# Veeam Backup for Microsoft Azure

Version 8

User Guide

April, 2025

**NOTE**

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

# Contents

# Contacting Veeam Software

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

## Customer Support

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

## Company Contacts

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

## Online Support

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

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

# About This Document

This guide is designed for IT professionals who plan to use Veeam Backup for Microsoft Azure. The guide includes system requirements, licensing information and step-by-step deployment instructions. It also provides a comprehensive set of features to ensure easy execution of protection and disaster recovery tasks in Microsoft Azure environments.

# Overview

Veeam Backup for Microsoft Azure is a solution developed for protection and disaster recovery tasks for Microsoft Azure environments: Azure VMs, Azure SQL databases, Cosmos DB accounts and Azure Files. Veeam Backup for Microsoft Azure also allows you to back up and restore Azure Virtual Network configurations.

With Veeam Backup for Microsoft Azure, you can perform the following data protection and disaster recovery operations:

- Create image-level backups and cloud-native snapshots of Azure VMs.
- Create backups of Azure SQL databases.
- [Available only for backup appliances managed by Veeam Backup & Replication] Create backups of Cosmos DB accounts.
- Create cloud-native snapshots of Azure file shares.
- [Available only for backup appliances managed by Veeam Backup & Replication] Create backups of virtual network configurations.
- Create backups of the Veeam Backup for Microsoft Azure configuration database.

To recover backed-up data, you can perform the following operations:

- Restore entire Azure VMs, individual virtual disks, and guest OS files and folders.
- Restore Azure SQL databases.
- [Available only for backup appliances managed by Veeam Backup & Replication] Restore Cosmos DB accounts.
- [Available only for backup appliances managed by Veeam Backup & Replication] Restore entire virtual network configurations of Azure subscriptions.
- [Available only for backup appliances managed by Veeam Backup & Replication] Restore specific items of virtual network configurations of Azure subscriptions.
- Restore individual files of Azure VMs.
- Restore individual files of Azure file shares.
- [Available only for backup appliances managed by Veeam Backup & Replication] Restore entire Azure VMs to AWS, Google Cloud and Nutanix AHV.
- [Available only for backup appliances managed by Veeam Backup & Replication] Perform Instant Recovery of Azure VMs to VMware vSphere and Hyper-V environments, and to Nutanix AHV clusters.
- Restore the Veeam Backup for Microsoft Azure configuration database to the same or another backup appliance.

> **IMPORTANT**
>
> Starting from Veeam Backup for Microsoft Azure version 6.0, Veeam Backup for Microsoft Azure is part of the Veeam Backup & Replication solution, and some features are available only for backup appliances managed by Veeam Backup & Replication. For more information, see Integration with Veeam Backup & Replication.

# Integration with Veeam Backup & Replication

Starting from Veeam Backup for Microsoft Azure version 6.0, Veeam Backup for Microsoft Azure is part of the Veeam Backup & Replication solution. Microsoft Azure Plug-in for Veeam Backup & Replication extends the Veeam Backup & Replication functionality and allows you to add backup appliances to Veeam Backup & Replication. With Microsoft Azure Plug-in for Veeam Backup & Replication, you can manage data protection and recovery operations for all these appliances from a single Veeam Backup & Replication console.

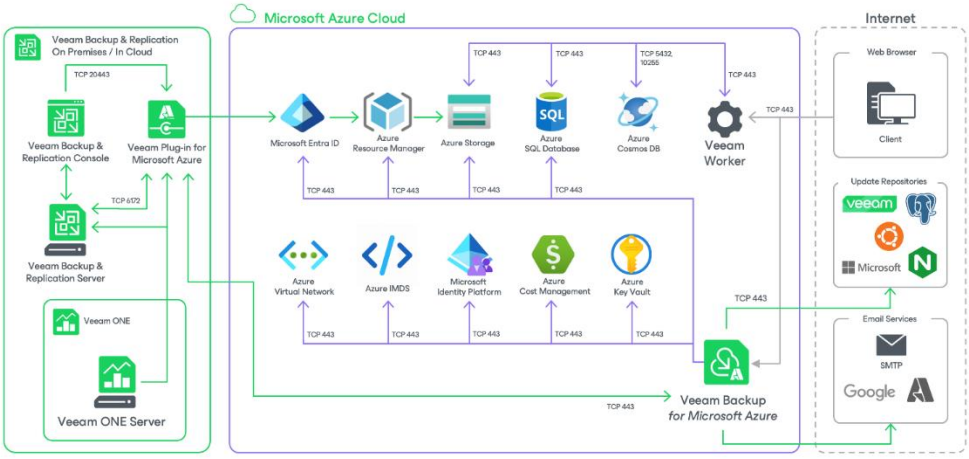
Versions 6.0, 7.0 and 8 come with 2 major features — the ability to create backups of Azure Virtual Network configuration components and the ability to back up Cosmos DB accounts. These features are available only for backup appliances managed by a Veeam Backup & Replication server. To unlock the full functionality, install Microsoft Azure Plug-in for Veeam Backup & Replication on the server and add your appliances to the backup infrastructure.

> **IMPORTANT**
>
> Consider the following:
>
> - If you remove a backup appliance from the backup infrastructure, the following will happen:
>   - You will no longer be able to enable and start the virtual network configuration backup policy.
>   - You will no longer be able to add and start Cosmos DB backup policies. Creating Cosmos DB backups manually will also be unavailable.
> - If the connection between a backup appliance and the backup server is lost for more than 31 days, the appliance will enter the standalone mode, and you will no longer be able to back up virtual network configurations and Cosmos DB accounts.

# Solution Architecture

The Veeam Backup for Microsoft Azure architecture includes the following components:

- Backup server
- Microsoft Azure Plug-In for Veeam Backup & Replication
- Backup appliances
- Backup repositories
- Worker instances
- Additional repositories and tape devices
- Gateway servers



# Backup Server

The backup server is a Windows-based physical or virtual machine on which Veeam Backup & Replication is installed. It is the core component of the backup infrastructure. For more information, see the Veeam Backup & Replication User Guide, section Backup Server.

# Microsoft Azure Plug-In for Veeam Backup & Replication

Plug-in is an architecture component that extends the Veeam Backup & Replication functionality and allows you to add backup appliances to the backup infrastructure. With Microsoft Azure Plug-in for Veeam Backup & Replication, you can manage data protection and disaster recovery operations from the Veeam Backup & Replication console.

# Backup Appliances

The backup appliance is a Linux-based Azure VM on which Veeam Backup for Microsoft Azure is installed.

If you have one or more backup appliances in Microsoft Azure, you can add the appliances to Veeam Backup & Replication, and then use the Veeam Backup & Replication console as the central management console for Veeam Backup for Microsoft Azure operations. For more information on the Veeam Backup & Replication console, see the Veeam Backup & Replication User Guide.

## Backup Appliance Software

The Azure VM running Veeam Backup for Microsoft Azure is deployed with the pre-installed set of software components:

- Ubuntu 22.04 LTS
- ASP.NET Core Runtime 8.0
- PostgreSQL 15
- nginx 1.18
- libpam-google-authenticator 20191231-2
- Veeam Backup for Microsoft Azure installation packages

In case any software updates become available for the backup appliance, these updates can be installed using the Veeam Updater service as described in section Updating Veeam Backup for Microsoft Azure.

## Backup Appliance Functionality

The backup appliance performs the following administrative activities:

- Manages architecture components.
- Coordinates snapshot creation, backup and recovery tasks.
- Controls backup policy scheduling.
- Generates daily reports and email notifications.

## Backup Appliance Components

The backup appliance uses the following components:

- **Backup service** – coordinates data protection and disaster recovery operations.
- **Configuration database** – stores data on the existing backup policies, worker instance configurations, connected Microsoft Azure accounts and so on, as well as information on the available and protected resources collected from Microsoft Azure.
- **Configuration restore service** – allows users to back up and restore the configuration of the backup appliance.
- **Web UI** – provides a web interface that allows users to access the Veeam Backup for Microsoft Azure functionality.
- **Updater service** – allows Veeam Backup for Microsoft Azure to check and install product and package updates.

- **REST API service** — allows users to perform operations with Veeam Backup for Microsoft Azure entities using HTTP requests and standard HTTP methods. For more information, see the Veeam Backup for Microsoft Azure REST API Reference.

# Backup Repositories

A backup repository is a folder in a blob container where Veeam Backup for Microsoft Azure stores image-level backups of Azure VMs, backups of Azure SQL databases, backups of Cosmos DB for PostgreSQL and Cosmos DB for MongoDB accounts for which backup to a repository is enabled, and backup copies of virtual network configurations.

To communicate with a backup repository, Veeam Backup for Microsoft Azure uses **Veeam Data Mover** — the service that runs on a worker instance and that is responsible for data processing and transfer. When a backup policy addresses the backup repository, the Veeam Data Mover establishes a connection with the repository to enable data transfer. To learn how Veeam Backup for Microsoft Azure communicates with backup repositories, see Managing Backup Repositories.

> **IMPORTANT**
>
> Backup files are stored in backup repositories in the native Veeam format and must be modified neither manually nor by 3rd party tools. Otherwise, Veeam Backup for Microsoft Azure may fail to restore the backed-up data.

## Encryption on Backup Repositories

For enhanced data security, Veeam Backup for Microsoft Azure allows you to enable encryption at the repository level. Veeam Backup for Microsoft Azure encrypts backup files stored in backup repositories the same way as Veeam Backup & Replication encrypts backup files stored in backup repositories. To learn what algorithms Veeam Backup & Replication uses to encrypt backup files, see the Veeam Backup & Replication User Guide, section Data Encryption.

To learn how to enable encryption at the repository level, configure the repository settings as described in section Adding Backup Repositories Using Web UI, and choose whether you want to encrypt data using a password or using an Azure Key Vault cryptographic key.

## Limitations for Repositories

To use a blob container as a target location for backups, you must connect to an Azure storage account in which this blob container resides, as described in section Adding Backup Repositories Using Web UI.

Veeam Backup for Microsoft Azure supports the following types of Azure storage accounts:

| Storage Account Type | Supported Performance Tiers | Supported Access Tiers |
|---|---|---|
| General-purpose V2 | Standard | Hot, Cool, Archive |
| BlobStorage | Standard | Hot, Cool, Archive |

**IMPORTANT**

Consider the following limitations for storage accounts:

- Veeam Backup for Microsoft Azure does not support creation of backup repositories in storage accounts with enabled blob soft delete option.
- Veeam Backup for Microsoft Azure does not support creation of backup repositories in the Cold access tier. For more information on access tiers for blob data, see Microsoft Docs.
- Due to Microsoft Azure limitations, Veeam Backup for Microsoft Azure does not support creation of archive repositories in storage accounts with the Zone-redundant storage (ZRS), Geo-zone-redundant storage (GZRS) or Read-access geo-zone-redundant storage (RA-GZRS) redundancy option enabled. For more information, see Microsoft Docs.

# Worker Instances

A worker instance is an auxiliary Linux-based virtual machine that is responsible for the interaction between the backup appliance and other Veeam Backup for Microsoft Azure components. Worker instances process backup workload and distribute backup traffic when transferring data to backup repositories.

## Worker Instance Components

A worker instance uses the following services:

- **Veeam Data Mover** — the service that performs data processing tasks. During backup, Veeam Data Mover retrieves data of protected Azure resources and transfers it to backup repositories. During restore, Veeam Data Mover transfers backed-up data from backup repositories to the target location.
- **File-level recovery browser** — the web service that allows you to find and save files and folders of a backed-up Azure VM to a local machine or to the original location. The file-level recovery browser is installed automatically on every worker instance that is launched for file-level recovery.

  For more information on recovering files of Azure VMs using the file-level recovery browser, see Performing File-Level Recovery.
- **Azure Queue Storage** — an Azure service used for communication between the worker instance and a backup appliance. For more information on Azure Queue Storage, see Microsoft Docs.

> **NOTE**
>
> By design, Veeam Backup for Microsoft Azure installs the `unattended-upgrades` package on every launched worker instance. This package automatically sends requests to the Ubuntu Security Repository (security.ubuntu.com) to get and install security updates on the worker instance. To reconfigure or disable these updates, open a support case.

## Security Certificates for Worker Instances

During the file-level recovery process, Veeam Backup for Microsoft Azure uses self-signed TLS certificates to establish secure communication between the web browser on a user workstation and the file-level recovery browser running on a worker instance. A self-signed certificate is generated automatically on the worker instance when the recovery session starts.

# How Worker Instances Work

Veeam Backup for Microsoft Azure automatically launches worker instances to process Azure VMs, Azure SQL databases, Cosmos DB for PostgreSQL clusters and Cosmos DB for MongoDB accounts when performing a backup or restore operation, and keeps the instances running for the duration of the operation. Veeam Backup for Microsoft Azure launches one worker instance per each Azure resource specified in a backup policy or restore task.

To minimize cross-region traffic charges and to speed up the data transfer, depending on the performed operation, Veeam Backup for Microsoft Azure launches worker instances in the following locations:

| Operation | Worker Instance Location | Default Worker Instance Size |
|---|---|---|
| Creating image-level backups of Azure VMs | Azure region in which a processed Azure VM resides | *Standard_F2s_v2*, 2 CPU, 4 GB RAM |

| Operation | Worker Instance Location | Default Worker Instance Size |
|---|---|---|
| Creating backups of Azure SQL databases | Azure region in which a SQL Server hosting the processed database resides | |
| Creating backups of Cosmos DB for PostgreSQL clusters and Cosmos DB for MongoDB accounts | Azure region in which a Cosmos DB account managing the processed database resides | |
| Azure file share indexing | Azure region in which a processed file share resides | |
| Creating archived image-level backups of Azure VMs | Azure region in which an archive backup repository storing backed-up data resides | *Standard_E2_v5*, 2 CPU 16 GB RAM |
| Creating archived backups of Azure SQL databases, Cosmos DB for PostgreSQL clusters and Cosmos DB for MongoDB accounts | Azure region in which an archive backup repository storing backed-up data resides | |
| Performing health check for created restore points | Azure region in which a target backup repository resides | *Standard_F2s_v2*, 2 CPU, 4 GB RAM |
| Applying retention policy settings to created restore points | Azure region in which a backup repository with backed-up data resides | |
| Repository synchronization | Azure region in which a backup repository with backed-up data resides | |
| Restoring Azure VMs, Azure SQL databases, Cosmos DB for PostgreSQL clusters and Cosmos DB for MongoDB accounts | Azure region in which the restored Azure VM, SQL Server hosting the restored database or Cosmos DB account managing the restored database resides | |
| Restoring individual virtual disks of Azure VMs | Azure region in which the restored virtual disk resides | |

| Operation | Worker Instance Location | Default Worker Instance Size |
|---|---|---|
| File-level restore from cloud-native snapshots | Azure region in which a cloud-native snapshot resides | |
| File-level restore from image-level backups | Azure region in which a backup repository storing backed-up data resides | |

Worker instances are launched based on worker configurations and profiles. For more information, see Managing Worker Instances.

> **IMPORTANT**
>
> Veeam Backup for Microsoft Azure requires 2 Veeam storage accounts for each Azure region where worker instances are launched during backup and restore operations: one account is used to store worker and Volume Shadow Copy Service (VSS) binary files, while another account ensures communication between the backup appliance and the worker instances using the Azure Queue Storage messaging service. When launching a worker instance in an Azure region, Veeam Backup for Microsoft Azure checks whether these 2 storage accounts exist in the region — if not, Veeam Backup for Microsoft Azure creates these storage accounts automatically. Since Veeam Backup for Microsoft Azure detects Veeam storage accounts by the *Veeam backup appliance ID* tag assigned to these accounts, it is not recommended that you modify tags of Veeam storage accounts manually.

## Requirements for Worker Instances

By default, Veeam Backup for Microsoft Azure creates a new network configuration for each Azure region in which it launches worker instances. However, you can add custom worker configurations to provide network settings that will be used to launch worker instances in a specific region. In this case, for every Azure region where worker instances will be launched, you must specify a virtual network and a subnet to which the worker instances will be connected. You can also specify a security group that will be associated with the specified subnet. To learn how to configure network settings for worker instances, see Adding Worker Configurations.

# Additional Repositories and Tape Devices

Additional repositories and tape devices are any repositories where Veeam Backup & Replication keeps and stores copies of Azure VMs backups. For more information, see the Veeam Backup & Replication User Guide, sections Backup Repository and Machines Backup to Tape.

# Gateway Servers

The gateway server is an auxiliary backup infrastructure component that provides access from the backup server to the repositories. By default, the role of a gateway server is assigned to the backup server.

Gateway server caches data when you copy backups and restore application items, which helps you decrease the amount of traffic being sent over the network and reduce data transfer costs. For more information on caching data, see the Veeam Backup & Replication User Guide, section Cache.

# Protecting Azure VMs

To produce cloud-native snapshots and image-level backups of Azure VMs, Veeam Backup for Microsoft Azure runs schedule-based and SLA-based backup policies:

- A schedule-based backup policy is a collection of settings that define the way backup operations are performed: what data to back up, where to store backups, when to start the backup process, and so on. When you configure a schedule-based backup policy, your data is protected according to a specific backup schedule (at an exact date and time).

  After Veeam Backup for Microsoft Azure finishes running a schedule-based backup policy, you can track the status of data protection for each Azure VM included in the policy in terms of whether the backup operation completed successfully.

- An SLA-based backup policy is a collection of settings that automate the way backup operations are performed: what data to back up, how frequently to run the backup process, what region-specific repositories to use to store backups, how many restore points should be created in time to meet SLA requirements, and so on. When you configure an SLA-based backup policy, your data is protected according to a periodic backup schedule (regularly, within a backup window).

  After Veeam Backup for Microsoft Azure finishes running an SLA-based backup policy, you can track the status of data protection for each Azure VM included in the policy in terms of whether the target SLA was met (in addition to monitoring the backup operation status).

Veeam Backup for Microsoft Azure does not install agent software to back up Azure VM data — it uses native Microsoft Azure capabilities instead. During every backup session, Veeam Backup for Microsoft Azure creates a cloud-native snapshot for each Azure VM added to a backup policy. The cloud-native snapshot is further used to create an image-level backup of the Azure VM. For more information on how VM backup works, see VM Backup.

## How To Protect Azure VMs

To create a backup policy, perform the following steps:

1. Check limitations and prerequisites.
2. Specify service accounts to access Azure services and resources.
3. [Optional] Add backup repositories to store backed-up data.
4. [Optional] Configure worker instance settings to launch workers while processing Azure VM data.
5. [Optional] Configure global retention settings for obsolete snapshots and session records.
6. [Optional] Configure email notification settings for automated delivery of backup policy results and daily reports.
7. Do either of the following:
   - To create a schedule-based backup policy, complete the Add VM Policy wizard.
   - To create an SLA-based backup policy:
     i. Complete the Add SLA Template wizard.
     ii. Complete the Add Storage Template wizard.
     iii. Complete the SLA-Based Policy wizard.

> **NOTE**
>
> Veeam Backup for Microsoft Azure prioritizes SLA-based backup policies over schedule-based backup policies. If an Azure VM is included into both a schedule-based and an SLA-based backup policy, it will be processed by the SLA-based backup policy only.

# VM Backup

Veeam Backup for Microsoft Azure performs VM backup in the following way:

1. Veeam Backup for Microsoft Azure creates snapshots of virtual disks that are attached to the processed Azure VM.

   Disk snapshots are assigned Azure tags upon creation. Values of Azure tags contain encrypted metadata that helps Veeam Backup for Microsoft Azure identify the related disk snapshots and treat them as a single unit — a cloud-native snapshot. For this reason, you must not delete any Azure tags whose names start with the word *veeam*.

> **IMPORTANT**
>
> Due to Microsoft Azure limitations, you can apply up to 50 tags directly to a subscription. That is why Veeam Backup for Microsoft Azure is able to create a snapshot only if the tag limit is not reached for the subscription to which the processed Azure VM belongs. If the limit is reached, the operation will fail with a serialization error. For more information on subscription limits, see Microsoft Docs.

2. If you enable image-level backup for the backup policy, Veeam Backup for Microsoft Azure performs the following operations:

   a. Launches a worker instance in an Azure region in which the processed Azure VM resides.

      By default, Veeam Backup for Microsoft Azure launches worker instances using virtual networks created automatically. However, you can add specific worker configurations. For more information, see Managing Worker Instances.

   b. Synchronizes data between the backup repository and the configuration database to ensure data consistency.

   c. Reads data from the created cloud-native snapshot using a shared access signature (SAS) URI, compresses the data and transfers it to the target backup repository, and stores it in the native Veeam format.

      To reduce the amount of data read from snapshots, Veeam Backup for Microsoft Azure uses the changed block tracking (CBT) mechanism: during incremental backup sessions, Veeam Backup for Microsoft Azure compares the new cloud-native snapshot with the previous one and reads only those data blocks that have changed since the previous backup session. For more information, see Changed Block Tracking.

> **NOTE**
>
> Veeam Backup for Microsoft Azure encrypts and compresses data saved to backup repositories. For more information on data encryption, see Data Encryption.

   d. Deallocates the worker instance when the backup session completes.

3. If you enable the backup archiving mechanism, Veeam Backup for Microsoft Azure performs the following operations:

   a. Launches a worker instance in an Azure region in which the target backup repository resides.

   b. Retrieves data from the backup repository and transfers it to the target archive repository.

   c. Deallocates the worker instance when the archive session completes.

NOTE

Veeam Backup for Microsoft Azure stores the backed-up data depending on the type of the virtual disk attached to the protected Azure VM:

- Snapshots created for managed virtual disks are saved to the same Azure region and resource group to which the Azure VM belongs.
- Snapshots created for unmanaged virtual disks are saved to the same Azure storage account where these disks reside.
- Backups created for managed and unmanaged virtual disks are saved to the target repository.

For more information on Azure virtual disk types, see Microsoft Docs.

# Snapshot Chain

During every backup session, Veeam Backup for Microsoft Azure creates a cloud-native snapshot of each Azure VM added to a backup policy. The cloud-native snapshot itself is a collection of point-in-time snapshots of virtual disks that Veeam Backup for Microsoft Azure creates using native Microsoft Azure capabilities.

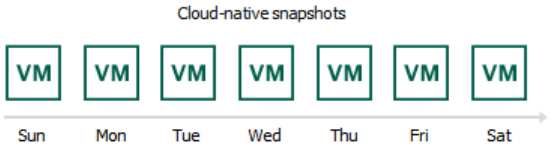
A sequence of cloud-native snapshots created during a set of backup sessions makes up a snapshot chain. Veeam Backup for Microsoft Azure builds the snapshot chain in the following way:

1. During the first backup session, Veeam Backup for Microsoft Azure creates a snapshot of all Azure VM data and saves it in a locally-redundant (LRS) standard HDD storage. This snapshot becomes a starting point in the snapshot chain.
2. During subsequent backup sessions, Veeam Backup for Microsoft Azure creates snapshots with only those data blocks that have changed since the previous backup session.

   The size of each snapshot depends on the total used size of all virtual disks attached to the processed Azure VM. For more information on how incremental Azure VM snapshots work, see Microsoft Docs.

Each cloud-native snapshot in the snapshot chain contains metadata. Metadata includes information about the protected Azure VM, the backup policy that created the snapshot, and the number of snapshots in the chain. Veeam Backup for Microsoft Azure uses metadata to identify outdated snapshots, to load the configuration of source Azure VMs during recovery operations, and so on.

Cloud-native snapshots act as independent restore points for backed-up Azure VMs. If you remove any snapshot, it will not break the snapshot chain — you will still be able to roll back your data to any existing restore point.




The number of cloud-native snapshots kept in the snapshot chain is defined by retention policy settings. For more information, see VM Snapshot Retention.

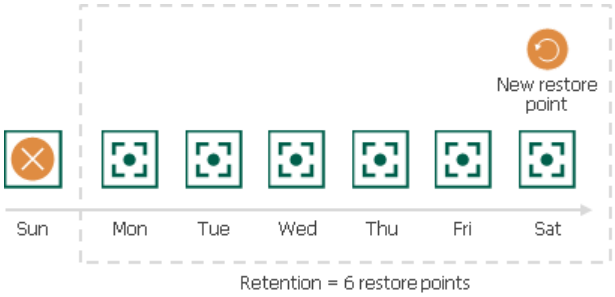
## VM Snapshot Retention

For cloud-native snapshots, Veeam Backup for Microsoft Azure retains the number of latest restore points defined in backup scheduling settings as described in section Creating VM Backup Policies.

During every successful backup session, Veeam Backup for Microsoft Azure creates a new restore point. If Veeam Backup for Microsoft Azure detects that the number of restore points in the snapshot chain exceeds the retention limit, it removes the earliest restore point from the chain. For more information on the snapshot deletion process, see Microsoft Docs.

**IMPORTANT**

Due to the CBT mechanism limitations, Veeam Backup for Microsoft Azure permanently retains in the snapshot chain 2 cloud-native snapshots of each processed Azure VM for snapshots used by schedule-based backup policies to create image-level backups. To learn how the CBT mechanism works, see Changed Block Tracking.




**NOTES**

- Consider that Veeam Backup for Microsoft Azure does not apply retention policy settings to cloud-native snapshots created manually. To learn how to remove these snapshots, see sections Managing VM Data and Managing Azure Files Data.
- Due to Microsoft Azure limitations, Veeam Backup for Microsoft Azure does not support retention of locked Azure VM snapshots. For more information on the lock feature, see Microsoft Docs.

# Backup Chain

If you enable image-level backups for a backup policy, Veeam Backup for Microsoft Azure creates a new backup in a backup repository during every backup session. A sequence of backups created during a set of backup sessions makes up a backup chain.

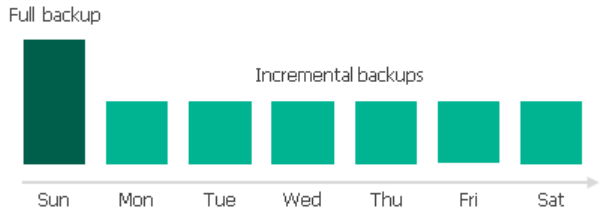
The backup chain includes backups of the following types:

- **Full** — a full backup stores a copy of the full Azure VM image.
- **Incremental** — incremental backups store incremental changes of the Azure VM image.

To create a backup chain for an Azure VM protected by a backup policy, Veeam Backup for Microsoft Azure implements the forever forward incremental backup method:

1. During the first backup session, Veeam Backup for Microsoft Azure copies the full Azure VM image and creates a full backup in a backup repository. The full backup becomes a starting point in the backup chain.

2. During subsequent backup sessions, Veeam Backup for Microsoft Azure copies only those data blocks that have changed since the previous backup session, and stores these data blocks to incremental backups in the backup repository. The content of each incremental backup depends on the content of the full backup and the preceding incremental backups in the backup chain.




Full and incremental backups act as restore points for backed-up Azure VMs that let you roll back your data to the necessary state. To recover an Azure VM to a specific point in time, the chain of backups created for the VM must contain a full backup and a set of incremental backups dependent on the full backup.

If some backup in the backup chain is missing, you will not be able to roll back to the necessary state. For this reason, you must not delete individual backups from the backup repository manually. Instead, you must specify retention policy settings that will let you maintain the necessary number of backups in the backup repository. For more information, see VM Backup Retention.

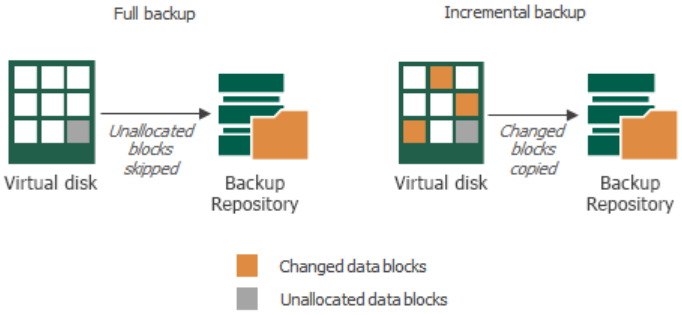
## Changed Block Tracking

The changed block tracking (CBT) mechanism allows Veeam Backup for Microsoft Azure to reduce the amount of data read from cloud-native snapshots, and to increase the speed and efficiency of incremental backups:

- During a full backup session, Veeam Backup for Microsoft Azure reads only written data blocks, while unallocated data blocks are filtered out.
- During an incremental backup session, Veeam Backup for Microsoft Azure reads only those data blocks that have changed since the previous backup session.

To detect unallocated and changed data blocks, CBT relies on Azure Compute APIs.

- During the first (full) backup session, Veeam Backup for Microsoft Azure creates a cloud-native snapshot of an Azure VM. Veeam Backup for Microsoft Azure sends API requests to access the content of the snapshot and to detect unallocated data blocks.
- During subsequent sessions, new cloud-native snapshots are created. Veeam Backup for Microsoft Azure sends API requests to access and to compare the content of the snapshot created during the previous backup session and the snapshot created during the current backup session. This allows Veeam Backup for Microsoft Azure to detect data blocks that have changed since the previous backup session.




To allow the CBT mechanism to be used when processing Azure VM data by a backup policy, the number of snapshots to keep in a snapshot chain must be enough to ensure that the cloud-native snapshot created during the previous backup session has not been removed from the chain by the retention policy before the next backup session runs. For more information on configuring snapshot retention settings, see Creating Backup Policies.

> **NOTE**
>
> The CBT mechanism is optional for SLA-based backup policies. For more information, see Temporary Restore Points.

Consider the following example. You want a schedule-based backup policy to daily create both image-level backups and cloud-native snapshots: cloud-native snapshots must be created at 7:00 AM, 9:00 AM, 11:00 AM 1:00 PM, 3:00 PM and 5:00 PM; image-level backups must be created at 7:00 AM and 5:00 PM. In this case, you must set the **Snapshots to keep** value to minimum 5. Veeam Backup for Microsoft Azure will run the backup policy the following way:

1. At 7:00 AM, a backup session will create a cloud-native snapshot, and then use this snapshot to create an image-level backup.
2. From 9:00 AM to 3:00 PM, backup sessions will create only cloud-native snapshots.
3. After a backup session runs at 5:00 PM, the first cloud-native snapshot (created at 7:00 AM) will still be present in the snapshot chain until the next backup session.

## Archive Backup Chain

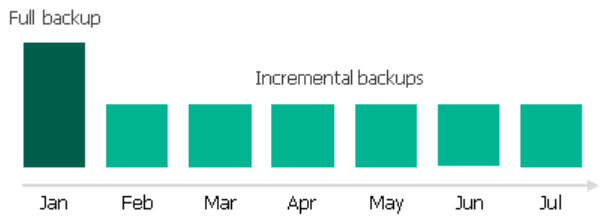
If you enable backup archiving for a backup policy, Veeam Backup for Microsoft Azure creates a new backup in an archive repository during every archive session. A sequence of backups created during a set of archive sessions makes up an archive backup chain.

The archive backup chain includes backups of the following types:

- **Full** — a full archive backup stores a copy of the full Azure VM image.
- **Incremental** — incremental archive backups store incremental changes of the Azure VM image.

To create an archive backup chain for an Azure VM protected by a backup policy, Veeam Backup for Microsoft Azure implements the forever forward incremental backup method:

1. During the first archive session, Veeam Backup for Microsoft Azure detects backed-up data that is stored in the full backup and all incremental backups existing in the backup chain, creates a full archive backup with all the data, and copies this backup to the archive repository. The full archive backup becomes a starting point in the archive chain.
2. During subsequent archive sessions, Veeam Backup for Microsoft Azure checks the backup chain to detect data blocks that have changed since the previous archive session, creates incremental archive backups with only those changed blocks, and copies these backups to the archive repository. The content of each incremental archive backup depends on the content of the full archive backup and the preceding incremental archive backups in the archive backup chain.




Full and incremental archive backups act as restore points for backed-up Azure VMs that let you roll back your data to the necessary state. To recover an Azure VM to a specific point in time, the chain of backups created for the VM must contain a full archive backup and a set of incremental archive backups.

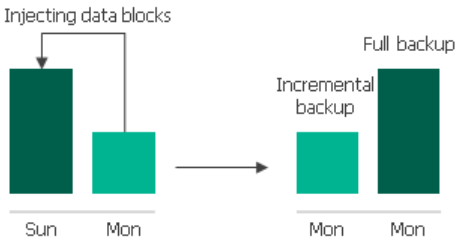
If some backup in the archive backup chain is missing, you will not be able to roll back to the necessary state. For this reason, you must not delete individual backups from the archive repository manually. Instead, you must specify retention policy settings that will let you maintain the necessary number of backups in the archive repository. For more information, see Retention Policy for Archived Backups.

## VM Backup Retention

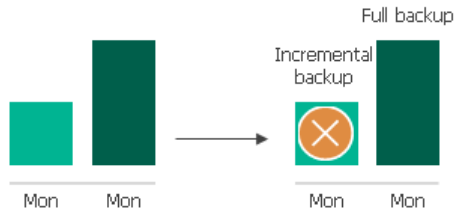
For image-level backups, Veeam Backup for Microsoft Azure retains restore points for the number of days defined in backup scheduling settings as described in section Creating VM Backup Policies.

To track and remove outdated restore points from a backup chain, Veeam Backup for Microsoft Azure performs the following actions once a day.

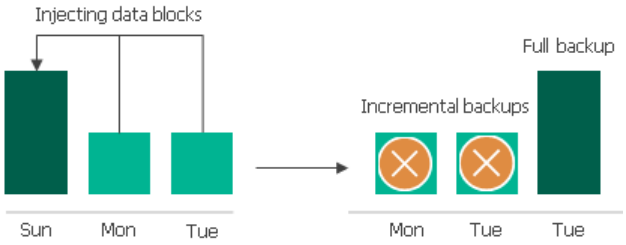
1. Veeam Backup for Microsoft Azure checks the configuration database to detect blob containers that contain outdated restore points.
2. If an outdated restore point exists in a blob container, Veeam Backup for Microsoft Azure deploys a worker instance in an Azure region in which the container with backed-up data resides.
3. Veeam Backup for Microsoft Azure transforms the backup chain in the following way:
   a. Veeam Backup for Microsoft Azure rebuilds the full backup to include data of the incremental backup that follows the full backup. To do that, Veeam Backup for Microsoft Azure injects into the full backup data blocks from the earliest incremental backup in the chain. This way, the full backup 'moves' forward in the backup chain.




   b. Veeam Backup for Microsoft Azure removes the earliest incremental backup from the chain as redundant — this data has already been injected into the full backup.




3. Veeam Backup for Microsoft Azure repeats step 2 for all other outdated restore points found in the backup chain until all the restore points are removed. As data from multiple restore points is injected into the rebuilt full backup, Veeam Backup for Microsoft Azure ensures that the backup chain is not broken and that you will be able to recover your data when needed.

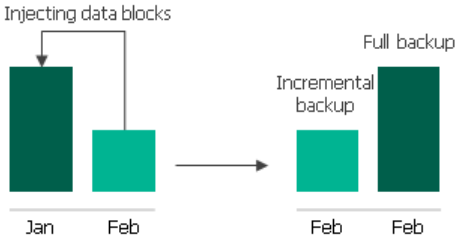


## Retention Policy for Archived Backups

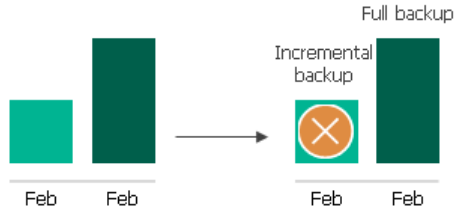
For archived backups, Veeam Backup for Microsoft Azure retains restore points for the number of days defined in backup scheduling settings as described in section Creating VM Backup Policies.

To track and remove outdated restore points from an archive backup chain, Veeam Backup for Microsoft Azure performs the following actions once a day:

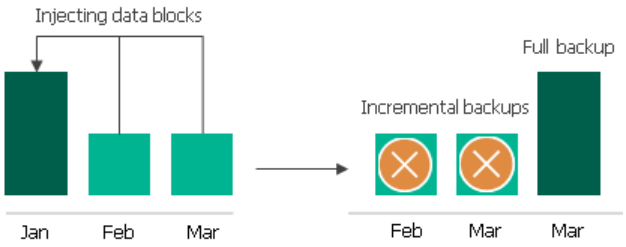
1. Veeam Backup for Microsoft Azure checks the configuration database to detect archive backup repositories that contain outdated restore points.
2. If an outdated restore point exists in a repository, Veeam Backup for Microsoft Azure transforms the archive backup chain in the following way:
   a. Veeam Backup for Microsoft Azure rebuilds the full archive backup to include in it data of the incremental archive backup that follows the full archive backup. To do that, Veeam Backup for Microsoft Azure injects into the full archive backup data blocks from the earliest incremental archive backup in the chain. This way, the full archive backup 'moves' forward in the archive backup chain.




   b. Veeam Backup for Microsoft Azure removes the earliest incremental archive backup from the chain as redundant — this data has already been injected into the full archive backup.




3. Veeam Backup for Microsoft Azure repeats step 2 for all other outdated restore points found in the archive backup chain until all the restore points are removed. As data from multiple restore points is injected into the rebuilt full archive backup, Veeam Backup for Microsoft Azure ensures that the archive backup chain is not broken and that you will be able to recover your data when needed.



# VM Restore

Veeam Backup for Microsoft Azure offers the following restore options:

- VM restore — restores an entire Azure VM from a cloud-native snapshot or an image-level backup. You can restore one or more Azure VMs at a time, to the original location or to a new location.
- Disk restore — restores virtual disks attached to an Azure VM from a cloud-native snapshot or an image-level backup. You can restore virtual disks to the original location or to a new location.
- File-level restore — restores individual files and folders of an Azure VM from a cloud-native snapshot or an image-level backup. You can download the necessary files and folders to a local machine, or restore the files and folders of the source Azure VM to the original location.

You can restore Azure VM data to the most recent state or to any available restore point.

## Entire VM Restore

To restore an Azure VM from a cloud-native snapshot, Veeam Backup for Microsoft Azure uses native Microsoft Azure capabilities. To restore an Azure VM from an image-level backup, Veeam Backup for Microsoft Azure performs the following steps:

1. [Applies only if you perform restore from an archived backup] Retrieves data from the archived restore point.
2. [Applies only if you perform restore to the original location] Creates a staging resource group in which virtual disks of the restored Azure VM will be created, and assigns the *Veeam backup appliance ID* tag to the group. The tag value is the ID of Azure VM running the backup appliance.
3. Creates empty virtual disks. The number of empty virtual disks equals the number of virtual disks attached to the source Azure VM.
4. Launches a worker instance in the Azure region where the restored Azure VM will reside, and then attaches empty virtual disks to the worker instance.
5. Restores backed-up data to the empty virtual disks on the worker instance.
6. Detaches the virtual disks with the restored data from the worker instance.
7. Deallocates the worker instance.
8. [Applies only if you perform restore to the original location] Removes the source Azure VM and the source disks from Microsoft Azure.
9. [Applies only if you perform restore to the original location] Moves the virtual disks from the staging resource group to the original resource group of the source Azure VM.
10. Creates an Azure VM in the specified location.
11. Attaches the created virtual disks with the restored data to the Azure VM.
12. [Applies only if you perform restore to the original location] Removes the staging resource group.

To learn how to restore an entire Azure VM from a cloud-native snapshot or an image-level backup, see Performing Entire VM Restore.

# Disk Restore

In case a disaster strikes, you can restore corrupted virtual disks of an Azure VM from a cloud-native snapshot or image-level backup. Veeam Backup for Microsoft Azure allows you to restore virtual disks to the original location or to a new location.

# How Disk Restore Works

To restore virtual disks from a cloud-native snapshot, Veeam Backup for Microsoft Azure uses native Microsoft Azure capabilities. To restore virtual disks from an image-level backup, Veeam Backup for Microsoft Azure performs the following steps:

1. [Applies only if you perform restore from an archived backup] Retrieves data from the archived restore point.
2. [Applies only if you perform restore to the original location] Creates a staging resource group in which virtual disks of the restored Azure VM will be created, and assigns the *Veeam backup appliance ID* tag to the group. The tag value is the ID of Azure VM running the backup appliance.
3. Creates empty virtual disks. The number of empty virtual disks equals the number of disks you want to restore.
4. Launches a worker instance in the Azure region where the restored virtual disks will reside, and attaches the empty virtual disks to the worker instance.
5. Restores backed-up data to the empty virtual disks on the worker instance.
6. Detaches the virtual disks with the restored data from the worker instance.
7. Deallocates the worker instance.
8. [Applies only if you perform restore to the original location] Removes the source virtual disks from Microsoft Azure.
9. [Applies only if you perform restore to the original location] Moves the virtual disks from the staging resource group to the original resource group.
10. [Applies only if you perform restore to the original location] Attaches the created virtual disks with the restored data to the Azure VM.
11. [Applies only if you perform restore to the original location] Removes the staging resource group.

> **NOTE**
>
> When restoring to a new location, Veeam Backup for Microsoft Azure does not attach the restored virtual disks to any Azure VM — the disks are placed to the specified location as standalone virtual disks.

To learn how to restore virtual disks attached to an Azure VM from a cloud-native snapshot or an image-level backup, see Performing Disk Restore.

# File-Level Recovery

To recover files and folders of a backed-up Azure VM, Veeam Backup for Microsoft Azure performs the following steps:

1. Launches a worker instance in either of the following Azure regions:
   - To recover files and folders from a cloud-native snapshot, the worker instance is launched in the region where the cloud-native snapshot resides.
   - To recover files and folders from an image-level backup, the worker instance is launched in the region where the backup repository storing backed-up data resides.
2. Attaches virtual disks of the Azure VM to the worker instance.

   The disks are not physically extracted from the backup — Veeam Backup for Microsoft Azure emulates their presence on the worker instance. The source backup itself remains in the read-only state.
3. [Applies only if you perform restore to the original location] Installs the Veeam restore tool on the source Azure VM.
4. Launches the file-level recovery browser.

   The file-level recovery browser displays the file system tree of the backed-up Azure VM. In the browser, you select the necessary files and folders to recover.
5. Saves the selected files and folders to the local machine, or restores the files and folders to the original Azure VM.
6. Detaches the virtual disks from the worker instance.
7. Deallocates the worker instance.

To learn how to restore individual files and folders of an Azure VM from a cloud-native snapshot or an image-level backup, see Performing File-Level Recovery.

# Protecting Azure SQL Databases

To produce backups of Azure SQL databases, Veeam Backup for Microsoft Azure runs backup policies. A backup policy is a collection of settings that define the way backup operations are performed: what data to back up, where to store backups, when to start the backup process, and so on.

Veeam Backup for Microsoft Azure does not install agent software to back up Azure SQL data — it uses native Microsoft Azure capabilities instead. During every backup session, Veeam Backup for Microsoft Azure creates a BACPAC file for each Azure SQL database added to a backup policy. The BACPAC file is further used to create a backup of the Azure SQL database. For more information on how SQL backup works, see SQL Backup.

## How To Protect Azure SQL Databases

To create an Azure SQL backup policy, perform the following steps:

1. Check limitations and prerequisites.
2. Specify service accounts to access Azure services and resources.
3. [Optional] Add backup repositories to store backed-up data.
4. [Optional] Configure worker instance settings to launch workers while processing Azure SQL data.
5. [Optional] Configure global retention settings for obsolete session records.
6. [Optional] Configure email notification settings for automated delivery of backup policy results and daily reports.
7. Complete the Add Azure SQL Policy wizard.

# SQL Backup

When processing an Azure SQL database added to a backup policy, Veeam Backup for Microsoft Azure can create a restore point of the database and transfer the point directly to a backup repository, or Veeam Backup for Microsoft Azure can copy the database to a staging server first, create a restore point and then transfer it to a repository. In the latter case, Veeam Backup for Microsoft Azure creates a transactionally consistent backup. This guarantees the consistency of the database state during recovery but can increase costs associated with cross-region data transfer.

Veeam Backup for Microsoft Azure performs SQL backup in the following way:

1. [Applies only if you perform backup using a staging server] Depending on the type of the processed Azure SQL database, Veeam Backup for Microsoft Azure does the following:
   - For an Azure SQL database residing on a SQL Server — creates a copy of the source database on the staging server using the Azure REST API.
   - For a database residing on an Azure SQL Managed Instance — creates a copy of the source database on the staging server using point-in-time restore (PITR). For more information on Azure point-in-time restore, see Microsoft Docs.

   For more information on the Azure SQL family of SQL Server database engine products, see Microsoft Docs.
2. Launches a worker instance in an Azure region where the staging server or the source database resides.
3. Synchronizes data between the backup repository and the configuration database to ensure data consistency.
4. Exports the database schema, indexes and constraints to a BACPAC file. For more information on BACPAC files, see Microsoft Docs.

   **IMPORTANT**

   BACPAC export of databases with external references is not supported. If a SQL database was migrated to an Azure SQL Database Server or Azure SQL Managed Instance, make sure to clear legacy references, orphaned database users and credentials set up with authentication types not supported by Azure SQL, to avoid BACPAC export errors.

4. Reads data from the exported BACPAC file on the worker instance, transfers the data to the target backup repository and stores it in the native Veeam format.
5. [Applies only if you perform backup using a staging server] Removes the copy of the source database from the staging server.
6. Deallocates the worker instance when the backup session completes.
7. If you enable the backup archiving mechanism, Veeam Backup for Microsoft Azure performs the following operations:
   a. Launches a worker instance in an Azure region in which the target backup repository resides.
   b. Retrieves data from the backup repository and transfers it to the target archive repository.
   c. Deallocates the worker instance when the archive session completes.

# Backup Chain

During every backup session, Veeam Backup for Microsoft Azure creates a new backup for each Azure SQL database added to a backup policy. A sequence of backups created during a set of backup sessions makes up a backup chain.

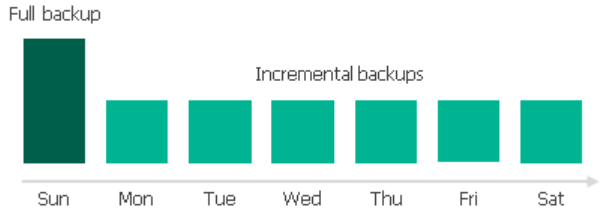
The backup chain includes backups of the following types:

- **Full** – a full backup stores a copy of the full Azure SQL database image.
- **Incremental** – incremental backups store incremental changes of the Azure SQL database images.

To create a backup chain for an Azure SQL database protected by a backup policy, Veeam Backup for Microsoft Azure implements the forever forward incremental backup method:

1. During the first backup session, Veeam Backup for Microsoft Azure copies the full Azure SQL database and creates a full backup in a backup repository. The full backup becomes a starting point in the backup chain.
2. During subsequent backup sessions, Veeam Backup for Microsoft Azure copies only those data blocks that have changed since the previous backup session and stores these data blocks to incremental backups in the backup repository. The content of each incremental backup depends on the content of the full backup and the preceding incremental backups in the backup chain.

> **NOTE**
>
> The changed block tracking (CBT) mechanism is not implemented for Azure SQL databases – during every incremental backup session, Veeam Backup for Microsoft Azure reads only the full Azure SQL database.




Full and incremental backups act as restore points for backed-up Azure SQL databases that let you roll back your data to the necessary state. To recover an Azure SQL database to a specific point in time, the chain of backups created for the database must contain a full backup and a set of incremental backups dependent on the full backup.

If some backup in the backup chain is missing, you will not be able to roll back to the necessary state. For this reason, you must not delete individual backups from the backup repository manually. Instead, you must specify retention policy settings that will let you maintain the necessary number of backups in the backup repository. For more information, see SQL Backup Retention.

## Archive Backup Chain

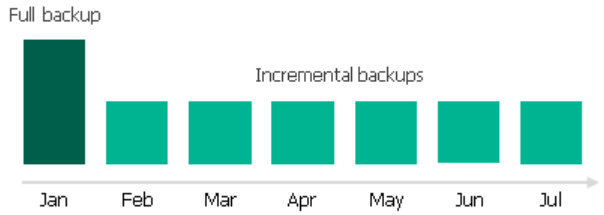
If you enable backup archiving for a backup policy, Veeam Backup for Microsoft Azure creates a new backup in an archive repository during every archive session. A sequence of backups created during a set of archive sessions makes up an archive backup chain.

The archive backup chain includes backups of the following types:

- **Full** – a full archive backup stores a copy of the full Azure SQL database image.
- **Incremental** – incremental archive backups store incremental changes of the Azure SQL database image.

To create an archive backup chain for an Azure SQL database protected by a backup policy, Veeam Backup for Microsoft Azure implements the forever forward incremental backup method:

1. During the first archive session, Veeam Backup for Microsoft Azure detects backed-up data that is stored in the full backup and all incremental backups existing in the backup chain, creates a full archive backup with all the data, and copies this backup to the archive repository. The full archive backup becomes a starting point in the archive chain.
2. During subsequent archive sessions, Veeam Backup for Microsoft Azure checks the backup chain to detect data blocks that have changed since the previous archive session, creates incremental archive backups with only those changed blocks, and copies these backups to the archive repository. The content of each incremental archive backup depends on the content of the full archive backup and the preceding incremental archive backups in the archive backup chain.




Full and incremental archive backups act as restore points for backed-up Azure SQL databases that let you roll back your data to the necessary state. To recover an Azure SQL database to a specific point in time, the chain of backups created for the database must contain a full archive backup and a set of incremental archive backups.

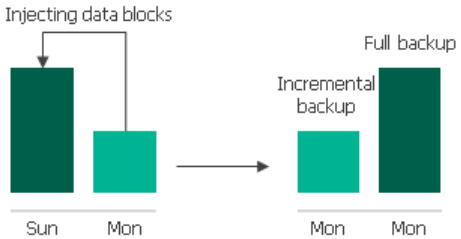
If some backup in the archive backup chain is missing, you will not be able to roll back to the necessary state. For this reason, you must not delete individual backups from the archive repository manually. Instead, you must specify retention policy settings that will let you maintain the necessary number of backups in the archive repository. For more information, see Retention Policy for Archived Backups.

## SQL Backup Retention

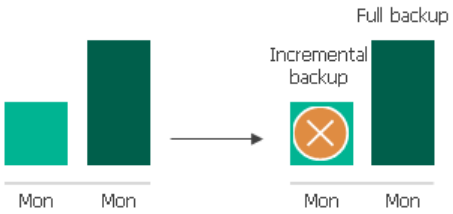
For image-level backups, Veeam Backup for Microsoft Azure retains restore points for the number of days defined in backup scheduling settings as described in section Creating SQL Backup Policies.

To track and remove outdated restore points from a backup chain, Veeam Backup for Microsoft Azure performs the following actions once a day.

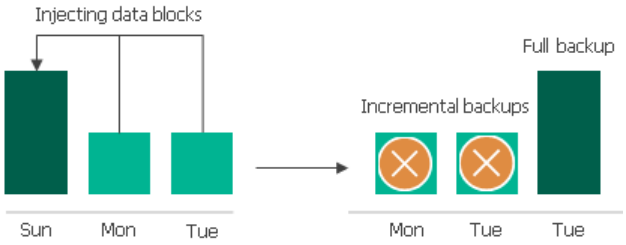
1. Veeam Backup for Microsoft Azure checks the configuration database to detect blob containers that contain outdated restore points.
2. If an outdated restore point exists in a blob container, Veeam Backup for Microsoft Azure deploys a worker instance in an Azure region in which the container with backed-up data resides.
3. Veeam Backup for Microsoft Azure transforms the backup chain in the following way:
   a. Veeam Backup for Microsoft Azure rebuilds the full backup to include data of the incremental backup that follows the full backup. To do that, Veeam Backup for Microsoft Azure injects into the full backup data blocks from the earliest incremental backup in the chain. This way, the full backup 'moves' forward in the backup chain.



b. Veeam Backup for Microsoft Azure removes the earliest incremental backup from the chain as redundant — this data has already been injected into the full backup.




3. Veeam Backup for Microsoft Azure repeats step 2 for all other outdated restore points found in the backup chain until all the restore points are removed. As data from multiple restore points is injected into the rebuilt full backup, Veeam Backup for Microsoft Azure ensures that the backup chain is not broken and that you will be able to recover your data when needed.

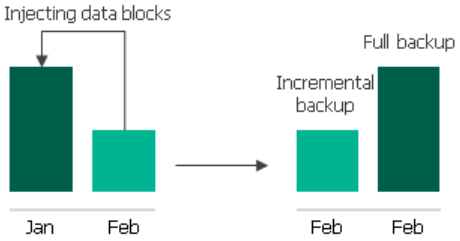



## Retention Policy for Archived Backups

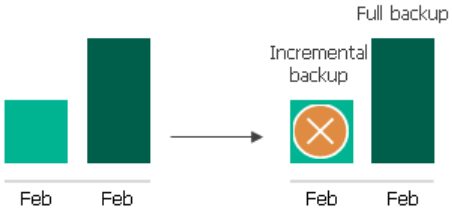
For archived backups, Veeam Backup for Microsoft Azure retains restore points for the number of days defined in backup scheduling settings as described in section Creating SQL Backup Policies.

To track and remove outdated restore points from an archive backup chain, Veeam Backup for Microsoft Azure performs the following actions once a day:

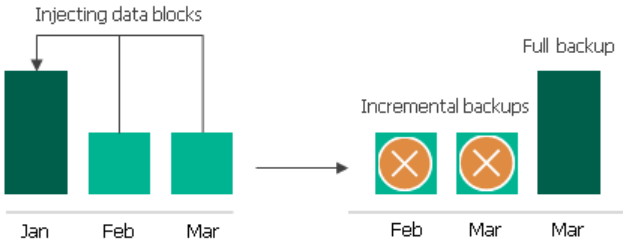
1. Veeam Backup for Microsoft Azure checks the configuration database to detect archive backup repositories that contain outdated restore points.
2. If an outdated restore point exists in a repository, Veeam Backup for Microsoft Azure transforms the archive backup chain in the following way:
   a. Veeam Backup for Microsoft Azure rebuilds the full archive backup to include in it data of the incremental archive backup that follows the full archive backup. To do that, Veeam Backup for Microsoft Azure injects into the full archive backup data blocks from the earliest incremental archive backup in the chain. This way, the full archive backup 'moves' forward in the archive backup chain.



b. Veeam Backup for Microsoft Azure removes the earliest incremental archive backup from the chain as redundant — this data has already been injected into the full archive backup.




3. Veeam Backup for Microsoft Azure repeats step 2 for all other outdated restore points found in the archive backup chain until all the restore points are removed. As data from multiple restore points is injected into the rebuilt full archive backup, Veeam Backup for Microsoft Azure ensures that the archive backup chain is not broken and that you will be able to recover your data when needed.



# SQL Restore

To restore an Azure SQL database from a backup, Veeam Backup for Microsoft Azure performs the following steps:

1. [Applies only if you perform restore from an archived backup] Retrieves data from the archived restore point.
2. Launches a worker instance in the Azure region where the SQL Server that will host the restored database resides.
3. Creates an empty database on the target SQL Server using the Azure REST API.
4. Restores backed-up data to a BACPAC file on the worker instance.
5. Imports data from the BACPAC file to the created database.
6. Performs consistency checks for the restored database.
7. Deallocates the worker instance.
6. [Applies only if you perform restore to the original location and if the source database is still present in the location] Renames the restored database and then removes the source database from the SQL Server.

To learn how to restore an entire Azure SQL database from a backup, see SQL Restore.

# Protecting Cosmos DB Accounts

To produce backups of Cosmos DB accounts, Veeam Backup for Microsoft Azure runs backup policies. A backup policy is a collection of settings that define the way backup operations are performed: what data to back up, where to store backups, when to start the backup process, and so on.

By default, Veeam Backup for Microsoft Azure does not install agent software to back up Cosmos DB account data — it uses native Microsoft Azure capabilities instead. Every time Veeam Backup for Microsoft Azure synchronizes data between Microsoft Azure and the configuration database, it creates a database record for each Cosmos DB account added to a backup policy. You can also instruct Veeam Backup for Microsoft Azure to create backups of the processed Cosmos DB for PostgreSQL clusters and Cosmos DB for MongoDB accounts. For more information on how Cosmos DB backup works, see Cosmos DB Backup.

## How To Protect Cosmos DB Accounts

To create a Cosmos DB backup policy, perform the following steps:

1. Check limitations and prerequisites.
2. Specify service accounts to access Azure services and resources.
3. [Optional] Add backup repositories to store backed-up data.
4. [Optional] Configure worker instance settings to launch workers while processing Cosmos DB data.
5. [Optional] Configure global retention settings for obsolete session records.
6. [Optional] Configure email notification settings for automated delivery of backup policy results and daily reports.
7. Complete the Add Cosmos DB Policy wizard.

# Cosmos DB Backup

When processing a Cosmos DB account added to a backup policy, Veeam Backup for Microsoft Azure uses continuous backup — a native Microsoft Azure capability that allows you to eliminate consumption of extra provisioned throughput without affecting the database performance and availability.

Every 8 hours, Veeam Backup for Microsoft Azure runs configuration sessions to check the continuous backup retention period defined in Microsoft Azure for all the Cosmos DB accounts added to the backup scope. If the retention period differs from the retention period specified in the backup policy settings, Veeam Backup for Microsoft Azure redefines the retention period in Microsoft Azure.

Every time Veeam Backup for Microsoft Azure synchronizes data between Microsoft Azure and the configuration database, it creates a database record for each Cosmos DB account added to a backup policy — the record can further be used to restore this account. For more information on how continuous backup is performed, see Microsoft Docs.

## Backup to Repository

If you enable backup to a repository, Veeam Backup for Microsoft Azure performs the following steps:

1. Launches a worker instance in an Azure region where the processed Cosmos DB for PostgreSQL or Cosmos DB for MongoDB account reside.

   By default, Veeam Backup for Microsoft Azure launches worker instances using virtual networks created automatically. However, you can add specific worker configurations. For more information, see Managing Worker Instances.

2. Synchronizes data between the backup repository and the configuration database to ensure data consistency.

3. Uses the worker instance to create a backup file of user data contained in the database, transfers the data to the target backup repository and stores it in the native Veeam format.

> **NOTE**
>
> Veeam Backup for Microsoft Azure does not include any metadata such as credentials in the backup file.

3. Deallocates the worker instance when the backup session completes.

4. If you enable the backup archiving mechanism, Veeam Backup for Microsoft Azure performs the following operations:

   a. Launches a worker instance in an Azure region in which the target backup repository resides.

   b. Retrieves data from the backup repository and transfers it to the target archive repository.

   c. Deallocates the worker instance when the archive session completes.

## Backup Chain

If you enable backup to a repository for a backup policy, Veeam Backup for Microsoft Azure creates a new backup for the database of each processed Cosmos DB for PostgreSQL or Cosmos DB for MongoDB account in a standard repository during every backup session. A sequence of backups created during a set of backup sessions makes up a regular backup chain.

Each Cosmos DB for PostgreSQL or Cosmos DB for MongoDB backup in the backup chain contains metadata that stores information about the protected instance, the backup policy that created the backup, as well as the date, time and configured retention settings. Veeam Backup for Microsoft Azure uses metadata to identify outdated backups, to retrieve information on the source database configuration during recovery operations, and so on.

> **NOTE**
>
> The forever forward incremental backup method is not implemented for Cosmos DB for PostgreSQL and Cosmos DB for MongoDB accounts — during every backup session, Veeam Backup for Microsoft Azure creates a full backup in the regular backup chain.

The period of time during which Cosmos DB for PostgreSQL and Cosmos DB for MongoDB backups are kept in the backup chain is defined by retention policy settings. For details, see Cosmos DB Backup Retention.

## Archive Backup Chain

If you enable backup archiving for a backup policy, Veeam Backup for Microsoft Azure creates a new backup in an archive repository during every archive session. A sequence of backups created during a set of archive sessions makes up an archive backup chain.

> **NOTE**
>
> The forever forward incremental backup method is not implemented for Cosmos DB for PostgreSQL and Cosmos DB for MongoDB accounts — during every archive session, Veeam Backup for Microsoft Azure creates a full backup in the regular backup chain (that is, every incremental backup contains the full database data set).

The period of time during which Cosmos DB for PostgreSQL and Cosmos DB for MongoDB backups are kept in the archive backup chain is defined by retention policy settings. For details, see Cosmos DB Backup Retention.

# Cosmos DB Backup Retention

For protected Cosmos DB accounts, Veeam Backup for Microsoft Azure retains records in the configuration database for the number of days defined in backup target settings as described in section Creating Cosmos DB Backup Policies.

Every 10 minutes, Veeam Backup for Microsoft Azure synchronizes data between Microsoft Azure and the configuration database to create a new database record. If Veeam Backup for Microsoft Azure detects that a record is older than the specified retention period, Veeam Backup for Microsoft Azure removes it from the database. For more information on the retention process, see Microsoft Docs.

Every time Veeam Backup for Microsoft Azure synchronizes data between Microsoft Azure and the configuration database, it also checks whether any of the protected Cosmos DB accounts have been removed from Microsoft Azure. If such an account is detected, it will acquire the *Deleted* status on the Protected Data page in the Veeam Backup for Microsoft Azure Web UI, and you will still be able to restore this account to any point in time within the specified retention period. After the retention period ends, Veeam Backup for Microsoft Azure will automatically remove all the records created for the account from the configuration database.

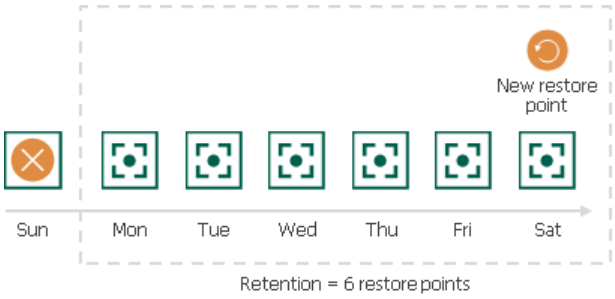
**IMPORTANT**

When a Cosmos DB for PostgreSQL or a Cosmos DB for MongoDB account is deleted from Microsoft Azure, Veeam Backup for Microsoft Azure instantly removes all the records created for this account from the configuration database and excludes the account from the list of protected resources on the **Protected Data** page. As a result, you will no longer be able to restore this account — unless you have protected it with the backup to a repository enabled.

# Backup to Repository Retention

If you enable backup to a repository for a backup policy, Veeam Backup for Microsoft Azure retains restore points for the number of days defined in backup scheduling settings as described in section Creating Cosmos DB Backup Policies.

The forever forward incremental backup method is not implemented for Cosmos DB for PostgreSQL and Cosmos DB for MongoDB accounts — during every backup session Veeam Backup for Microsoft Azure creates a full backup in the regular backup chain. If Veeam Backup for Microsoft Azure detects an outdated restore point in a standard or an archive backup repository, Veeam Backup for Microsoft Azure removes this restore point from the backup chain.



# Cosmos DB Restore

Veeam Backup for Microsoft Azure offers the following restore operations:

- **Point-in-time restore** — restores an entire Cosmos DB account or its specific items using the native Microsoft Azure point-in-time restore feature. You can restore Cosmos DB account data to the most recent or to any available point in time (timestamp).

  To restore a Cosmos DB account to a restorable timestamp, Veeam Backup for Microsoft Azure sends REST API requests to Microsoft Azure to create a new Cosmos DB account with the configuration specified in the restore settings.

- **Restore from repository** — restores the database of a specific Cosmos DB for PostgreSQL account or databases and collections of a specific Cosmos DB for MongoDB account from a backup stored in a repository. You can restore the database data to the most recent state or to any available restore point.

  To restore an item of a Cosmos DB account from a backup, Veeam Backup for Microsoft Azure performs the following steps:

  a. [Applies only if you perform restore from an archived backup] Retrieves data from the archived restore point.

  b. Launches a worker instance in an Azure region where the target Cosmos DB for PostgreSQL or Cosmos DB for MongoDB account to which the item will be restored resides.

  c. Uses the worker instance to retrieve user data contained in the backup, and then imports this data to the target Cosmos DB account.

  d. Deallocates the worker instance.

To learn how to restore a Cosmos DB account to a restorable timestamp, see Performing Point-in-time Restore. To learn how to restore the database of a Cosmos DB for PostgreSQL account or databases and collections of a Cosmos DB for MongoDB account from a backup, see Performing Restore From Repository.

# Protecting Azure File Shares

To produce snapshots of Azure file shares, Veeam Backup for Microsoft Azure runs backup policies. A backup policy is a collection of settings that define the way snapshots are created: what data to protect, when to start the snapshot creation process, and so on.

Veeam Backup for Microsoft Azure does not install agent software to back up Azure Files data — it uses native Microsoft Azure capabilities instead. During every backup session, Veeam Backup for Microsoft Azure creates a cloud-native snapshot for each Azure file share added to a backup policy. For more information on how Azure Files backup works, see Azure Files Backup.

## How To Protect Azure File Shares

To create an Azure Files backup policy, perform the following steps:

1. Check limitations and prerequisites.
2. Specify service accounts to access Azure services and resources.
3. [Optional] Configure worker instance settings to launch workers while processing Azure Files data.
4. [Optional] Configure global retention settings for obsolete snapshots and session records.
5. [Optional] Configure email notification settings for automated delivery of backup policy results and daily reports.
6. Complete the Add Azure Files Policy wizard.

# Azure Files Backup

Veeam Backup for Microsoft Azure performs Azure Files backup in the following way:

1. Creates a share snapshot of the processed Azure file share using Microsoft Azure native capabilities.

> **NOTE**
>
> Due to Microsoft Azure limitations, the maximum number of snapshots to keep for one file share is 200.

2. If you enable file share indexing, Veeam Backup for Microsoft Azure performs the following operations:
   a. Launches a worker instance in an Azure region in which the processed file share resides.

      By default, Veeam Backup for Microsoft Azure launches worker instances using virtual networks created automatically. However, you can add specific worker configurations. For more information, see Managing Worker Instances.

   b. Re-creates the file share from the share snapshot created at step 1 and mounts the share to the worker instance.

   c. Reads data from the file share on the worker instance, creates a catalog of files and folders (that is, the index) of the share, and saves the index as a .ZIP file on the backup appliance.

      The creation of the .ZIP file may take significant time to complete. If a new backup policy session starts and the previous indexing session is still running, a new indexing session will not be launched.

   d. Deallocates the worker instance when the indexing session completes.

## Snapshot Chain

During every backup session, Veeam Backup for Microsoft Azure creates a cloud-native snapshot of each Azure file share added to a backup policy. The cloud-native snapshot itself is a collection of point-in-time snapshots of share files that Veeam Backup for Microsoft Azure takes using native Microsoft Azure capabilities.

A sequence of cloud-native snapshots created during a set of backup sessions makes up a snapshot chain. Veeam Backup for Microsoft Azure creates the snapshot chain in the following way:

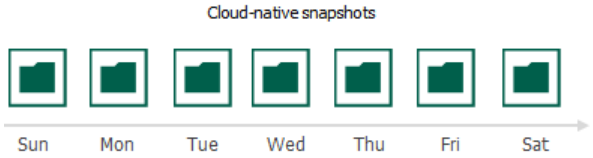
1. During the first backup session, Veeam Backup for Microsoft Azure creates a snapshot of all Azure Files data and saves it on the processed file share. This snapshot becomes a starting point in the snapshot chain.

2. During subsequent backup sessions, Veeam Backup for Microsoft Azure creates snapshots with only those files and directories that have changed since the previous backup session.

   For more information on how snapshots work, see Microsoft Docs.

Each cloud-native snapshot in the snapshot chain contains metadata. Metadata includes information about the processed file share, the backup policy that created the snapshot, and a number of snapshots in the chain. Veeam Backup for Microsoft Azure uses metadata to identify outdated snapshots, to load the configuration of source file shares during recovery operations, and so on.

Cloud-native snapshots act as independent restore points for backed-up file shares. If you remove any snapshot, it will not break the snapshot chain — you will still be able to roll back your data to any existing restore point.

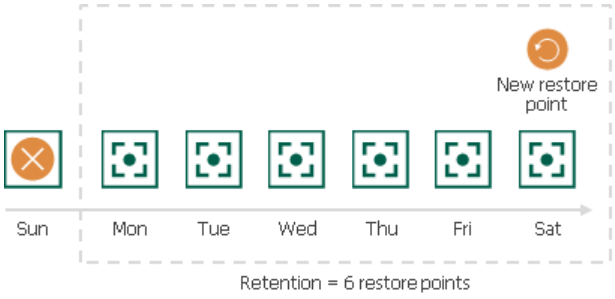



The number of cloud-native snapshots kept in the snapshot chain is defined by retention policy settings. For more information, see File Share Snapshot Retention.

## File Share Snapshot Retention

For cloud-native snapshots, Veeam Backup for Microsoft Azure retains the number of latest restore points defined in backup scheduling settings as described in section Creating Azure Files Backup Policies.

During every successful backup session, Veeam Backup for Microsoft Azure creates a new restore point. If Veeam Backup for Microsoft Azure detects that the number of restore points in the snapshot chain exceeds the retention limit, it removes the earliest restore point from the chain. For more information on the snapshot deletion process, see Microsoft Docs.




**NOTE**

Consider that Veeam Backup for Microsoft Azure does not apply retention policy settings to cloud-native snapshots created manually. To learn how to remove these snapshots, see sections Managing VM Data and Managing Azure Files Data.

# Azure Files Restore

To restore files and folders of an Azure file share, Veeam Backup for Microsoft Azure performs the following steps:

1. On the backup appliance, restores the file share tree.
2. Launches the file-level recovery browser.

   The file-level recovery browser displays the file tree of the backed-up file share. In the browser, you can specify the necessary restore point, and select files and folders that will be restored.
3. Restores the specified backed-up files and folders from the restore point to the selected file share.

To learn how to restore individual files and folders stored in a file system from an Azure Files backup, see File Share Restore.

# Protecting Virtual Network Configurations

To protect Azure virtual network configurations, Veeam Backup for Microsoft Azure retrieves configuration data through API and saves this data to the configuration database. For more information on how virtual network configuration backup works, see Virtual Network Configuration Backup.

## How To Protect Virtual Network Configurations

To configure the virtual network configuration backup policy settings, perform the following steps:

1. Check limitations and prerequisites.
2. Specify service accounts to access Azure services and resources.
3. Add backup repositories to save additional virtual network configuration backup copies.
4. [Optional] Configure worker instance settings to launch workers while processing virtual network configuration data.
5. [Optional] Configure global retention settings for obsolete snapshots and session records.
6. [Optional] Configure email notification settings for automated delivery of backup policy results and daily reports.
7. Complete the Edit Virtual Network Configuration Backup Policy wizard.

# Virtual Network Configuration Backup

Veeam Backup for Microsoft Azure performs virtual network configuration backup in the following way:

1. Sends API requests to Microsoft Azure to retrieve the virtual network configuration data, and saves this data in the configuration database.

   To back up virtual network configurations of Azure subscriptions added to backup policies, Veeam Backup for Microsoft Azure uses permissions of service accounts specified in the backup policy settings. The virtual network configuration data is collected for the Microsoft Entra tenants to which the specified service accounts belong.

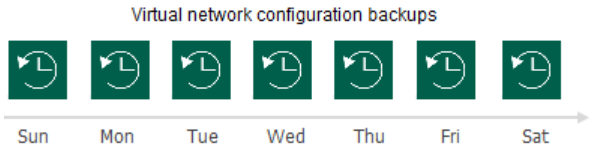
2. Creates a configuration record for each pair of an Microsoft Entra tenant and an Azure subscription whose virtual network configuration data is being backed up. Every time the Virtual Network Configuration Backup policy runs, Veeam Backup for Microsoft Azure updates the record to create a new restore point for each protected virtual network configuration.

3. If you enable additional backup copy for the Virtual Network Configuration Backup policy, Veeam Backup for Microsoft Azure launches the Veeam Data Mover service on the backup appliance to copy the restore points from the configuration database to the target repository, creating an individual folder for each Azure subscription whose virtual network configuration data is protected by the policy.

## Backup Chain

During every backup session, Veeam Backup for Microsoft Azure creates a restore point with backed-up virtual network configuration data for each Azure subscription protected by the Virtual Network Configuration Backup policy. The restore point contains metadata that includes information on the date and time when the policy ran, Azure subscriptions whose virtual network configuration settings were backed up by the policy, and Microsoft Entra tenants whose service accounts were used to collect virtual network configuration settings for each Azure subscription.

A sequence of restore points created during a set of backup sessions makes up a virtual network configuration backup chain for each configuration record.




You cannot delete specific restore points created for a configuration record — these points are removed automatically according to the specified retention policy settings. However, you can manually remove a configuration record with all restore points created for it, as described in section Removing Virtual Network Configuration Backups.

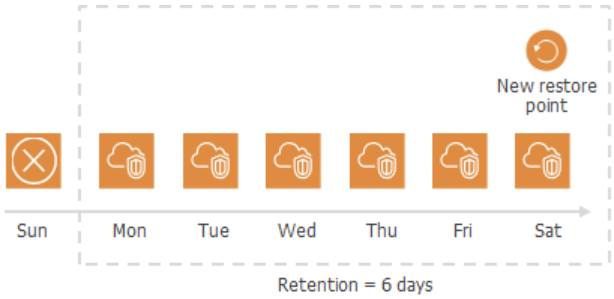
## Virtual Network Configuration Backup Retention

For virtual network configuration backups, Veeam Backup for Microsoft Azure retains restore points for the period of time specified in backup retention settings.

During every successful backup session, Veeam Backup for Microsoft Azure creates a restore point and saves the date, time and the applied retention settings in the restore point metadata. If Veeam Backup for Microsoft Azure detects that the period of time for which the restore point was stored exceeds the period specified in the retention settings, it automatically removes the restore point from the virtual network configuration backup chain. You can also remove unnecessary virtual network configuration backups manually as described in section Removing Virtual Network Configuration Backups.

NOTE

Veeam Backup for Microsoft Azure applies the retention settings configured for the Virtual Network Configuration Backup policy both to virtual network configuration backups stored in the Veeam Backup for Microsoft Azure database and to virtual network configuration backups stored in the backup repository selected for the policy. For virtual network configuration backups stored in backup repositories that are not specified in the Virtual Network Configuration Backup policy settings, Veeam Backup for Microsoft Azure applies retention settings saved in the backup metadata.



# Virtual Network Configuration Restore

Veeam Backup for Microsoft Azure offers the following disaster recovery operations:

- Full restore — restores the entire virtual network configuration from a virtual network configuration backup. You can restore the virtual network configuration to the original location or to a new location.
- Granular restore — restores the selected virtual network configuration items from a virtual network configuration backup. You can restore specific virtual network configuration items only to the original location.

You can restore the virtual network configuration data to the most recent state or to any available restore point.

## Entire Virtual Network Configuration Restore

To restore the entire virtual network configuration from a backup, Veeam Backup for Microsoft Azure performs the following steps:

1. Retrieves the backed-up virtual network configuration from the Veeam Backup for Microsoft Azure database.
2. Validates the restore operation: sends API requests to Microsoft Azure to verify that Azure service quotas are not exceeded and there are no subnet CIDR block conflicts.
3. Retrieves information on existing items and their settings in the current Azure virtual network configuration.
4. Restores the backed-up virtual network configuration:
    a. Creates the missing virtual network configuration items.
    b. Modifies settings of the existing items that do not match the backed-up settings.

To learn how to restore the entire virtual network configuration from a virtual network configuration backup, see Performing Entire Virtual Network Configuration Restore.

## Granular Restore

To restore specific items of the virtual network configuration from a backup, Veeam Backup for Microsoft Azure performs the following steps:

1. Retrieves from the Veeam Backup for Microsoft Azure database the backed-up virtual network configuration data on items added to a restore list.
2. Validates the restore operation: sends a REST API request to Microsoft Azure to verify that Azure service quotas are not exceeded and there are no subnet CIDR block conflicts.
3. Retrieves information on existing items and their settings in the current Azure virtual network configuration.
4. Restores the selected items of the backed-up virtual network configuration:
    - Creates the missing virtual network configuration items.
    - Modifies settings of the existing items that do not match the backed-up settings.

To learn how to restore restores the selected virtual network configuration items from a virtual network configuration backup, see Performing Granular Restore.

# SLA-Based Backup Policies

To simplify data protection and monitor compliance with your target SLA, Veeam Backup for Microsoft Azure introduces SLA-based backup policies. An SLA-based backup policy is a collection of settings that automate the way backup operations are performed: how frequently to run the backup process, what region-specific repositories to use to store backups, how many restore points should be created in time to meet SLA requirements, and so on.

To help you eliminate error-prone manual steps and save time configuring SLA-based backup policies, Veeam Backup for Microsoft Azure offers 2 types of templates:

- SLA template — includes a periodic backup schedule and a target SLA value that you can use to define protection settings for workloads processed by SLA-based backup policies.
- Storage template — includes backup storage settings and region-specific storage options that you can use to define target locations for backups created by SLA-based backup policies.

> **NOTE**
>
> In Veeam Backup for Microsoft Azure version 8, you can use SLA-based backup policies to protect Azure VMs only.

# SLA Templates

An SLA template is a collection of settings that allows you to protect your data according to a periodic backup schedule (regularly, within a backup window) in a way the data protection complies with SLA standards in your company. These standards are defined by a specific target SLA value that indicates how much data you can afford to lose in case a disaster strikes, which allows you to troubleshoot backup issues and facilitate backup infrastructure audit.

The target SLA value is a percentage of successfully created restore points out of the total number of restore points expected to be produced by an SLA-based backup policy. Based on this percentage, Veeam Backup for Microsoft Azure estimates the SLA compliance ratio for all SLA-based backup policies that have the related SLA template assigned. For more information, see How Veeam Backup for Microsoft Azure Estimates SLA Compliance.

One SLA template can be assigned to one or more SLA-based backup policies. When configuring an SLA template, you can create separate independent schedules for cloud-native snapshots, image-level backups and archived backups. For more information on how Veeam Backup for Microsoft Azure builds snapshot, backup and archive backup chains, see sections Snapshot Chain, Backup Chain and Archive Backup Chain.

> **NOTE**
>
> Cloud-native snapshots created according to snapshot schedules do not participate in the process of producing backups. To produce image-level backups according to backup schedules, Veeam Backup for Microsoft Azure takes temporary snapshots but then removes these snapshots based on their own retention settings.

## Data Protection Windows

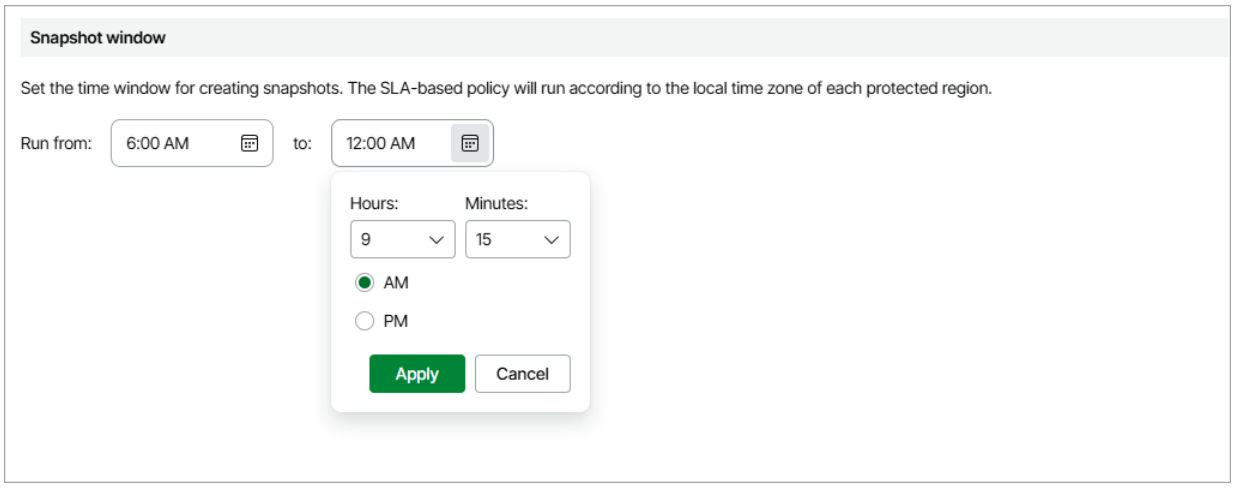
A data protection window is a time interval during which SLA-based backup policies are allowed to create restore points of protected resources. Data protection windows can be helpful if you do not want SLA-based backup policies to produce unwanted overhead for the production environment or do not want the policies to overlap production hours.

When you specify a data protection window for an SLA-based backup policy, Veeam Backup for Microsoft Azure adjusts this window to the time zone of each region added to the policy. For example, if you instruct Veeam Backup for Microsoft Azure to create daily snapshots of Azure VMs residing in the Central US and North Europe regions between 9:00 AM and 9:00 PM, Veeam Backup for Microsoft Azure will create cloud-native snapshots in the following way:

1. At 9:00 AM North European time (9:00 UTC), Veeam Backup for Microsoft Azure will start creating the first daily snapshot in the North Europe region.
2. At 9:00 AM Central US time (15:00 UTC), Veeam Backup for Microsoft Azure will start creating the first daily snapshot in the Central US region.

> **NOTE**
>
> If an SLA-based backup policy exceeds the allowed data protection window, Veeam Backup for Microsoft Azure will not stop the policy immediately and will continue creating restore points — but will not take the created restore points into account when estimating the SLA compliance for the policy. That is why it is recommended that data protection windows do not overlap in one SLA template.

Keep in mind that the value that you specify as the end of a data protection window is excluded from this window. For example, if you instruct Veeam Backup for Microsoft Azure to create daily snapshots every hour between 10:00 AM and 1:00 PM, Veeam Backup for Microsoft Azure will create 3 snapshots over this interval: at 10:00 AM, 11:00 AM and 12:00 PM. However, if you instruct Veeam Backup for Microsoft Azure to create daily snapshots every hour between 10:00 AM and 1:05 PM, Veeam Backup for Microsoft Azure will create 4 snapshots: at 10:00 AM, 11:00 AM, 12:00 PM and 1:00 PM.




# Temporary Restore Points

When running SLA-based backup policies, Veeam Backup for Microsoft Azure creates 2 types of temporary restore points — temporary snapshots and temporary backups.

# Temporary Snapshots

To produce image-level backups according to backup schedules configured for SLA templates, Veeam Backup for Microsoft Azure takes temporary snapshots but then automatically removes them. The retention of these temporary snapshots depends on whether you enable the changed block tracking (CBT) mechanism for these templates:

- If CBT is enabled for an SLA template, Veeam Backup for Microsoft Azure keeps the latest temporary snapshot in the snapshot chain until the next backup session runs. In this case, Veeam Backup for Microsoft Azure processes only those data blocks that have changed since the previous snapshot was created. This allows you to increase the speed and efficiency of incremental backups but can incur additional costs of storing snapshots in Microsoft Azure.
- If CBT is disabled for an SLA template, Veeam Backup for Microsoft Azure removes the latest temporary snapshot from the snapshot chain during the next retention session at 12:00 AM (according to the time zone set on the backup appliance). In this case, Veeam Backup for Microsoft Azure processes not only those data blocks that have changed since the previous snapshot was created, but also all other data blocks of the snapshot. This allows you to reduce the cost of storing snapshots in Microsoft Azure but decreases the speed and efficiency of incremental backups.

That is, it is recommended that you take into account both backup schedules and your cost management strategy when choosing whether to enable CBT for SLA templates.

> **IMPORTANT**
>
> Do not remove temporary snapshots from Microsoft Azure manually as Veeam Backup for Microsoft Azure will not be able to produce image-level backups.

# Temporary Backups

To build archive backup chains for Azure VMs protected by SLA-based backup policies, Veeam Backup for Microsoft Azure implements the same forever forward incremental backup method that applies to schedule-based backup policies. For more information, see Archive Backup Chain.

However, if Veeam Backup for Microsoft Azure fails to detect any full backups added to a backup chain on the same day when the archive session runs, it creates a temporary full backup that is then used to produce an archived backup in the target archive repository. After the archived backup is produced, Veeam Backup for Microsoft Azure automatically removes the temporary backup from the backup chain during the next retention session (as soon as Veeam Backup for Microsoft Azure finalizes the backup window in all protected regions).

# Storage Templates

A storage template is a collection of settings that allows you to define target locations for backups and archived backups. A target location is a repository where an SLA-based backup policy stores restore points; it can be the same repository for all regions protected by the policy, or you can specify separate repositories for each region.

Using region-specific repositories allows you to avoid cross-region transaction costs associated with data transfer between Azure regions during backup and archive operations, while using a single default repository may help you ensure data protection regardless of the source location.

# Retention Policies

Cloud-native snapshots and image-level backups are not kept forever — they are removed according to retention policy settings specified in the backup schedule settings while creating a backup policy.

Depending on the data protection scenario, retention policies can be specified:

- **In restore points** — for cloud-native snapshots produced by schedule-based backup policies.

  The snapshot chain can contain only the allowed number of restore points. If the number of allowed restore points is exceeded, Veeam Backup for Microsoft Azure removes the earliest restore point from the snapshot chain. For more information, see VM Snapshot Retention and File Share Snapshot Retention.

- **In days/months/years** — for image-level backups and archived backups as well as for cloud-native snapshots produced by SLA-based backup policies.

  Restore points in the backup chain (either regular or archive) can be stored in the backup repository only for the allowed period of time. If a restore point is older than the specified time limit, Veeam Backup for Microsoft Azure removes it from the backup chain. For more information, see sections VM Backup Retention, SQL Backup Retention and Cosmos DB Backup Retention.

You can also specify retention settings for snapshots that become obsolete. For more information, see Configuring Global Retention Settings.

# Immutability

Veeam Backup for Microsoft Azure allows you to protect VM, SQL, Cosmos DB for PostgreSQL, Cosmos DB for MongoDB and virtual network configuration data stored in backup repositories from deletion by making the data temporarily immutable. To do that, Veeam Backup for Microsoft Azure uses Immutable storage for Azure Blob Storage — once imposed, Immutable storage prevents objects from being deleted or overwritten for a specific immutability period. The immutability period is set based on the retention policy configured in the backup policy settings.

> **NOTE**
>
> To reduce the number of requests sent to immutable repositories during VM, SQL, Cosmos DB and virtual network configuration backup operations, Veeam Backup for Microsoft Azure leverages the Block Generation mechanism.

