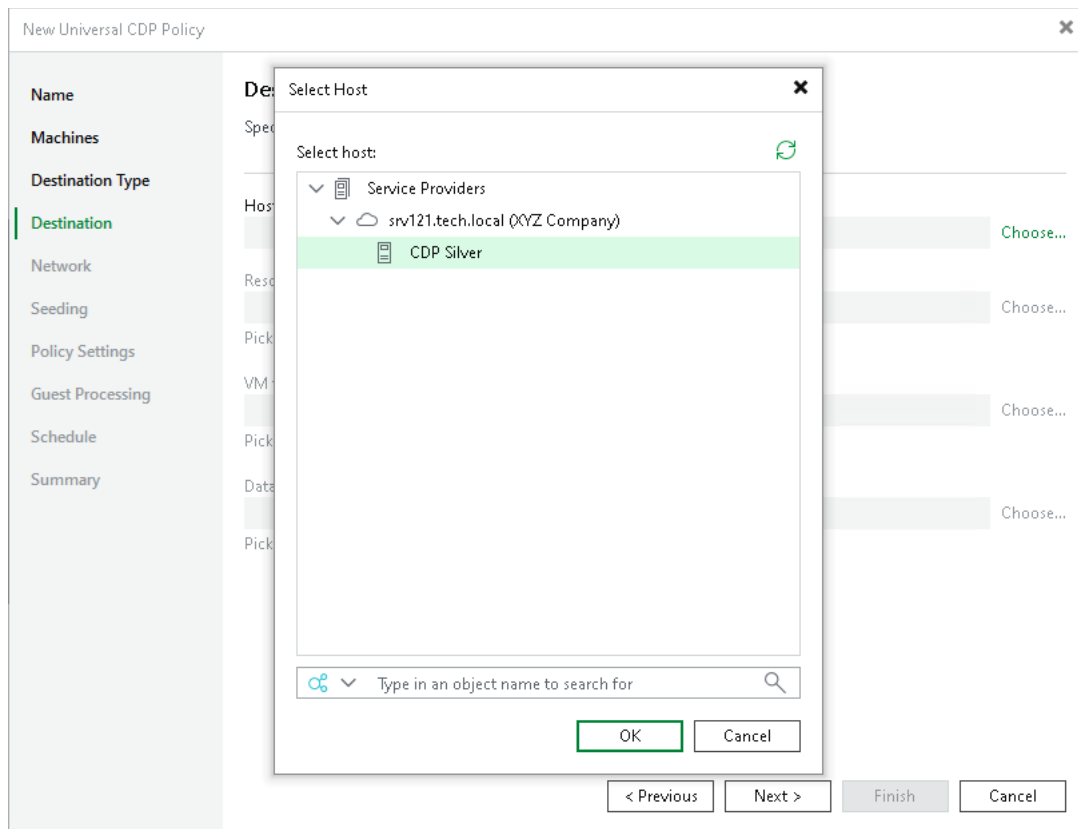
☒ Replica seeding (for low bandwidth DR sites)

☒ Network remapping (for DR sites with different virtual networks)

☐ Replica re-IP (for DR sites with different IP addressing scheme)

< Previous Next > Finish Cancel

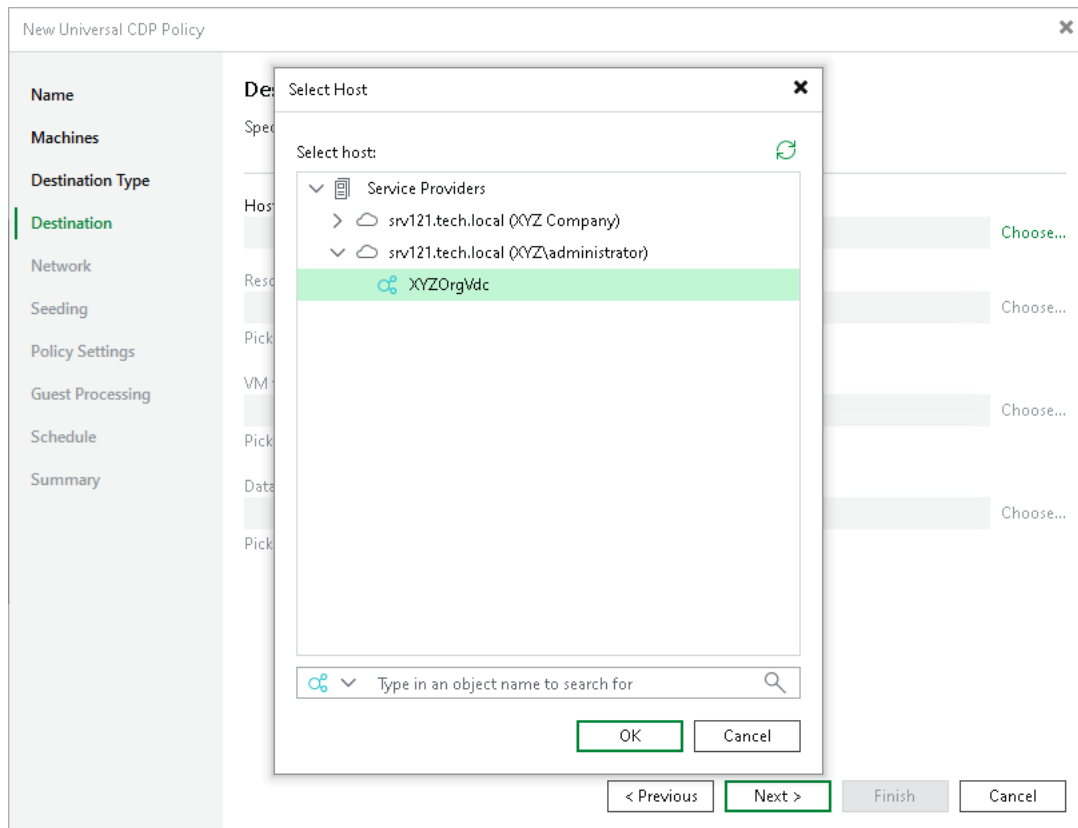
7. At the **Destination** step of the wizard, in the **Host or cluster** section, click **Choose** and select **Cloud host**. Then select the cloud host allocated to you by the SP:
- If the SP allocated to you replication resources on a VMware vSphere host, select the cloud host provided to you through a hardware plan.



- 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:
- [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.

The screenshot shows the 'New Universal CDP Policy' wizard with the 'Destination' step selected in the left-hand navigation pane. The main area is titled 'Destination' and contains the instruction 'Specify where replicas should be created in the DR site.' Below this, there are two sections: 'Host or cluster:' and 'Datastore:'. The 'Host or cluster:' section shows 'CDP Silver' selected with a 'Choose...' link to its right. The 'Datastore:' section shows 'CDP Replicas [500 GB free]' selected with a 'Choose...' link to its right. At the bottom of the wizard, there are four buttons: '< Previous', 'Next >' (which is highlighted with a green border), 'Finish', and 'Cancel'.

- [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.

The screenshot shows the 'New Universal CDP Policy' wizard with the 'Destination' step selected in the left sidebar. The main area is titled 'Destination' and contains the instruction 'Specify where replicas should be created in the DR site.' Below this, there are three configuration sections, each with a dropdown menu and a 'Choose...' link:

- Organization VDC:** The dropdown shows 'XYZOrgVdc'.
- vApp:** The dropdown shows 'Cloud Connect (Default)' for selected replicas.
- Storage policy:** The dropdown shows 'Veeam CDP Replication (Default) [300 GB free]' for selected virtual disks.

At the bottom right, there are four buttons: '< Previous', 'Next >' (highlighted with a green border), 'Finish', and 'Cancel'.

9. At the **Network** step of the wizard, click **Network** and select the network on the cloud host to which CDP replicas must be connected.

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.

New Universal CDP Policy

Name

Machines

Destination Type

Destination

Network

Seeding

Policy Settings

Guest Processing

Schedule

Summary

Network

Specify how virtual networks map to each other between production and DR sites.

Name	Target Network
 Other machines	CDP Silver network 1

+

 Add...

-

 Remove

 Network...

< Previous

Next >

Finish

Cancel

10. At the **Seeding** step of the wizard, configure replica seeding and mapping.

If you want to use initial seeding, select the **Get seed from the following backup repository** check box and from the list of available backup repositories, select the repository where your replica seeds are stored.

If you want to use replica mapping, select the **Map replica to existing Machines** check box and select the copy of the necessary machines.

The screenshot shows the 'New Universal CDP Policy' wizard, specifically the 'Seeding' step. The left sidebar contains a list of steps: Name, Machines, Destination Type, Destination, Network, Seeding (highlighted), Policy Settings, Guest Processing, Schedule, and Summary. The main content area is titled 'Seeding' and includes a description: 'Specify the backup repository with backup files of production machines. The backup repository must be located in the DR site.'

The 'Initial seeding' section has a checked checkbox 'Get seed from the following backup repository:' with a dropdown menu showing 'Cloud repository 1 (Cloud repository)' and a status bar indicating '72.4 GB free of 149 GB'.

The 'Replica mapping' section has a checked checkbox 'Map replica to existing Machines'. Below it is a table with two columns: 'Original Machine' and 'Replica Machine'. The table contains one row with 'websrv03.tech.local' in the first column and 'no mapping' in the second column. To the right of the table are three buttons: 'Edit...' (pencil icon), 'Remove' (minus icon), and 'Detect' (magnifying glass icon).

Below the table, a note states: 'If you already have replicas in the target site, replication job can reuse them. This way, only differences will be transferred over WAN by the first job run.'

At the bottom right, there are four buttons: '< Previous', 'Next >' (highlighted with a green border), 'Finish', and 'Cancel'.

11. At the **Policy Settings** step of the wizard, click **Choose** next to the **Source proxy** field to select a source 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 CDP replicas. To register a CDP replica on the target host in the SP site, Veeam Backup & Replication appends the specified suffix to the name of the source workload.

New Universal CDP Policy

Name

Machines

Destination Type

Destination

Network

Seeding

Policy Settings

Guest Processing

Schedule

Summary

Policy Settings

Choose how machine data should be transferred to the target site, specify the replica name suffix, and customize advanced policy settings if required.

Data transfer

When replicating between sites, we highly recommend that you deploy at least one backup proxy server locally in both sites to allow direct access to storage.

Source proxy:

Automatic selection

Choose...

Target proxy:

Service provider's proxy

Choose...

Replica settings

Replica name suffix:

_replica

Use advanced policy settings to configure notification options

< Previous

Next >

Finish

Cancel

553 | Veeam Cloud Connect | Administrator Guide | 13.1.0.411

13. 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](#).

The screenshot shows the 'New Universal CDP Policy' wizard window. The left sidebar contains a list of steps: Name, Machines, Destination Type, Destination, Network, Seeding, Policy Settings, **Guest Processing** (highlighted with a green bar), Schedule, and Summary. The main content area is titled 'Guest Processing' and includes the instruction 'Choose guest OS processing options available for running VMs.' Below this, there is a checkbox labeled 'Enable application-aware processing' which is checked. A description follows: 'Detects and prepares applications for consistent backup, performs transaction logs processing, and configures the OS to perform required application restore steps upon first boot.' Below the description is a link: 'Application handling options for individual machines'. Further down, there is a section for 'Guest interaction proxy:' with a dropdown menu currently showing 'Automatic selection' and a 'Choose...' button to its right. At the bottom right of the window are four buttons: '< Previous', 'Next >' (highlighted with a green border), 'Finish', and 'Cancel'.

14. At the **Schedule** step of the wizard, configure schedule and retention policy settings for the CDP policy:
- 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 machines 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 CDP replicas and send this data to the target destination. Note that short-term restore points are crash-consistent.
 - 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 **RPO 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.
 - In the **Short-term retention** section, configure the short-term retention policy, that is, specify for how long to store short-term restore points.
 - 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 crash-consistent long-term restore points, click **Schedule**, then select the necessary time area for crash-consistent long-term restore points.

For Universal CDP policies, application-consistent restore points are not supported, and those time periods cannot be specified. **Crash-consistent** is selected by default.

NOTE

For Linux-based machines, universal CDP creates crash-consistent short-term and long-term restore points. Application-consistent restore points are not supported.

The screenshot shows the 'New Universal CDP Policy' wizard, specifically the 'Schedule' step. The left sidebar contains a list of steps: Name, Machines, Destination Type, Destination, Network, Seeding, Policy Settings, Guest Processing, **Schedule** (highlighted in green), and Summary. The main area is titled 'Schedule' and contains the following settings:

- Recovery Point Objective (RPO):** 15 (dropdown), Seconds (dropdown), with a [Schedule...](#) link.
- BPO reporting...** (link)
- Short-term retention** (header)
- Enable point-in-time recovery within:** 4 (dropdown), Hours (dropdown).
- Long-term retention** (header)
- Create additional restore points every:** 8 (dropdown), hours, with a [Schedule...](#) link.
- Keep these restore points for:** 7 (dropdown), days.

At the bottom, there are four buttons: '< Previous', **Next >** (highlighted with a green border), 'Finish', and 'Cancel'.

15. 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.
16. 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

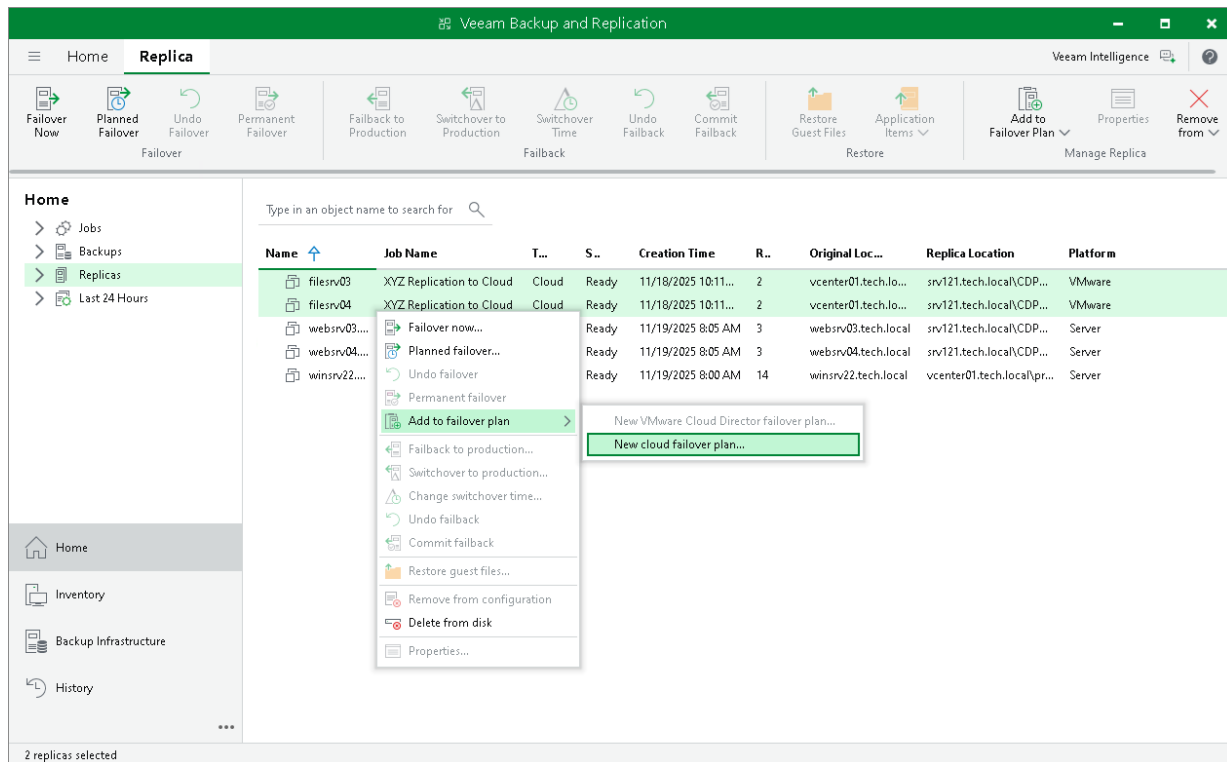
Before you create a cloud failover plan, check the following prerequisites and limitations:

- 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 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 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.

Cloud Failover Plan



Failover Plan

Type in a name and description for this failover plan.

Failover Plan

Machines

Default Gateways

Public IP Addresses

Summary

Name:

ABC Company Failover Plan

Description:

Cloud failover plan for ABC Company full site failover

< Previous

Next >

Finish

Cancel

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.

Cloud Failover Plan

vm

Machines

Add machines to be failed over as a part of this plan. Use machine order and delays to ensure all application dependencies are met.

Failover Plan

Machines

Default Gateways

Public IP Addresses

Summary

Machines:

Name	Delay	Replica state
filesrv03	60 sec	less than a day ago (10:11 P...
filesrv04	60 sec	less than a day ago (10:11 P...

Add...

Remove

Set Delay...

Up

Down

< Previous

Next >

Finish

Cancel

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](#).

The screenshot shows the 'Cloud Failover Plan' wizard window, specifically the 'Default Gateways' step. The window has a title bar 'Cloud Failover Plan' and a close button. Below the title bar is a 'Default Gateways' section with a VM icon and the text: 'Specify default gateways for all production IP networks. This information is used by network extension appliance during the full site failover.' On the left is a sidebar with navigation links: 'Failover Plan', 'Machines', 'Default Gateways' (selected), 'Public IP Addresses', and 'Summary'. The main area is titled 'Default gateways:' and contains a table with three columns: 'Cloud network', 'IP network', and 'Default gateway'. The 'Cloud network' column contains two entries: 'CDP Silver network 1 ...' and 'CDP Silver network 1'. The 'IP network' and 'Default gateway' columns are empty. At the bottom right of the table area is a link 'Manage default gateways'. At the bottom of the window are four buttons: '< Previous', 'Next >' (highlighted with a blue border), 'Finish', and 'Cancel'.

Cloud network	IP network	Default gateway
CDP Silver network 1 ...		
CDP Silver network 1		

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 production network.

5. In the **Description** field, provide a description for future reference.

6. Click **OK**.

Cloud Failover Plan

Public IP Addresses
Assign public IP addresses supplied by your service provider to VMs in the failover plan. Public IP address enables connecting to a VM from the internet after full site failover.

Failover Plan
Machines
Default Gateways
Public IP Addresses
Summary

☒ Assign public IP addresses

Machine

Public IP Address Mapping Rule

Replica VM: filesrv03 Add...

Public IP address: 198.51.100.1 Port: 8888

Internal IP address of replica VM: 172.24.26.134 Port: 3339

Description: Public IP address for filesrv03

OK Cancel

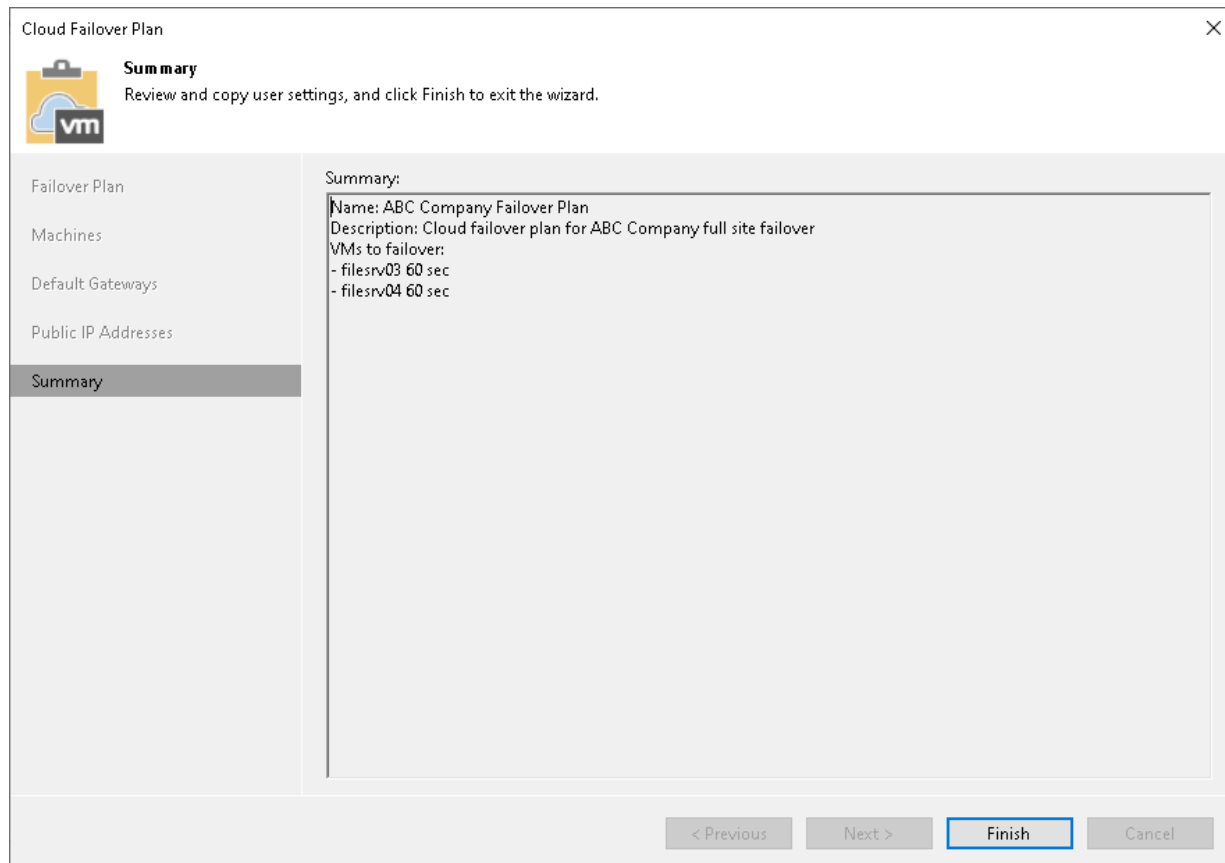
Add... Edit... Remove

< Previous Next > Finish Cancel

Step 6. 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:

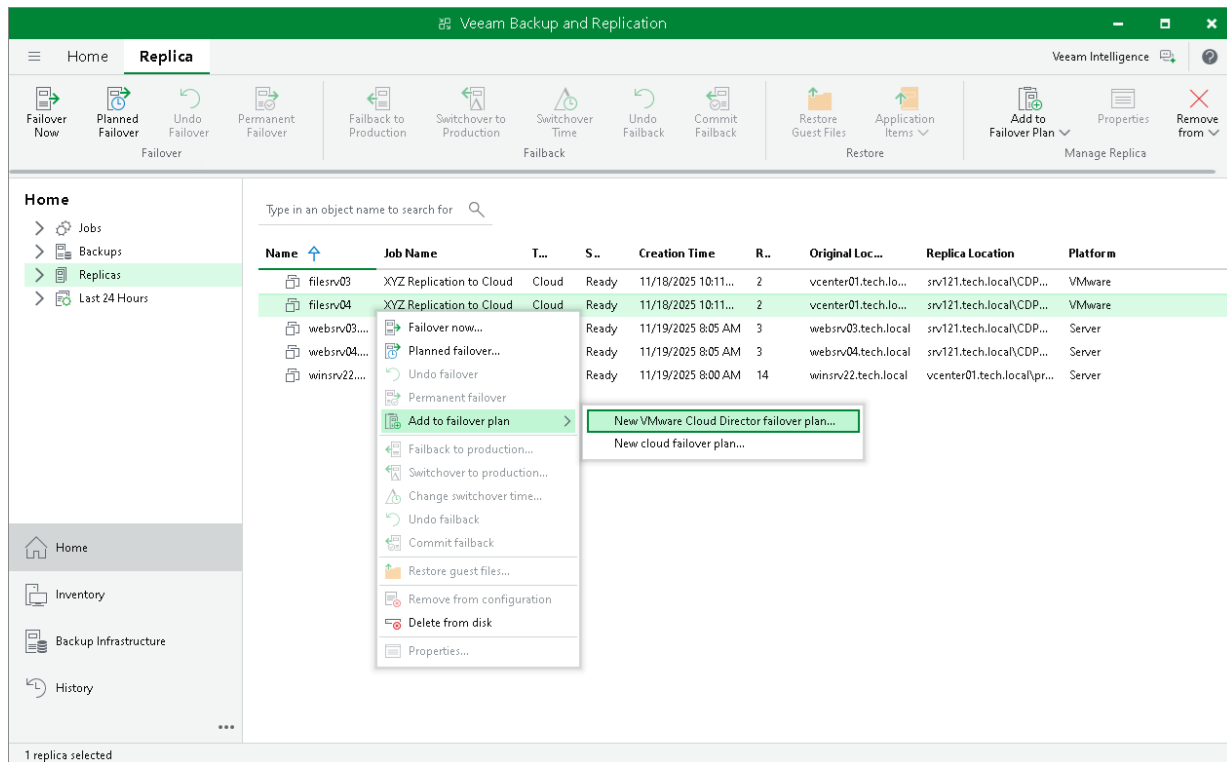
- VMs that you plan to include in the failover plan must be successfully replicated at least once.

- You cannot select to use pre-failover and 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 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 in 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.

Cloud Failover Plan

General
Type in name and description for this failover plan, and optionally specify scripts to trigger before and after the failover.

Failover Plan
Virtual Machines
Summary

Name:
TechCompany Failover Plan

Description:
Cloud failover plan for TechCompany full site failover to VMware Cloud Director

< Previous Next > Finish Cancel

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.

Cloud Failover Plan

Machines
Add machines to be failed over as a part of this plan. Use machine order and delays to ensure all application dependencies are met.

Failover Plan

Virtual Machines

Summary

Name	Delay	Replica state
filesrv03	60 sec	less than a day ago (10:11 P...
filesrv04	60 sec	less than a day ago (10:11 P...

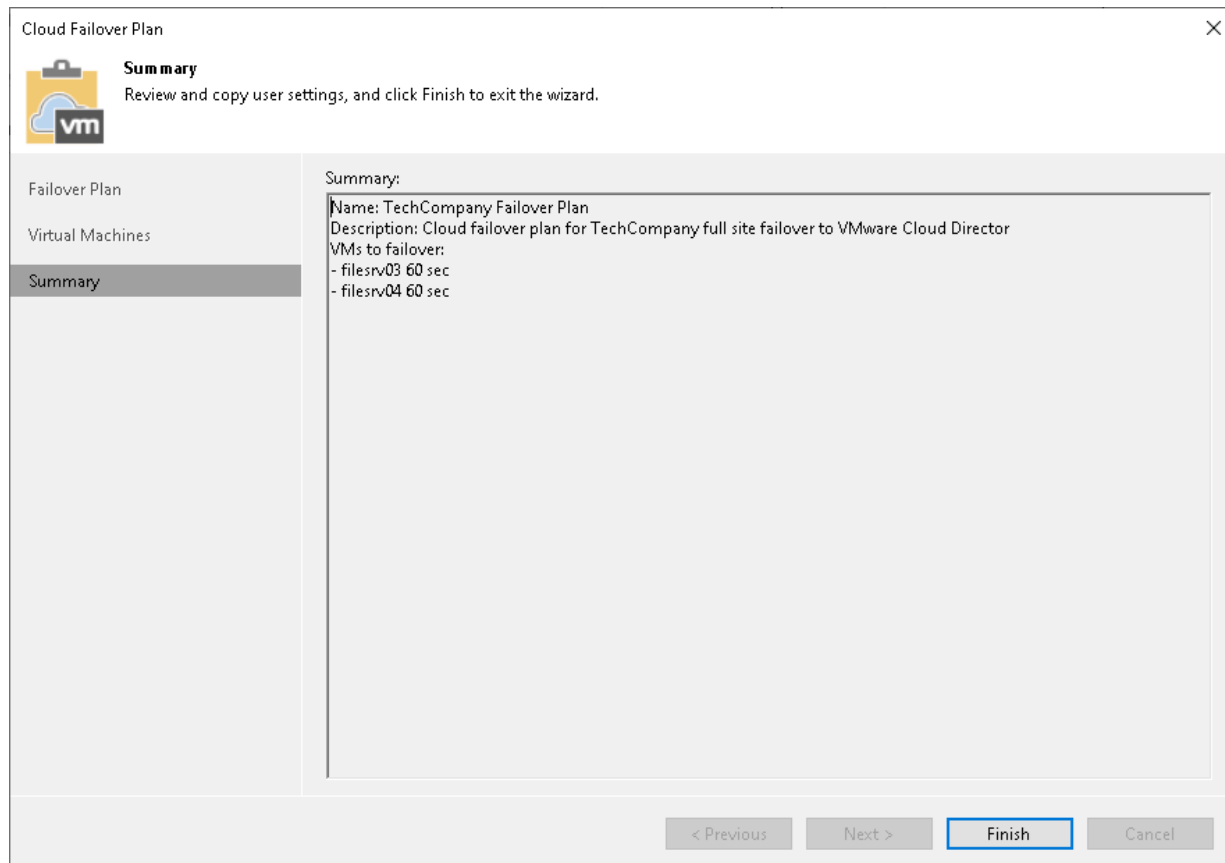
Buttons: Add..., Remove, Set Delay..., Up, Down

Navigation: < Previous, Next >, Finish, Cancel

Step 4. 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.

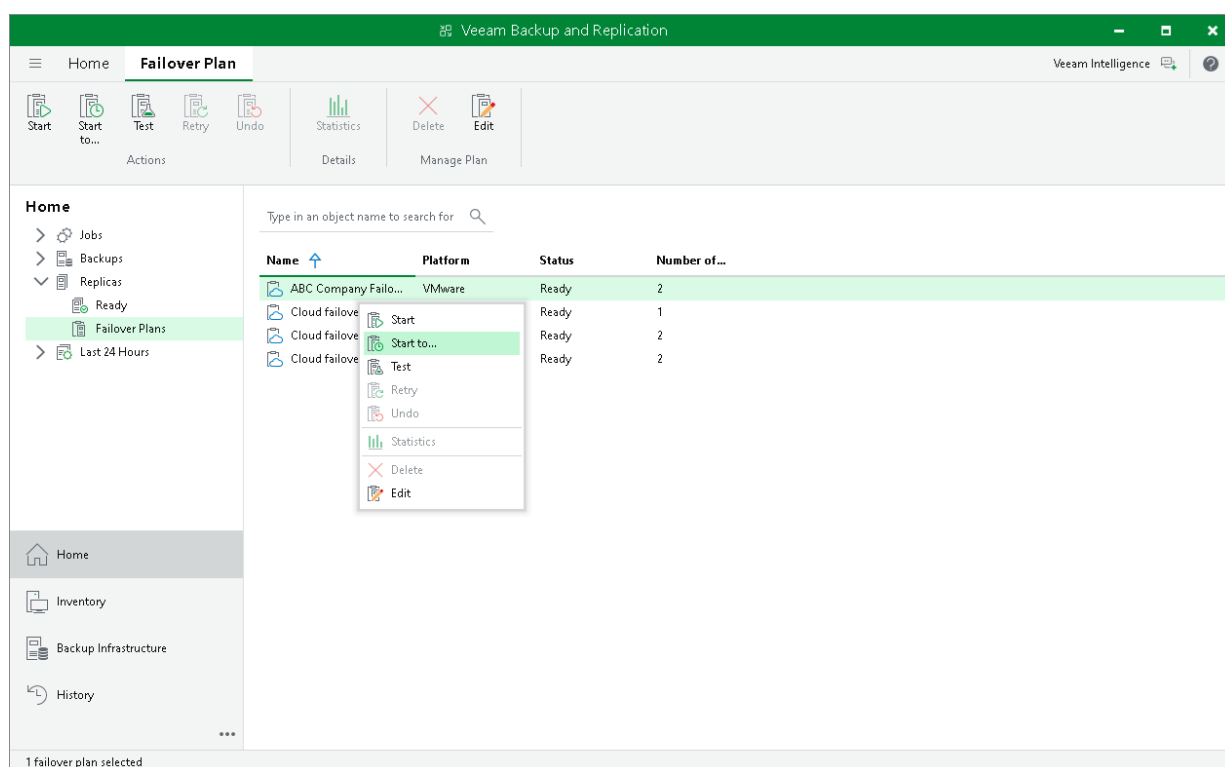
To fail over to the VM replicas latest restore point:

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.