## Considerations and Limitations

Before you start creating immutable backups, keep in mind the following limitations:

- You cannot manually remove immutable data from immutable repositories using the Veeam Backup for Microsoft Azure Web UI, as described in sections Removing VM Backups and Snapshots, Removing SQL Backups, Removing Cosmos DB Backups and Removing Virtual Network Configuration Backups.
- You can neither remove data from Microsoft Azure using any cloud service provider tools nor request the technical support department to do it for you — none of the protected objects can be overwritten or deleted by any user, including the Global Administrator in your Microsoft Entra ID.

## How To Create Immutable Backups

To protect backups created with Veeam Backup for Microsoft Azure from deletion by making them temporarily immutable, perform the following steps:

1. Add a backup repository with immutability enabled.
2. Create a backup policy and specify the repository with immutability enabled as the target location for image-level backups. For more information, see sections Creating VM Backup Policies, Creating SQL Backup Policies, Creating Cosmos DB Backup Policies and Editing Virtual Network Configuration Backup Policy.

# Block Generation

If you choose a repository with immutability settings enabled as the target location for image-level backups, Veeam Backup for Microsoft Azure creates an immutable backup chain in the repository instead of a regular backup chain. Immutable backup chains are built the same way as standard and archive backup chains, which means that each immutability chain is composed of a set of backups produced during a sequence of backup sessions, and that the same retention policies apply to these chains. The only difference is that files in immutable backup chains can be neither removed nor modified until the immutability period is over. Therefore, every time Veeam Backup for Microsoft Azure creates a new incremental backup containing modified data blocks, the retention period of the dependent unchanged data blocks (in the preceding incremental and full backups) is supposed to be extended. This can cause a substantial increase in I/O operations and incur additional associated costs in Microsoft Azure.

To reduce the number of requests to the repository, thus to save traffic and to reduce transaction costs, Veeam Backup for Microsoft Azure leverages the Block Generation mechanism. A generation is a period of up to 10 days that extends the retention period configured for backups in the immutable backup chain. This means that the retention period is not explicitly extended for each dependent data block every time Veeam Backup for Microsoft Azure creates a new incremental backup in the chain within one generation (during these 10 days).

> **NOTE**
>
> Veeam Backup for Microsoft Azure initiates a dedicated generation for each type of the backup schedule configured in the VM backup policy settings, SQL backup policy settings or in the Cosmos DB backup policy settings.

## How Block Generation Works

Block Generation works in the following way:

1. During the first backup session, Veeam Backup for Microsoft Azure creates a full backup in a backup repository and adds 10 days to its retention period. The full backup becomes a starting point in the first generation of the immutable backup chain.
2. During subsequent backup sessions, Veeam Backup for Microsoft Azure copies only those data blocks that have changed since the previous backup session, and stores these data blocks to incremental backups in the backup repository. The content of each incremental backup depends on the content of the full backup and the preceding incremental backups in the immutable backup chain. Veeam Backup for Microsoft Azure adds *<10 - N>* days to the retention period of these backups, where *N* is the number of days since the first backup in the generation was created.

   As a result, all backups within one generation will have the same retention date, and will not be removed by the retention policy before this date.
3. On the 11th day a new block generation period is initiated. Veeam Backup for Microsoft Azure creates a new incremental backup and adds 10 days to its retention period. This backup becomes a starting point in the second generation of the immutable backup chain. The new generation is automatically applied to all dependent data blocks from the preceding backups.
4. Veeam Backup for Microsoft Azure repeats step 2 for the second generation.
5. Veeam Backup for Microsoft Azure continues keeping dependent data blocks immutable by applying new generations to these blocks, thus continuously extending their retention period.

**IMPORTANT**

Consider the following:

- As soon as a block generation is initiated, the immutability period of data blocks in the generation cannot be reduced. Even if you change the retention period configured for image-level backups in the backup policy settings, this will not affect the expiration date of the restore points that have been already created.
- It is recommended that you do not frequently change the retention period configured for image-level backups in the backup policy settings, as this will increase the number of requests sent to the backup repository, resulting in additional service costs.

# Block Generation Example

Consider the following example. You want a backup policy to create image-level backups of your critical workloads once a day starting from March 1, and to keep the backed-up data immutable for 5 days. In this case, you do the following:

1. In the policy target settings, you set the **Enable backups** toggle to *On*, and select a backup repository with immutability enabled as the target location for the created backups.
2. In the daily scheduling settings, you select an hour when backups will be created (for example, *7:00 AM*), and specify the number of days for which Veeam Backup for Microsoft Azure will retain the created backups (*5 days*).

According to the specified scheduling settings, Veeam Backup for Microsoft Azure will create image-level backups in the following way:

1. On March 1, a backup session will start at 7:00 AM to create the full backup in the immutable backup chain. Veeam Backup for Microsoft Azure will add 10 days to the retention period specified in the backup policy settings. Thus, the retention period of the backup will be prolonged to 15 days, and the expiration date will become March 16.
2. On March 2, Veeam Backup for Microsoft Azure will create a new incremental backup at 7:00 AM and add 9 days to the retention period specified in the backup policy settings. Thus, the retention period of the incremental backup will be prolonged to 14 days, and the retention date will become March 16.
3. On March 3-10, Veeam Backup for Microsoft Azure will continue creating incremental backups and extending their retention period so that the retention date will still remain March 16.
4. On March 11, Veeam Backup for Microsoft Azure will create a new backup at 7:00 AM. During the backup session, Veeam Backup for Microsoft Azure will initiate a new block generation period, and apply the new generation to the newly created backup and all dependent data blocks. The retention period of this backup will be prolonged to 15 days, and the immutability expiration date will become March 26.

   Then, all data blocks of the preceding backups whose retention period has not been extended will be removed by a retention session due to the immutability period expiration.

# Private Network Deployment

The private deployment feature allows you to increase the security of your environment by retaining network traffic within a private network.

With Veeam Backup for Microsoft Azure, you can perform the following operations in a private environment:

- Create image-level backups and cloud-native snapshots of Azure VMs.
- Create backups of Azure SQL databases.
- Create backups of Cosmos DB accounts.
- Create cloud-native snapshots of Azure file shares.

When a backup appliance is deployed in a private environment, it is not assigned any public IPv4 address, and you will have to perform a number of additional configuration actions to allow private network access. For more information, see Working in Private Environments.

# VM Backup in Private Environment

If the private network deployment functionality is enabled for a backup appliance, Veeam Backup for Microsoft Azure performs VM backup in the following way:

1. Veeam Backup for Microsoft Azure creates snapshots of virtual disks that are attached to the processed Azure VM.

   Disk snapshots are assigned Azure tags upon creation. Values of Azure tags contain encrypted metadata that helps Veeam Backup for Microsoft Azure identify the related disk snapshots and treat them as a single unit — a cloud-native snapshot. For this reason, you must not delete any Azure tags whose names start with the word *veeam*.

2. In the region where the processed Azure VM resides, Veeam Backup for Microsoft Azure checks whether there is a virtual network configured for worker instances, and whether there is a storage account assigned the *Veeam backup appliance ID* tag with the ID of Azure VM running the backup appliance in the tag value. If there is no such network or storage account in the region, Veeam Backup for Microsoft Azure creates it.

   Veeam Backup for Microsoft Azure also checks whether the following private endpoints are configured for the Veeam storage account: one endpoint required for Azure Blob Storage and another for Azure Queue Storage. If there are no such endpoints, Veeam Backup for Microsoft Azure creates them in the same resource group, VNet and subnet where the worker instance will be launched at step 3.

3. Veeam Backup for Microsoft Azure launches the worker instance in the Azure region where the processed Azure VM resides in the following way:

   a. Uploads worker binary files to the Veeam storage account using a shared access signature (SAS) URI. Veeam Backup for Microsoft Azure validates every file by checking its MD5 key.

   b. Deploys an Azure VM running Ubuntu 22.04 LTS.

   c. Sends a Run Command to the deployed Azure VM to download the worker binary files from the Veeam storage account using a SAS URI. These files are then used to install software components required for the worker instance to perform backup and restore operations.

   d. Creates an Azure Queue in the Azure region where the backup appliance resides. Veeam Backup for Microsoft Azure then uses the Azure Queue Storage messaging service to communicate with the worker instance.

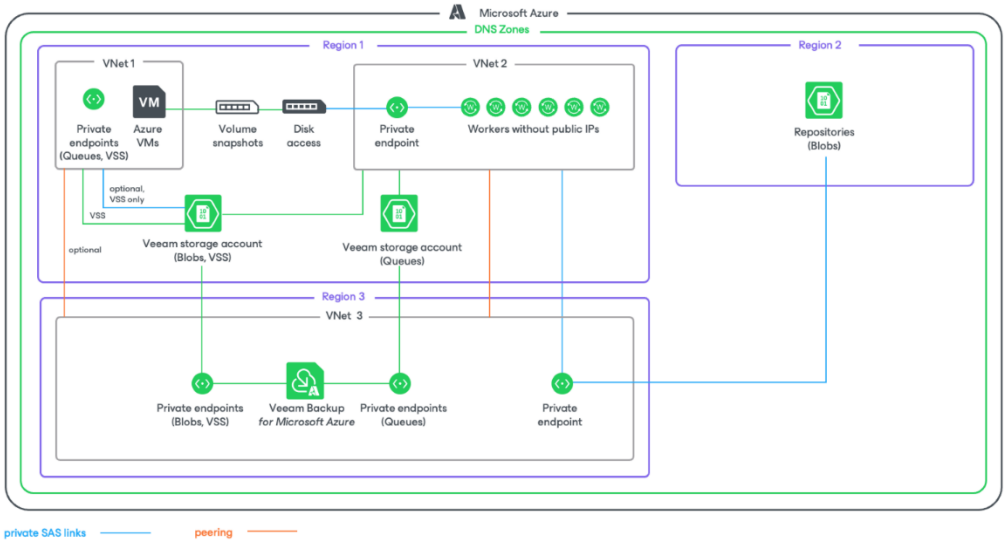
4. [Applies only if the processed Azure VM and the backup appliance are associated with the same Azure subscription] In the region where the worker instance is launched, Veeam Backup for Microsoft Azure checks whether disk access resources sufficient for the backup operation are created for the Azure subscription associated with the backup appliance. If the disk access resources are insufficient, Veeam Backup for Microsoft Azure creates them and associates these resources with the cloud-native snapshot created at step 1.

5. Veeam Backup for Microsoft Azure reads data from the cloud-native snapshot using SAS URIs, compresses the data and transfers it to the target backup repository, and stores it in the native Veeam format. Then, Veeam Backup for Microsoft Azure removes the SAS URIs.

   To reduce the amount of data read from snapshots, Veeam Backup for Microsoft Azure uses the changed block tracking (CBT) mechanism: during incremental backup sessions, Veeam Backup for Microsoft Azure compares the new cloud-native snapshot with the previous one and reads only those data blocks that have changed since the previous backup session. For more information, see Changed Block Tracking.

6. When the backup session completes, Veeam Backup for Microsoft Azure deallocates the worker instance.

7. If you enable the backup archiving mechanism, Veeam Backup for Microsoft Azure performs the following operations:
    a. Launches a worker instance in an Azure region in which the target backup repository resides.
    b. Retrieves data from the backup repository and transfers it to the target archive repository.
    c. When the archive session completes, deallocates the worker instance.



# SQL Backup in Private Environment

If the private network deployment functionality is enabled for a backup appliance, Veeam Backup for Microsoft Azure performs SQL backup in the following way:

1. [Applies only if you perform backup using a staging server] Depending on the type of the processed Azure SQL database, Veeam Backup for Microsoft Azure does the following:
   - For an Azure SQL database residing on a SQL Server — creates a copy of the source database on the staging server using the Azure REST API.
   - For a database residing on an Azure SQL Managed Instance — creates a copy of the source database on the staging server using point-in-time restore (PITR).

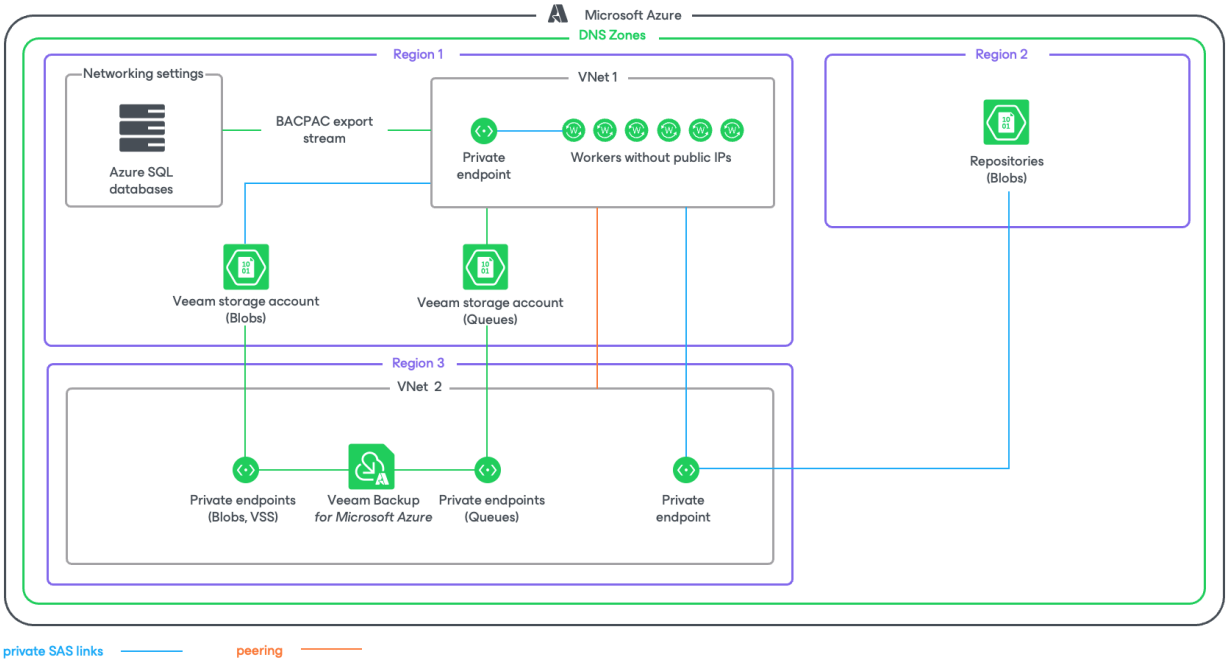
   For more information on the Azure SQL family of SQL Server database engine products, see Microsoft Docs.
2. In the region where the processed Azure SQL database resides, Veeam Backup for Microsoft Azure checks whether there is a virtual network configured for worker instances, and whether there is a storage account assigned the *Veeam* tag. If there is no such network or storage account in the region, Veeam Backup for Microsoft Azure creates it.

   Veeam Backup for Microsoft Azure also checks whether the following private endpoints are configured for the Veeam storage account: one endpoint required for Azure Blob Storage and another for Azure Queue Storage. If there are no such endpoints, Veeam Backup for Microsoft Azure creates them in the same resource group, VNet and subnet where the worker instance will be launched at step 3.
3. Veeam Backup for Microsoft Azure launches the worker instance in an Azure region where the processed Azure SQL database resides in the following way:
   a. Uploads worker binary files to the Veeam storage account using a shared access signature (SAS) URI. Veeam Backup for Microsoft Azure validates every file by checking its MD5 key.
   b. Deploys an Azure VM running Ubuntu 22.04 LTS.
   c. Sends a Run Command to the deployed Azure VM to download the worker binary files from the Veeam storage account using a SAS URI. These files are then used to install software components required for the worker instance to perform backup and restore operations.
   d. Creates an Azure Queue in the Azure region where the backup appliance resides. Veeam Backup for Microsoft Azure then uses the Azure Queue Storage messaging service to communicate with the worker instance.
4. Exports the database schema, indexes and constraints to a BACPAC file. For more information on BACPAC files, see Microsoft Docs.

> **IMPORTANT**
>
> BACPAC export of databases with external references is not supported. If a SQL database was migrated to an Azure SQL Database Server or Azure SQL Managed Instance, make sure to clear legacy references, orphaned database users and credentials set up with authentication types not supported by Azure SQL, to avoid BACPAC export errors.

5. Reads data from the exported BACPAC file on the worker instance, compresses the data and transfers it to the target backup repository, and stores it in the native Veeam format.
6. [Applies only if you perform backup using a staging server] Removes the copy of the source database from the staging server.

7. When the backup session completes, Veeam Backup for Microsoft Azure deallocates the worker instance.
8. If you enable the backup archiving mechanism, Veeam Backup for Microsoft Azure performs the following operations:
    a. Launches a worker instance in an Azure region in which the target backup repository resides.
    b. Retrieves data from the backup repository and transfers it to the target archive repository.
    c. Deallocates the worker instance when the archive session completes.



# Cosmos DB Backup in Private Environment

If the private network deployment functionality is enabled for a backup appliance, Veeam Backup for Microsoft Azure performs Cosmos DB backup in the private environment using continuous backup — a native Microsoft Azure capability that allows you to eliminate consumption of extra provisioned throughput without affecting the database performance and availability. For more information on how continuous backup is performed, see Microsoft Docs.

If you enable backup to a repository, Veeam Backup for Microsoft Azure performs Cosmos DB backup in the following way:

1. In the region where the source Cosmos DB for PostgreSQL cluster or the source Cosmos DB for MongoDB account resides, Veeam Backup for Microsoft Azure checks whether there is a virtual network configured for worker instances, and whether there is a storage account assigned the *Veeam* tag. If there is no such network or storage account in the region, Veeam Backup for Microsoft Azure creates it.

   Veeam Backup for Microsoft Azure also checks whether the following private endpoints are configured for the Veeam storage account: one endpoint required for Azure Blob Storage and another for Azure Queue Storage. If there are no such endpoints, Veeam Backup for Microsoft Azure creates them in the same resource group, VNet and subnet where the worker instance will be launched at step 2.

2. Veeam Backup for Microsoft Azure launches the worker instance in an Azure region where the processed cluster or account resides in the following way:

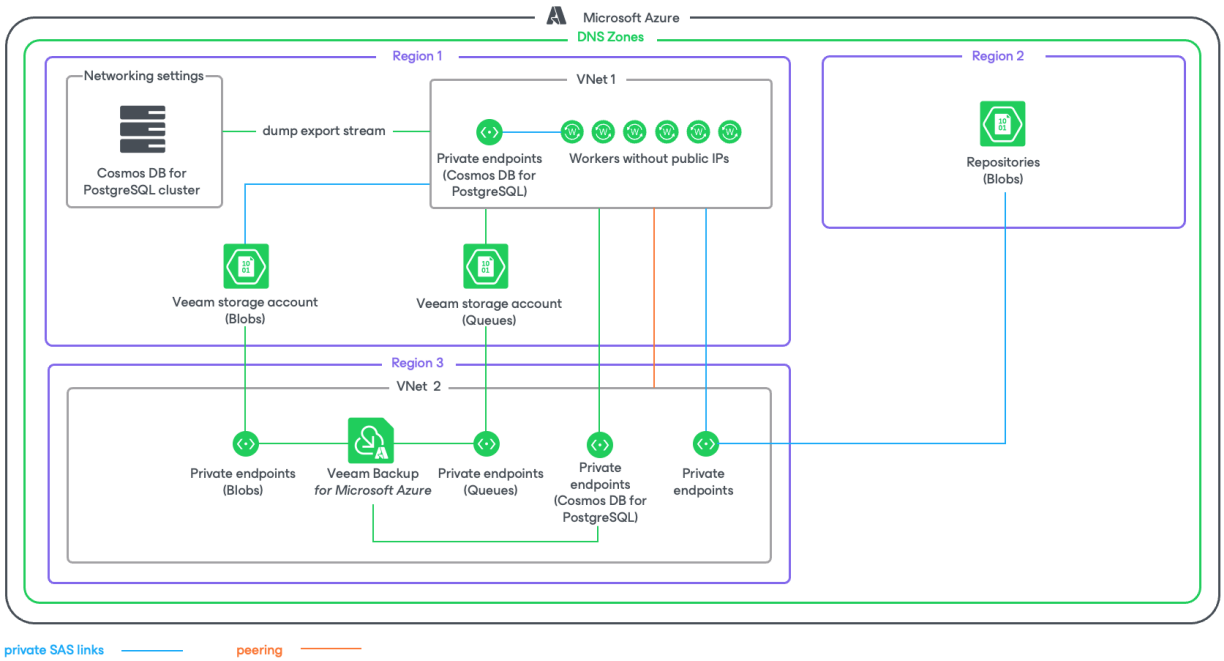
   a. Uploads worker binary files to the Veeam storage account using a shared access signature (SAS) URI. Veeam Backup for Microsoft Azure validates every file by checking its MD5 key.

   b. Deploys an Azure VM running Ubuntu 22.04 LTS.

   c. Sends a Run Command to the deployed Azure VM to download the worker binary files from the Veeam storage account using a SAS URI. These files are then used to install software components required for the worker instance to perform backup and restore operations.

   d. Creates an Azure Queue in the Azure region where the backup appliance resides. Veeam Backup for Microsoft Azure then uses the Azure Queue Storage messaging service to communicate with the worker instance.

3. If you enable backup to a repository, Veeam Backup for Microsoft Azure creates a backup file of user data contained in the database, transfers the data to the target backup repository and stores it in the native Veeam format.



# Azure Files Backup in Private Environment

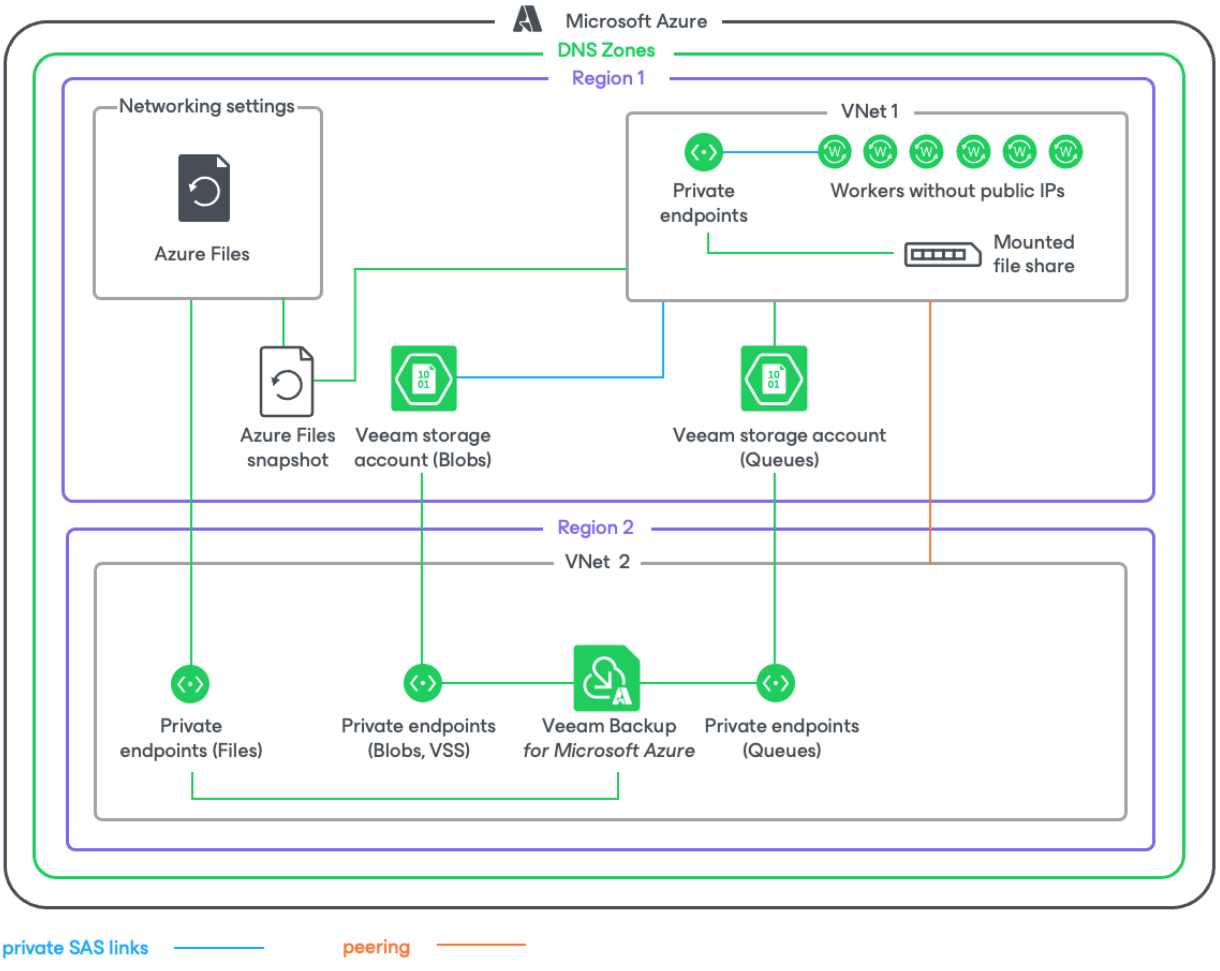
If the private network deployment functionality is enabled for a backup appliance, Veeam Backup for Microsoft Azure performs Azure Files backup in the following way:

1. Creates a share snapshot of the processed Azure file share using Microsoft Azure native capabilities.

> **NOTE**
>
> Due to Microsoft Azure limitations, the maximum number of snapshots to keep for one file share is 200.

2. If you enable file share indexing, Veeam Backup for Microsoft Azure performs the following operations:
   a. Launches a worker instance in an Azure region in which the processed file share resides.
   b. Re-creates the file share from the share snapshot created at step 1 and mounts the share to the worker instance.
   c. Reads data from the file share on the worker instance, creates a catalog of files and folders (that is, the index) of the share, and saves the index as a .ZIP file on the backup appliance.

      The creation of the .ZIP file may take significant time to complete. If a new backup policy session starts and the previous indexing session is still running, a new indexing session will not be launched.
   d. Deallocates the worker instance when the indexing session completes.



# Data Encryption

By default, Azure Storage uses service-side encryption (SSE) to automatically encrypt data. For more information on Azure Storage encryption, see Microsoft Docs.

For enhanced data security, Veeam Backup for Microsoft Azure allows you to encrypt backed-up data in backup repositories using Veeam encryption mechanisms. Veeam Backup for Microsoft Azure encrypts backup files stored in backup repositories the same way as Veeam Backup & Replication encrypts backup files stored in backup repositories. To learn what algorithms Veeam Backup & Replication uses to encrypt backup files, see the Veeam Backup & Replication User Guide, section Data Encryption.

> **NOTE**
>
> Sensitive customer data (credentials of user accounts required to connect to virtual servers and other systems, cloud credentials, and so on) is stored in the configuration database in the encrypted format.

To enable encryption for a backup repository added to Veeam Backup for Microsoft Azure, configure the repository settings as described in section Adding Backup Repositories and choose whether you want to encrypt backed-up data using a password or an Azure Key Vault cryptographic key. After you create a backup policy and specify the backup repository as a target location for Azure VM image-level backups, Azure SQL backups, Cosmos DB for PostgreSQL and Cosmos DB for MongoDB backups to a repository or virtual network configuration backup copies as described in sections Creating VM Backup Policies, Creating SQL Backup Policies, Creating Cosmos DB Backup Policies and Editing Virtual Network Configuration Backup Policy, Veeam Backup for Microsoft Azure performs the following steps:

1. Based on the provided password or Azure Key Vault key, generates an encryption key to protect instance data stored in the backup repository, and stores the key in the configuration database on the backup appliance.
2. Uses the generated key to encrypt backed-up data transferred to the backup repository when running the backup policy.

# Planning and Preparation

Before you start using Veeam Backup for Microsoft Azure, consider the following requirements:

- Hardware and software requirements.
- Network ports that must be open to ensure proper communication of Veeam Backup for Microsoft Azure components.
- Azure services to which Veeam Backup for Microsoft Azure must have outbound internet access.
- Permissions that must be assigned to accounts used to perform operations using the Veeam Backup & Replication console.
- Permissions that must be assigned to service accounts used to perform Veeam Backup for Microsoft Azure operations.
- Azure resource providers that must be registered in subscriptions.
- Considerations and limitations that should be kept in mind before you deploy Veeam Backup for Microsoft Azure.

# System Requirements

When you plan to install Microsoft Azure Plug-in for Veeam Backup & Replication, consider the following hardware and software requirements.

## Backup Server

The machine where Microsoft Azure Plug-in for Veeam Backup & Replication will run must meet system requirements described in the Veeam Backup & Replication User Guide, section System Requirements. Additionally, the following software must be installed:

- Microsoft .NET Core Runtime 8.0
- Microsoft ASP.NET Core Shared Framework 8.0

**IMPORTANT**

If the version of Microsoft .NET Core Runtime differs from the version of Microsoft ASP.NET Core Shared Framework, Microsoft Azure Plug-in for Veeam Backup & Replication services will not be able to start.

## Azure Services

The backup appliance and worker instances must have outbound internet access to a number of Microsoft Azure services. For the list of services, see Azure Services.

## Web Browsers

Internet Explorer is not supported. To access Veeam Backup for Microsoft Azure, use Microsoft Edge (latest version), Mozilla Firefox (latest version) or Google Chrome (latest version).

## Version Compatibility

**NOTE**

On February 1, 2025, the Azure AD Graph API service was retired in Microsoft Azure. As a result, Microsoft Entra applications using Azure AD Graph are no longer able to send requests to Azure AD Graph APIs. That is why Veeam Backup for Microsoft Azure versions prior to version 6.0 are not supported, as these versions use Azure AD Graph.

The following table lists compatible versions of Veeam Backup & Replication, Microsoft Azure Plug-in for Veeam Backup & Replication and Veeam Backup for Microsoft Azure.

| Veeam Backup & Replication Build | Microsoft Azure Plug-in for Veeam Backup & Replication Build | Veeam Backup for Microsoft Azure Build | Veeam Backup for Microsoft Azure Version | Backup Appliance OS Version |
|---|---|---|---|---|
| 12.3.1.1139 | 12.8.0.293 | 8.0.0.334 | 8.0 | |

| Veeam Backup & Replication Build | Microsoft Azure Plug-in for Veeam Backup & Replication Build | Veeam Backup for Microsoft Azure Build | Veeam Backup for Microsoft Azure Version | Backup Appliance OS Version |
|---|---|---|---|---|
| 12.1.2.172 and later | 12.7.1.18 | 7.1.0.59 | 7.0 | Ubuntu 22.04 LTS |
| | | 7.1.0.22 | | |
| | 12.7.0.218 | 7.0.0.467 | | |
| 12.1.0.2131 | 12.6.0.1009 | 6.0.0.234 | 6.0 | |
| 12.0.0.1420 | 12.1.5.99 | 5.1.0.75 | 5a | |
| | 12.0.5.740 | 5.0.0.579 | 5.0 | Ubuntu 18.04 LTS |
| 11.0.1.1261, including all cumulative patches starting from P20211211 (CP3) | 11.0.4.465 | 4.0.0.679 | 4.0 | |
| 11.0.1.1261, including all cumulative patches prior to P20211211 (CP3) | 11.0.3.209 | 3.0.1.19 | 3a | |
| | | 3.0.0.666 | 3.0 | |

# Ports

As Microsoft Azure Plug-in for Veeam Backup & Replication is installed on the same machine where Veeam Backup & Replication runs, it uses the same ports as those described in the Veeam Backup & Replication User Guide, section Ports. In addition, Microsoft Azure Plug-in for Veeam Backup & Replication also uses ports listed in the following table.

> **TIP**
>
> To allow inbound access to an Azure service, you can use the IP address, DNS name or virtual network service tag of the service. If you want to use an IP address, you can download a .JSON file with the full list of Azure IP ranges and service tags from the Microsoft Download Center.

| From | To | Protocol | Port | Description |
|---|---|---|---|---|
| Web browser (local machine) | Backup appliance | TCP/HTTPS | 443 | Required to access the Web UI component from a user workstation. |
| | | | | [Optional] Default port required to communicate with the public REST API service running on the backup appliance. For more information on Veeam Backup for Microsoft Azure REST API, see the Veeam Backup for Microsoft Azure REST API Reference. |
| | Worker instances | TCP/HTTPS | 443 | Required to access the file-level recovery browser running on a worker instance during the file-level restore process. |

| From | To | Protocol | Port | Description |
|---|---|---|---|---|
| Backup appliance | Veeam Update Repository (DNS name: repository.veeam.com), Amazon CloudFront (DNS names: cloudfront.net, amazonaws.com) | TCP/HTTPS | 443 | Required to download available product updates, worker deployment packages and restore utilities.<br>**Note**: Veeam Update Repository uses the Amazon CloudFront service to distribute traffic when downloading product updates. |
| | Ubuntu Security Repository (DNS name: security.ubuntu.com) and OS Update Repository (DNS name: archive.ubuntu.com) | TCP/HTTP | 80 | Required to get OS security updates. |
| | PostgreSQL Apt Repository (DNS name: apt.postgresql.org) | TCP/HTTPS | 443 | Required to get PostgreSQL updates. |
| | PostgreSQL Website (DNS name: postgresql.org) | TCP/HTTPS | 443 | Required to download the PostgreSQL Apt Repository key. |
| | Microsoft Package Repository (DNS name: packages.microsoft.com) | TCP/HTTPS | 443 | Required to get .NET updates. |
| | SMTP server (DNS name or IP address of the SMTP server) | TCP/SMTP | 25 | Default port used for sending email notifications.<br>**Note**: The TCP port **25** is used for unencrypted connection to SMTP servers. To instruct Veeam Backup for Microsoft Azure to use encrypted connection when sending email notifications, use port **587**. |
| | Microsoft Entra ID service (service tag: AzureActiveDirectory) | TCP/HTTPS | 443 | Required to add service accounts. |

| From | To | Protocol | Port | Description |
|---|---|---|---|---|
| | Azure Resource Manager service (service tag: AzureResourceManager) | TCP/HTTPS | 443 | |
| | Azure Storage service (service tag: Storage) | TCP/HTTPS | 443 | Required to access Azure storage accounts, and to communicate with worker instances using the Azure Queue Storage messaging service.<br><br>If you are planning to protect Windows-based Azure VMs, this port is also required to use the Azure Queue Storage messaging service to communicate with Volume Shadow Copy Service (VSS) agents installed on source Azure VMs with enabled guest processing option. For more information, see Performing Backup. |
| | Azure Key Vault service (service tag: AzureKeyVault) | TCP/HTTPS | 443 | Required to encrypt backup repositories using cryptographic keys. |
| | Azure Virtual Network service (service tag: VirtualNetwork) | TCP/HTTPS | 443 | Required to communicate with storage accounts where Veeam applications and scripts are stored.<br><br>**Note:** This connection is required to back up Azure resources that operate in private environments only. |
| | nginx web server (DNS name: nginx.org) | TCP/HTTPS | 443 | Required to upgrade the backup appliance. |

| From | To | Protocol | Port | Description |
|---|---|---|---|---|
| | Azure Cost Management service (DNS name: apim-ratecard-v1.azure-api.net) | TCP/HTTPS | 443 | Required to calculate estimated costs for backup policies. |
| Azure VMs | Azure Storage service (service tag: Storage) | TCP/HTTPS | 443 | [Applies to Windows-based Azure VMs only] Required to download VSS binary files and guest OS files when performing file-level recovery to the original location. |
| Worker instances | Ubuntu Security Repository (DNS name: security.ubuntu.com) and OS Update Repository (DNS name: archive.ubuntu.com) | TCP/HTTP | 80 | Required to get OS security updates. |
| | PostgreSQL Apt Repository (DNS name: apt.postgresql.org) | TCP/HTTP | 80 | Required to get PostgreSQL updates. |
| | PostgreSQL Website (DNS name: postgresql.org) | TCP/HTTPS | 443 | Required to download the PostgreSQL Apt Repository key. |
| | Azure SQL Database (service tag: Sql.*<region>*, where *<region>* is the code name of the Azure region) | TCP | 1433, 11000-11999 | Required to connect to SQL Servers.<br>**Note:** The usage of the specified TCP ports depends on the networking settings of SQL Servers. If the **Redirect** option is selected, port 1433 is used to establish only the first connection. If the **Proxy** option is selected, port 1433 is used to establish all connections by default. For more information on networking settings of SQL Servers, see Microsoft Docs. |

| From | To | Protocol | Port | Description |
|---|---|---|---|---|
| | Azure SQL Managed Instances (DNS name or IP address of the Managed Instance) | TCP | 3342 | Required to connect to Azure SQL Managed Instances using public endpoints. |
| | | TCP | 1433, 11000-11999 | Required to connect to Azure SQL Managed Instances using private endpoints.<br>**Note**: The usage of the specified TCP ports depends on the networking settings of SQL Servers. If the **Redirect** option is selected, port 1433 is used to establish only the first connection. If the **Proxy** option is selected, port 1433 is used to establish all connections by default. For more information on networking settings of SQL Servers, see Microsoft Docs. |
| | Azure Cosmos DB for PostgreSQL (service tag: AzureCosmosDB) | TCP | 5432 | Required to connect to Cosmos DB for PostgreSQL accounts. |
| | Azure Cosmos DB for MongoDB (service tag: AzureCosmosDB) | TCP | 10255 | Required to connect to Cosmos DB for MongoDB accounts. |
| | Azure Storage service (service tag: Storage) | TCP | 443 | Required to download worker binary files from Veeam storage accounts. |
| [Deprecated in Veeam Backup for Microsoft | Worker instances | TCP | 443 | Required to perform image-level backup and restore operations. |

| From | To | Protocol | Port | Description |
|---|---|---|---|---|
| Azure version 8] Service Bus service | Backup appliance | TCP | 443 | Required to communicate with Windows-based Azure VMs with enabled guest processing option. For more information, see Performing Backup. |
| Microsoft Azure Plug-in for Veeam Backup & Replication | Backup server | TCP | 6172 | Port used by Microsoft Azure Plug-in for Veeam Backup & Replication to connect to a component that enables communication with the Veeam Backup & Replication database. |
| | Backup appliance | TCP/HTTPS | 443 | Port used for communication with Veeam Backup for Microsoft Azure. |
| | Azure Resource Manager service<br><br>(DNS name: management.azure.com) | TCP/HTTPS | 443 | Required to communicate with Microsoft Azure. |
| | Microsoft Entra ID service<br><br>(DNS name: login.microsoftonline.com) | TCP/HTTPS | 443 | |
| | Microsoft Graph API<br><br>(DNS name: graph.microsoft.com) | TCP/HTTPS | 443 | Required to check permissions of Microsoft Entra applications during the upgrade of Microsoft Azure Plug-in for Veeam Backup & Replication. |
| | AWS CheckIP service<br><br>(DNS name: checkip.amazonaws.com) | TCP/HTTPS | 443 | Required to get the public IP address of the Veeam Backup & Replication server during the deployment of Microsoft Azure Plug-in for Veeam Backup & Replication. |

| From | To | Protocol | Port | Description |
|---|---|---|---|---|
| | Azure Storage service<br>(DNS name: *<blob_name>*.blob.core.windows.net, where *<blob_name>* is the name of the Azure storage account) | TCP/HTTPS | 443 | Required to access Azure storage accounts when creating backup repositories using Microsoft Azure Plug-in for Veeam Backup & Replication. |
| Veeam Backup & Replication console and Veeam ONE server | Backup server | TCP | 20443 | Port used to connect to Microsoft Azure Plug-in for Veeam Backup & Replication. |

**NOTE**

When you deploy a backup appliance from the Veeam Backup & Replication console, Veeam Backup & Replication automatically creates firewall rules for the required ports to allow communication between the backup server and the appliance components.

# Azure Services

To perform backup and restore operations in both public and private environments, Microsoft Azure Plug-in for Veeam Backup & Replication, backup appliance and worker instances must have outbound network access to the following Microsoft Azure services.

## Azure Services Required for Microsoft Azure Plug-in for Veeam Backup & Replication

- Microsoft Entra ID
- Azure Resource Manager
- Azure Storage

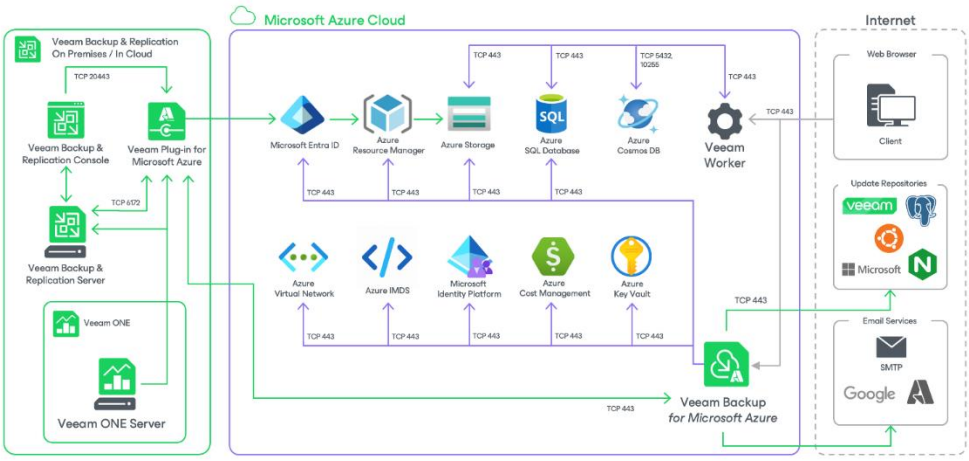
## Azure Services Required for Backup Appliance

- Microsoft Entra ID
- Azure Cost Management
- Azure Instance Metadata Service
- Azure Key Vault
- Azure Queue Storage
- Azure Resource Manager
- Azure Storage
- Azure Virtual Network, for Azure resources that operate in private environments only
- Microsoft Identity Platform

## Azure Services Required for Worker Instances

- Azure Storage
- Azure SQL Database
- Azure Cosmos DB for PostgreSQL
- Azure Cosmos DB for MongoDB

> **IMPORTANT**
>
> Consider the following:
>
> - To allow access to the services, you must open all the required network ports using either Azure network security groups or firewall rules. For the list of required network ports, see Ports.
> - If your backup appliance used the Azure Service Bus messaging service in versions prior to version 8, you must switch to the Azure Queue Storage service immediately after you upgrade to version 8. Otherwise, Veeam Backup for Microsoft Azure will no longer be able to perform backup and restore operations. For more information, see Configuring Deployment Mode.


Microsoft Azure Cloud
Internet
Veeam Backup & Replication On Premises / In Cloud
TCP 20443
Veeam Backup & Replication Console
Veeam Plug-in for Microsoft Azure
TCP 6172
Veeam Backup & Replication Server
Veeam ONE
Veeam ONE Server
Microsoft Entra ID
Azure Resource Manager
Azure Storage
Azure SQL Database
Azure Cosmos DB
Veeam Worker
Azure Virtual Network
Azure IMDS
Microsoft Identity Platform
Azure Cost Management
Azure Key Vault
Veeam Backup for Microsoft Azure
TCP 443
TCP 5432, 10255
Web Browser
Client
Update Repositories
Microsoft
Email Services
SMTP
Google

# Plug-In Permissions

To perform backup and restore operations, accounts that Microsoft Azure Plug-in for Veeam Backup & Replication uses to perform data protection and disaster recovery operations must be granted the following permissions.

## Veeam Backup & Replication User Account Permissions

A user account that you plan to use when installing and working with Veeam Backup & Replication must have permissions described in the Veeam Backup & Replication User Guide, section Installing and Using Veeam Backup & Replication.

If you plan to connect to a Veeam Backup & Replication using Remote Access Console, you must run the console as administrator.

## Veeam Backup for Microsoft Azure User Account Permissions

To get access to Veeam Backup for Microsoft Azure functionality, Veeam Backup & Replication uses user accounts of backup appliances.

A user account that will be used by Veeam Backup & Replication to authenticate against the backup appliance and get access to the appliance functionality must be assigned the Portal Administrator role. For more information on user roles, see Managing User Accounts.

> **NOTE**
>
> If you deploy a backup appliance from the Veeam Backup & Replication console, Veeam Backup & Replication will automatically create the necessary user account that will be assigned all the required permissions.

## Service Account Permissions

Microsoft Azure Plug-in for Veeam Backup & Replication requires a Microsoft Azure compute account (service account) whose permissions are used to create, connect and manage backup appliances, and to perform data protection and disaster recovery operations with Microsoft Azure resources.

You can specify an existing account or instruct Veeam Backup & Replication to create a new account:

- If you instruct Veeam Backup & Replication to create a new account, Veeam Backup & Replication creates a Microsoft Entra application in Microsoft Azure, and automatically assigns the Owner, Key Vault Crypto User and Storage Queue Data Contributor roles to the application.
- If you specify an existing account, Veeam Backup & Replication connects to an existing Microsoft Entra application that must be assigned the following set of permissions:

  Full list of permissions

```
{
"permissions": [
        {
        "actions": [
                "Microsoft.Authorization/locks/Read",
                "Microsoft.Authorization/roleAssignments/read",
```

```
                "Microsoft.Commerce/RateCard/read",
                "Microsoft.Compute/availabilitySets/read",
                "Microsoft.Compute/availabilitySets/vmSizes/read",
                "Microsoft.Compute/diskAccesses/delete",
                "Microsoft.Compute/diskAccesses/privateEndpointConnection
s/read",
                "Microsoft.Compute/diskAccesses/privateEndpointConnection
s/write",
                "Microsoft.Compute/diskAccesses/PrivateEndpointConnection
sApproval/action",
                "Microsoft.Compute/diskAccesses/read",
                "Microsoft.Compute/diskAccesses/write",
                "Microsoft.Compute/diskEncryptionSets/read",
                "Microsoft.Compute/disks/beginGetAccess/action",
                "Microsoft.Compute/disks/delete",
                "Microsoft.Compute/disks/endGetAccess/action",
                "Microsoft.Compute/disks/read",
                "Microsoft.Compute/disks/write",
                "Microsoft.Compute/snapshots/beginGetAccess/action",
                "Microsoft.Compute/snapshots/delete",
                "Microsoft.Compute/snapshots/endGetAccess/action",
                "Microsoft.Compute/snapshots/read",
                "Microsoft.Compute/snapshots/write",
                "Microsoft.Compute/sshPublicKeys/read",
                "Microsoft.Compute/sshPublicKeys/write",
                "Microsoft.Compute/sshPublicKeys/generateKeyPair/action",
                "Microsoft.Compute/virtualMachines/deallocate/action",
                "Microsoft.Compute/virtualMachines/delete",
                "Microsoft.Compute/virtualMachines/extensions/delete",
                "Microsoft.Compute/virtualMachines/extensions/read",
                "Microsoft.Compute/virtualMachines/extensions/write",
                "Microsoft.Compute/virtualMachines/read",
                "Microsoft.Compute/virtualMachines/runCommand/action",
                "Microsoft.Compute/virtualMachines/start/action",
                "Microsoft.Compute/virtualMachines/write",
                "Microsoft.DevTestLab/Schedules/write",
                "Microsoft.DevTestLab/Schedules/read",
                "Microsoft.Insights/eventtypes/values/Read",
                "Microsoft.Insights/MetricDefinitions/Read",
                "Microsoft.Insights/Metrics/Read",
                "Microsoft.KeyVault/vaults/deploy/action",
                "Microsoft.KeyVault/vaults/keys/versions/read",
                "Microsoft.KeyVault/vaults/read",
                "Microsoft.Marketplace/offerTypes/publishers/offers/plans
/agreements/read",
                "Microsoft.Marketplace/offerTypes/publishers/offers/plans
/agreements/write",
                "Microsoft.MarketplaceOrdering/offerTypes/publishers/offe
rs/plans/agreements/read",
                "Microsoft.MarketplaceOrdering/offerTypes/publishers/offe
rs/plans/agreements/write",
                "Microsoft.Network/ddosProtectionPlans/join/action",
                "Microsoft.Network/ddosProtectionPlans/read",
                "Microsoft.Network/loadBalancers/backendAddressPools/join
/action",
                "Microsoft.Network/loadBalancers/read",
                "Microsoft.Network/natGateways/join/action",
                "Microsoft.Network/natGateways/read",
                "Microsoft.Network/networkInterfaces/delete",
                "Microsoft.Network/networkInterfaces/join/action",
```

```
                "Microsoft.Network/networkInterfaces/read",
                "Microsoft.Network/networkInterfaces/write",
                "Microsoft.Network/networkSecurityGroups/delete",
                "Microsoft.Network/networkSecurityGroups/join/action",
                "Microsoft.Network/networkSecurityGroups/read",
                "Microsoft.Network/networkSecurityGroups/securityRules/de
lete",
                "Microsoft.Network/networkSecurityGroups/securityRules/re
ad",
                "Microsoft.Network/networkSecurityGroups/securityRules/wr
ite",
                "Microsoft.Network/networkSecurityGroups/write",
                "Microsoft.Network/privateDnsZones/delete",
                "Microsoft.Network/privateDnsZones/join/action",
                "Microsoft.Network/privateDnsZones/read",
                "Microsoft.Network/privateDnsZones/write",
                "Microsoft.Network/privateEndpoints/delete",
                "Microsoft.Network/privateEndpoints/privateDnsZoneGroups/
read",
                "Microsoft.Network/privateEndpoints/privateDnsZoneGroups/
write",
                "Microsoft.Network/privateEndpoints/read",
                "Microsoft.Network/privateEndpoints/write",
                "Microsoft.Network/privateLinkServices/delete",
                "Microsoft.Network/privateLinkServices/PrivateEndpointCon
nectionsApproval/action",
                "Microsoft.Network/privateLinkServices/privateEndpointCon
nections/read",
                "Microsoft.Network/privateLinkServices/privateEndpointCon
nections/write",
                "Microsoft.Network/privateLinkServices/privateEndpointCon
nections/delete",
                "Microsoft.Network/privateLinkServices/read",
                "Microsoft.Network/privateLinkServices/write",
                "Microsoft.Network/publicIPAddresses/delete",
                "Microsoft.Network/publicIPAddresses/join/action",
                "Microsoft.Network/publicIPAddresses/read",
                "Microsoft.Network/publicIPAddresses/write",
                "Microsoft.Network/routeTables/join/action",
                "Microsoft.Network/routeTables/read",
                "Microsoft.Network/routeTables/routes/delete",
                "Microsoft.Network/routeTables/routes/read",
                "Microsoft.Network/routeTables/routes/write",
                "Microsoft.Network/routeTables/write",
                "Microsoft.Network/virtualNetworks/checkIpAddressAvailabi
lity/read",
                "Microsoft.Network/virtualNetworks/delete",
                "Microsoft.Network/virtualNetworks/join/action",
                "Microsoft.Network/virtualNetworks/peer/action",
                "Microsoft.Network/virtualNetworks/read",
                "Microsoft.Network/virtualNetworks/subnets/joinViaService
Endpoint/action",
                "Microsoft.Network/virtualNetworks/subnets/join/action",
                "Microsoft.Network/virtualNetworks/subnets/read",
                "Microsoft.Network/virtualNetworks/subnets/write",
                "Microsoft.Network/virtualNetworks/virtualNetworkPeerings
/read",
                "Microsoft.Network/virtualNetworks/virtualNetworkPeerings
/write",
                "Microsoft.Network/virtualNetworks/write",
```

```
                "Microsoft.Resources/subscriptions/resourceGroups/delete"
,
                "Microsoft.Resources/subscriptions/resourceGroups/moveRes
ources/action",
                "Microsoft.Resources/subscriptions/resourceGroups/read",
                "Microsoft.Resources/subscriptions/resourceGroups/write",
                "Microsoft.Resources/subscriptions/resourceGroups/validat
eMoveResources/action",
                "Microsoft.ServiceBus/namespaces/delete",
                "Microsoft.ServiceBus/namespaces/networkrulesets/delete",
                "Microsoft.ServiceBus/namespaces/networkrulesets/read",
                "Microsoft.ServiceBus/namespaces/networkrulesets/write",
                "Microsoft.ServiceBus/namespaces/operationresults/read",
                "Microsoft.ServiceBus/namespaces/queues/authorizationRule
s/ListKeys/action",
                "Microsoft.ServiceBus/namespaces/queues/authorizationRule
s/read",
                "Microsoft.ServiceBus/namespaces/queues/authorizationRule
s/write",
                "Microsoft.ServiceBus/namespaces/queues/delete",
                "Microsoft.ServiceBus/namespaces/queues/read",
                "Microsoft.ServiceBus/namespaces/queues/write",
                "Microsoft.ServiceBus/namespaces/read",
                "Microsoft.ServiceBus/namespaces/write",
                "Microsoft.ServiceBus/register/action",
                "Microsoft.Sql/locations/*",
                "Microsoft.Sql/managedInstances/databases/delete",
                "Microsoft.Sql/managedInstances/databases/read",
                "Microsoft.Sql/managedInstances/databases/write",
                "Microsoft.Sql/managedInstances/encryptionProtector/read"
,
                "Microsoft.Sql/managedInstances/read",
                "Microsoft.Sql/servers/databases/azureAsyncOperation/read
",
                "Microsoft.Sql/servers/databases/delete",
                "Microsoft.Sql/servers/databases/read",
                "Microsoft.Sql/servers/databases/syncGroups/read",
                "Microsoft.Sql/servers/databases/transparentDataEncryptio
n/read",
                "Microsoft.Sql/servers/databases/usages/read",
                "Microsoft.Sql/servers/databases/write",
                "Microsoft.Sql/servers/elasticPools/read",
                "Microsoft.Sql/servers/encryptionProtector/read",
                "Microsoft.Sql/servers/read",
                "Microsoft.Storage/storageAccounts/blobServices/container
s/read",
                "Microsoft.Storage/storageAccounts/blobServices/container
s/write",
                "Microsoft.Storage/storageAccounts/blobServices/read",
                "Microsoft.Storage/storageAccounts/delete",
                "Microsoft.Storage/storageAccounts/listKeys/action",
                "Microsoft.Storage/storageAccounts/managementPolicies/wri
te",
                "Microsoft.Storage/storageAccounts/privateEndpointConnect
ions/write",
                "Microsoft.Storage/storageAccounts/PrivateEndpointConnect
ionsApproval/action",
                "Microsoft.Storage/storageAccounts/queueServices/queues/d
elete",
```

```
                "Microsoft.Storage/storageAccounts/queueServices/queues/r
ead",
                "Microsoft.Storage/storageAccounts/queueServices/queues/w
rite",
                "Microsoft.Storage/storageAccounts/read",
                "Microsoft.Storage/storageAccounts/write"
        ],
        "notActions": [],
        "dataActions": [
                "Microsoft.KeyVault/vaults/keys/encrypt/action",
                "Microsoft.KeyVault/vaults/keys/decrypt/action",
                "Microsoft.KeyVault/vaults/keys/read",
                "Microsoft.Storage/storageAccounts/queueServices/queues/m
essages/delete",
                "Microsoft.Storage/storageAccounts/queueServices/queues/m
essages/read",
                "Microsoft.Storage/storageAccounts/queueServices/queues/m
essages/write"
        ],
        "notDataActions": []
        }
    ]
}
```

› List of permissions to upgrade backup appliance to version 8

```
{
"permissions": [
        {
        "actions": [
                "Microsoft.Authorization/roleAssignments/read",
                "Microsoft.Compute/diskEncryptionSets/read",
                "Microsoft.Compute/disks/beginGetAccess/action",
                "Microsoft.Compute/disks/delete",
                "Microsoft.Compute/disks/endGetAccess/action",
                "Microsoft.Compute/disks/read",
                "Microsoft.Compute/disks/write",
                "Microsoft.Compute/snapshots/delete",
                "Microsoft.Compute/snapshots/read",
                "Microsoft.Compute/snapshots/write",
                "Microsoft.Compute/virtualMachines/deallocate/action",
                "Microsoft.Compute/virtualMachines/delete",
                "Microsoft.Compute/virtualMachines/extensions/delete",
                "Microsoft.Compute/virtualMachines/extensions/read",
                "Microsoft.Compute/virtualMachines/extensions/write",
                "Microsoft.Compute/virtualMachines/read",
                "Microsoft.Compute/virtualMachines/runCommand/action",
                "Microsoft.Compute/virtualMachines/start/action",
                "Microsoft.Compute/virtualMachines/write",
                "Microsoft.Network/networkInterfaces/delete",
                "Microsoft.Network/networkInterfaces/join/action",
                "Microsoft.Network/networkInterfaces/read",
                "Microsoft.Network/networkInterfaces/write",
                "Microsoft.Network/networkSecurityGroups/join/action",
                "Microsoft.Network/networkSecurityGroups/read",
                "Microsoft.Network/networkSecurityGroups/write",
                "Microsoft.Network/publicIPAddresses/join/action",
                "Microsoft.Network/publicIPAddresses/read",
```

```
                "Microsoft.Network/publicIPAddresses/write",
                "Microsoft.Network/virtualNetworks/read",
                "Microsoft.Network/virtualNetworks/subnets/join/action",
                "Microsoft.MarketplaceOrdering/offerTypes/publishers/offe
rs/plans/agreements/read",
                "Microsoft.MarketplaceOrdering/offerTypes/publishers/offe
rs/plans/agreements/write",
                "Microsoft.Resources/subscriptions/resourceGroups/read"
        ],
        "notDataActions": []
        }
    ]
}
```

# Azure SQL Account

An Azure SQL account that you plan to use to restore Microsoft Azure databases must be assigned full administrative permissions on Azure SQL servers and Azure SQL Managed Instances to which you restore databases.

# Virtualization Servers and Hosts Service Account Permissions

If you plan to copy backups to on-premises repositories, to perform restore to VMware vSphere and Microsoft Hyper-V environments, or to perform other tasks related to virtualization servers and hosts, you must check whether the service account specified for these servers and hosts has the required permissions described in the Veeam Backup & Replication User Guide for VMware vSphere and Veeam Backup & Replication User Guide for Microsoft Hyper-V, section *Using Virtualization Servers and Hosts*.

# Google Cloud Service Account Permissions

A service account that you plan to use to restore Azure VMs to Google Cloud must have permissions described in the Veeam Backup & Replication User Guide, section Google Compute Engine IAM User Permissions.

# AWS IAM User Permissions

An IAM user whose one-time access keys you plan to use to restore Azure VMs to AWS must have permissions described in the Veeam Backup & Replication User Guide, section AWS IAM User Permissions.

# Service Account Permissions

Veeam Backup for Microsoft Azure uses service accounts to perform the following operations:

- To enumerate resources added to backup policies.
- To create snapshots and backups of Azure resources protected by policies.
- To create and manage worker instances.
- To create and manage backup repositories.
- To restore Azure VMs, virtual disks, and files and folders from cloud-native snapshots and image-level backups.
- To restore Azure SQL databases and Cosmos DB accounts from backups.
- To restore files of Azure file shares from cloud-native snapshots.
- To create backups of Azure virtual network configurations.
- To restore backups of Azure virtual network configurations from backups.

To allow your backup appliance to perform these operations, service accounts that will be used to access Azure resources must be added to Veeam Backup for Microsoft Azure as described in section Adding Service Accounts. You can add the service accounts either automatically or using existing Microsoft Entra applications:

- If you choose to add an account automatically, you will not have to take any additional configuration steps since Veeam Backup for Microsoft Azure will grant all the required permissions to this account automatically.
- If you choose to add an account using an existing Microsoft Entra application, you will have to make sure the application has the following permissions granted:

```
{
"permissions": [
       {
       "actions": [
                "Microsoft.Authorization/locks/delete",
                "Microsoft.Authorization/locks/Read",
                "Microsoft.Authorization/locks/write",
                "Microsoft.Authorization/roleAssignments/read",
                "Microsoft.Commerce/RateCard/read",
                "Microsoft.Compute/availabilitySets/read",
                "Microsoft.Compute/availabilitySets/vmSizes/read",
                "Microsoft.Compute/diskAccesses/delete",
                "Microsoft.Compute/diskAccesses/privateEndpointConnections/read"
,
                "Microsoft.Compute/diskAccesses/privateEndpointConnections/write
",
                "Microsoft.Compute/diskAccesses/PrivateEndpointConnectionsApprov
al/action",
                "Microsoft.Compute/diskAccesses/read",
                "Microsoft.Compute/diskAccesses/write",
                "Microsoft.Compute/diskEncryptionSets/read",
                "Microsoft.Compute/disks/beginGetAccess/action",
                "Microsoft.Compute/disks/delete",
                "Microsoft.Compute/disks/endGetAccess/action",
                "Microsoft.Compute/disks/read",
                "Microsoft.Compute/disks/write",
                "Microsoft.Compute/snapshots/beginGetAccess/action",
                "Microsoft.Compute/snapshots/delete",
                "Microsoft.Compute/snapshots/endGetAccess/action",
                "Microsoft.Compute/snapshots/read",
                "Microsoft.Compute/snapshots/write",
                "Microsoft.Compute/virtualMachines/deallocate/action",
                "Microsoft.Compute/virtualMachines/delete",
                "Microsoft.Compute/virtualMachines/extensions/delete",
                "Microsoft.Compute/virtualMachines/extensions/read",
                "Microsoft.Compute/virtualMachines/extensions/write",
                "Microsoft.Compute/virtualMachines/read",
                "Microsoft.Compute/virtualMachines/runCommand/action",
                "Microsoft.Compute/virtualMachines/start/action",
                "Microsoft.Compute/virtualMachines/write",
                "microsoft.dbforpostgresql/servergroupsv2/*/read",
                "microsoft.dbforpostgresql/servergroupsv2/*/write",
                "Microsoft.DevTestLab/Schedules/read",
                "Microsoft.DevTestLab/Schedules/write",
                "Microsoft.DocumentDB/databaseAccounts/delete",
                "Microsoft.DocumentDB/databaseAccounts/gremlinDatabases/graphs/r
ead",
                "Microsoft.DocumentDB/databaseAccounts/gremlinDatabases/graphs/w
rite",
                "Microsoft.DocumentDB/databaseAccounts/gremlinDatabases/read",
                "Microsoft.DocumentDB/databaseAccounts/gremlinDatabases/write",
                "Microsoft.DocumentDB/databaseAccounts/listConnectionStrings/act
ion",
                "Microsoft.DocumentDB/databaseAccounts/metrics/read",
```

```
                "Microsoft.DocumentDB/databaseAccounts/mongodbDatabases/collecti
ons/read",
                "Microsoft.DocumentDB/databaseAccounts/mongodbDatabases/collecti
ons/throughputSettings/read",
                "Microsoft.DocumentDB/databaseAccounts/mongodbDatabases/collecti
ons/write",
                "Microsoft.DocumentDB/databaseAccounts/mongodbDatabases/read",
                "Microsoft.DocumentDB/databaseAccounts/mongodbDatabases/throughp
utSettings/read",
                "Microsoft.DocumentDB/databaseAccounts/mongodbDatabases/write",
                "Microsoft.DocumentDB/databaseAccounts/read",
                "Microsoft.DocumentDB/databaseAccounts/restore/action",
                "Microsoft.DocumentDB/databaseAccounts/sqlDatabases/containers/r
ead",
                "Microsoft.DocumentDB/databaseAccounts/sqlDatabases/read",
                "Microsoft.DocumentDB/databaseAccounts/sqlDatabases/write",
                "Microsoft.DocumentDB/databaseAccounts/tables/read",
                "Microsoft.DocumentDB/databaseAccounts/tables/write",
                "Microsoft.DocumentDB/databaseAccounts/write",
                "Microsoft.DocumentDB/locations/restorableDatabaseAccounts/*/rea
d",
                "Microsoft.DocumentDB/locations/restorableDatabaseAccounts/read"
,
                "Microsoft.DocumentDB/locations/restorableDatabaseAccounts/resto
re/action",
                "Microsoft.Insights/eventtypes/values/Read",
                "Microsoft.Insights/MetricDefinitions/Read",
                "Microsoft.Insights/Metrics/Read",
                "Microsoft.KeyVault/vaults/deploy/action",
                "Microsoft.KeyVault/vaults/keys/versions/read",
                "Microsoft.KeyVault/vaults/read",
                "Microsoft.Network/ddosProtectionPlans/join/action",
                "Microsoft.Network/ddosProtectionPlans/read",
                "Microsoft.Network/loadBalancers/backendAddressPools/join/action
",
                "Microsoft.Network/loadBalancers/read",
                "Microsoft.Network/natGateways/join/action",
                "Microsoft.Network/natGateways/read",
                "Microsoft.Network/networkInterfaces/delete",
                "Microsoft.Network/networkInterfaces/join/action",
                "Microsoft.Network/networkInterfaces/read",
                "Microsoft.Network/networkInterfaces/write",
                "Microsoft.Network/networkSecurityGroups/join/action",
                "Microsoft.Network/networkSecurityGroups/read",
                "Microsoft.Network/networkSecurityGroups/securityRules/delete",
                "Microsoft.Network/networkSecurityGroups/securityRules/read",
                "Microsoft.Network/networkSecurityGroups/securityRules/write",
                "Microsoft.Network/networkSecurityGroups/write",
                "Microsoft.Network/privateDnsZones/A/write",
                "Microsoft.Network/privateDnsZones/delete",
                "Microsoft.Network/privateDnsZones/join/action",
                "Microsoft.Network/privateDnsZones/read",
                "Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",
                "Microsoft.Network/privateDnsZones/virtualNetworkLinks/write",
```

```
                "Microsoft.Network/privateDnsZones/write",
                "Microsoft.Network/privateEndpoints/delete",
                "Microsoft.Network/privateEndpoints/privateDnsZoneGroups/read",
                "Microsoft.Network/privateEndpoints/privateDnsZoneGroups/write",
                "Microsoft.Network/privateEndpoints/read",
                "Microsoft.Network/privateEndpoints/write",
                "Microsoft.Network/privateLinkServices/delete",
                "Microsoft.Network/privateLinkServices/privateEndpointConnection
s/delete",
                "Microsoft.Network/privateLinkServices/privateEndpointConnection
s/read",
                "Microsoft.Network/privateLinkServices/privateEndpointConnection
s/write",
                "Microsoft.Network/privateLinkServices/PrivateEndpointConnection
sApproval/action",
                "Microsoft.Network/privateLinkServices/read",
                "Microsoft.Network/privateLinkServices/write",
                "Microsoft.Network/publicIPAddresses/delete",
                "Microsoft.Network/publicIPAddresses/join/action",
                "Microsoft.Network/publicIPAddresses/read",
                "Microsoft.Network/publicIPAddresses/write",
                "Microsoft.Network/routeTables/join/action",
                "Microsoft.Network/routeTables/read",
                "Microsoft.Network/routeTables/routes/delete",
                "Microsoft.Network/routeTables/routes/read",
                "Microsoft.Network/routeTables/routes/write",
                "Microsoft.Network/routeTables/write",
                "Microsoft.Network/virtualNetworks/checkIpAddressAvailability/re
ad",
                "Microsoft.Network/virtualNetworks/delete",
                "Microsoft.Network/virtualNetworks/join/action",
                "Microsoft.Network/virtualNetworks/peer/action",
                "Microsoft.Network/virtualNetworks/read",
                "Microsoft.Network/virtualNetworks/subnets/join/action",
                "Microsoft.Network/virtualNetworks/subnets/joinViaServiceEndpoin
t/action",
                "Microsoft.Network/virtualNetworks/subnets/read",
                "Microsoft.Network/virtualNetworks/subnets/write",
                "Microsoft.Network/virtualNetworks/virtualNetworkPeerings/delete
",
                "Microsoft.Network/virtualNetworks/virtualNetworkPeerings/read",
                "Microsoft.Network/virtualNetworks/virtualNetworkPeerings/write"
,
                "Microsoft.Network/virtualNetworks/write",
                "Microsoft.Resources/subscriptions/resourceGroups/delete",
                "Microsoft.Resources/subscriptions/resourceGroups/moveResources/
action",
                "Microsoft.Resources/subscriptions/resourceGroups/read",
                "Microsoft.Resources/subscriptions/resourceGroups/validateMoveRe
sources/action",
                "Microsoft.Resources/subscriptions/resourceGroups/write",
                "Microsoft.Search/searchServices/sharedPrivateLinkResources/oper
ationStatuses/read",
```

```
                "Microsoft.Search/searchServices/sharedPrivateLinkResources/read
",
                "Microsoft.Search/searchServices/sharedPrivateLinkResources/writ
e",
                "Microsoft.Sql/locations/*",
                "Microsoft.Sql/managedInstances/databases/delete",
                "Microsoft.Sql/managedInstances/databases/read",
                "Microsoft.Sql/managedInstances/databases/write",
                "Microsoft.Sql/managedInstances/encryptionProtector/read",
                "Microsoft.Sql/managedInstances/read",
                "Microsoft.Sql/servers/databases/azureAsyncOperation/read",
                "Microsoft.Sql/servers/databases/delete",
                "Microsoft.Sql/servers/databases/read",
                "Microsoft.Sql/servers/databases/syncGroups/read",
                "Microsoft.Sql/servers/databases/transparentDataEncryption/read"
,
                "Microsoft.Sql/servers/databases/usages/read",
                "Microsoft.Sql/servers/databases/write",
                "Microsoft.Sql/servers/elasticPools/read",
                "Microsoft.Sql/servers/encryptionProtector/read",
                "Microsoft.Sql/servers/read",
                "Microsoft.Storage/storageAccounts/blobServices/containers/read"
,
                "Microsoft.Storage/storageAccounts/blobServices/containers/write
",
                "Microsoft.Storage/storageAccounts/blobServices/read",
                "Microsoft.Storage/storageAccounts/listKeys/action",
                "Microsoft.Storage/storageAccounts/managementPolicies/write",
                "Microsoft.Storage/storageAccounts/privateEndpointConnections/wr
ite",
                "Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApp
roval/action",
                "Microsoft.Storage/storageAccounts/queueServices/queues/delete",
                "Microsoft.Storage/storageAccounts/queueServices/queues/read",
                "Microsoft.Storage/storageAccounts/queueServices/queues/write",
                "Microsoft.Storage/storageAccounts/read",
                "Microsoft.Storage/storageAccounts/write"
        ],
        "notActions": [],
        "dataActions": [
                "Microsoft.KeyVault/vaults/keys/decrypt/action",
                "Microsoft.KeyVault/vaults/keys/encrypt/action",
                "Microsoft.KeyVault/vaults/keys/read",
                "Microsoft.Storage/storageAccounts/queueServices/queues/messages
/delete",
                "Microsoft.Storage/storageAccounts/queueServices/queues/messages
/read",
                "Microsoft.Storage/storageAccounts/queueServices/queues/messages
/write"
        ],
        "notDataActions": []
        }
    ]
}
```

NOTES

- The `"Microsoft.Authorization/roleAssignments/read"` permission is required for Veeam Backup for Microsoft Azure to be able to check all other permissions granted to the related service account, and to assign new permissions to this account.
- The `dataActions` list of permissions is required only if you plan to use service accounts to manage backup repositories, and to encrypt data stored in backup repositories using the Azure Key Vault Service. Alternatively, you can assign the *Key Vault Crypto Officer* Azure built-in role to the Microsoft Entra application associated with the service account that you plan to use for backup repository management and data encryption with Azure Key Vault keys.

# Repository Permissions

To allow Veeam Backup for Microsoft Azure to create a backup repository in an Azure blob container and to access the repository when performing backup and restore operations, the service account that will be used to manage the backup repository must have the following permissions:

```
{
"permissions": [
       {
       "actions": [
                "Microsoft.Authorization/roleAssignments/read",
                "Microsoft.Compute/diskAccesses/delete",
                "Microsoft.Compute/diskAccesses/privateEndpointConnections/read"
,
                "Microsoft.Compute/diskAccesses/privateEndpointConnections/write
",
                "Microsoft.Compute/diskAccesses/PrivateEndpointConnectionsApprov
al/action",
                "Microsoft.Compute/diskAccesses/read",
                "Microsoft.Compute/diskAccesses/write",
                "Microsoft.Insights/eventtypes/values/Read",
                "Microsoft.KeyVault/vaults/deploy/action",
                "Microsoft.KeyVault/vaults/keys/versions/read",
                "Microsoft.KeyVault/vaults/read",
                "Microsoft.Network/privateEndpoints/delete",
                "Microsoft.Network/privateEndpoints/read",
                "Microsoft.Network/privateEndpoints/write",
                "Microsoft.Network/privateLinkServices/privateEndpointConnection
s/delete",
                "Microsoft.Network/privateLinkServices/privateEndpointConnection
s/read",
                "Microsoft.Network/privateLinkServices/privateEndpointConnection
s/write",
                "Microsoft.Network/virtualNetworks/subnets/joinViaServiceEndpoin
t/action",
                "Microsoft.Resources/subscriptions/resourceGroups/read",
                "Microsoft.Storage/storageAccounts/blobServices/containers/read"
,
                "Microsoft.Storage/storageAccounts/blobServices/containers/write
",
                "Microsoft.Storage/storageAccounts/blobServices/read",
                "Microsoft.Storage/storageAccounts/listKeys/action",
                "Microsoft.Storage/storageAccounts/privateEndpointConnections/wr
ite",
                "Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApp
roval/action",
                "Microsoft.Storage/storageAccounts/read"
       ],
       "notActions": [],
       "dataActions": [
                "Microsoft.KeyVault/vaults/keys/decrypt/action",
                "Microsoft.KeyVault/vaults/keys/encrypt/action",
                "Microsoft.KeyVault/vaults/keys/read"
       ],
       "notDataActions": []
       }
   ]
}
```

# Worker Permissions

To allow Veeam Backup for Microsoft Azure to launch a worker instance in an Microsoft Entra tenant and to access the instance when performing backup and restore operations, the service account that will be used to manage the worker instance must have the following permissions:

```
{
"permissions": [
       {
       "actions": [
                "Microsoft.Authorization/locks/delete",
                "Microsoft.Authorization/locks/read",
                "Microsoft.Authorization/locks/write",
                "Microsoft.Authorization/roleAssignments/read",
                "Microsoft.Commerce/RateCard/read",
                "Microsoft.Compute/diskAccesses/delete",
                "Microsoft.Compute/diskAccesses/privateEndpointConnections/read"
,
                "Microsoft.Compute/diskAccesses/privateEndpointConnections/write
",
                "Microsoft.Compute/diskAccesses/PrivateEndpointConnectionsApprov
al/action",
                "Microsoft.Compute/diskAccesses/read",
                "Microsoft.Compute/diskAccesses/write",
                "Microsoft.Compute/disks/delete",
                "Microsoft.Compute/disks/read",
                "Microsoft.Compute/disks/write",
                "Microsoft.Compute/snapshots/beginGetAccess/action",
                "Microsoft.Compute/snapshots/endGetAccess/action",
                "Microsoft.Compute/snapshots/read",
                "Microsoft.Compute/snapshots/write",
                "Microsoft.Compute/virtualMachines/deallocate/action",
                "Microsoft.Compute/virtualMachines/delete",
                "Microsoft.Compute/virtualMachines/extensions/delete",
                "Microsoft.Compute/virtualMachines/extensions/read",
                "Microsoft.Compute/virtualMachines/extensions/write",
                "Microsoft.Compute/virtualMachines/read",
                "Microsoft.Compute/virtualMachines/runCommand/action",
                "Microsoft.Compute/virtualMachines/start/action",
                "Microsoft.Compute/virtualMachines/write",
                "Microsoft.Insights/eventtypes/values/Read",
                "Microsoft.Insights/MetricDefinitions/Read",
                "Microsoft.Insights/Metrics/Read",
                "Microsoft.Network/natGateways/join/action",
                "Microsoft.Network/networkInterfaces/delete",
                "Microsoft.Network/networkInterfaces/join/action",
                "Microsoft.Network/networkInterfaces/read",
                "Microsoft.Network/networkInterfaces/write",
                "Microsoft.Network/networkSecurityGroups/join/action",
                "Microsoft.Network/networkSecurityGroups/read",
                "Microsoft.Network/networkSecurityGroups/write",
                "Microsoft.Network/privateDnsZones/A/write",
                "Microsoft.Network/privateDnsZones/join/action",
                "Microsoft.Network/privateDnsZones/read",
                "Microsoft.Network/privateDnsZones/virtualNetworkLinks/write",
                "Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",
                "Microsoft.Network/privateDnsZones/write",
                "Microsoft.Network/privateEndpoints/delete",
                "Microsoft.Network/privateEndpoints/privateDnsZoneGroups/read",
                "Microsoft.Network/privateEndpoints/privateDnsZoneGroups/write",
```

```
                "Microsoft.Network/privateEndpoints/read",
                "Microsoft.Network/privateEndpoints/write",
                "Microsoft.Network/privateLinkServices/privateEndpointConnection
s/delete",
                "Microsoft.Network/privateLinkServices/privateEndpointConnection
s/read",
                "Microsoft.Network/privateLinkServices/privateEndpointConnection
s/write",
                "Microsoft.Network/publicIPAddresses/delete",
                "Microsoft.Network/publicIPAddresses/join/action",
                "Microsoft.Network/publicIPAddresses/read",
                "Microsoft.Network/publicIPAddresses/write",
                "Microsoft.Network/virtualNetworks/delete",
                "Microsoft.Network/virtualNetworks/join/action",
                "Microsoft.Network/virtualNetworks/read",
                "Microsoft.Network/virtualNetworks/subnets/join/action",
                "Microsoft.Network/virtualNetworks/subnets/joinViaServiceEndpoin
t/action",
                "Microsoft.Network/virtualNetworks/subnets/read",
                "Microsoft.Network/virtualNetworks/subnets/write",
                "Microsoft.Network/virtualNetworks/write",
                "Microsoft.Resources/subscriptions/resourceGroups/read",
                "Microsoft.Search/searchServices/sharedPrivateLinkResources/oper
ationStatuses/read",
                "Microsoft.Search/searchServices/sharedPrivateLinkResources/read
",
                "Microsoft.Search/searchServices/sharedPrivateLinkResources/writ
e",
                "Microsoft.Storage/storageAccounts/blobServices/containers/read"
,
                "Microsoft.Storage/storageAccounts/blobServices/containers/write
",
                "Microsoft.Storage/storageAccounts/blobServices/read",
                "Microsoft.Storage/storageAccounts/listKeys/action",
                "Microsoft.Storage/storageAccounts/managementPolicies/write",
                "Microsoft.Storage/storageAccounts/privateEndpointConnections/wr
ite",
                "Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApp
roval/action",
                "Microsoft.Storage/storageAccounts/queueServices/queues/delete",
                "Microsoft.Storage/storageAccounts/queueServices/queues/read",
                "Microsoft.Storage/storageAccounts/queueServices/queues/write",
                "Microsoft.Storage/storageAccounts/read",
                "Microsoft.Storage/storageAccounts/write"
        ],
        "notActions": [],
        "dataActions": [
                "Microsoft.Storage/storageAccounts/queueServices/queues/messages
/delete",
                "Microsoft.Storage/storageAccounts/queueServices/queues/messages
/read",
                "Microsoft.Storage/storageAccounts/queueServices/queues/messages
/write"
        ],
```

```
        "notDataActions": []
        }
    ]
}
```

# Azure VM Permissions

To allow Veeam Backup for Microsoft Azure to protect Azure VMs, the service account that will be used for backup and restore operations with these VMs must have the following permissions.

## Azure VM Snapshot and Backup Permissions

```
{
"permissions": [
        {
        "actions": [
                "Microsoft.Authorization/roleAssignments/read",
                "Microsoft.Compute/disks/beginGetAccess/action",
                "Microsoft.Compute/disks/endGetAccess/action",
                "Microsoft.Compute/disks/read",
                "Microsoft.Compute/snapshots/beginGetAccess/action",
                "Microsoft.Compute/snapshots/delete",
                "Microsoft.Compute/snapshots/endGetAccess/action",
                "Microsoft.Compute/snapshots/read",
                "Microsoft.Compute/snapshots/write",
                "Microsoft.Compute/virtualMachines/read",
                "Microsoft.DevTestLab/Schedules/read",
                "Microsoft.Insights/eventtypes/values/Read",
                "Microsoft.Network/loadBalancers/read",
                "Microsoft.Network/networkInterfaces/read",
                "Microsoft.Network/networkSecurityGroups/read",
                "Microsoft.Network/publicIPAddresses/read",
                "Microsoft.Network/routeTables/join/action",
                "Microsoft.Network/virtualNetworks/read",
                "Microsoft.Resources/subscriptions/resourceGroups/read"
        ],
        "notActions": [],
        "dataActions": [],
        "notDataActions": []
        }
    ]
}
```

# Azure VM Restore Permissions

```
{
"permissions": [
        {
        "actions": [
                "Microsoft.Authorization/locks/Read",
                "Microsoft.Authorization/roleAssignments/read",
                "Microsoft.Compute/availabilitySets/read",
                "Microsoft.Compute/availabilitySets/vmSizes/read",
                "Microsoft.Compute/diskAccesses/delete",
                "Microsoft.Compute/diskAccesses/privateEndpointConnections/read"
,
                "Microsoft.Compute/diskAccesses/privateEndpointConnections/write
",
                "Microsoft.Compute/diskAccesses/PrivateEndpointConnectionsApprov
al/action",
                "Microsoft.Compute/diskAccesses/read",
                "Microsoft.Compute/diskAccesses/write",
                "Microsoft.Compute/diskEncryptionSets/read",
                "Microsoft.Compute/disks/beginGetAccess/action",
                "Microsoft.Compute/disks/delete",
                "Microsoft.Compute/disks/endGetAccess/action",
                "Microsoft.Compute/disks/read",
                "Microsoft.Compute/disks/write",
                "Microsoft.Compute/snapshots/beginGetAccess/action",
                "Microsoft.Compute/snapshots/read",
                "Microsoft.Compute/virtualMachines/deallocate/action",
                "Microsoft.Compute/virtualMachines/delete",
                "Microsoft.Compute/virtualMachines/read",
                "Microsoft.Compute/virtualMachines/write",
                "Microsoft.DevTestLab/Schedules/write",
                "Microsoft.Insights/eventtypes/values/Read",
                "Microsoft.Network/loadBalancers/backendAddressPools/join/action
",
                "Microsoft.Network/networkInterfaces/delete",
                "Microsoft.Network/networkInterfaces/join/action",
                "Microsoft.Network/networkInterfaces/read",
                "Microsoft.Network/networkInterfaces/write",
                "Microsoft.Network/networkSecurityGroups/join/action",
                "Microsoft.Network/networkSecurityGroups/read",
                "Microsoft.Network/privateEndpoints/delete",
                "Microsoft.Network/privateEndpoints/read",
                "Microsoft.Network/privateEndpoints/write",
                "Microsoft.Network/privateLinkServices/privateEndpointConnection
s/delete",
                "Microsoft.Network/privateLinkServices/privateEndpointConnection
s/read",
                "Microsoft.Network/privateLinkServices/privateEndpointConnection
s/write",
                "Microsoft.Network/publicIPAddresses/join/action",
                "Microsoft.Network/publicIPAddresses/read",
                "Microsoft.Network/publicIPAddresses/write",
                "Microsoft.Network/virtualNetworks/checkIpAddressAvailability/re
ad",
                "Microsoft.Network/virtualNetworks/read",
```

```
                "Microsoft.Network/virtualNetworks/subnets/join/action",
                "Microsoft.Network/virtualNetworks/subnets/joinViaServiceEndpoin
t/action",
                "Microsoft.Network/virtualNetworks/write",
                "Microsoft.Resources/subscriptions/resourceGroups/delete",
                "Microsoft.Resources/subscriptions/resourceGroups/moveResources/
action",
                "Microsoft.Resources/subscriptions/resourceGroups/read",
                "Microsoft.Resources/subscriptions/resourceGroups/validateMoveRe
sources/action",
                "Microsoft.Resources/subscriptions/resourceGroups/write",
                "Microsoft.Storage/storageAccounts/privateEndpointConnections/wr
ite",
                "Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApp
roval/action",
                "Microsoft.Storage/storageAccounts/write"
        ],
        "notActions": [],
        "dataActions": [],
        "notDataActions": []
        }
    ]
}
```

# Azure SQL Permissions

To allow Veeam Backup for Microsoft Azure to protect Azure SQL databases, the service account that will be used for backup and restore operations with these databases must have the following permissions.

## Azure SQL Backup Permissions

```
{
"permissions": [
        {
        "actions": [
                "Microsoft.Authorization/roleAssignments/read",
                "Microsoft.Insights/eventtypes/values/Read",
                "Microsoft.Resources/subscriptions/resourceGroups/read",
                "Microsoft.Sql/locations/*",
                "Microsoft.Sql/managedInstances/databases/delete",
                "Microsoft.Sql/managedInstances/databases/read",
                "Microsoft.Sql/managedInstances/databases/write",
                "Microsoft.Sql/managedInstances/encryptionProtector/read",
                "Microsoft.Sql/managedInstances/read",
                "Microsoft.Sql/servers/databases/azureAsyncOperation/read",
                "Microsoft.Sql/servers/databases/delete",
                "Microsoft.Sql/servers/databases/read",
                "Microsoft.Sql/servers/databases/syncGroups/read",
                "Microsoft.Sql/servers/databases/transparentDataEncryption/read"
,
                "Microsoft.Sql/servers/databases/usages/read",
                "Microsoft.Sql/servers/databases/write",
                "Microsoft.Sql/servers/elasticPools/read",
                "Microsoft.Sql/servers/encryptionProtector/read",
                "Microsoft.Sql/servers/read"
        ],
        "notActions": [],
        "dataActions": [],
        "notDataActions": []
        }
   ]
}
```

# Azure SQL Restore Permissions

```
{
"permissions": [
       {
       "actions": [
                "Microsoft.Authorization/roleAssignments/read",
                "Microsoft.Insights/eventtypes/values/Read",
                "Microsoft.Resources/subscriptions/resourceGroups/read",
                "Microsoft.Sql/locations/*",
                "Microsoft.Sql/managedInstances/databases/delete",
                "Microsoft.Sql/managedInstances/databases/read",
                "Microsoft.Sql/managedInstances/databases/write",
                "Microsoft.Sql/managedInstances/read",
                "Microsoft.Sql/servers/databases/azureAsyncOperation/read",
                "Microsoft.Sql/servers/databases/delete",
                "Microsoft.Sql/servers/databases/read",
                "Microsoft.Sql/servers/databases/write",
                "Microsoft.Sql/servers/elasticPools/read",
                "Microsoft.Sql/servers/read"
       ],
       "notActions": [],
       "dataActions": [],
       "notDataActions": []
       }
   ]
}
```

# Cosmos DB Permissions

To allow Veeam Backup for Microsoft Azure to protect Cosmos DB accounts, the service account that will be used for backup and restore operations with these accounts must have the following permissions.