This operation is supported for cloud failover plans that contain snapshot-based replicas and failover plans that contain CDP replicas.

NOTE

Consider the following limitations:

- Veeam Backup & Replication does not support this operation for failover plans that contain CDP replicas with I/O filters older than version 12.1 installed on the cluster where the VMs that you plan to protect reside and where replicas will reside. To learn more about updating I/O filters, see the [Updating and Uninstalling I/O Filter](#) section in the Veeam Backup & Replication User Guide.
- If the SP starts the cloud failover plan test for CDP replicas created with Veeam Backup & Replication version 12.2 (or earlier), long-term retention policy creation will be stopped while testing.

TIP

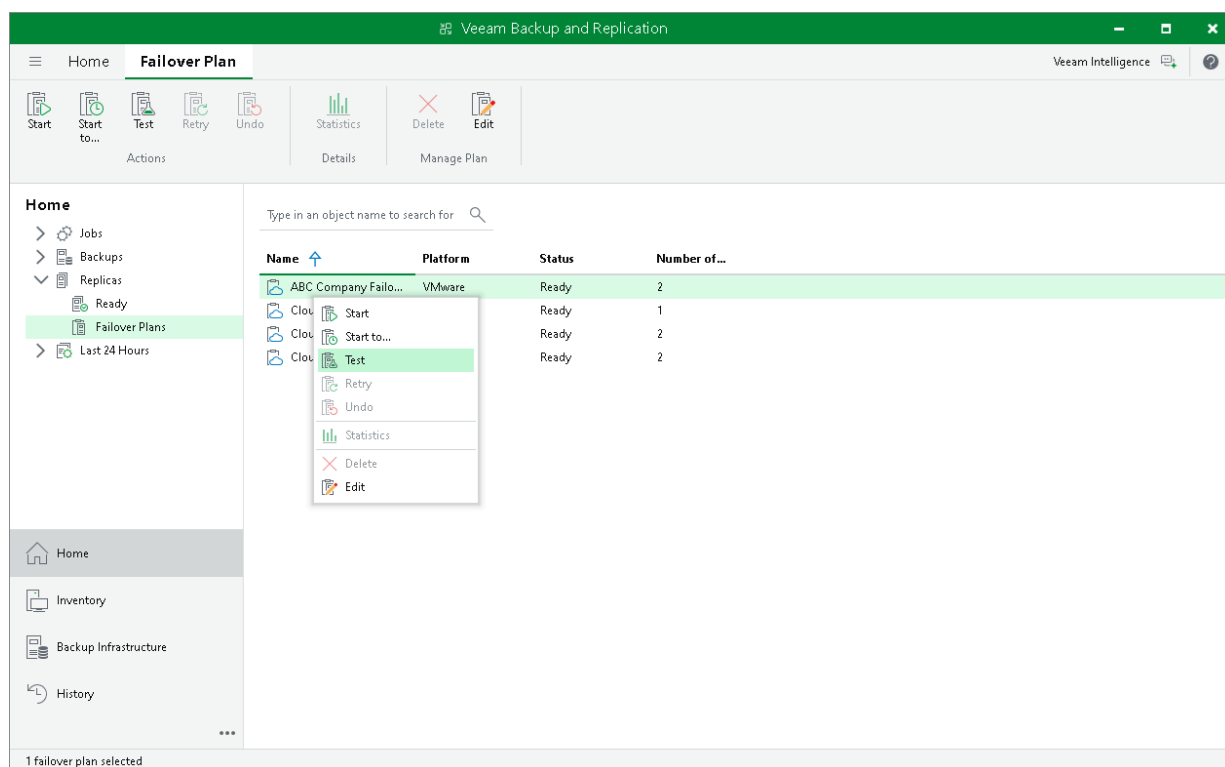
To keep CDP replica VMs running, for example, to reach data from the VM or from an application installed on the VM, you can use Veeam PowerShell cmdlets. To perform the operation, use the *KeepAlive* parameter. For detailed instructions, see the [Start-VBRFailoverPlan](#) section in the Veeam PowerShell Reference.

The following limitations apply to the operation:

- You can use the keep alive mode only for cloud failover plans that contain CDP replicas. This operation is not supported for cloud failover plans that contain snapshot-based replicas.
- By default, this operation is available only for the SP. The SP can use a registry key to allow this operation to the tenant. The SP must configure the allowed keep alive time for their tenants by a registry key `CdpTenantTestFailoverKeepAliveDurationLimitMin`. For details, see [Allowing Tenants to Keep CDP Replicas Running](#).

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**.



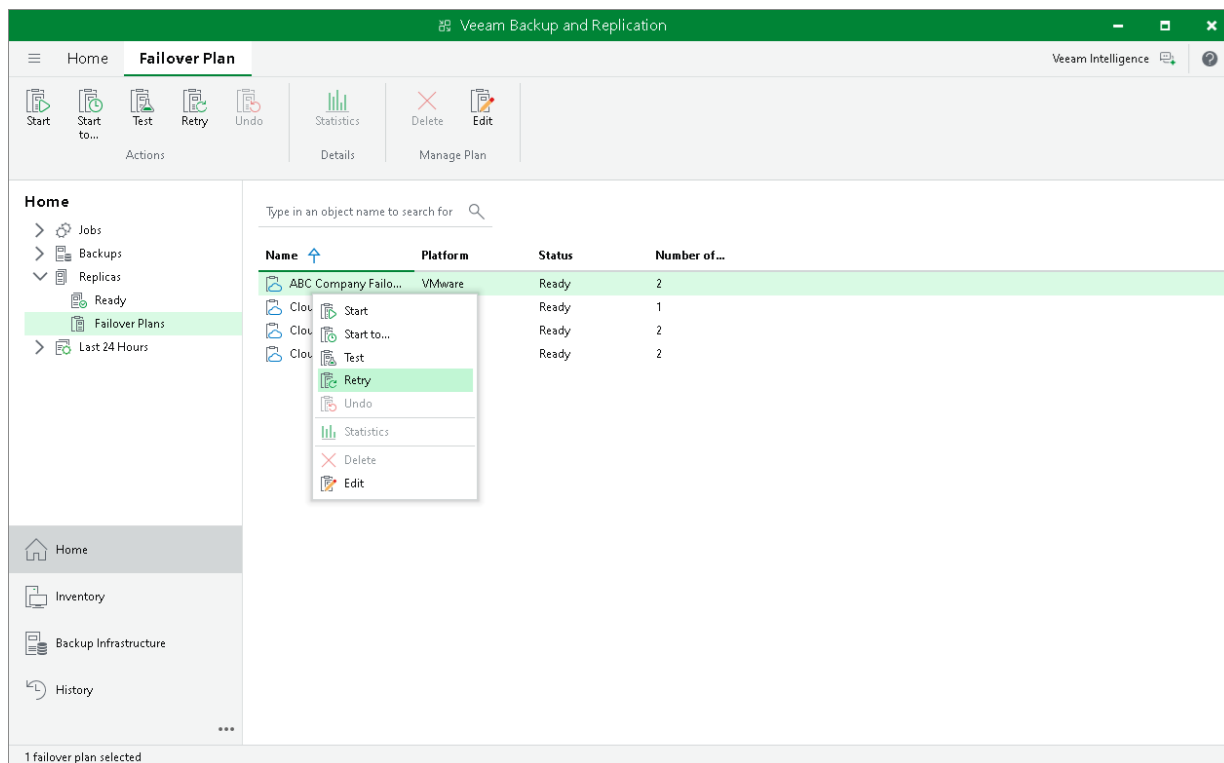
Retrying Cloud Failover Plan

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**.