## Cosmos DB Backup Permissions

```
{
"permissions": [
       {
       "actions": [
                    "Microsoft.Authorization/roleAssignments/read",
                    "microsoft.dbforpostgresql/servergroupsv2/*/read",
                    "Microsoft.DocumentDB/databaseAccounts/listConnectionStrings
/action",
                    "Microsoft.DocumentDB/databaseAccounts/metrics/read",
                    "Microsoft.DocumentDB/databaseAccounts/mongodbDatabases/coll
ections/read",
                    "Microsoft.DocumentDB/databaseAccounts/mongodbDatabases/coll
ections/throughputSettings/read",
                    "Microsoft.DocumentDB/databaseAccounts/mongodbDatabases/read
",
                    "Microsoft.DocumentDB/databaseAccounts/mongodbDatabases/thro
ughputSettings/read",
                    "Microsoft.DocumentDB/databaseAccounts/read",
                    "Microsoft.DocumentDB/databaseAccounts/write",
                    "Microsoft.DocumentDB/locations/restorableDatabaseAccounts/*
/read",
                    "Microsoft.DocumentDB/locations/restorableDatabaseAccounts/r
ead",
                    "Microsoft.Insights/eventtypes/values/Read",
                    "Microsoft.Insights/Metrics/Read",
                    "Microsoft.Resources/subscriptions/resourceGroups/read"
       ],
       "notActions": [],
       "dataActions": [],
       "notDataActions": []
       }
   ]
}
```

# Cosmos DB Restore Permissions

```
{
"permissions": [
       {
       "actions": [
                "Microsoft.Authorization/roleAssignments/read",
                "microsoft.dbforpostgresql/servergroupsv2/*/read",
                "microsoft.dbforpostgresql/servergroupsv2/*/write",
                "Microsoft.DocumentDB/databaseAccounts/delete",
                "Microsoft.DocumentDB/databaseAccounts/gremlinDatabases/graphs/r
ead",
                "Microsoft.DocumentDB/databaseAccounts/gremlinDatabases/graphs/w
rite",
                "Microsoft.DocumentDB/databaseAccounts/gremlinDatabases/read",
                "Microsoft.DocumentDB/databaseAccounts/gremlinDatabases/write",
                "Microsoft.DocumentDB/databaseAccounts/listConnectionStrings/act
ion",
                "Microsoft.DocumentDB/databaseAccounts/mongodbDatabases/collecti
ons/read",
                "Microsoft.DocumentDB/databaseAccounts/mongodbDatabases/collecti
ons/throughputSettings/read",
                "Microsoft.DocumentDB/databaseAccounts/mongodbDatabases/collecti
ons/write",
                "Microsoft.DocumentDB/databaseAccounts/mongodbDatabases/read",
                "Microsoft.DocumentDB/databaseAccounts/mongodbDatabases/throughp
utSettings/read",
                "Microsoft.DocumentDB/databaseAccounts/mongodbDatabases/write",
                "Microsoft.DocumentDB/databaseAccounts/read",
                "Microsoft.DocumentDB/databaseAccounts/restore/action",
                "Microsoft.DocumentDB/databaseAccounts/sqlDatabases/containers/r
ead",
                "Microsoft.DocumentDB/databaseAccounts/sqlDatabases/read",
                "Microsoft.DocumentDB/databaseAccounts/sqlDatabases/write",
                "Microsoft.DocumentDB/databaseAccounts/tables/read",
                "Microsoft.DocumentDB/databaseAccounts/tables/write",
                "Microsoft.DocumentDB/databaseAccounts/write",
                "Microsoft.DocumentDB/locations/restorableDatabaseAccounts/*/rea
d",
                "Microsoft.DocumentDB/locations/restorableDatabaseAccounts/read"
,
                "Microsoft.DocumentDB/locations/restorableDatabaseAccounts/resto
re/action",
                "Microsoft.Insights/eventtypes/values/Read",
                "Microsoft.Resources/subscriptions/resourceGroups/read"
       ],
       "notActions": [],
       "dataActions": [],
       "notDataActions": []
       }
   ]
}
```

# Azure Files Permissions

To allow Veeam Backup for Microsoft Azure to protect Azure file shares, the service account that will be used for backup and restore operations with the file shares must have the following permissions.

## Azure Files Snapshot and Restore Permissions

```
{
"permissions": [
        {
        "actions": [
                "Microsoft.Authorization/roleAssignments/read",
                "Microsoft.Insights/eventtypes/values/Read",
                "Microsoft.Resources/subscriptions/resourceGroups/read",
                "Microsoft.Storage/storageAccounts/listKeys/action",
                "Microsoft.Storage/storageAccounts/read"
        ],
        "notActions": [],
        "dataActions": [],
        "notDataActions": []
        }
    ]
}
```

# Virtual Network Configuration Permissions

To allow Veeam Backup for Microsoft Azure to protect virtual network configurations, the service account that will be used for backup and restore operations with these configurations must have the following permissions.

## Virtual Network Configuration Backup Permissions

```
{
"permissions": [
        {
        "actions": [
                "Microsoft.Authorization/roleAssignments/read",
                "Microsoft.Network/networkInterfaces/read",
                "Microsoft.Network/networkSecurityGroups/read",
                "Microsoft.Network/networkSecurityGroups/securityRules/read",
                "Microsoft.Network/privateDnsZones/read",
                "Microsoft.Network/privateEndpoints/privateDnsZoneGroups/read",
                "Microsoft.Network/privateEndpoints/read",
                "Microsoft.Network/privateLinkServices/privateEndpointConnection
s/read",
                "Microsoft.Network/privateLinkServices/read",
                "Microsoft.Network/publicIPAddresses/read",
                "Microsoft.Network/routeTables/read",
                "Microsoft.Network/routeTables/routes/read",
                "Microsoft.Network/virtualNetworks/read"
        ],
        "notActions": [],
        "dataActions": [],
        "notDataActions": []
        }
   ]
}
```

# Virtual Network Configuration Restore Permissions

```
{
"permissions": [
        {
        "actions": [
                "Microsoft.Authorization/roleAssignments/read",
                "Microsoft.Network/ddosProtectionPlans/join/action",
                "Microsoft.Network/ddosProtectionPlans/read",
                "Microsoft.Network/natGateways/join/action",
                "Microsoft.Network/natGateways/read",
                "Microsoft.Network/networkInterfaces/join/action",
                "Microsoft.Network/networkInterfaces/read",
                "Microsoft.Network/networkInterfaces/write",
                "Microsoft.Network/networkSecurityGroups/join/action",
                "Microsoft.Network/networkSecurityGroups/read",
                "Microsoft.Network/networkSecurityGroups/securityRules/delete",
                "Microsoft.Network/networkSecurityGroups/securityRules/read",
                "Microsoft.Network/networkSecurityGroups/securityRules/write",
                "Microsoft.Network/networkSecurityGroups/write",
                "Microsoft.Network/privateDnsZones/delete",
                "Microsoft.Network/privateDnsZones/join/action",
                "Microsoft.Network/privateDnsZones/read",
                "Microsoft.Network/privateDnsZones/write",
                "Microsoft.Network/privateEndpoints/delete",
                "Microsoft.Network/privateEndpoints/privateDnsZoneGroups/read",
                "Microsoft.Network/privateEndpoints/privateDnsZoneGroups/write",
                "Microsoft.Network/privateEndpoints/read",
                "Microsoft.Network/privateEndpoints/write",
                "Microsoft.Network/privateLinkServices/delete",
                "Microsoft.Network/privateLinkServices/privateEndpointConnection
s/delete",
                "Microsoft.Network/privateLinkServices/privateEndpointConnection
s/read",
                "Microsoft.Network/privateLinkServices/privateEndpointConnection
s/write",
                "Microsoft.Network/privateLinkServices/PrivateEndpointConnection
sApproval/action",
                "Microsoft.Network/privateLinkServices/read",
                "Microsoft.Network/privateLinkServices/write",
                "Microsoft.Network/publicIPAddresses/join/action",
                "Microsoft.Network/publicIPAddresses/read",
                "Microsoft.Network/publicIPAddresses/write",
                "Microsoft.Network/routeTables/join/action",
                "Microsoft.Network/routeTables/read",
                "Microsoft.Network/routeTables/routes/delete",
                "Microsoft.Network/routeTables/routes/read",
                "Microsoft.Network/routeTables/routes/write",
                "Microsoft.Network/routeTables/write",
                "Microsoft.Network/virtualNetworks/join/action",
                "Microsoft.Network/virtualNetworks/peer/action",
                "Microsoft.Network/virtualNetworks/read",
                "Microsoft.Network/virtualNetworks/subnets/join/action",
                "Microsoft.Network/virtualNetworks/subnets/joinViaServiceEndpoin
t/action",
                "Microsoft.Network/virtualNetworks/subnets/read",
```

```
                "Microsoft.Network/virtualNetworks/subnets/write",
                "Microsoft.Network/virtualNetworks/virtualNetworkPeerings/delete
",
                "Microsoft.Network/virtualNetworks/virtualNetworkPeerings/read",
                "Microsoft.Network/virtualNetworks/virtualNetworkPeerings/write"
,
                "Microsoft.Network/virtualNetworks/write",
                "Microsoft.Resources/subscriptions/resourceGroups/read"
            ],
            "notActions": [],
            "dataActions": [],
            "notDataActions": []
            }
    ]
}
```

# Permissions Changelog

This section describes the latest changes in service account permissions required for Veeam Backup for Microsoft Azure to perform operations.

When you update Veeam Backup for Microsoft Azure version 7.0 to version 8, consider that service accounts must be assigned additional permissions:

- For Veeam Backup for Microsoft Azure to be able to back up Cosmos DB for MongoDB accounts, service accounts must be additionally assigned the following permissions:

```
"Microsoft.DocumentDB/databaseAccounts/listConnectionStrings/action",
"Microsoft.DocumentDB/databaseAccounts/mongodbDatabases/collections/read",
"Microsoft.DocumentDB/databaseAccounts/mongodbDatabases/collections/throughputSettings/read",
"Microsoft.DocumentDB/databaseAccounts/mongodbDatabases/read",
"Microsoft.DocumentDB/databaseAccounts/mongodbDatabases/throughputSettings/read"
```

- For Veeam Backup for Microsoft Azure to be able to restore Cosmos DB for MongoDB accounts, service accounts must be additionally assigned the following permissions:

```
"Microsoft.DocumentDB/databaseAccounts/listConnectionStrings/action",
"Microsoft.DocumentDB/databaseAccounts/mongodbDatabases/collections/throughputSettings/read",
"Microsoft.DocumentDB/databaseAccounts/mongodbDatabases/throughputSettings/read",
"Microsoft.Insights/eventtypes/values/Read"
```

- For Veeam Backup for Microsoft Azure to be able to be able to allow worker instances to perform backup and restore operations in private environments, service accounts must be additionally assigned the following permissions:

```
"Microsoft.Authorization/locks/delete",
"Microsoft.Authorization/locks/read",
"Microsoft.Authorization/locks/write",
"Microsoft.Network/natGateways/join/action",
"Microsoft.Network/privateDnsZones/A/write",
"Microsoft.Network/privateDnsZones/join/action",
"Microsoft.Network/privateDnsZones/read",
"Microsoft.Network/privateDnsZones/virtualNetworkLinks/write",
"Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",
"Microsoft.Network/privateDnsZones/write",
"Microsoft.Network/privateEndpoints/privateDnsZoneGroups/read",
"Microsoft.Network/privateEndpoints/privateDnsZoneGroups/write",
"Microsoft.Network/virtualNetworks/join/action"
```

- For Veeam Backup for Microsoft Azure to be able to create and manage backup repositories and to protect Azure VMs, Azure SQL databases and Azure file shares, service accounts must be additionally assigned the following permission:

```
"Microsoft.Insights/eventtypes/values/Read"
```

# Azure Resource Providers

To perform operations, Veeam Backup for Microsoft Azure requires the following providers to be registered in your subscriptions:

- Microsoft.Authorization
- Microsoft.Commerce
- Microsoft.Compute
- Microsoft.DevTestLab
- Microsoft.KeyVault
- Microsoft.Network
- Microsoft.Resources
- Microsoft.Storage
- Microsoft.Sql
- Microsoft.ManagedServices

For more information on Azure resource providers, see Microsoft Docs.

# Considerations and Limitations

> **IMPORTANT**
>
> Veeam Backup for Microsoft Azure does not support Microsoft Azure features that are currently in the preview state. For more information, see Microsoft Docs.

When you plan to deploy and configure Veeam Backup for Microsoft Azure, keep in mind the following limitations and considerations.

## Hardware

| Component | Recommended Azure VM size |
|---|---|
| Backup appliance | • *Standard_B2s* with 2 CPUs and 4 GB RAM<br>• *Standard_B2ms* with 2 CPUs and 8 GB RAM |
| Worker instances | • *Standard_F2s_v2* with 2 CPUs and 4 GB RAM for regular backup<br>• *Standard_E2_v5* with 2 CPUs and 16 GB RAM for archived backup |

For more information on Azure VM sizes, see Microsoft Docs.

## Software

To access Veeam Backup for Microsoft Azure, use Microsoft Edge (latest version), Mozilla Firefox (latest version) or Google Chrome (latest version). Internet Explorer is not supported.

## Security Certificates

Veeam Backup for Microsoft Azure supports certificates in the formats .PFX and .P12.

## Backup Appliances

Before you start deploying backup appliances, consider the following:

- Microsoft Azure Plug-in for Veeam Backup & Replication does not support the deployment of backup appliances using Microsoft Azure compute accounts registered in China. For more information, see Microsoft Docs.

## Backup Repositories

Before you start managing backup repositories, consider the following:

- Veeam Backup for Microsoft Azure does not support creation of backup repositories in storage accounts with the Azure Data Lake Storage Gen2 hierarchical namespace enabled.
- Veeam Backup for Microsoft Azure does not support creation of backup repositories in storage accounts with the container soft delete option enabled.

- Veeam Backup for Microsoft Azure does not support creation of backup repositories in storage accounts with the blob soft delete option enabled.
- Veeam Backup for Microsoft Azure does not support creation of backup repositories in the Cold access tier. For more information on access tiers for blob data, see Microsoft Docs.
- Veeam Backup for Microsoft Azure does not support creation of mutable backup repositories in storage accounts with the blob versioning option enabled. to use an account with blob versioning enabled, consider that this may result in extra costs for storing objects that have been removed by the retention policy.
- Due to Microsoft Azure limitations, Veeam Backup for Microsoft Azure does not support creation of archive repositories in storage accounts with the Zone-redundant storage (ZRS), Geo-zone-redundant storage (GZRS) or Read-access geo-zone-redundant storage (RA-GZRS) redundancy option enabled. For more information, see Microsoft Docs.
- Veeam Backup for Microsoft Azure does not support copying backup data from one Azure blob container to another using Microsoft Azure tools and adding the new container as a repository.
- By default, Veeam Backup for Microsoft Azure does not download and check the Certificate Revocation List (CRL) files of storage accounts when creating backup repositories. If you want to instruct Veeam Backup for Microsoft Azure to download and check these files, open a support case.
- One backup repository must not be added to multiple backup appliances simultaneously. Retention sessions running on different backup appliances may corrupt backups stored in the repository, which may result in unpredictable data loss.
- If you move a storage account in which a backup repository was created to another resource group and remove the original resource group from Microsoft Azure, all operations related to that repository will fail.
- It is recommended that you use a dedicated storage account for backup repositories where Veeam Backup for Microsoft Azure will store backed-up data. Otherwise, Veeam Backup for Microsoft Azure may fail to recover the data due to folder synchronization issues.

# Network Settings for Worker Instances

Before you start adding worker configurations, consider the following:

- A virtual network service endpoint (routing) for the *Microsoft.Storage.Global* service must be configured for virtual networks to which worker instances will be connected — you can either configure the endpoint manually in Microsoft Azure beforehand or let Veeam Backup for Microsoft Azure do it for you automatically while deploying the worker instances. To learn how to configure virtual network service endpoints manually, see Microsoft Docs.
- A subnet to which worker instances will be connected must have at least one free IP address in the subnet range — Veeam Backup for Microsoft Azure will be able to launch and simultaneously run as many worker instances as many free IP addresses there are in the subnet range.
- By default, worker instances use public endpoints to connect to Azure SQL Managed Instances through port **3342**. If a worker tries to connect to an Azure SQL Managed Instance and public endpoints are disabled for this instance, the worker will use a private endpoint to connect to the instance through port **1433** instead. However, for the worker to be able to establish the connection, virtual networks to which the worker and the Azure SQL Managed Instance are connected must be peered in the Microsoft Azure portal. To learn how to peer virtual networks, see Microsoft Docs.
- For each automatically created worker configuration, Veeam Backup for Microsoft Azure creates a virtual network, a subnet and a network security group.

- It is not recommended that you manually change settings of automatically created configurations. If you want to use a specific worker configuration, add it manually as described in section Adding Worker Configurations.

For more information on worker configurations, see Managing Worker Instances.

# Backup

Before you start protecting Azure resources, consider the following:

- Veeam Backup for Microsoft Azure prioritizes SLA-based backup policies over schedule-based backup policies. If an Azure VM is included into both a schedule-based and an SLA-based backup policy, it will be processed by the SLA-based backup policy only.
- If you specify a management group as the service account scope, Veeam Backup for Microsoft Azure can include in the backup scope only those Azure subscriptions that are located at the root level of the selected management group.
- Health check cannot be performed for encrypted backups with missing metadata files, or for backups with corrupted metadata files.
- Veeam Backup for Microsoft Azure does not support backup of Azure VMs whose source disks have the data access authentication mode enabled. For more information on the data access authentication mode, see Microsoft Docs.
- Veeam Backup for Microsoft Azure does not support restore of Azure confidential VMs. For more information on Azure confidential VMs, see Microsoft Docs.
- Due to Microsoft Azure limitations, Veeam Backup for Microsoft Azure does not support backup of Ephemeral OS disks.
- Due to Microsoft Azure limitations, you can apply up to 50 tags directly to a subscription. That is why Veeam Backup for Microsoft Azure is able to create a snapshot only if the tag limit is not reached for the subscription to which the processed Azure VM belongs. If the limit is reached, the operation will fail with a serialization error. For more information on subscription limits, see Microsoft Docs.
- You can create SQL backup policies to protect only Azure SQL databases running on SQL Servers and databases located on SQL Managed Instances. If you want to protect a database hosted by a SQL Server on Azure VM, create an Azure VM backup policy. Note that in this case, you will not be able to restore a single database without restoring the entire VM.
- Veeam Backup for Microsoft Azure does not support backup of databases hosted by Azure Arc-enabled SQL Managed Instances and SQL Servers on Azure Arc-enabled servers.
- Veeam Backup for Microsoft Azure uses BACPAC files to back up SQL databases. BACPAC export of databases with external references is not supported. That is why if a SQL database was migrated to an Azure SQL Database Server or Azure SQL Managed Instance, make sure to clear legacy references, orphaned database users and credentials set up with authentication types not supported by Azure SQL, to avoid BACPAC export errors.
- Veeam Backup for Microsoft Azure does not support adding of Azure SQL Server accounts using Microsoft Entra ID authentication. To add an Azure SQL Server account, you must specify credentials of a SQL Server Admin account.
- Veeam Backup for Microsoft Azure allows you to protect only Cosmos DB accounts created using the following APIs: NoSQL, MongoDB RU-based, Apache Gremlin, Table and PostgreSQL.
- Veeam Backup for Microsoft Azure does not support backup of Cosmos DB accounts that have periodic backup or multi-region writes enabled.

- Due to Microsoft Azure limitations, Veeam Backup for Microsoft Azure does not support restore of Cosmos DB accounts encrypted using customer-managed keys.
- Due to Microsoft Azure limitations, Veeam Backup for Microsoft Azure does not support backup of NFS Azure file shares.
- If you delete a file share from Microsoft Azure, all snapshots of this file share will be deleted as well. To protect your snapshots from accidental deletion, you can use the file share soft delete option. For more information on the soft delete option for Azure Files, see Microsoft Docs.
- Before you create an Azure Files policy, make sure the **Allow storage account key access** option for Shared Key authorization is enabled for the storage accounts where the file shares you plan to protect reside — otherwise, backup operations will fail. For more information on Shared Key authorization, see Microsoft Docs.
- When performing indexing operations, Veeam Backup for Microsoft Azure uses the Server Message Block (SMB) 3.0 and New Technology LAN Manager (NTLM) v2 protocols to authenticate against the processed file shares. For more information on SMB security settings, see Microsoft Docs.
- Veeam Backup Enterprise Manager does not support management of backup policies created in Veeam Backup for Microsoft Azure.
- If you choose to back up Azure resources that are managed by specific subscriptions, belong to specific resource groups or have specific tags assigned, it may take up to 24 hours for Veeam Backup for Microsoft Azure to detect resources that either are newly deployed in the specified subscriptions and resource groups or recently have the specified tags assigned. To speed up this process and update the backup scope list, rescan the resources as described in section Performing Backup.
- Since Veeam Backup for Microsoft Azure runs retention sessions at 12:00 AM according to the time zone set on the backup appliance, it is not recommended that you schedule backup policies to execute at 12:00 AM. Otherwise, Veeam Backup for Microsoft Azure will not be able to run retention sessions.
- Since Veeam Backup for Microsoft Azure runs retention sessions for SLA-based backup policies as soon as it finalizes the backup window in all protected regions, it is recommended that you estimate how long it may take for Veeam Backup for Microsoft Azure to complete a retention session first, and then configure a backup window. Otherwise, Veeam Backup for Microsoft Azure will not be able to run retention sessions, and obsolete data will not be removed from the configuration database and backup repositories.
- Due to Microsoft Azure limitations, Veeam Backup for Microsoft Azure does not support retention of locked snapshots. This means that Veeam Backup for Microsoft Azure will not be able to remove an outdated snapshot during a retention session if the snapshot is protected from deletions and modifications using the lock feature. For more information on the lock feature, see Microsoft Docs.

# Restore

Before you start restoring Azure resources, consider the following:

- When performing restore operations, Veeam Backup for Microsoft Azure assigns Azure tags to the processed resources. If you have any Azure policies that do not allow tag assignment, the restore operations will fail. That is why it is recommended that you do not configure such policies in Microsoft Azure. For more information on Azure policies, see Microsoft Docs.
- When restoring virtual disks of an Azure VM to a new location from a cloud-native snapshot or image-level backup, Veeam Backup for Microsoft Azure does not attach the restored virtual disks to any Azure VM — the disks are placed to the specified location as standalone virtual disks.
- Veeam Backup for Microsoft Azure does not support restore of files and folders stored on volumes with Windows-native Data Deduplication enabled. For more information on the deduplication feature, see Microsoft Docs.

- Veeam Backup for Microsoft Azure does not support restore to the original location of locked Azure VMs and Azure virtual disks. For more information on the lock feature, see Microsoft Docs.
- File-level recovery is supported for the following file systems only: FAT, FAT32, NTFS, ext2, ext3, ext4, XFS, Btrfs.
- For Microsoft Windows systems, Veeam Backup for Microsoft Azure supports file-level recovery for Microsoft Windows basic volumes only. If you use Windows Storage Spaces to store data, restore an entire Azure VM to get access to your files and folders. For more information on Storage Spaces, see Microsoft Docs.
- Veeam Backup for Microsoft Azure does not support file-level recovery to the original location for files and folders of Arm-based Azure VMs. For more information on Arm-based Azure VMs, see Microsoft Docs.

# Immutability

Consider that you cannot perform the following operations with image-level backups and archived backups stored in repositories with immutability enabled:

- You cannot remove data manually using the Veeam Backup for Microsoft Azure Web UI, as described in sections Removing VM Backups and Snapshots, Removing SQL Backups, Removing Cosmos DB Backups and Removing Virtual Network Configuration Backups.
- You can neither remove data from Microsoft Azure using any cloud service provider tools nor request the technical support department to do it for you — none of the protected objects can be overwritten or deleted by any user, including the Global Administrator in your Microsoft Entra ID.

# Azure Disk Encryption

Azure Disk Encryption is supported with the following limitations:

- Backup and restore operations are supported within one Azure region only. If you choose to back up or restore your data to another region, you must first migrate to the target region all Azure key vaults, cryptographic keys and secrets used to encrypt the source Azure resources, as described in Microsoft Docs.
- File-level recovery is not supported for VMs whose virtual disks are encrypted using Azure Disk Encryption. That is, you cannot restore and browse guest OS files on disks encrypted by BitLocker for Windows-based Azure VMs, by DM-Crypt for Linux-based Azure VMs, as well as by any custom disk encryption tools.

For more information on Azure Disk Encryption, see Microsoft Docs.

# Sizing and Scalability Guidelines

This section is intended for professionals who search for a best practice answer to sizing-related issues, and assumes you have already read the whole Veeam Backup for Microsoft Azure User Guide.

Be aware that a best practice is not the only answer available. It will fit in the majority of cases but can also be totally wrong under different circumstances. Make sure you understand the implications of the recommended practices, or request assistance. If in doubt, reach out to Veeam professionals on Veeam R&D Forums.

> **IMPORTANT**
>
> You must also consider the following:
>
> - The Azure service quotas associated with your Microsoft Entra tenants and subscriptions, as well as the performance of Azure VMs of specific sizes. Some of the options may look good; however, make sure to take into account disk size, speed and burst credits.
> - The performance of Azure Storage accounts specific to your region. Storage accounts with different redundancy options (LRS, ZRS, GRS) in different regions have different speeds, and there is a maximum throughput per storage account.

# Backup Appliance

You can choose the size of the Azure VM running Veeam Backup for Microsoft Azure during the deployment, or change it later as the environment grows.

> **NOTE**
>
> In Veeam Backup for Microsoft Azure version 8, you can only choose the *B2s*, *D4s_v3* or *D8s_v3* VM size.

## General Recommendations

The following recommendations and examples apply to the latest Veeam Backup for Microsoft Azure builds.

| Azure VM Size | Recommended Maximum Number of Protected Workloads | Recommended Maximum Number of Launched Worker Instances |
|---|---|---|
| B2s (2 vCPU, 4 GB RAM) | • 500<br>• 300 (if backed up simultaneously) | 20 |
| D4s_v3 (4 vCPU, 16 GB RAM) | • 1,500<br>• 500 (if backed up simultaneously) | 150 |
| D8s_v3 (8 vCPU, 32 GB RAM) | • 3,000<br>• 1,500 (if backed up simultaneously) | 300 |

> **NOTE**
>
> For product deployments running on Azure VMs whose size is larger than *D4s_v3*, Veeam Backup for Microsoft Azure may simultaneously launch 100 worker instances per region — however, this can trigger throttling issues in Microsoft Azure. If you are facing these issues, it is recommended that you use a maximum of 70 worker instances per region at a time. Alternatively, consider reducing the number of worker instances launched simultaneously by configuring different schedules for your backup policies or by specifying different target regions. For more information, see Performing Backup.

## Veeam Backup & Replication Integration

When you connect a backup appliance to the backup infrastructure, its backup policies, cloud-native snapshots, image-level backups, backup repositories and sessions imported into the Veeam Backup & Replication database.

You can connect multiple backup appliances to a single Veeam Backup & Replication server. However, when working in an Azure subscription with cross-region data transfer, it is recommended to use one Veeam Backup & Replication server per region, to help you avoid latency issues and meet potential data residency regulations.

# Azure Files

You can adjust several configuration settings to improve the restore process by editing the configuration file `/etc/veeam/azurebackup/Config.ini`.

When you perform an FLR operation, Veeam Backup for Microsoft Azure processes simultaneously 25 folders and 25 files by default, regardless of the item size. To optimize the restore performance, you can edit the configuration file `/etc/veeam/azurebackup/Config.ini` to modify the number of items to be processed. Higher values can be especially useful when restoring files to the original location, as the speed of this restore type can far exceed the speed of restoring items to a new location.

```
[FileShareFlrOptions]
DirectoryRestoreConcurrency=25
FileRestoreConcurrency=25
```

There are also other factors that may affect the restore performance:

- The amount of CPU and RAM resources consumed by Veeam Backup for Microsoft Azure.
- The size of files if they are being restored to a new location. Larger files can increase the number of requests to Azure operations as this can trigger throttling issues.
- The subscription limits and quotas of Azure storage accounts.

> **IMPORTANT**
>
> If you encounter a throttling issue, modifying the values in the configuration file will not resolve it. In this case, it is recommended that you contact Veeam or Microsoft support for assistance.

# Backup Repository

Veeam Backup for Microsoft Azure compresses all backed-up data when saving it to backup repositories. The compression rate depends on the type and structure of source data and usually varies from 50% to 60%. This means that the compressed data typically consumes 50% less storage space than the source data.

| Parameter | Value |
|---|---|
| Average size of backed-up data | 40%-50% of source data |
| Compression rate | 50%-60% |

## Object Sizes

Depending on whether you choose to keep backed-up data in short-term or long-term storage, Veeam Backup for Microsoft Azure saves different objects to Azure blob containers.

| Object Type | Block Size |
|---|---|
| Backup data (hot and cool tiers) | 1 MB (compressed to ~512 KB) |
| Backup data (archive tier) | 512 MB |
| Metadata | 4 KB (per 1 GB of VM source data) |

## Storage Account Limits

Storage accounts have throughput limits that vary per region. It is recommended to configure multiple repositories for a single Veeam Backup for Microsoft Azure deployment, or even, in some cases, one per policy. This changes regularly, currently these limits are:

| Resource | Limit |
|---|---|
| Default maximum request rate per storage account | 20K IOPS (~512 KB block size) |
| Default maximum write speed in large regions | 60 Gbps |
| Default maximum write speed in other regions | 25 Gbps |
| Default maximum write speed for legacy storage accounts | 10 Gbps |

# Cost Estimation

Veeam Backup for Microsoft Azure comes with a built-in cost calculator that allows you to estimate your Azure expenses. It uses publicly available Microsoft Azure price lists, so it may not reflect your exact cost in case of custom pricing or an enterprise agreement. Full details can be found at the cost estimation step of the **Add Policy** wizard.

# Backup Policies

Since one policy can be used to protect multiple workloads at the same time, it is recommended that you limit the number of processed workloads to simplify the backup schedule and to optimize the backup performance.

## General Recommendations

This section provides best practices for the maximum number of workloads per policy. This number does not depend on the Azure VM size of the backup appliance.

| Resource | Maximum Workloads per Policy |
|---|---|
| Azure VM | 500 |
| Azure SQL database | 200 |

In Microsoft Azure, there is an ingress limit for Azure storage accounts, which is 7.5 GBps or approximately 60 Gbps. With 50 workloads per repository, the expected writing speed to the target backup repository is approximately 7.3 GBps (engaging 50 worker instances of the *F8s_v2 Azure* VM size), which falls under the limit. It is possible to protect more than 50 workloads per policy; however, you must configure the load options for the target backup repository as described in section Adding Backup Repositories.

> **NOTE**
>
> The performance of backup operations depends on the total volume of the processed workload data and on the size of incremental backups. That is why you need to make sure that your backup appliance has enough time to successfully run both backup and retention sessions.

## Maximizing Throughput

The number of worker instances simultaneously launched to process workloads added to a policy is defined by the speed of data upload to the repository specified for the policy. To maximize policy processing throughput, take into account that every backup and archive session started during policy execution requires a separate worker instance to be launched. For more information, see Worker Instances.

For example, one backup policy can only write to one storage account. When using a *F2s_v2* worker size with 80 MBps throughput to a storage account that can handle 25 Gbps, you can have a maximum of 3 GBps of throughput to the storage account, so a maximum of 38 worker instances. This means that for a policy that protects approximately 50 workloads, the recommended maximum number of worker instances processing simultaneously is 38.

| Workloads in Policy | Recommended Maximum Number of Worker Instances | Worker Instance Size | Worker Instance Throughput | Storage Account Throughput |
|---|---|---|---|---|
| 50 | 38<br><br>(change to fit maximum storage account throughput) | *F2s_v2*<br><br>(change to fit whatever size you choose) | 38 * 80 MBps or ~3 GBps | 25 Gbps or ~3 GBps<br><br>(check your specific storage account type and region) |

# Worker Instances

Each worker instance is deployed as an Ubuntu image, and the binaries are downloaded from the provisioning Azure storage account. Azure VM sizes of worker instances depend on the total size of virtual disks attached to the processed Azure VM, on the total size of the processed Azure SQL database, or on the total size of the processed Cosmos DB for PostgreSQL cluster or the processed Cosmos DB for MongoDB account.

If you want initial full backups to be processed quickly, it is recommended to use a larger worker profile, and then change it to a smaller profile for incremental backup. You can change worker profile settings on a regional basis, so make sure that the Azure VM sizes of worker instance size is appropriate to process the largest workload within the required time. For more information on configuring worker profiles, see Managing Worker Instances.

| Worker Profile | Default Azure VM Size | Usage | Backup Speed |
|---|---|---|---|
| Small | F2s_v2 | Backing up Azure VMs with disks smaller than 100 GB, Azure SQL databases whose total size is less than 1 GB, Cosmos DB for PostgreSQL clusters whose total size is less than 22 GB (default) | 70-85 MBps |
| Medium | F4s_v2 | Backing up Azure VMs with disks between 100 GB and 1 TB, Azure SQL databases whose total size is between 1 GB and 50 GB, Cosmos DB for PostgreSQL clusters whose total size is between 22 GB and 112 GB (default) | 90-100 MBps |
| Large | F8s_v2 | Backing up Azure VMs with disks over 1 TB, Azure SQL databases whose total size is more than 50 GB, Cosmos DB for PostgreSQL clusters whose total size is more than 112 GB, also recommended for initial full backup (default) | 125-140 MBps |
| Archiving | E2_v5 | Data tiering (default) | 85-110 MBps |

For more information on Azure VM pricing, see Microsoft Docs.

## Recommended Maximums

You can modify the default number of worker instances to reduce the amount of processing time, and choose profiles that will be used to launch worker instances in the selected regions to boost operational performance. For more information, see Adding Worker Profiles.

> **NOTE**
>
> If you are planning to perform operations that require more than 50 worker instances at a time, or if you want to use custom worker profiles for retention operations or for Cosmos DB backup and restore, open a support case.

| Purpose | Recommended Maximum Number of Worker Instances |
| --- | --- |
| Default appliance size | 50 |
| Medium appliance size | 250 |
| Large appliance size | 500 |
| Maximum per region per appliance | 1,000 |
| Azure ARM API reads (per tenant/user/hour)* | 12,000 |
| Azure ARM API writes (per tenant/user/hour)* | 1,200 |

*For more information on the Azure Management API request limits and throttling, see Microsoft Docs.

# Service Providers

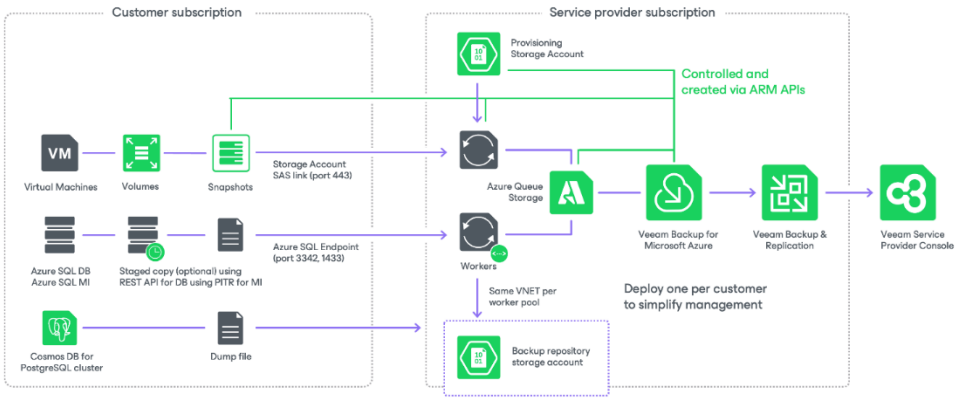
You can connect multiple backup appliances to one backup server. Normally, one backup appliance is deployed per customer, but it is possible to deploy more appliances, depending on the scale. This can be managed with Veeam Cloud Connect and the Veeam Service Provider Console (VSPC).

Worker instances and resources will be launched in the same subscription and resource group where the backup appliance is deployed. If you need to have them in the customer subscription, deploy the appliance there, and everything will work as if deployed per individual customer. You can then connect it to Veeam Backup & Replication and Veeam Service Provider Console to fulfill service provider functions.

You can use one Veeam Backup for Microsoft Azure instance to back up more than one subscription in multiple Microsoft Entra tenants. This can be done by adding an account that has access to multiple subscriptions and tenants, or by adding multiple accounts. While this is useful to segment resources, it is still recommended to deploy one backup appliance per customer from a management and scaling perspective.

You can place the backup repository storage account in a subscription separate from both the customer and service provider subscriptions, as long as you have access.

> **IMPORTANT**
>
> If your backup appliance operates in a private environment, you can protect only those Azure VMs that belong to the same tenant and subscription where this backup appliance is deployed. In this case, make sure that worker instances are also launched in the same tenant — to learn how to specify a destination for worker instances, see Managing Worker Configurations.



# Deployment

To deploy Veeam Backup for Microsoft Azure, do the following:

1. Deploy the backup server as described in the Veeam Backup & Replication User Guide, section Installing Veeam Backup & Replication.

   Alternatively, you can use a backup server that already exists in your backup infrastructure if it meets the Microsoft Azure Plug-in for Veeam Backup & Replication system requirements.

2. Install Microsoft Azure Plug-in for Veeam Backup & Replication on the backup server.

3. Deploy a backup appliance in Microsoft Azure.

# Deploying Plug-In

If your installation package of Veeam Backup & Replication does not provide features that allow you to protect Azure resources, you must install Microsoft Azure Plug-in for Veeam Backup & Replication on the backup server to be able to add your backup appliances to the backup infrastructure.

# Installing Plug-In

The default installation package of Veeam Backup & Replication does not provide features that allow you to protect Microsoft Azure resources. To be able to add your backup appliances to the backup infrastructure, you must install Microsoft Azure Plug-in for Veeam Backup & Replication on the backup server.

> **NOTE**
>
> Before you install Microsoft Azure Plug-in for Veeam Backup & Replication, stop all running policies, disable all jobs, and close the Veeam Backup & Replication console.

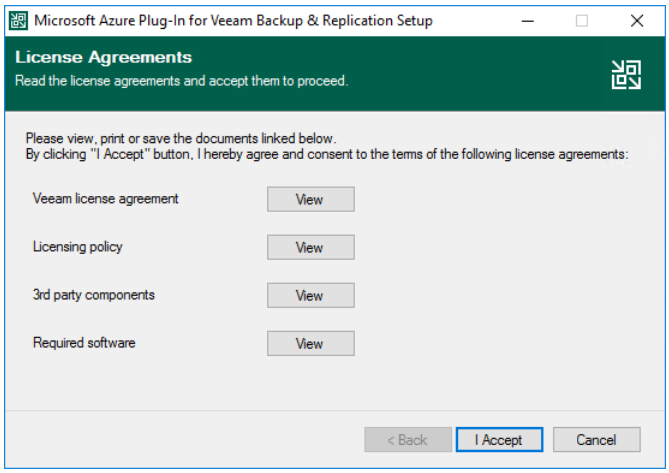
To install Microsoft Azure Plug-in for Veeam Backup & Replication, do the following:

1. Log in to the backup server using an account with the local Administrator permissions.
2. In a web browser, navigate to the Veeam Backup & Replication: Download page, switch to the **Cloud Plug-ins** in the **Additional Downloads** section, and click the **Download** icon to download Microsoft Azure Plug-in for Veeam Backup & Replication.
3. Open the downloaded `MicrosoftAzurePlugin_12.8.0.293.zip` file and launch the `MicrosoftAzurePlugin_12.8.0.293.exe` installation file.
4. Complete the **Microsoft Azure Plug-in for Veeam Backup & Replication** wizard:
   a. At the **License Agreements** step, read and accept the Veeam license agreement and licensing policy, as well as the license agreements of 3rd party components that Veeam incorporates, and the license agreements of required software. If you reject the agreements, you will not be able to continue installation.

      To read the terms of the agreements, click **View**.

   b. At the **Installation Path** step, you can specify the installation directory. To do that, click **Browse**. In the **Browse for folder** window, select the installation directory for the product or create a new one, and click **OK**.

c. At the **Ready to Install** step, click **Install** to begin installation.



# Installing and Uninstalling Plug-In in Unattended Mode

You can install or uninstall Microsoft Azure Plug-in for Veeam Backup & Replication in the unattended mode using the command line interface. The unattended mode does not require user interaction — the installation runs automatically in the background, and you do not have to respond to the installation wizard prompts. You can use it to automate processes in large-scale environments.

To install Microsoft Azure Plug-in for Veeam Backup & Replication in unattended mode, use either of the following options:

- If Microsoft Azure Plug-in for Veeam Backup & Replication is a part of Veeam Backup & Replication installation package, follow the instructions provided in the Veeam Backup & Replication User Guide, section Installing Veeam Backup & Replication in Silent Mode.
- If Microsoft Azure Plug-in for Veeam Backup & Replication is delivered as a separate .EXE file, use the instructions from this subsection.

## Before You Begin

Before you start unattended installation, do the following:

1. Download the Microsoft Azure Plug-in for Veeam Backup & Replication .EXE file as described in section Installing Plug-In (steps 1-4).
2. Check compatibility of Microsoft Azure Plug-in for Veeam Backup & Replication and Veeam Backup & Replication versions. For more information, see System Requirements.

## Installation Command-Line Syntax

Open the command prompt and run the .EXE file using the following parameters:

```
%path% /silent /accepteula /acceptlicensingpolicy /acceptthirdpartylicenses /ac
ceptrequiredsoftware [/uninstall]
```

The following command-line parameters are used to run the setup file:

| Parameter | Required | Description |
|---|---|---|
| %path% | Yes | Specifies a path to the installation .EXE file on the backup server or in a network shared folder. |
| /silent | Yes | Sets the user interface level to *None*, which means no user interaction is needed during installation. |
| /accepteula | Yes | Confirms that you accept the terms of the Veeam license agreement. |

| Parameter | Required | Description |
| --- | --- | --- |
| /acceptlicensingpolicy | Yes | Confirms that you accept the Veeam licensing policy. |
| /acceptthirdpartylicenses | Yes | Confirms that you accept the license agreement for 3rd party components that Veeam incorporates. |
| /acceptrequiredsoftware | Yes | Confirms that you accept the license agreements for each required software that Veeam will install. |
| /uninstall | No | Uninstalls the plug-in.<br>**Example:** `"AzurePlugin_12.8.0.293.exe /silent /accepteula /acceptlicensingpolicy /acceptthirdpartylicenses /acceptrequiredsoftware /uninstall"` |

# Upgrading Plug-In

To upgrade Microsoft Azure Plug-in for Veeam Backup & Replication, do the following:

1. Install the new version of Microsoft Azure Plug-in for Veeam Backup & Replication as described in section Installing Plug-In.
2. Upgrade backup appliances from the Veeam Backup & Replication console as described in section Updating Appliances Using Console.

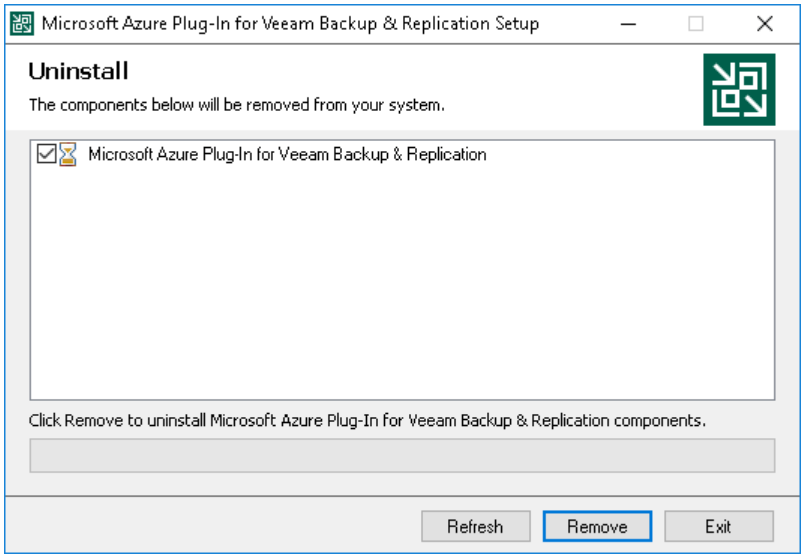
# Uninstalling Plug-In

Before you uninstall Microsoft Azure Plug-in for Veeam Backup & Replication, it is recommended to remove all connected backup appliances from the backup infrastructure. If you keep the appliances in the backup infrastructure, the following will happen:

- You will be able to see information on snapshots of Azure VMs and file shares in the Veeam Backup & Replication console. However, you will not be able to perform any operations with these snapshots.
- You will be able to see information on backups of Azure SQL databases. However, you will not be able to perform any operations with these backups.
- You will be able to see information on image-level backups of Azure VMs and perform data recovery operations using these backups. However, restore of entire VMs to Microsoft Azure will start working as described in the Veeam Backup & Replication User Guide, section How Restore to Microsoft Azure Works.
- You will be able to see information on backup policies. However, you will only be able to remove these policies from the Veeam Backup & Replication console.

To uninstall Microsoft Azure Plug-in for Veeam Backup & Replication, do the following:

1. Log in to the backup server using an account with the local Administrator permissions.
2. Open the **Start** menu, navigate to **Control Panel** > **Programs** > **Programs and Features**.
3. In the program list, click **Microsoft Azure Plug-in for Veeam Backup & Replication** and click **Uninstall**.
4. In the opened window, click **Remove**.




**NOTE**

After you uninstall Microsoft Azure Plug-in for Veeam Backup & Replication, you will be no longer able to add backup appliances and new external repositories to the backup infrastructure.

# Deploying Backup Appliance

Veeam Backup for Microsoft Azure is installed on an Azure VM that is created in a selected Azure subscription during the product installation. You can deploy Veeam Backup for Microsoft Azure from the Veeam Backup & Replication console only.

When deploying Veeam Backup for Microsoft Azure, Veeam Backup & Replication performs the following steps:

1. Deploys an Azure VM from the Ubuntu 22.04 LTS image.
2. Creates a temporary storage account in Microsoft Azure and uploads Veeam Backup for Microsoft Azure installation packages and their dependencies to the account.

   Alternatively, Veeam Backup & Replication can use a custom storage account with private access. For Veeam Backup & Replication to be able to do that, the account must belong to the resource group where the backup appliance will reside and must be assigned the *Veeam backup for Azure deployment account* Azure tag with an empty value. To learn how to apply tags to Azure resources, see Microsoft Docs.
3. Installs the required software components on the Azure VM.
4. Creates a default service account on the backup appliance. This service account will then be used to perform data protection and recovery operations within the Azure subscription to which the backup appliance belongs. Out of the box, the account is already assigned all the required permissions listed in section Service Account Permissions.

   You will be able to add other service accounts later, after Veeam Backup for Microsoft Azure installation. For more information, see Managing Service Accounts.
5. Removes the temporary storage account from Microsoft Azure.

## How to Perform Appliance Deployment

To deploy a new backup appliance from the Veeam Backup & Replication console, do the following:

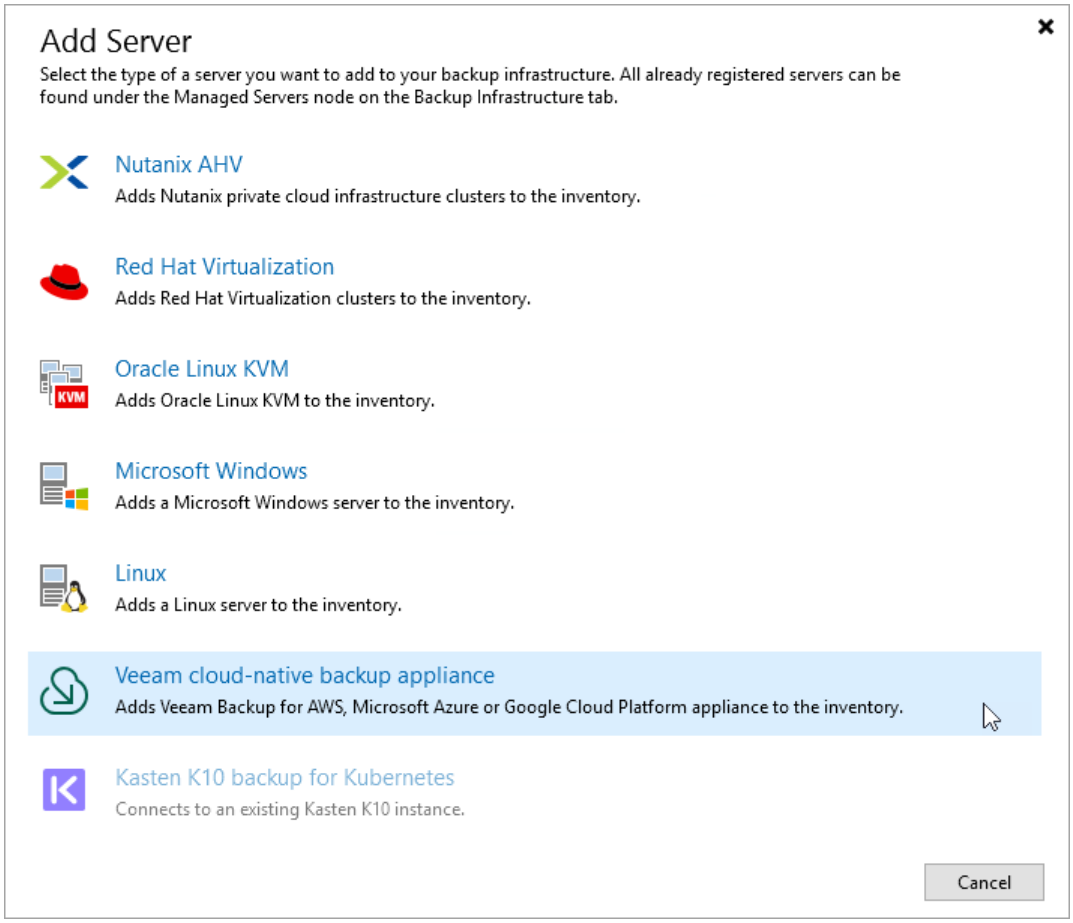
1. Launch the New Veeam Backup for Microsoft Azure appliance wizard.
2. Choose a deployment mode.
3. Specify service account settings.
4. Specify an Azure subscription in which the appliance will be deployed.
5. Specify a name and description for the appliance.
6. Specify the connection type.
7. Specify network settings for the appliance.
8. Specify credentials for the default user account.
9. Wait for the appliance to be added to the backup infrastructure.
10. Finish working with the wizard.

# Step 1. Launch New Veeam Backup for Microsoft Azure Appliance Wizard

To launch the **New Veeam Backup for Microsoft Azure Appliance** wizard, do the following:

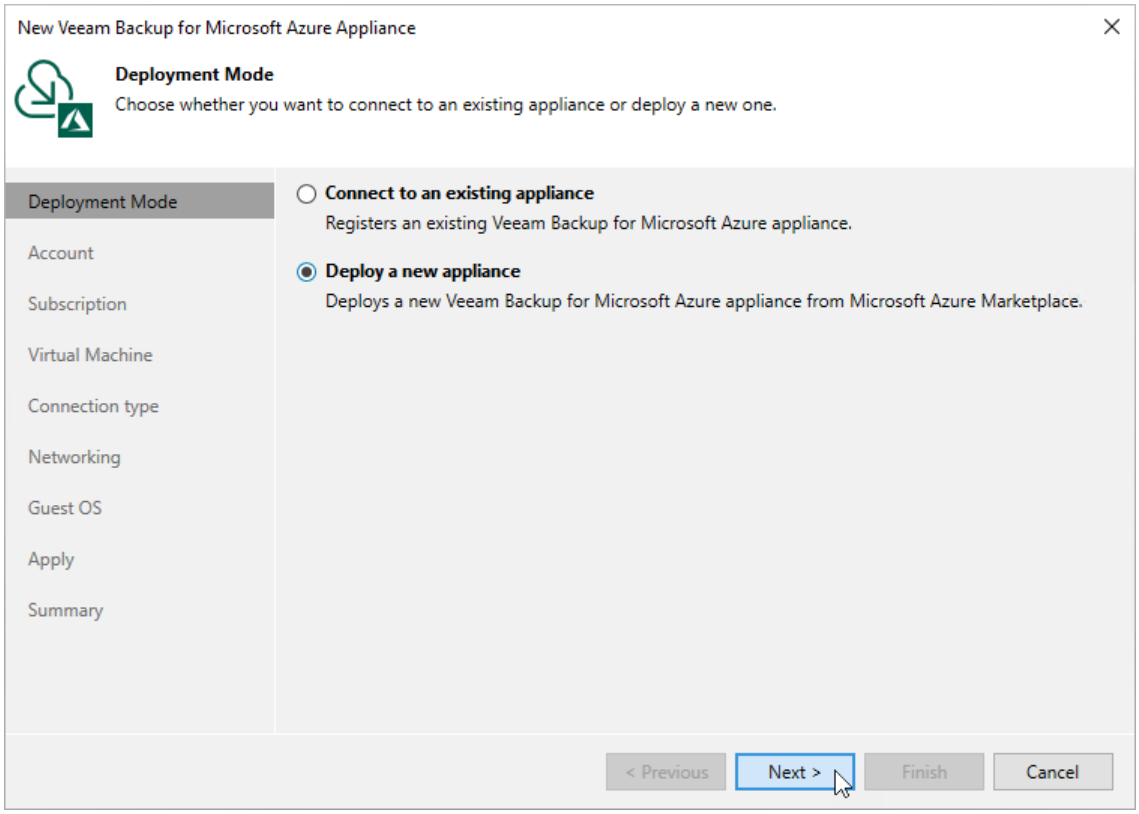
1. In the Veeam Backup & Replication console, open the **Backup Infrastructure** view.
2. Navigate to **Managed Servers** and click **Add Server** on the ribbon.

   Alternatively, you can right-click the **Managed Servers** node and select **Add Server**.
3. In the **Add Server** window:
   a. [Applies only if you have several cloud plug-ins installed] Click **Veeam cloud-native backup appliance**.
   b. Choose **Veeam Backup for Microsoft Azure**.



# Step 2. Choose Deployment Mode

At the **Deployment Mode** step of the wizard, select the **Deploy a new appliance** option.



# Step 3. Specify Microsoft Azure Compute Account Settings

At the **Account** step of the wizard, select a Microsoft Azure compute account whose permissions will be used to deploy the new backup appliance. By default, Veeam Backup & Replication will also use the Microsoft Entra application associated with the Microsoft Azure compute account to create a default service account on the backup appliance. If you do not want Veeam Backup & Replication to create the default service account, make sure the **Create the default service account by importing this compute account** check box is not selected.

> **NOTE**
>
> Out of the box, Veeam Backup for Microsoft Azure does not create any default service accounts for standalone backup appliances — only Veeam Backup & Replication can automatically create such an account in Veeam Backup for Microsoft Azure during the backup appliance deployment from the Veeam Backup & Replication console.

For a Microsoft Azure compute account to be displayed in the **Microsoft Azure compute account** drop-down list, it must be added to the Cloud Credentials Manager as described in the Veeam Backup & Replication User Guide, section Microsoft Azure Compute Accounts. If you have not added the necessary account to the Cloud Credentials Manager beforehand, you can do it without closing the **New Veeam Backup for Microsoft Azure Appliance** wizard. To do that, click either the **Manage accounts** link or the **Add** button, and complete the **Microsoft Azure Compute Account** wizard.

When completing the **Microsoft Azure Compute Account** wizard, you will have 2 options at the **Account Type** step — either to use an existing or to create a new Microsoft Entra application:

- If you select the **Create a new account** option, Veeam Backup & Replication will create a new Microsoft Entra application in your Microsoft Entra ID.

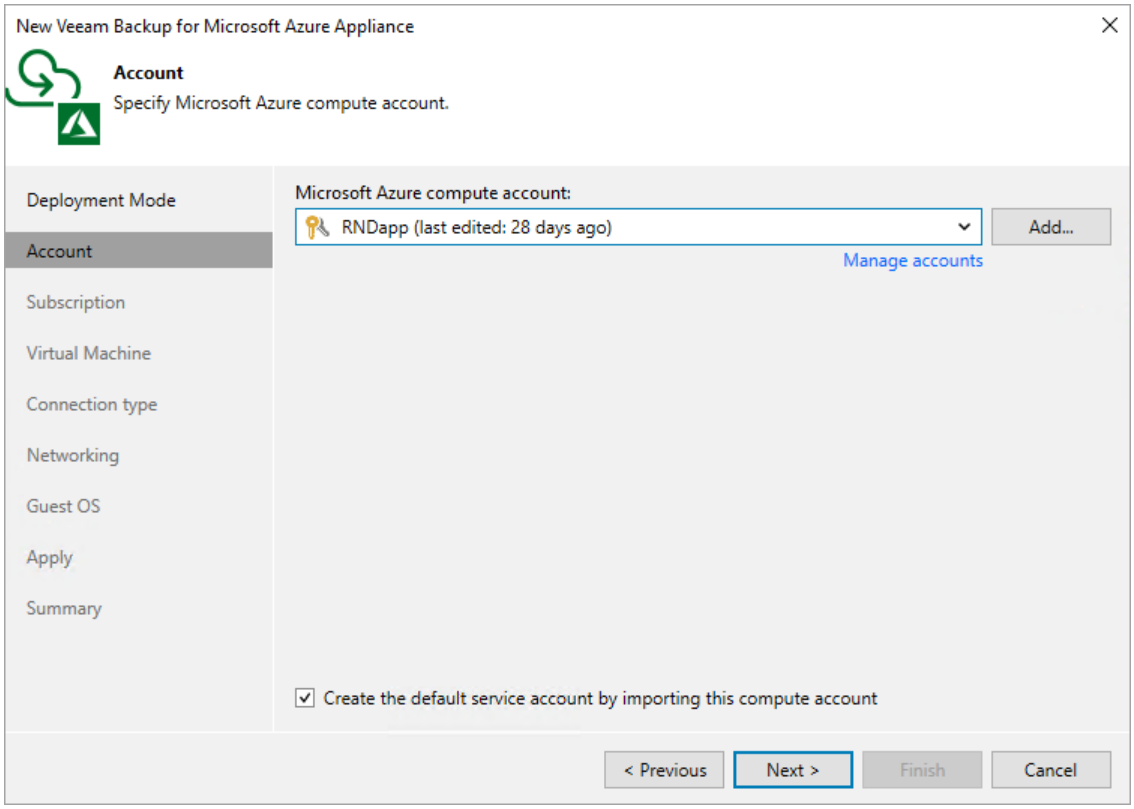
  The newly created application will be automatically assigned the *Key Vault Crypto User*, *Owner* and *Storage Queue Data Contributor* Azure built-in roles. Note that the *Owner* role has a wide scope of permissions and capabilities, which is required for the Microsoft Azure Compute account to perform restore operations in Veeam Backup & Replication. That is why it is not recommended that you unassign any operational roles from the default service account in Veeam Backup for Microsoft Azure — if you want the application to be assigned a limited list of permissions, manually create a Microsoft Entra application in Microsoft Azure as described in Microsoft Docs.

- If you select the **Use the existing account** option, Veeam Backup & Replication will use the scope of permissions assigned to an existing Microsoft Entra application.

  For Veeam Backup & Replication to be able to connect to the application, it must be created in Microsoft Azure as described in Microsoft Docs, and must have all the permissions required to perform backup and restore operations. For the list of required permissions, see Plug-In Permissions.

  To provide permissions to the application, you must create a custom role in Microsoft Azure, grant the necessary permissions to this role, and then assign the role to the application.

> **IMPORTANT**
>
> Microsoft Azure Stack Hub accounts are not supported. For more information, see Microsoft Docs.


New Veeam Backup for Microsoft Azure Appliance
Account
Specify Microsoft Azure compute account.
Deployment Mode
Account
Subscription
Virtual Machine
Connection type
Networking
Guest OS
Apply
Summary
Microsoft Azure compute account:
RNDapp (last edited: 28 days ago)
Add...
Manage accounts
Create the default service account by importing this compute account
< Previous
Next >
Finish
Cancel

# Step 4. Specify Subscription

At the **Subscription** step of the wizard, do the following:

1. From the **Subscription** drop-down list, select an Azure subscription that will be used to manage costs of the backup appliance.

   For a subscription to be displayed in the list of available subscriptions, it must be created in Microsoft Azure and associated with the Microsoft Entra tenant to which the Microsoft Azure compute account specified at step 3 of the wizard belongs.

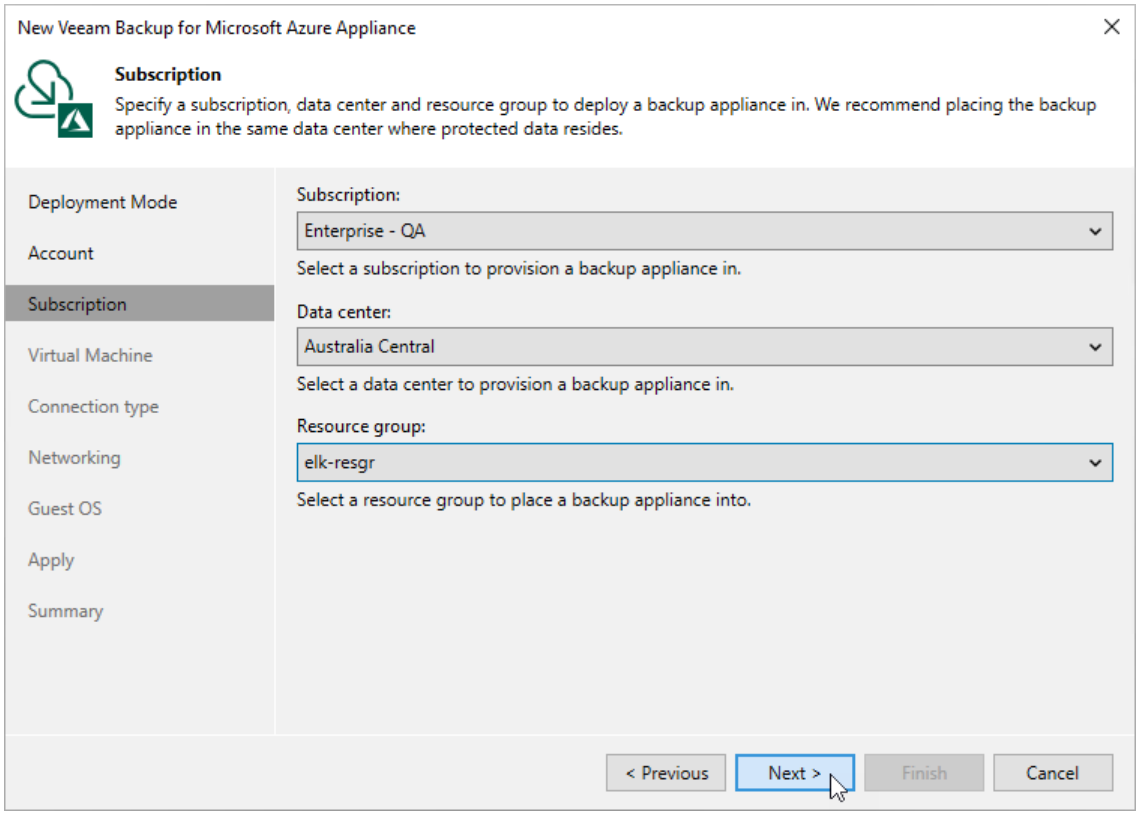
2. From the **Data center** drop-down list, select an Azure region in which the backup appliance will reside.

   For more information on Azure regions, see Microsoft Docs.

3. Choose a resource group that will hold resources related to the appliance.

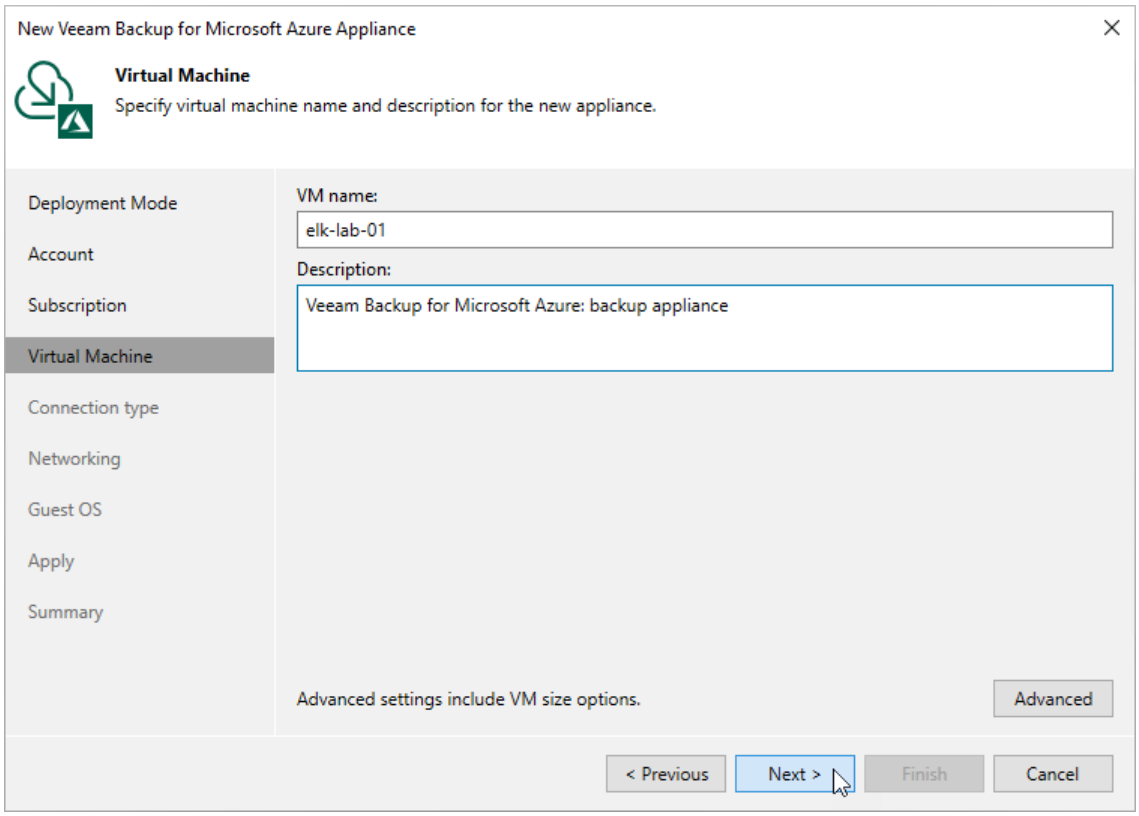
   You can create a new resource group or specify an existing one:

   - To create a new resource group, select the **(create new)** option from the **Resource group** drop-down list. Veeam Backup & Replication will automatically create the *veeam-<VMname>-rg<GUID>* resource group.
   - To specify an existing resource group, select it from the **Resource group** drop-down list. For a resource group to be displayed in the list of available resource groups, it must be created in Microsoft Azure as described in Microsoft Docs.



# Step 5. Specify VM Instance Name and Description

At the **Virtual Machine** step of the wizard, specify a name and description for the Azure VM on which Veeam Backup for Microsoft Azure will be deployed. Note that the name must meet the Microsoft Azure resource name rules.



# Step 6. Specify Connection Type

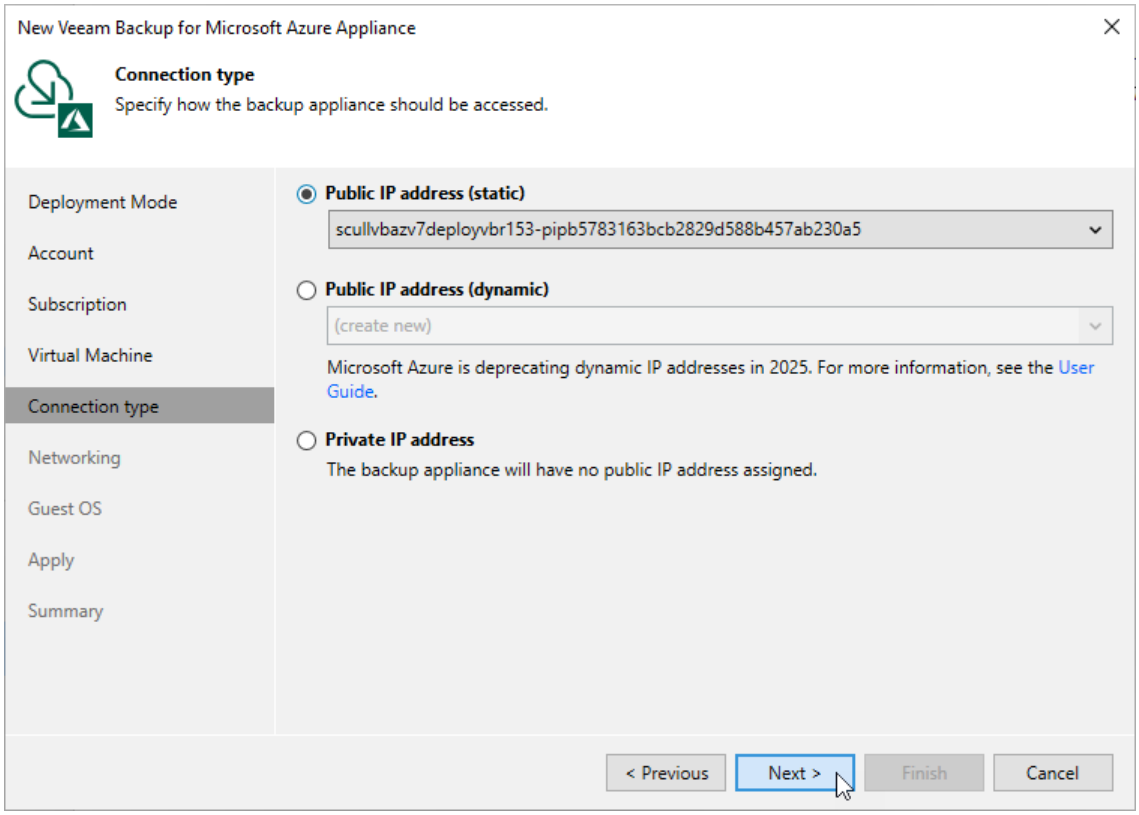
At the **Connection Type** step of the wizard, choose whether you want to assign a dynamic or a static public IP address, or a private IP address to the backup appliance. After the backup appliance is deployed, Veeam Backup & Replication will use the specified connection type to connect to the appliance.

To assign a dynamic or static IP address, you can either reserve a new address or specify an existing one:

- To reserve a new IP address, select the **(create new)** option from the drop-down list.
- To assign an existing IP address, select it from the drop-down list. For an IP address to be displayed in the list of available IP addresses, it must be reserved in Microsoft Azure as described in Microsoft Docs.

> **NOTE**
>
> On September 30, 2025, dynamic (Basic SKU) public IP addresses will be retired in Microsoft Azure. That is why it is recommended that you select a static IP address. For more information, see Microsoft Docs.

If you choose the **Private IP address** option, you must allow communication between the Veeam Backup & Replication server and the backup appliance. If your backup appliance resides in the same virtual network as the Veeam Backup & Replication server, the communication will be established using private IP addresses. If the backup appliance and the Veeam Backup & Replication server reside in different virtual networks, one possible solution is to establish a Site-to-Site VPN connection between the virtual network of the appliance and your on-premises network. To allow your backup appliance to perform all backup and restore operations in the private environments, you will need to perform additional configuration actions as described in section Working in Private Environments.



# Step 7. Specify Network Settings

At the **Networking** step of the wizard, do the following:

1. Choose a virtual network to which the backup appliance will be connected.

   You can create a new network or specify an existing one:

   - [Applies only if you have chosen to assign a public IP address to the backup appliance at the **Connection Type** step of the wizard] To create a new virtual network, select the **(create new)** option from the **Virtual network** drop-down list. Veeam Backup & Replication automatically create a network with a set of predefined security rules.
   - To specify an existing virtual network, select it from the **Virtual network** drop-down list. For a virtual network to be displayed in the list of available networks, it must be created in Microsoft Azure for the region specified at step 4 of the wizard as described in Microsoft Docs.

2. Choose a subnet to which the backup appliance will be connected.

   You can create a new subnet or specify an existing one:

   - [Applies only if you have selected the **create new** option from the **Virtual network** drop-down list] To create a new subnet, select the **(create new)** option from the **Subnet** drop-down list.
     Veeam Backup & Replication will automatically create a subnet in the specified virtual network.
   - To specify an existing subnet, select it from the **Subnet** drop-down list. For a subnet to be displayed in the list of available subnets, it must be created in the specified virtual network as described in Microsoft Docs.

3. Choose a network security group that will be associated with the backup appliance.

   You can create a new security group or specify an existing one:

   - To create a new security group, select the **(create new)** option from the **Network security group** drop-down list. Veeam Backup & Replication will automatically create a group.
   - To specify an existing security group, select it from the **Network security group** drop-down list. For a security group to be displayed in the list of available groups, it must be created in Microsoft Azure as described in Microsoft Docs.

> **IMPORTANT**
>
> If you select an existing security group, consider that security rules added to the group must allow inbound internet access from both the backup server and a local machine that you plan to use to work with Veeam Backup for Microsoft Azure. To learn how to create security rules, see Microsoft Docs.

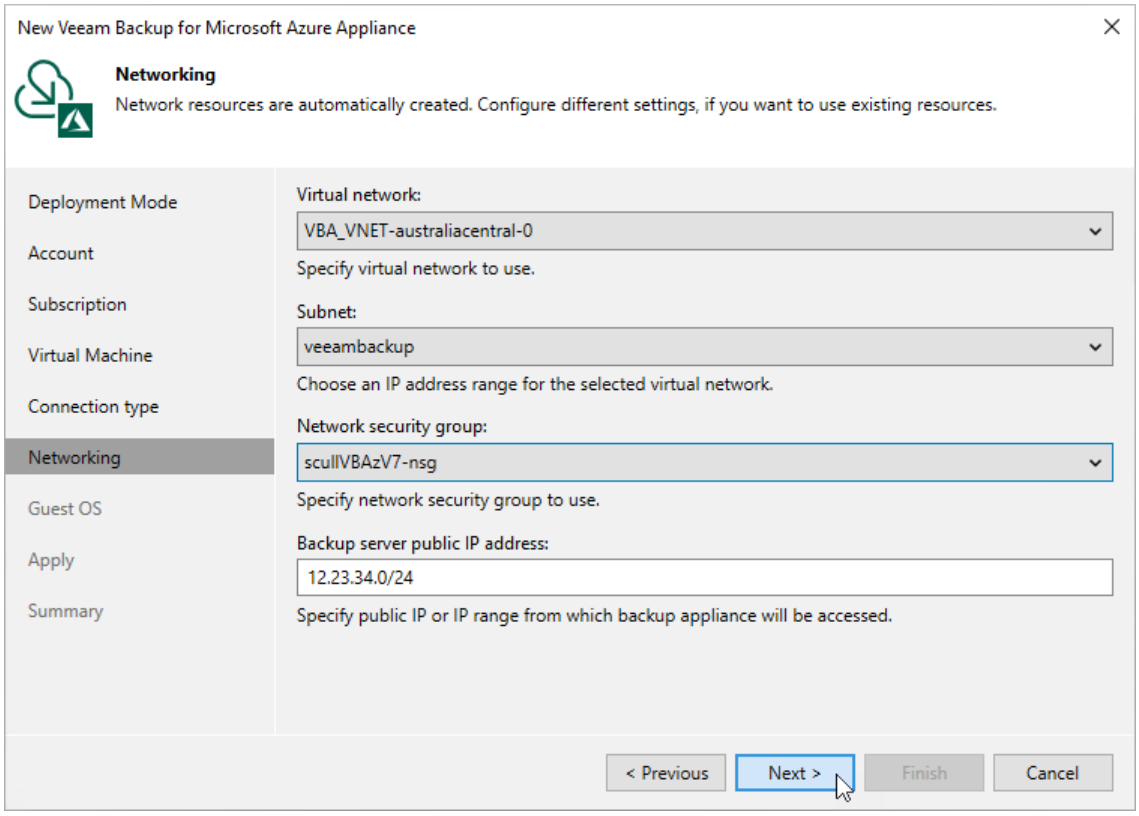
4. [Applies only if you have chosen to assign a public IP address to the backup appliance at the **Connection Type** step of the wizard] In the **Backup server public IP address** field, specify an IP address or a range of IP addresses that will be allowed to access the backup appliance.

   - If you have chosen to create a new security group, Veeam Backup & Replication will create a security rule for the specified specified IP address ranges. Note that the backup server IP address must fall into the specified IP address range.
   - If you have chosen to specify an existing security group, Veeam Backup & Replication will verify whether the security group allows inbound HTTPS traffic (port **443**) from the specified IP addresses. If the security group restricts inbound HTTPS traffic, you will not be able to proceed with the wizard.

5. [Applies only if you have chosen to assign a private IP address to the backup appliance at the **Connection Type** step of the wizard] In the **Backup server IP address** field, specify an IP address or a range of IP addresses that will be allowed to access the backup appliance. Note that the backup server IP address must fall into the specified IP address range.

   Veeam Backup & Replication will verify whether the specified security group allows inbound HTTPS traffic (port **443**) from the specified IP addresses. If the security group restricts inbound HTTPS traffic, you will not be able to proceed with the wizard.

> **TIP**
>
> The IPv4 address ranges must be specified in the CIDR notation (for example, `12.23.34.0/24`). To specify multiple IP addresses or multiple IP address ranges, use a comma-separated list.



# Step 8. Specify User Credentials

At the **Guest OS** step of the wizard, do the following:

1. From the **Create the following administrator credentials** drop-down list, select a user whose credentials will be used by Veeam Backup & Replication to create the Default Admin account on the backup appliance.

   For a user to be displayed in the **Create the following administrator credentials** drop-down list, it must be added to the Credentials Manager as described in the Veeam Backup & Replication User Guide, section Standard Accounts. If you have not added the necessary user to the Credentials Manager beforehand, you can do it without closing the **New Veeam Backup for Microsoft Azure Appliance** wizard. To do that, click either the **Manage accounts** link or the **Add** button, and specify the user name, password and description in the **Credentials** window.

> **NOTE**
>
> When you specify user credentials, Veeam Backup & Replication automatically verifies the provided password. If the password does not meet the Microsoft security requirements, or if the password is present in any of the Ubuntu 22.04 LTS cracklib dictionaries, you will get an error message notifying you that the password cannot be verified.

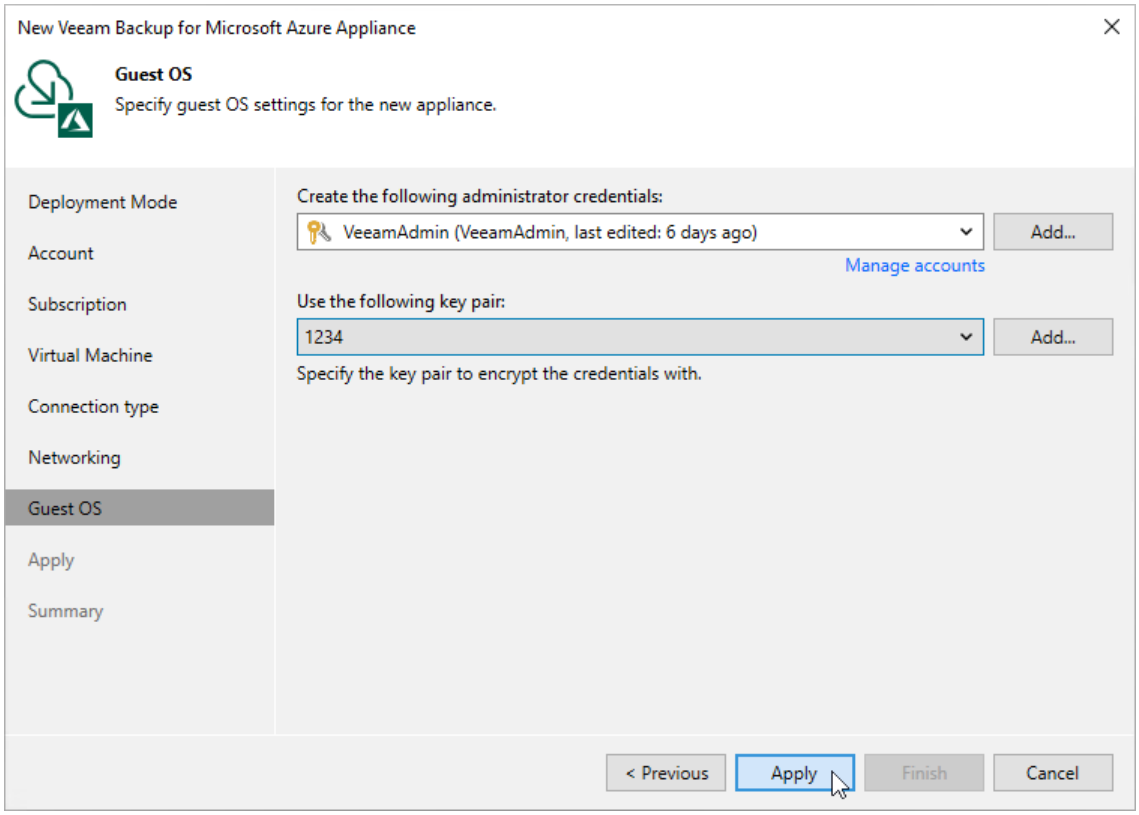
2. In the **Use the following key pair** field, select a key pair that will be used to authenticate against the backup appliance.

   For a key pair to be displayed in the list of available key pairs, it must be created in Microsoft Azure as described in Microsoft Docs. If you have not created the necessary key pair beforehand, you can do it without closing the **New Veeam Backup for Microsoft Azure** wizard. To do that, click **Add** and specify the key pair name and folder path to the pair in the **New Key Pair** window.

**NOTE**

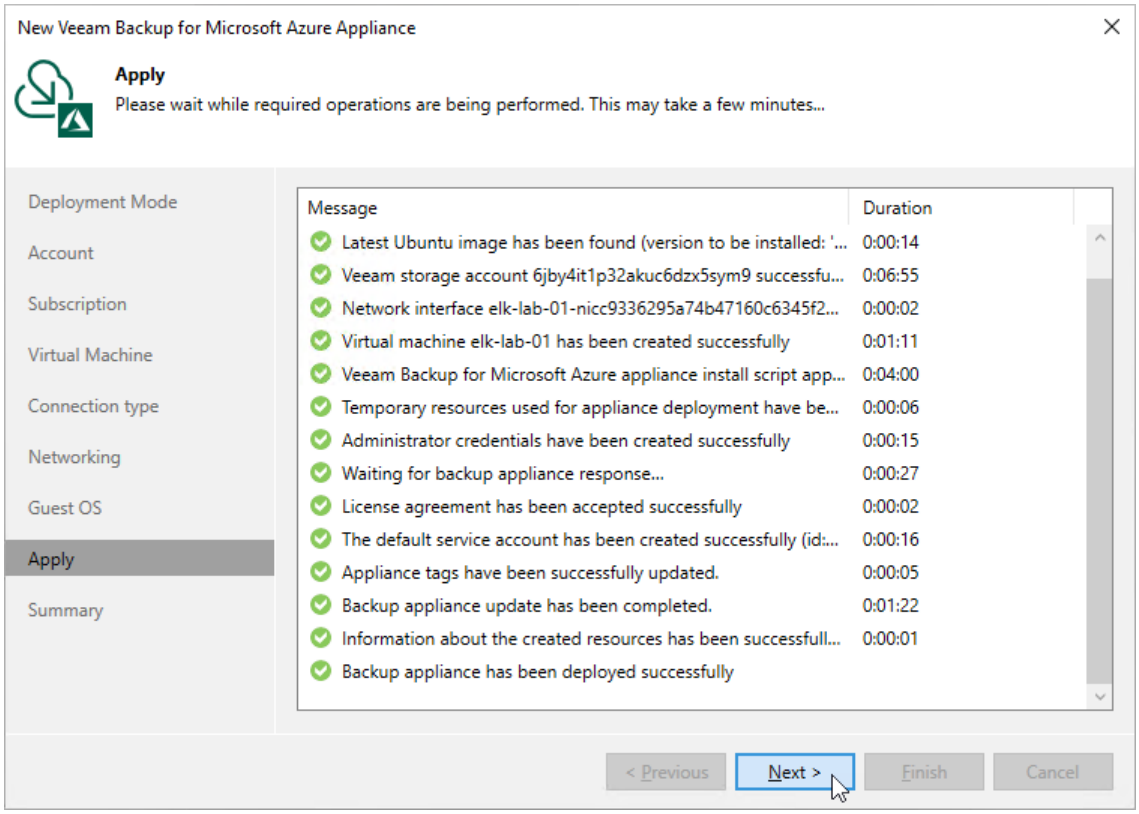
Consider the following:

- If you choose to create a new key pair, the key pair will be stored in the resource group specified at step 4 of the wizard. However, if you have selected the (create new) option when specifying the resource group, Veeam Backup & Replication will store the created key pair in the VeeamSSHKeys resource group.
- If you change the password of the Default Admin account on the backup appliance, you must also change this user password in the Veeam Backup & Replication console as described in the Veeam Backup & Replication User Guide, section Editing and Deleting Credentials Records. Otherwise, the connection will not be established.



# Step 9. Track Progress

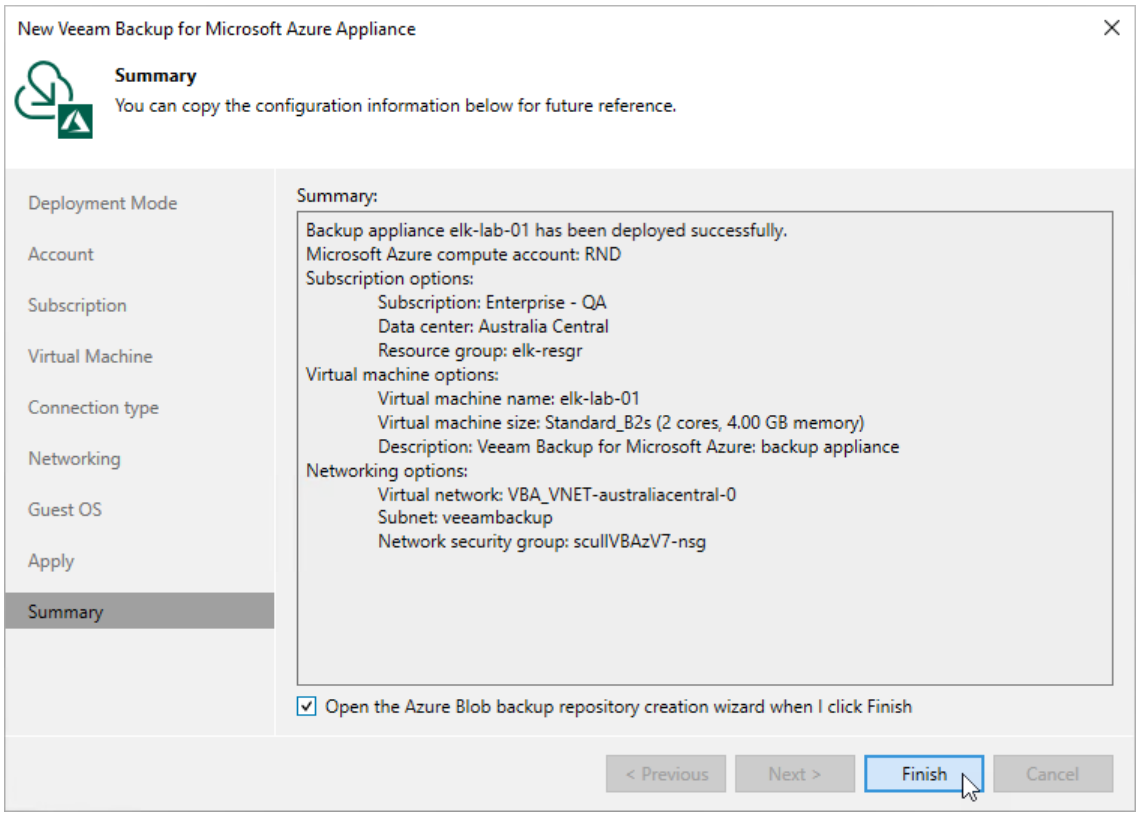
Veeam Backup & Replication will display the results of every step performed while deploying the backup appliance. At the **Apply** step of the wizard, wait for the process to complete and click **Next**.



# Step 10. Finish Working with Wizard

At the **Summary** step of the wizard, review summary information and click **Finish**. After the backup appliance is deployed, you will be able to configure its settings in the Veeam Backup for Microsoft Azure Web UI as described in section Configuring Veeam Backup for Microsoft Azure.

> **TIP**
>
> If you want to configure repositories immediately after the backup appliance is deployed, select the **Open the Azure Blob backup repository creation wizard when I click Finish** check box and follow the instructions provided in section Adding Repositories.



# Licensing

Veeam Backup for Microsoft Azure is licensed per protected instance. An instance is defined as a single Azure resource — an Azure VM, Azure SQL Server, Cosmos DB account or Azure file share. An instance is considered to be protected if it has a restore point (snapshot or backup) created by a backup policy during the past 31 days. Each protected instance consumes 1 license unit. However, if an instance has only manually created snapshots or backups, it does not consume any license units.

> **NOTE**
>
> Protected Azure SQL databases do not consume separate license units. If there is a number of protected databases located on a licensed Azure SQL Server, all these databases consume the license unit of this server.

Veeam Backup for Microsoft Azure is available in 2 editions:

- **Free** — allows you to protect up to 10 instances free of charge. This edition applies only to backup appliances that are no longer managed by Veeam Backup & Replication servers.

  Note that this edition does not support indexing of Azure Files, creating backups of Azure Virtual Network configuration components and protecting Cosmos DB accounts.

- **Paid** — allows you to protect the number of instances equivalent to the number of units specified in your license. This edition is licensed using the Veeam Universal License (VUL) installed on the Veeam Backup & Replication server. For more information on Veeam licensing terms and conditions, see Veeam Licensing Policy.

  When the license expires, Veeam Backup for Microsoft Azure offers a grace period to ensure a smooth license update and to provide sufficient time to install a new license file. The duration of the grace period is 31 days after the expiration of the license. During this period, you can perform all types of data protection and disaster recovery operations. After the grace period is over, Veeam Backup for Microsoft Azure stops processing all instances and disables all scheduled backup policies. You must update your license before the end of the grace period.

> **IMPORTANT**
>
> If you plan to use the Veeam Universal License (VUL), consider that only the *Subscription* license type is supported.

If a backup appliance is managed by a Veeam Backup & Replication server, it uses the same license that is installed on this server. For more information, see Scenarios.

# Limitations

Keep in mind the following limitations and considerations:

- If you use the *Veeam Cloud Connect service provider* license, the Microsoft Azure Plug-in for Veeam Backup & Replication functionality is available from Veeam Service Provider Console only. For more information, see the Veeam Service Provider Console Guide for Service Providers.
- If you use a *Perpetual* per-socket license installed on the backup server, and you want to connect a backup appliance to the backup infrastructure, you must install an additional *Perpetual* per-instance license or a subscription license. When you install an additional license, the new license is automatically merged with the existing *Perpetual* per-socket license. For more information on the merging process, see the Veeam Backup & Replication User Guide, section Merging Licenses.

  If you do not install an additional *Perpetual* per-instance license or a subscription license, you will be able to use one free license instance per each socket (maximum 6 free instances per instance). After you exceed the limit of free instances, Veeam Backup for Microsoft Azure backup policies protecting resources that are not covered by the license will fail.

  To obtain an additional license, contact a Veeam sales representative at Sales Inquiry.
- If an instance has not been backed up within the past 31 days, Veeam Backup for Microsoft Azure automatically revokes the license unit from the instance. If you need to manually revoke a license unit, follow the instructions provided in section Revoking License Units.

# Scenarios

Backup appliances managed by a Veeam Backup & Replication server use the same license that is installed on the backup server. To learn what types of licenses and licensing models are incorporated in Veeam solutions, see:

- The Veeam Backup & Replication User Guide, section Licensing
- The Veeam Backup & Replication Veeam Cloud Connect Guide, section Licensing for Service Providers

## Licensing of New Backup Appliances

When you deploy a new backup appliance from the Veeam Backup & Replication console, workloads start consuming license units from the license installed on the backup server after you create and run backup policies. After you remove the appliance from the backup infrastructure, Veeam Backup & Replication stops counting backed-up workloads and Veeam Backup for Microsoft Azure switches to the *Free* edition that allows you to protect up to 10 workloads free of charge.

> **NOTE**
>
> When you connect to an existing backup appliance, the license installed on the appliance is replaced with the license installed on the backup server. However, protected instances start consuming license units from the license installed on the backup server only after the backup policy sessions run on the connected appliance. After you remove the appliance from the backup infrastructure, Veeam Backup & Replication stops counting backed-up workloads. Veeam Backup for Microsoft Azure continues using the license that was used before you added the appliance to the backup infrastructure.

## Licensing When Connection to Veeam Backup & Replication is Lost

Veeam Backup for Microsoft Azure stores information on protected workloads licensed by Veeam Backup & Replication. This information allows you to back up workloads even if the connection between the backup appliance and backup server is lost. However, the following conditions must be met:

- The workload must have already been licensed by the backup server.
- The workload must be listed as licensed on the backup appliance side. For more information, see Revoking License Units.
- The connection must be lost not more than 31 days ago.

Note that the loss of connection with Veeam Backup & Replication does not affect restore processes and creating of snapshots manually.

# Viewing License Information

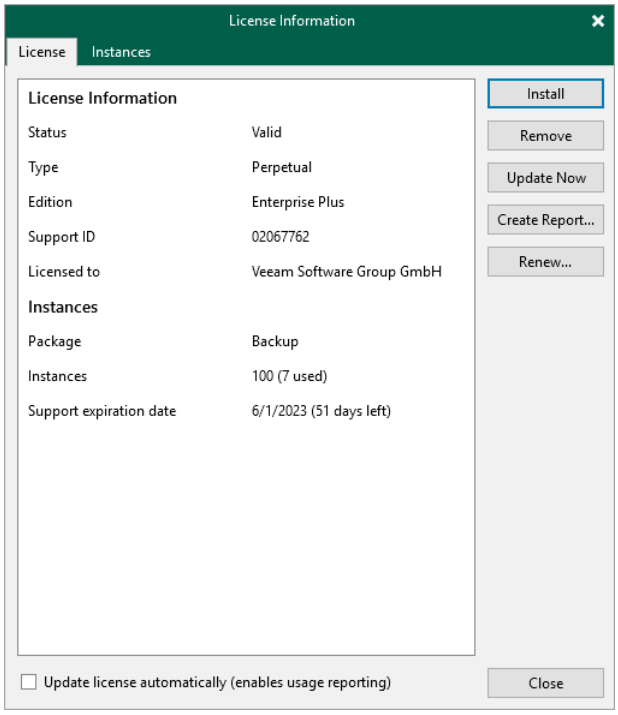
After you add a backup appliance to the backup infrastructure, you can view the number of protected workloads in the Veeam Backup & Replication console.

## Viewing License Details Using Veeam Backup & Replication Console

To view Microsoft Azure Plug-in for Veeam Backup & Replication license details in the Veeam Backup & Replication console, open the main menu and select **License**.

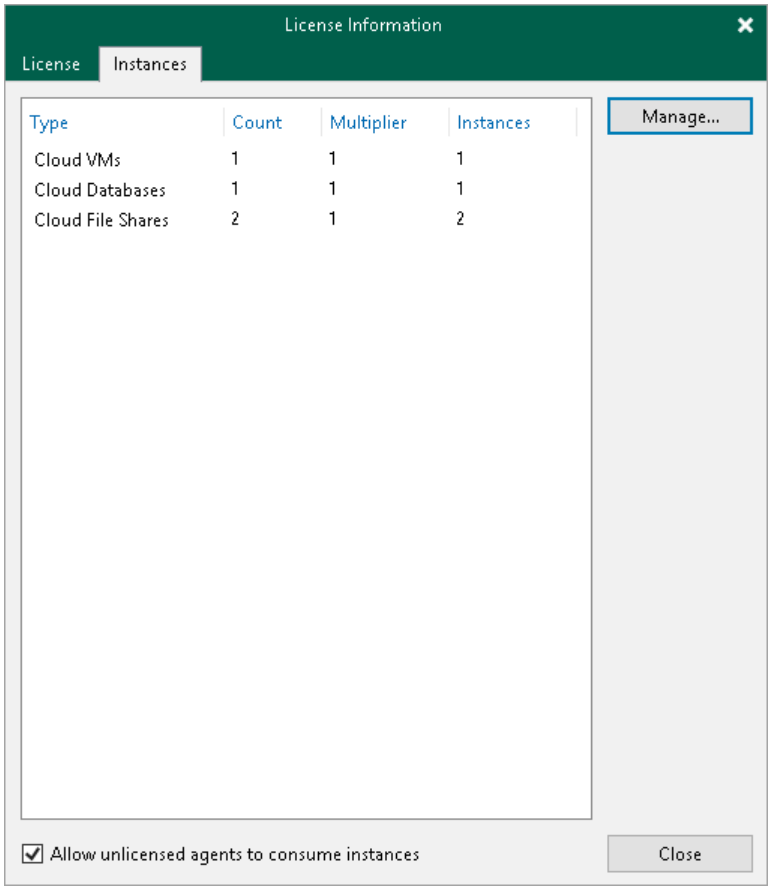
The **License** tab of the **License Information** window provides general information on the currently installed Microsoft Azure Plug-in for Veeam Backup & Replication license:

- **Status** – the license status. The status will depend on the license type, the number of days remaining until license expiration, the number of days remaining in the grace period (if any), and the number of workloads that exceeded the allowed increase limit (if any).
- **Type** – the license type (*Perpetual*, *Subscription*, *Rental*, *Evaluation*, *NFR*, *Free*).
- **Edition** – the license edition (*Community*, *Standard*, *Enterprise*, *Enterprise Plus*).
- **Support ID** – the ID of the contract (required for contacting Veeam Customer Support).
- **Licensed to** – the name of an organization to which the license was issued.
- **Package** – the software product for which the license was issued.
- **Instances** – the total number of license units included in the license file and the number of units consumed by protected workloads.
- **Support expiration date** – the date when the license will expire.



The **Instances** tab of the **License Information** window provides information on the currently protected workloads:

- **Type** – the type of protected workloads.
  - **Cloud VMs** – protected Azure VMs.
  - **Cloud File Shares** – protect Azure files shares.
  - **Cloud Databases** – protected Azure SQL Servers and Cosmos DB accounts.
- **Count** – the number of protected workloads.
- **Multiplier** – the number of license units one protected workload consumes.
- **Instances** – the total number of the consumed license units.




# Viewing License Details Using Veeam Backup for Microsoft Azure Web UI

To view details on the license that is currently installed on the backup appliance, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **Licensing** > **License Info**.

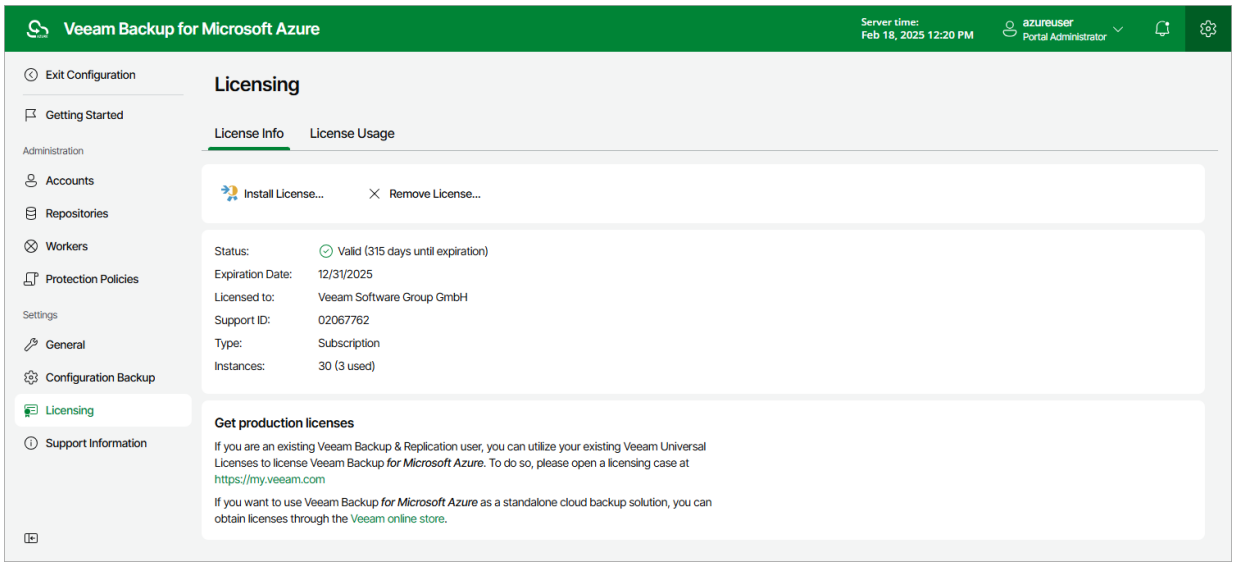
The **License Info** tab provides general information on the Veeam Backup for Microsoft Azure license:

- **Status** – the license status. The status depends on the license edition, the number of days remaining until license expiration and the number of days remaining in the grace period (if any).

- **Type** – the license edition (*Free*, *Managed*).
- **Instances** – the total number of license units included in the license file and the number of units consumed by protected resources.

  Each instance that has a restore point created in the past 31 days is considered to be protected and consumes one license unit. To view the list of instances that consume license units, switch to the **License Usage** tab.

> **IMPORTANT**
>
> Starting from Veeam Backup for Microsoft Azure version 8, installing licenses is not supported for backup appliances that are not managed by any Veeam Backup & Replication servers. As a workaround, install Microsoft Azure Plug-in for Veeam Backup & Replication on a backup server and add the appliance to the backup infrastructure.



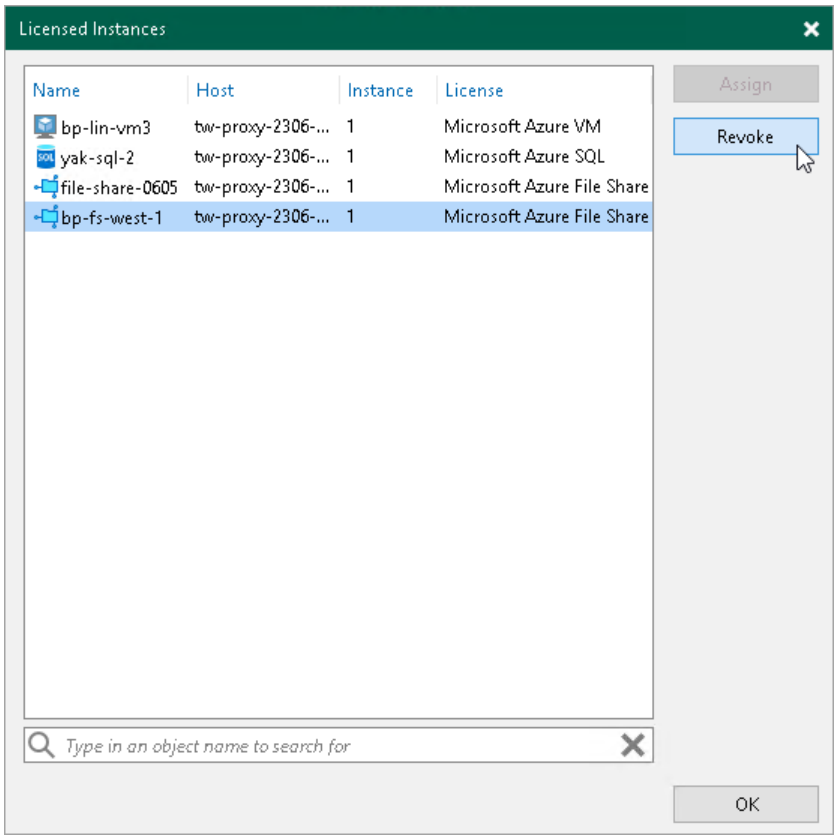
# Revoking License Units

By default, Veeam Backup for Microsoft Azure automatically revokes a license unit from a protected instance if no new restore points have been created by the backup policy during the past 31 days. However, you can manually revoke license units from protected instances — this can be helpful, for example, if you remove a number of instances from a backup policy and do not want to protect them anymore.

## Revoking License Units Using Veeam Backup & Replication Console

You can revoke license units from a protected instance in the Veeam Backup & Replication console, do the following:

1. In the Veeam Backup & Replication console, open the main menu and select **License**.
2. In the **License Information** window, switch to the **Instances** tab and click **Manage**.
3. In the **Licensed Instances** window, select a protected workload and click **Revoke**. Veeam Backup & Replication will revoke a license unit from the selected workload.

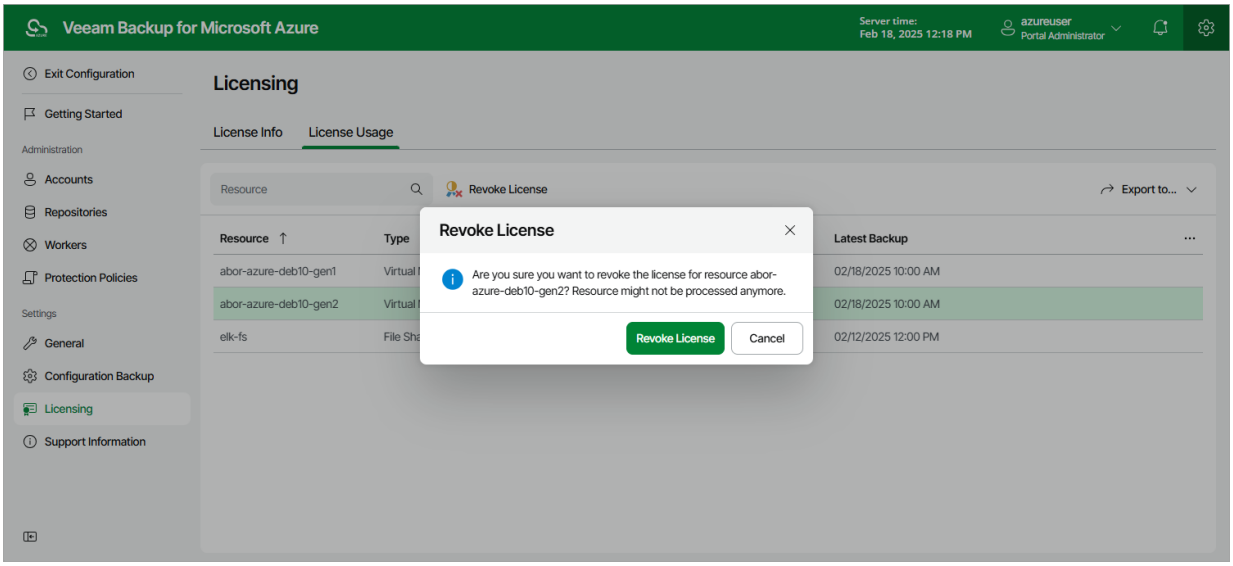



## Revoking License Units Using Veeam Backup for Microsoft Azure Web UI

To revoke a license unit from a protected instance in the Veeam Backup for Microsoft Azure Web UI, do the following:

1. Switch to the **Configuration** page.

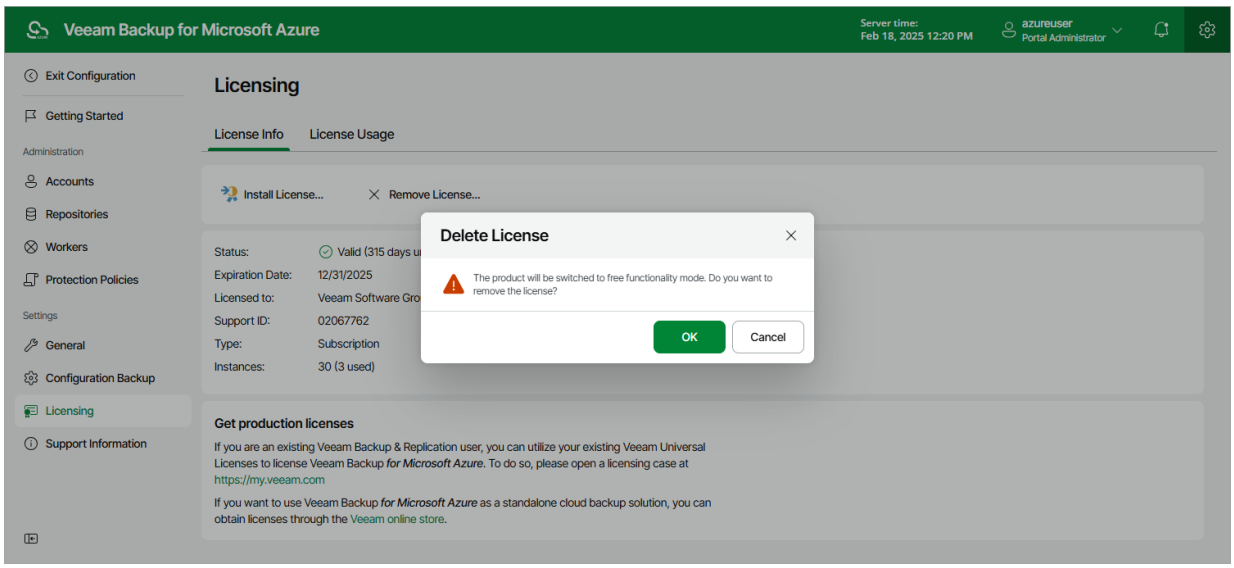
2. Navigate to **Licensing** > **License Usage**.
3. Select the instance that you no longer want to protect.
4. Click **Revoke License**.



# Removing License

To remove the license installed on a backup appliance that was previously deployed from the Microsoft Azure Marketplace:

1. Switch to the **Configuration** page.
2. Navigate to **Licensing** > **License Info**.
3. Click **Remove License**.
4. In the **Remove License** window, click **Yes** to confirm that you want to remove the license.




After you remove a license, Veeam Backup for Microsoft Azure will automatically switch back to the *Free* edition. In this case, according to the FIFO (first-in first-out) queue, only the first 10 instances registered in the configuration database will remain protected. You can revoke license units from these instances as described in section Revoking License Units.

# Accessing Veeam Backup for Microsoft Azure

After you install Veeam Backup for Microsoft Azure and add backup appliances to the backup infrastructure, you will be able to back up and restore Azure resources using both the Veeam Backup & Replication console and the Veeam Backup for Microsoft Azure Web UI.

## Accessing Veeam Backup & Replication Console

The Veeam Backup & Replication console is a client-side component of the backup infrastructure that provides access to the backup server. The console allows you to log in to Veeam Backup & Replication and to perform data protection and disaster recovery operations on the server. To learn how to access the Veeam Backup & Replication console, see the Veeam Backup & Replication User Guide, section Logging in to Veeam Backup & Replication.

By default, the Veeam Backup & Replication console is installed on the backup server automatically when you install Veeam Backup & Replication. However, in addition to the default console, you can install the Veeam Backup & Replication console on a dedicated machine to access the backup server remotely. To learn how to install Veeam Backup & Replication console, see the Veeam Backup & Replication User Guide, section Installing Veeam Backup & Replication Console.

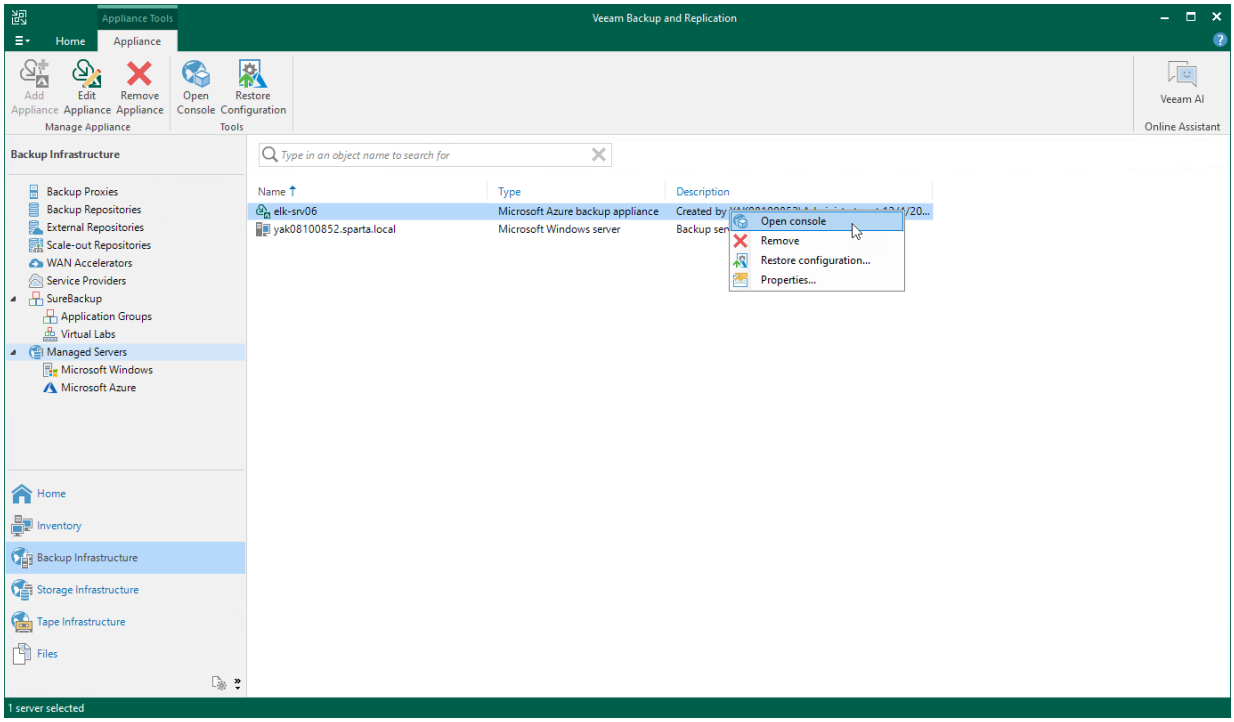
# Accessing Web UI from Console

To access the Veeam Backup for Microsoft Azure Web UI from the Veeam Backup & Replication console, do the following:

1. Open the **Backup Infrastructure** view.
2. Navigate to **Managed Servers**.
3. Select the backup appliance whose Web UI you want to open, and click **Open Console** on the ribbon.

   Alternatively, you can right-click the appliance and select **Open console**.

Veeam Backup & Replication will open the Veeam Backup for Microsoft Azure Web UI in your default web browser.



# Accessing Web UI from Workstation

To access Veeam Backup for Microsoft Azure Web UI from a workstation, navigate to the Veeam Backup for Microsoft Azure web address in a web browser. The address consists of a public IPv4 address or DNS hostname of the backup appliance. Note that the website is available over HTTPS only.

> **IMPORTANT**
>
> Consider the following:
>
> - If you backup appliance is deployed without a public IP address, you must enable the private network deployment functionality for the appliance. For more information, see Working in Private Environments.
> - Internet Explorer is not supported. To access the Veeam Backup for Microsoft Azure Web UI, use Microsoft Edge (latest version), Mozilla Firefox (latest version) or Google Chrome (latest version).

You can access Veeam Backup for Microsoft Azure using a local user account or a user account of an external identity provider. To learn how to add user accounts to Veeam Backup for Microsoft Azure, see Adding User Accounts.

> **NOTE**
>
> The web browser may display a warning notifying that the connection is untrusted. To eliminate the warning, you can replace the TLS certificate that is currently used to secure traffic between the browser and the backup appliance with a trusted TLS certificate. To learn how to replace certificates, see Replacing Security Certificates.

## Logging In Using Local User Account

To log in using credentials of a Veeam Backup for Microsoft Azure user account, do the following:

1. In the **Username** and **Password** fields, specify credentials of an authorized user account.

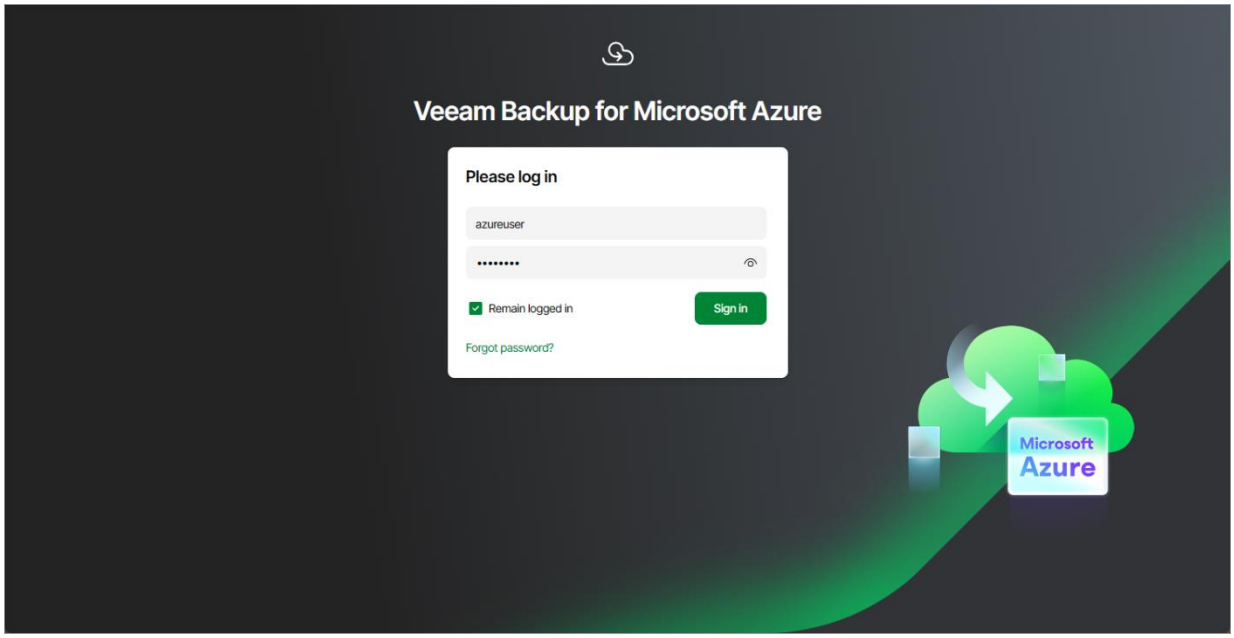
   If you log in for the first time, use credentials of the Administrator account that was created after the product installation. In future, you can add other user accounts to grant access to Veeam Backup for Microsoft Azure. For more information, see Managing User Accounts.

> **TIP**
>
> If you do not remember the password, you can reset it. To do that, click the **Forgot password?** link and follow the instructions provided in the **Password Reset** window.

2. Select the **Remain logged in** check box to stay logged in for 24 hours. Otherwise, you will remain logged in for 1 hour.

3. Click **Log in**.

   If multi-factor authentication (MFA) is enabled for the user, Veeam Backup for Microsoft Azure will prompt you to enter a code to verify the user identity. In the **Verification code** field, enter the temporary six-digit code generated by the authentication application running on your trusted device. Then, click **Log in**.



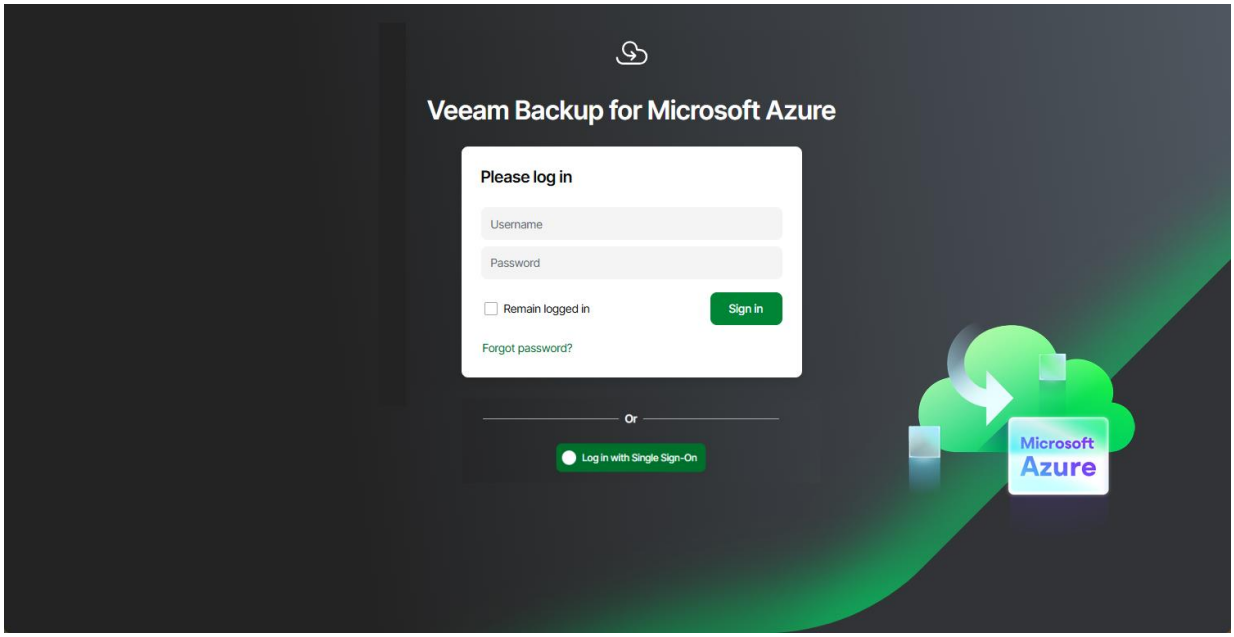

# Logging In Using Identity Provider User Account

> **IMPORTANT**
>
> To access Veeam Backup for Microsoft Azure under a user account of your identity provider, you must first configure single sign-on settings and then add the identity provider user account to Veeam Backup for Microsoft Azure.

To log in using an identity provider, do the following:

1. Click **Log in with Single Sign-On**. You will be redirected to your identity provider portal.

2. If you have not logged in yet, log in to the identity provider portal. You will be redirected to the **Veeam Backup for Microsoft Azure Overview** page as an authorized user.




# Logging Out

To log out, at the top right corner of the Veeam Backup for Microsoft Azure window, click the user name and then click **Log Out**.

# Configuring Veeam Backup for Microsoft Azure

To start working with Veeam Backup for Microsoft Azure, perform a number of steps for its configuration:

1. Add backup appliances to the backup infrastructure.
2. Add repositories that will be used to store backed-up data.

   This step applies if you plan to protect Azure VMs, Azure SQL databases, Cosmos DB for PostgreSQL accounts or Cosmos DB for MongoDB accounts with backups, or to save additional copies of virtual network configuration backups to a backup repository.
3. Configure the added backup appliances:
   a. Add service accounts to get access to Azure services and resources.
   b. [Optional] Add user accounts to control access to Veeam Backup for Microsoft Azure.
   c. [Optional] Configure worker instance settings.

      If you do not configure settings for worker instances, Veeam Backup for Microsoft Azure will use the default settings of Azure regions where worker instances will be launched.
   d. Configure policy templates that will be used by SLA-based backup policies.
   e. [Optional] Configure deployment, global retention, email notification and single sign-on settings.

> **NOTE**
>
> Even after you add accounts that manage your Azure resources and configure all the necessary settings, Veeam Backup for Microsoft Azure will populate neither the list of Azure VMs nor the list of Azure SQL databases nor the list of Cosmos DB accounts nor the list of Azure file shares on the Resources page — unless you create backup policies and specify regions where the Azure resources belong, as described in section Performing Backup.

# Managing Backup Appliances

Microsoft Azure Plug-in for Veeam Backup & Replication allows you to add backup appliances to the backup infrastructure, and to view and manage all the added appliances from the Veeam Backup & Replication console.

# Adding Appliances

After you install Microsoft Azure Plug-in for Veeam Backup & Replication, you must add backup appliances to the backup infrastructure. To do that, use either of the following options:

- Deploy new backup appliances from the Veeam Backup & Replication console.
- Connect to existing backup appliances if you have already deployed them as described in section Deploying Backup Appliance.

> **NOTE**
>
> One backup appliance can be managed by one backup server only. If you add the appliance to the backup infrastructure of another backup server, the synchronization between the appliance and the previous backup server will be terminated, and appliance will be displayed as unavailable.

## Connecting to Existing Appliances

If you have already deployed a backup appliance, you can add the appliance to the backup infrastructure:

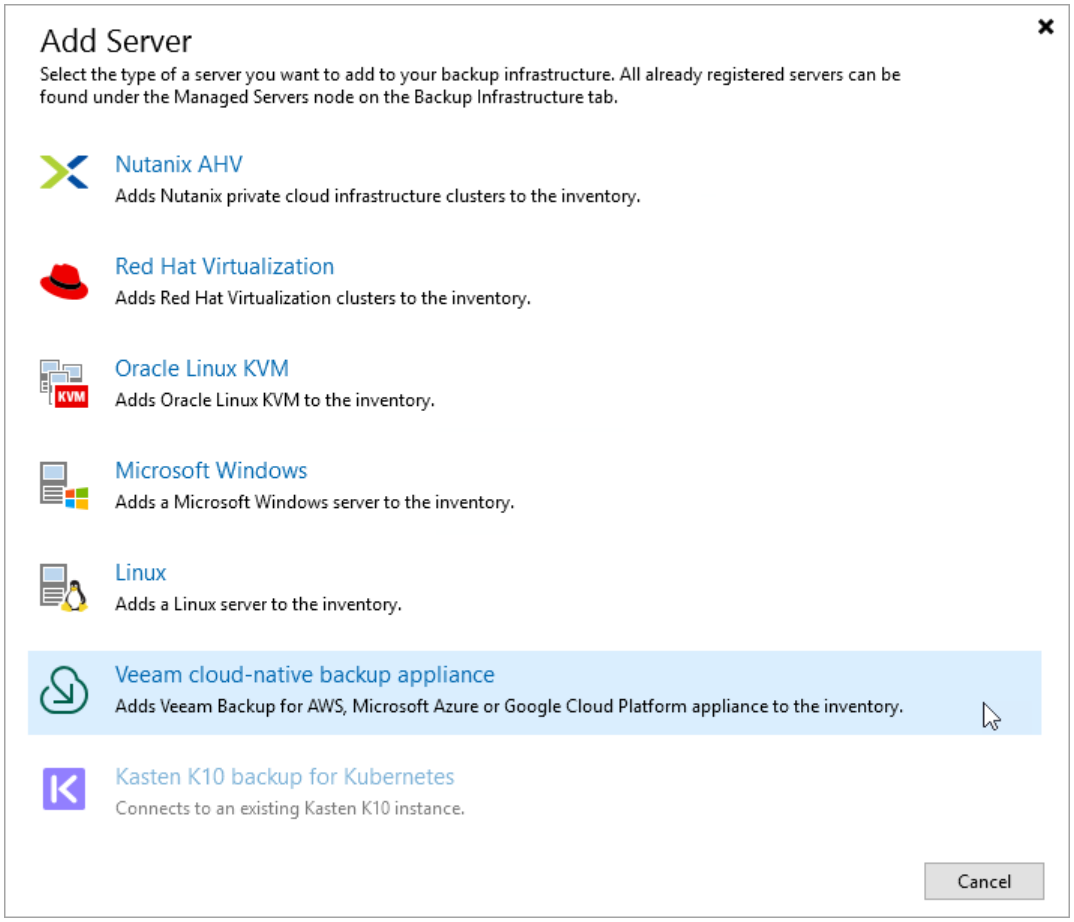
1. Launch the New backup appliance wizard.
2. Specify a deployment mode.
3. Specify service account settings.
4. Specify an Azure subscription.
5. Choose the appliance that you want to connect to.
6. Specify the connection type.
7. Specify a user whose credentials will be used to connect to the appliance.
8. Configure repository settings.
9. Wait for the appliance to be added to the backup infrastructure.
10. Finish working with the wizard.

## Step 1. Launch New Veeam Backup for Microsoft Azure Appliance Wizard

To launch the **New Veeam Backup for Microsoft Azure Appliance** wizard, do the following:

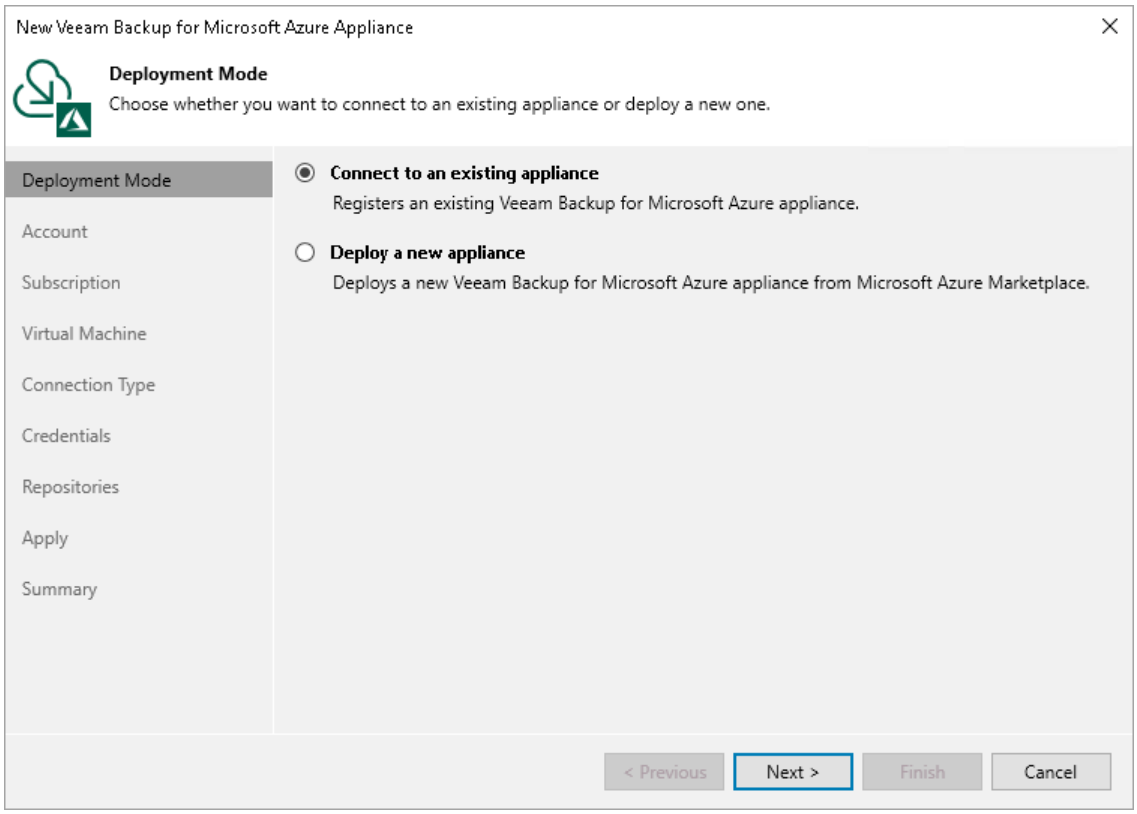
1. In the Veeam Backup & Replication console, open the **Backup Infrastructure** view.
2. Navigate to **Managed Servers** and click **Add Server** on the ribbon.

   Alternatively, you can right-click the **Managed Servers** node and select **Add Server**.
3. In the **Add Server** window:
   a. [Applies only if you have several cloud plug-ins installed] Click **Veeam cloud-native backup appliance**.
   b. Choose **Veeam Backup for Microsoft Azure**.



## Step 2. Choose Deployment Mode

At the **Deployment Mode** step of the wizard, select the **Connect to an existing appliance** option.



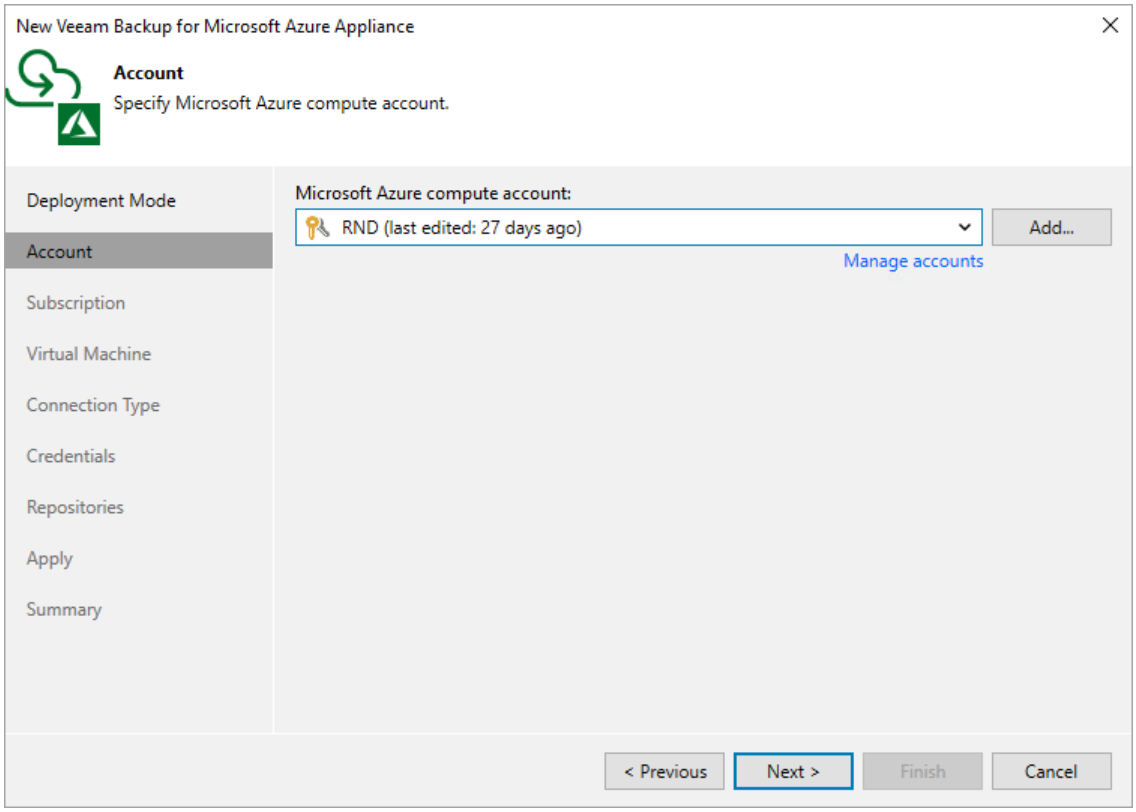
# Step 3. Specify Microsoft Azure Compute Account Settings

At the **Account** step of the wizard, select a Microsoft Azure compute account whose permissions will be used to connect the backup appliance.

For a Microsoft Azure compute account to be displayed in the **Microsoft Azure compute account** drop-down list, it must be added to the Cloud Credentials Manager as described in the Veeam Backup & Replication User Guide, section Microsoft Azure Compute Accounts. If you have not added the necessary credentials to the Cloud Credentials Manager beforehand, you can do it without closing the **New Veeam Backup for Microsoft Azure Appliance** wizard. To do that, click either the **Manage accounts** link or the **Add** button, and complete the **Microsoft Azure Compute Account** wizard.

For each newly created account, Veeam Backup & Replication creates a new Microsoft Entra application in your Microsoft Entra ID. The application is automatically assigned the *Key Vault Crypto User*, *Owner* and *Storage Queue Data Contributor* Azure built-in roles. Note that the *Owner* role has a wide scope of permissions and capabilities. If you want the application to be assigned a limited list of permissions, create an application manually in Microsoft Azure. For more information on the required permissions that must be assigned to the Microsoft Entra application, see Plug-In Permissions.

> **IMPORTANT**
>
> Microsoft Azure Stack Hub accounts are not supported.



# Step 4. Specify Subscription and Region

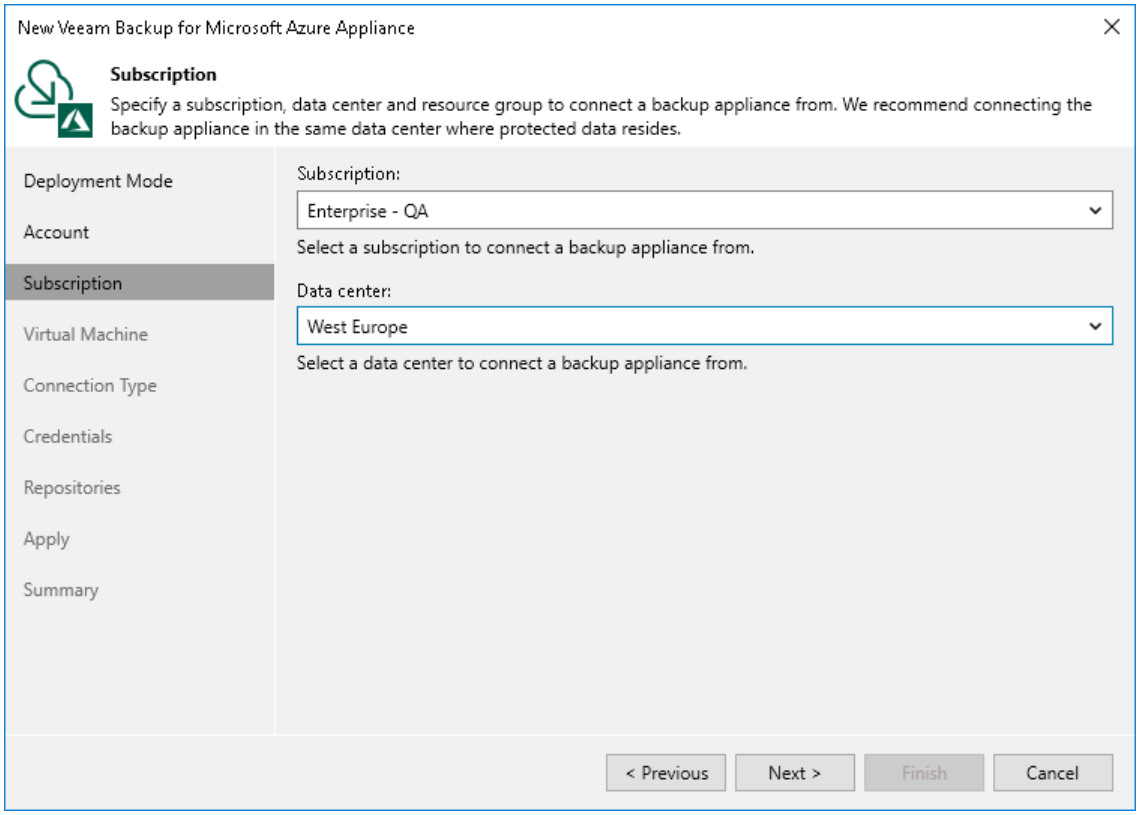
At the **Subscription** step of the wizard, do the following:

1. From the **Subscription** drop-down list, select an Azure subscription that is used to manage costs of the backup appliance.

   For a subscription to be displayed in the list of available subscriptions, it must be created in Microsoft Azure and associated with the Microsoft Entra tenant to which the Microsoft Azure compute account specified at step 3 of the wizard belongs.

2. From the **Data center** drop-down list, select the Azure region in which the backup appliance resides.

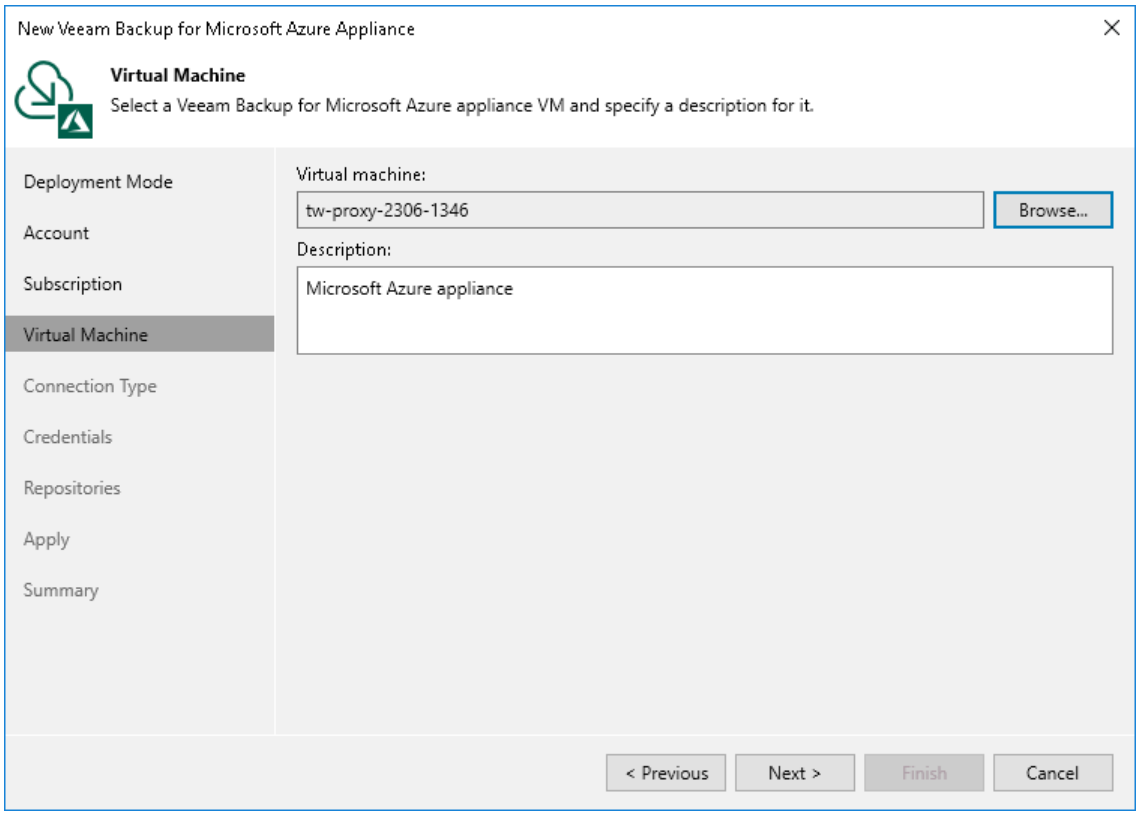
   For more information on regions and zones, see Microsoft Docs.



## Step 5. Select Appliance

At the **Virtual Machine** step of the wizard, choose the backup appliance that you want to add to the backup infrastructure:

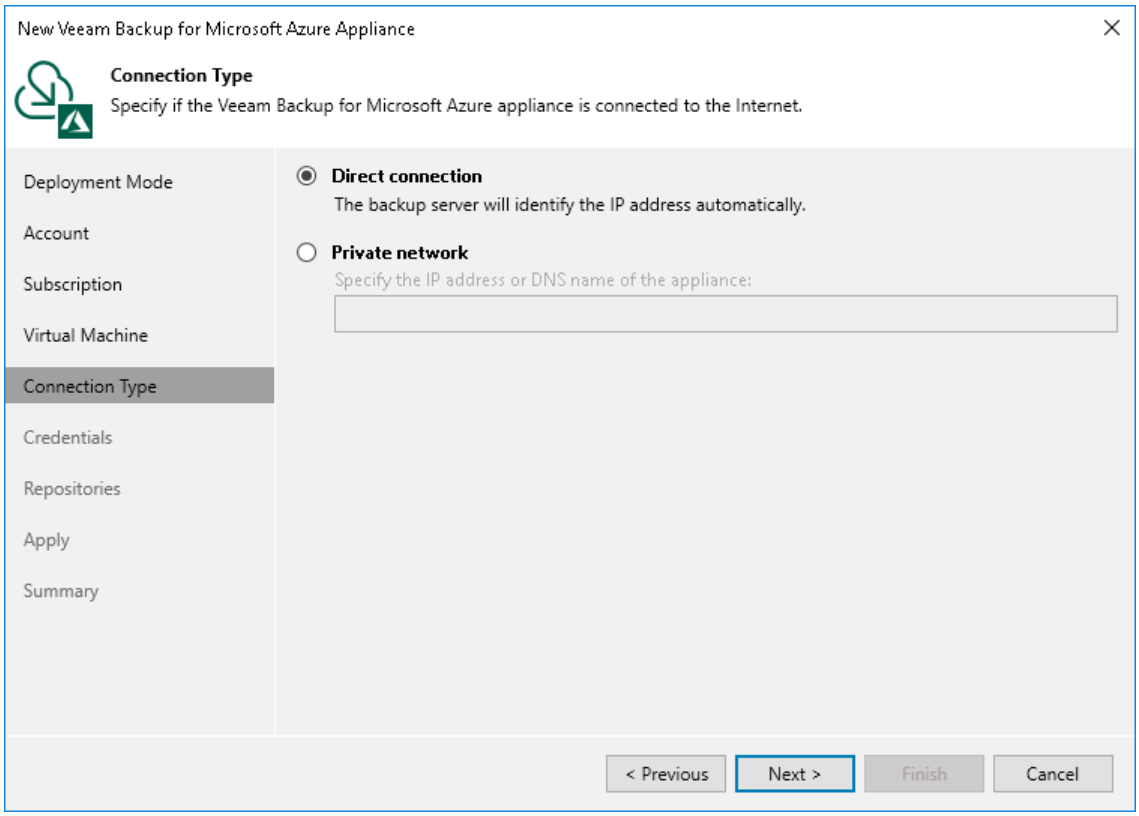
1. Click **Browse**.
2. In the **Select Virtual Machine** window, select the necessary appliance and click **OK**.
3. In the **Description** field, specify a description for future reference.



# Step 6. Specify Connection Type

At the **Connection Type** step of the wizard, specify the way Veeam Backup & Replication will connect to the backup appliance:

- Select the **Direct connection** option if the backup appliance is connected to a virtual network with inbound internet access allowed and you want the backup server to connect to this appliance over the internet. In this case, Veeam Backup & Replication will detect the public IP address of the appliance automatically.
- Select the **Private network** option if the backup appliance and the backup server are connected to the same private virtual network, or you want the backup server to connect to the appliance over VPN. In this case, you must specify the private IP address or the DNS hostname of the appliance in the **Specify the IP address or DNS name of the appliance** field.



## Step 7. Specify User Credentials

At the **Credentials** step of the wizard, specify a user whose credentials Veeam Backup & Replication will use to connect to the backup appliance.

For a user to be displayed in the **Credentials** list, it must be added to the Credentials Manager as described in the Veeam Backup & Replication User Guide, section Standard Accounts. If you have not added the necessary user to the Credentials Manager beforehand, you can do it without closing the **New Veeam Backup for Microsoft Azure Appliance** wizard. To do that, click either the **Manage accounts** link or the **Add** button, and specify the user name, password and description in the **Credentials** window.

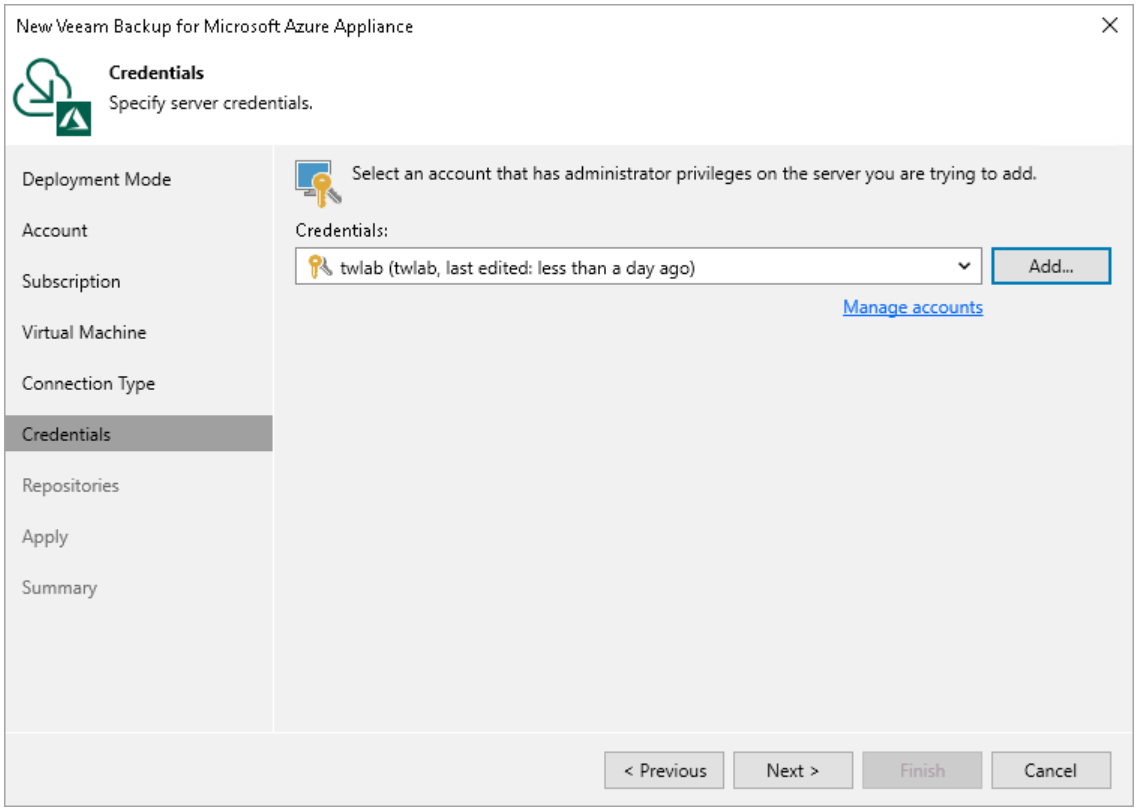
> **IMPORTANT**
>
> The specified user must have multi-factor authentication (MFA) disabled and the Portal Administrator role assigned.

If you try to add to the backup infrastructure an appliance that runs a version of Veeam Backup for Microsoft Azure that is not compatible with the version of Veeam Backup & Replication, Veeam Backup & Replication will display a warning notifying that the appliance must be upgraded. To eliminate the warning, click **Yes**. Veeam Backup & Replication will automatically upgrade the appliance to the necessary version. Note that the Microsoft Azure compute account specified at step 3 of the wizard must have permissions required to upgrade the appliance. For more information, see Plug-In Permissions.

When you add a backup appliance to the backup infrastructure, Veeam Backup & Replication automatically verifies the TLS certificate installed on the appliance:

- If the certificate is trusted, Veeam Backup & Replication saves a thumbprint of the certificate in the configuration database. When Veeam Backup & Replication connects to the appliance, it uses the saved thumbprint to verify the appliance identity and to avoid the man-in-the-middle attack.
- If the certificate is not trusted, Veeam Backup & Replication does not save a thumbprint of the certificate in the configuration database. When Veeam Backup & Replication connects to the appliance, the appliance is shown in the Veeam Backup & Replication console as unavailable.

> **IMPORTANT**
>
> - Do not change the role of a Veeam Backup for Microsoft Azure user whose credentials are used by Veeam Backup & Replication to connect to the backup appliance.
> - If you change the password of a Veeam Backup for Microsoft Azure user whose credentials are used by Veeam Backup & Replication to connect to the backup appliance, you must also change this user password in the Veeam Backup & Replication console as described in the Veeam Backup & Replication User Guide, section Editing and Deleting Credentials Records. Otherwise, the connection will not be established.


New Veeam Backup for Microsoft Azure Appliance
Credentials
Specify server credentials.
Deployment Mode
Account
Subscription
Virtual Machine
Connection Type
Credentials
Repositories
Apply
Summary
Select an account that has administrator privileges on the server you are trying to add.
Credentials:
twlab (twlab, last edited: less than a day ago)
Add...
Manage accounts
< Previous
Next >
Finish
Cancel

## Step 8. Configure Repository Settings

The **Repositories** step of the wizard, a list of all standard and archive repositories already configured on the selected backup appliance will be displayed. After you complete the wizard, Veeam Backup & Replication will automatically add these repositories to the backup infrastructure.

You can specify the following configuration settings for each repository whose restore points you want to use to recover backed-up data:

> **NOTE**
>
> The following procedure applies only to standard repositories. For archive repositories, there is no possibility to specify any configuration settings.

1. In the **Repositories** list, select the necessary standard repository and click **Edit**.
2. In the **Repository Settings** window:
   a. From the **Credentials** drop-down list, select credentials of a Microsoft Azure storage account where the target blob container resides. Veeam Backup & Replication will use these credentials to access the repository. For more information on supported types of storage accounts, see the Veeam Backup & Replication User Guide, section Cloud Credentials Manager.

      For credentials to be displayed in the list of available credentials, they must be added to the Cloud Credentials Manager as described in the Veeam Backup & Replication User Guide, section Microsoft Azure Storage Accounts (Shared Key). If you have not added the necessary credentials to the Cloud Credentials Manager beforehand, you can do it without closing the **New Veeam Backup for Microsoft Azure Appliance** wizard. To do that, click either the **Manage cloud accounts** link or the **Add** button, and specify the storage account name and access key generated for the account in the **Credentials** window.

> **NOTE**
>
> If you do not specify credentials of the Microsoft Azure storage account for a standard repository, you will only be able to use the Veeam Backup & Replication console to perform entire VM restore, SQL database restore and Cosmos DB restore from backups stored in this repository. Moreover, encrypted backups will be displayed as non-encrypted ones, and information on the repository displayed in the **Backup Infrastructure** view under the **External Repositories** node will not include statistics on the amount of storage space that is currently consumed by restore points created by Veeam Backup for Microsoft Azure.

   b. From the **Use the following gateway server for the Internet access** drop-down list, select a gateway server that will be used to provide access to the repository.

      For a gateway server to be displayed in the **Use the following gateway server for the Internet access** drop-down list, it must be added to the backup infrastructure. For more information on gateway servers, see Gateway Servers.

   c. If encryption is enabled for the repository, the following scenarios may apply:

- If data in the repository is encrypted using a password, select the **Use the following password for encrypted backups** check box. From the drop-down list, select the password that is used to encrypt data. Veeam Backup & Replication will use the specified password to decrypt backup files stored in this repository.

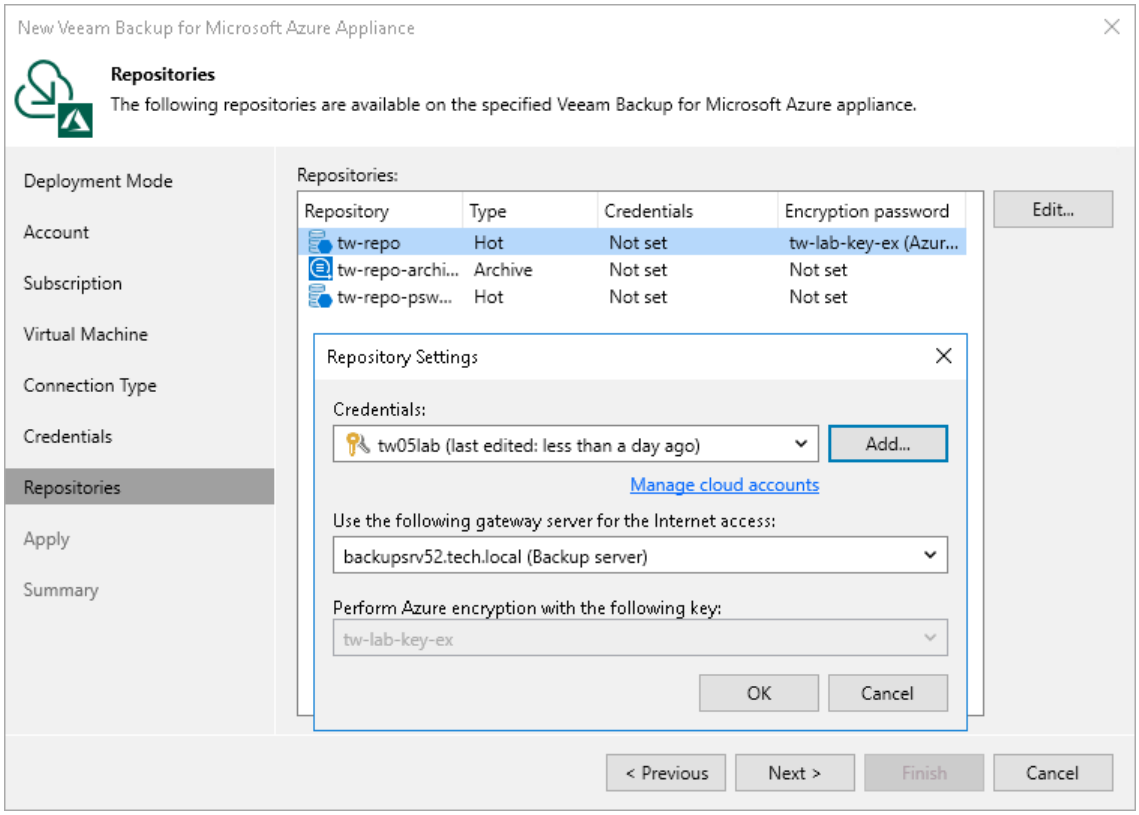
  For a password to be displayed in the **Use the following password for encrypted backups** drop-down list, it must be added to the backup infrastructure as described in the Veeam Backup & Replication User Guide, section Creating Passwords. If you have not added the necessary password beforehand, you can do it without closing the **Repository Settings** window. To do that, click either the **Manage cloud accounts** link or the **Add** button, and specify the password and hint in the **Password** window.

> **NOTE**
>
> If you do not specify a password for a standard repository with encryption enabled, you will have to decrypt data stored in this repository manually as described in section Managing Backed-Up Data Using Console.

- If data in the standard repository is encrypted with an Azure Key Vault cryptographic key, Veeam Backup & Replication will show the used key in the **Perform Azure encryption with the following key** drop-down list, but will not allow you change it.

After you finish working with the wizard, all the added repositories will be displayed in the **Backup Infrastructure** view under the **External Repositories** node.

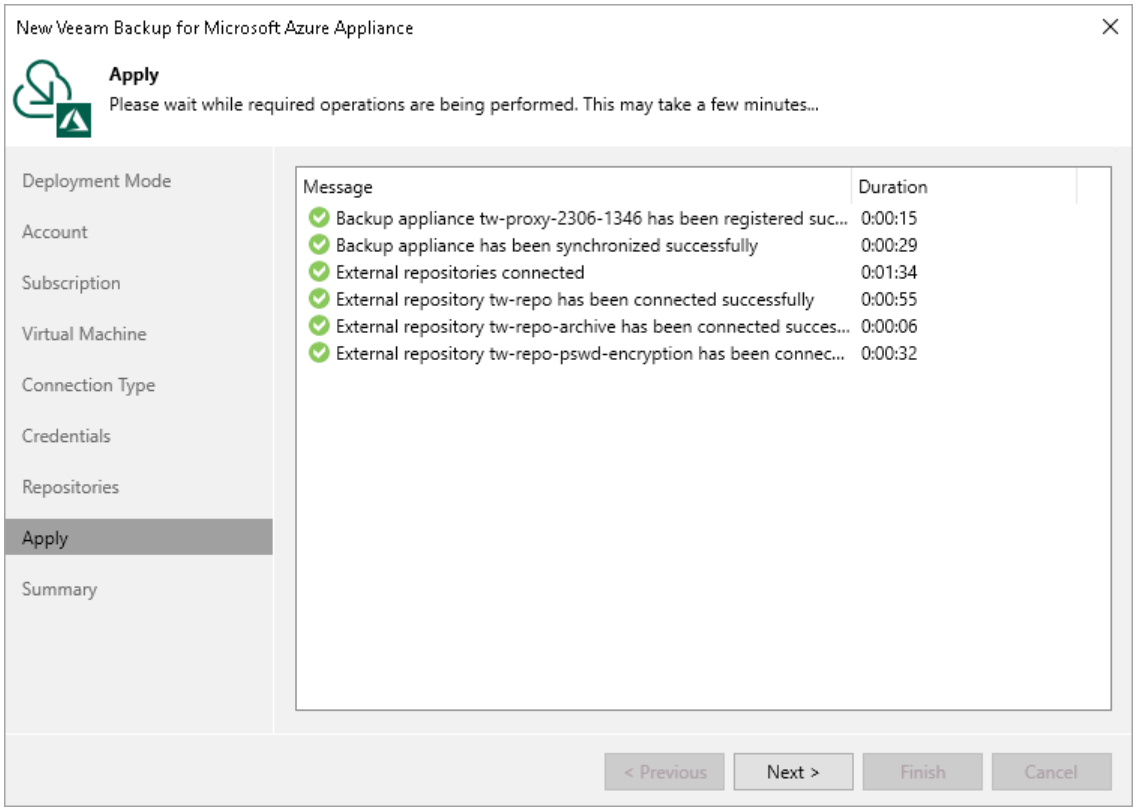
> **NOTE**
>
> If some of the repositories are already added to the backup infrastructure of another backup server, you will be prompted to claim the ownership of these repositories. To learn how to claim the ownership, see the Veeam Backup & Replication User Guide, section Ownership.



## Step 9. Track Progress

Veeam Backup & Replication will display the results of every step performed while connecting the backup appliance. At the **Apply** step of the wizard, wait for the process to complete and click **Next**.

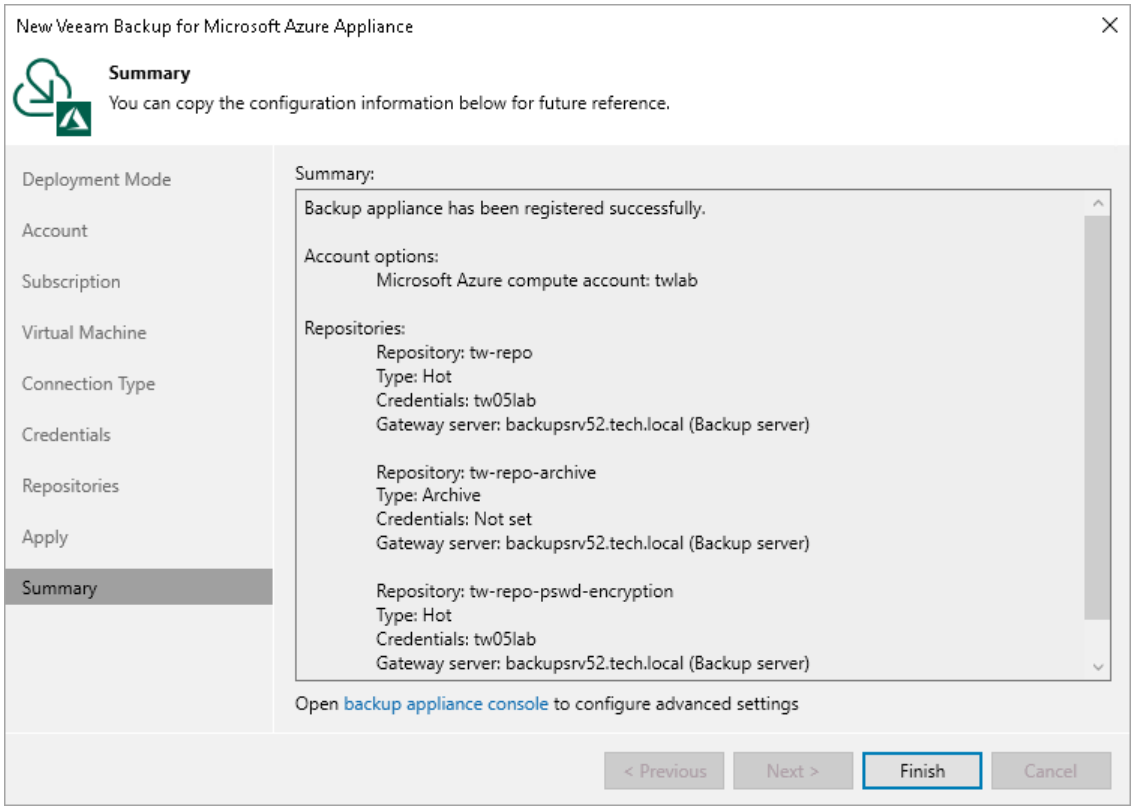
> **NOTE**
>
> When adding an existing appliance to the backup infrastructure, Veeam Backup & Replication collects session results only for the past 24 hours, as well as information on all snapshots, backups and policies.



# Step 10. Finish Working with Wizard

At the **Summary** step of the wizard, review summary information and click **Finish**.

After the backup appliance is added to the infrastructure, you can configure its settings in the Veeam Backup for Microsoft Azure Web UI as described in section Configuring Veeam Backup for Microsoft Azure. If you want Veeam Backup & Replication to open the Web UI of the added appliance immediately, click the **backup appliance console** link.



# Editing Appliance Settings

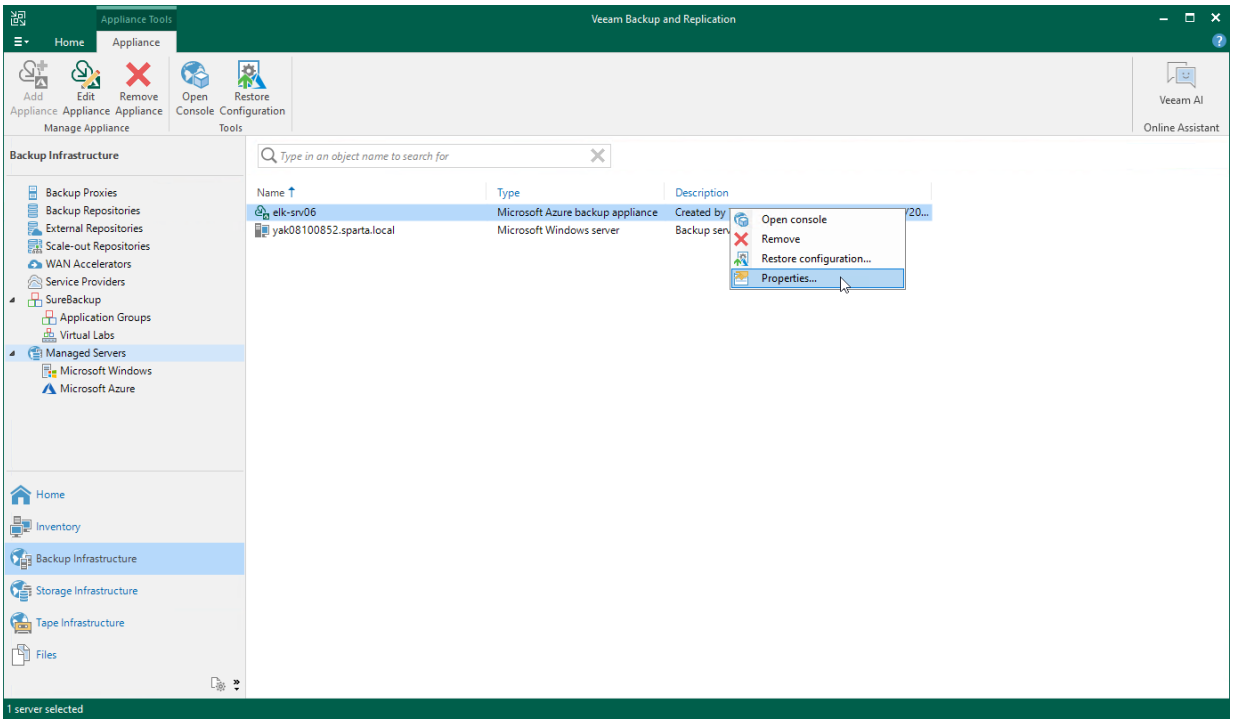
For each backup appliance managed by the backup server, you can modify the settings configured while adding the appliance to the backup infrastructure.

To edit the backup appliance settings, do the following:

1. In the Veeam Backup & Replication console, open the **Backup Infrastructure** view.
2. Navigate to **Managed Servers**.
3. Select the necessary appliance and click **Edit Appliance** on the ribbon.

   Alternatively, right-click the appliance and select **Properties**.
4. Complete the **Edit Veeam Backup for Microsoft Azure Appliance** wizard:
   a. To change the Microsoft Azure compute account that is used to connect to the backup appliance, follow the instructions provided in section Connecting to Existing Appliances (step 3).
   b. To provide a new description for the backup appliance, follow the instructions provided in section Connecting to Existing Appliances (step 5).
   c. To change the way Veeam Backup & Replication connects to the backup appliance, follow the instructions provided in section Connecting to Existing Appliances (step 6).
   d. To change the user whose credentials Veeam Backup & Replication uses to connect to the backup appliance, follow the instructions provided in section Connecting to Existing Appliances (step 7).
   e. To edit settings of the backup appliance repositories added to the backup infrastructure, follow the instructions provided in section Connecting to Existing Appliances (step 8).
   f. At the **Summary** step of the wizard, review summary information and click **Finish**.

> **NOTE**
>
> As soon as you click **Next** at step c, Veeam Backup & Replication will verify the connection to the specified backup appliance. If the appliance is assigned a dynamic IP address, Veeam Backup & Replication will display a warning notifying that dynamic IP addresses will be retired in 2025. To learn how to eliminate this warning, see Eliminating Warnings.



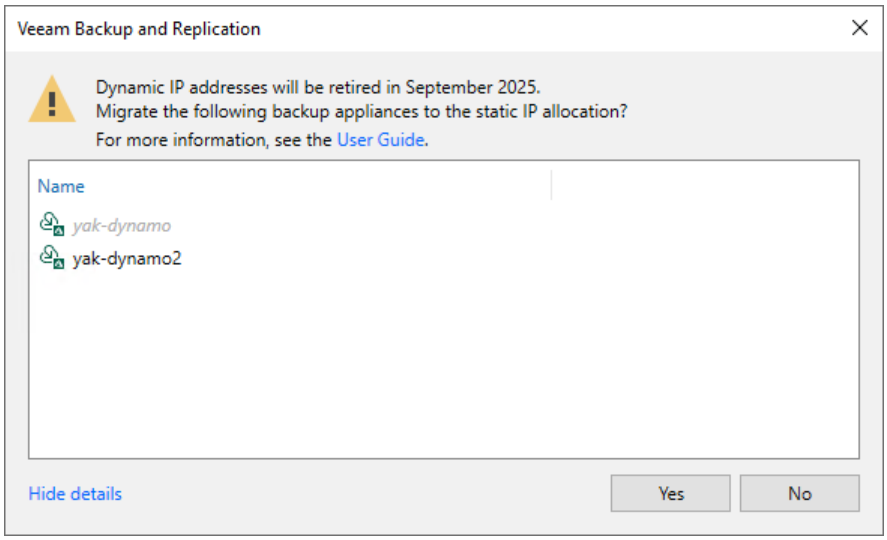

# Eliminating Warnings

On September 30, 2025, dynamic (Basic SKU) public IP addresses will be retired in Microsoft Azure. That is why starting from Veeam Backup for Microsoft Azure version 7.0, Veeam Backup & Replication checks the IP allocation method specified for backup appliances in case the following conditions are met:

- An available update is detected for any of these backup appliances.
- You either log in to the backup server, edit settings of a backup appliance, or upgrade one or multiple backup appliances.

In this case, Veeam Backup & Replication will display a warning notifying that dynamic IP addresses will be retired soon. To eliminate the warning, click **Show details** and choose whether you want to instruct Veeam Backup & Replication to migrate the appliances to static IP addresses automatically. You can also migrate the appliances manually as described in Microsoft Docs.

> **NOTE**
>
> If any of the backup appliances displayed in the notification window are grayed out, it means that these appliances have custom network configurations. In this case, it is recommended that you migrate these appliances manually.