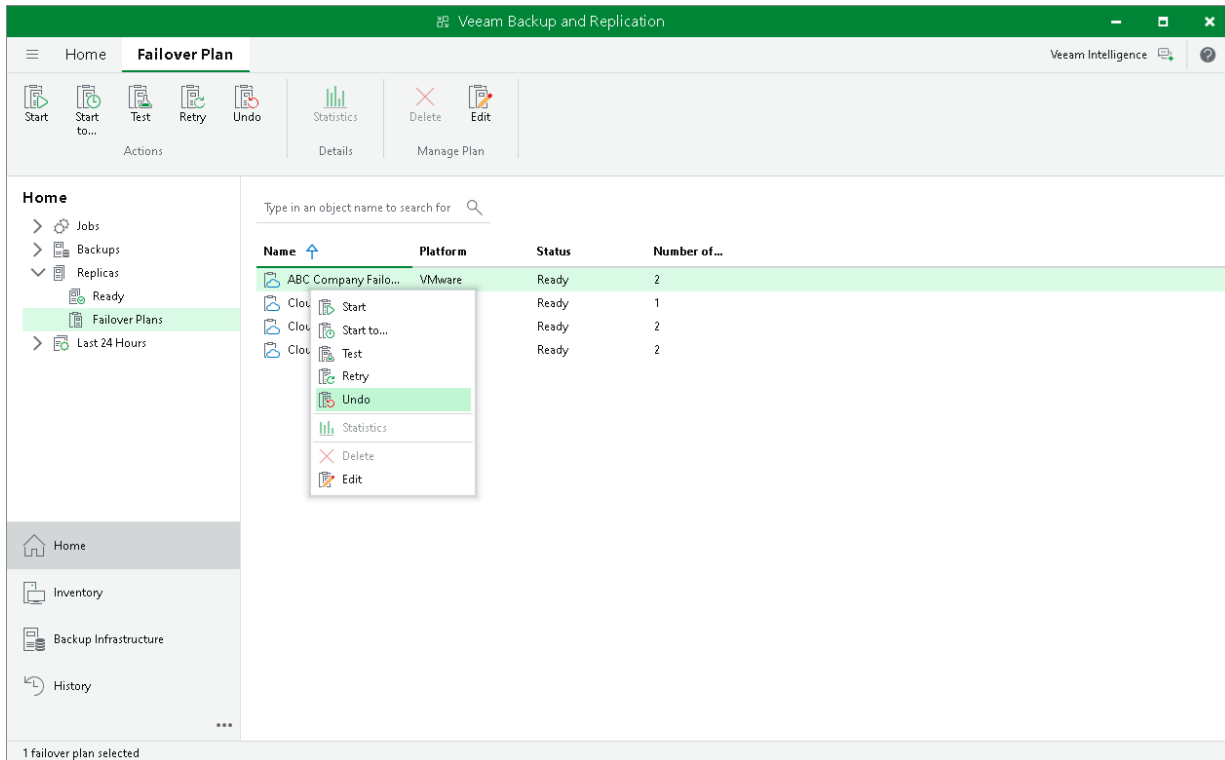
Undoing Failover by Cloud Failover Plan

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

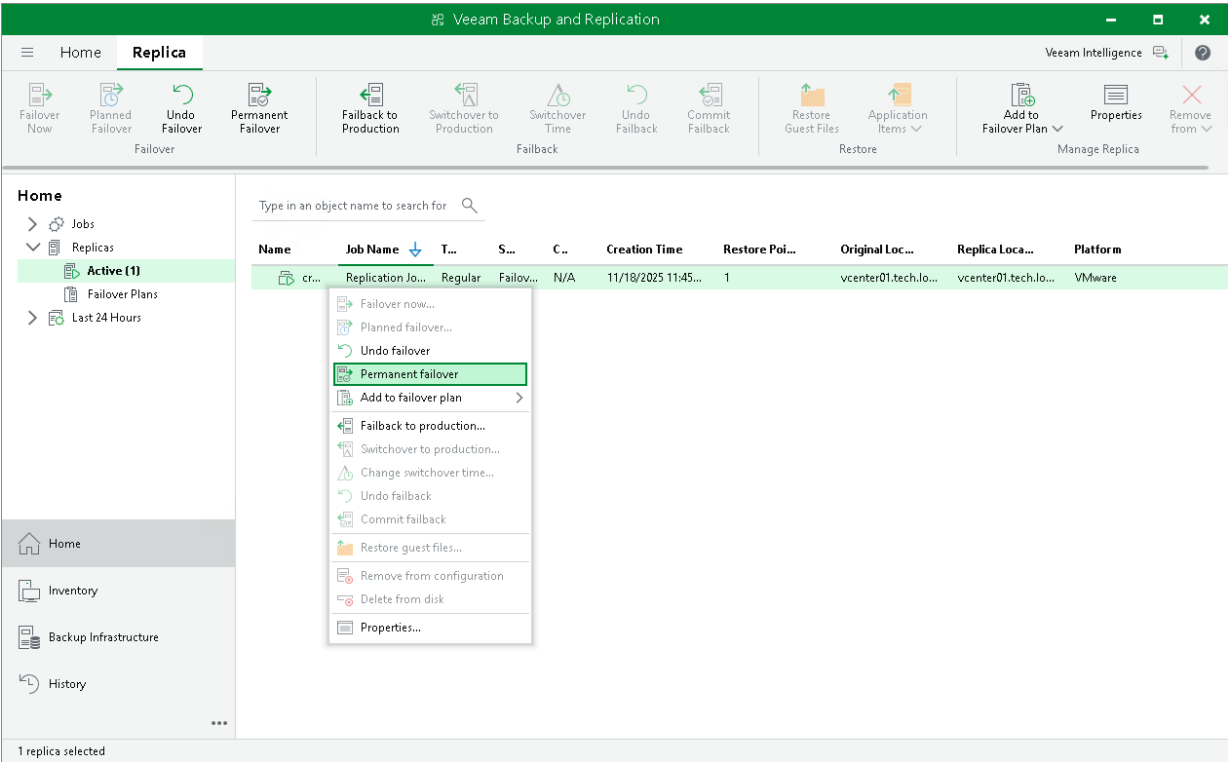
To finalize the full site failover process, you can perform permanent failover. With permanent failover, you can permanently switch from the original VM to a VM replica and use the VM replica on the cloud host as the original VM.

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.



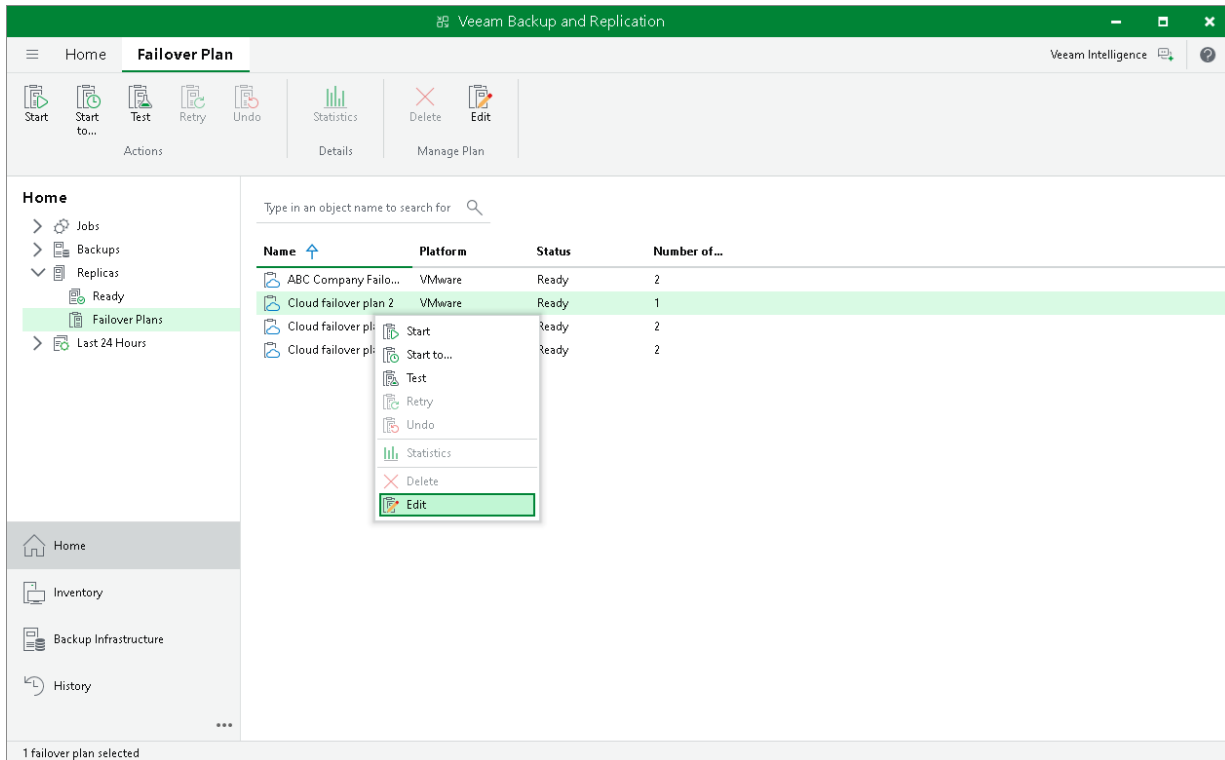
Editing Cloud Failover Plan Settings

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.



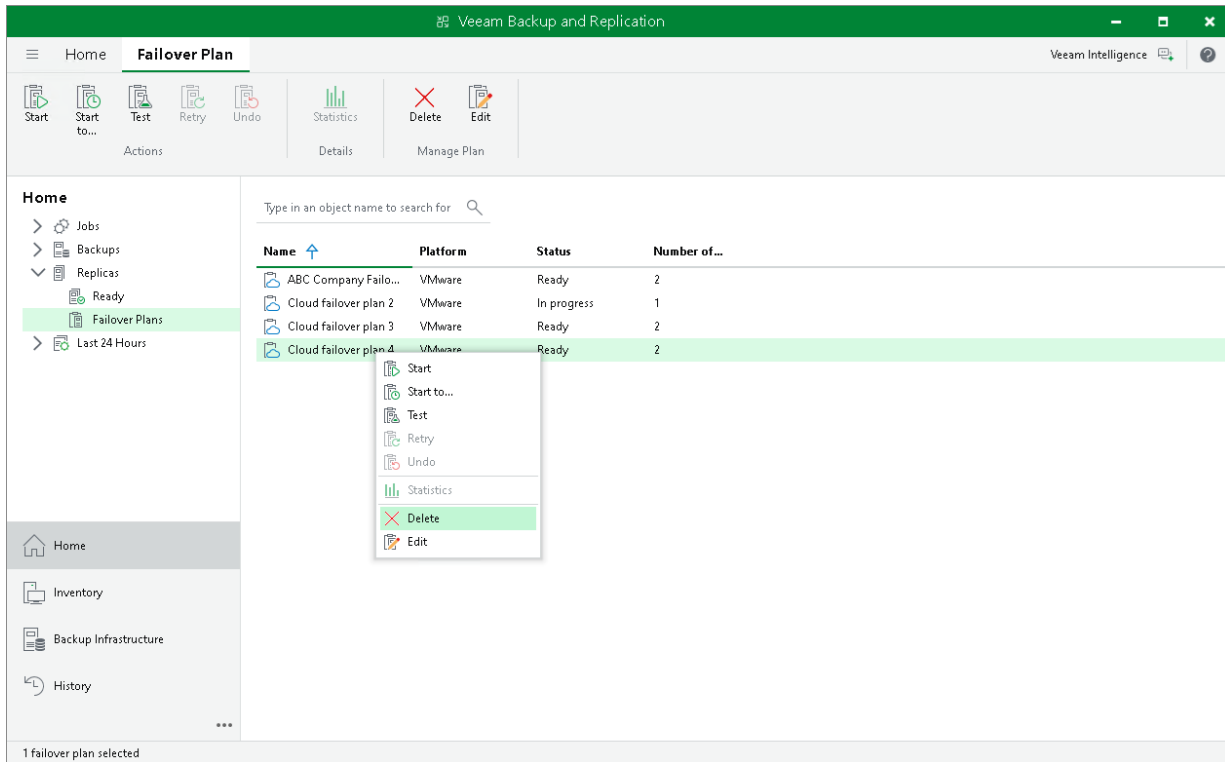
Deleting Cloud Failover Plan

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 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 in the Veeam Backup & Replication User Guide:

- [Replication for VMware vSphere: Failover](#)
- [Replication for Microsoft Hyper-V: Failover](#)

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:
 - Open the **Home** view and select the **Replicas** node. In the working area, select the necessary VM and click **Failover Now** on the ribbon.
 - Open the **Home** view and select the **Replicas** node. In the working area, right-click the necessary VM and select **Failover now**.
 - 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 **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 **Machines to failover** list and click **Point**.

Failover

Machines

Reason

Summary

Machines

Select machines to failover to their replicas. To perform failover to an earlier restore point, click Point to select the desired one.

Machines to failover:

Type in a machine name for instant lookup

Name	Size	Restore point
 filesrv03	174 MB	less than a day ago (10:11 PM T...

+ Add...

⌚ Point...

- Remove

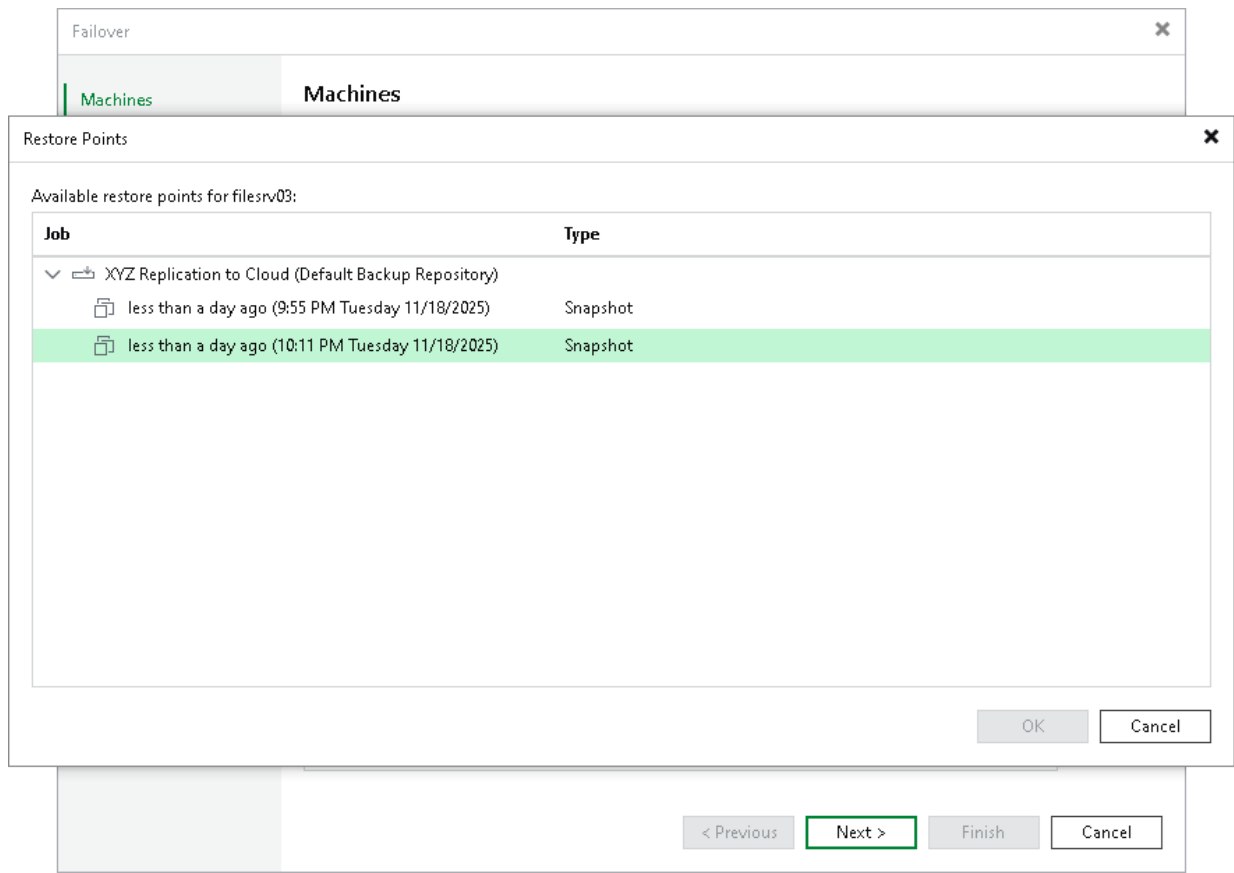
< Previous

Next >

Finish

Cancel

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**.



- At the **Reason** step of the wizard, specify the reason for failing over to the VM replicas for future reference.

The screenshot shows the 'Failover' wizard window. On the left is a sidebar with three items: 'Machines', 'Reason' (highlighted with a green bar), and 'Summary'. The main area is titled 'Reason' and contains the text: 'Type in the reason for performing this restore operation. This information will be logged in the restore sessions history for later reference.' Below this text is a large text input area with the placeholder text 'Recovering failed VMs'. At the bottom left of the main area is a checkbox labeled 'Do not show me this page again'. At the bottom right are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

- 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:

- Launch the failover wizard in one of the following ways:
 - Open the **Home** view and select the **Replicas** node. In the working area, select the necessary VM and click **Failover Now** on the ribbon.

- Open the **Home** view and select the **Replicas** node. In the working area, right-click the necessary VM and select **Failover now**.
- 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 **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 **Machines to failover** list and click **Point**.

The screenshot shows the 'Failover' wizard window with the 'Machines' step selected. The left sidebar contains 'Machines', 'Reason', and 'Summary'. The main area is titled 'Machines' and contains instructions: 'Select machines to failover to their replicas. To perform failover to an earlier restore point, click Point to select the desired one.' Below this is a search bar labeled 'Machines to failover:' with the placeholder text 'Type in a machine name for instant lookup'. A table lists the machines to failover:

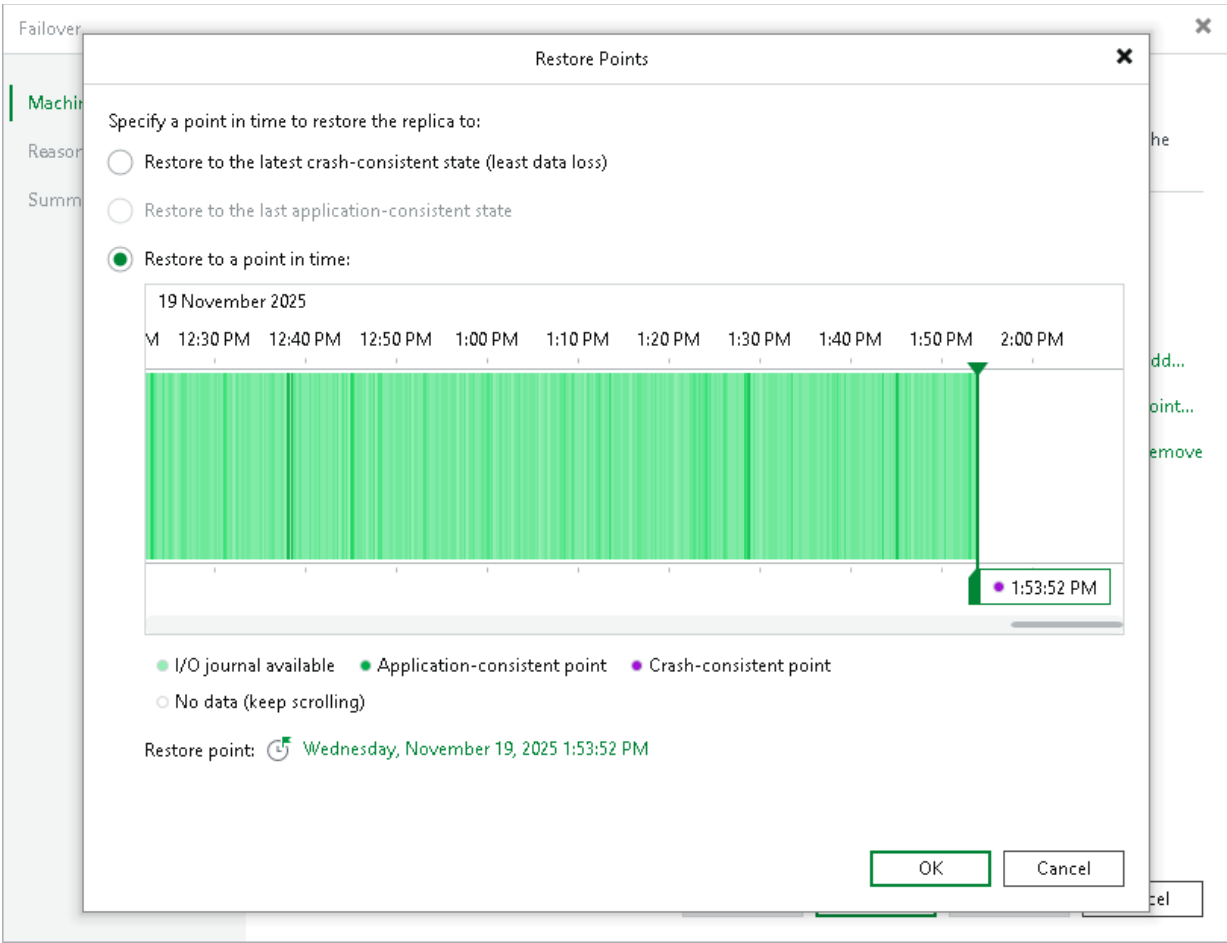
Name	Size	Restore point
webserv03.tech.local	1.93 GB	1:53 PM Wednesday 11/19/2025

To the right of the table are three buttons: '+ Add...', '⌚ Point...', and '- Remove'. At the bottom of the window are four buttons: '< Previous', 'Next >' (highlighted with a green border), 'Finish', and 'Cancel'.

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. The color indicates the amount of data traffic for each time point.



- At the **Reason** step of the wizard, specify the reason for failing over to the VM replicas for future reference.

The screenshot shows the 'Failover' wizard window. On the left is a sidebar with 'Machines', 'Reason' (selected), and 'Summary'. The main area is titled 'Reason' and contains the instruction: 'Type in the reason for performing this restore operation. This information will be logged in the restore sessions history for later reference.' Below this is a large text area with the placeholder text 'Recovering failed VMs'. At the bottom left of the main area is a checkbox labeled 'Do not show me this page again'. At the bottom right are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

- 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.

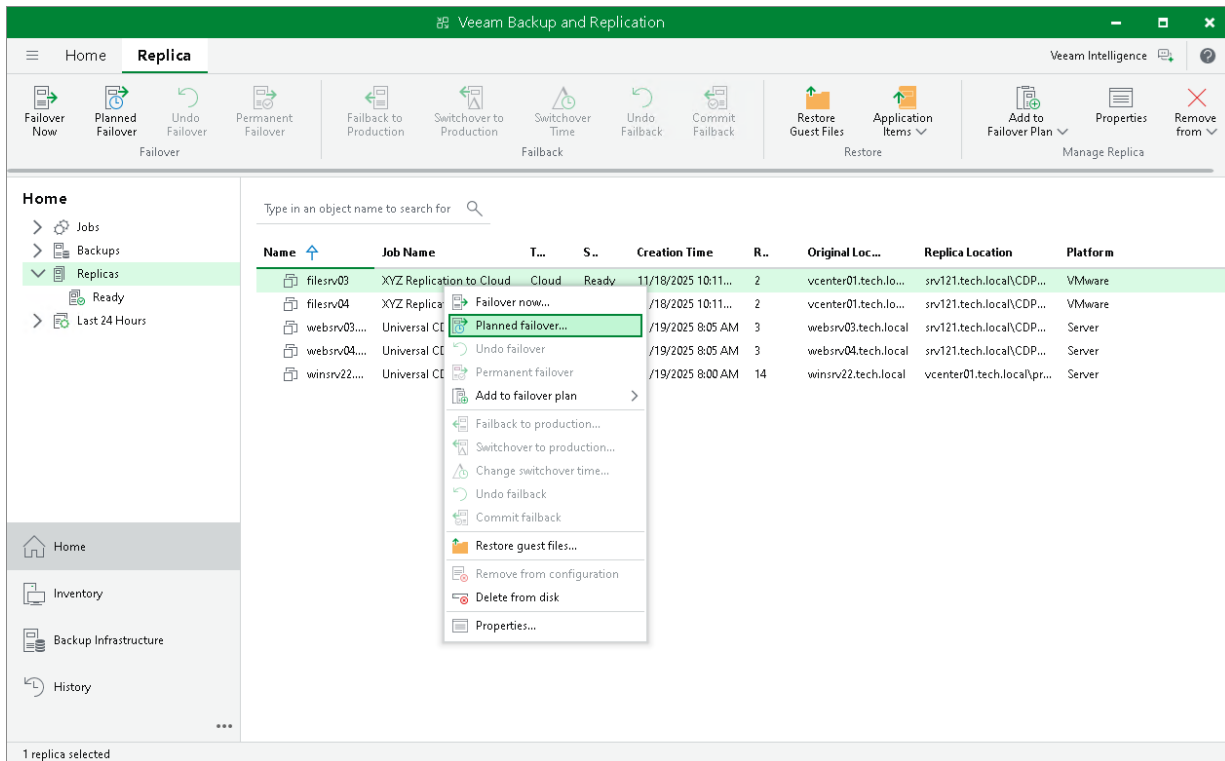
Performing Planned Failover

Within the partial site failover scenario, you can perform planned failover for replicas on the cloud host. This operation is supported for both snapshot-based replicas and CDP replicas. 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 **Planned 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.