Veeam Backup and Replication
Dynamic IP addresses will be retired in September 2025.
Migrate the following backup appliances to the static IP allocation?
For more information, see the User Guide.
Name
yak-dynamo
yak-dynamo2
Hide details
Yes
No

# Rescanning Appliances

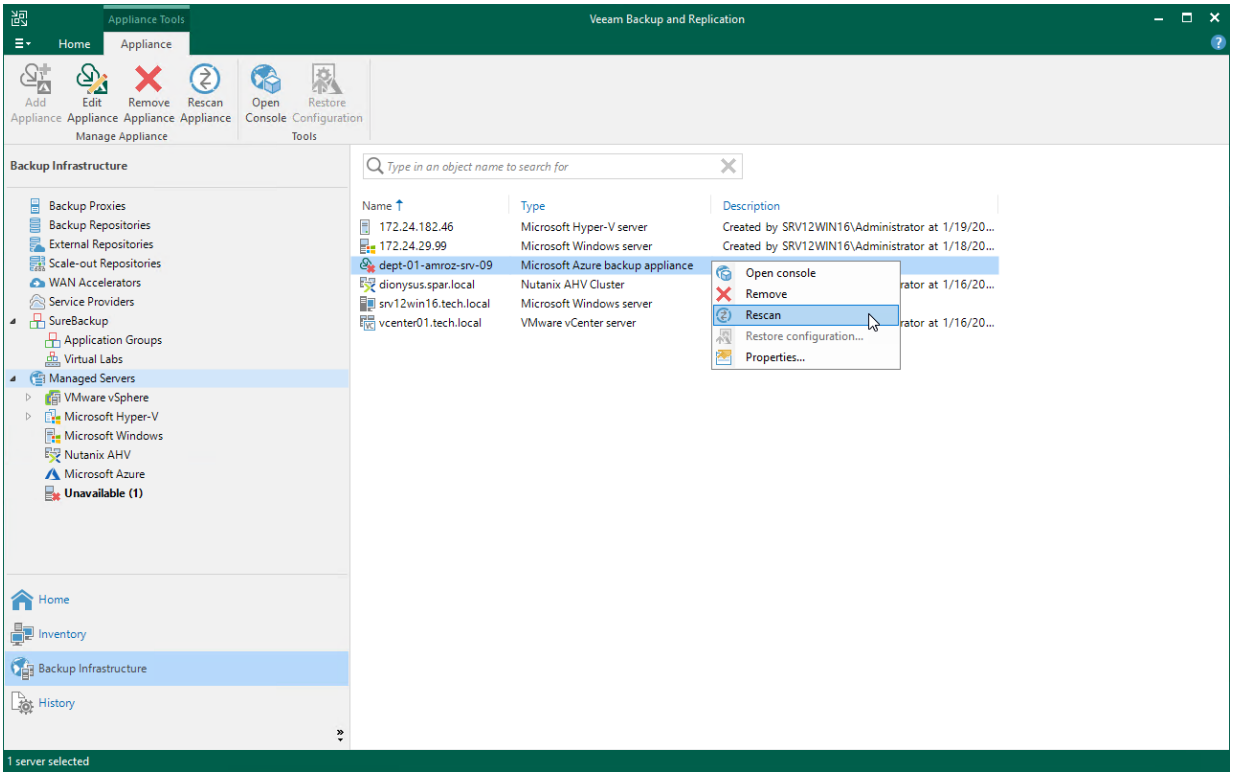
If a backup appliance become unavailable, for example, due to connectivity problems, you can rescan the appliance:

1. In the Veeam Backup & Replication console, open the **Backup Infrastructure** view.
2. Navigate to **Managed Servers**.
3. Select the necessary backup appliance and click **Rescan appliance** on the ribbon.

   Alternatively, you can right-click the appliance and select **Rescan**.
4. In the opened window, click **Yes**.

Veeam Backup & Replication will remove all data collected from the appliance configuration database. Then, Veeam Backup & Replication will recollect session results for the past 24 hours, as well as information on all created snapshots, backups and policies.

> **NOTE**
>
> The rescan operation cannot be performed for available backup appliances and appliances that require upgrade. To learn how to upgrade backup appliances, see Updating Appliances Using Console.



# Removing Appliances

Microsoft Azure Plug-in for Veeam Backup & Replication allows you to permanently remove backup appliances from the backup infrastructure.

> **NOTE**
>
> After you remove a backup appliance, the following limitations will apply:
>
> - Repositories for which you have not specified credentials of a Microsoft Azure storage accounts will be removed automatically from the backup infrastructure.
> - Repositories for which you have specified credentials of a Microsoft Azure storage accounts will remain in the backup infrastructure. However, you will have to rescan the repositories to collect information on all newly created and recently deleted (both manually and by retention) restore points.
> - You will not be able to manage backup policies created on the appliance.
> - You will not be able to restore Azure VMs from snapshots.
> - Restore to Azure from image-level backups will start working as described in the Veeam Backup & Replication User Guide, section How Restore to Microsoft Azure Works.
>
>   Also, the restore process will start taking more time to complete causing data transfer costs to increase as Veeam Backup & Replication will not be able to use native Microsoft Azure capabilities and will have to process more data.

To remove a backup appliance, do the following:

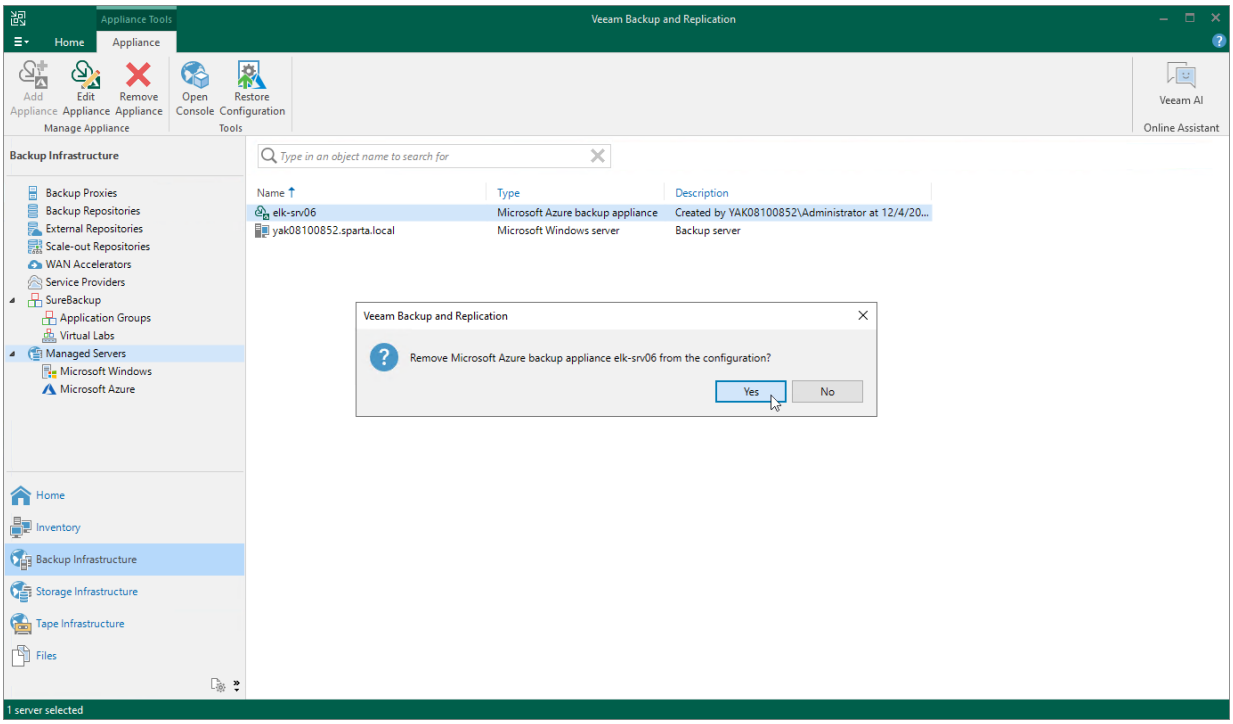
1. In the Veeam Backup & Replication console, open the **Backup Infrastructure** view.
2. Navigate to **Managed Servers**.
3. Select the necessary backup appliance and click **Remove Appliance** on the ribbon.

   Alternatively, right-click the appliance and select **Remove**.
4. In the **Veeam Backup & Replication** window, click **Yes** to acknowledge the operation.

### TIP

If you want to remove an appliance from both the backup infrastructure and Microsoft Azure, select the **Delete cloud resources associated with the backup appliance?** check box in the opened window. Veeam Backup for Microsoft Azure will remove all resources associated with this appliance in Microsoft Azure.

However, if an appliance has been deployed from the Microsoft Azure Marketplace or is running Veeam Backup for Microsoft Azure version 2.x (or earlier), to remove resources from Microsoft Azure, you must follow the instructions provided in section Uninstalling Backup Appliances Deployed from Microsoft Azure Marketplace.




### NOTE

If the selected appliance has been deployed from the Veeam Backup & Replication console and Veeam Backup & Replication uses a newly created key pair to authenticate against the backup appliance, you must remove the key pair from the resource group that holds resources related to the appliance.

# Uninstalling Backup Appliances Deployed from Microsoft Azure Marketplace

Starting from version 7.0, you can deploy Veeam Backup for Microsoft Azure from the Veeam Backup & Replication console only. However, if an appliance was previously deployed from the Microsoft Azure Marketplace or is running Veeam Backup for Microsoft Azure version 2.x (or earlier), perform the following steps to uninstall Veeam Backup for Microsoft Azure:

1. Remove backed-up data.
2. Remove IAM roles and Microsoft Entra applications used by Veeam Backup for Microsoft Azure to access Azure resources.
3. Remove Microsoft Azure resources created by Veeam Backup for Microsoft Azure.

> **IMPORTANT**
>
> Before you uninstall the solution, remove all worker instances and created worker configurations as described in section Managing Worker Instances.

## Removing Backed-Up Data

When you remove the backup appliance and all resources associated with it, backups and snapshots created by this backup appliance are not removed from your Microsoft Azure account automatically. You can later import the created Azure VM image-level backups, Azure SQL backups, Cosmos DB for PostgreSQL backups, Cosmos DB for MongoDB backups to a repository and backup copies of virtual network configurations to a new backup appliance as described in section Adding Backup Repositories.

If you do not want to keep the backed-up data, remove it manually as described in section Managing Backed-Up Data before you uninstall the solution. Alternatively, you can remove the data using the Microsoft Azure portal.

> **NOTE**
>
> Consider that snapshots of Azure file shares and Azure VMs with unmanaged disks created by the Veeam backup service have no specific tags assigned. The snapshots cannot be distinguished from other snapshots of Azure file shares and Azure VMs with unmanaged disks created in Microsoft Azure. That is why we recommend to delete these snapshots from the Veeam Backup for Microsoft Azure Web UI before you uninstall the solution.

To remove the backup data using the Microsoft Azure portal, do the following:

1. Sign in to the Microsoft Azure portal using credentials of the Microsoft Azure account that you used to install Veeam Backup for Microsoft Azure.
2. Navigate to **Resource groups** and click the resource group to which the backed-up data belong.
3. Remove the backed-up data:
   - To remove backups, click a storage account where the backup repository storing the backed-up data resides. Navigate to **Containers** and select a container where the backups are stored. Select the check box next to the **Veeam** folder and click **Delete**.
   - To remove cloud-native snapshots, select check boxes next to the necessary snapshots. In the **Delete Resources** window, type *Yes* to confirm the action and click **Delete**.

**IMPORTANT**

If the Azure VM running Veeam Backup for Microsoft Azure resides in a resource group that contains more than one backup appliance, it is recommended that you first remove snapshots and backups created by this backup appliance, as described in section Managing Backed-Up Data. Otherwise, you will not be able to identify snapshots created by the removed backup appliance.

# Removing IAM Roles and Microsoft Entra Applications

**IMPORTANT**

Do not remove IAM roles and Microsoft Entra applications if they are still used by other backup appliances.

To remove IAM roles and Microsoft Entra applications created by Veeam Backup for Microsoft Azure, do the following:

1. Sign in to the Microsoft Azure portal using credentials of the Microsoft Azure account that you used to install Veeam Backup for Microsoft Azure.
2. Navigate to **Microsoft Entra ID** > **App registrations**.
   a. On the **All applications** tab, click **Start typing a display name or application (client) ID** and enter an application ID in the search field.

**TIP**

If you do not know the ID of an Microsoft Entra application created by Veeam Backup for Microsoft Azure, navigate to **Accounts**, switch to the **Service Accounts** tab, select the necessary account and click **Edit**. At the account type step of the opened wizard, select the **Specify existing account** option and click **Next**. Then, navigate to the **Application ID** field and copy the ID to the clipboard.

   b. On the application page, click **Delete**.

      In the **Delete app registration** window, click **Delete** to confirm the action.
3. Navigate to **Subscriptions** and click the subscription that manages costs of the backup appliance.

   On the subscription page, do the following:

   a. Navigate to **Access control (IAM)** > **Roles**.

   b. Select check boxes next to each *Veeam Service Account* role you want to remove and click **Remove**.

# Removing Azure Resources

Veeam Backup for Microsoft Azure creates a number of resources while operating in Microsoft Azure, and these resources are not removed from Microsoft Azure automatically when you uninstall the solution. That is why you must perform the following steps to remove the backup appliance and all resources created by Veeam Backup for Microsoft Azure:

1. Sign in to the Microsoft Azure portal using credentials of the Microsoft Azure account that you used to install Veeam Backup for Microsoft Azure.
2. Navigate to **Resource groups** and click the resource group in which the backup appliance is deployed.

3. On the resource group page, remove the Azure VM running Veeam Backup for Microsoft Azure, Azure VMs running worker instances and all resources associated with these VMs; you must also remove the storage accounts created by Veeam Backup for Microsoft Azure. To do that:

   a. To remove the backup appliance, do the following:

      i. In the **Resources** section, enter the name of the necessary VM in the search field.

      ii. In the **Resources** list, select check boxes next to the resources of the *Virtual machine*, *Network interface*, *Public IP address* and *Disk* types, and click **Delete**.

      In the **Delete Resources** window, type *Yes* to confirm the action and click **Delete**.

   b. To remove a worker instance, do the following:

      i. In the **Resources** section, enter the name of the necessary VM in the search field.

      ii. In the **Resources** list, select check boxes next to the resources of the *Virtual machine*, *Network interface* and *Disk* types, and click **Delete**.

      In the **Delete Resources** window, type *Yes* to confirm the action and click **Delete**.

   c. To remove the storage accounts created by Veeam Backup for Microsoft Azure, do the following:

      ii. In the **Resources** section, enter *veeam* in the search field.

      iii. In the **Resources** list, select check boxes next to the resources of the *Storage account* type and click **Delete**.

      In the **Delete Resources** window, type *Yes* to confirm the action and click **Delete**.

TIPS

- You can filter resources by the *Veeam backup appliance ID* tag. To find all resources associated with a backup appliance, navigate to the Overview page of the appliance and click the *Veeam backup appliance ID* tag.
- If you have specified a custom destination for worker instances, you will have to perform additional steps after you remove the Azure VM running Veeam Backup for Microsoft Azure. First, go back to **Resource groups**, click the resource group in which worker instances reside, and then repeat step 3b to remove the worker instances.

# Managing Accounts

To perform data protection and disaster recovery operations, and to add objects to Veeam Backup for Microsoft Azure, you must first create the following types of accounts:

- Service accounts — to get access to Azure resources that you want to protect.
- SMTP and Database accounts — to authenticate against SMTP servers and Azure databases.

# Managing Service Accounts

For each data protection and disaster recovery operation performed for an Azure resource, you must specify a service account that has access to the resource and a set of permissions that determine what operations are allowed for the resource.

Particularly, Veeam Backup for Microsoft Azure uses service accounts to perform the following tasks:

- To enumerate resources added to backup policies.
- To create snapshots and backups of Azure resources protected by policies.
- To create and manage worker instances.
- To create and manage backup repositories.
- To attach virtual disks to worker instances when performing image-level backup.
- To restore Azure VMs, virtual disks, and files and folders from cloud-native snapshots and image-level backups.
- To restore Azure SQL databases and Cosmos DB accounts from backups.
- To restore files of Azure file shares from cloud-native snapshots.
- To create backups of Azure virtual network configurations.
- To restore backups of Azure virtual network configurations from backups.

## Adding Service Accounts

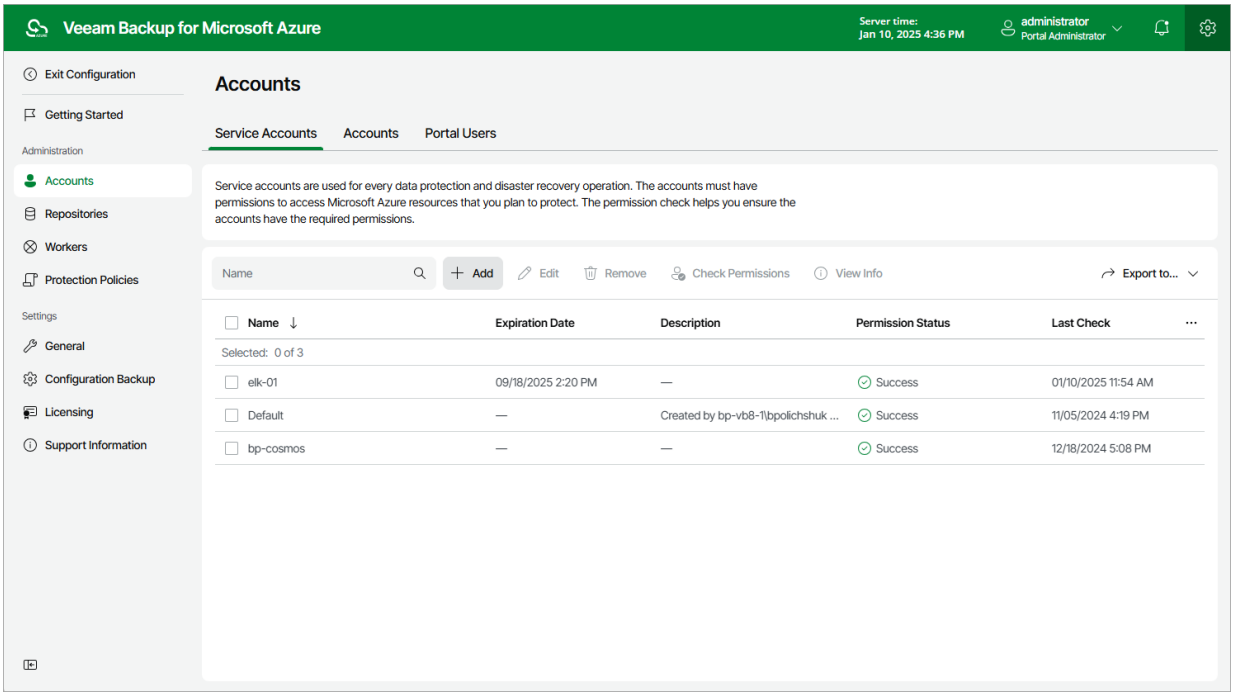
To add a new service account, do the following:

1. Launch the Add Account wizard.
2. Specify an account name and description.
3. Choose an account type.
4. Choose a scope for the account.
5. Specify account roles.
6. Check the required permissions.
7. Finish working with the wizard.

# Step 1. Launch Add Account Wizard

To launch the **Add Account** wizard, do the following:

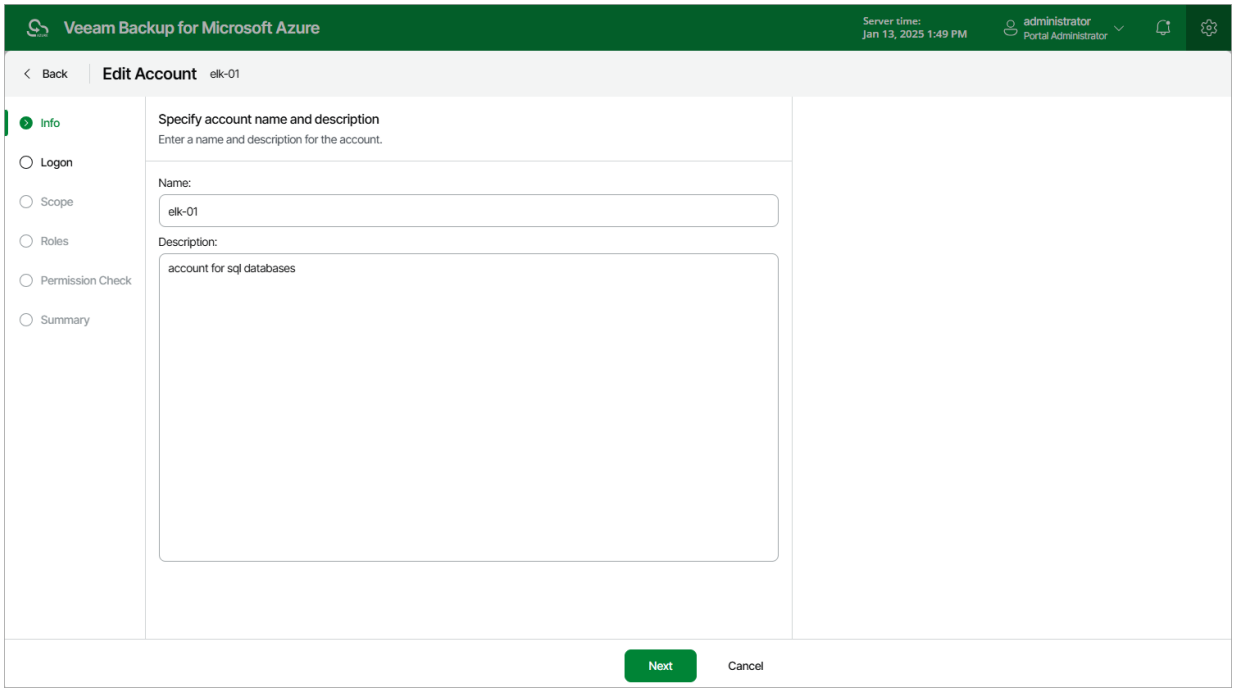
1. Switch to the **Configuration** page.
2. Navigate to **Accounts** > **Service Accounts**.
3. Click **Add**.



# Step 2. Specify Account Info

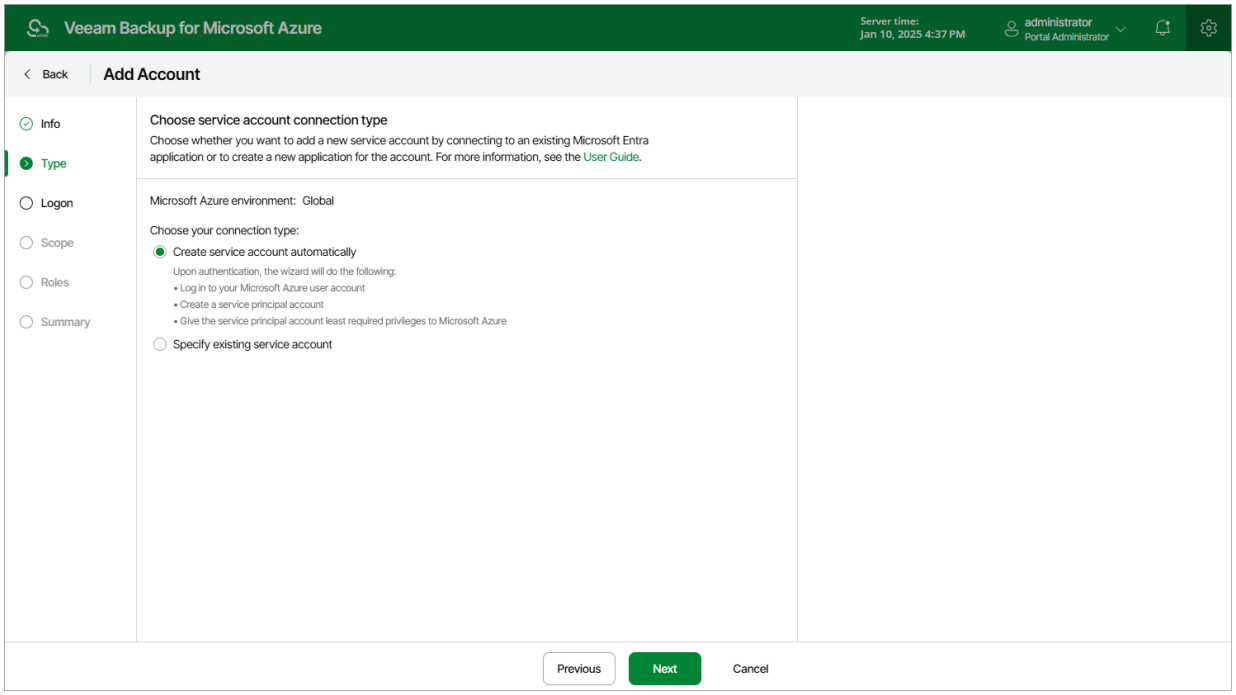
At the **Info** step of the wizard, use the **Name** and **Description** fields to enter a name for the new account and to provide a description for future reference.

The maximum length of the name is 255 characters. The following characters are supported: Latin letters, numeric characters, underscores and dashes. The following characters are not supported: / " ' : | < > + = ; , ? * @ & $ .



# Step 3. Select Connection Type

At the **Type** step of the wizard, choose whether you want to add a service account using an Microsoft Entra application that already exists in Microsoft Azure, or to create a new Microsoft Entra application and connect it to the service account.




## Creating New Microsoft Entra Application

[This step applies only if you have selected the **Create service account automatically** option at the **Type** step of the wizard]

When you choose to create a service account automatically, Veeam Backup for Microsoft Azure creates a new Microsoft Entra application in your Microsoft Entra ID. To create the Microsoft Entra application, Veeam Backup for Microsoft Azure uses the Microsoft Azure Cross-platform Command Line Interface (Azure CLI). To authenticate to the Azure CLI, you must provide a single-use verification code.

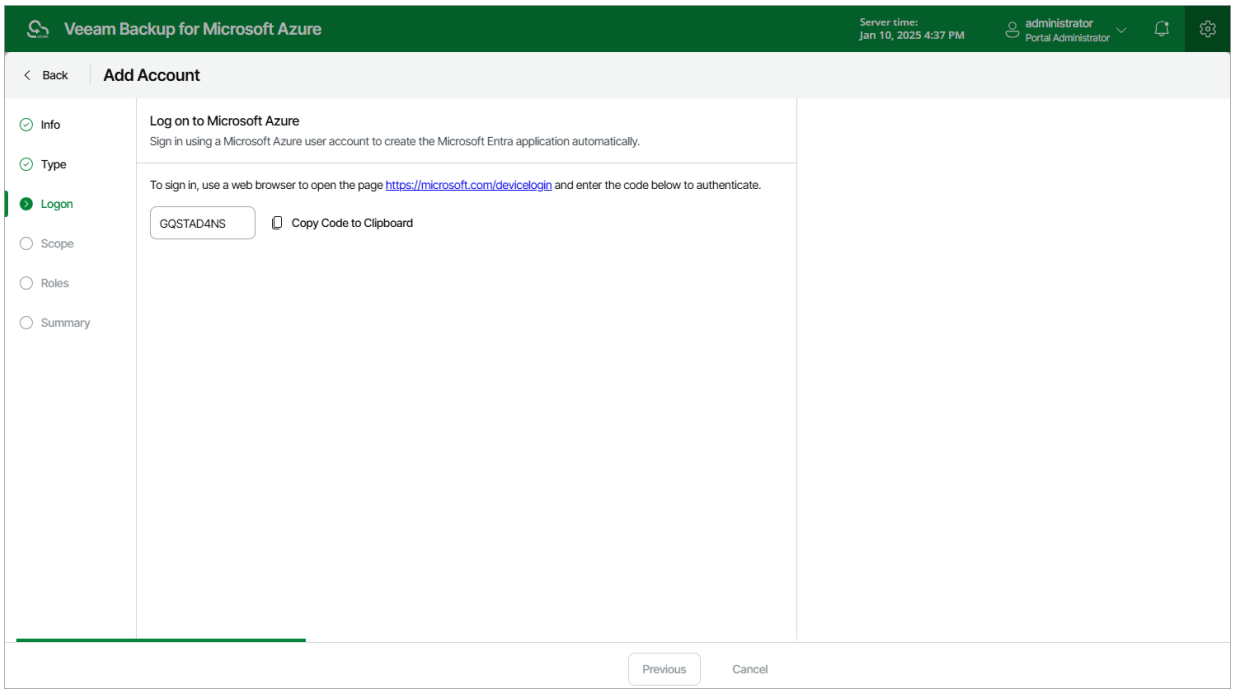
> **IMPORTANT**
>
> Consider the following:
>
> - If you have disabled the **Users can register applications option** in the Microsoft Azure portal, the Microsoft Azure account that you use to access the Azure CLI must be assigned the *Application Developer*, *Application Administrator* or *Global Administrator* role. For more information on Microsoft Entra ID roles, see Microsoft Docs.
> - The Microsoft Azure account that you use to access the Azure CLI must have the *Microsoft.Authorization/*/Write* permission specified in the subscription associated with the backup appliance. For more information on managing role permissions and security in Microsoft Azure, see Microsoft Docs.
> - When registering new Microsoft Entra applications, Veeam Backup for Microsoft Azure also creates client secrets that will be further used to authorize access to Microsoft Azure (one client secret for each Microsoft Entra application). The lifetime of a client secret is limited to one year. To view the expiration date of a client secret, navigate to **Service Accounts**. To renew a client secret that is about to expire, follow the instructions provided in section Editing Service Accounts.

At the **Logon** step of the wizard, do the following:

1. Click **Copy Code to Clipboard**.
2. Click **https://microsoft.com/devicelogin**.
3. On the Microsoft Azure device authentication page, do the following:
   a. Paste the code that you have copied and click **Next**.
   b. Select a Microsoft Azure account that will be used to access the Azure CLI. The account must be assigned either the *User Access Administrator* or the *Owner* role.

> **IMPORTANT**
>
> Using a personal Microsoft account is not recommended — use a work account instead.

4. Back to the **Add Account** wizard, check whether any errors occurred during the authentication process and click **Next**.




## Specifying Existing Microsoft Entra Application

[This step applies only if you have selected the **Specify existing service account** option at the **Type** step of the wizard]

When you choose to specify an existing service account, Veeam Backup for Microsoft Azure connects to an existing Microsoft Entra application that grants access to your Azure resources. For Veeam Backup for Microsoft Azure to be able to connect to the Microsoft Entra application and to protect Azure resources, the application must be created in Microsoft Azure, and have the *Contributor*, *Key Vault Crypto User* and *Storage Queue Data Contributor* Azure built-in roles assigned. To learn how to create Microsoft Entra applications and assign Azure roles, see Microsoft Identity Platform and Azure RBAC documentation.

> **TIP**
>
> If you want the service account to have granular permissions, you can create a custom role in Microsoft Azure, grant the necessary permissions to this role, and then assign the role to the Microsoft Entra application instead of the built-in roles. For the list of required permissions, see Service Account Permissions.

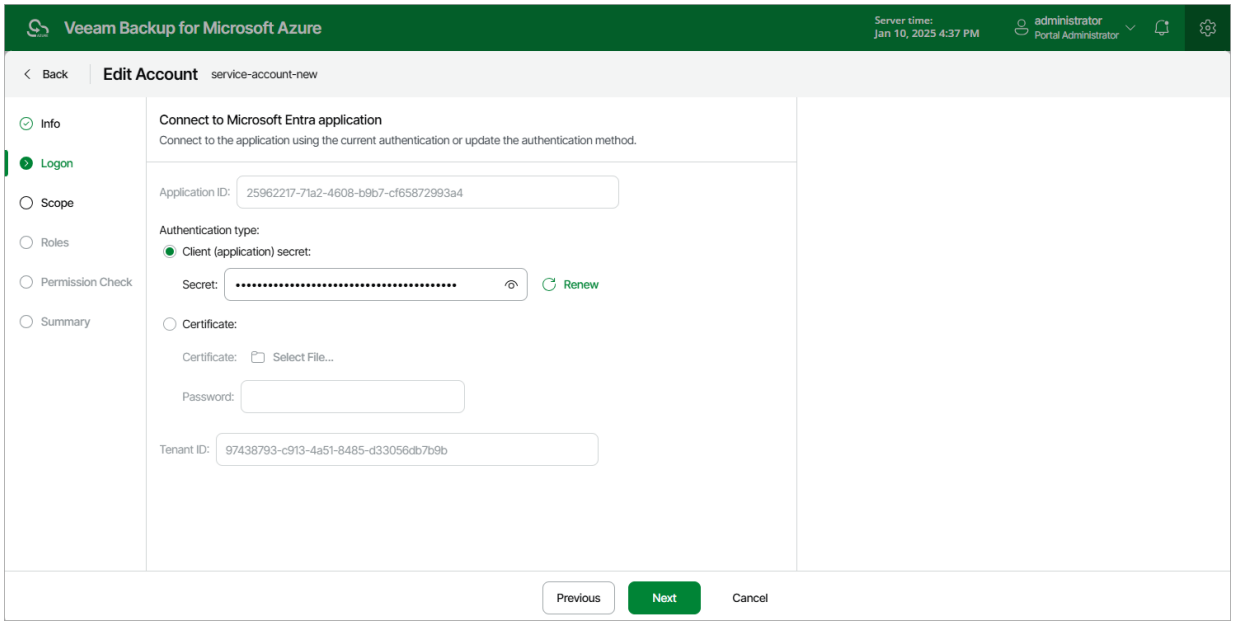
At the **Logon** step of the wizard, specify an existing service account that grants access to your Azure resources:

1. In the **Application ID** field, enter the application identifier. You can find the identifier on the **Overview** page of your Microsoft Entra application in the Microsoft Azure portal. For more information, see Microsoft Docs.
2. Select an application authentication type:
   - Select the **Client (application) secret** option to use a client secret created in the specified Microsoft Entra application. In the **Secret** field, enter the value of the secret. To learn how to create client secrets, see Microsoft Docs.
   - Select the **Certificate** option to use a certificate uploaded to the specified Microsoft Entra application. In the **Certificate** field, click **Select File** to locate the certificate. Then, provide a password used to encrypt the certificate in the **Password** field. To learn how to upload certificates to Microsoft Entra applications, see Microsoft Docs.

> **IMPORTANT**
>
> Veeam Backup for Microsoft Azure supports certificates only in the formats .PFX and .P12.

3. In the **Tenant ID** field, enter the tenant ID of the specified Microsoft Entra application.

   You can find the tenant ID on the **Overview** page of your Microsoft Entra application in the Microsoft Azure portal. For more information, see Microsoft Docs.



## Step 4. Select Account Scope

At the **Scope** step of the wizard, specify the account scope — select subscriptions whose data you want to protect.

# Configuring Scope of Automatically Created Accounts

If you have selected the **Create service account automatically** option at the **Type** step of the wizard, do the following:

1. Click the link in the **Tenant ID** field and choose an Microsoft Entra tenant in which the Microsoft Entra application associated with the service account will be created. For a tenant to be displayed in the list of available tenants, the Microsoft Azure account that you use to access the Azure CLI must have access to this tenant.

   The value displayed in the **App Registration** column defines whether the Microsoft Azure account that you use to access the Azure CLI has permissions to create Microsoft Entra applications in the tenant. If the Microsoft Azure account does not have these permissions, assign the *Application Developer*, *Application Administrator* or *Global Administrator* role to the account in Microsoft Azure as described in Microsoft Docs. To make sure that the role has been successfully assigned, click **Recheck**.

2. In the **Subscriptions to protect** field, use either of the following options:

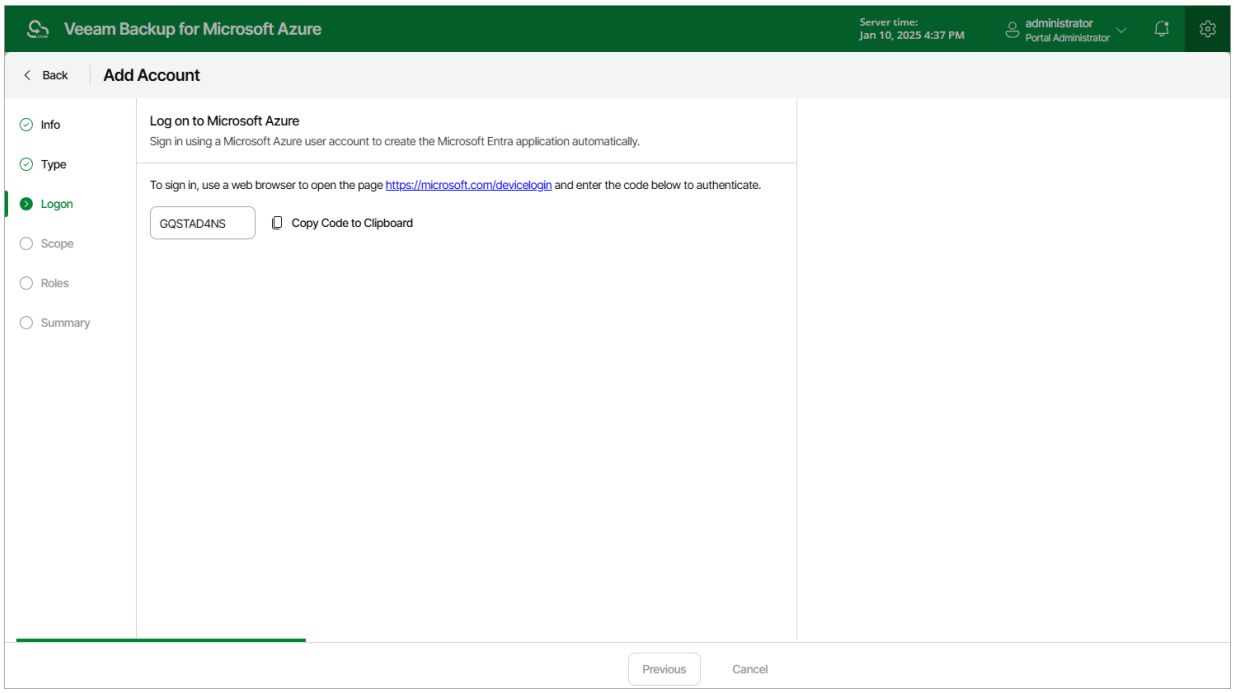
   - To manually specify Azure subscriptions to which the resources that you want to protect belong, click the link in the **Protected subscriptions** field and select all necessary Azure subscriptions. For a subscription to be displayed in the list of available subscriptions, it must be associated with the selected Microsoft Entra tenant as described in Microsoft Docs.

     The value displayed in the **Permissions State** column defines whether the Microsoft Azure account that you use to access the Azure CLI has the *Microsoft.Authorization/*/Write* permission to create roles and role assignments for the subscription. If the Microsoft Azure account does not have this permission, grant it to the account in Microsoft Azure as described in Microsoft Docs. To make sure that the permission has been successfully granted, click **Recheck**.

   - To back up Azure resources that belong to Azure subscriptions added to a management group, select the **Use management group** option and specify a group that manages subscriptions to which the resources that you want to protect belong. For a group to be displayed in the list of available management groups, it must be created in the Microsoft Azure portal as described in Microsoft Docs.

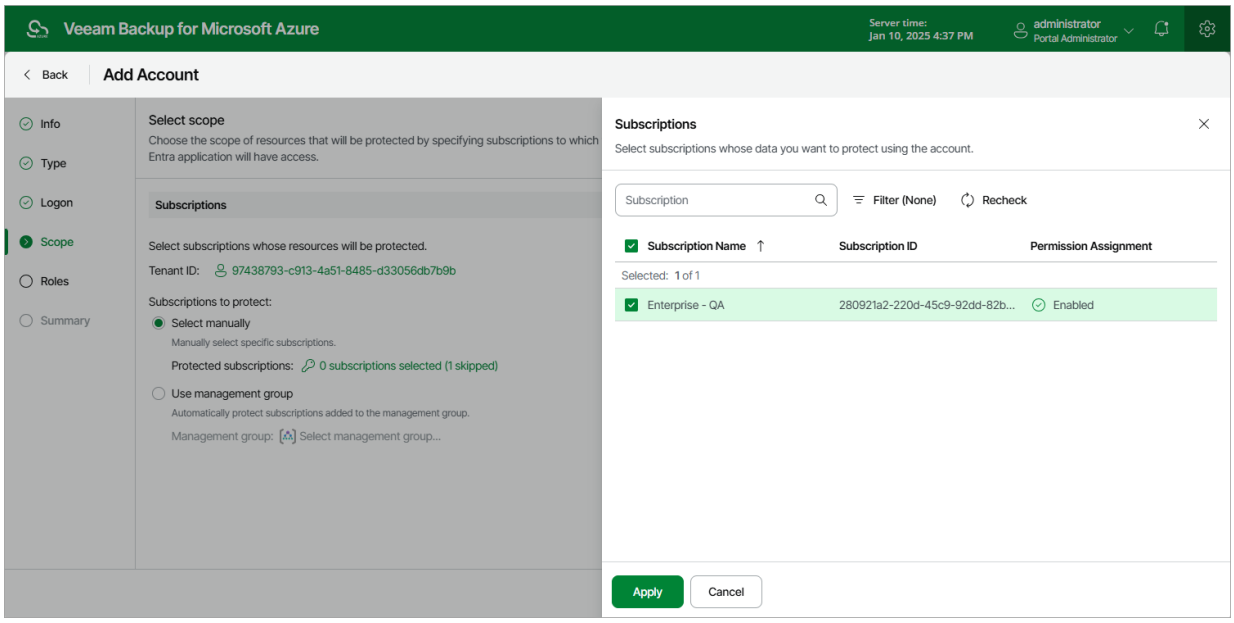
     If you specify a management group as the account scope, Veeam Backup for Microsoft Azure will regularly check for new subscriptions added to the specified group and automatically update the account settings to include these subscriptions in the scope. However, this does not apply to subscriptions added to nested management groups — if the specified group contains other management groups and you want to protect resources that belong to subscriptions in these groups, it is recommended that you move the subscriptions from the nested groups to the root one.

> **IMPORTANT**
>
> To be able to select a management group as a scope for the created service account, the Microsoft Azure account that you use to access the Azure CLI must meet the following requirements:
>
> - It must have elevated access to manage all Azure subscriptions and management groups in Microsoft Entra ID. To learn how to elevate access for Microsoft Azure accounts, see Microsoft Docs.
> - It must have the *Owner* built-in role assigned at the management group scope. To learn how to assign Azure roles, see Azure RBAC documentation.




# Configuring Scope of Existing Accounts

If you have selected the **Specify existing service account** option at the **Type** step of the wizard, click the link in the **Subscriptions to protect** field and choose Azure subscriptions to which the resources that you want to protect belong. For a subscription to be displayed in the list of available subscriptions, the Microsoft Entra application specified at step 3 of the wizard must have the *Contributor* Azure built-in role assigned in this subscription. To learn how to assign Azure roles, see Microsoft Docs.



## Step 5. Select Account Roles

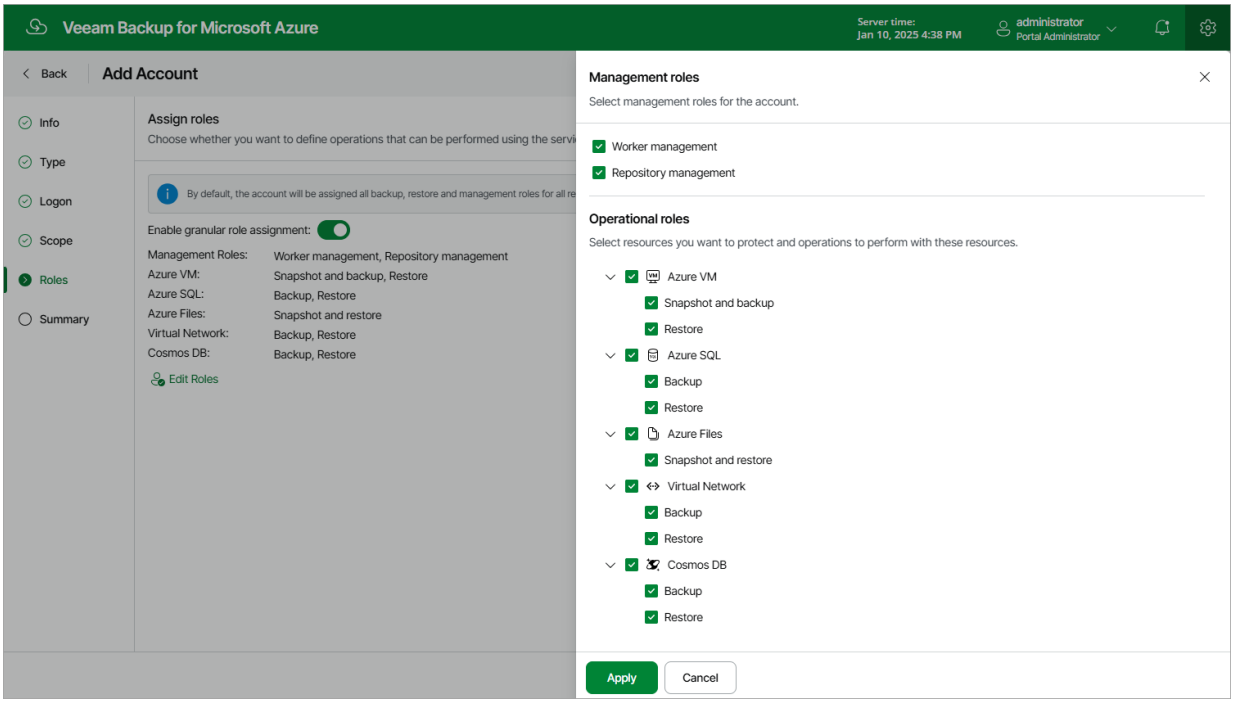
At the **Roles** step of the wizard, you can define specific operations that Veeam Backup for Microsoft Azure will be able to perform using permissions of the service account:

1. Set the **Enable granular role assignment** toggle to *On* and click **Edit Roles**.
2. In the **Management roles** section, choose actions that will be performed using the service account:
   - **Worker management** — permissions of this service account will be used to launch worker instances. If you create a service account of this type, you will be able to select it when managing worker configurations.
   - **Repository management** — permissions of this service account will be used to create new repositories in target Azure blob containers and to further access the repositories during data protection and disaster recovery operations. If you create a service account of this type, you will be able to select it when configuring repository settings.

> **IMPORTANT**
>
> For Veeam Backup for Microsoft Azure to perform the selected actions using the service account, the account must be assigned the permissions listed in sections Worker Permissions and Repository Permissions.

3. In the **Operational roles** section, choose resources that will be protected using permissions of the service account, and operations that will be performed with these resources:
   - If you select the **Backup** operation, you will be able to specify the service account when performing VM backup, SQL backup, Cosmos DB backup and virtual network configuration backup.
   - If you select the **Snapshot** operation, you will be able to specify the service account when performing VM backup and Azure Files backup.
   - If you select the **Restore** operation, you will be able to specify the service account when performing VM restore, SQL restore, file share restore, Cosmos DB restore and virtual network configuration restore.

> **IMPORTANT**
>
> Keep in mind that Veeam Backup for Microsoft Azure does not grant any permissions automatically, unless you have selected the **Create service account automatically** option at step 3 of the wizard. That is why it is recommended that you check whether the added service account has all the permissions required to perform operations with the selected resources, as described in section Checking Service Account Permissions.


Veeam Backup for Microsoft Azure
Server time:
Jan 10, 2025 4:38 PM
administrator
Portal Administrator
Back
Add Account
Info
Type
Logon
Scope
Roles
Summary
Assign roles
Choose whether you want to define operations that can be performed using the servi
By default, the account will be assigned all backup, restore and management roles for all re
Enable granular role assignment:
Management Roles: Worker management, Repository management
Azure VM: Snapshot and backup, Restore
Azure SQL: Backup, Restore
Azure Files: Snapshot and restore
Virtual Network: Backup, Restore
Cosmos DB: Backup, Restore
Edit Roles
Management roles
Select management roles for the account.
Worker management
Repository management
Operational roles
Select resources you want to protect and operations to perform with these resources.
Azure VM
Snapshot and backup
Restore
Azure SQL
Backup
Restore
Azure Files
Snapshot and restore
Virtual Network
Backup
Restore
Cosmos DB
Backup
Restore
Apply
Cancel

# Step 6. Check Account Permissions

[This step applies only if you have selected the **Specify existing service account** option at the **Type** step of the wizard]

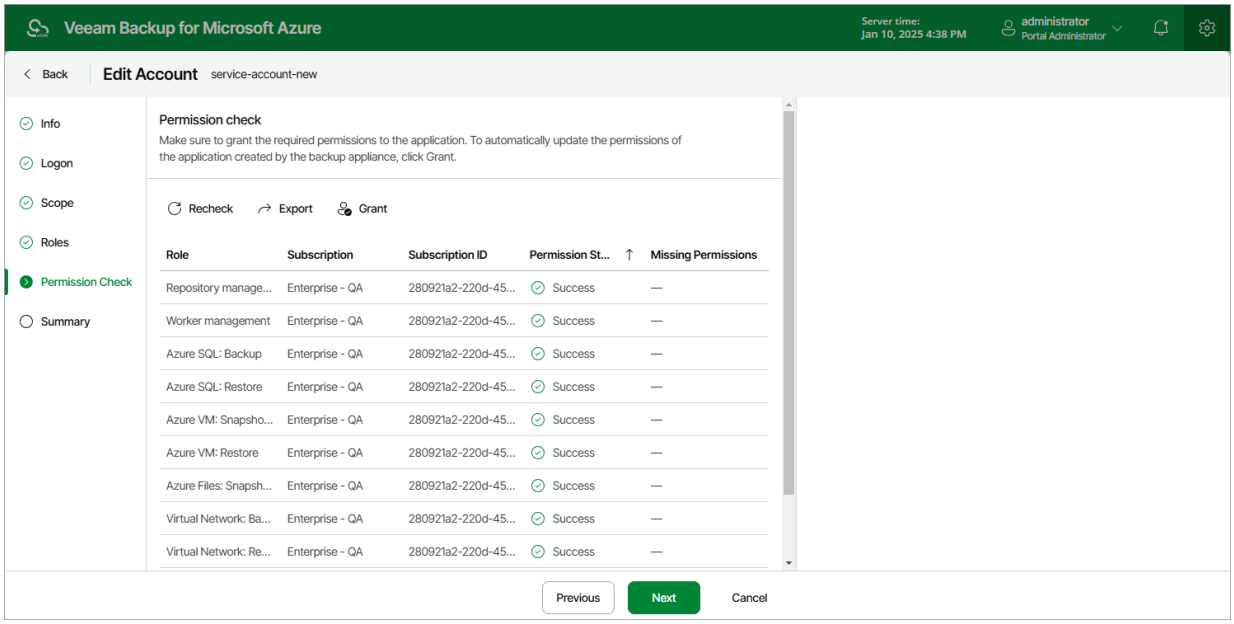
At the **Permissions Check** step of the wizard, Veeam Backup for Microsoft Azure will verify whether the new service account has all the permissions required to access Azure resources that you want to protect. For more information on the required permissions, see Service Account Permissions.

> **NOTE**
>
> To be able to check all the permissions granted to the service account, the Microsoft Entra application that you used to create the account at step 3 must have the `"Microsoft.Authorization/roleAssignments/read"` permission assigned.

In case any of the permission checks fail, do the following:

1. Click **Export**. Veeam Backup for Microsoft Azure will save the .JSON file with the full list of all required permissions to the default download directory on the local machine.
2. Use the downloaded file to create a custom role in Microsoft Azure as described in Microsoft Docs.
3. Assign the created role to the Microsoft Entra application associated with the new service account as described in Microsoft Docs.

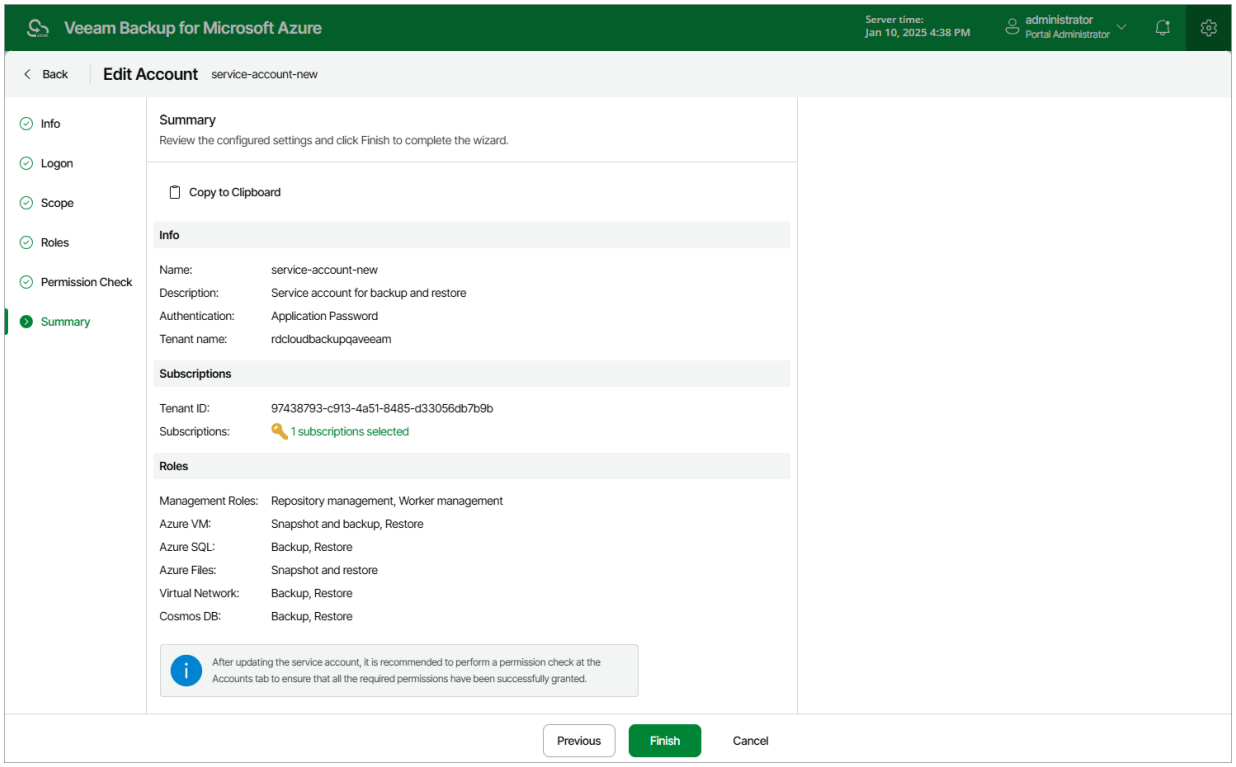
To make sure that the missing permissions have been successfully granted, click **Recheck**. Keep in mind that it may take up to 15 minutes for Veeam Backup for Microsoft Azure to detect the newly granted permissions.



## Step 7. Finish Working with Wizard

At the **Summary** step of the wizard, review configuration information and click **Finish**.

> **TIP**
>
> It is recommended that you check whether the account has all the permissions required to perform backup and restore operations. For more information, see Checking Service Account Permissions.




# Editing Service Accounts

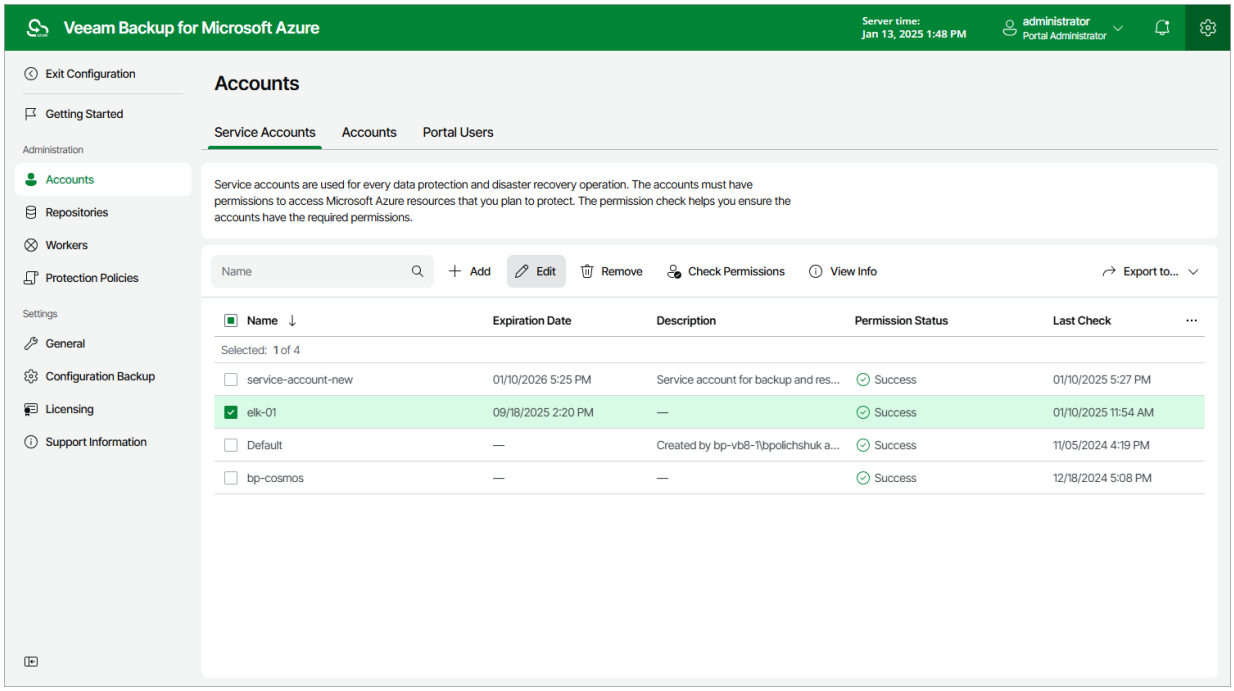
To edit a service account, do the following:

1. Launch the Edit Account wizard.
2. Update the account name and description.
3. Connect to the Microsoft Entra application with which the account is associated.
4. Change the account scope.
5. Update account roles.
6. Check the required permissions.
7. Finish working with the wizard.

# Step 1. Launch Edit Account Wizard

To launch the **Edit Account** wizard, do the following:

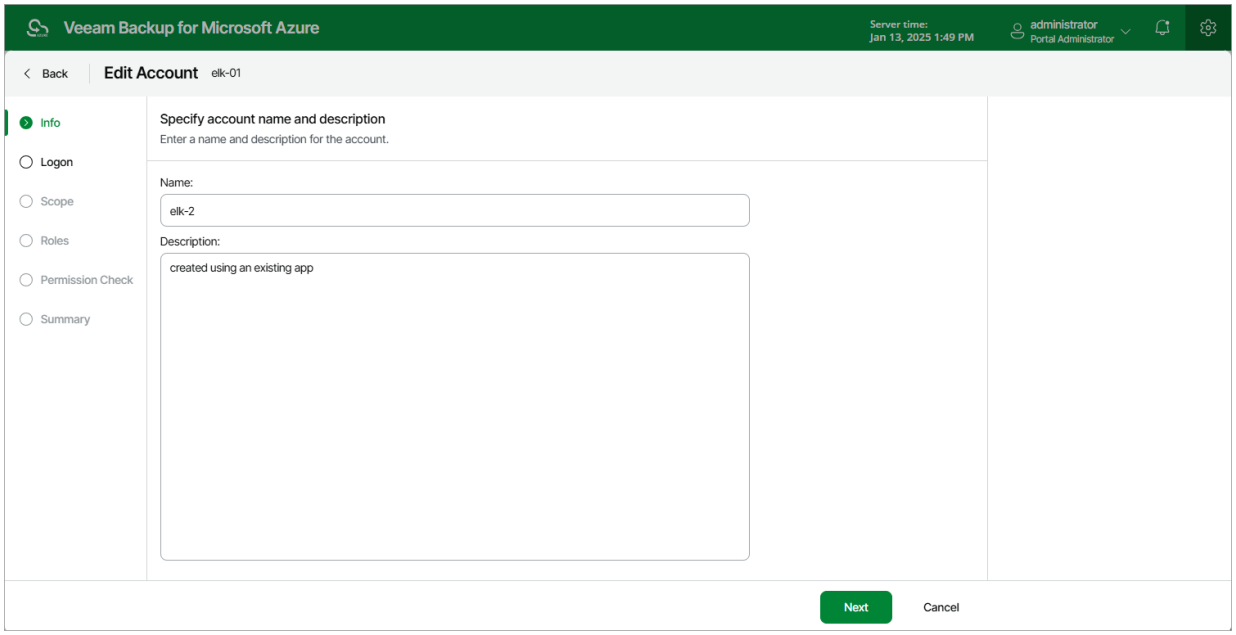
1. Switch to the **Configuration** page.
2. Navigate to **Accounts** > **Service Accounts**.
3. Select the service account and click **Edit**.



# Step 2. Update Account Info

At the **Info** step of the wizard, use the **Name** and **Description** fields to provide a new name and description for the account.

The maximum length of the name is 255 characters. The following characters are supported: Latin letters, numeric characters, underscores and dashes. The following characters are not supported: / " ' : | < > + = ; , ? * @ & $ .



### Step 3. Connect to Microsoft Entra Application

At the **Logon** step of the wizard, you can review the authentication method that is currently used to connect to the Microsoft Entra application with which the service account is associated. You can also renew a client secret that is about to expire, or associate a new Microsoft Entra application with the service account in case the application that was previously used is no longer available.

## Renewing Microsoft Entra Application Secret

To renew a client secret that is about to expire, use either of the following options:

- If you have selected the **Specify existing service account** option at the **Type** step of the **Add Account** wizard, create a new client secret in the specified Microsoft Entra application, enter the secret value in the **Secret** field and then click **Next**. To learn how to create client secrets, see Microsoft Docs.
- If you have selected the **Create service account automatically** option at the **Type** step of the **Add Account** wizard, do the following:
  a. Click **Renew** next to the **Secret** field.
  b. In the **Logon to Microsoft Azure** window, click **Copy Code to Clipboard** and then click **https://microsoft.com/devicelogin**.
  c. On the Microsoft Azure device authentication page, do the following:
     i. Paste the code that you have copied and click **Next**.
     ii. Select a Microsoft Azure account that will be used to access the Azure CLI. The account must be assigned either the *User Access Administrator* or the *Owner* role.
  d. Back to the **Logon to Microsoft Azure** window, check whether any errors occurred during the authentication process and click **OK**.

## Re-creating Microsoft Entra Application

If the Microsoft Entra application that has been used to create the service account is not available or no longer exists in Microsoft Azure, you can create a new Microsoft Entra application that will be associated with the service account. To do that, use either of the following options:

- If you have selected the **Create service account automatically** option at the **Type** step of the **Add Account** wizard, do the following:
  a. Click **Re-create** next to the **Application ID** field.
  b. In the **Logon to Microsoft Azure** window, click **Copy Code to Clipboard** and then click **https://microsoft.com/devicelogin**.
  c. On the Microsoft Azure device authentication page, do the following:
     iii. Paste the code that you have copied and click **Next**.
     iv. Select a Microsoft Azure account that will be used to access the Azure CLI. The account must be assigned either the *User Access Administrator* or the *Owner* role.
  c. Back to the **Logon to Microsoft Azure** window, check whether any errors occurred during the authentication process and click **OK**.

- If you have selected the **Specify existing service account** option at the **Type** step of the **Add Account** wizard, provide another Microsoft Entra application:

  a. In the **Application ID** field, enter the application identifier. You can find the identifier on the **Overview** page of your Microsoft Entra application in the Microsoft Azure portal. For more information, see Microsoft Docs.

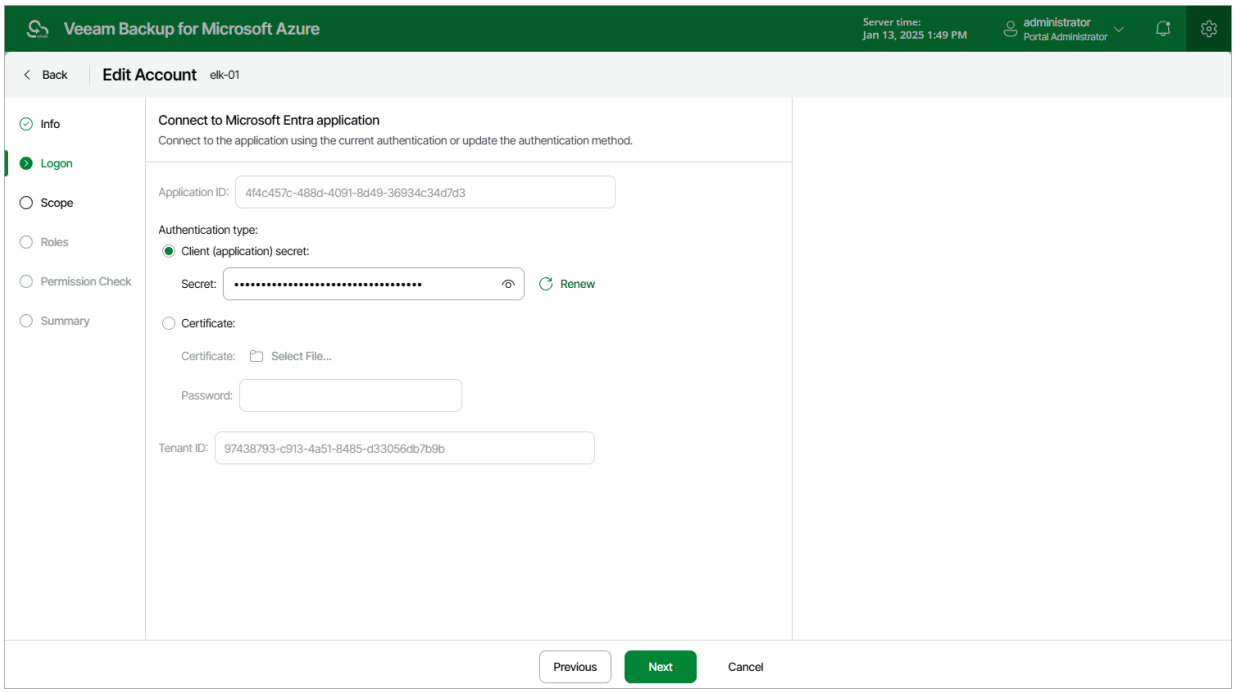
  b. Select an application authentication type:

  - Select the **Client (application) secret** option to use a client secret created in the specified Microsoft Entra application. In the **Secret** field, enter the value of the secret. To learn how to create client secrets, see Microsoft Docs.
  - Select the **Certificate** option to use a certificate uploaded to the specified Microsoft Entra application. In the **Certificate** field, click **Select File** to locate the certificate. Then, provide a password used to encrypt the certificate in the **Password** field. To learn how to upload certificates to Microsoft Entra applications, see Microsoft Docs.

**IMPORTANT**

Consider the following:

- For Veeam Backup for Microsoft Azure to be able to connect to the specified Microsoft Entra application, the application must be created in Microsoft Azure, and have the *Contributor*, *Key Vault Crypto User* and *Storage Queue Data Contributor* Azure built-in roles assigned. To learn how to create Microsoft Entra applications and assign Azure roles, see Microsoft Identity Platform and Azure RBAC documentation.
- Veeam Backup for Microsoft Azure supports certificates only in the formats .PFX and .P12.

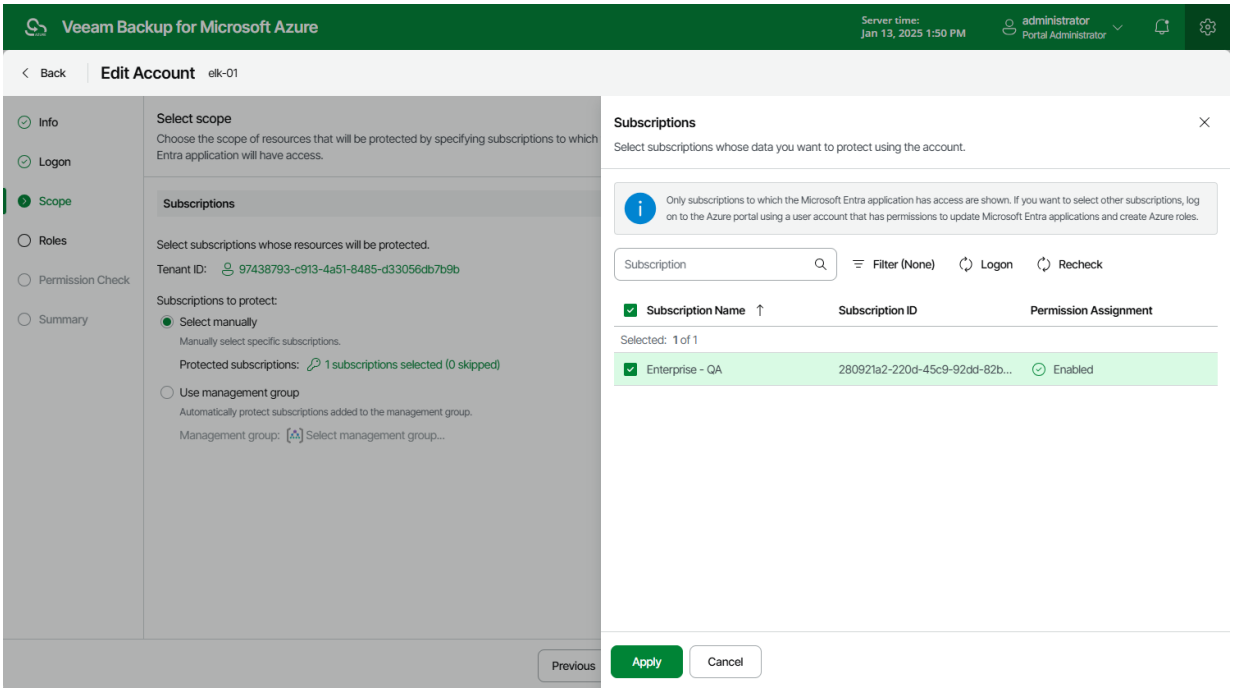


# Step 4. Update Account Scope

At the **Scope** step of the wizard, you can change the account scope — select subscriptions whose data you want to protect using permissions of the service account. To do that, click the link in the **Subscriptions to protect** field and choose Azure subscriptions to which the resources that you want to protect belong.

For a subscription to be displayed in the list of available subscriptions, the Microsoft Entra application with which the service account is associated must have the *Contributor* Azure built-in role assigned in this subscription. To learn how to assign Azure roles, see Microsoft Docs.

[Applies only if the service account has been created automatically] If you have not logged in to Azure portal at step 3 of the wizard, to update the list of available subscriptions, click **Logon**. The value displayed in the **Permission Assignment** column defines whether the Microsoft Azure account that you used to access the Azure CLI has the *Microsoft.Authorization/*/Write* permission to create roles and role assignments for the subscription. If the Microsoft Azure account does not have this permission, grant it to the account in Microsoft Azure as described in Microsoft Docs. To make sure that the permission has been successfully granted, click **Recheck**.



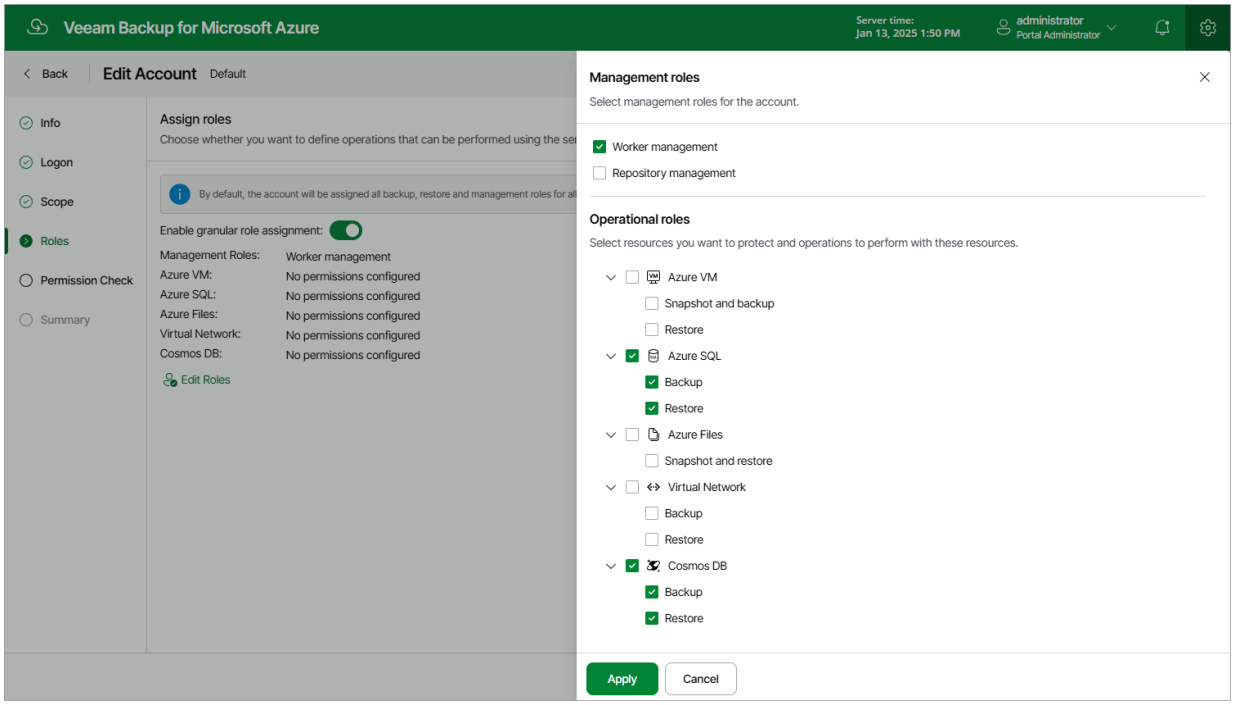
# Step 5. Update Account Roles

At the **Roles** step of the wizard, you can modify the list of operations that Veeam Backup for Microsoft Azure will be able to perform using permissions of the service account:

1. Set the **Enable granular role assignment** toggle to *On* and click **Edit Roles**.
2. In the **Management roles** section, choose actions that will be performed using the service account:
   - **Worker management** – permissions of this service account will be used to launch worker instances. If you create a service account of this type, you will be able to select it when managing worker configurations.
   - **Repository management** – permissions of this service account will be used to create new repositories in target Azure blob containers and to further access the repositories during data protection and disaster recovery operations. If you create a service account of this type, you will be able to select it when configuring repository settings.

> **IMPORTANT**
>
> For Veeam Backup for Microsoft Azure to perform the selected actions using the service account, the account must be assigned the permissions listed in sections Worker Permissions and Repository Permissions.

3. In the **Operational roles** section, choose resources that will be protected using permissions of the service account, and operations that will be performed with these resources:
   - If you select the **Backup** operation, you will be able to specify the service account when performing VM backup, SQL backup, Cosmos DB backup and virtual network configuration backup.
   - If you select the **Snapshot** operation, you will be able to specify the service account when performing VM backup and Azure Files backup.
   - If you select the **Restore** operation, you will be able to specify the service account when performing VM restore, SQL restore, Cosmos DB restore, file share restore and virtual network configuration restore.



## Step 6. Check Account Permissions

At the **Permissions Check** step of the wizard, you can check whether the service account has all the permissions required to access Azure resources that you want to protect. For more information on the required permissions, see Service Account Permissions.

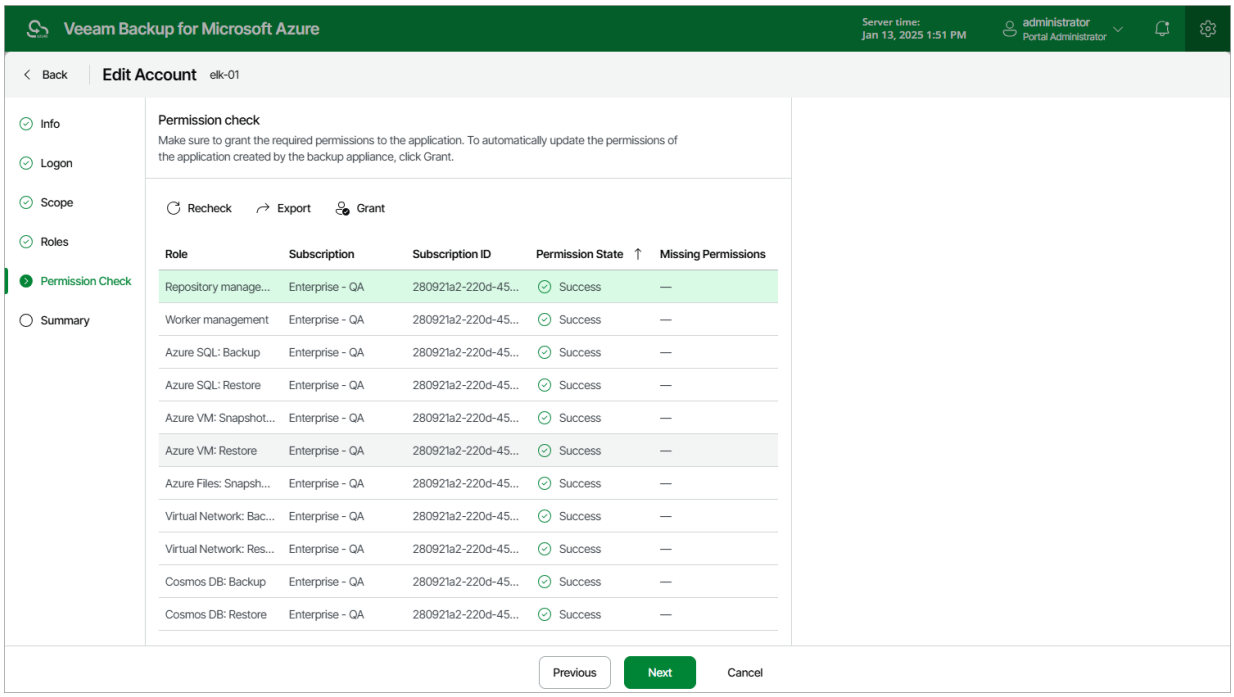
> **NOTE**
>
> To be able to check all the permissions granted to the service account, the Microsoft Entra application to which you connected at step 3 must have the `"Microsoft.Authorization/roleAssignments/read"` permission assigned.

In case any of the permission checks fail, use either of the following options:

- If the service account has been created automatically, click **Grant**. If you have already logged in to Azure portal at step 3 or step 4 of the wizard, Veeam Backup for Microsoft Azure will automatically grant the missing permissions to the Microsoft Entra application with which the service account is associated. If you have not logged in to Azure portal, do the following:
  a. In the **Logon to Microsoft Azure** window, click **Copy Code to Clipboard** and then click **https://microsoft.com/devicelogin**.
  b. On the Microsoft Azure device authentication page, do the following:
     i. Paste the code that you have copied and click **Next**.
     ii. Select a Microsoft Azure account that will be used to access the Azure CLI. The account must be assigned either the *User Access Administrator* or the *Owner* role.
  c. Back to the **Logon to Microsoft Azure** window, check whether any errors occurred during the authentication process and click **OK**.
- If the service account has been created using an existing Microsoft Entra application, do the following:
  a. Click **Export**. Veeam Backup for Microsoft Azure will save the .JSON file with the full list of all required permissions to the default download directory on the local machine.
  b. Use the downloaded file to create a custom role in Microsoft Azure as described in Microsoft Docs.
  c. Assign the created role to the Microsoft Entra application with which the service account is associated, as described in Microsoft Docs.

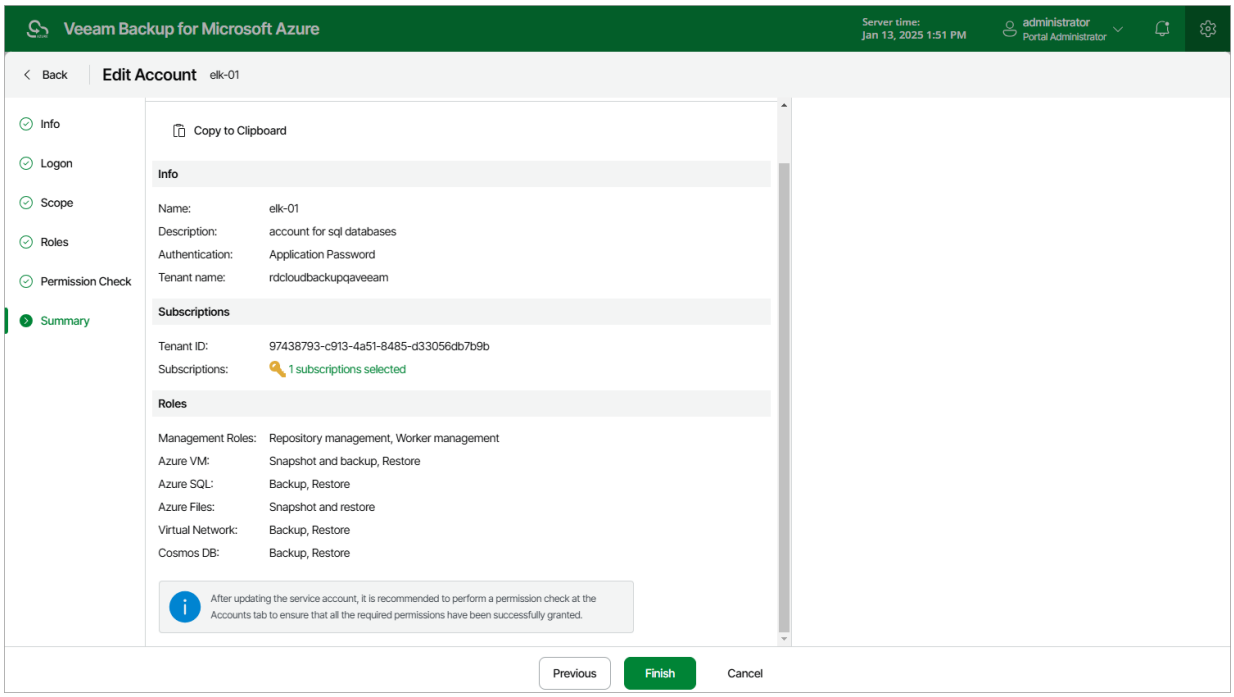
To make sure that the missing permissions have been successfully granted, click **Recheck**.

> **NOTE**
>
> If you removed any roles at step 5 of the wizard, you also need to click **Grant** to update the list of operations that Veeam Backup for Microsoft Azure will be able to perform using permissions of the service account.


Veeam Backup for Microsoft Azure
Server time:
Jan 13, 2025 1:51 PM
administrator
Portal Administrator
Back
Edit Account
elk-01
Info
Logon
Scope
Roles
Permission Check
Summary
Permission check
Make sure to grant the required permissions to the application. To automatically update the permissions of the application created by the backup appliance, click Grant.
Recheck
Export
Grant
Role
Subscription
Subscription ID
Permission State
Missing Permissions
Repository manage...
Enterprise - QA
280921a2-220d-45...
Success
—
Worker management
Enterprise - QA
280921a2-220d-45...
Success
—
Azure SQL: Backup
Enterprise - QA
280921a2-220d-45...
Success
—
Azure SQL: Restore
Enterprise - QA
280921a2-220d-45...
Success
—
Azure VM: Snapshot...
Enterprise - QA
280921a2-220d-45...
Success
—
Azure VM: Restore
Enterprise - QA
280921a2-220d-45...
Success
—
Azure Files: Snapsh...
Enterprise - QA
280921a2-220d-45...
Success
—
Virtual Network: Bac...
Enterprise - QA
280921a2-220d-45...
Success
—
Virtual Network: Res...
Enterprise - QA
280921a2-220d-45...
Success
—
Cosmos DB: Backup
Enterprise - QA
280921a2-220d-45...
Success
—
Cosmos DB: Restore
Enterprise - QA
280921a2-220d-45...
Success
—
Previous
Next
Cancel

## Step 7. Finish Working with Wizard

At the **Summary** step of the wizard, review configuration information and click **Finish**.




# Checking Service Account Permissions

For each service account, you can check whether the account has all the permissions required to access Azure resources that you want to protect:

1. Switch to the **Configuration** page.
2. Navigate to **Accounts** > **Service Accounts**.
3. Select the service account and click **Check Permissions**.

If any of the permission checks fail, you must assign the missing permissions to the account either automatically or manually — depending on whether you chose to create the account automatically or to specify an existing account.

# Granting Permissions Automatically

To grant the missing permissions automatically, do the following:

1. In the **Permission Check** window, click **Grant**.
2. In the **Logon to Microsoft Azure** window, click **Copy Code to Clipboard** and then click **https://microsoft.com/devicelogin**.
3. On the Microsoft Azure device authentication page, do the following:
   a. Paste the code that you have copied and click **Next**.
   b. Select a Microsoft Azure account that will be used to access the Azure CLI. The account must be assigned either the *User Access Administrator* or the *Owner* role.

4. Back to the **Logon to Microsoft Azure** window, check whether any errors occurred during the authentication process and click **OK**.

To make sure that the missing permissions have been successfully granted, click **Recheck**.

# Assigning Permissions Manually

To assign the missing permissions manually, do the following:

1. In the **Permission Check** window, click **Export Permissions**.

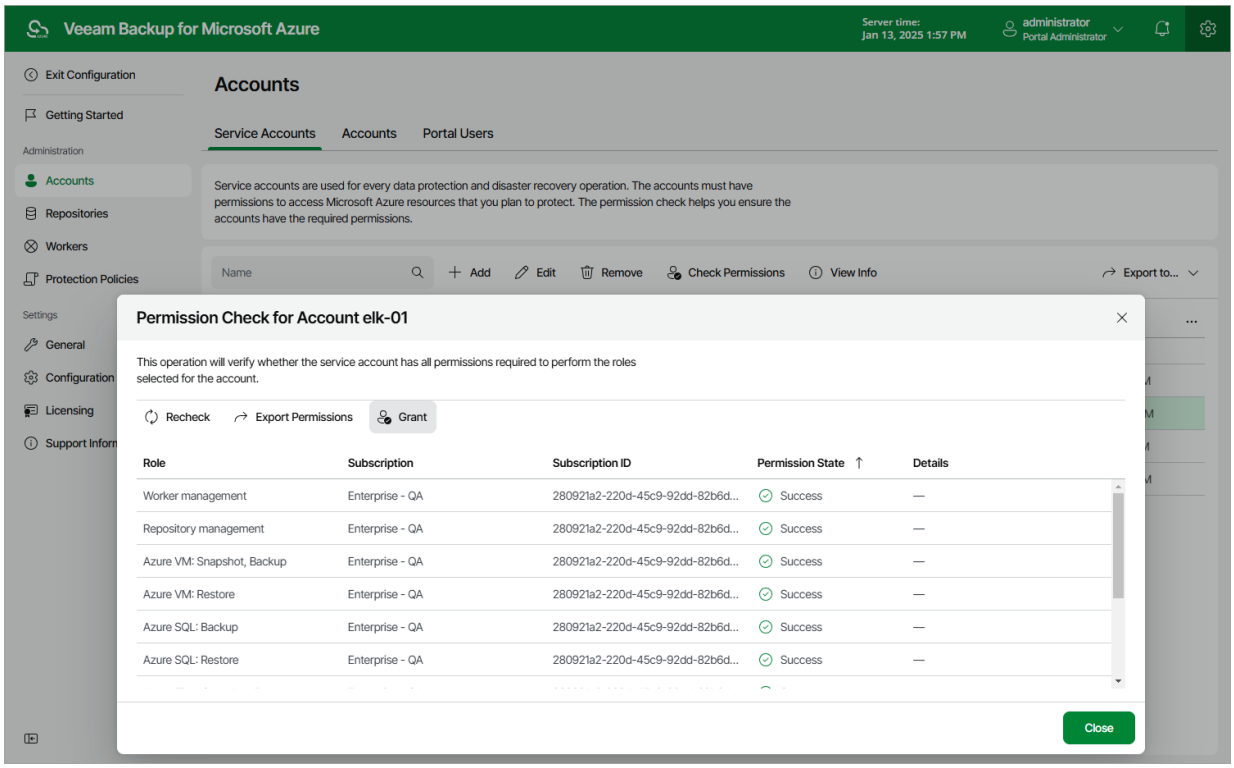
   Veeam Backup for Microsoft Azure will save the .JSON file with the full list of all required permissions to the default download directory on the local machine. For more information on the required permissions, see Service Account Permissions.

2. Use the downloaded file to create a custom role in Microsoft Azure as described in Microsoft Docs.

3. Assign the created role to the Microsoft Entra application associated with the service account as described in Microsoft Docs.

To make sure that the missing permissions have been successfully granted, click **Recheck**.

> **TIP**
>
> To see the list of operations that Veeam Backup for Microsoft Azure will be able to perform using permissions of a service account, select the service account and click **View Info**.



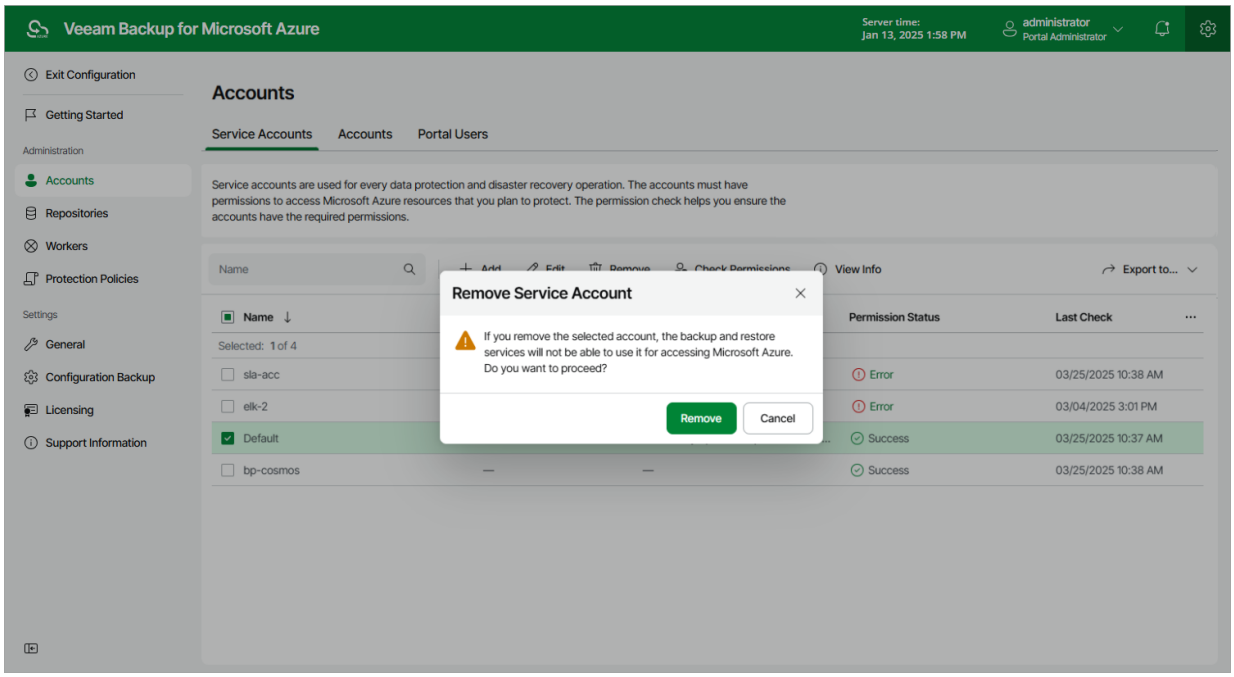

# Removing Service Accounts

You can remove a service account from Veeam Backup for Microsoft Azure if it is no longer used to perform data protection and disaster recovery operations.

> **IMPORTANT**
>
> You cannot remove a service account that is used to access backup repositories or is specified in the settings of any configured backup policy. <select another SA in a repo or backup policy settings>

To remove a service account, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **Accounts** > **Service Accounts**.
3. Select the service account and click **Remove**.



# Managing SMTP and Database Accounts

To allow Veeam Backup for Microsoft Azure to authenticate against Azure databases protected by backup policies and SMTP servers used for sending email notifications, you must specify credentials of accounts that will be used to access these databases and servers.

## Adding SMTP and Database Accounts

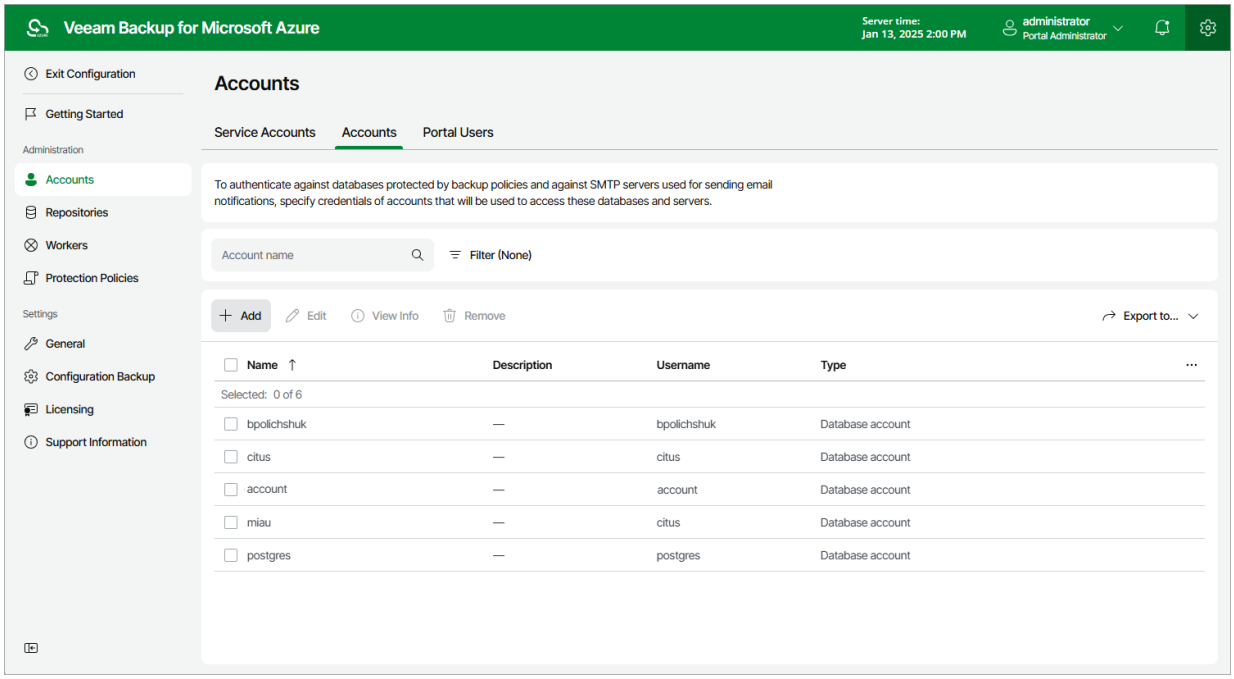
To add a new SMTP or database account, do the following:

1. Launch the Add Account wizard.
2. Specify an account name and description.
3. Specify general settings.
4. Finish working with the wizard.

# Step 1. Launch Add Account Wizard

To launch the **Add Account** wizard, do the following:

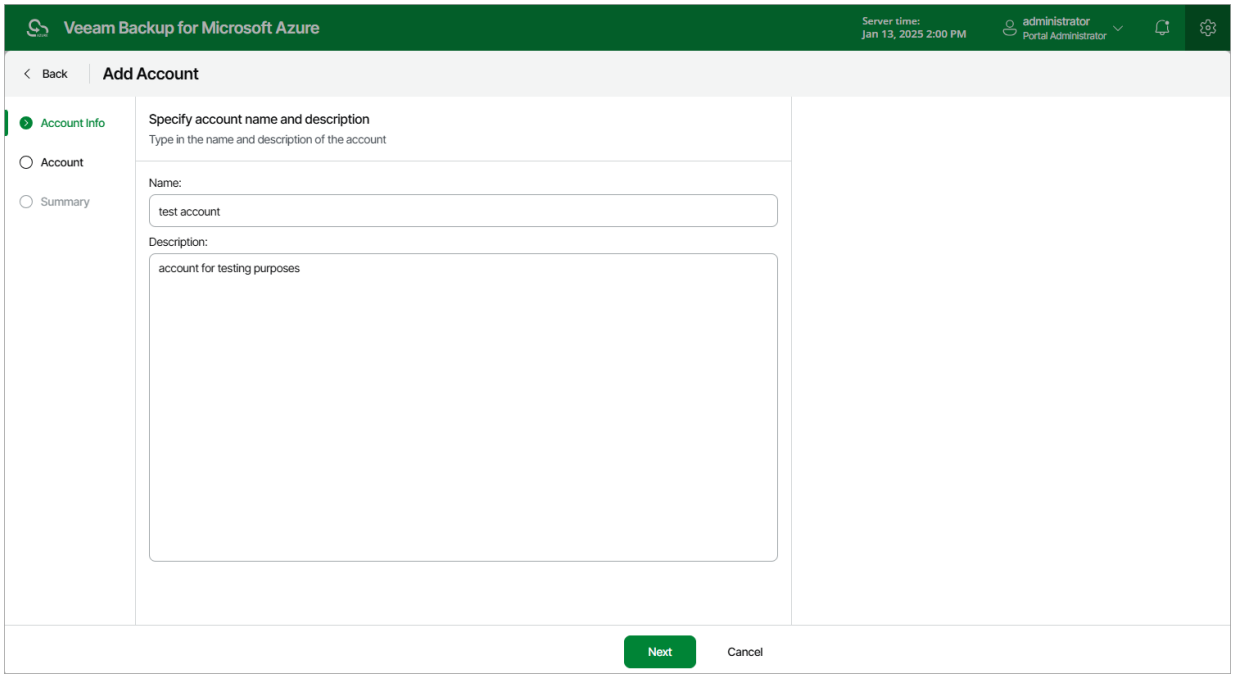
1. Switch to the **Configuration** page.
2. Navigate to **Accounts** > **Accounts**.
3. Click **Add**.



# Step 2. Specify Account Name and Description

At the **Account Info** step of the wizard, use the **Name** and **Description** fields to enter a name for the new account and to provide a description for future reference.

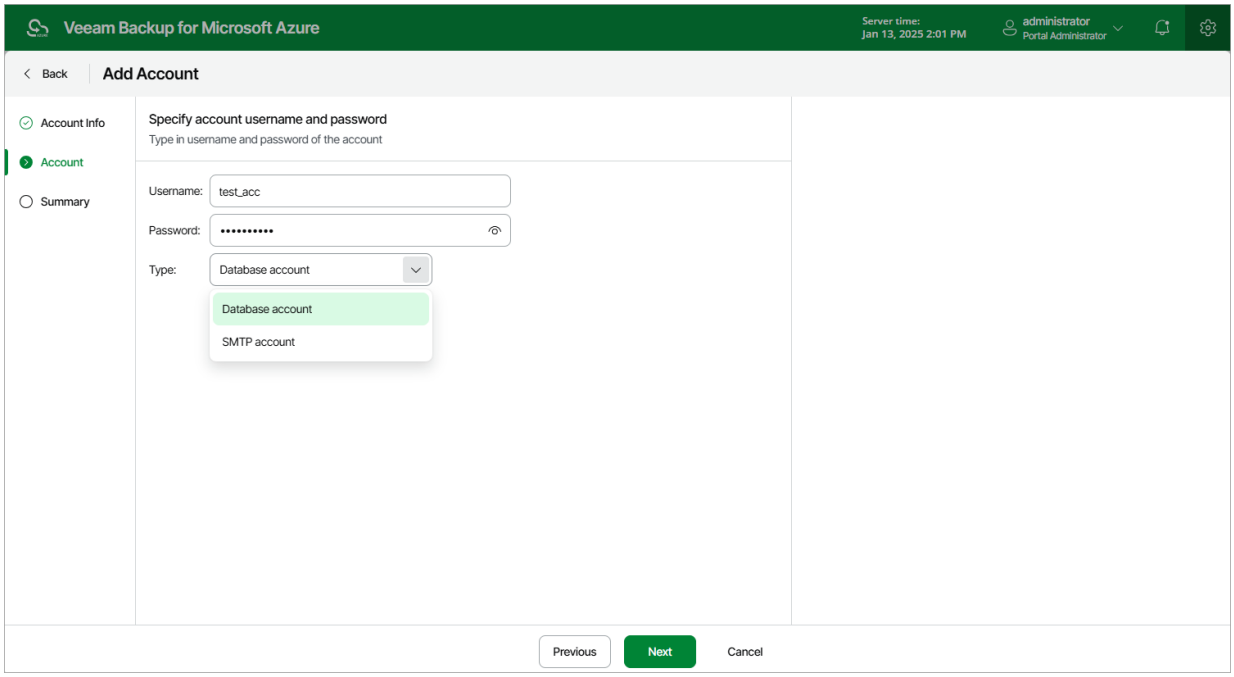
The maximum length of the account name is 32 characters. The following characters are supported: Latin letters, numeric characters, underscores and dashes. The following characters are not supported: \ / " ' [ ] : | < > + = ; , ? * @ & $.



# Step 3. Specify General Settings

At the **Account** step of the wizard, choose whether the account will be used to connect to SMTP servers or Azure databases, and specify credentials of a user account that will be used to authenticate against the servers or databases.

> **IMPORTANT**
>
> If you select the **Database account** option, consider the following:
>
> - The specified credentials must belong to a user account that has the following roles assigned:
>   - [Applies to SQL Server user accounts] The ##MS_DatabaseManager##, ##MS_LoginManager##, ##MS_DatabaseConnector## and ##MS_DefinitionReader## server-level roles, and the *db_owner* database-level role. For more information on server-level roles and database-level roles, see Microsoft Docs.
>     Consider that the *db_owner* database-level role is required for backup operations only.
>   - [Applies to Cosmos DB for PostgreSQL user accounts] Any role that has administrative permissions; it is recommended that you use an account that has the built-in *citus* role assigned. For more information on native PostgreSQL roles, see Microsoft Docs.
> - Microsoft Entra ID authentication is not supported.

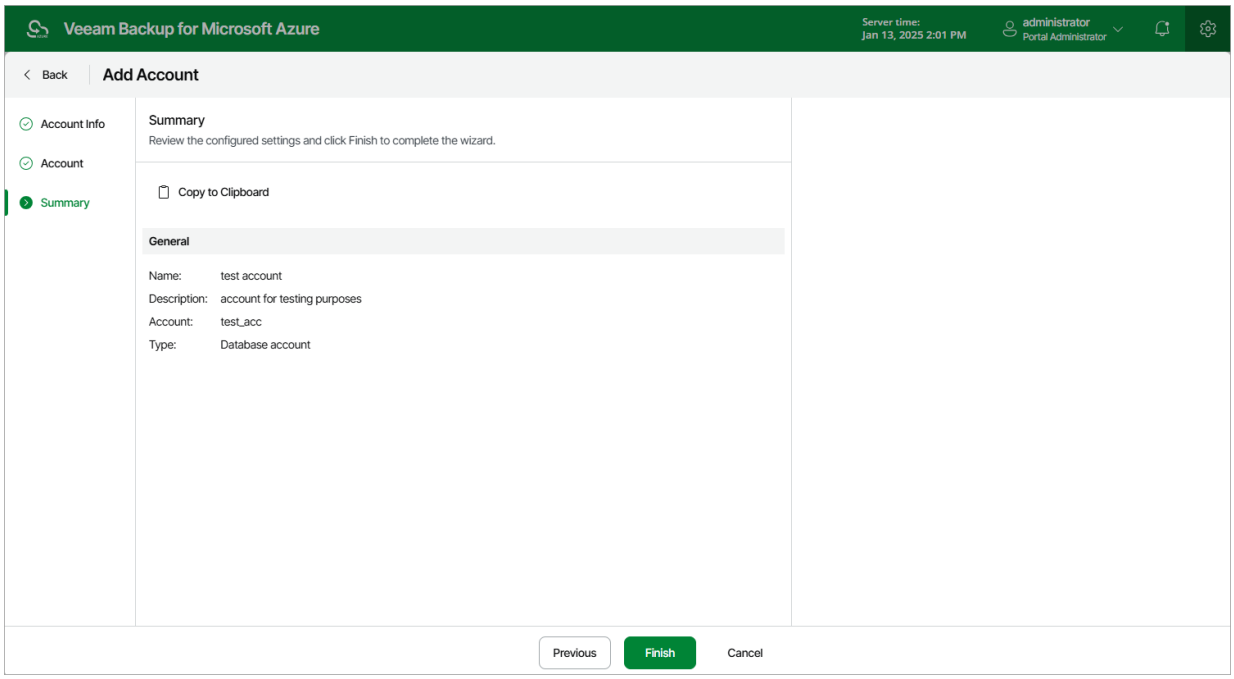


### Step 4. Finish Working with Wizard

At the **Summary** step of the wizard, review summary information and click **Finish** to confirm the changes.

**TIPS**

- After you add a database account, you will be able to specify this account while creating backup policies and restoring protected resources to allow Veeam Backup for Microsoft Azure to access source Azure SQL databases and Cosmos DB for PostgreSQL accounts, as well as to authenticate against target SQL Servers and Cosmos DB for PostgreSQL clusters. For more information, see sections Performing Backup and Performing Restore.
- After you add an SMTP account, you will be able to specify this account while configuring global notification settings to allow Veeam Backup for Microsoft Azure to send backup policy results and daily reports. For more information, see Configuring Global Notification Settings.

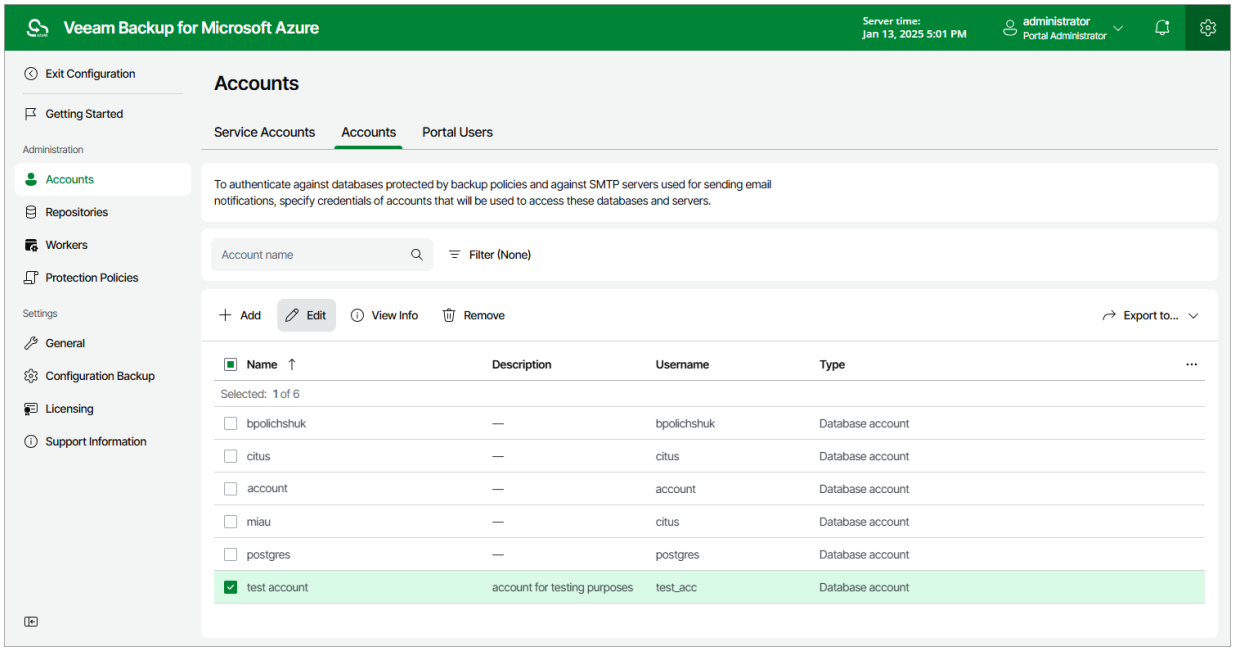



# Editing SMTP and Database Accounts

For each SMTP and database account added to the backup appliance, you can modify the settings of the account:

1. Switch to the **Configuration** page.
2. Navigate to **Accounts** > **Accounts**.
3. Select the account and click **Edit**.
4. Complete the **Edit Account** wizard.
   a. To specify a new name and description for the account, follow the instructions provided in section Adding SMTP and Database Accounts (step 2).
   b. To modify credentials of the account, follow the instructions provided in section Adding SMTP and Database Accounts (step 3).

c. At the **Summary** step of the wizard, review summary information and click **Finish** to confirm the changes.

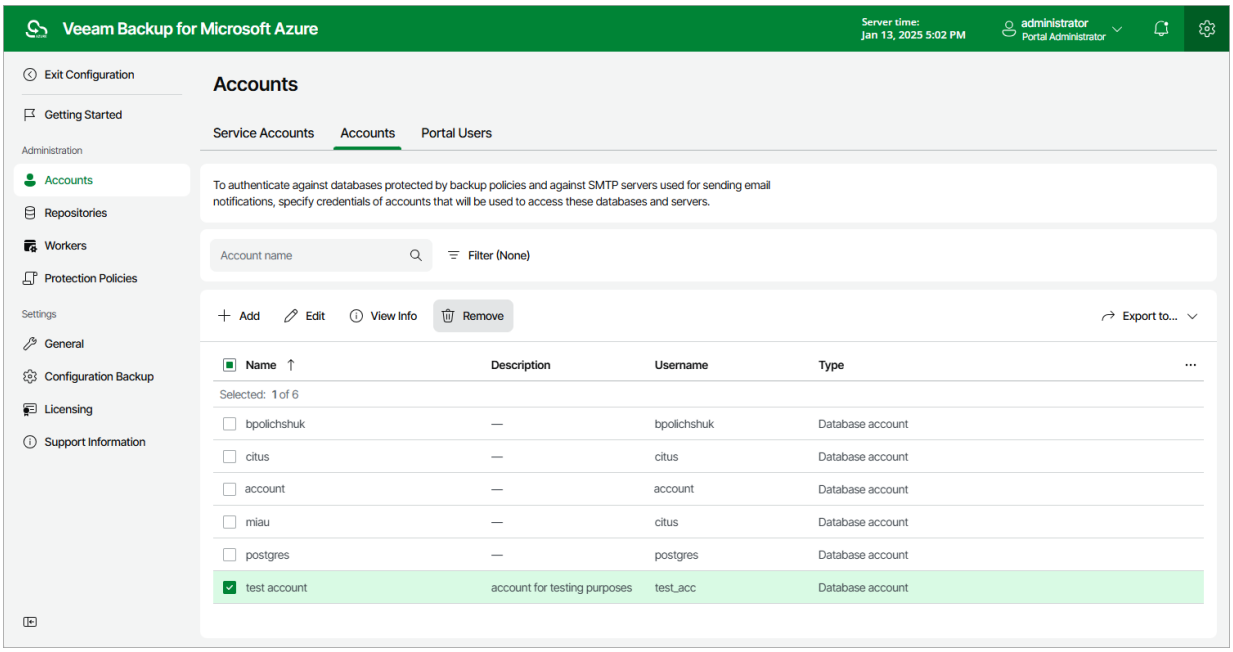



# Removing SMTP and Database Accounts

Veeam Backup for Microsoft Azure allows you to permanently remove an SMTP or database account from the configuration database if you no longer need it:

1. Switch to the **Configuration** page.
2. Navigate to **Accounts** > **Accounts**.
3. Select the account and click **Remove**.

> **IMPORTANT**
>
> You cannot remove a database account that is associated with any backup policy. Modify the settings of all the related policies to remove references to the account — and then try removing the account again.


Veeam Backup for Microsoft Azure
Server time:
Jan 13, 2025 5:02 PM
administrator
Portal Administrator
Exit Configuration
Getting Started
Administration
Accounts
Repositories
Workers
Protection Policies
Settings
General
Configuration Backup
Licensing
Support Information
Accounts
Service Accounts
Accounts
Portal Users
To authenticate against databases protected by backup policies and against SMTP servers used for sending email notifications, specify credentials of accounts that will be used to access these databases and servers.
Account name
Filter (None)
Add
Edit
View Info
Remove
Export to...
Name
Description
Username
Type
Selected: 1 of 6
bpolichshuk — bpolichshuk Database account
citus — citus Database account
account — account Database account
miau — citus Database account
postgres — postgres Database account
test account account for testing purposes test_acc Database account

# Managing Backup Repositories

Veeam Backup for Microsoft Azure uses blob containers as target locations for image-level backups of Azure VMs, backups of Azure SQL databases Cosmos DB for PostgreSQL accounts and Cosmos DB for MongoDB accounts, and backup copies of virtual network configurations. To store backups in blob containers, configure backup repositories. A repository is a specific folder created by Veeam Backup for Microsoft Azure in a blob container.

> **IMPORTANT**
>
> A backup repository must not be added to multiple backup appliances. Otherwise, retention sessions running on different backup appliances may corrupt backups stored in the repository, which may result in unpredictable data loss.

# Adding Backup Repositories Using Console

Depending on whether you want to store backups in a short-term storage or a long-term storage, you can configure repositories of the following access tiers:

- **Standard repositories**

  Use repositories of the Hot access tier to store data that you plan to access frequently, and repositories of the Cool access tier to store data that you plan to access infrequently. Backups stored in these repositories are shown under the **External Repository** node.

  To store backups in a standard repository, first add it to the backup infrastructure and then enable Azure VM image-level backups, Azure SQL backups, Cosmos DB for PostgreSQL backups, Cosmos DB for MongoDB backups to a repository or virtual network configuration backup copy in the backup policy settings. For more information, see sections Creating VM Backup Policies, Creating SQL Backup Policies, Creating Cosmos DB Backup Policies and Editing Virtual Network Configuration Backup Policy.

- **Archive repositories**

  Use repositories of the Archive access tier to store data that you plan to access less than once a year. Backups stored in these repositories are shown under the **External Repository (Archive)** node.

  To store backups in an archive repository, first add it to the backup infrastructure and then enable backup archiving for any backup policy that will store backups in this repository. For more information, see sections Creating VM Backup Policies, Creating SQL Backup Policies and Creating Cosmos DB Backup Policies.

  To learn how backup archiving works, see Enabling Backup Archiving.

> **IMPORTANT**
>
> Note that you can perform a limited scope of operations with archive repositories from the Veeam Backup & Replication console:
>
> - You cannot edit and rescan archive repositories.
> - You can only restore entire Azure VMs and entire Azure SQL databases from backups stored in archive repositories. However, you can perform disk and file-level restore operations from these backups using the backup appliance Web UI. For more information, see sections Performing Disk Restore or Performing File-Level Recovery.

For more information on access tiers for blob data, see Microsoft Docs.

## How to Add Backup Repositories

After you add a backup appliance to the backup infrastructure, you can configure repositories that will be used to store backups. To do that, use either of the following options:

- Create new repositories.
- Add existing repositories to the backup infrastructure if you have already configured them on the backup appliance.

## Creating New Repositories

To add a new repository, do the following:

1. Launch the Add External Repository wizard.

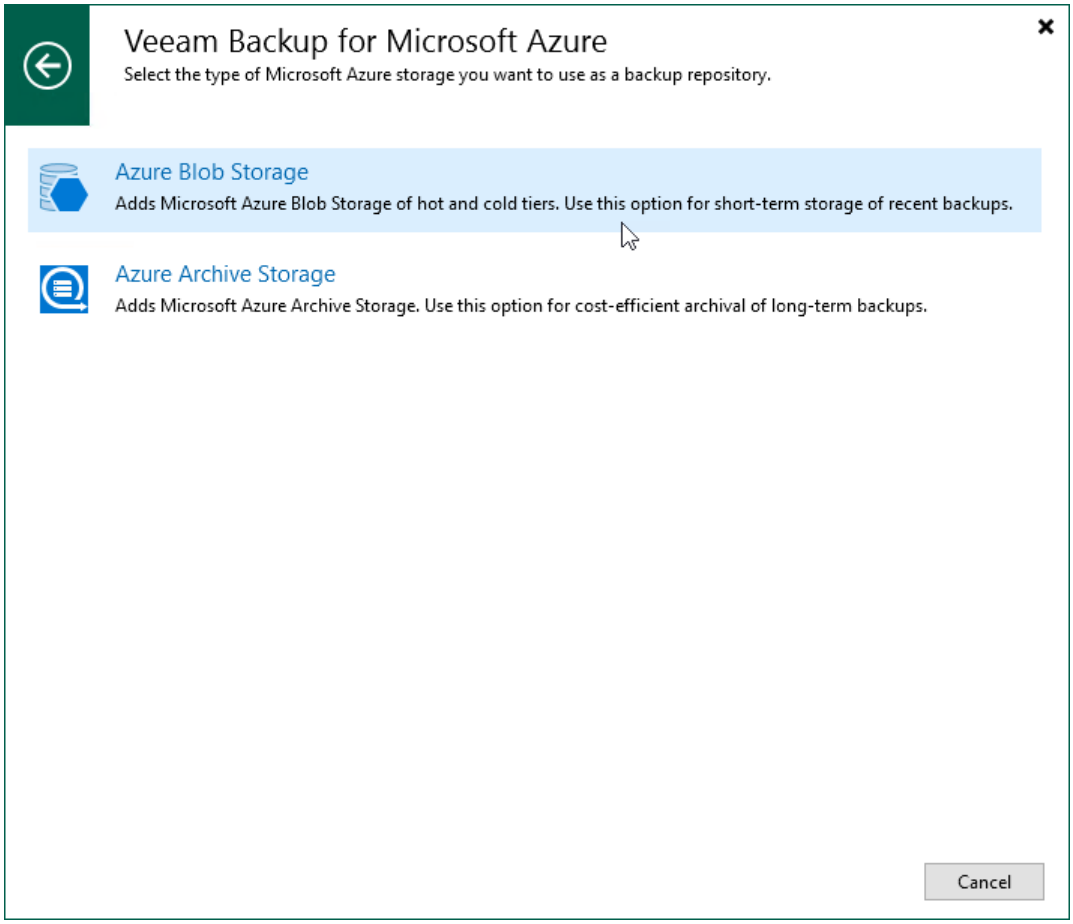
2. Specify an appliance, and provide repository name and description.
3. Configure repository settings.
4. Specify a service account to access a blob container.
5. Select a blob container.
6. Enable data encryption.
7. Wait for the repository to be added to the backup infrastructure.
8. Finish working with the wizard.

## Step 1. Launch Add External Repository Wizard

To launch the **Add External Repository** wizard, do the following:

1. In the Veeam Backup & Replication console, open the **Backup Infrastructure** view.
2. Navigate to **External Repositories** and click **Add Repository** on the ribbon.

   Alternatively, you can right-click the **External Repositories** node and select **Add**.
3. In the **Add External Repository** window:
   a. [Applies only if you have several cloud plug-ins installed] Click **Veeam Backup for Microsoft Azure**.
   b. Choose whether you want to create a standard or an archive repository:
      - Select the **Azure Blob Storage** option if you want to create a repository of the Hot or Cool access tier. In this case, the repository will be assigned the access tier selected in Microsoft Azure for the storage account that you will specify at step 3 of the wizard.
      - Select the **Azure Archive Storage** option if you want to create a repository of the Archive access tier. Consider that to restore data from an archive repository, you first need to retrieve data from it. To learn how to retrieve data, see Retrieving Data from Archive.



## Step 2. Specify Repository Details

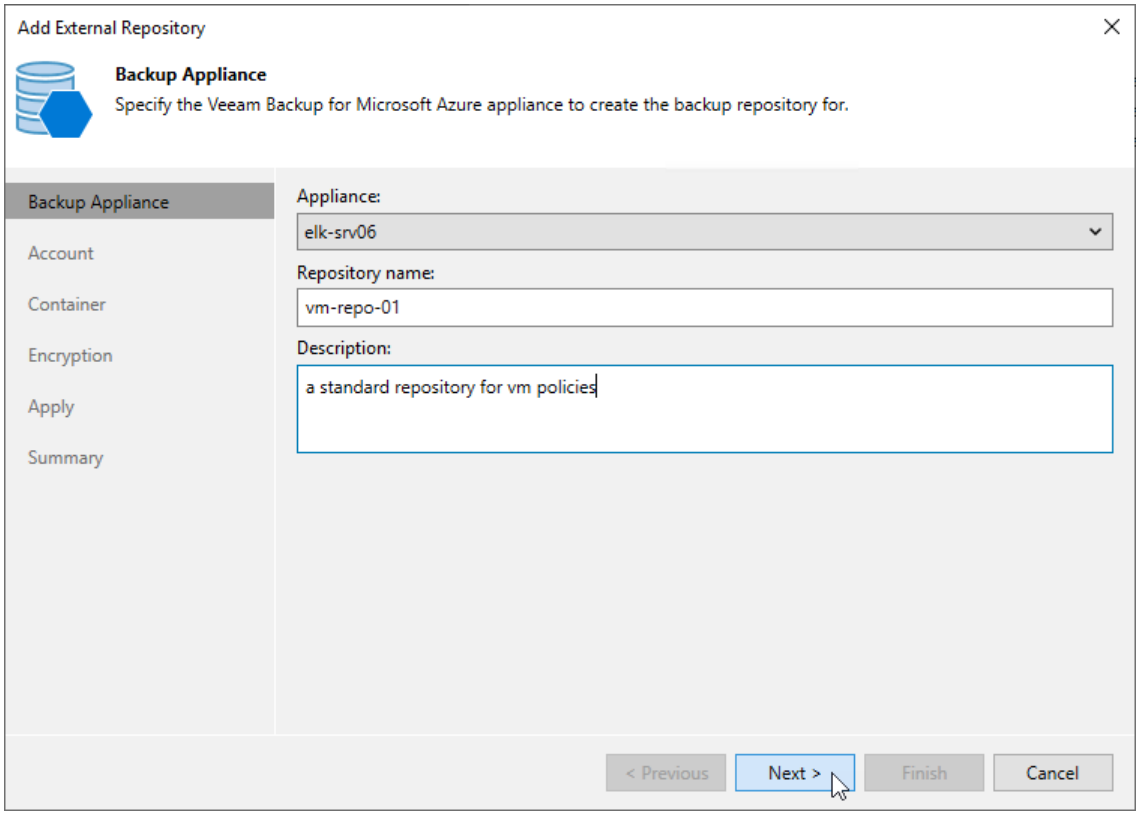
At the **Backup Appliance** step of the wizard, do the following:

1. From the **Appliance** drop-down list, select a backup appliance that will manage the repository.

   For an appliance to be displayed in the **Appliance** drop-down list, it must be added to the backup infrastructure as described in section Adding Appliances.

2. Use the **Repository name** and **Description** fields to enter a name for the new repository and to provide a description for future reference. The maximum length of the name is 127 characters; the following characters are not supported: \ / " ' [ ] : | < > + = ; , ? * @ & _ .

   Veeam Backup & Replication will create a folder with the specified name in the blob container that you will specify at step 5 of the wizard. This folder will be used to store backed-up data.



## Step 3. Configure Repository Settings

At the **Account** step of the wizard, do the following:

1. From the **Credentials** drop-down list, select credentials of a Microsoft Azure storage account in which the repository will reside. Veeam Backup & Replication will use these credentials to access the repository. For more information on supported types of storage accounts, see the Veeam Backup & Replication User Guide, section Cloud Credentials Manager.

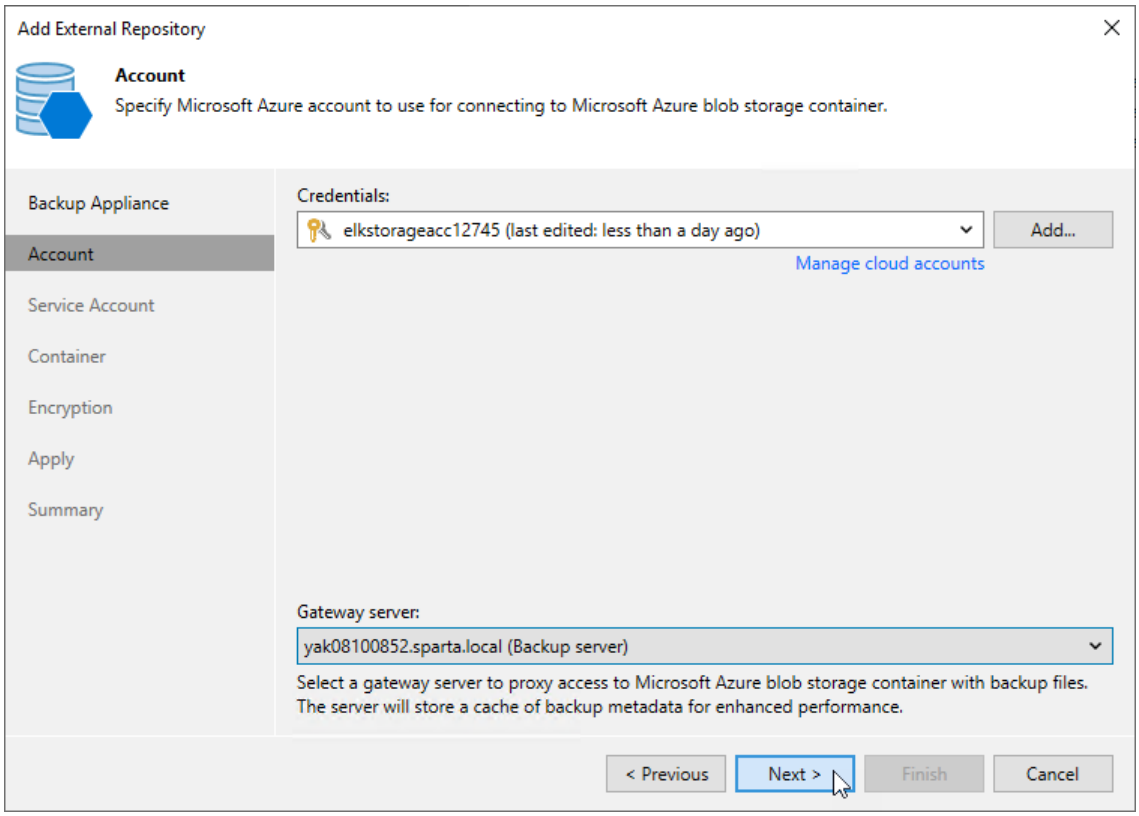
> **IMPORTANT**
>
> Note that the **Enable storage account key access** option must be enabled in the storage account settings for Shared Key authorization. For more information, see Microsoft Docs.

   For credentials to be displayed in the list of available credentials, they must be added to the Cloud Credentials Manager as described in the Veeam Backup & Replication User Guide, section Microsoft Azure Storage Accounts (Shared Key). If you have not added the necessary credentials to the Cloud Credentials Manager beforehand, you can do it without closing the **Add External Repository** wizard. To do that, click either the **Manage cloud accounts** link or the **Add** button, and specify the storage account name and access key generated for the account in the **Credentials** window.

> **NOTE**
>
> If you want to create the repository with immutability enabled, make sure that either version-level immutability support or blob versioning is enabled on the specified storage account, and the default time-based retention policy is not configured for the account. For more information, see Immutability.

2. [Applies only if you choose to create a standard repository] From the **Gateway server** drop-down list, select a gateway server that will be used to access the repository.

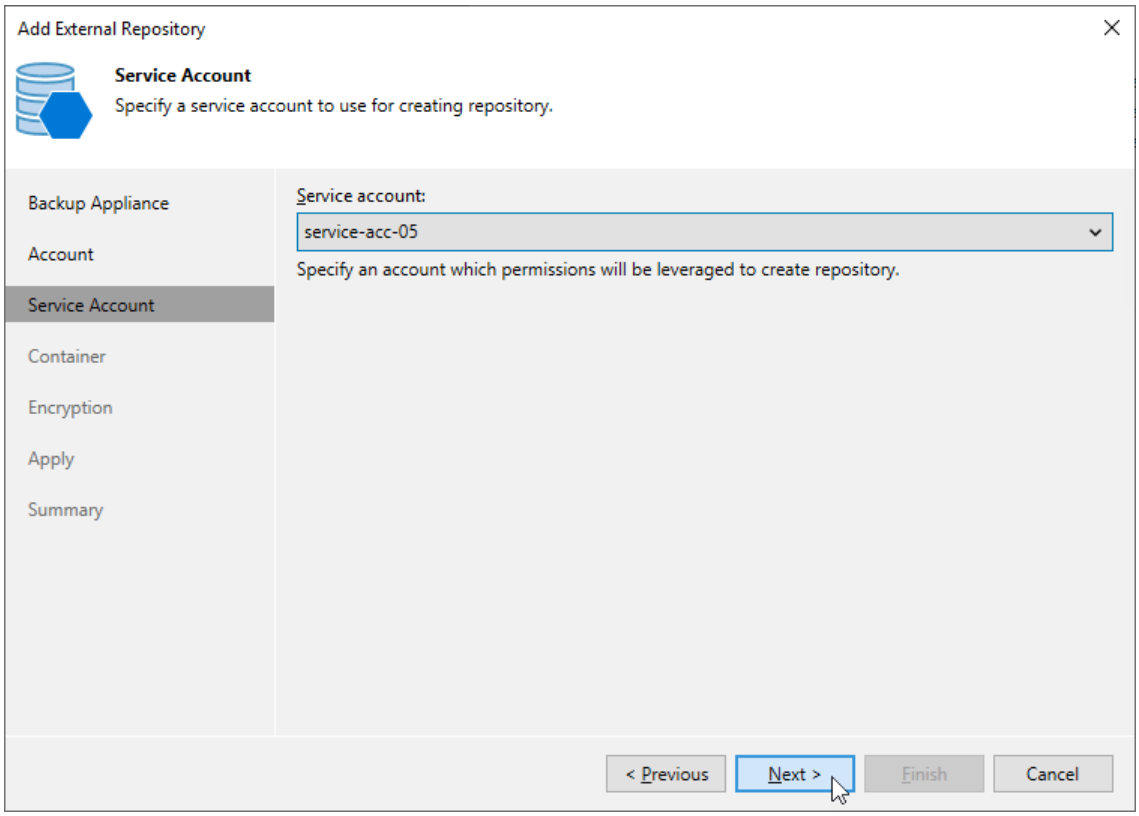
   For a server to be displayed in the **Gateway server** list, it must be added to the backup infrastructure. For more information on gateway servers, see Gateway Servers.



# Step 4. Specify Service Account

At the **Service Account** step of the wizard, specify a service account whose permissions Veeam Backup for Microsoft Azure will use to access the Microsoft Azure storage account specified at step 3 of the wizard.

For a service account to be displayed in the **Service account** list, it must be added to the backup appliance as described in section Adding Service Accounts.



## Step 5. Specify Blob Container

At the **Container** step of the wizard, do the following:

1. Choose whether you want to use an existing blob container or to create a new one as the target location for image-level backups of Azure VMs, backups of Azure SQL databases, backups of Cosmos DB for PostgreSQL and Cosmos DB for MongoDB accounts, and backup copies of virtual network configurations:
   - To specify an existing container, select it from the **Container** drop-down list.

     For a container to be displayed in list of available containers, it must be created for the selected storage account in Microsoft Azure as described in Microsoft Docs.
   - To create a new container, click **Add**. In the **New Container** window, enter a name for the container. Veeam Backup & Replication will automatically create a container in the same region where the backup appliance resides.

> **NOTE**
>
> If you want to create the repository with immutability enabled, consider the following:
>
> - Version-level immutability support must be enabled for the specified blob container. To learn how to enable version-level immutability support for blob containers, see Microsoft Docs.
> - If you choose to create a new container, note that Veeam Backup & Replication can create blob containers with version-level immutability support enabled only in storage accounts with version-level immutability support enabled.

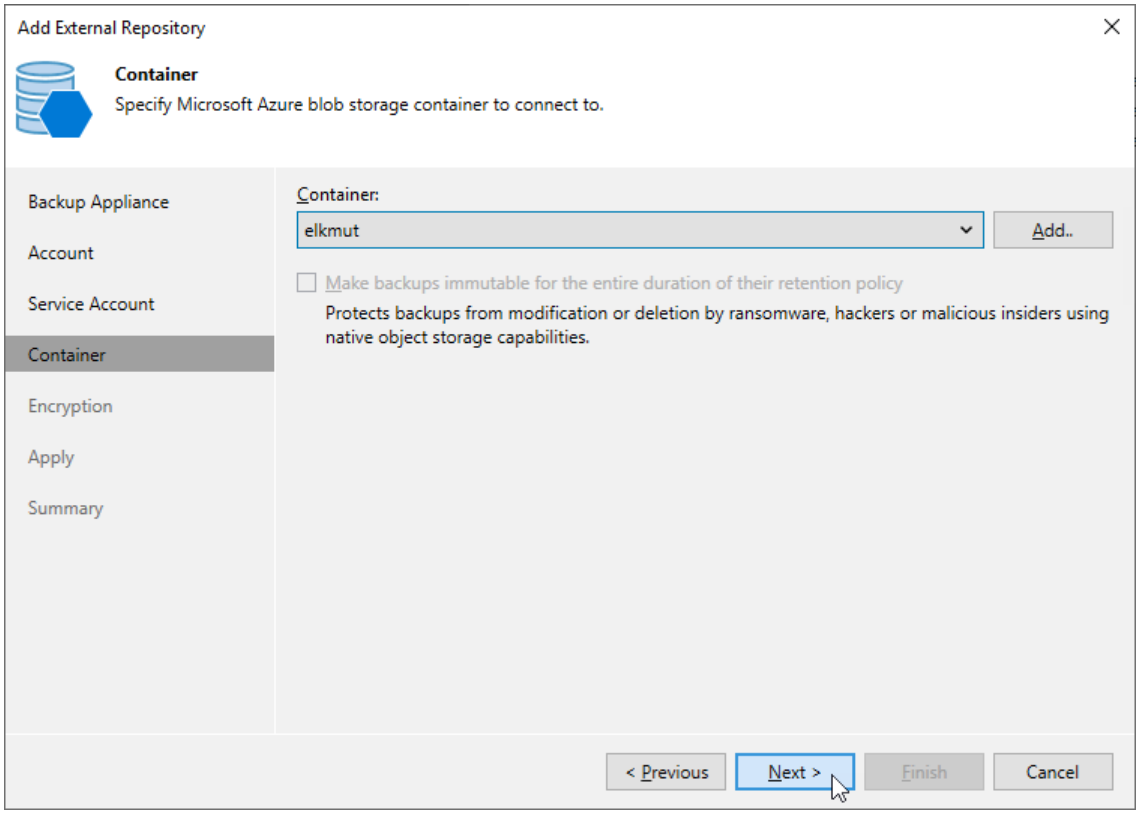
2. If you want to protect backups stored in the repository from being lost as a result of malware, ransomware or any other malicious actions, you can create the repository with immutability settings enabled. To do that, you must select a Microsoft Azure storage account with version-level immutability support or blob versioning enabled at step 3 of the wizard and a blob container with version-level immutability support enabled.

   If the storage account and blob container meet the immutability requirements, the **Make backups immutable for the entire duration of their retention policy** check box will be automatically selected. For more information, see Immutability.

**IMPORTANT**

Consider the following:

- You cannot create standard repositories with the disabled immutability settings in blob containers with version-level immutability support enabled.
- You cannot edit the configured immutability settings for the repository.



## Step 6. Enable Data Encryption

At the **Encryption** step of the wizard, choose whether you want to encrypt backups stored in the created repository.

> **IMPORTANT**
>
> After you create a repository with encryption enabled, you can no longer disable encryption for this repository. However, you will be able to change encryption settings as described in section Editing Backup Repository Settings.

If you select the **Enable backup file encryption** check box, also choose whether you want to use a password or an Azure Key Vault cryptographic key to encrypt the backed-up data:

- To encrypt data using a cryptographic key, select the **Perform Azure encryption with the following key** option and do the following:
  a. From the **Subscription** drop-down list, select an Azure subscription to which the Key Vault belongs.

     For a subscription to be displayed in the list of available subscriptions, it must be created in Microsoft Azure and associated with the Microsoft Entra tenant to which the service account specified at step 4 of the wizard belongs.

  b. From the **Key vault** drop-down list, select the Azure Key Vault where the encryption key is stored.

     For an Azure Key Vault to be displayed in the list of available vaults, it must be created in Microsoft Azure as described in Microsoft Docs.

> **IMPORTANT**
>
> To list Azure Key Vaults and cryptographic keys and further to decrypt backups stored in the repository, Veeam Backup & Replication uses permissions of the service account specified at step 4 of the wizard. For more information on the required permissions, see Plug-In Permissions.

  c. From the **Encryption key** drop-down list, select the necessary cryptographic key.

     For a cryptographic key to be displayed in the list of available encryption keys, it must be created in Microsoft Azure as described in Microsoft Docs.

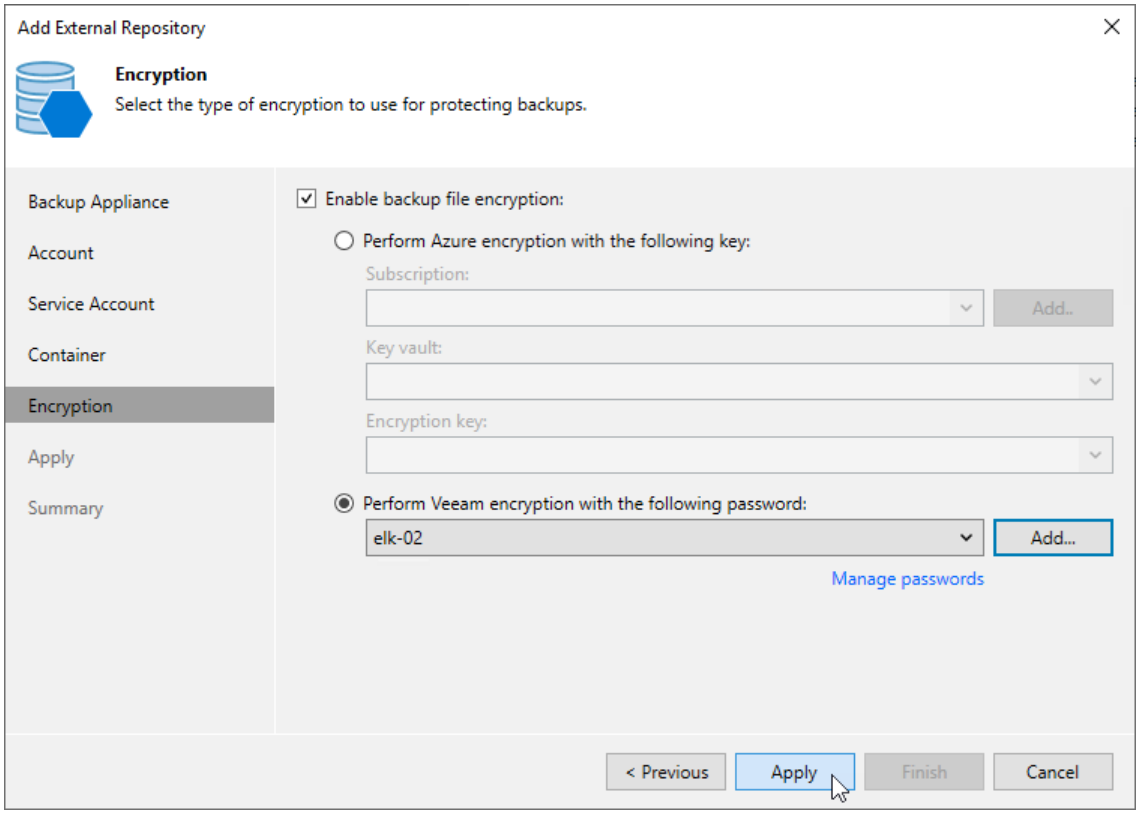
- To encrypt data using a password, select the **Perform Veeam encryption with the following password** option and choose the necessary password from the drop-down list.

  For a password to be displayed in the list of available passwords, it must be added to the Veeam Backup & Replication as described in the Veeam Backup & Replication User Guide, section Creating Passwords. If you have not added the necessary password beforehand, you can do it without closing the **Add External Repository** wizard. To do that, click either the **Manage passwords** link or the **Add** button, and specify the password and hint in the **Password** window.

**IMPORTANT**

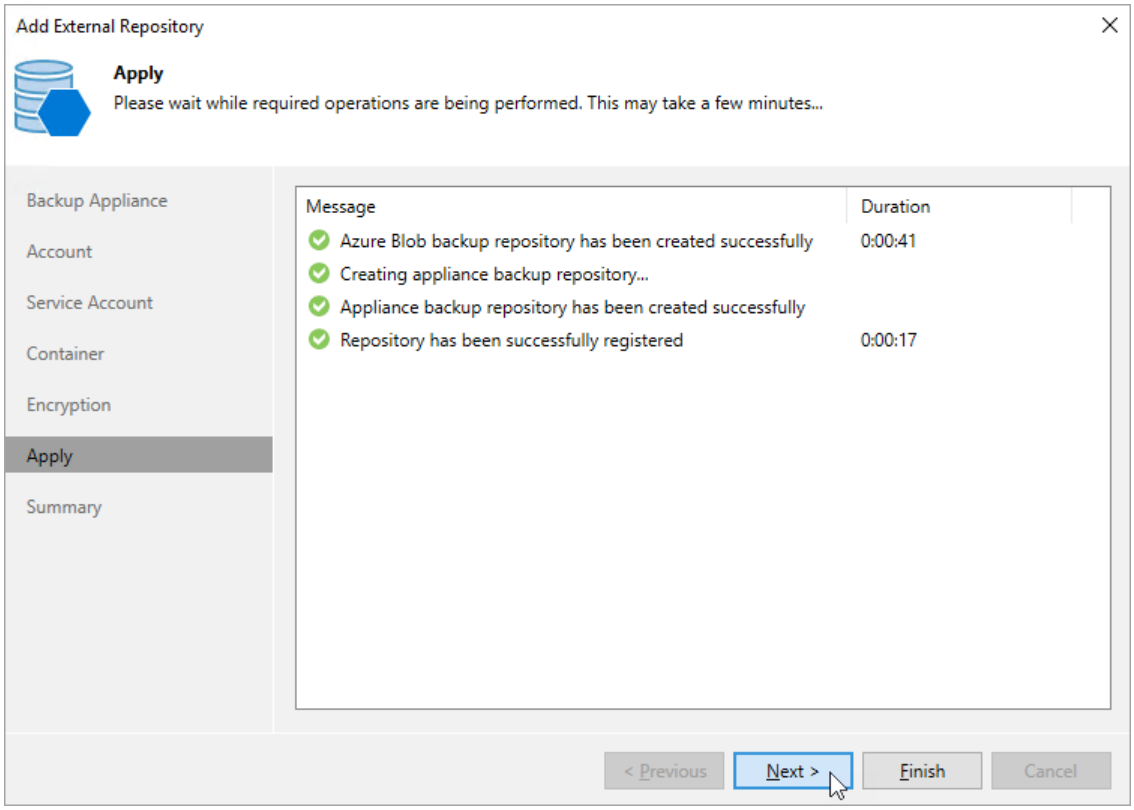
If you want to use an Azure Key Vault cryptographic key for encryption at the repository level, consider the following:

- Do not disable cryptographic keys specified in the repository settings. Otherwise, Veeam Backup for Microsoft Azure will not be able to encrypt data, and backup policies that use the encrypted repository for storing backups will fail.
- Do not delete cryptographic keys specified in the repository settings. Otherwise, Veeam Backup for Microsoft Azure will not be able to decrypt data stored in the repository.



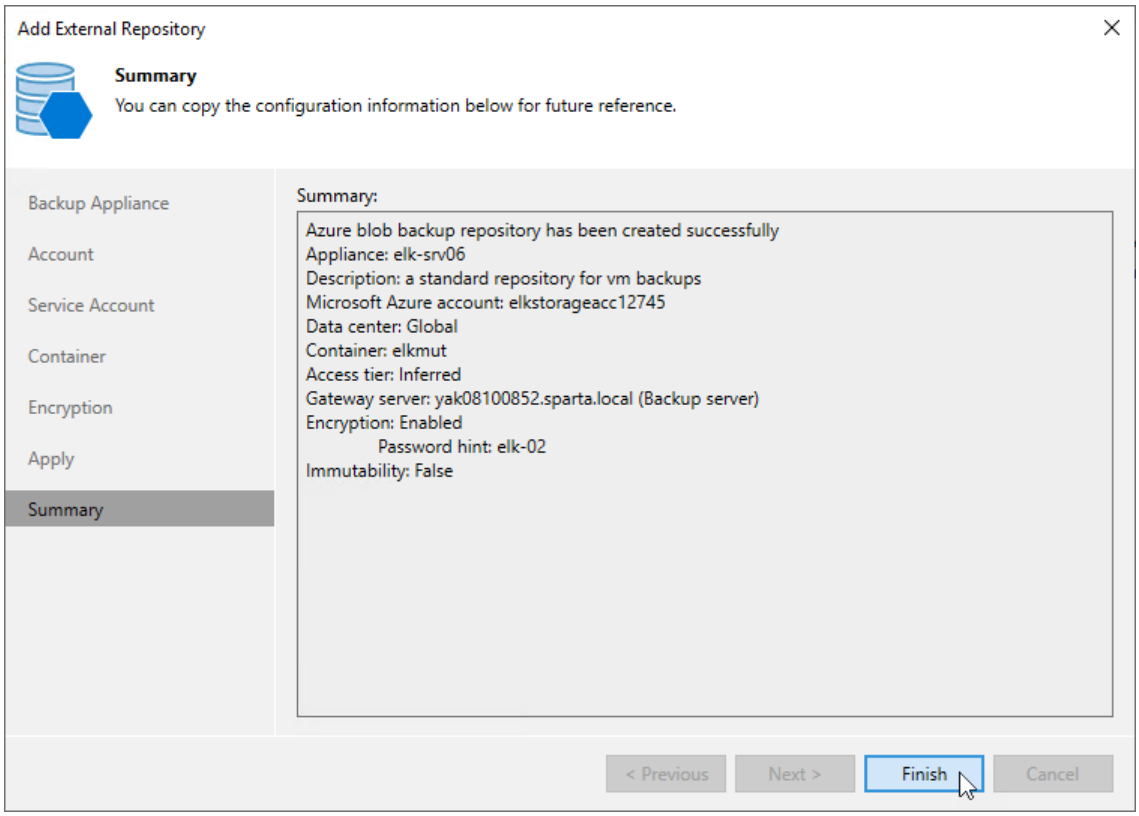
## Step 7. Track Progress

Veeam Backup & Replication will display the results of every step performed while creating the repository. At the **Apply** step of the wizard, wait for the process to complete and click **Next**.



## Step 8. Finish Working with Wizard

At the **Summary** step of the wizard, review summary information and click **Finish**.




# Connecting to Existing Repositories

When you connect to a backup appliance, all repositories that have already been configured on the appliance are automatically added to the backup infrastructure.

If an existing repository is not displayed under the **External Repositories** node or if you have recently configured a new repository on the appliance that is already connected to the backup server, do the following:

1. In the Veeam Backup & Replication console, open the **Backup Infrastructure** view.
2. Navigate to **Managed Servers**.
3. Select a backup appliance that manages the necessary repository and click **Edit Appliance** on the ribbon.

   Alternatively, you can right-click the backup appliance and select **Properties**.
4. In the **Edit Veeam Backup for Microsoft Azure Appliance** wizard, do the following:
   a. Navigate to the **Repositories** step of the wizard and complete the step as described in section Adding Appliances (step 8).
   b. Complete the **Edit Veeam Backup for Microsoft Azure Appliance** wizard as described in section Adding Appliances (steps 9-10).

Open the **Backup Infrastructure** view to verify that the repository is displayed under the **External Repositories** node.

NOTE

If you do not specify credentials of the Microsoft Azure storage account for a standard repository, you will only be able to use the Veeam Backup & Replication console to perform entire VM restore and SQL database restore from backups stored in this repository. Moreover, information on the repository displayed in the **Backup Infrastructure** view under the **External Repositories** node will not include statistics on the amount of storage space that is currently consumed by restore points created by Veeam Backup for Microsoft Azure.

# Adding Backup Repositories Using Web UI

> **IMPORTANT**
>
> If your backup appliance is managed by a Veeam Backup & Replication server and you add a new backup repository using the Veeam Backup for Microsoft Azure Web UI, Veeam Backup for Microsoft Azure will not propagate these settings to the Veeam Backup & Replication server automatically. To discover new backup repositories created in the backup appliance, follow the instructions provided in section Connecting to Existing Repositories.

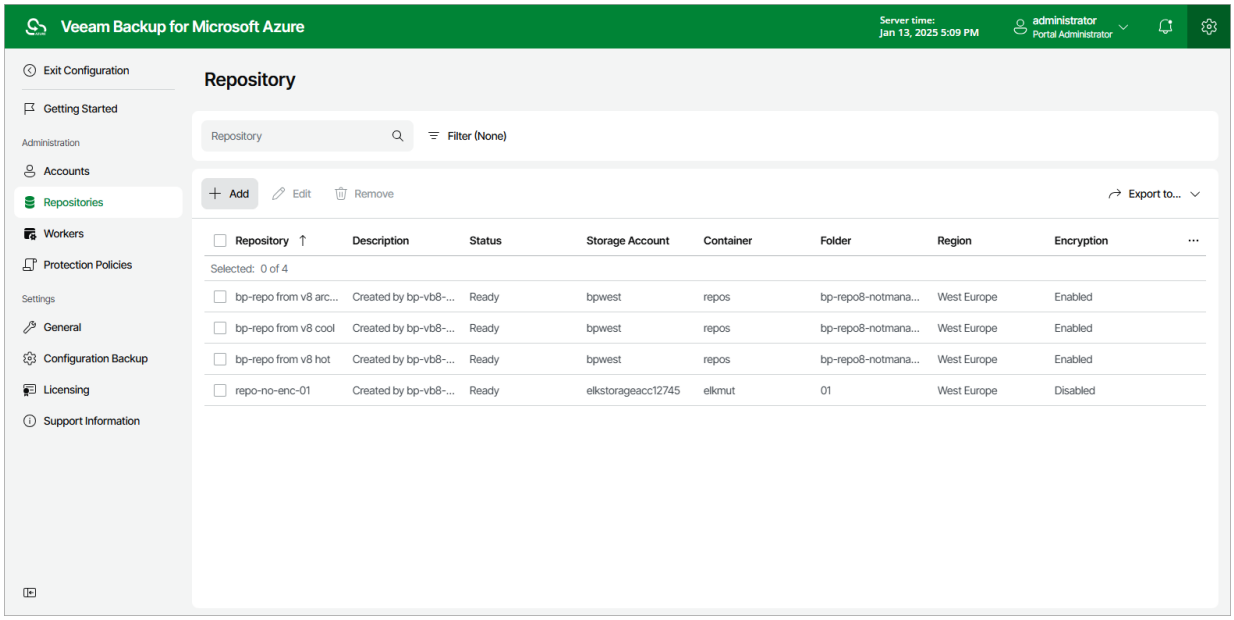
To add a new backup repository, do the following:

1. Launch the Add Repository wizard.
2. Specify a repository name and description.
3. Configure repository settings.
4. Enable encryption for the backup repository.
5. Configure load options for the backup repository.
6. Finish working with the wizard.

# Step 1. Launch Add Repository Wizard

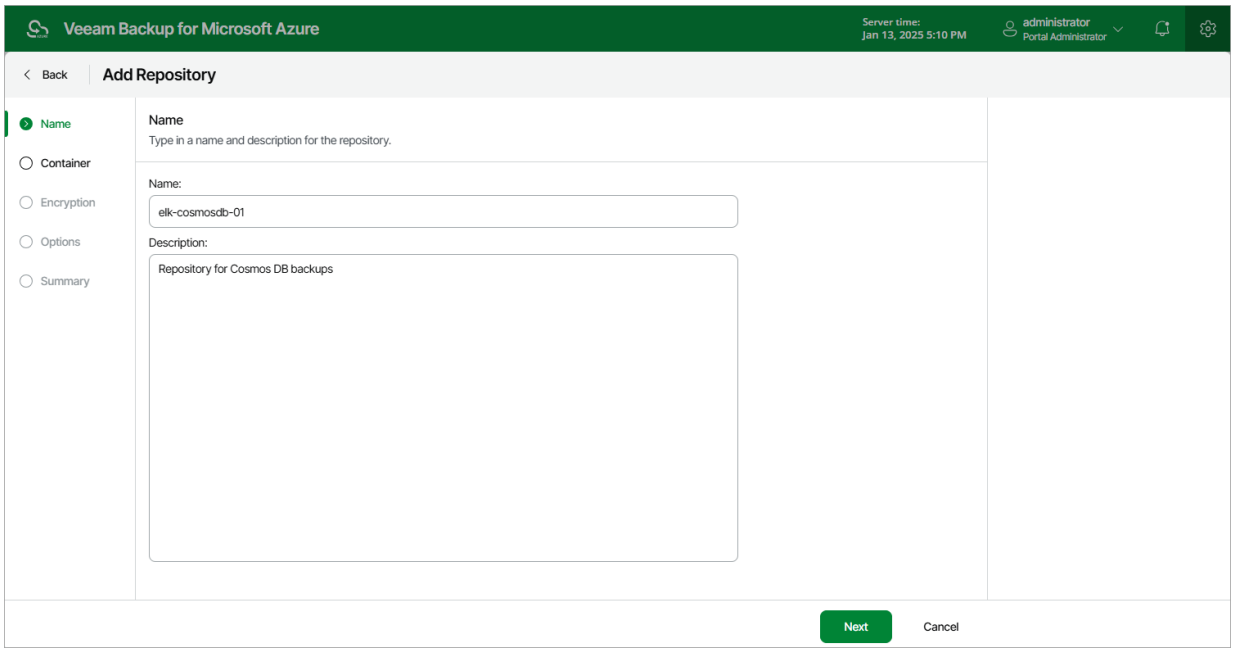
To launch the **Add Repository** wizard, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **Repositories**.
3. Click **Add**.



# Step 2. Specify Repository Name

At the **Name** step of the wizard, use the **Name** and **Description** fields to enter a name for the new backup repository and to provide a description for future reference. The maximum length of the name is 125 characters. The following characters are not supported: * : / \ ? " < > | ! @ # $ % ^ & .



# Step 3. Configure Repository Settings

At the **Container** step of the wizard, select a service account that will be used to access the created repository, specify a location where the repository will be created, and configure immutability settings for the repository.

# Specifying Service Account

In the **Account** section, select a service account whose permissions Veeam Backup for Microsoft Azure will use to create the new repository in the target Azure blob container and further to access the repository when performing data protection and recovery tasks. The specified service account must be assigned permissions listed in section Repository Permissions.

For an account to be displayed in the **Account** list, it must be added to Veeam Backup for Microsoft Azure and assigned the *Repository Management* role as described in section Adding Service Accounts. If you have not added the necessary account to Veeam Backup for Microsoft Azure beforehand, you can do it without closing the **Add Repository** wizard. To do that, click **Add** and complete the **Add Account** wizard.

# Choosing Repository Location

In the **Location** section, do the following:

1. Specify a storage account where the target blob container resides. To do that, click **Specify storage account** and select the necessary storage account in the **Select storage account** window. Veeam Backup for Microsoft Azure will use the account to access the backup repository.

   For a storage account to be displayed in the list of available accounts, it must be created in the Microsoft Azure portal as described in Microsoft Docs.

> **IMPORTANT**
>
> Consider the following:
>
> - Veeam Backup for Microsoft Azure does not support creation of backup repositories in storage accounts with the blob soft delete option enabled.
> - Due to Microsoft Azure limitations, Veeam Backup for Microsoft Azure does not support creation of archive repositories in storage accounts with the Zone-redundant storage (ZRS), Geo-zone-redundant storage (GZRS) or Read-access geo-zone-redundant storage (RA-GZRS) redundancy option enabled. For more information, see Microsoft Docs.

2. Choose a blob container that will be used as a target location for backups of Azure resources. To do that, click **Not specified** and select the necessary blob container in the **Select container** window.

   For a container to be displayed in the **Container** list, it must be created for the selected storage account in the Microsoft Azure portal as described in Microsoft Docs.

3. Choose whether you want to use an existing folder inside the selected blob container or to create a new one to group backup files stored in the container.

   - To create a new folder, select the **Create new folder** option and specify a name for the folder. The maximum length of the name is 256 characters; the slash (/) and backslash (\) characters are not supported.

- To use an existing folder, select the **Use existing folder** option and click **Select folder**. In the **Select folder** window, select the necessary folder and click **Apply**.

  For a folder to be displayed in the **Folder** list, it must be created by any backup appliance as a repository (either existing or already removed from the backup infrastructure) in the selected blob container.

**IMPORTANT**

If you select an existing folder for storing backup files, consider the following:

- The created backup repository will have the storage tier that has been specified when creating the folder. You cannot change the storage tier for the repository.
- If encryption is enabled for the selected folder at the repository level, you must provide a password or an encryption key for this folder at step 4 of the wizard.
- If the selected folder already contains backups created by the Veeam backup service, Veeam Backup for Microsoft Azure will import the backup data to the configuration database. You can use this data to perform all disaster recovery operations described in section Performing Restore.

  By default, Veeam Backup for Microsoft Azure applies retention settings saved in the backup metadata to the imported backups. However, if the selected folder contains backups of resources that you plan to protect by a backup policy with the created repository specified as a backup target, Veeam Backup for Microsoft Azure will rewrite the saved retention settings and will apply to the imported backups new retention settings configured for that backup policy.

4. [Applies only if you have selected the **Create new folder** option] In the **Storage class** section, choose whether you want to specify a tier for the repository manually, or to instruct Veeam Backup for Microsoft Azure to create 3 separate repositories of the Hot, Cool and Archive access tiers automatically.

   If you select the **Choose your tier** option, you must specify the access tier that will be used to manage the costs of storing backed-up data.

   - Select the **Hot** tier if you plan to access the backed-up data frequently.
   - Select the **Cool** tier if you plan to store the backed-up data for at least 30 days and do not plan to access it frequently.
   - Select the **Archive** tier if you plan to store the backed-up data for at least 180 days.

     Note that to restore data from an archive, you will first need to retrieve data from it. To learn how to retrieve the data, see Retrieving Data from Archive.
   - Select the **Inferred** tier if you plan to use the same access tier as specified for the storage account where the selected repository resides.

   For more information on access tiers for blob data, see Microsoft Docs.

**IMPORTANT**

If you select the **Archive** tier for a backup repository, consider the following:

- Veeam Backup for Microsoft Azure supports only the following storage account data redundancy options: locally redundant storage (LRS), geo-redundant storage (GRS), read-access geo-redundant storage (RA-GRS).
- The archive tier is not available in specific Azure regions. For more information, see Microsoft Docs.

# Reviewing Immutability Settings

Veeam Backup for Microsoft Azure allows you to protect backups stored in the repository from being lost as a result of malware, ransomware or any other malicious actions. To do that, you can create repositories with immutability enabled. For more information, see Immutability.

If you plan to enable immutability settings for the created repository, make sure that:

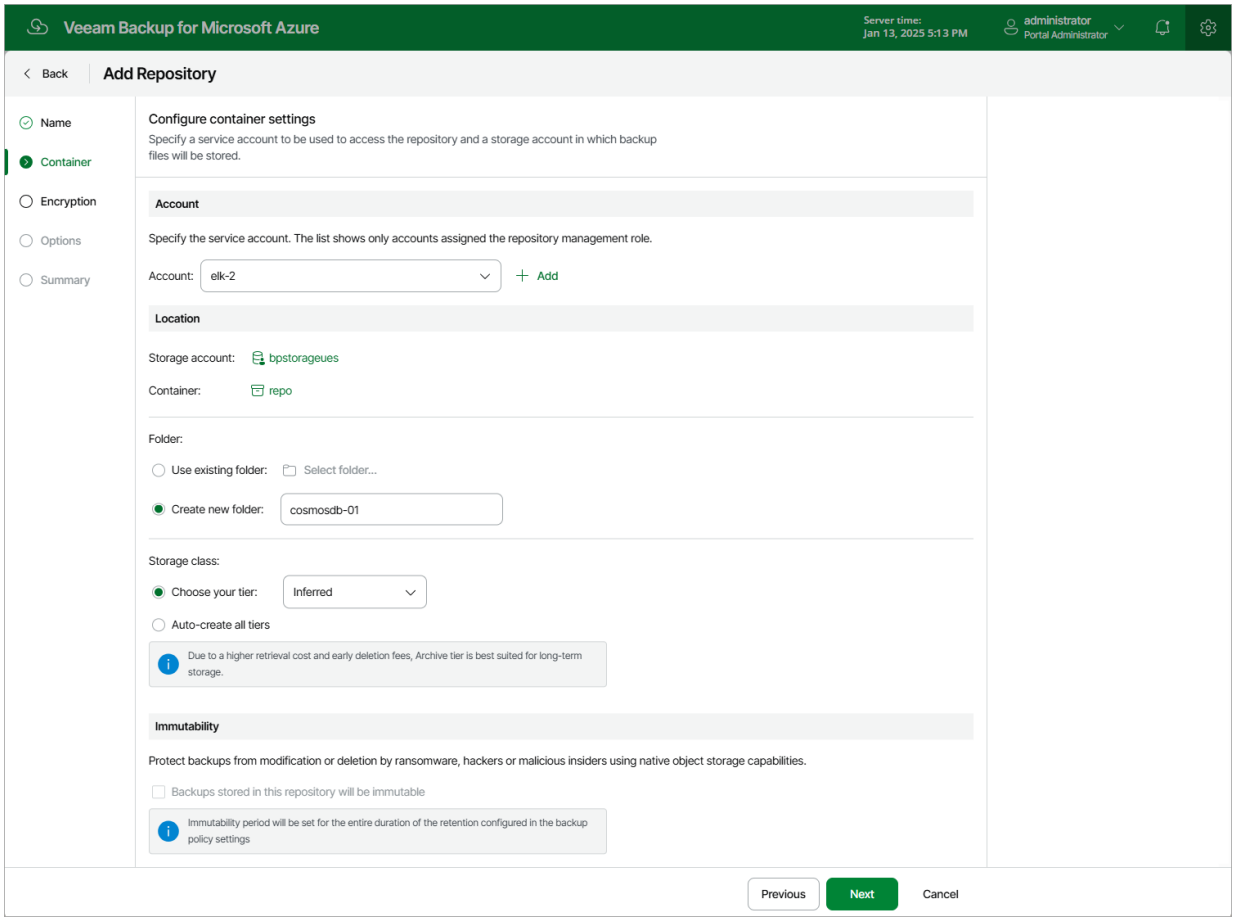
- Either version-level immutability support or blob versioning is enabled for the specified storage account, and the default time-based retention policy is not configured for the account.
- Version-level immutability support is enabled for the specified blob container.

> **NOTE**
>
> For security reasons, it is recommended that you have a dedicated Azure subscription that will manage Azure storage accounts in which immutable backup files will be stored. To do that, specify a service account associated with the necessary subscription as described in section Specifying Service Account, and then choose an Azure storage account and Azure blob container that meet the immutability requirements.

As soon as you select a blob container, Veeam Backup for Microsoft Azure verifies the settings configured for the storage account and blob container, and displays the following information in the **Immutability** section:

- If the storage account and the container meet the immutability requirements, Veeam Backup for Microsoft Azure automatically selects the **Backups stored in this repository will be immutable** check box. In this case, the repository will be created with immutability enabled.

- If the storage account or the container does not meet the immutability requirements, Veeam Backup for Microsoft Azure automatically clears the **Backups stored in this repository will be immutable** check box. In this case, the repository will be created with immutability disabled.




# Repository Ownership Alert

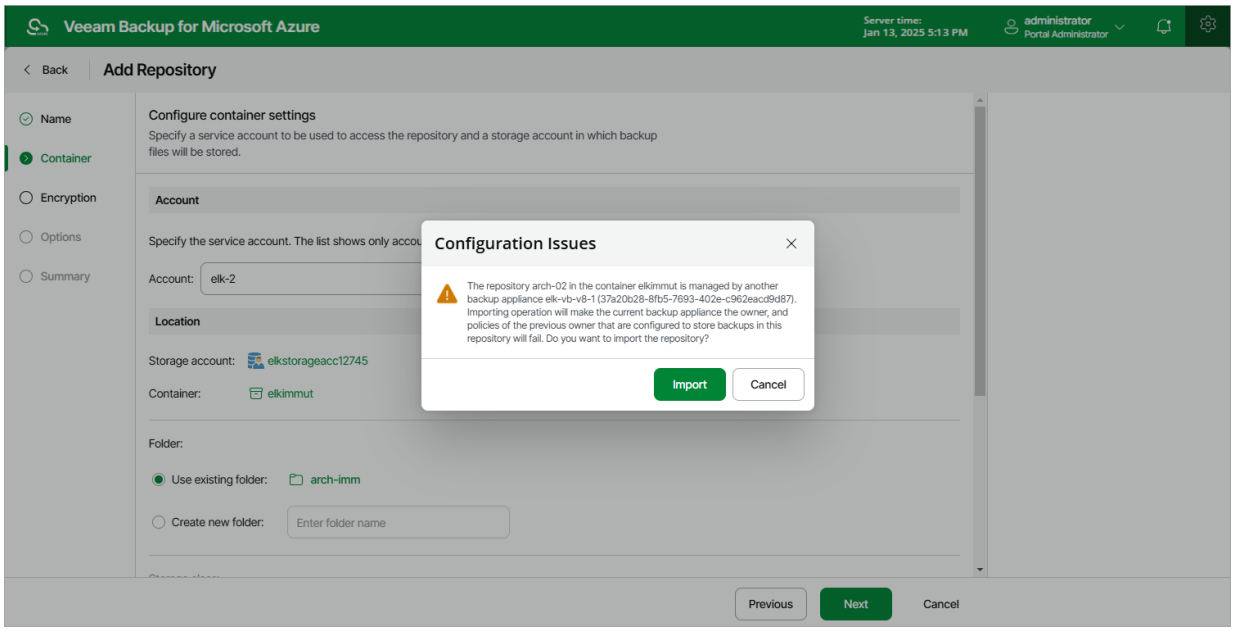
To prevent the same backup repository from being used simultaneously on different backup appliances, Veeam Backup for Microsoft Azure verifies whether the backup repository is managed by any backup appliance when you add an existing folder as a target backup repository. Retention sessions running on different appliances may corrupt backup files stored in this repository, which may result in unpredictable data loss.

If the backup repository is already connected to any backup appliance, Veeam Backup for Microsoft Azure will display a warning notifying that the backup repository has a different backup appliance owner. To allow Veeam Backup for Microsoft Azure to take ownership of this repository, click **Import**. If you do not want to import the repository to the current backup appliance, click **Cancel** and choose another folder as a target backup repository.

**IMPORTANT**

Consider the following:

- Veeam Backup for Microsoft Azure verifies the backup appliance owner only for those backup repositories that were added to Veeam Backup for Microsoft Azure version 7.0 or later.
- As soon as you import the backup repository to the current backup appliance, the backup policies configured on the previous backup appliance will start failing.
- As soon as you import the backup repository to the current backup appliance, Veeam Backup for Microsoft Azure launches a worker instance in an Azure region in which the repository resides.
- Make sure to remove the repository from the previous backup appliance to prevent possible data corruption.



# Step 4. Enable Data Encryption

At the **Encryption** step of the wizard, choose whether you want to encrypt backups stored in the selected blob container.

> **NOTE**
>
> If you have selected an existing folder at the **Container** step of the wizard, you cannot change the encryption settings while adding the repository. If encryption is enabled for this folder at the repository level, you must provide the currently used password or an encryption key to let Veeam Backup for Microsoft Azure access this folder and add it as a backup repository. You will be able to edit the repository settings later as described in section Editing Backup Repository Settings.

To enable encryption for the backup repository, do the following:

1. Click **Edit Encryption Settings**.
2. In the **Encryption settings** window, set the **Enable encryption** toggle to *On*.

> **IMPORTANT**
>
> After you create a repository with encryption enabled, you will not be able to disable encryption for this repository. However, you will still be able to change the encryption settings as described in section Editing Backup Repository Settings.

3. Choose whether you want to use a password or an Azure Key Vault cryptographic key to encrypt the backed-up data.
   - To use password encryption, select the **Use password encryption** option and specify a password that will be used to encrypt data.
   - To encrypt data using an Azure Key Vault cryptographic key, select the **Use Azure Key Vault encryption key** option, choose an Azure Key Vault where the cryptographic key is stored, and then choose the necessary key.

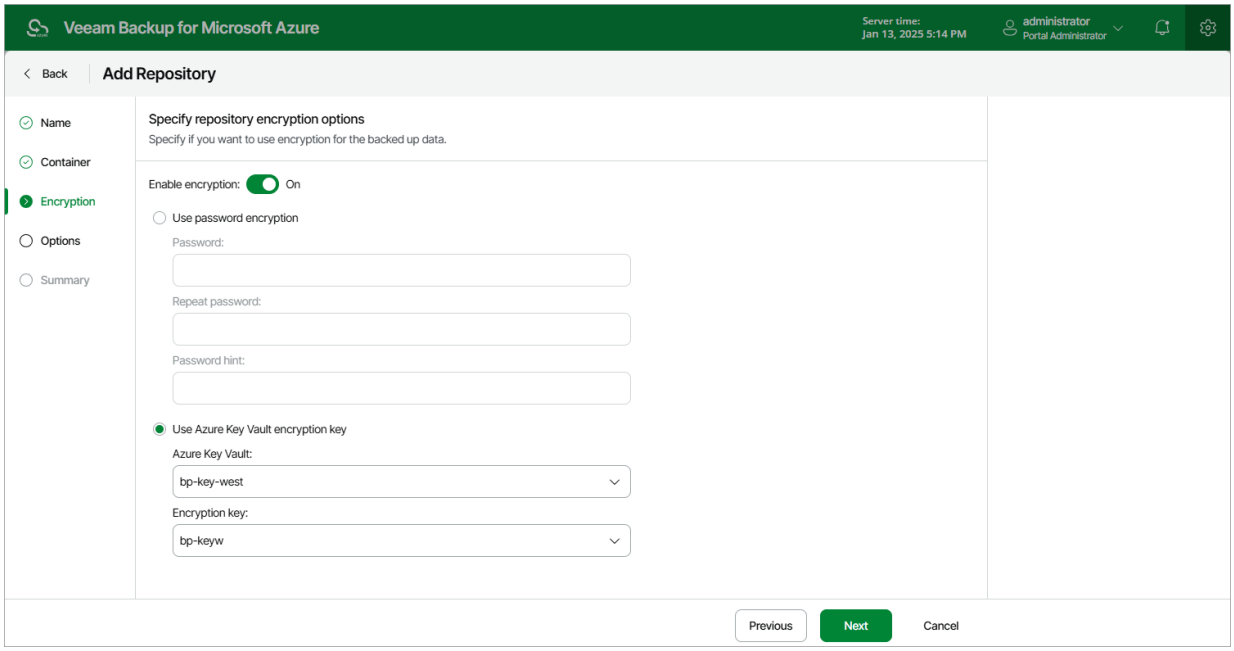
     For an Azure vault to be displayed in the list of available vaults, it must be created in Microsoft Azure as described in Microsoft Docs. For a cryptographic key to be displayed in the list of available encryption keys, it must be created in Microsoft Azure as described in Microsoft Docs.

**IMPORTANT**

If you want to use an Azure Key Vault cryptographic key for encryption at the repository level, consider the following:

- Do not disable cryptographic keys specified in the repository settings. Otherwise, Veeam Backup for Microsoft Azure will not be able to encrypt data, and backup policies that store backups in these repositories will fail to complete successfully.
- Do not delete cryptographic keys specified in the repository settings. Otherwise, Veeam Backup for Microsoft Azure will not be able to decrypt data stored in these repositories.

  If a cryptographic key is scheduled for deletion, it will acquire the Pending deletion state. In this case, Veeam Backup for Microsoft Azure will raise a warning, and, during the following 7 days, you must either change the encryption settings for the backup repository in Veeam Backup for Microsoft Azure or cancel the key deletion.

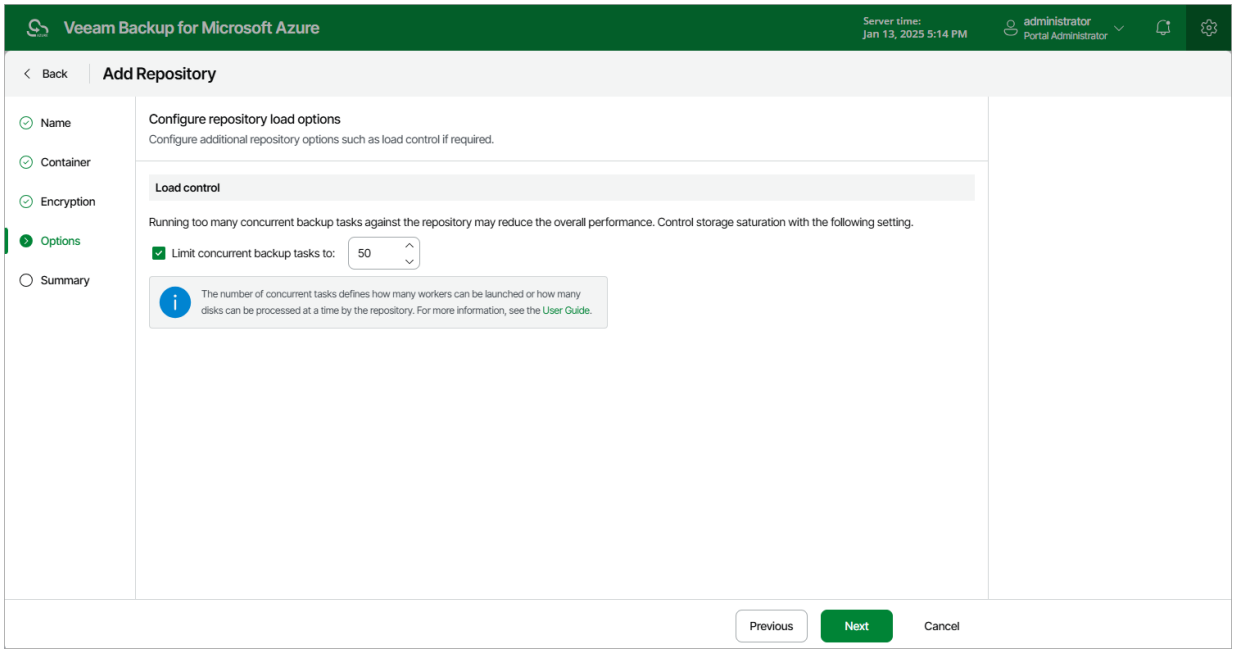


# Step 5. Configure Load Options

While backing up Azure resources, Veeam Backup for Microsoft Azure launches worker instances responsible for processing and transfer of backed-up data to backup repositories. When a backup policy addresses a backup repository, worker instances establish connections with the repository to retrieve data. To learn how Veeam Backup for Microsoft Azure performs backup operations, see Overview.