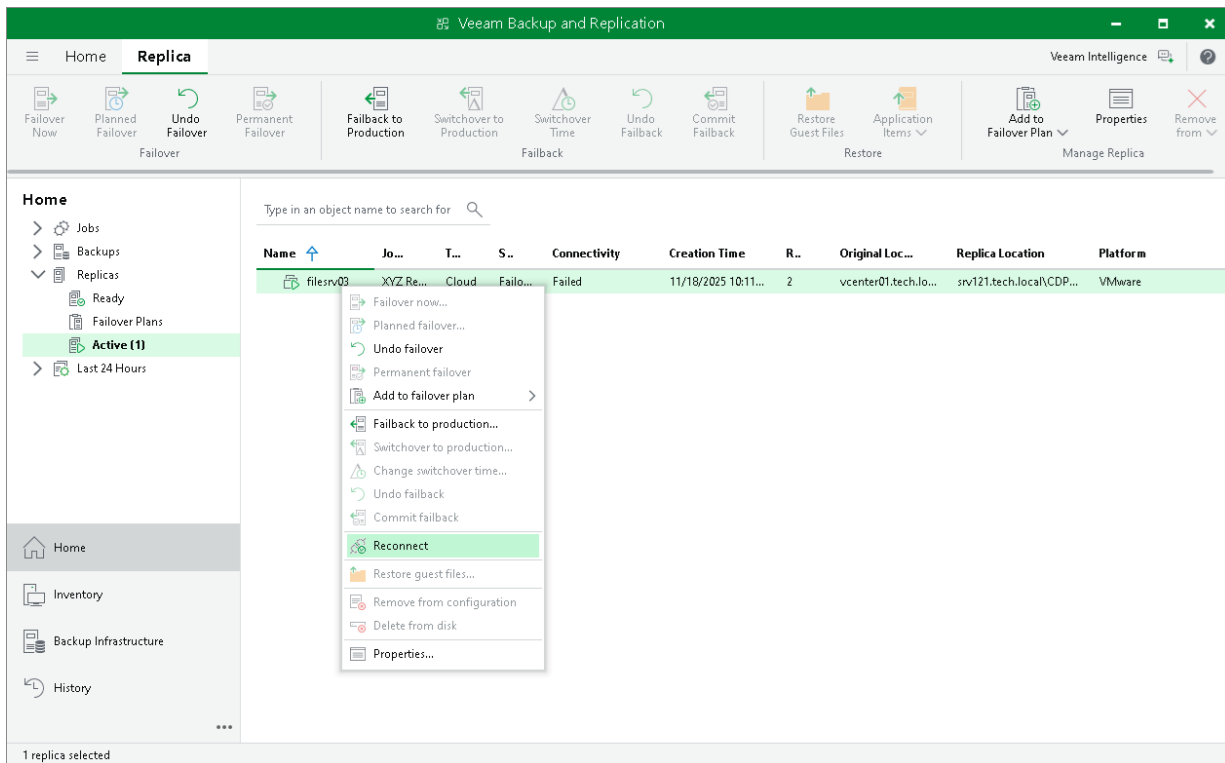
To view the VPN connection state:

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.



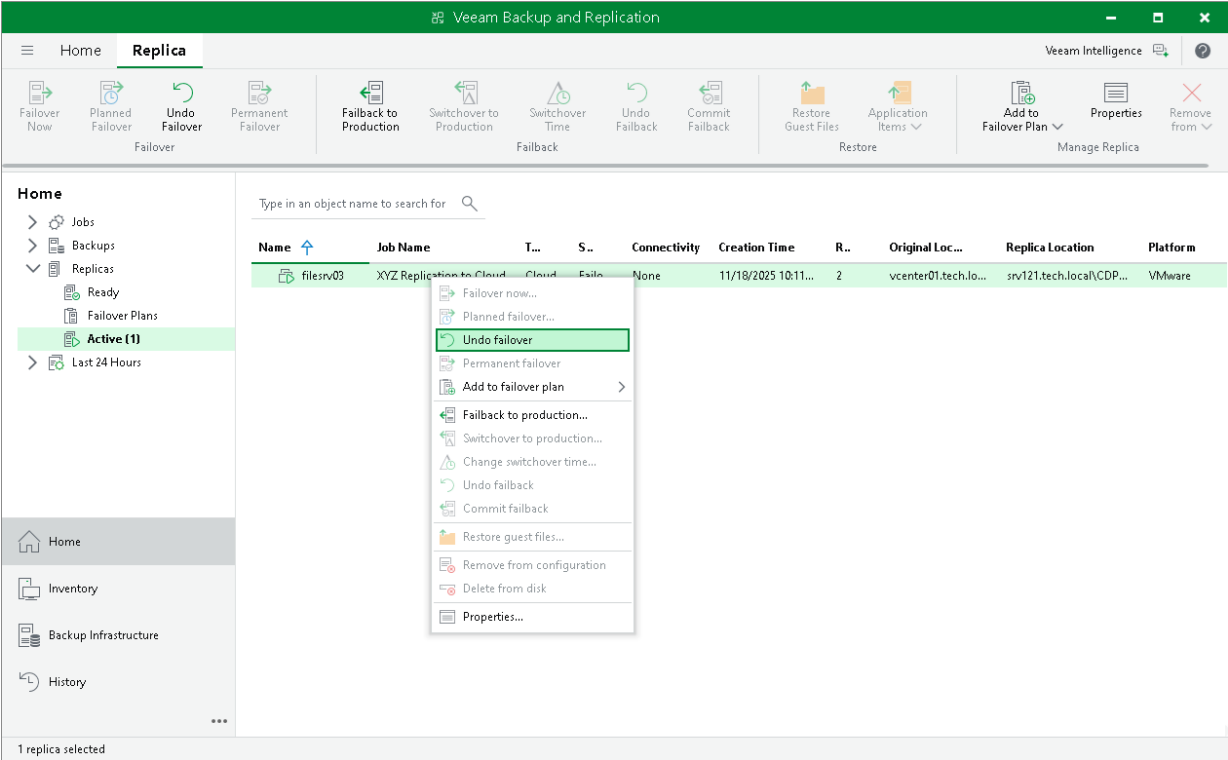
Undoing Partial Site Failover

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.

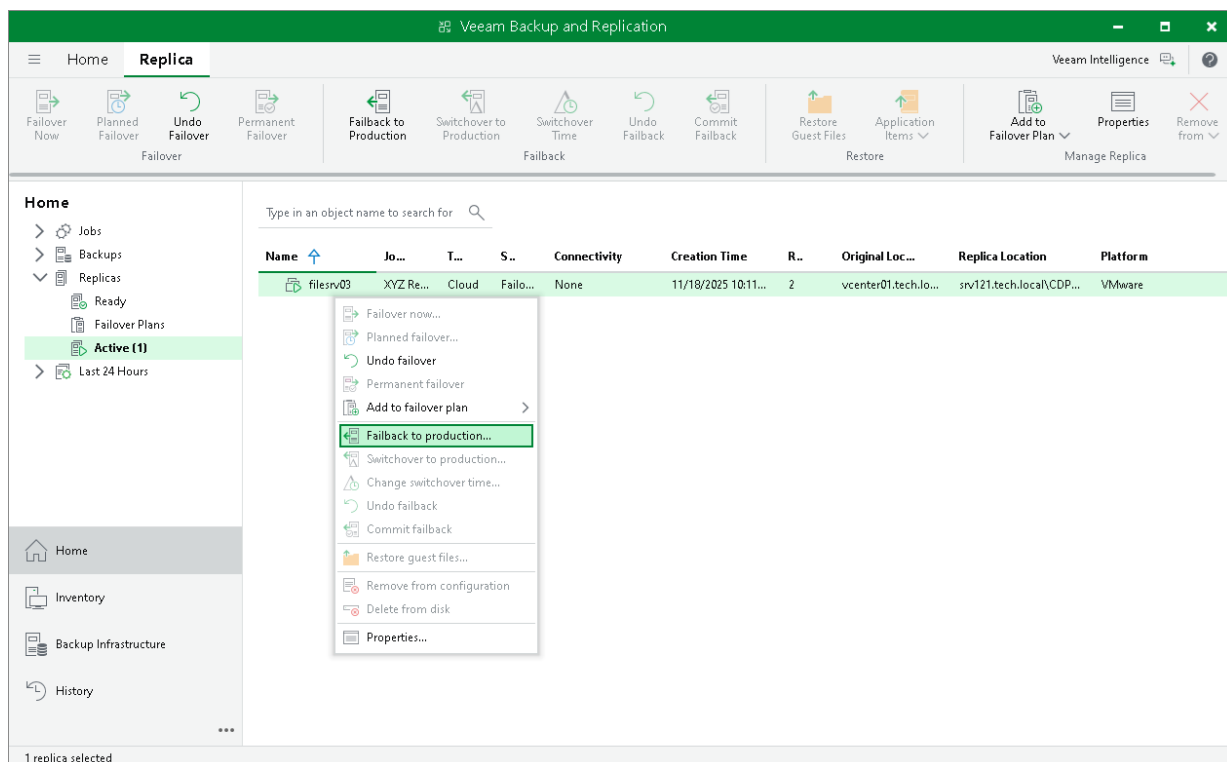


Performing Failback

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 replicas of Microsoft Windows VMs on the cloud host. This operation is supported for both snapshot-based replicas and CDP replicas.

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 Restore](#) 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.
 - [For snapshot-based replicas] Select the necessary restore point from the list.