Too many connections to a repository at a time may cause performance issues due to Microsoft Azure ingress limits for storage accounts. To avoid these issues, you can limit the number of concurrent connections of worker instances at the **Options** step of the wizard. To do that, select the **Limit concurrent backup tasks to** check box and specify the maximum number of tasks that can be simultaneously processed when addressing the repository.

The number of concurrent tasks limits connections to the backup repository and, therefore, defines how many worker instances can be launched to process Azure resources whose backups will be stored in this repository. Consider that if the number of concurrent tasks is less than the maximum number of worker instances that Veeam Backup for Microsoft Azure is allowed to launch and use simultaneously to process Azure resources during backup operations, Veeam Backup for Microsoft Azure will only launch as many worker instances as many concurrent tasks are specified. To learn how to set the maximum number of worker instances, see Adding Worker Profiles.

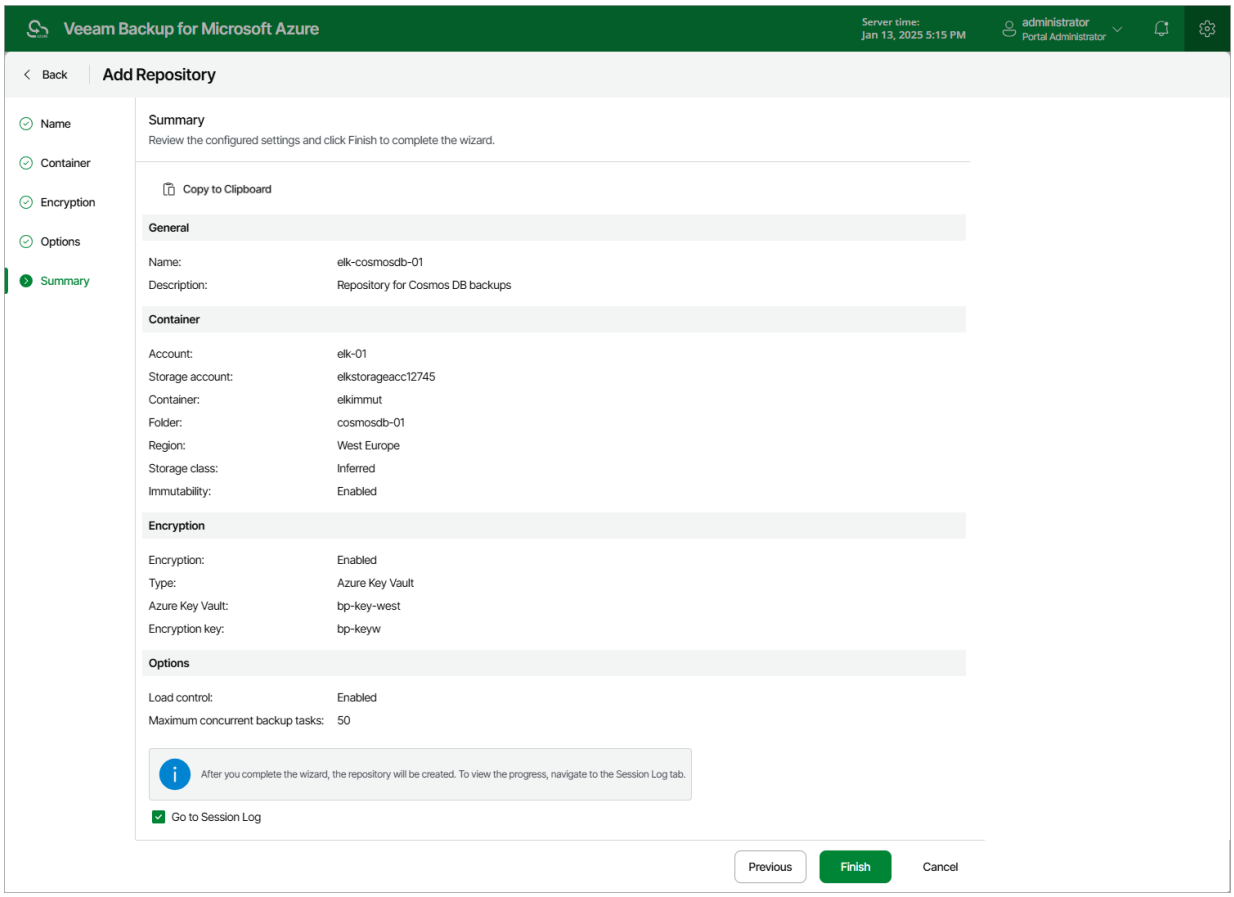


# Step 6. Finish Working with Wizard

At the **Summary** step of the wizard, review summary information, choose whether you want to proceed to the Session Log page to track the progress of repository creation, and click **Finish**.

As soon as you click **Finish**, Veeam Backup for Microsoft Azure will check whether any restore points were previously stored in this repository — and will automatically import all the detected restore points to the configuration database. Veeam Backup for Microsoft Azure will then periodically rescan repositories for newly created restore points and metadata. For more information, see Rescanning Backup Repositories.

> **TIP**
>
> Veeam Backup for Microsoft Azure does not rescan backups of virtual network configurations stored in the repositories. If you accidentally delete a virtual network configuration backup from the database, you can perform an import operation manually to restore this backup using its copy in the repository, as described in section Importing Virtual Network Configuration Data.



# Editing Backup Repository Settings

The settings that you can modify for a backup repository depend on whether the repository has been added to the backup infrastructure using the Veeam Backup & Replication console or the Veeam Backup for Microsoft Azure Web UI.

## Editing Backup Repository Settings Using Veeam Backup & Replication Console

For each standard repository, you can modify settings configured while adding the repository to the backup infrastructure:

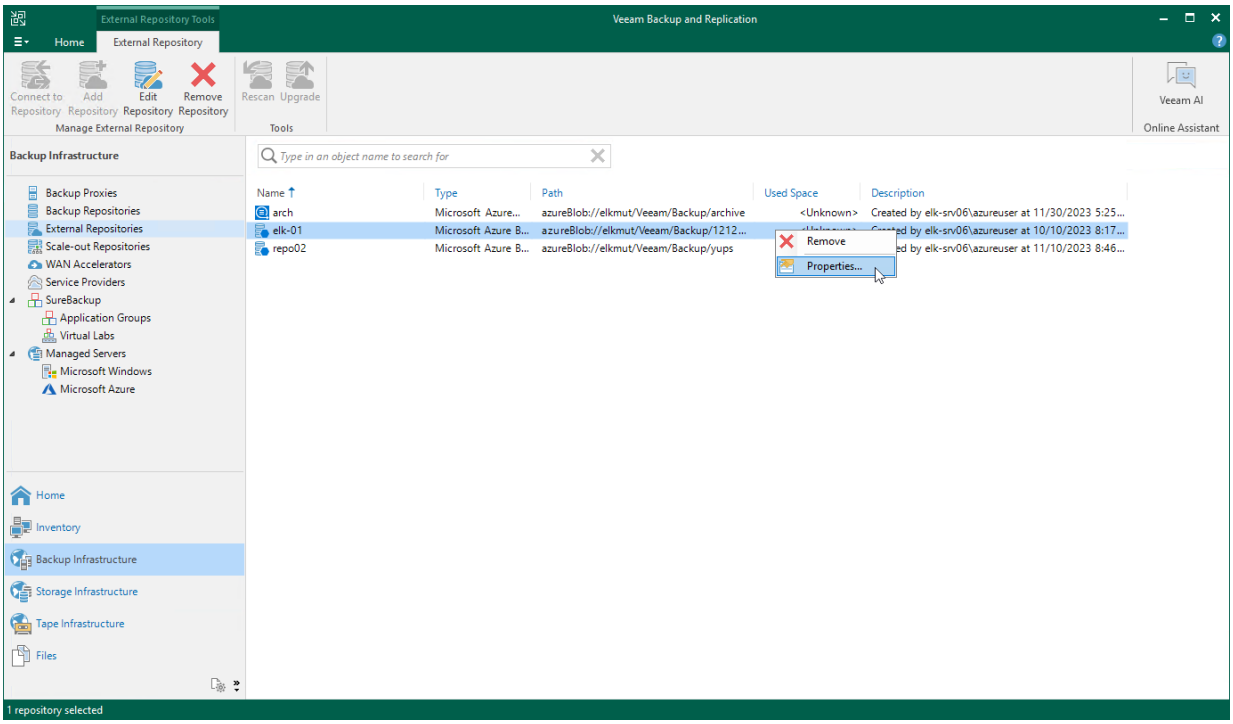
1. In the Veeam Backup & Replication console, open the **Backup Infrastructure** view.
2. Navigate to **External Repositories**.
3. Select the necessary repository and click **Edit Repository** on the ribbon.

   Alternatively, you can right-click the repository and select **Properties**.
4. Complete the **Edit External Repository** wizard:
   a. To specify a new name and description for the repository, follow the instructions provided in section Creating New Repositories (step 2).
   b. To change the credentials of the Microsoft Azure storage account and the gateway server used to access the repository, follow the instructions provided in section Creating New Repositories (step 3).
   c. To enable encryption or change the encryption settings of the repository, follow the instructions provided in section Creating New Repositories (step 6).

> **IMPORTANT**
>
> If you change the encryption settings of a standard backup repository using the Veeam Backup & Replication console, Veeam Backup & Replication will not propagate these settings to the backup appliance automatically. Consider updating the settings manually as described in section Editing Backup Repository Settings Using Veeam Backup for Microsoft Azure Web UI.

   d. At the **Apply** step of the wizard, wait for the changes to be applied and click **Next**.

e. At the **Summary** step of the wizard, review summary information and click **Finish**.




# Editing Backup Repository Settings Using Veeam Backup for Microsoft Azure Web UI

For each backup repository, you can modify settings configured while adding the repository to Veeam Backup for Microsoft Azure:

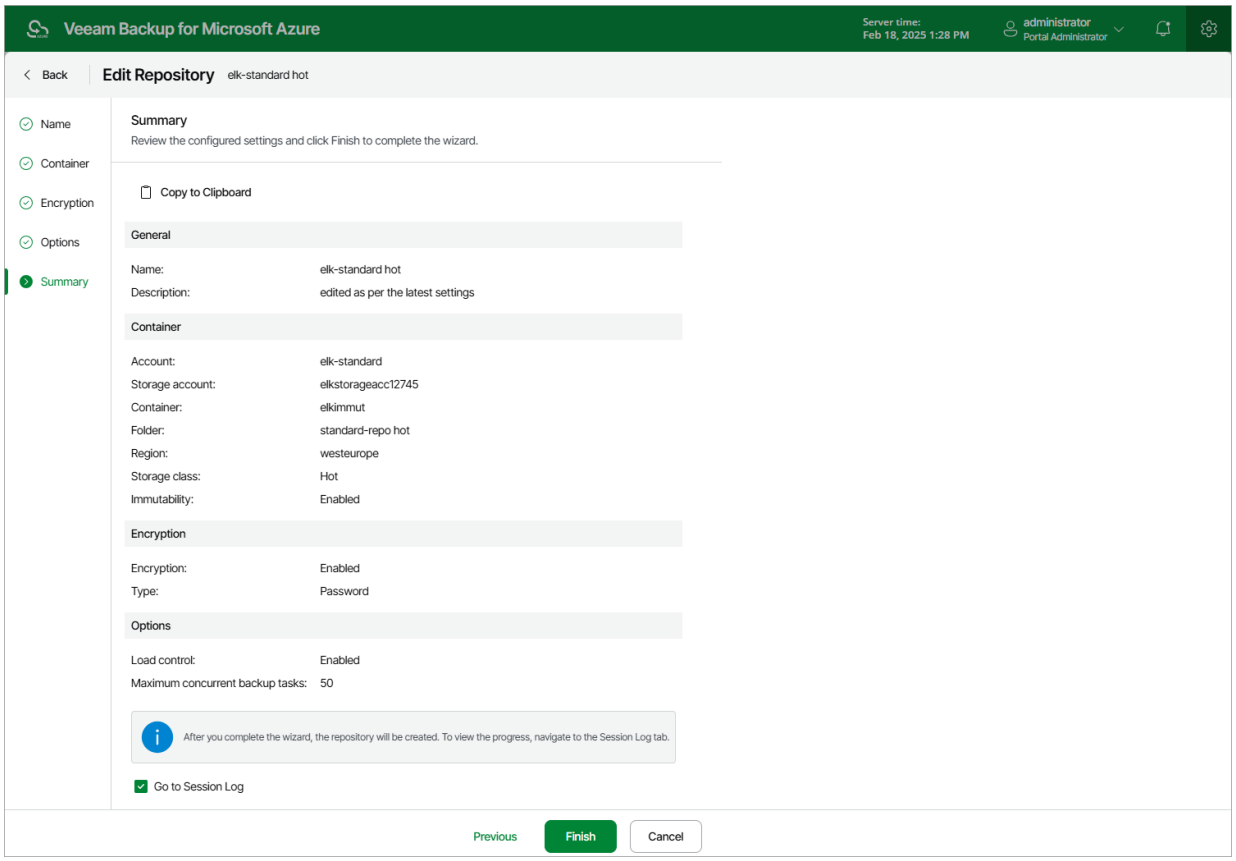
1. Switch to the **Configuration** page.
2. Navigate to **Repositories**.
3. Select the repository and click **Edit**.
4. Complete the **Edit Repository** wizard.
   a. To provide a new name and description for the repository, follow the instructions provided in section Adding Backup Repositories Using Web UI (step 2).
   b. To change the service account whose permissions Veeam Backup for Microsoft Azure uses to access the repository, follow the instructions provided in section Adding Backup Repositories Using Web UI (step 3).
   c. [Applies only to repositories managed by another backup appliance] To change the owner of the repository, switch to the **Container** step and click **Next**. Then, follow the instructions provided in section Adding Backup Repositories Using Web UI (step 3).
   d. To enable data encryption or change the configured encryption settings, follow the instructions provided in section Adding Backup Repositories Using Web UI (step 4).

**IMPORTANT**

If your backup appliance is managed by a Veeam Backup & Replication server and you change the encryption settings of a backup repository using the Veeam Backup for Microsoft Azure Web UI, Veeam Backup for Microsoft Azure will not propagate these settings to the Veeam Backup & Replication server automatically. Consider updating the settings manually as described in section Editing Backup Repository Settings Using Veeam Backup & Replication Console.

e. To change the configured load settings for the repository, follow the instructions provided in section Adding Backup Repositories Using Web UI (step 5).

f. At the **Summary** step of the wizard, review summary information, choose whether you want to proceed to the Session Log page to track the progress of modifying the backup repository settings, and click **Finish** to confirm the changes.



# Rescanning Backup Repositories

Veeam Backup & Replication periodically rescans standard repositories for newly created restore points and metadata — the results of every rescan session are displayed in the **History** view under the **System** node. A rescan operation is launched automatically every 24 hours or in the following cases:

- After you add a repository to the backup infrastructure.
- After a backup chain is modified in the repository (for example, if a restore point is added or deleted from the chain).

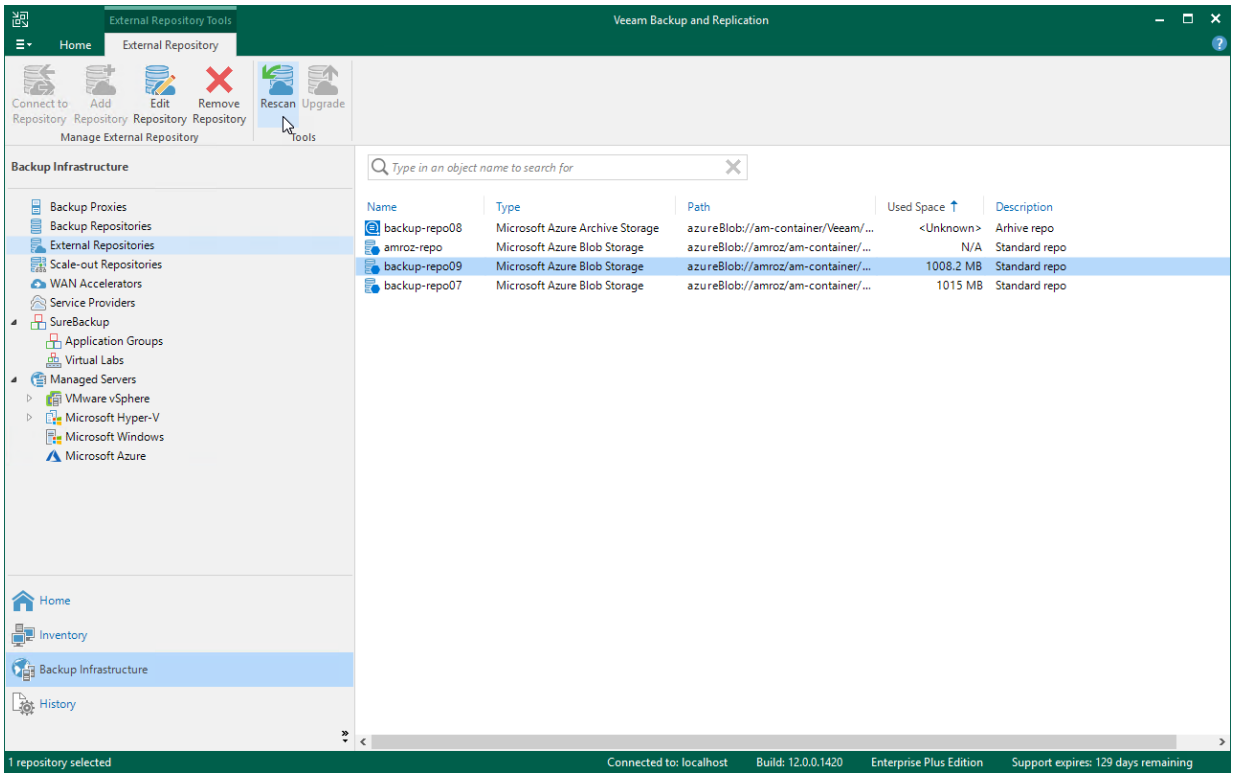
However, you can perform a rescan operation for a repository manually:

1. In the Veeam Backup & Replication console, open the **Backup Infrastructure** view.
2. Navigate to **External Repositories**.
3. Select the necessary repository and click **Rescan** on the ribbon.

   Alternatively, you can right-click the repository and select **Rescan**.

If multiple repositories are present in the backup infrastructure, you can perform the rescan operation for all repositories simultaneously. To do that, right-click the **External Repositories** node and select **Rescan**.

> **NOTE**
>
> Veeam Backup & Replication does not rescan backups of virtual network configurations stored in repositories.



# Removing Backup Repositories

The consequences of actions performed with a backup repository depend on whether the repository has been added to the backup infrastructure using the Veeam Backup & Replication console or the Veeam Backup for Microsoft Azure Web UI.

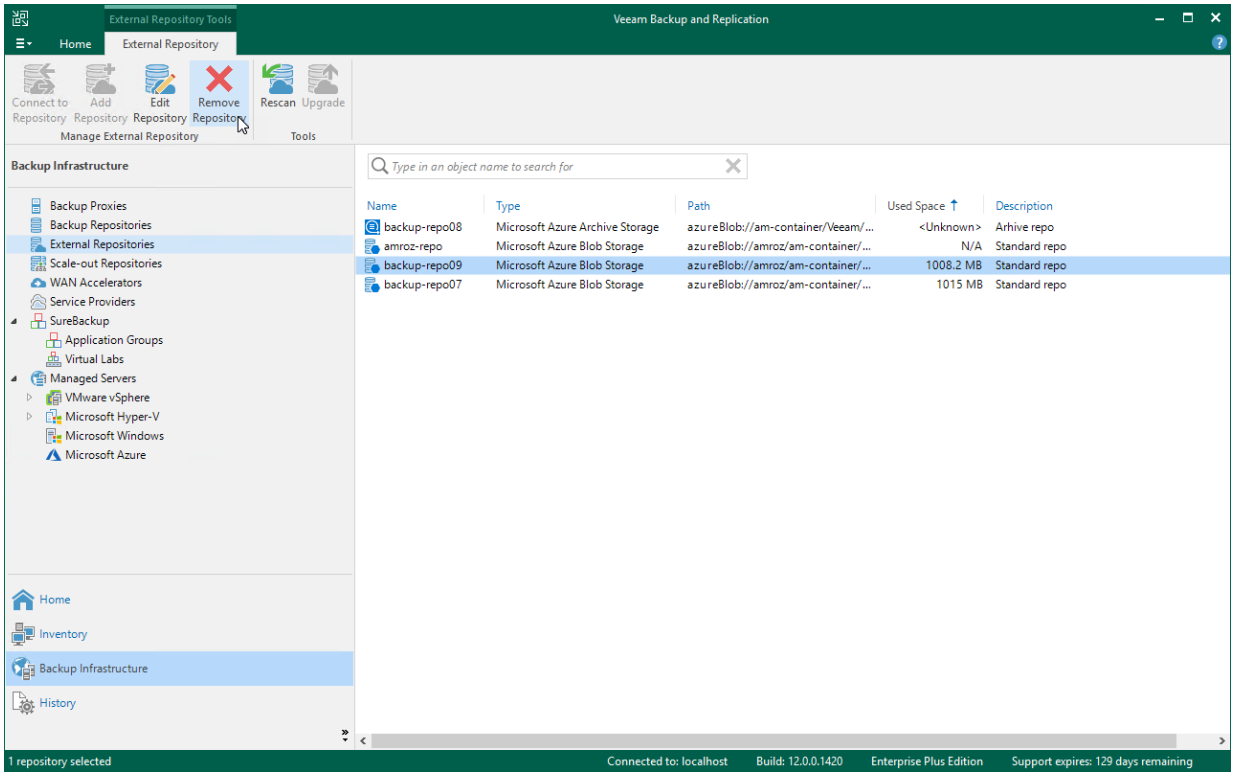
## Removing Backup Repository Using Veeam Backup & Replication Console

Microsoft Azure Plug-in for Veeam Backup & Replication allows you to permanently remove repositories from the backup infrastructure:

1. In the Veeam Backup & Replication console, open the **Backup Infrastructure** view.
2. Navigate to **External Repositories**.
3. Select the necessary repository and click **Remove Repository** on the ribbon.

   Alternatively, you can right-click the repository and select **Remove**.

Note that the repository will not be removed from the backup appliance. To learn how to remove repositories from backup appliances, see Removing Backup Repository Using Veeam Backup for Microsoft Azure Web UI.




## Removing Backup Repository Using Veeam Backup for Microsoft Azure Web UI

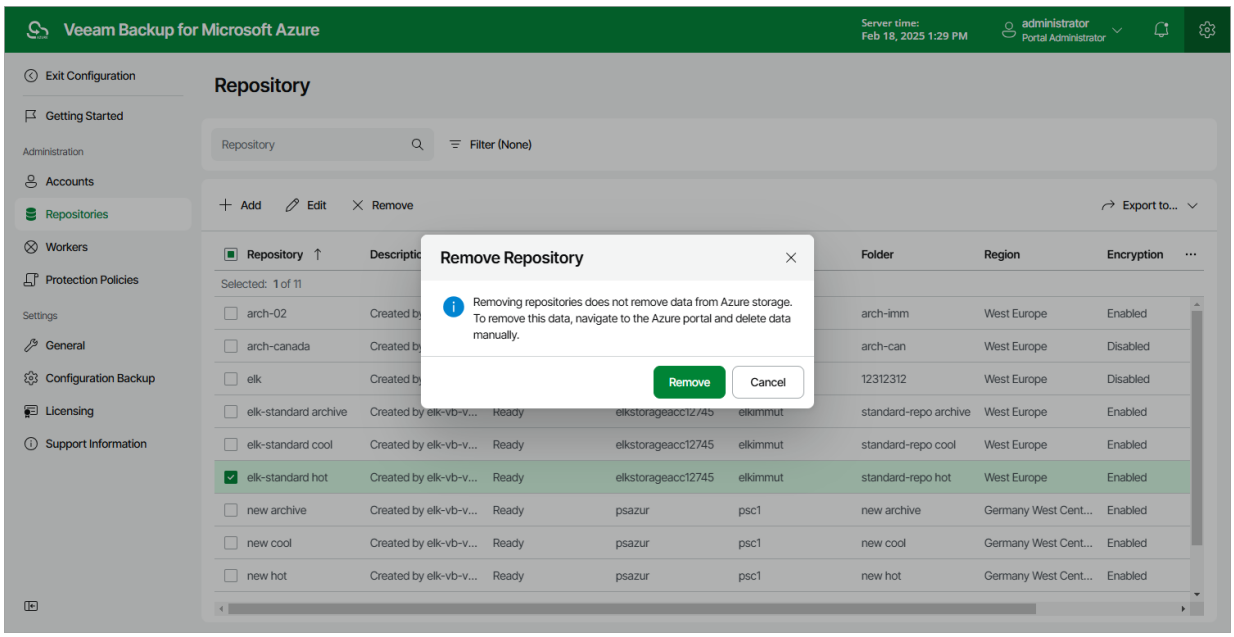
The Veeam Backup for Microsoft Azure Web UI allows you to permanently remove backup repositories if you no longer need them. When you remove a backup repository, Veeam Backup for Microsoft Azure unassigns the repository from the folder in the target blob container so that the folder is no longer used as a repository.

> **NOTE**
>
> Even though the folder is no longer used as a repository, Veeam Backup for Microsoft Azure preserves all backups previously stored in the repository and keeps these backups in Microsoft Azure. You can assign the folder to a new backup repository so that Veeam Backup for Microsoft Azure imports the backed-up data to the configuration database. In this case, you will be able to perform all disaster recovery operations described in section Performing Restore.
>
> If you no longer need the backed-up data, you can remove it as described in section Managing Backed-Up Data.

To remove a backup repository, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **Repositories**.
3. Select the repository and click **Remove**.

> **IMPORTANT**
>
> Consider the following:
>
> - You cannot remove a backup repository that is used by any backup policy or by a scheduled configuration backup. Modify the settings of all the related policies to remove references to the repository — and then try removing the repository again.
> - When you remove a backup repository from a backup appliance managed by a Veeam Backup & Replication server, this repository will not be removed from the Veeam Backup & Replication console automatically. In this case, you need to remove the repository manually.



# Managing User Accounts

Veeam Backup for Microsoft Azure controls access to its functionality with the help of user roles. A role defines what operations users can perform and what range of data is available to them in the Veeam Backup for Microsoft Azure UI.

There are 3 user roles that you can assign to users working with Veeam Backup for Microsoft Azure:

- **Portal Administrator** – can perform all configuration actions, and can also act as a Portal Operator and Restore Operator.
- **Portal Operator** – can create, edit and start backup policies, manage the protected data, perform all restore operations and view session statistics.
- **Restore Operator** – can only perform restore operations and view session statistics.
- **Read-Only User** – can only view and export backup and restore operation data without performing any operations.

> **IMPORTANT**
>
> The list of portal users may display user accounts with the *Company Administrator* role assigned – these accounts are intended to be used for the integration of Veeam Backup for Microsoft Azure and Veeam Service Provider Console, and are created using the Veeam Service Provider Console plug-in. It is not recommended that you perform any actions with these users.

The following table describes the functionality available to users with different roles in the Veeam Backup for Microsoft Azure UI.

| Tab | Functionality | Portal Administrator | Portal Operator | Restore Operator | Read-Only User |
|---|---|---|---|---|---|
| **Overview** | Dashboard | Full | Full | N/A | Full |
| **Resources** | Infrastructure | Full | Full | N/A | N/A |
| **Policies** | Backup policies | Full | Full | N/A | Read-only |
| **Protected Data** | Protected resources list | Full | Full | Full | Read-only |
| | Restore | Full | Full | Full | N/A |
| | File-level restore | Full | Full | Full | N/A |
| | Remove | Full | Full | N/A | N/A |
| **Session Log** | Session logs | Full | Full | Full | Full |

| Tab | Functionality | Portal Administrator | Portal Operator | Restore Operator | Read-Only User |
|---|---|---|---|---|---|
| | Stop session execution | Full | Full | Full | N/A |
| Configuration | | | | | |
| **Accounts** | Service accounts, SQL Server and SMTP accounts, portal users | Full | N/A | N/A | N/A |
| **Repositories** | Backup repositories | Full | N/A | N/A | N/A |
| **Worker Instances** | Worker instances | Full | N/A | N/A | N/A |
| **Policy Templates** | SLA and storage templates | Full | Full | N/A | N/A |
| **Settings** | General settings | Full | N/A | N/A | N/A |
| **Licensing** | Licensing | Full | N/A | N/A | N/A |
| **Support Information** | Updates and logs | Full | N/A | N/A | N/A |

# Adding User Accounts

To manage access to Veeam Backup for Microsoft Azure, you can create local user accounts or add user accounts of your identity provider. To be able to retrieve user identities from the identity provider, you must first configure single sign-on settings.

To add a Veeam Backup for Microsoft Azure user account, do the following:

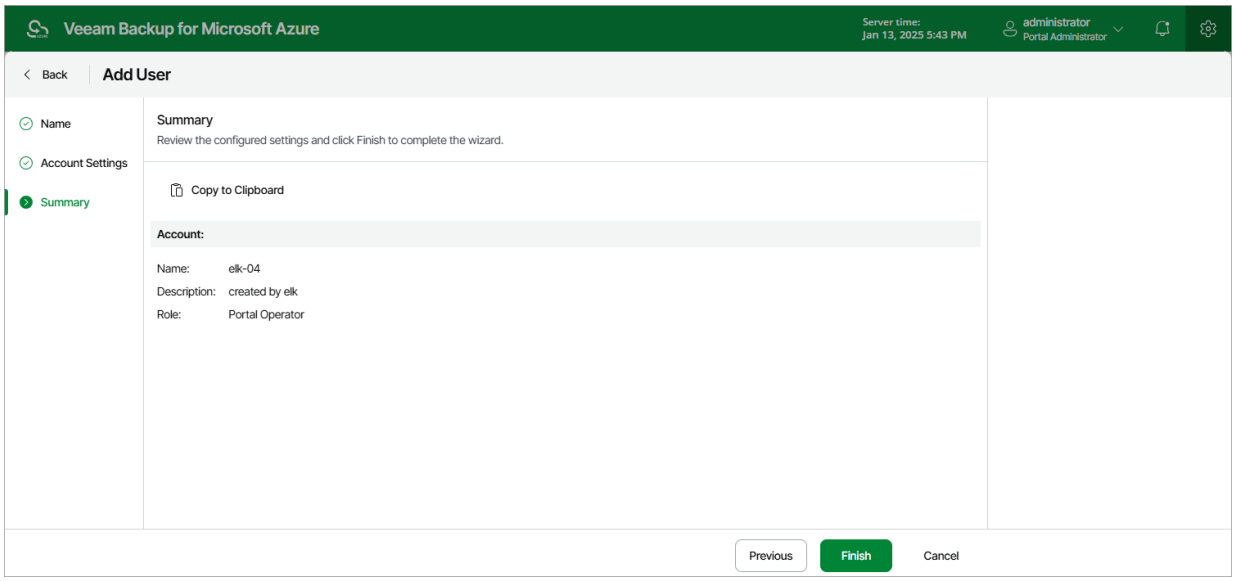
1. Switch to the **Configuration** page.
2. Navigate to **Accounts** > **Portal Users**.
3. Click **Add**.
4. Complete the **Add User** wizard.
   a. At the **Type** step of the wizard, choose whether you want to create a new Veeam Backup for Microsoft Azure user or to retrieve a user identity from your identity provider.
   b. At the **Name** step of the wizard, specify a name and description for the user account.

      The maximum length of the account name is 32 characters. An account name can contain only lowercase and uppercase Latin letters, numeric characters, underscores and dashes. A description can contain only lowercase and uppercase Latin letters, numeric characters, dots, commas and spaces.

> **IMPORTANT**
>
> If you have selected the **Identity Provider account** option at step 4.a, the name specified for a user account must match the value of an attribute that the identity provider will send to Veeam Backup for Microsoft Azure to authenticate the user. For more information, see Configuring SSO Settings.

   c. At the **Account Settings** step of the wizard, select a role for the user account. For more information on user roles, see Managing User Accounts.

      If you have selected the **Veeam Backup for Microsoft Azure account** option at step 4.a, specify a password for the new Veeam Backup for Microsoft Azure user account.
   d. At the **Summary** step of the wizard, review summary information and click **Finish**.

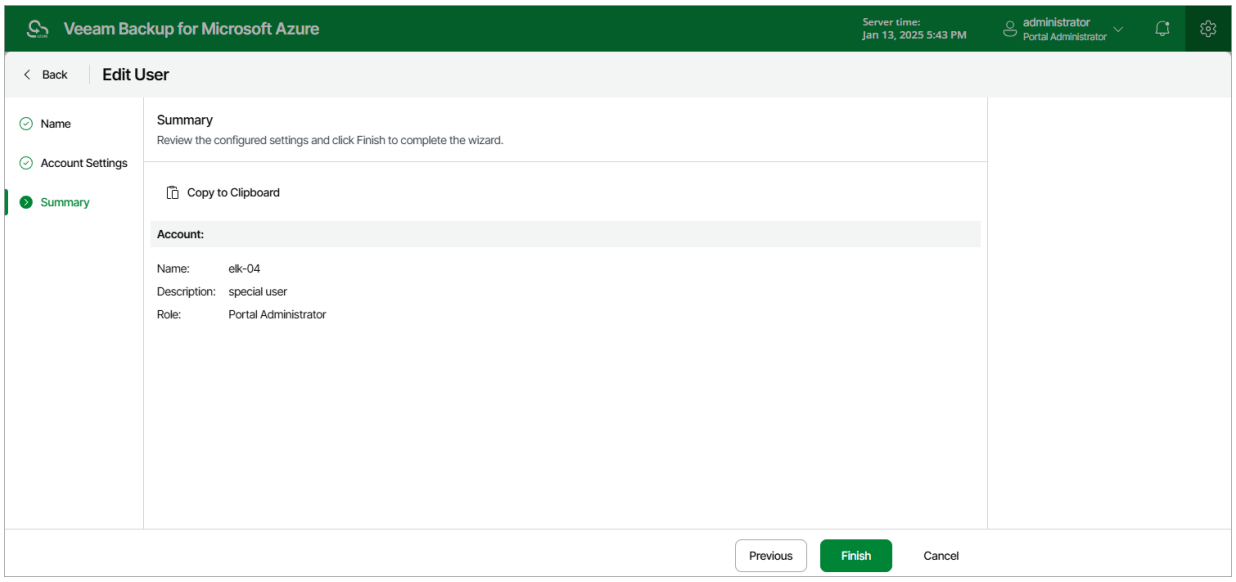


# Editing User Accounts

For each user account, you can modify settings configured while adding the account:

1. Switch to the **Configuration** page.
2. Navigate to **Accounts** > **Portal Users**.
3. Select the account and click **Edit**.
4. Complete the **Edit User** wizard:
   a. At the **Name** step, provide a new description for the account.
   b. At the **Account Settings** step, choose a new role for the account.
   c. At the **Summary** step, review summary information and click **Finish** to confirm the changes.

> **IMPORTANT**
>
> If your backup appliance is managed by a Veeam Backup & Replication server, do not change the role of a user whose credentials Veeam Backup & Replication uses to connect to the backup appliance. Otherwise, the connection will not be established.



# Changing User Passwords

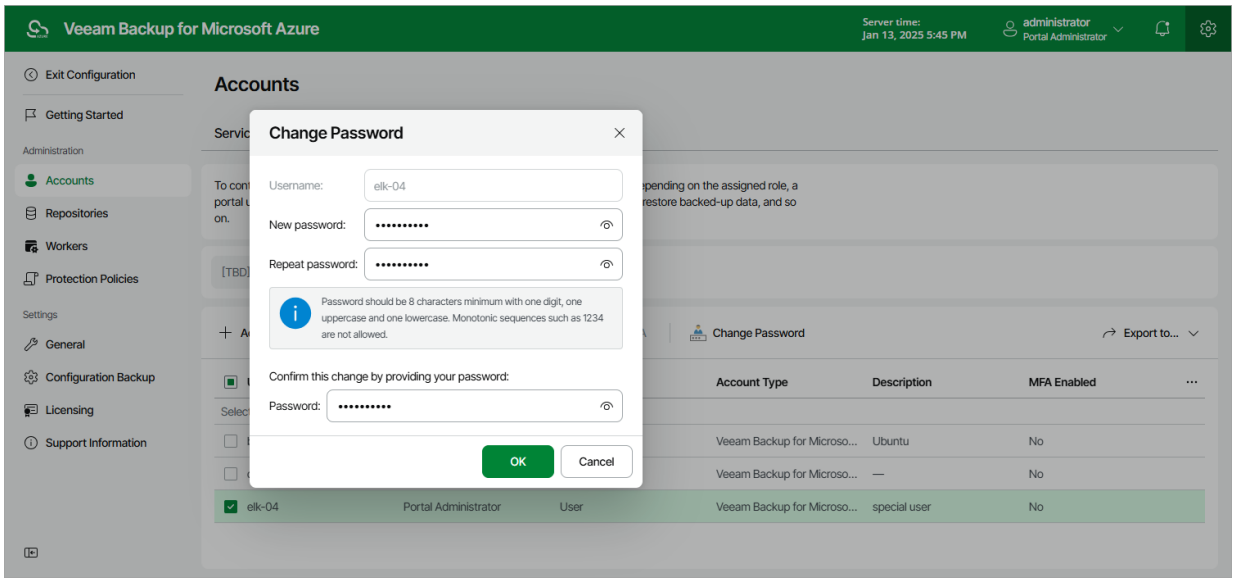
For Veeam Backup for Microsoft Azure user accounts, you can change the password specified while creating the account.

> **NOTE**
>
> Consider the following:
>
> - Passwords of accounts whose user identities were obtained from an identity provider cannot be changed by any user accounts, including their own. These passwords can only be changed on the identity provider side.
> - If your backup appliance is managed by a Veeam Backup & Replication server and you change the password of a user whose credentials Veeam Backup & Replication uses to connect to the backup appliance, you must also change this user password in the Veeam Backup & Replication console as described in the Veeam Backup & Replication User Guide, section Editing and Deleting Credentials Records. Otherwise, the connection will not be established.

To change the password, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **Accounts** > **Portal Users**.
3. Select the user account and click **Change Password**.
4. In the **Change Password** window, enter the currently used password, enter and confirm a new password, and then click **OK**.

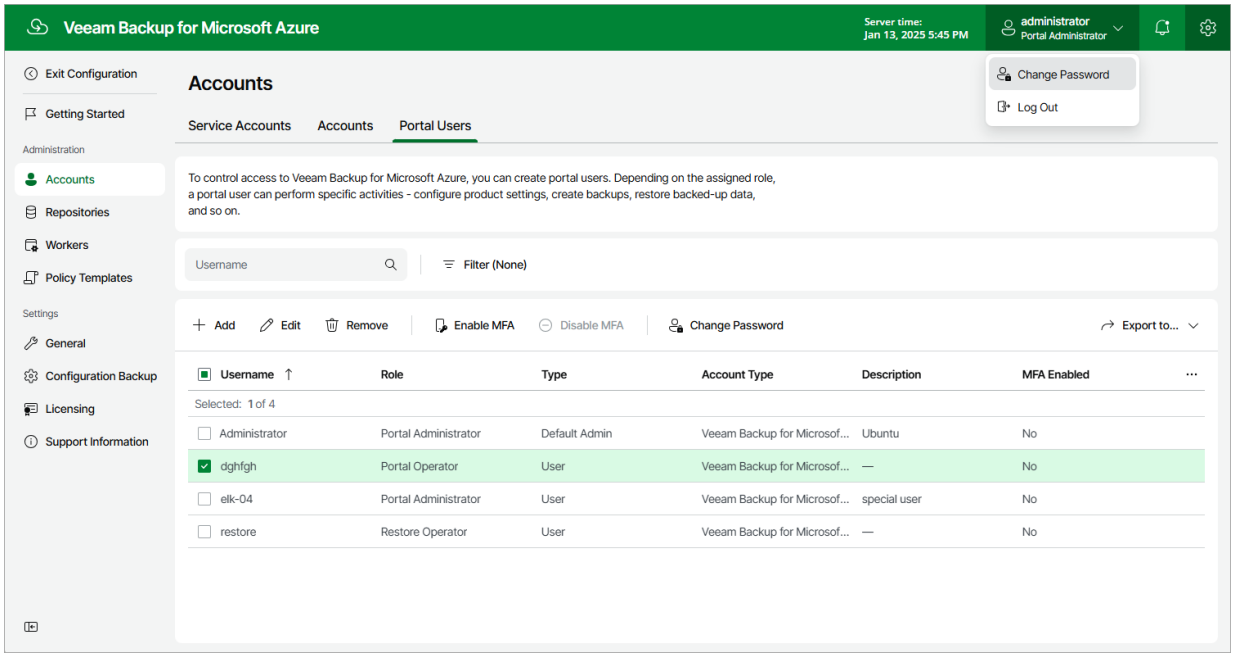
> **TIP**
>
> You can change a password of a user that is currently logged in as described in section Changing Default Admin Password.



# Changing Default Admin Password

To change the password of the Default Admin account:

1. Log in to Veeam Backup for Microsoft Azure using credentials of the Default Admin account.
2. At the top right corner, click the user name and select **Change Password**.
3. In the **Change Password** window, enter the currently used password, enter and confirm a new password, and click **OK**.



# Enabling Multi-Factor Authentication

Multi-factor authentication (MFA) in Veeam Backup for Microsoft Azure is based on the Time-based One-Time Password (TOTP) method that requires the user to verify their identity by providing a temporary six-digit code generated by an authentication application running on a trusted device.

> **IMPORTANT**
>
> You cannot enable MFA for a user account whose user identity was obtained from an identity provider.

To enable MFA for a user account, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **Accounts** > **Portal Users**.
3. Select the account and click **Enable MFA**.
4. Follow the instructions provided in the **Enabling MFA** window:
   a. Install a supported authentication application on a trusted device. To view the list of authentication applications supported by Veeam Backup for Microsoft Azure, click **See a list of compatible applications**.

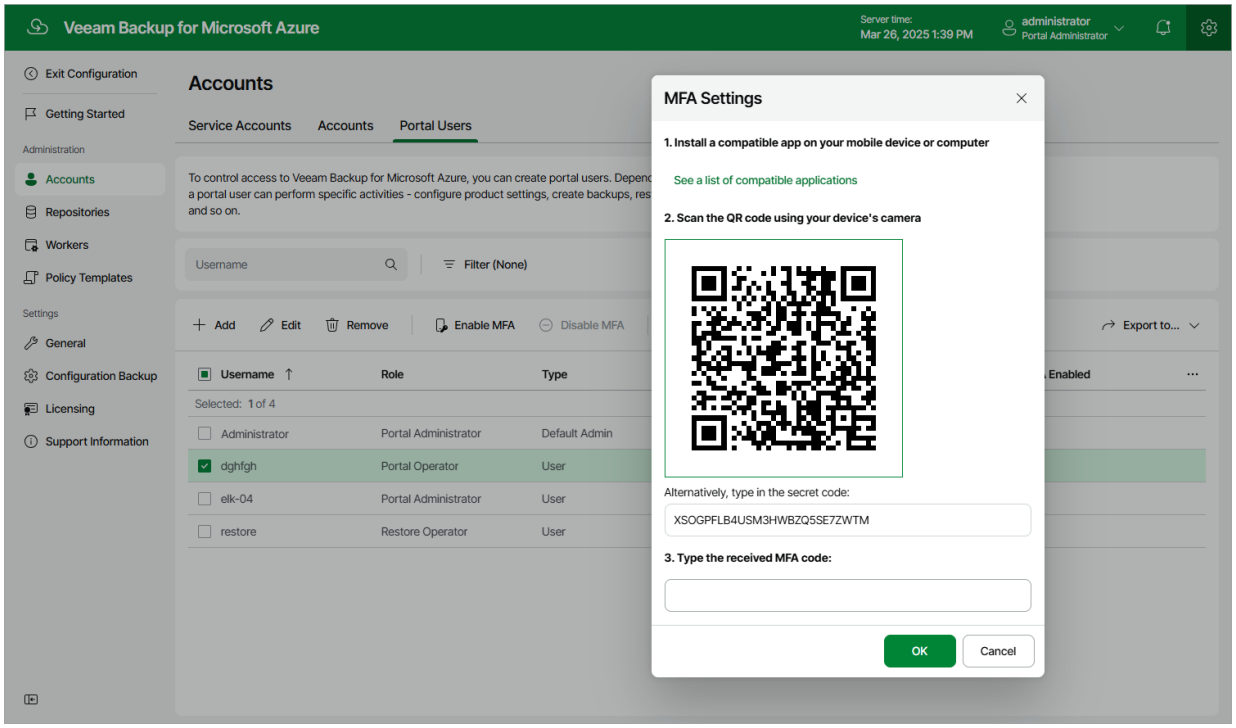
      You can use any application that supports the TOTP protocol.

   b. Scan the displayed QR code using the camera of the trusted device.

      You can also provide a secret code that you can find in the **Alternatively, type in the secret code** field if you do not want to scan the QR code.

   c. Enter a verification code sent by the authentication application.

   d. Click **OK**.



# Managing Worker Instances

To perform most data protection and disaster recovery operations (such as creating image-level backups in backup repositories and restoring backed-up data), Veeam Backup for Microsoft Azure uses worker instances. A worker instance is an auxiliary Linux-based virtual machine that is responsible for the interaction between the backup appliance and other Veeam Backup for Microsoft Azure components. Worker instances process backup workload and distribute backup traffic when transferring data to backup repositories.

Each worker instance is launched in a specific Azure region and keeps running for the duration of the backup or restore process. For more information on regions in which Veeam Backup for Microsoft Azure launches worker instances, see Worker Instances.

> **NOTE**
>
> You can tell worker instances from other Azure VMs running in your environment — all worker instances launched by Veeam Backup for Microsoft Azure will have the word ***VBA*** in their names, and the *Veeam backup appliance ID* tag. To learn how to assign custom tags to worker instances, see Adding Worker Instance Tags.

# Managing Worker Configurations

A configuration is a group of network settings that Veeam Backup for Microsoft Azure uses to launch worker instances in a specific Azure region to perform data protection and disaster recovery operations. Veeam Backup for Microsoft Azure launches one worker instance per each Azure resource added to a backup policy or restore task.

By default, Veeam Backup for Microsoft Azure automatically creates a new network configuration for each Azure region in which it launches worker instances. However, you can add custom worker configurations to provide network settings that will be used to launch worker instances in a specific region.

**IMPORTANT**

Consider the following:

- For each automatically created worker configuration, Veeam Backup for Microsoft Azure creates a virtual network, a subnet and a network security group.
- It is not recommended that you manually change settings of automatically created configurations. If you want to use a specific worker configuration, add it manually as described in section Adding Worker Configurations.

## Specifying Destination for Worker Instances

By default, Veeam Backup for Microsoft Azure launches worker instances in the same Microsoft Entra tenant, Azure subscription and resource group in which the backup appliance is deployed. However, you can specify another destination for the worker instances, as well as a service account that will be used to launch the instances:

1. Switch to the **Configuration** page.
2. Navigate to **Workers** > **Network**.
3. To specify a service account that will be used to launch the worker instances, click the link in the **Service account** field, and select the necessary destination (a service account, a tenant and a subscription) in the **Choose Account** window.

   For a service account to be displayed in the list of available accounts, it must be added to Veeam Backup for Microsoft Azure and assigned the *Worker Management* role as described in section Adding Service Accounts.

**IMPORTANT**

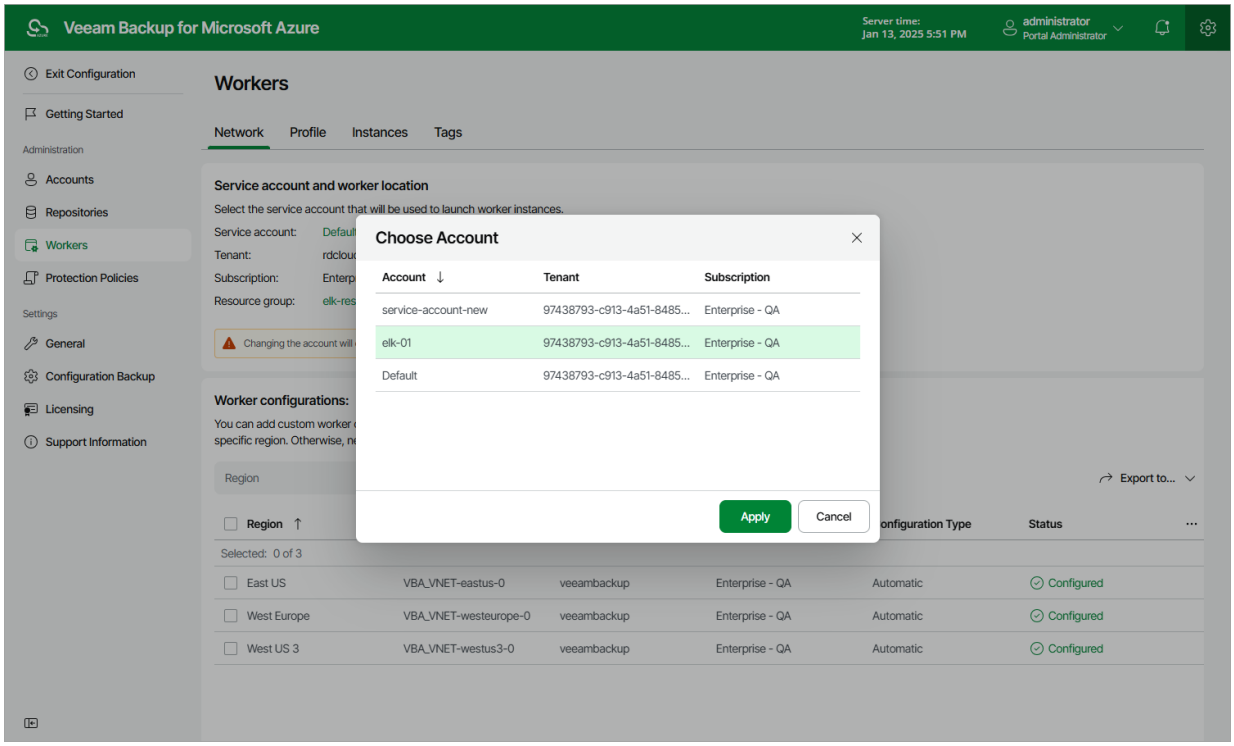
If your backup appliance operates in a private environment, you cannot specify another tenant for worker instances.

4. To specify a resource group where the worker instances will be launched, click the link in the **Resource group** field, and select the necessary group in the **Choose Resource Group** window.

   For a resource group to be displayed in the list of available groups, it must be created in Microsoft Azure as described in Microsoft Docs and must belong to the tenant and subscription specified at step 3.

If you change the service account, it is recommended that you check whether the newly selected service account has all the permissions required to launch worker instances. To do that, click **Check Permissions** and follow the instructions provided in section Checking Service Account Permissions.

> **NOTE**
>
> If you change the subscription, Veeam Backup for Microsoft Azure will disable all worker configurations created for the previously used subscription — but will not remove them automatically. If you plan to use the worker configurations again, switch back to the previous subscription to allow Veeam Backup for Microsoft Azure to re-enable these configurations. Otherwise, you can remove the configurations manually as described in section Removing Worker Configurations.




# Adding Worker Configurations

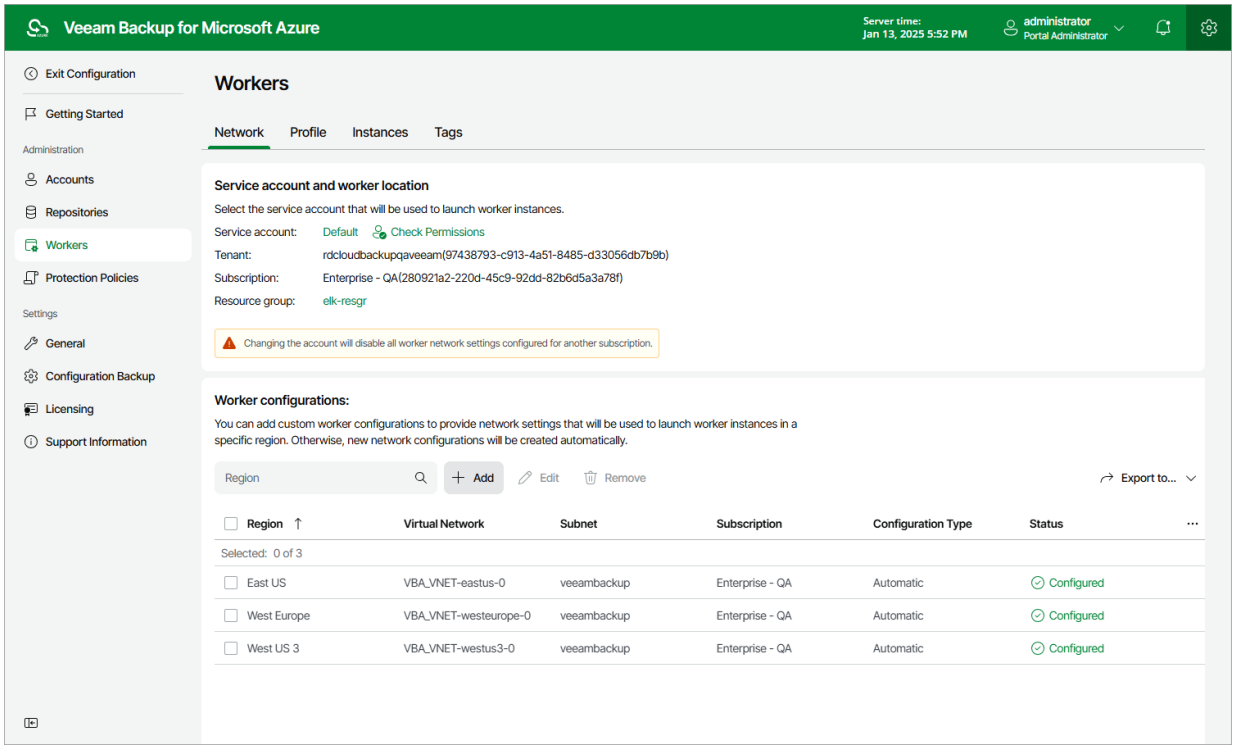
To add a new worker configuration, do the following:

1. Launch the Add Worker Network Configuration wizard.
2. Specify general settings for the worker configuration.
3. Specify network settings for the worker configuration.
4. Finish working with the wizard.

# Step 1. Launch Add Worker Network Configuration Wizard

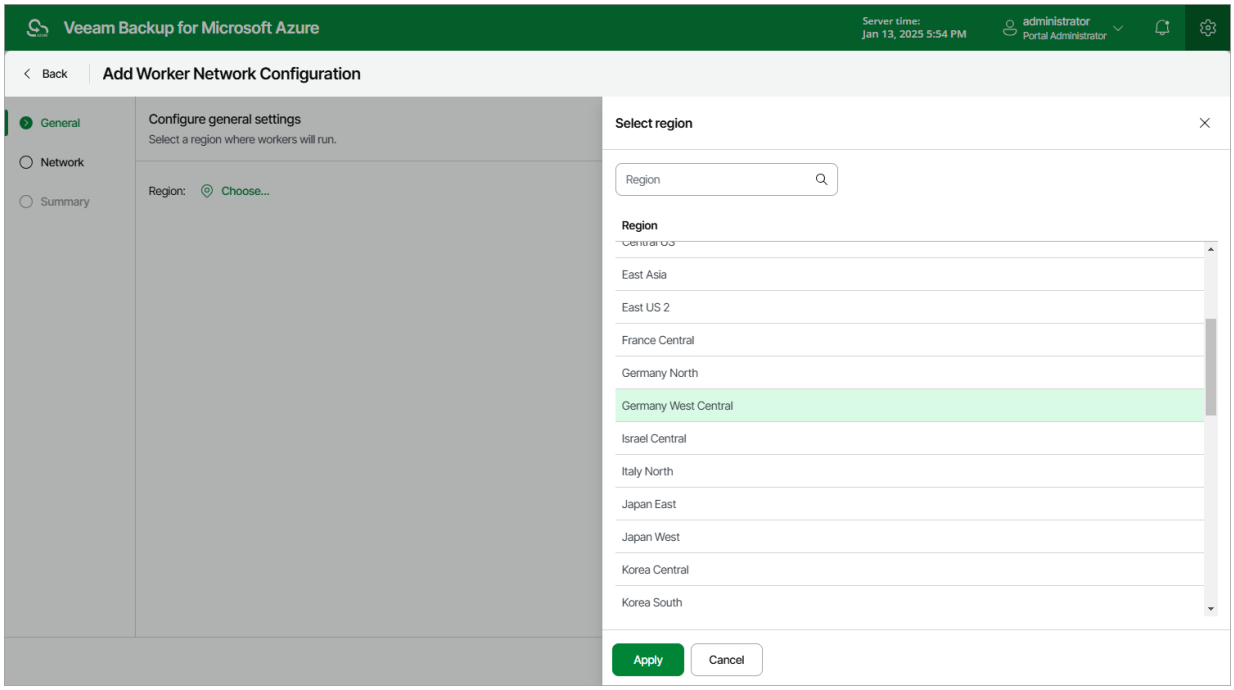
To launch the **Add Worker Network Configuration** wizard, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **Workers** > **Network**.
3. In the **Worker configurations** section, click **Add**.



# Step 2. Specify General Settings

At the **General** step of the wizard, select an Azure region where new worker instances will operate. For more information on Azure regions in which Veeam Backup for Microsoft Azure launches worker instances to perform operations, see Worker Instances.



## Step 3. Specify Network Settings

At the **Network** step of the wizard, do the following:

1. Select a network and subnet to which you want to connect worker instances created based on the new worker configuration. You can either use an existing virtual network or create a new one.

   To create a new network:

   a. Click **Add**.

   b. In the **Create Network** window, specify names and ranges of IP addresses for the new virtual network and the new subnet, and click **OK**.

      To specify IP address ranges, use the CIDR (Classless Inter-Domain Routing) notation. For more information on building networks in Microsoft Azure, see Microsoft Docs.

**IMPORTANT**

- The specified subnet address range must have at least one free IP address — Veeam Backup for Microsoft Azure will launch and simultaneously run as many worker instances as many free IP addresses there are in the subnet range.
- For virtual networks to which worker instances will be connected, virtual network service endpoints for the following services must be configured:
  - *Microsoft.Storage.Global* — either configure an endpoint for this service manually in Microsoft Azure beforehand or let Veeam Backup for Microsoft Azure do it for you automatically while deploying the worker instances.
  - *Microsoft.Sql* — manually configure an endpoint for this service if you plan to back up Azure SQL databases.
  - *Microsoft.AzureCosmosDB* — manually configure an endpoint for this service if you plan to back up Cosmos DB for PostgreSQL accounts.

  To learn how to configure virtual network service endpoints manually, see Microsoft Docs.

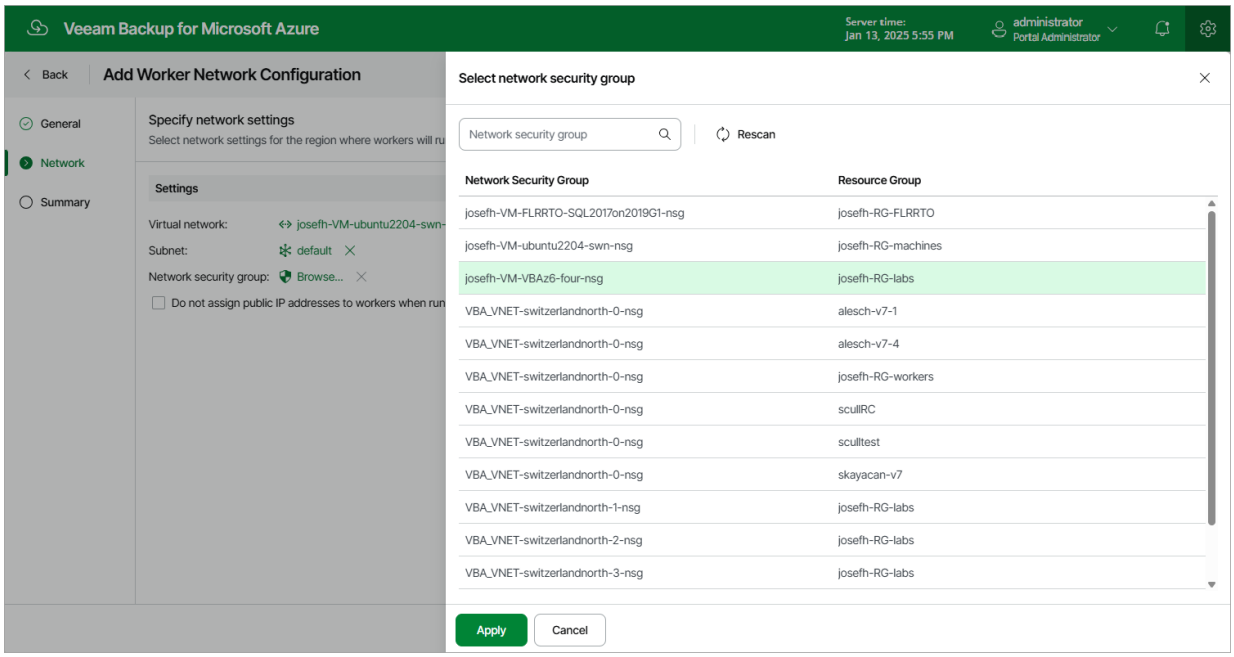
2. Select a security group that will be associated with the specified subnet.

   For a group to be displayed in the **Network Security Group** list, it must be created beforehand as described in Microsoft Docs.

**IMPORTANT**

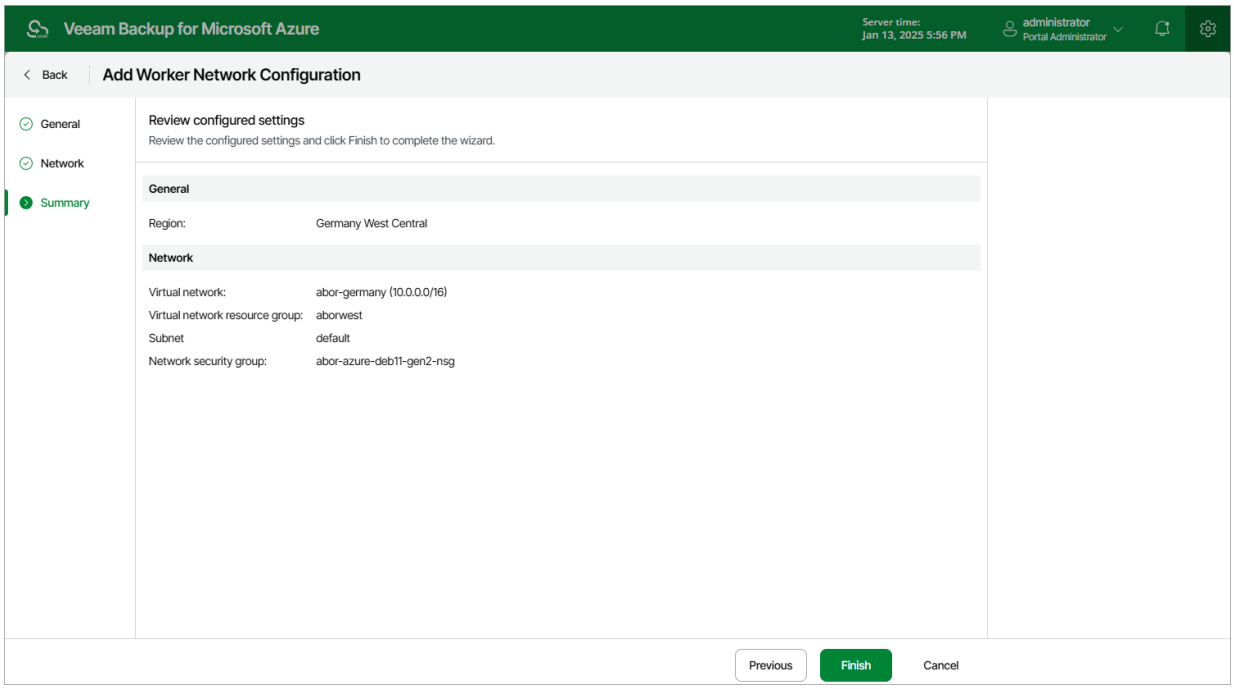
If you want worker instances created based on the new worker configuration to process resources that reside in private virtual networks, the selected security group must allow access to storage accounts created by Veeam Backup for Microsoft Azure. You can tell these resources from other Azure resources by the word *veeam* in their names and by the backup appliance ID in their tag values.

3. Choose whether you want Veeam Backup for Microsoft Azure to assign public IP addresses to worker instances used for file-level recovery operations.


Veeam Backup for Microsoft Azure
Server time:
Jan 13, 2025 5:55 PM
administrator
Portal Administrator
Back
Add Worker Network Configuration
General
Network
Summary
Specify network settings
Select network settings for the region where workers will ru
Settings
Virtual network:
josefh-VM-ubuntu2204-swn-
Subnet:
default
Network security group:
Browse...
Do not assign public IP addresses to workers when run
Select network security group
Network security group
Rescan
Network Security Group
Resource Group
josefh-VM-FLRRTO-SQL2017on2019G1-nsg
josefh-RG-FLRRTO
josefh-VM-ubuntu2204-swn-nsg
josefh-RG-machines
josefh-VM-VBAz6-four-nsg
josefh-RG-labs
VBA_VNET-switzerlandnorth-0-nsg
alesch-v7-1
VBA_VNET-switzerlandnorth-0-nsg
alesch-v7-4
VBA_VNET-switzerlandnorth-0-nsg
josefh-RG-workers
VBA_VNET-switzerlandnorth-0-nsg
scullRC
VBA_VNET-switzerlandnorth-0-nsg
sculltest
VBA_VNET-switzerlandnorth-0-nsg
skayacan-v7
VBA_VNET-switzerlandnorth-1-nsg
josefh-RG-labs
VBA_VNET-switzerlandnorth-2-nsg
josefh-RG-labs
VBA_VNET-switzerlandnorth-3-nsg
josefh-RG-labs
Apply
Cancel

## Step 4. Finish Working with Wizard

At the **Summary** step of the wizard, review summary information and click **Finish**.

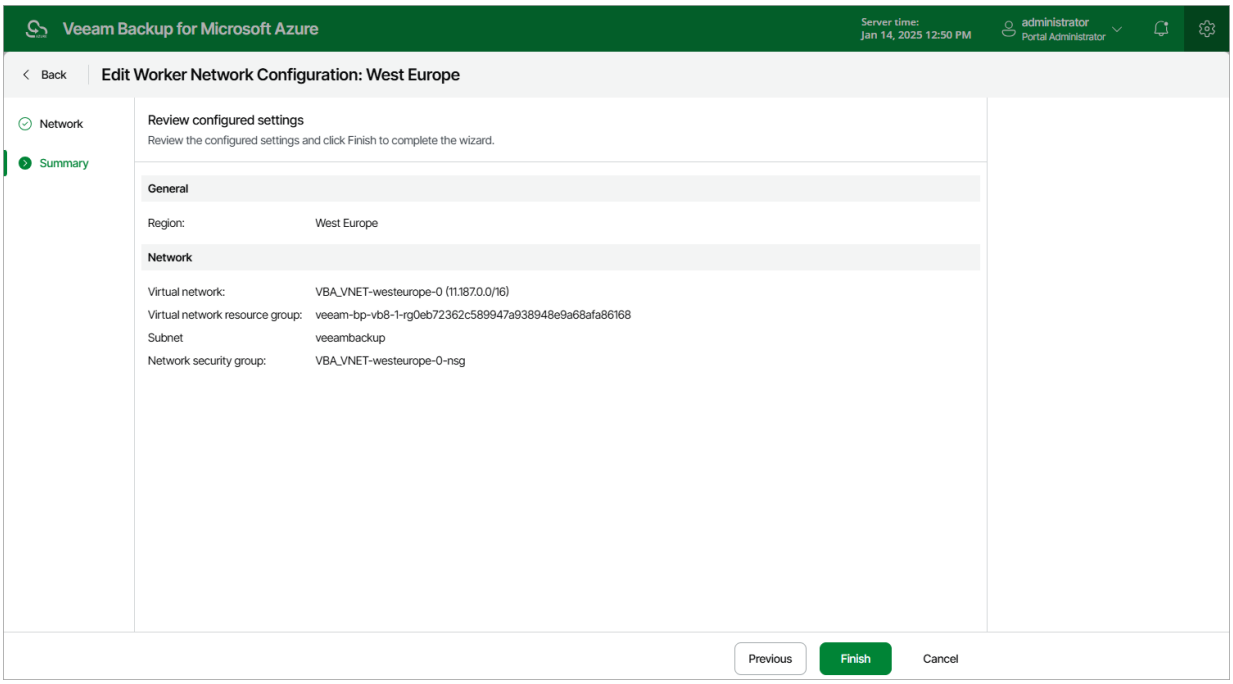



# Editing Worker Configurations

For each worker configuration, you can modify settings specified while adding the worker configuration to Veeam Backup for Microsoft Azure:

1. Switch to the **Configuration** page.
2. Navigate to **Workers** > **Network**.
3. Select the worker network configuration and click **Edit**.
4. Complete the **Edit Worker Network Configuration** wizard:
    a. To choose another virtual network and subnet for the related worker instances, and to change the security group associated with the specified subnet, follow the instructions provided in section Adding Worker Configurations (step 3).
    b. At the **Summary** step of the wizard, review configuration information and click **Finish** to confirm the changes.

> **NOTE**
>
> If there are any worker instances created based on the selected configuration that are currently involved in a backup or restore process, the changes will be applied only when the process completes.

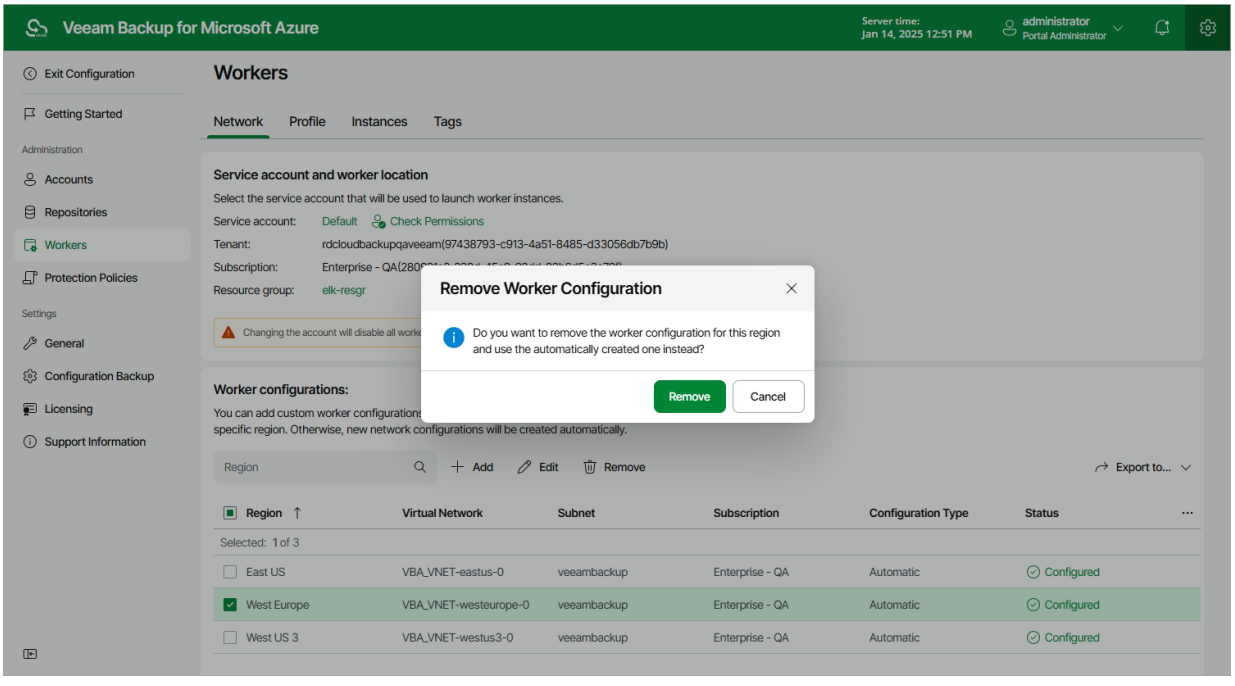



# Removing Worker Configurations

Veeam Backup for Microsoft Azure allows you to permanently remove worker configurations if you no longer need them. When you remove a worker configuration, Veeam Backup for Microsoft Azure does not remove currently running worker instances that have been created based on this configuration — these instances are removed only when the related operations complete.

To remove a worker configuration from Veeam Backup for Microsoft Azure, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **Workers** > **Network**.
3. Select the worker network configuration and click **Remove**.



# Managing Worker Profiles

A profile is the VM size of a worker instance that Veeam Backup for Microsoft Azure launches in a specific Azure region to perform a backup, restore, retention, archive, file share indexing, repository synchronization or health check operation. Veeam Backup for Microsoft Azure launches one worker instance per each Azure resource added to a backup policy or restore task.

Out of the box, Veeam Backup for Microsoft Azure comes with the default set of worker profiles where the primary profile is *Standard_F2s_v2* and the archive profile is *Standard_E2_v5*. However, to boost operational performance, you can add custom sets of worker profiles to specify VM sizes of worker instances that will operate in different regions. When configuring worker profiles, you can choose the profile of each launched worker instance depending on the performed operation and the total size of the processed data:

| Worker Profile | Default Azure VM Size | Usage |
|---|---|---|
| Small | Standard_F2s_v2 | • Backup and restore of the following workloads:<br>  ○ Azure VMs whose total disk size is less than 100 GB<br>  ○ Azure SQL databases whose total size is less than 1 GB<br>  ○ Cosmos DB for PostgreSQL clusters whose total size is less than 22 GB<br>• File-level recovery of Azure VMs<br>• Retention of backup chains whose total size is less than 100 GB, or whose length is less than 100 restore points<br>• Repository synchronization, file share indexing and health check |
| Medium | Standard_F4s_v2 | • Backup and restore of the following workloads:<br>  ○ Azure VMs whose total disk size is between 100 GB and 1 TB<br>  ○ Azure SQL databases whose total size is between 1 GB and 50 GB<br>  ○ Cosmos DB for PostgreSQL clusters whose total size is between 22 GB and 112 GB<br>• Retention of backup chains whose total size is between 100 GB and 1024 GB, or whose length is between 100 and 250 restore points |
| Large | Standard_F8s_v2 | • Backup and restore of the following workloads:<br>  ○ Azure VMs whose total disk size is more than 1 TB<br>  ○ Azure SQL databases whose total size is more than 50 GB<br>  ○ Cosmos DB for PostgreSQL clusters whose total size is more than 112 GB<br>• Retention of backup chains whose total size is more than 1024 GB, or whose length is more than 250 restore points |

| Worker Profile | Default Azure VM Size | Usage |
| --- | --- | --- |
| Archiving | Standard_E2_v5 | • Backup archiving<br>• Data retrieval operations |

# Adding Worker Profiles

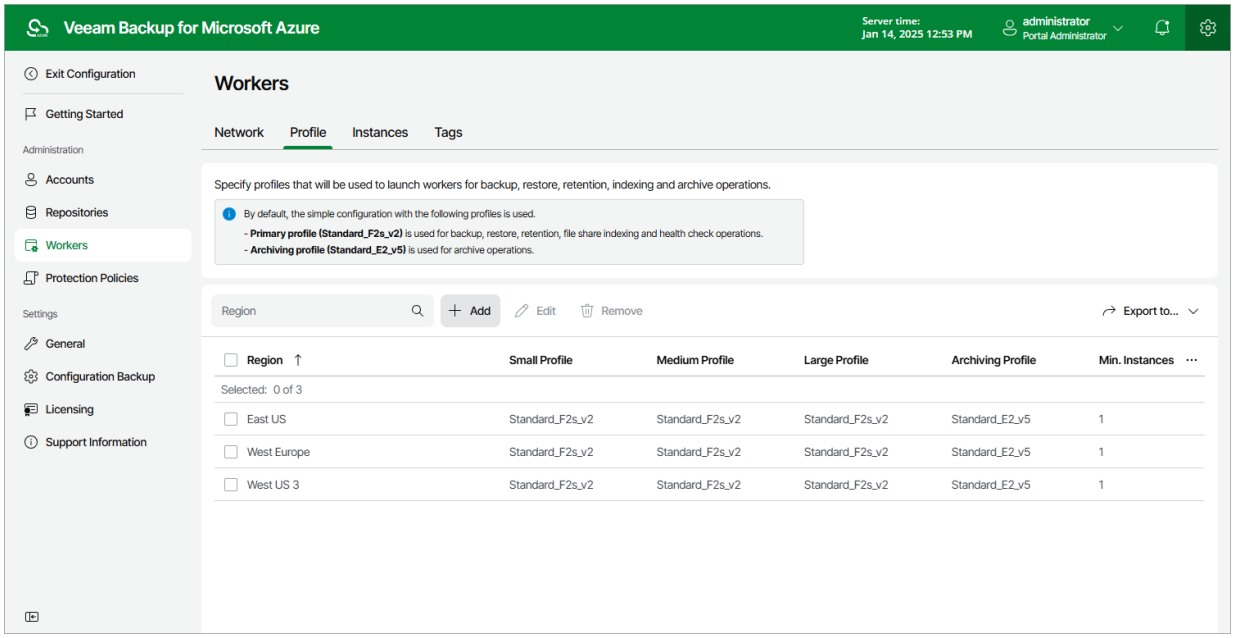
To add a new custom set of worker profiles for one or more regions, do the following:

1. Launch the Add Worker Profiles wizard.
2. Choose the necessary regions.
3. Choose the profiles for worker instances in these regions.
4. Finish working with the wizard.

# Step 1. Launch Add Worker Profiles Wizard

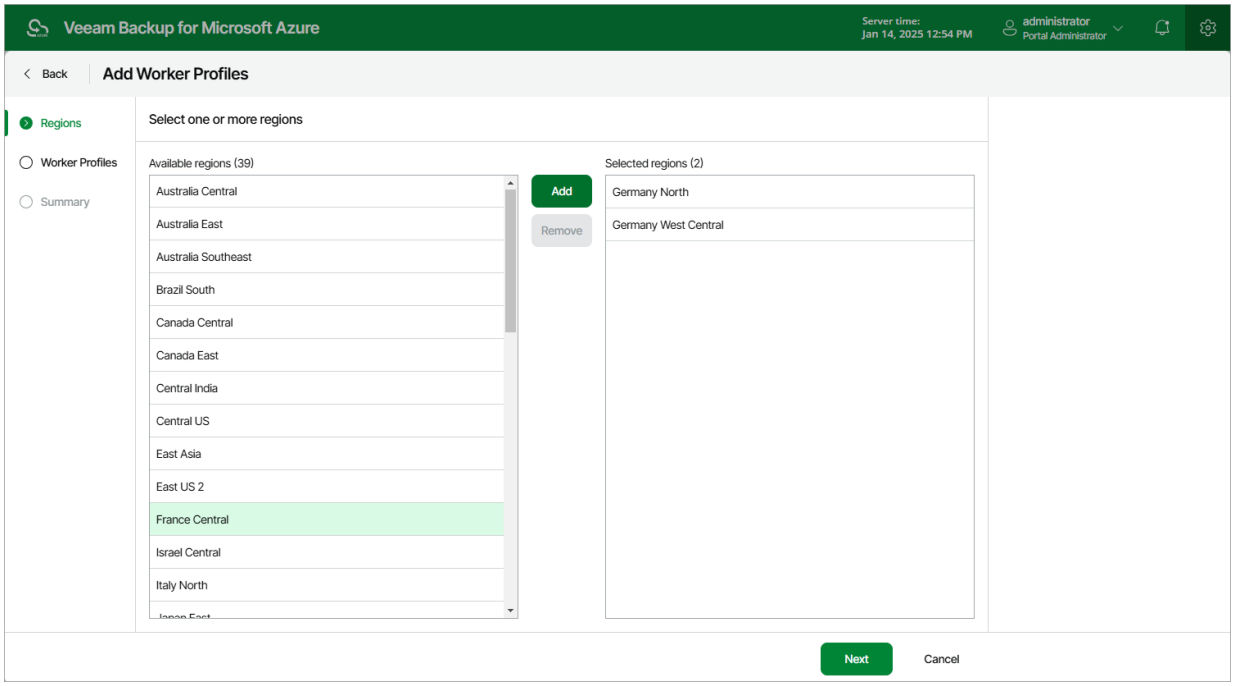
To launch the **Add Worker Profiles** wizard, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **Workers** > **Profile**.
3. Click **Add**.



# Step 2. Choose Regions

At the **Regions** step of the wizard, select regions for which you want to specify worker profiles.



## Step 3. Choose Worker Profiles

By default, Veeam Backup for Microsoft Azure launches minimum 1 and maximum 5 worker instances depending on the number of Azure resources processed while performing a backup or restore operation. Each worker instance can process only one Azure resource at a time. If the number of processed resources exceeds the maximum number of worker instances specified in the worker configuration, the resources exceeding this limit are queued.

At the **Worker Profiles** step of the wizard, you can modify the default number of worker instances to reduce the amount of processing time, and choose profiles that will be used to launch worker instances in the selected regions to boost operational performance.

1. In the **Backup operations** section, click **Edit Settings**.
2. In the **Choose worker configuration** window, do the following:
   a. Use the **Simple configuration** and **Advanced configuration** options to choose whether you want to use one single VM size for all worker instances that will be launched in the selected regions to perform backup, restore and retention operations, or to specify a small, medium and large profile for the instances.

      To help you choose VM sizes, tables in the **Select Virtual Machine Size** windows will provide information on the number of vCPU cores and the amount of system RAM for each available VM size. For the full description of Azure VM sizes, see Microsoft Docs.

   b. In the **Minimum workers** and **Maximum workers** fields, specify the minimum and the maximum number of worker instances that Veeam Backup for Microsoft Azure will launch and use simultaneously to process Azure resources in the selected regions during backup and restore operations after you finish working with the wizard.

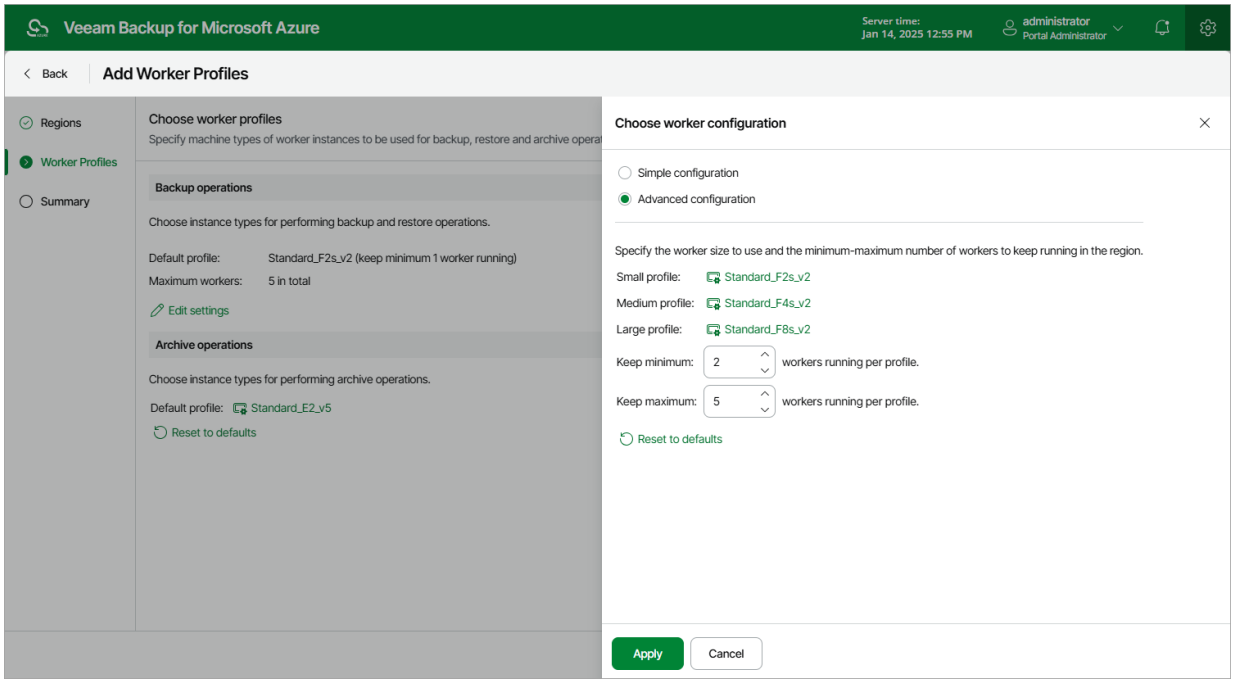
      Consider that both the minimum and the maximum numbers are specified per profile.

> **TIP**
>
> After a backup or restore operation completes, Veeam Backup for Microsoft Azure keeps the minimum number of worker instances running for 10 minutes and then deallocates them; the other instances are automatically removed from the backup infrastructure. To optimize infrastructure costs, set the minimum number of worker instances to *0*.

   c. To save changes made to the worker profiles, click **Apply**.