File Level Restore

Restore point

Select the restore point to restore guest OS files from.

VM name: srv12 Original host: vcenter01.tech.local
VM size: 496 B Mount server: Automatic selection (Windows)

Available restore points:

Created	Type	Backup
less than a day ago (11:45 AM Tuesday 11/18/2...	Snapshot	Replication Job 1

< Previous **Next >** Browse Cancel

- [For CDP replicas] Select the necessary point in time to restore to. The color indicates the amount of data traffic for each time point.

File Level Restore

Restore point

Reason

Summary

Restore point

Select the restore point to restore guest OS files from.

VM name: webserv04.tech.local

Mount server: Automatic selection (Windows)

Restore to a point in time:

19 November 2025

12:40 PM

12:50 PM

1:00 PM

1:10 PM

1:20 PM

1:30 PM

1:40 PM

1:50 PM

2:00 PM

2:10 PM

I/O journal available

Application-consistent point

Crash-consistent point

No data (keep scrolling)

Restore point: Wednesday, November 19, 2025 2:00:52 PM

< Previous

Next >

Browse

Cancel

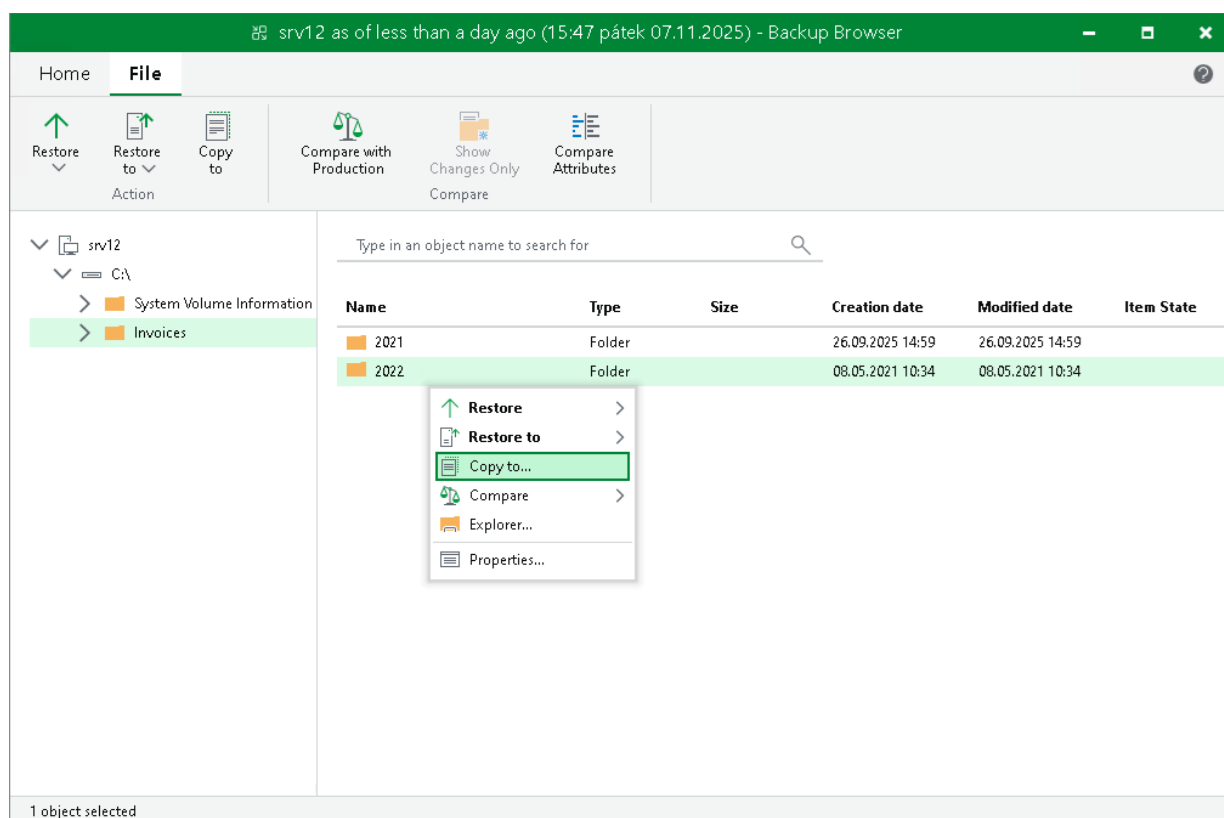
- At the **Reason** step of the wizard, specify the reason for future reference.
- Click **Next**. Then click **Browse**.
- Veeam Backup & Replication will display a file browser with the file system tree of the VM. Right-click the necessary file or folder and select the necessary option.
 - To restore 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.
 - 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**.

- 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.
- 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:

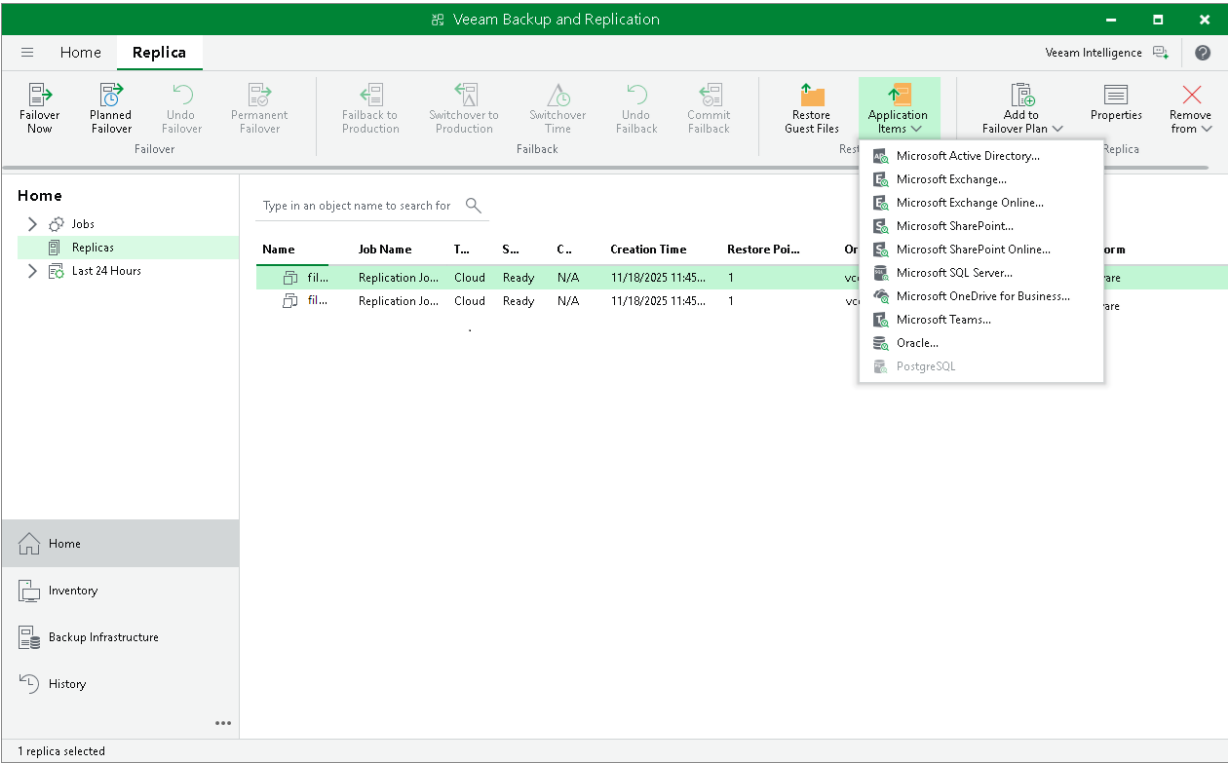
- Microsoft Active Directory
- Microsoft Exchange
- Microsoft SharePoint
- Microsoft SQL Server
- Microsoft OneDrive for Business
- Microsoft Teams
- Oracle
- PostgreSQL

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 Overview](#) section in the Veeam Backup & Replication 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.

The screenshot shows the Veeam Backup and Replication console interface. The top bar is green with the text "Veeam Backup and Replication". Below it is a navigation bar with icons for Backup Job, Replication Job, CDP Policy, Backup Copy, Copy Job, SureBackup Job, Restore, Failover Plan, Import Backup, Export Backup, and Security & Compliance. The main area is divided into a left sidebar and a main content area. The sidebar has a "Home" section with a search bar and a list of items: Jobs, Backups, Replicas (selected), Ready, Failover Plans, Active (1), and Last 24 Hours. The main content area displays a table of replicas.

Name	Job Name	T...	S..	Creation Time	R..	Original Loc...	Replica Location	Platform
filesrv03	XYZ Replication to Cloud	Cloud	Ready	11/18/2025 10:11...	2	vcenter01.tech.lo...	srv121.tech.local\CDP...	VMware
filesrv04	XYZ Replication to Cloud	Cloud	Ready	11/18/2025 10:11...	2	vcenter01.tech.lo...	srv121.tech.local\CDP...	VMware
websrv03...	Universal CDP to Cloud	CDP	Ready	11/19/2025 8:05 AM	3	websrv03.tech.local	srv121.tech.local\CDP...	Server
websrv04...	Universal CDP to Cloud	CDP	Ready	11/19/2025 8:05 AM	3	websrv04.tech.local	srv121.tech.local\CDP...	Server

4 replicas

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 could become permanently inaccessible for a tenant. The tenant may 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**.

Servers Replication Replica Properties

Virtual machine:

filesrv03

Original location:

vcenter01.tech.local\

Files:

Date	Restore Point Size	Status
 2 days ago (22:26 pondělí 03.11.2025)	270,9 KB	OK
 3 days ago (22:26 neděle 02.11.2025)	270,9 KB	OK

Total size: 270,9 KB

OK

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**.

The screenshot shows the Veeam Backup and Replication console interface. The top bar is green with the title 'Veeam Backup and Replication'. Below it is a navigation pane on the left with 'Home' selected. The main area displays a table of VM replicas. A context menu is open over the first replica, with 'Delete from disk' highlighted in green.

Name	Job Name	T...	S...	C...	Creation Time	Restore Poi...	Original Loc...	Replica Loca...	Platform
fil...	Replication Jo...	Cloud	Ready	N/A	11/18/2025 11:45...	1	vcenter01.tech.lo...	vcenter01.tech.lo...	VMware
fil...	Failover now...			N/A	11/18/2025 11:45...	1	vcenter01.tech.lo...	vcenter01.tech.lo...	VMware

Context menu options:

- Failover now...
- Planned failover...
- Undo failover
- Permanent failover
- Add to failover plan
- Failback to production...
- Switchover to production...
- Change switchover time...
- Undo failback
- Commit failback
- Restore guest files...
- Remove from configuration
- Delete from disk**
- Properties...