3. In the **Archive operations** section, click the link in the **Default profile** field to specify a VM size for worker instances that will be launched in the selected regions to perform archive operations.

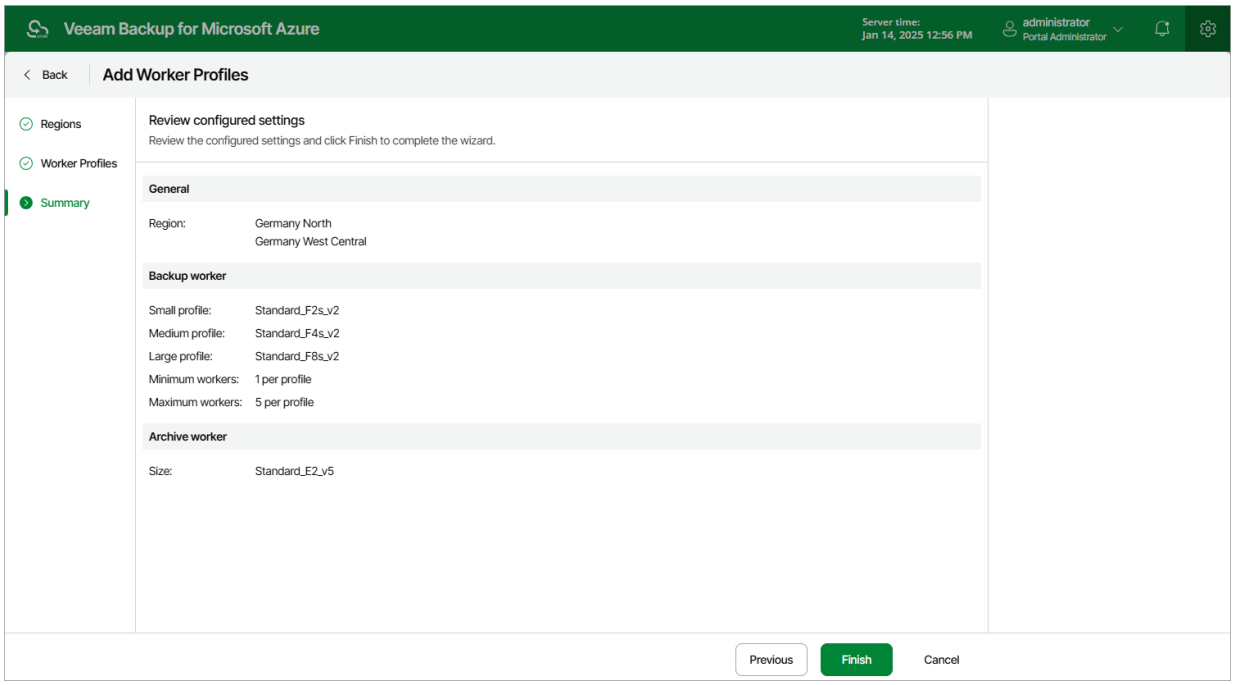
   To help you choose the VM size, the table in the **Select Virtual Machine Size** window will provide information on the number of vCPU cores and the amount of system RAM for each available VM size. For the full description of Azure VM sizes, see Microsoft Docs.



## Step 4. Finish Working with Wizard

At the **Summary** step of the wizard, review summary information and click **Finish**.

As soon as you click **Finish**, Veeam Backup for Microsoft Azure will create a separate set of worker profiles for each of the selected regions.

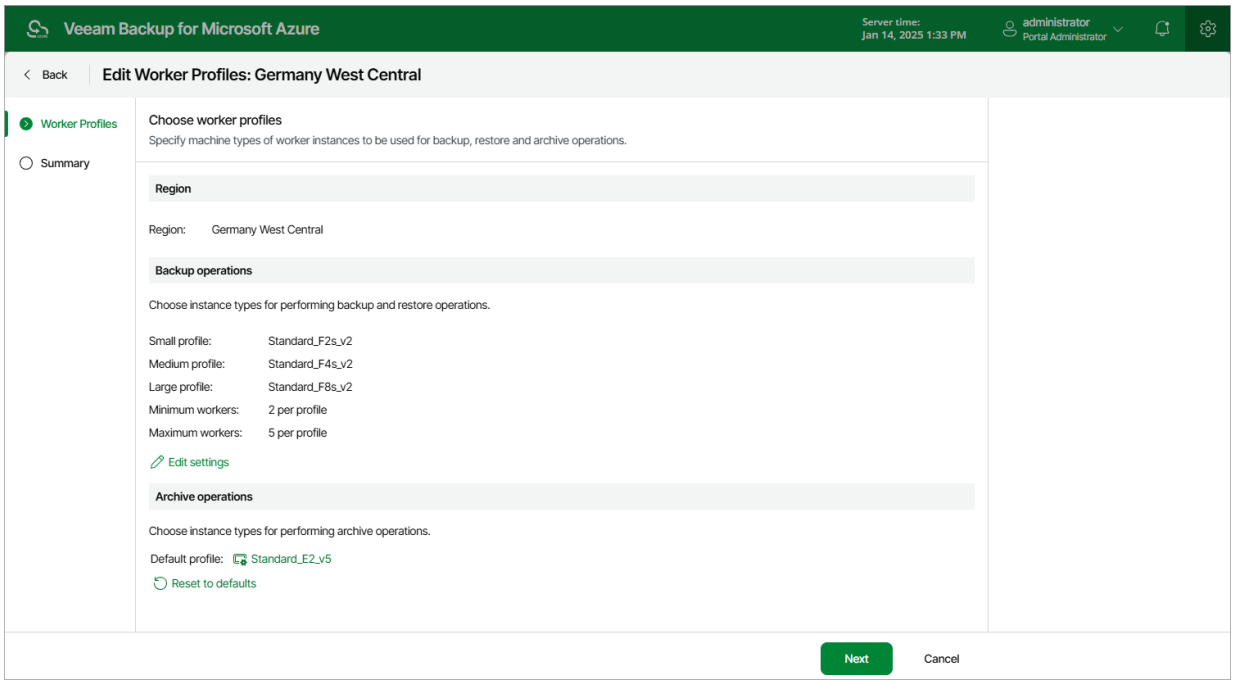



# Editing Worker Profiles

For each set of worker profiles created for an Azure region, you can modify settings specified while creating the profile set:

1. Switch to the **Configuration** page.
2. Navigate to **Workers** > **Profile**.
3. Select the profile set and click **Edit**.
4. Complete the **Edit Worker Profiles** wizard:
    a. To change profiles that will be used to launch worker instances in the selected region, follow the instructions provided in section Adding Worker Profiles (step 3).
    b. At the **Summary** step of the wizard, review configuration information and click **Finish** to confirm the changes.

> **NOTE**
>
> If there are any worker instances that are currently involved in a backup, restore or archive process in the selected region, the changes will be applied only when the process completes.




# Removing Worker Profiles

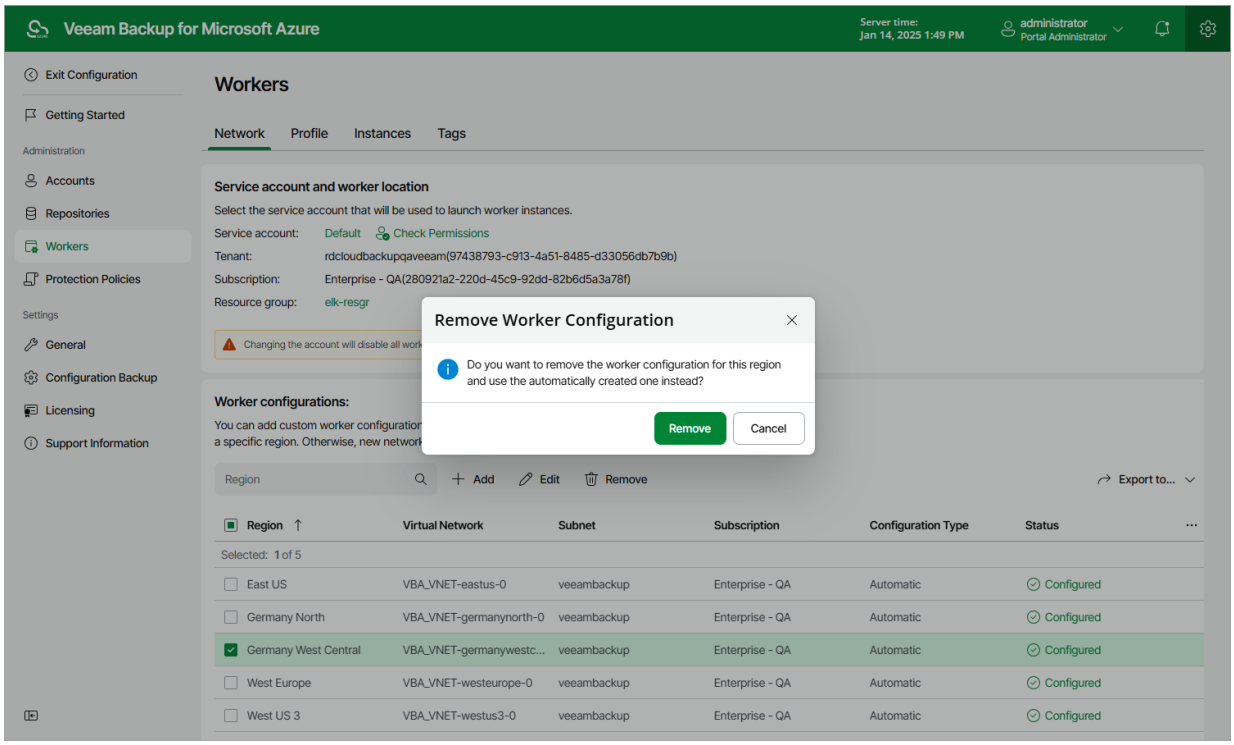
Veeam Backup for Microsoft Azure allows you to permanently remove sets of worker profiles if you no longer need them.

> **NOTE**
>
> You cannot remove a profile set if any worker instances that have been created based on this set are currently running. Wait for all the related operations to complete — and then try removing the profile set again.

To remove a profile set from Veeam Backup for Microsoft Azure, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **Workers** > **Profile**.

3. Select the profile set and click **Remove**.



# Adding Worker Instance Tags

For all worker instances that are launched in specific Azure subscriptions for the duration of backup, restore and retention processes, you can assign custom Azure tags, which may help you differentiate worker instances that have the same or similar names:

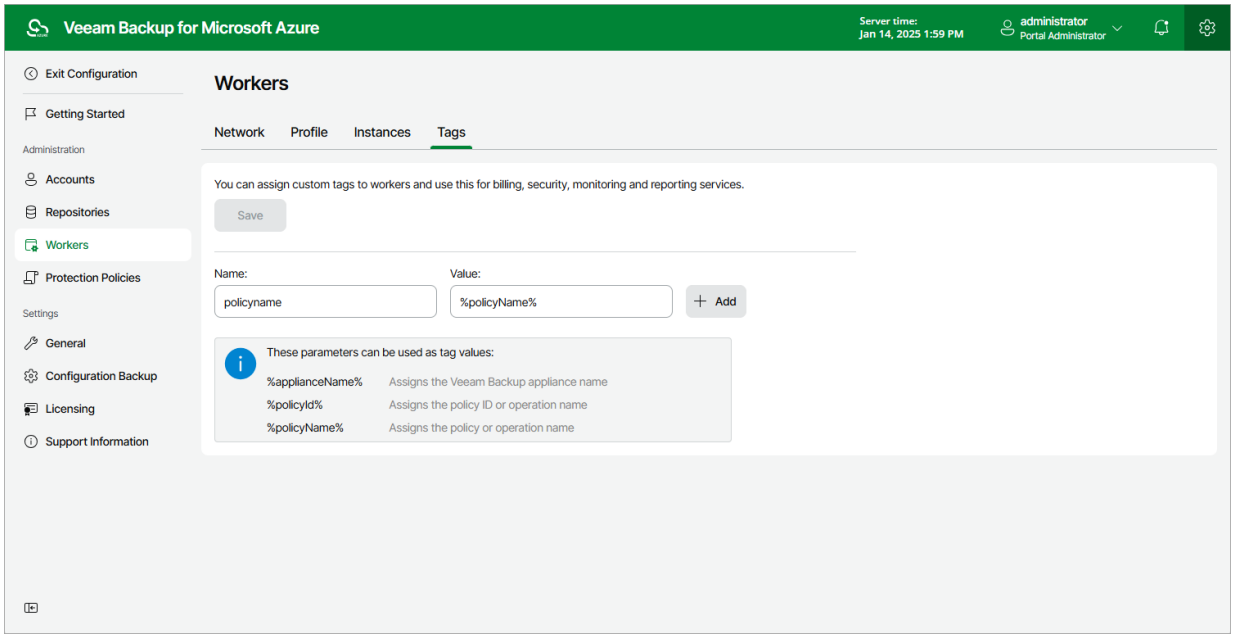
1. Switch to the **Configuration** page.
2. Navigate to **Workers** > **Tags**.
3. Use the **Key** and **Value** fields to specify a key and a value for a new custom Azure tag, and then click **Add**. Note that you cannot add more than 50 custom Azure tags.

   Consider the following limitations:

   - The maximum length of the tag key is 128 characters.
   - The maximum length of the tag value is 256 characters.
   - The following characters are not supported: < > # % + & \ ? / .

   For more information on tag limitations, see Microsoft Docs.
4. Click **Save**.

> **TIP**
>
> You can use a number of runtime variables as tag values to allow Veeam Backup for Microsoft Azure for worker instances launched during data protection operations. However, for worker instances deployed during restore operations, retention tasks and configuration checks, the values of the *%policyid%* and *%policyName%* variables will be replaced with operation names.



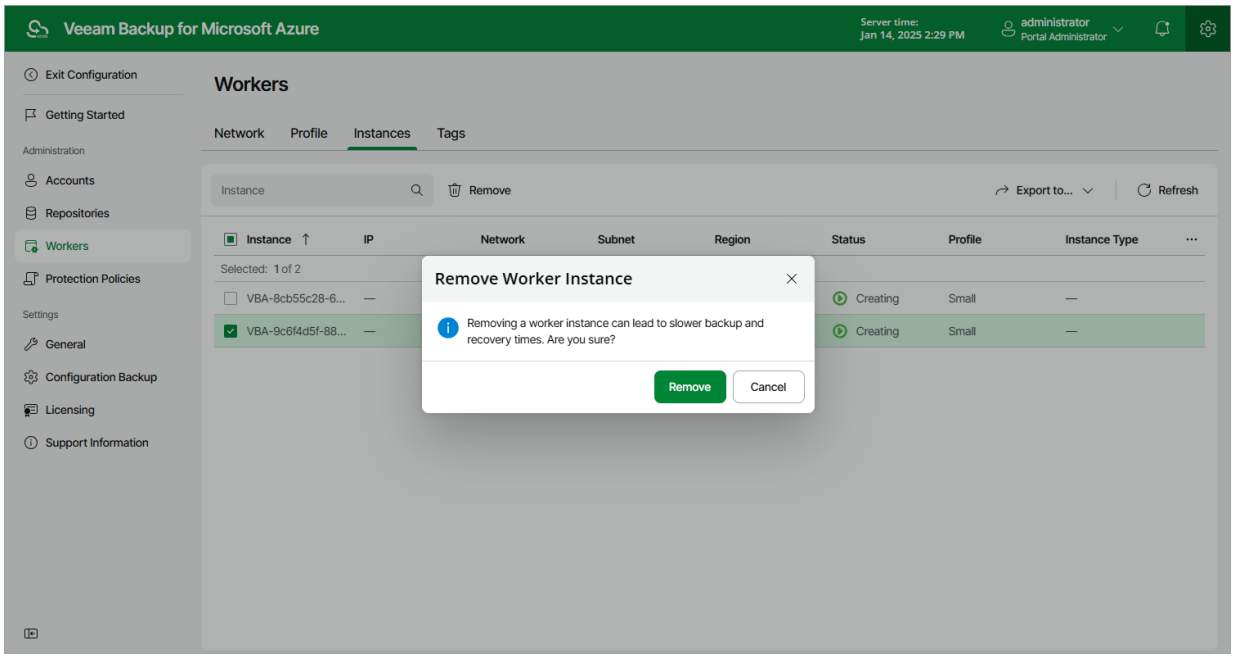
# Removing Worker Instances

Veeam Backup for Microsoft Azure allows you to permanently remove worker instances created based on worker configurations and profiles if you no longer need them.

To remove a worker instance from Veeam Backup for Microsoft Azure, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **Workers** > **Instances**.
3. Select the worker instance and click **Remove**.

> **NOTE**
>
> If the selected worker instance is currently involved in a backup or restore process, it will be removed only when the process completes.



# Managing SLA and Storage Templates

Veeam Backup for Microsoft Azure allows you to simplify data protection and monitor compliance with your target SLA by configuring SLA-based backup policies. An SLA-based backup policy is a collection of settings that automate the way backup operations are performed: how frequently to run the backup process, what region-specific repositories to use to store backups, how many restore points should be created in time to meet SLA requirements, and so on.

To configure an SLA-based backup policy, you must first add an SLA template and a storage template to your backup appliance.

# Managing SLA Templates

An SLA template is a collection of settings that allows you to protect your data according to a periodic backup schedule (regularly, within a backup window) in a way the data protection complies with SLA standards in your company. One SLA template can be assigned to one or more SLA-based backup policies. For more information, see SLA Templates.

## Adding SLA Templates

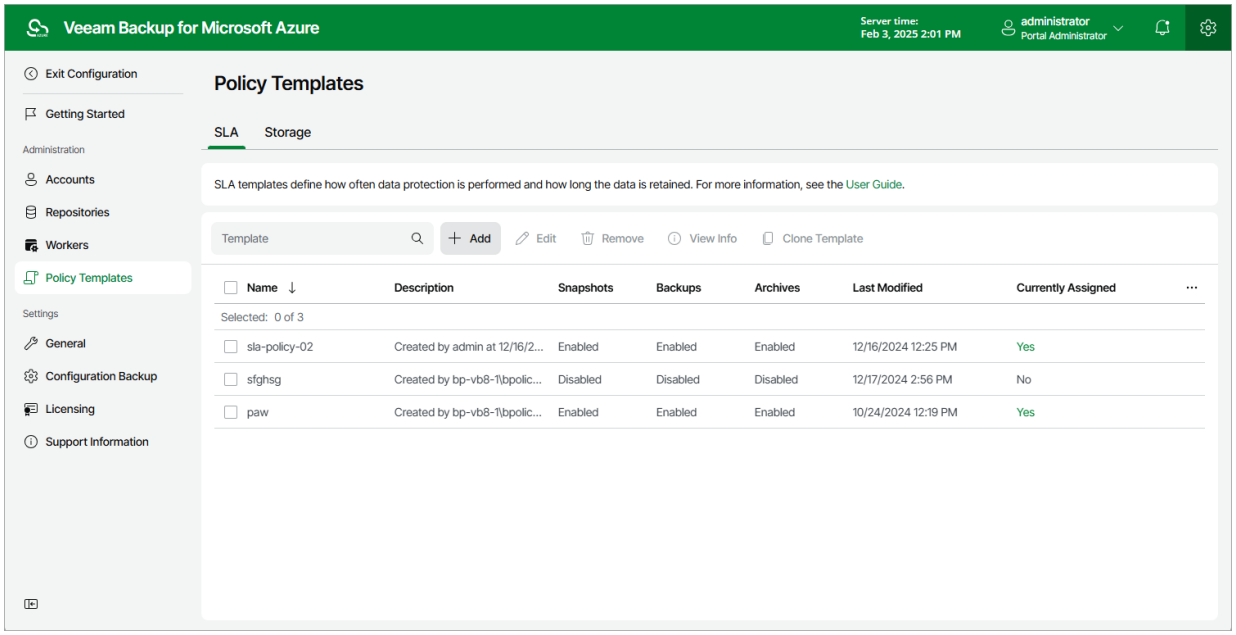
To add an SLA template, do the following:

1. Launch the Add SLA Template wizard.
2. Specify a template name and description.
3. Configure snapshot settings.
4. Configure backup settings.
5. Specify an SLA threshold and configure health check settings.
6. Finish working with the wizard.

# Step 1. Launch Add SLA Template Wizard

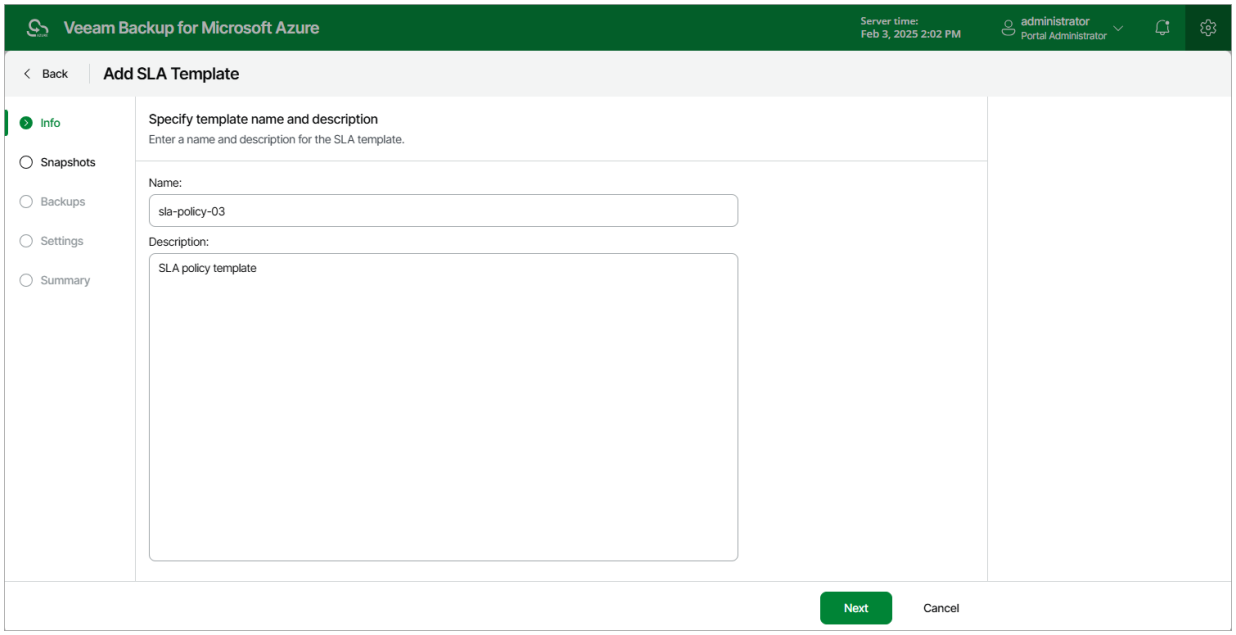
To launch the **Add SLA Template** wizard, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **Policy Templates** > **SLA**.
3. Click **Add**.



# Step 2. Specify Template Name

At the **Info** step of the wizard, use the **Name** and **Description** fields to enter a name for the new SLA template and to provide a description for future reference. The maximum length of the name is 255 characters. The following characters are not supported: / \ " ' : | < > + = ; , ? ! * % # ^ @ & $ .



# Step 3. Configure Snapshot Settings

At the **Snapshots** step of the wizard, you can configure the following snapshot settings:

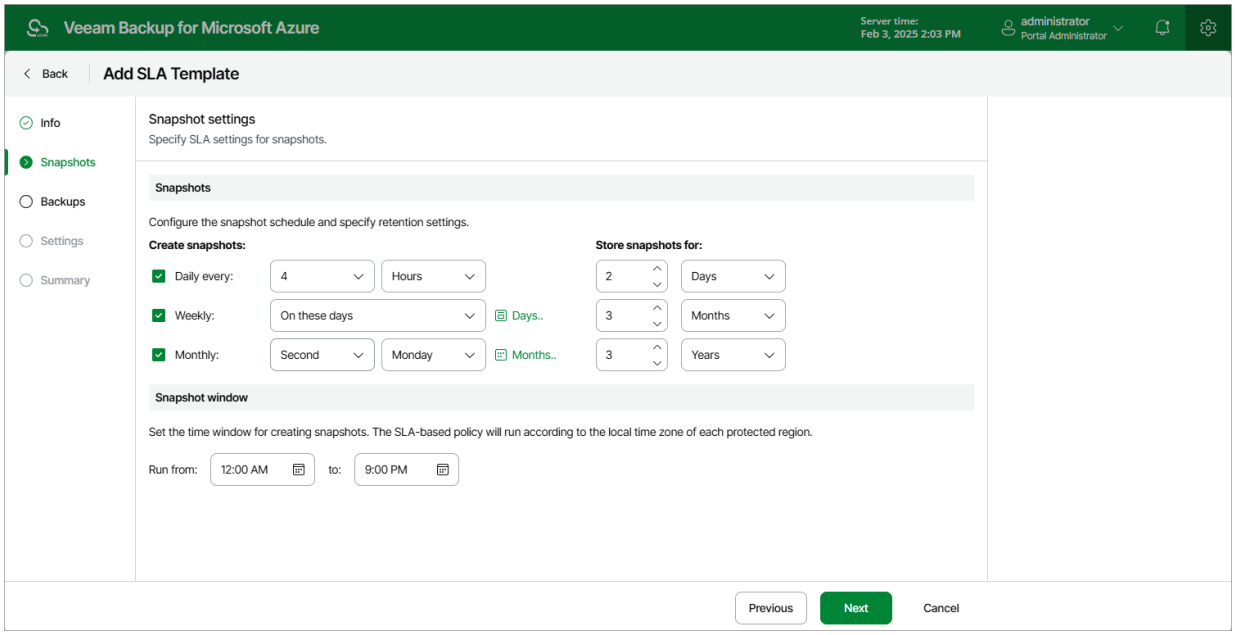
1. In the **Snapshots** section, you can instruct Veeam Backup for Microsoft Azure to create cloud-native snapshots on a daily, weekly and monthly basis, and to keep the created snapshots in a snapshot chain for a specific number of days, months or years. If a snapshot is older than the specified time limit, Veeam Backup for Microsoft Azure removes the snapshot from the chain.

   Note that if you configure a schedule but do not select the corresponding check box, Veeam Backup for Microsoft Azure will ignore the specified settings and will not create snapshots according to this schedule.

2. In the **Snapshot window** section, you can instruct Veeam Backup for Microsoft Azure to create daily snapshots within a specific time interval if you do not want backup operations to overlap production hours.

   Veeam Backup for Microsoft Azure automatically adjusts the specified snapshot window to the time zone of each region added to all SLA-based backup policies that have this SLA template assigned. For more information, see Data Protection Windows.

When you combine multiple types of snapshot schedules, Veeam Backup for Microsoft Azure re-uses snapshots created according to a more-frequent schedule (daily or weekly) to achieve the desired SLA compliance for less-frequent schedules (weekly and monthly). For example, if you configure a daily and a monthly schedule, the first snapshot successfully created according to the daily schedule will be marked as both a daily and a monthly snapshot.



## Step 4. Configure Backup Settings

At the **Backups** step of the wizard, you can configure the following backup settings:

1. In the **Backups** section, you can instruct Veeam Backup for Microsoft Azure to create backups on a daily, weekly and monthly basis, and to keep the created backups in a backup chain for a specific number of days, months or years. If a backup is older than the specified time limit, Veeam Backup for Microsoft Azure removes the backup from the chain.

   Note that if you configure a schedule but do not select the corresponding check box, Veeam Backup for Microsoft Azure will ignore the specified settings and will not create backups according to this schedule.

> **TIP**
>
> Veeam Backup for Microsoft Azure allows you to quickly configure a backup schedule by applying the same settings that you have configured at step 3 of the wizard. To do that, click **Copy Snapshot Schedule**.
>
> However, keep in mind that snapshot schedules do not affect backup schedules, meaning that cloud-native snapshots do not participate in the process of producing image-level backups. To produce backups, Veeam Backup for Microsoft Azure takes temporary restore points but then automatically removes these points based on their own retention settings. For more information, see Temporary Restore Points.

2. In the **Changed block tracking** section, you can enable the changed block tracking (CBT) mechanism that allows Veeam Backup for Microsoft Azure to reduce the amount of data read from processed Azure VMs.

   Enabling CBT increases the speed and efficiency of backup operations but can incur additional costs of storing restore points in Microsoft Azure. For more information, see SLA Templates.

3. In the **Archives** section, you can instruct Veeam Backup for Microsoft Azure to store backed-up data in the low-cost, long-term Archive access tier, and to keep the archived data for a specific time period.

   Note that it is usually more expensive and takes more time to restore data from archived backups than from regular backups as it requires Veeam Backup for Microsoft Azure to retrieve the data from the Archive access tier. For more information, see Retrieving Data From Archive.

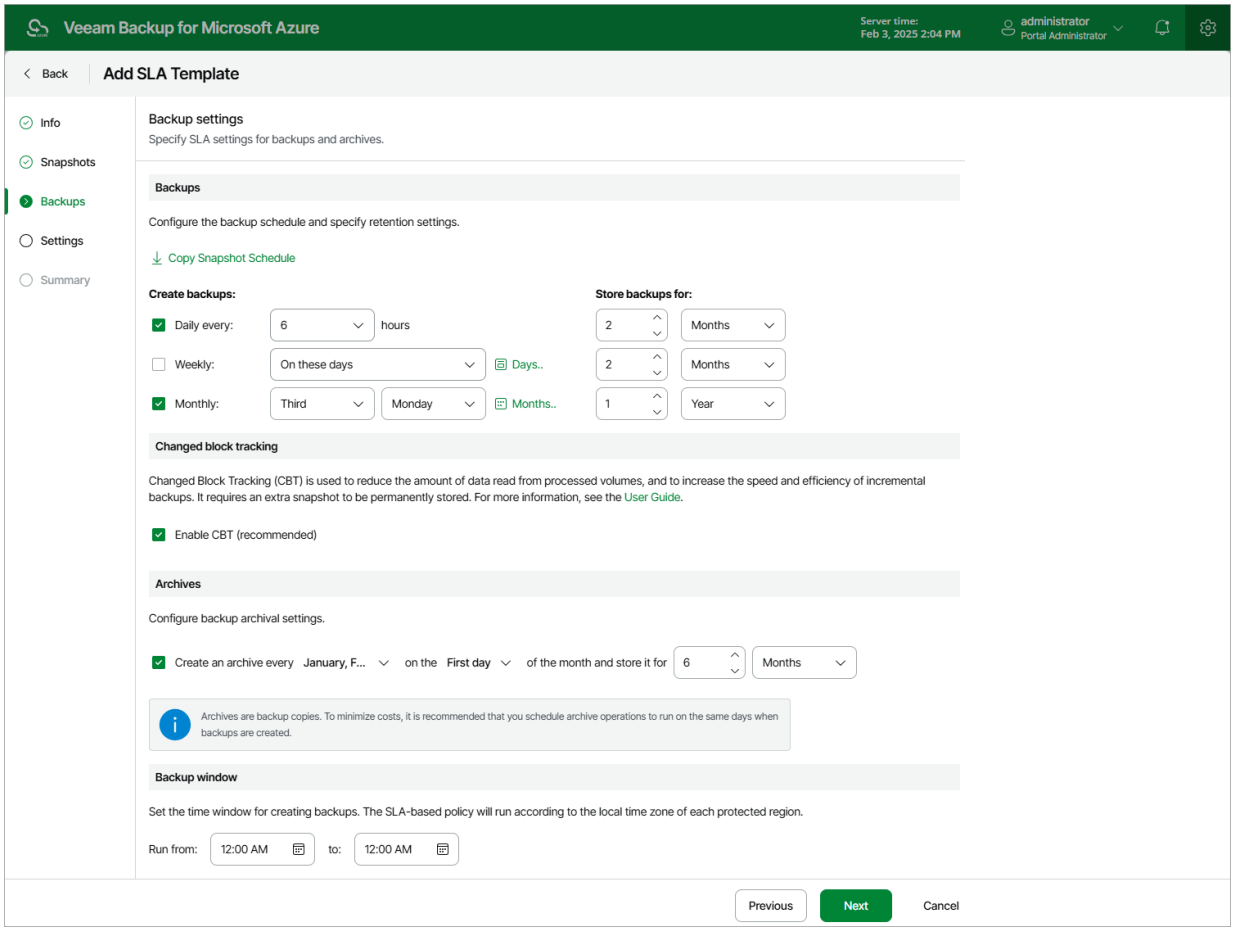
4. In the **Backup window** section, you can instruct Veeam Backup for Microsoft Azure to create daily backups within a specific time interval if you do not want backup operations to overlap production hours.

   Veeam Backup for Microsoft Azure automatically adjusts the specified backup window to the time zone of each region added to SLA-based backup policies that have this SLA template assigned. For more information, see Data Protection Windows.

   Since Veeam Backup for Microsoft Azure runs retention sessions for the related SLA-based backup policies as soon as it finalizes the backup window in all protected regions, it is recommended that you estimate how long it may take Veeam Backup for Microsoft Azure to complete these retention sessions first (the larger the infrastructure, the longer the retention sessions run) before you configure a backup window. Otherwise, Veeam Backup for Microsoft Azure may encounter throttling issues when trying to remove obsolete data from backup repositories.

> **TIP**
>
> In large environments, it is recommended that you configure separate windows for backups and snapshots to optimize backup performance and decrease the load on your infrastructure.

When you combine multiple types of backup schedules, Veeam Backup for Microsoft Azure re-uses backups created according to a more-frequent schedule (daily or weekly) to achieve the desired SLA compliance for less-frequent schedules (weekly and monthly). For example, if you configure a daily and a monthly schedule, the first backup successfully created according to the daily schedule will be marked as both a daily and a monthly backup.



## Step 5. Configure Template General Settings

At the **Settings** step of the wizard, you can specify SLA threshold settings and schedule health checks for the SLA template.

# SLA Threshold Settings

The SLA threshold is a percentage of successfully created restore points out of the total number of restore points expected to be produced by an SLA-based backup policy (97% by default). Based on this percentage, Veeam Backup for Microsoft Azure estimates the SLA compliance ratio for all SLA-based backup policies that have this SLA template assigned. For more information, see How Veeam Backup for Microsoft Azure Estimates SLA Compliance.

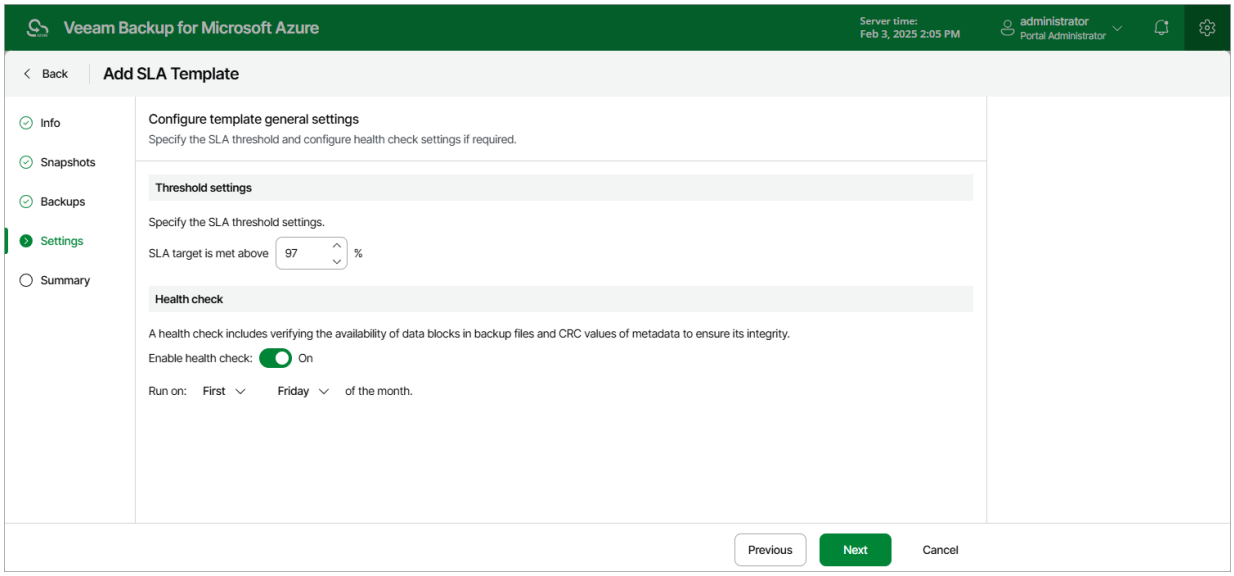
# Health Check Settings

If you have configured a backup schedule at step 4 of the wizard, you can instruct Veeam Backup for Microsoft Azure to periodically perform a health check for backup restore points created by all SLA-based backup policies that have this SLA template assigned. During the health check, Veeam Backup for Microsoft Azure performs an availability check for data blocks in the whole regular backup chain, and a cyclic redundancy check (CRC) for metadata to verify its integrity. The health check helps you ensure that the restore points are consistent and that you will be able to restore data using these restore points. For more information on the health check, see How Health Check Works.

To instruct Veeam Backup for Microsoft Azure to perform a health check, do the following:

1. In the **Health check** section of the step, set the **Enable health check** toggle to *On*.
2. Use the **Run on** drop-down lists to schedule a specific day for the health check to run.

> **NOTE**
>
> Veeam Backup for Microsoft Azure performs the health check regardless of the configured backup schedule. By default, the health check runs on a monthly basis — if you want to instruct Veeam Backup for Microsoft Azure to run it on a weekly basis, open a support case.



## How Health Check Works

When Veeam Backup for Microsoft Azure saves a new backup restore point to a backup repository, it calculates CRC values for metadata in the backup chain and saves these values to the chain metadata, together with the instance data. When performing a health check, Veeam Backup for Microsoft Azure verifies the availability of data blocks and uses the saved values to ensure that the restore points being verified are consistent.

If you have enabled health checks for the backup policy, Veeam Backup for Microsoft Azure performs the following operations at the day scheduled for a health check to run:

1. As soon as a backup policy session completes successfully, Veeam Backup for Microsoft Azure starts the health check as a new session. For each restore point in the standard backup chain, Veeam Backup for Microsoft Azure calculates CRC values for backup metadata and compares them to the CRC values that were previously saved to the restore point. Veeam Backup for Microsoft Azure also checks whether data blocks that are required to rebuild the restore point are available.

   If the backup policy session completes with an error, Veeam Backup for Microsoft Azure tries to run the backup policy again, taking into account the maximum number of retries specified in the automatic retry settings. After the first successful retry (or after the last one out of the maximum number of retries), Veeam Backup for Microsoft Azure starts the health check.

2. If Veeam Backup for Microsoft Azure does not detect data inconsistency, the health check session completes successfully. Otherwise, the session completes with an error.

   Depending on the detected data inconsistency, Veeam Backup for Microsoft Azure performs the following operations:

   - If the health check detects corrupted metadata in a full or incremental restore point, Veeam Backup for Microsoft Azure marks the backup chain as corrupted in the configuration database. During the next backup policy session, Veeam Backup for Microsoft Azure copies the full instance image, creates a full restore point in the backup repository and starts a new backup chain in the backup repository.

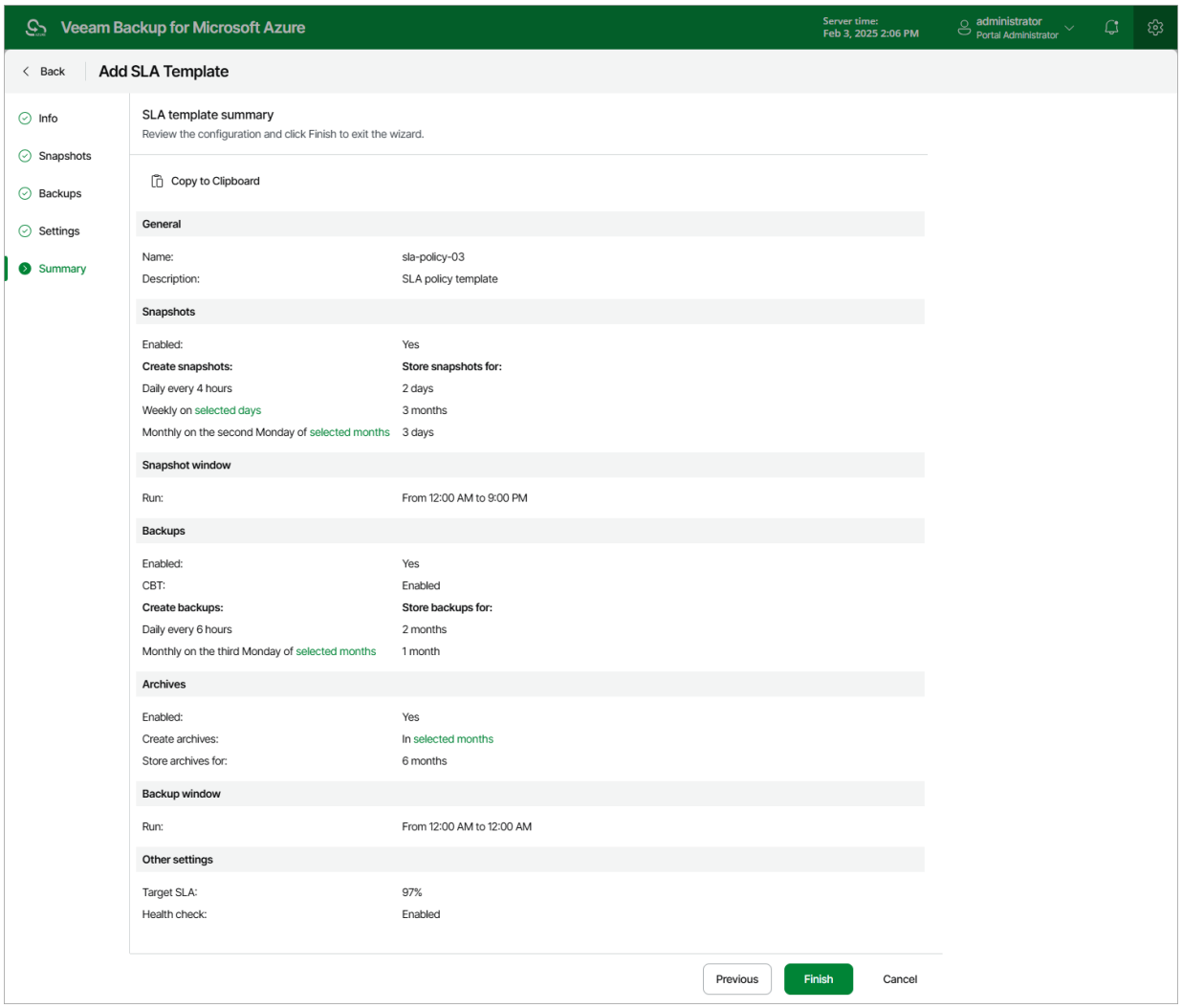
> **NOTE**
>
> Veeam Backup for Microsoft Azure does not support metadata check for encrypted backup chains.

   - If the health check detects corrupted disk blocks in a full or an incremental restore point, Veeam Backup for Microsoft Azure marks the restore point that includes the corrupted data blocks and all subsequent incremental restore points as incomplete in the configuration database. During the next backup policy session, Veeam Backup for Microsoft Azure copies not only those data blocks that have changed since the previous backup session but also data blocks that have been corrupted, and saves these data blocks to the latest restore point that has been created during the current session.

## Step 6. Finish Working with Wizard

At the **Summary** step of the wizard, review summary information and click **Finish**.

> **TIP**
>
> After you create an SLA template and assign it to a number of SLA-based backup policies as described in section Performing Backup Using Web UI, you will be able to see the full list of all the related policies on the **SLA** page. To do that, select the necessary template and click the link in the **Currently Assigned** column.




# Editing SLA Templates

For each SLA template, you can modify settings configured while creating the template:

1. Switch to the **Configuration** page.
2. Navigate to **Policy Templates** > **SLA** and click **Edit**.
3. Complete the **Edit SLA Template** wizard:
    a. To provide a new name and description for the template, follow the instructions provided in section Adding SLA Templates (step 2).

b. To modify the configured snapshot settings, follow the instructions provided in section Adding SLA Templates (step 3).

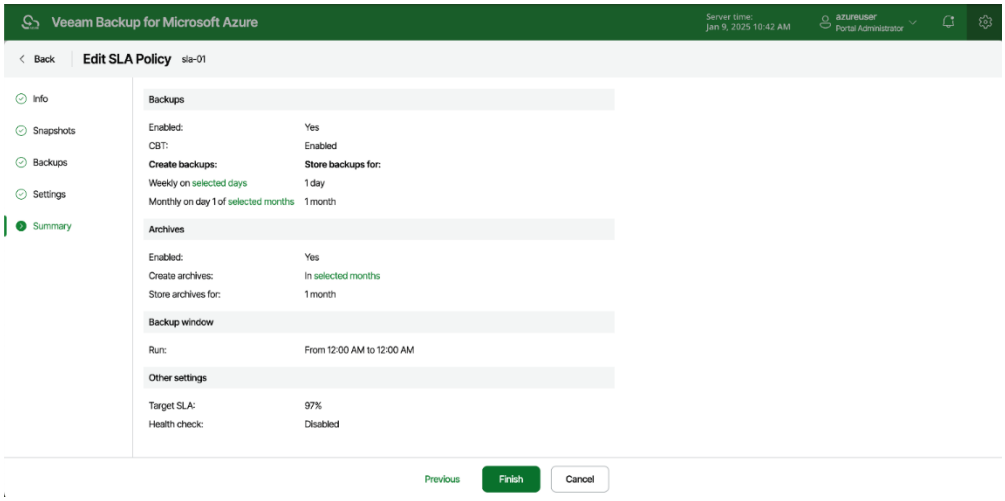
c. To modify the configured backup settings, follow the instructions provided in section Adding SLA Templates (step 4).

d. To adjust the target SLA value and change the health check schedule for the template, follow the instructions provided in section Adding SLA Templates (step 5).

e. At the **Summary** step of the wizard, review configuration information and click **Finish** to confirm the changes.

> **TIP**
>
> After you click **Finish**, Veeam Backup for Microsoft Azure will update the timestamp in the **Last Modified** column on the **SLA** page, regardless of whether you have actually modified the template settings or not. If you want to simply view the configured settings without making any changes, click **View Info**.

Note that modifying snapshot and backup settings for SLA templates that are already assigned to SLA-based backup policies may cause Veeam Backup for Microsoft Azure to incorrectly calculate the SLA compliance ratio for these policies on the day when this modification is made. For more information on how Veeam Backup for Microsoft Azure estimates SLA compliance, see Viewing SLA-Based Backup Policy Details.



# Managing Storage Templates

A storage template is a collection of settings that allows you to define target locations (that is, repositories where Veeam Backup for Microsoft Azure keeps restore points produced by SLA-based backup policies) for backups and archived backups. One storage template can be assigned to one or more SLA-based backup policies. For more information, see Storage Templates.

## Adding Storage Templates

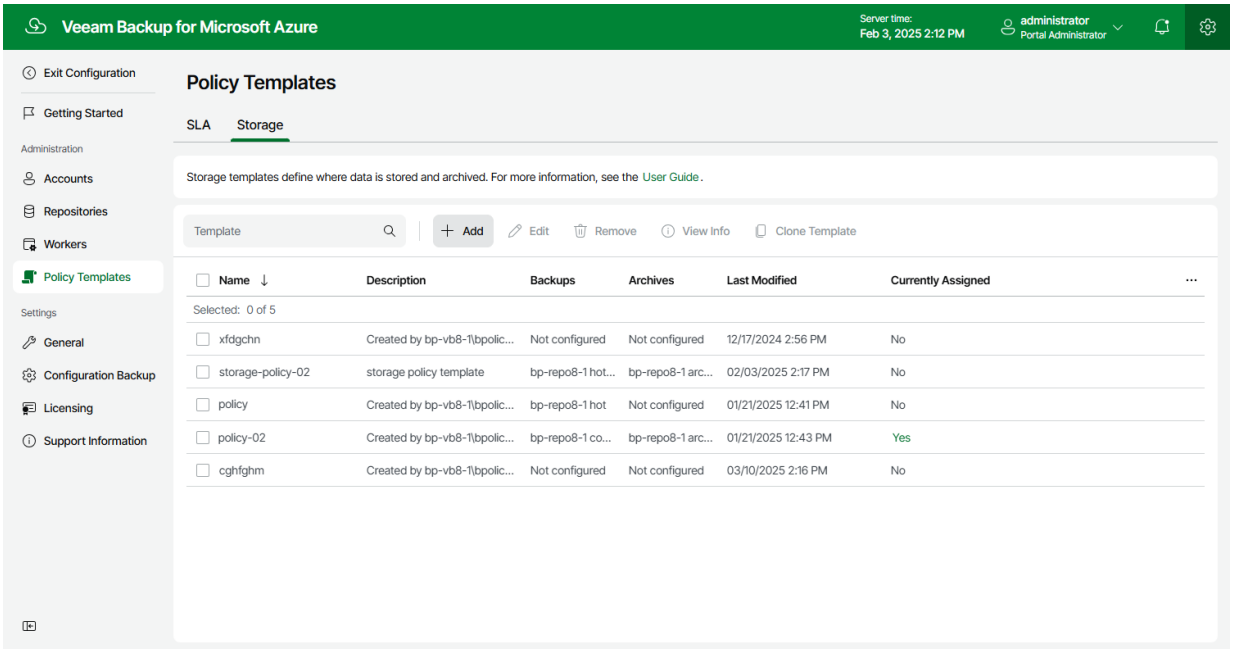
To add a storage template, do the following:

1. Launch the Add Storage Template wizard.
2. Specify a template name and description.
3. Configure target location settings.
4. Finish working with the wizard.

# Step 1. Launch Add Storage Template Wizard

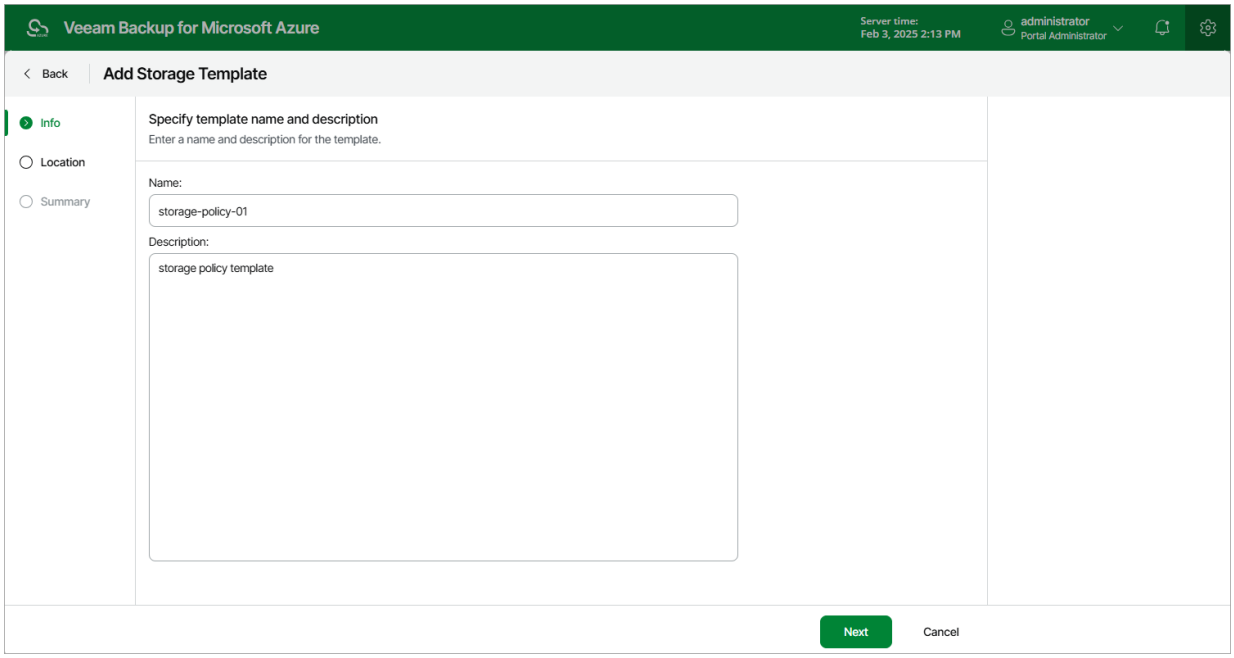
To launch the **Add Storage Template** wizard, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **Policy Templates** > **Storage**.
3. Click **Add**.



# Step 2. Specify Template Name

At the **Info** step of the wizard, use the **Name** and **Description** fields to enter a name for the new storage template and to provide a description for future reference. The maximum length of the name is 255 characters. The following characters are not supported: / \ " ' : | < > + = ; , ? ! * % # ^ @ & $ .



## Step 3. Configure Location Settings

At the **Location** step of the wizard, you can specify target locations where Veeam Backup for Microsoft Azure will keep restore points produced by all SLA-based backup policies that will have this storage template assigned.

By design, Veeam Backup for Microsoft Azure 8 stores cloud-native snapshots produced by SLA-based backup policies in the same Azure regions where the source VMs reside — snapshots created for Azure VMs with managed disks are saved to the same resource groups to which the source VMs belong, while snapshots created for Azure VMs with unmanaged disks are saved to the same Azure storage account where these disks reside. This means that the current version of Veeam Backup for Microsoft Azure does not allow you to choose another target location for cloud-native snapshots; however, you can choose target locations for image-level backups and archived backups.

> **NOTE**
>
> Unmanaged disks will be retired in Microsoft Azure on September 30, 2025. That is why it is recommended that you migrate your Azure VMs to managed disks. For more information, see Microsoft Docs.

To configure location settings for the storage template, do the following:

1. Specify a target location (backup repository) where image-level backups will be stored. To do that, click the link in the **Backups** section. Then, select the necessary repository from the **Default repository** drop-down list in the **Backup repository settings** window.

   By default, Veeam Backup for Microsoft Azure will use the selected repository for all protected regions. To instruct Veeam Backup for Microsoft Azure to use separate repositories for each region:

   a. Set the **Configure region-specific repositories** toggle to *On*.

   b. In the **Region-specific backup repository settings** section, click **Add Region**.

   c. In the **Configure Region Settings** window, choose a region and a repository that you want to use for this region.

   For a backup repository to be displayed in the list of available repositories, it must be added to Veeam Backup for Microsoft Azure as described in section Managing Backup Repositories. If you have not added the repository to Veeam Backup for Microsoft Azure beforehand, you can do it without closing the **Select Repository** and **Configure Region Settings** windows. To do that, click **Add** and complete the **Add Repository** wizard.

2. Specify a target location (archive repository) where archived backups will be stored. To do that, click the link in the **Archives** section. Then, select the necessary repository from the **Default repository** drop-down list in the **Archive repository settings** window.

   By default, Veeam Backup for Microsoft Azure will use the selected repository for all protected regions. To instruct Veeam Backup for Microsoft Azure to use separate repositories for each region:

   a. Set the **Configure region-specific repositories** toggle to *On*.

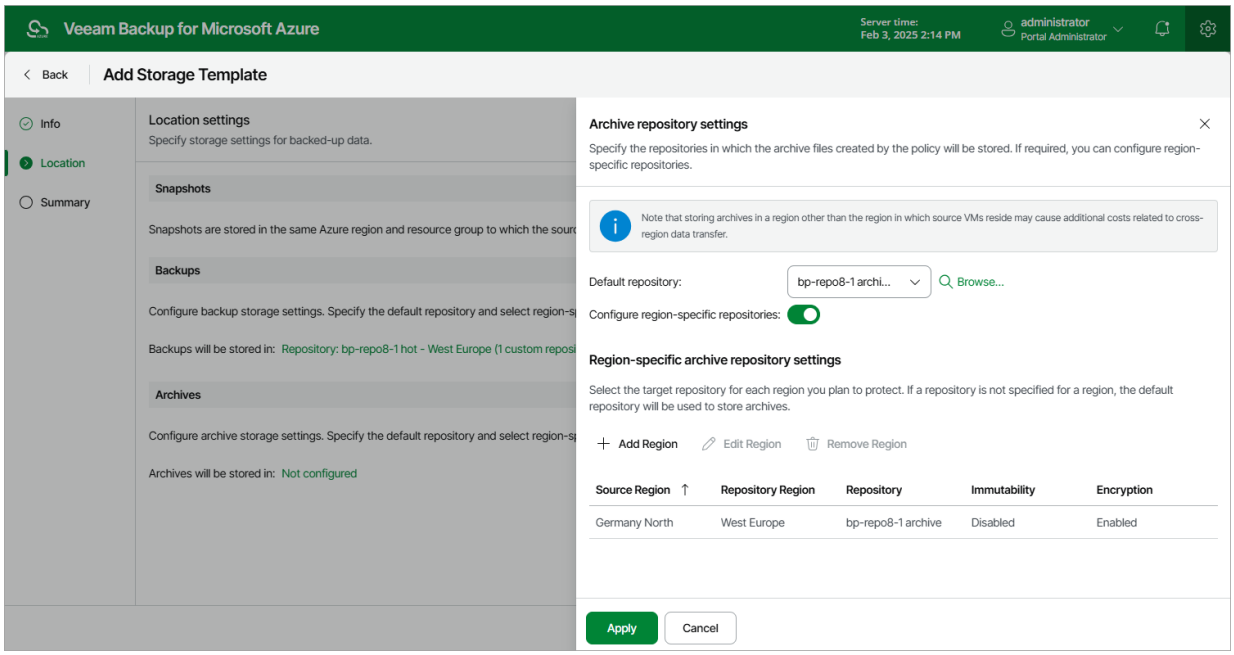
   d. In the **Region-specific archive repository settings** section, click **Add Region**.

   e. In the **Configure Region Settings** window, choose a region and a repository that you want to use for this region.

   For an archive repository to be displayed in the list of available repositories, it must be added to Veeam Backup for Microsoft Azure as described in section Managing Backup Repositories. If you have not added the repository to Veeam Backup for Microsoft Azure beforehand, you can do it without closing the **Select Repository** and **Configure Region Settings** windows. To do that, click **Add** and complete the **Add Repository** wizard.

## IMPORTANT

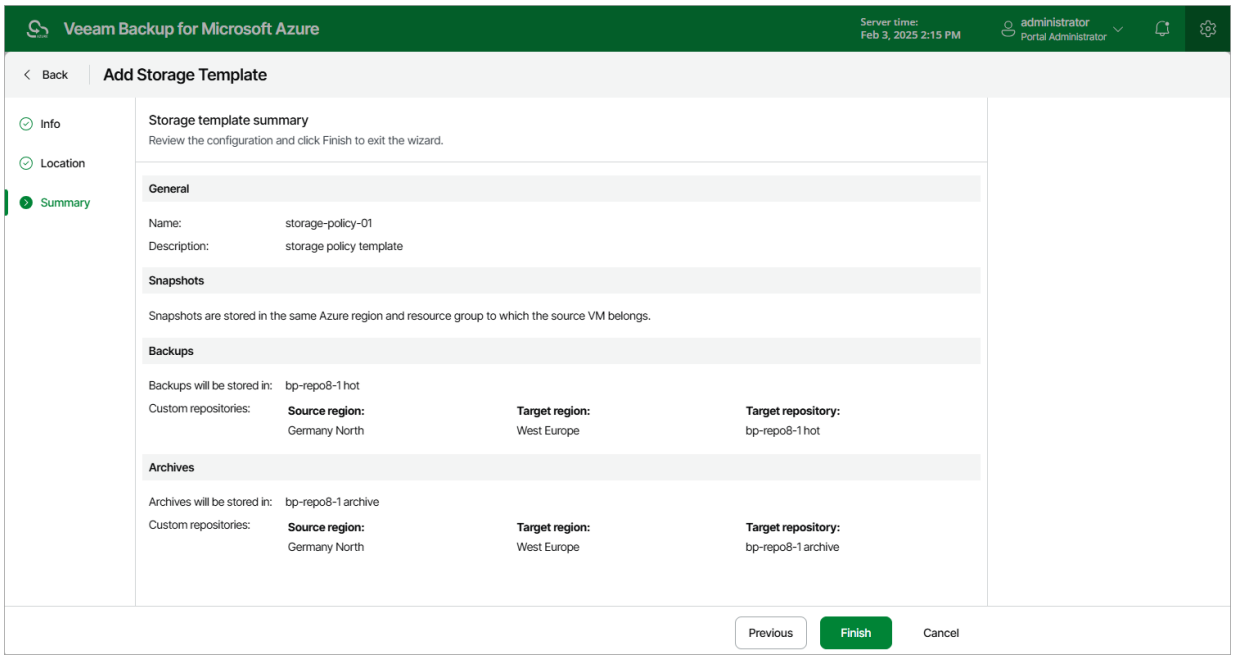
To be able to choose a target location for archived backups, you must specify a target location for image-level backups first.



## Step 4. Finish Working with Wizard

At the **Summary** step of the wizard, review summary information and click **Finish**.

> **TIP**
>
> After you create a storage template and assign it to a number of SLA-based backup policies as described in section Performing Backup Using Web UI, you will be able to see the full list of all the related policies on the **Storage** page. To do that, select the necessary template and click the link in the **Currently Assigned** column.




# Editing Storage Templates

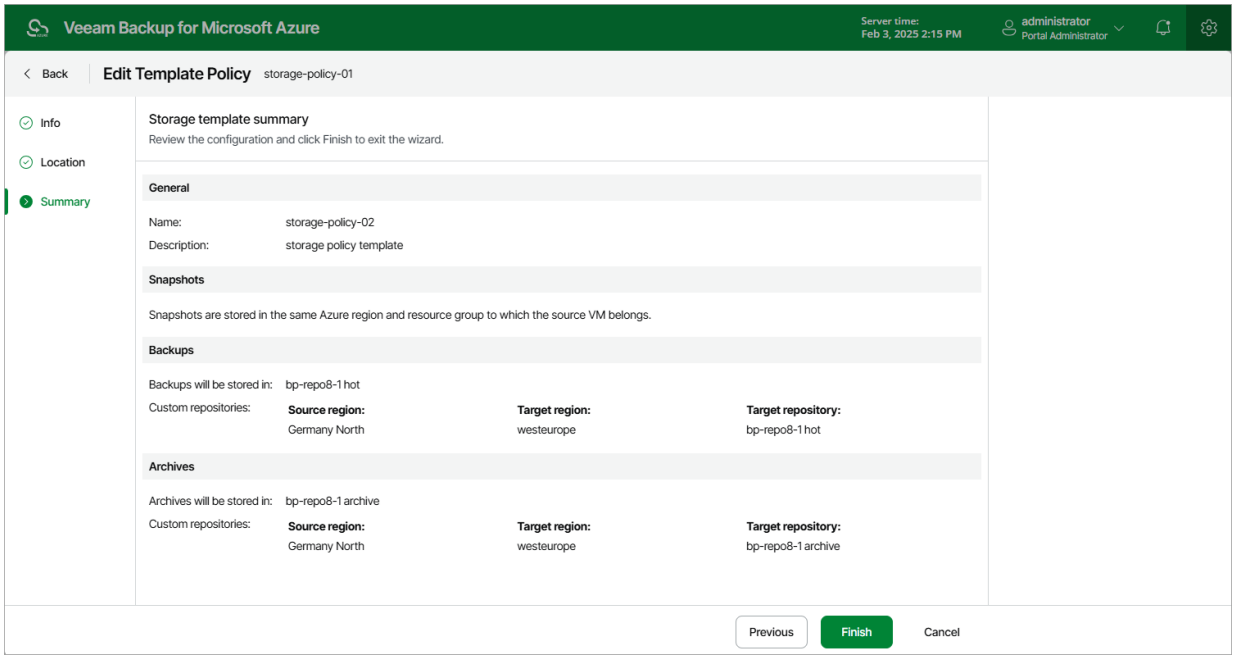
> **IMPORTANT**
>
> If a storage template is already assigned to at least one SLA-based backup policy, modifying its location settings will cause Veeam Backup for Microsoft Azure to start a new chain of restore points in the specified location. The old chain of restore points will be retained in the previous location until removed according to retention settings specified for the SLA template assigned to this SLA-based backup policy.

For each storage template, you can modify settings configured while creating the template:

1. Switch to the **Configuration** page.
2. Navigate to **Policy Templates** > **Storage** and click **Edit**.
3. Complete the **Edit Storage Template** wizard:
   a. To provide a new name and description for the template, follow the instructions provided in section Adding Storage Templates (step 2).
   b. To modify the configured location settings, follow the instructions provided in section Adding Storage Templates (step 3).

c. At the **Summary** step of the wizard, review configuration information and click **Finish** to confirm the changes.

> **TIP**
>
> After you click **Finish**, Veeam Backup for Microsoft Azure will update the timestamp in the **Last Modified** column on the **Storage** page, regardless of whether you have actually modified the template settings or not. If you want to simply view the configured settings without making any changes, click **View Info**.

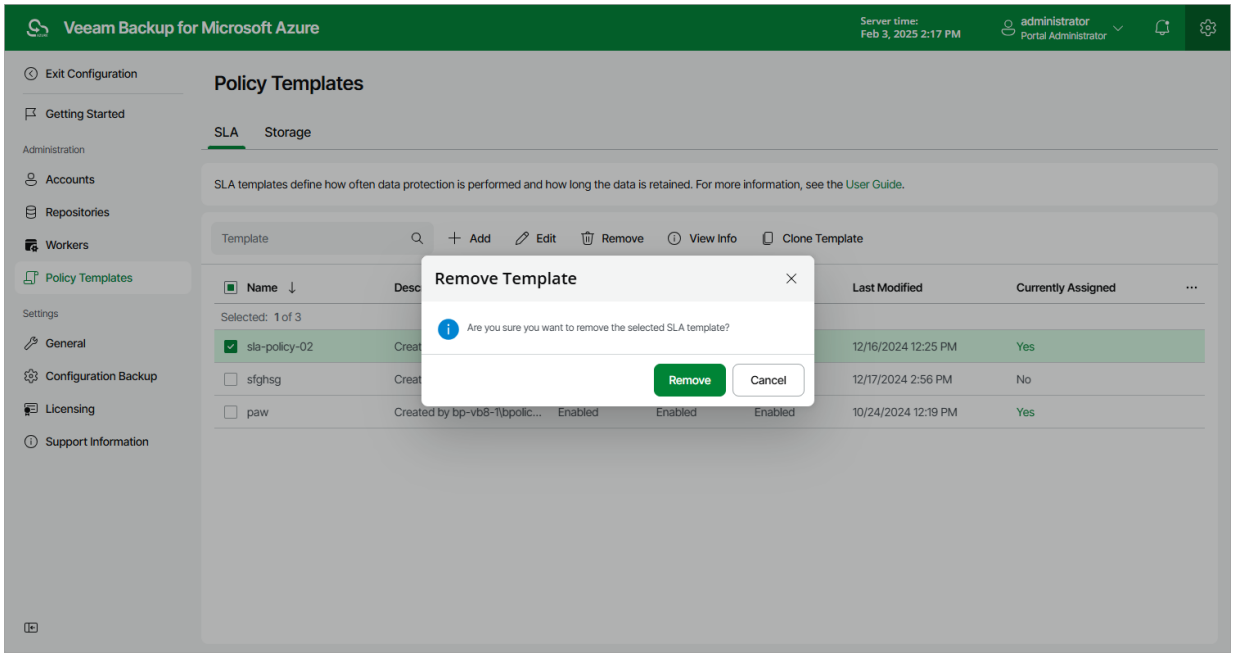


# Removing SLA and Storage Templates

Veeam Backup for Microsoft Azure allows you to permanently remove a policy template from the configuration database if you no longer need it:

1. Switch to the **Configuration** page.
2. Navigate to **Policy Templates**.
3. Switch to the necessary tab and select the template.
4. Click **Remove**.

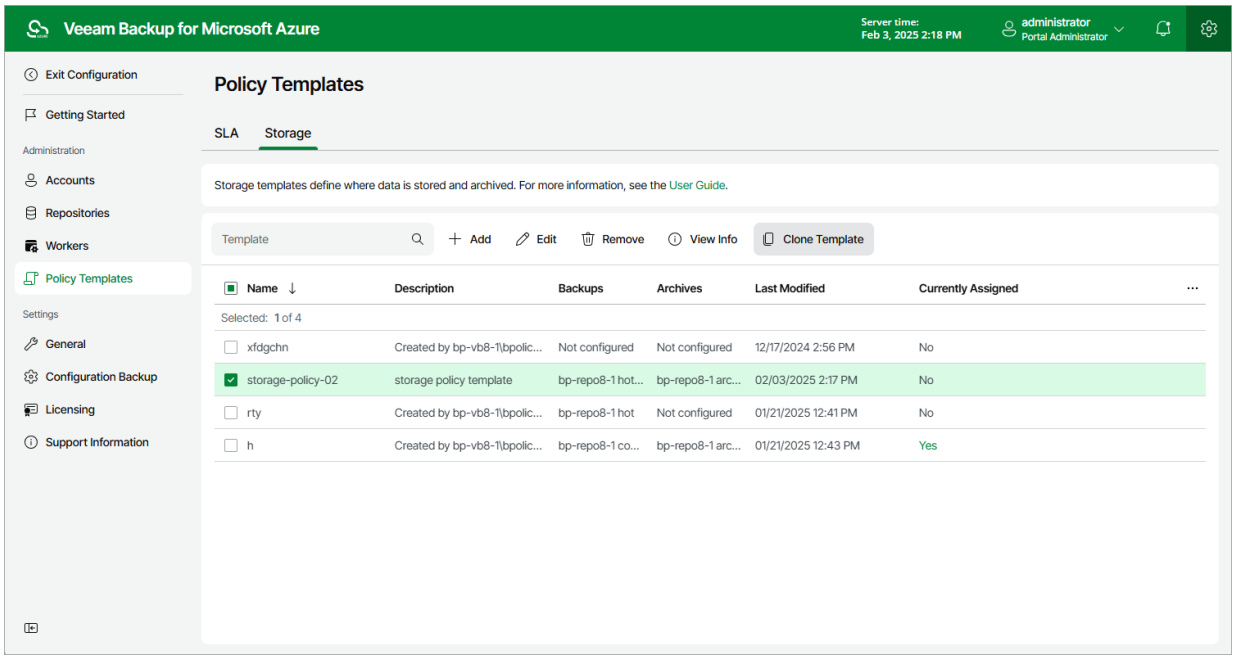
> **IMPORTANT**
>
> You cannot remove a template that is used by any SLA-based backup policy. Modify the settings of all the related policies to remove references to the template — and then try removing the template again.



# Cloning SLA and Storage Templates

Veeam Backup for Microsoft Azure allows you to create a new policy template based on the settings of an existing one:

1. Switch to the **Configuration** page.
2. Navigate to **Policy Templates**.
3. Switch to the necessary tab and select the template.
4. Click **Clone**.
5. Complete the **Clone SLA Template** or the **Clone Storage Template** wizard as described in section Adding SLA Templates or Adding Storage Templates.



# Configuring General Settings

Veeam Backup for Microsoft Azure allows you to configure general settings that are applied to all performed operations and deployed architecture components:

- Enable the private network deployment functionality and choose a messaging service that will be used to transfer data.
- Define for how long obsolete snapshots and session records will be retained.
- Provide certificates to secure connections between Veeam Backup for Microsoft Azure architecture components.
- Configure notification settings for automated delivery of reports.
- Change the time zone set on the backup appliance.
- Configure single sign-on settings to retrieve user identities from an identity provider.

# Configuring Deployment Mode

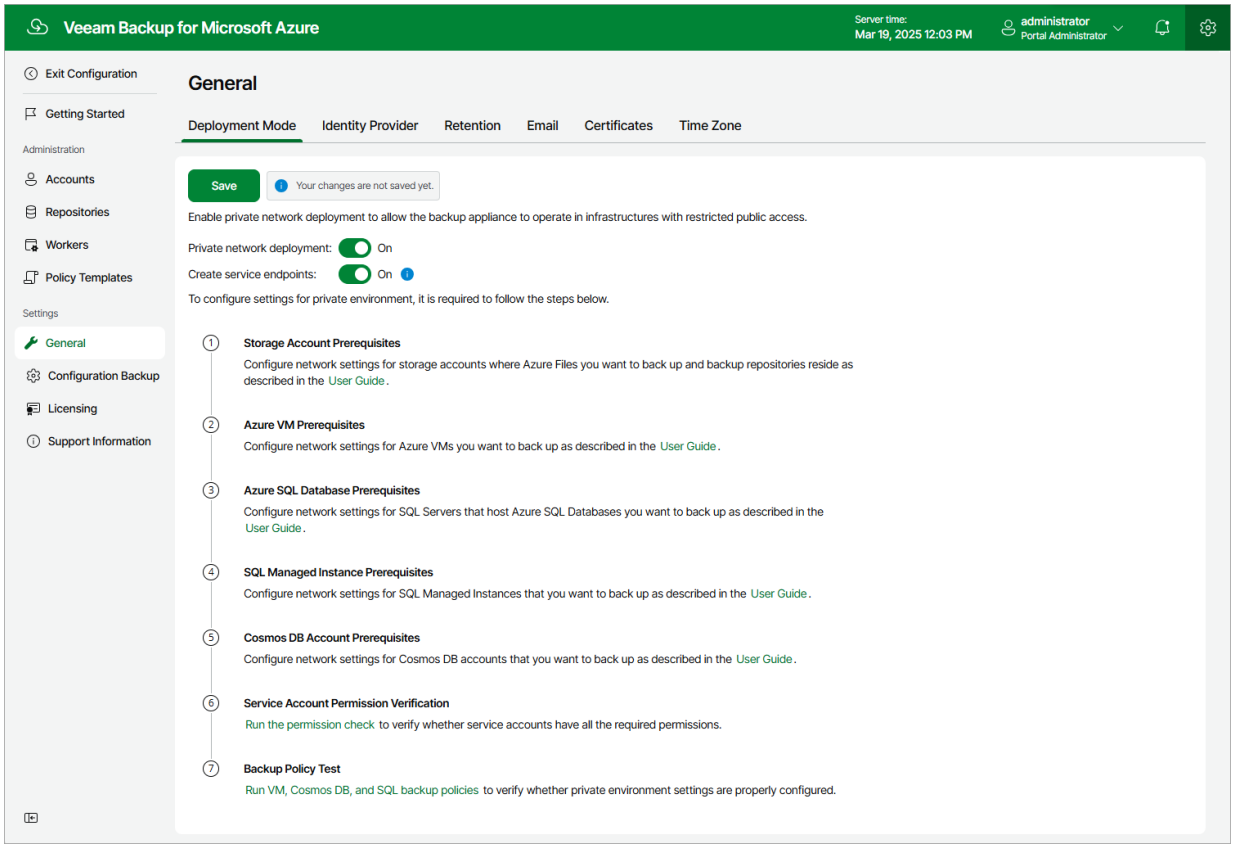
By default, worker instances launched by Veeam Backup for Microsoft Azure access protected Azure resources through public virtual networks. If you want worker instances to process resources that reside in private virtual networks, you can enable the private network deployment functionality and instruct Veeam Backup for Microsoft Azure to launch worker instances without public IPv4 addresses. In this case, Veeam Backup for Microsoft Azure will automatically configure worker settings to allow private network access; however, you will also need to perform a number of configuration steps manually as described in section Working in Private Environments.

To enable the private network deployment functionality, do the following:

1. Switch to the **Configuration** page, navigate to **General** > **Deployment Mode** and set the **Private network deployment** toggle to *On*.
2. By design, Veeam Backup for Microsoft Azure automatically creates a virtual network service endpoint for the *Microsoft.Storage.Global* service to communicate with worker instances in public virtual networks. However, for worker instances operating in private environments, you must do either of the following:
   - Configure the virtual network service endpoint manually in Microsoft Azure as described in Microsoft Docs.
   - Set the **Create service endpoints** toggle to *On*.
3. To allow Veeam Backup for Microsoft Azure to launch the worker instances while backing up unmanaged Azure VMs and file shares, configure network settings for your storage accounts as described in section Configuring Network Settings for Storage Accounts.
4. To allow Veeam Backup for Microsoft Azure to back up Azure VMs in a private environment, configure network settings for these VMs as described in section Configuring Network Settings for VM Backup.
5. To allow Veeam Backup for Microsoft Azure to launch the worker instances while backing up SQL Servers, configure network settings for these servers as described in section Configuring Network Settings for SQL Servers.
6. To allow Veeam Backup for Microsoft Azure to launch the worker instances while backing up SQL Managed Instances, configure network settings for these instances as described in section Configuring Network Settings for SQL Managed Instances.
7. To allow Veeam Backup for Microsoft Azure to to back up Cosmos DB accounts in a private environment, configure network settings for these accounts as described in section Configuring Networking Settings for Cosmos DB Accounts.
8. To check whether you have configured all the necessary settings correctly, run your backup policies as described in section Performing Backup.

> **IMPORTANT**
>
> If you enable the private network deployment functionality for your backup appliance, the subnet in which the appliance is deployed must have at least 2 free IP addresses for each Azure region where worker instances are launched during backup and restore operations. Otherwise, the subnet may run out of free IP addresses and deplete.

After you enable the private network deployment functionality, it is recommended that you check whether service accounts have all the permissions required to use this functionality as described in section Checking Service Account Permissions.




# Choosing Messaging Service

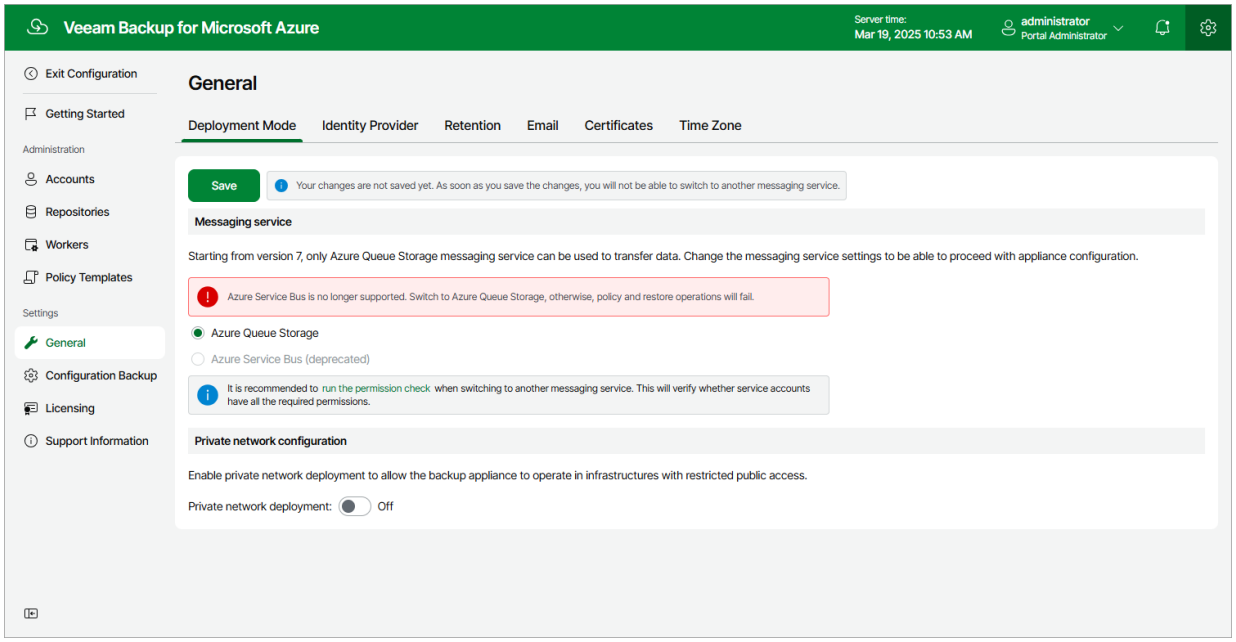
[Applies only to upgraded appliances that still use Azure Service Bus as a messaging service]

Veeam Backup for Microsoft Azure uses a messaging service to allow communication between the architecture components. In versions prior to 7.0, Veeam Backup for Microsoft Azure used the Azure Service Bus messaging service by default. In version 7.0, Azure Service Bus was replaced by Azure Queue Storage. That is why you must manually switch to the Azure Queue Storage service immediately after you upgrade the backup appliance — otherwise, Veeam Backup for Microsoft Azure will fail to perform backup and restore operations. For more information on the Azure Queue Storage messaging service, see Microsoft Docs.

**IMPORTANT**

After you switch to the Azure Queue Storage service, you must do the following:

1. Check whether service accounts have all the permissions required to use this service, as described in section Checking Service Account Permissions.
2. Manually remove from Microsoft Azure the Service Bus premium namespaces created by Veeam Backup for Microsoft Azure. To do that:
   a. Sign in to the Microsoft Azure portal using credentials of the Microsoft Azure account that you used to install Veeam Backup for Microsoft Azure.
   b. Navigate to **Resource groups** and click the resource group in which the backup appliance is deployed.
   c. In the **Resources** section on the resource group page, enter *veeam* in the search field.
   d. In the **Resources** list, select check boxes next to the resources of the *Service Bus namespace* type and click **Delete**.
   e. In the **Delete Resources** window, type *Yes* to confirm the action and click **Delete**.




# Working in Private Environments

For Veeam Backup for Microsoft Azure to be able to work with Azure resources that operate in private environments, do the following:

1. Switch to the **Configuration** page, navigate to **General** > **Deployment Mode** and set the **Private network deployment** toggle to *On*.
2. Set the **Create service endpoints toggle** to *On*, or configure the virtual network service endpoint manually in Microsoft Azure as described in Microsoft Docs.
3. Click **Save**.

Additionally, there is a list of configuration actions that must be performed both on the Veeam Backup for Microsoft Azure and the client side.

# Actions Performed by Veeam Backup for Microsoft Azure

Veeam Backup for Microsoft Azure will automatically configure network settings required:

- To allow secure communication between the backup appliance and storage accounts where Veeam applications and scripts are stored.

  Veeam Backup for Microsoft Azure creates these accounts in Azure regions where worker instances are launched and protected VMs with VSS agents reside.

- To allow the Azure Queue Storage messaging service to transfer data between services in private virtual networks.

# Actions Performed by Client

> **NOTE**
>
> This section provides instructions on steps performed in a third-party application. Keep in mind that the instructions may become outdated. For up-to-date instructions, see Microsoft Docs.

To back up and restore Azure resources operating within private virtual networks (VNets), you must grant Veeam Backup for Microsoft Azure access to these resources. To do that, configure specific network settings to allow traffic from VNets to which the backup appliance and worker instances are connected to reach your resources. Depending on the Azure resource to which you want to grant access, do either of the following:

- Configure network settings for an Azure VM.
- Configure network settings for a SQL Server.
- Configure network settings for a SQL Managed Instance.
- Configure network settings for a Cosmos DB account.
- Configure network settings for a repository, an unmanaged Azure VM or an Azure file share.

## Configuring Network Settings for VMs

To allow Veeam Backup for Microsoft Azure to back up Azure VMs in a private environment, perform the following steps:

1. Create private DNS zones.
2. Add a custom worker configuration.
3. Add the VNets of the backup appliance and worker instances to the private DNS zones.
4. Configure network settings for backup appliance.
5. Create and run a backup policy to automatically create storage accounts and private endpoints.
6. Configure automatically created private endpoints.
7. Run the backup policy to automatically create disk access resources.
8. Configure settings for the automatically created disk access resources.
9. Run the backup policy to check whether the configuration was successful.

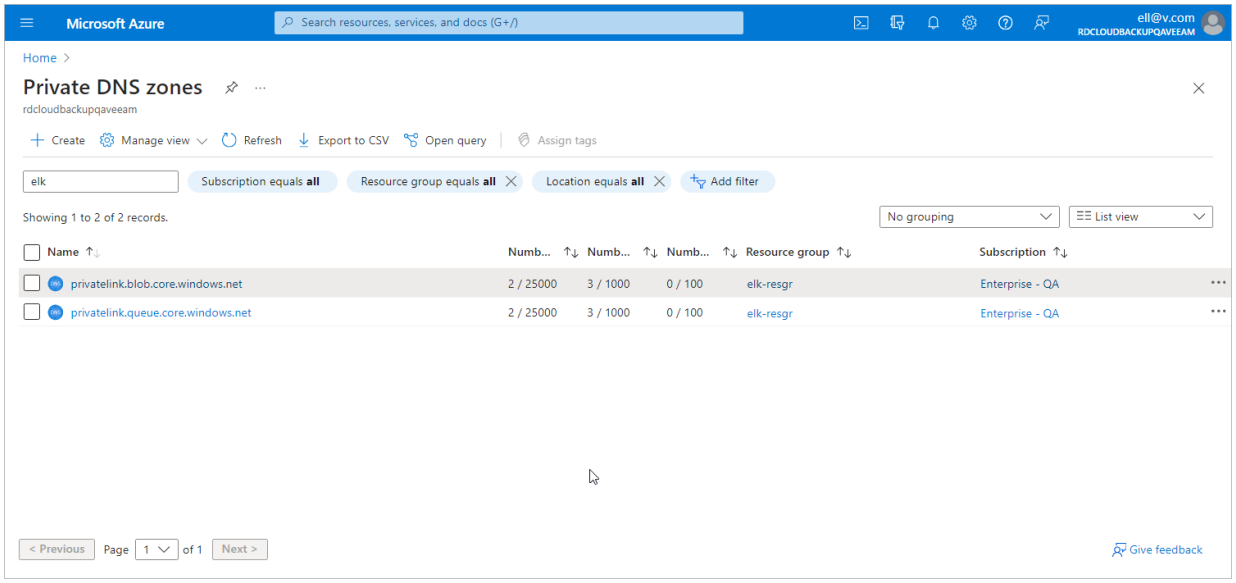
**IMPORTANT**

To allow Veeam Backup for Microsoft Azure to store backups of Azure VMs in repositories, you must also configure network settings as described in section Configuring Network Settings for Storage Accounts.

## Step 1. Create Private DNS Zones

To create Azure private DNS zones that will allow Veeam Backup for Microsoft Azure to operate in your private environment, log in to the Microsoft Azure portal and create two Azure private DNS zones named *privatelink.blob.core.windows.net* and *privatelink.queue.core.windows.net* as described in Microsoft Docs. It is recommended that you create the DNS zones in the same resource group where the backup appliance resides, to simplify resource management.

> **IMPORTANT**
>
> Make sure that the names of the created private DNS zones are unique within the resource group in which they reside.



## Step 2. Add Worker Configuration

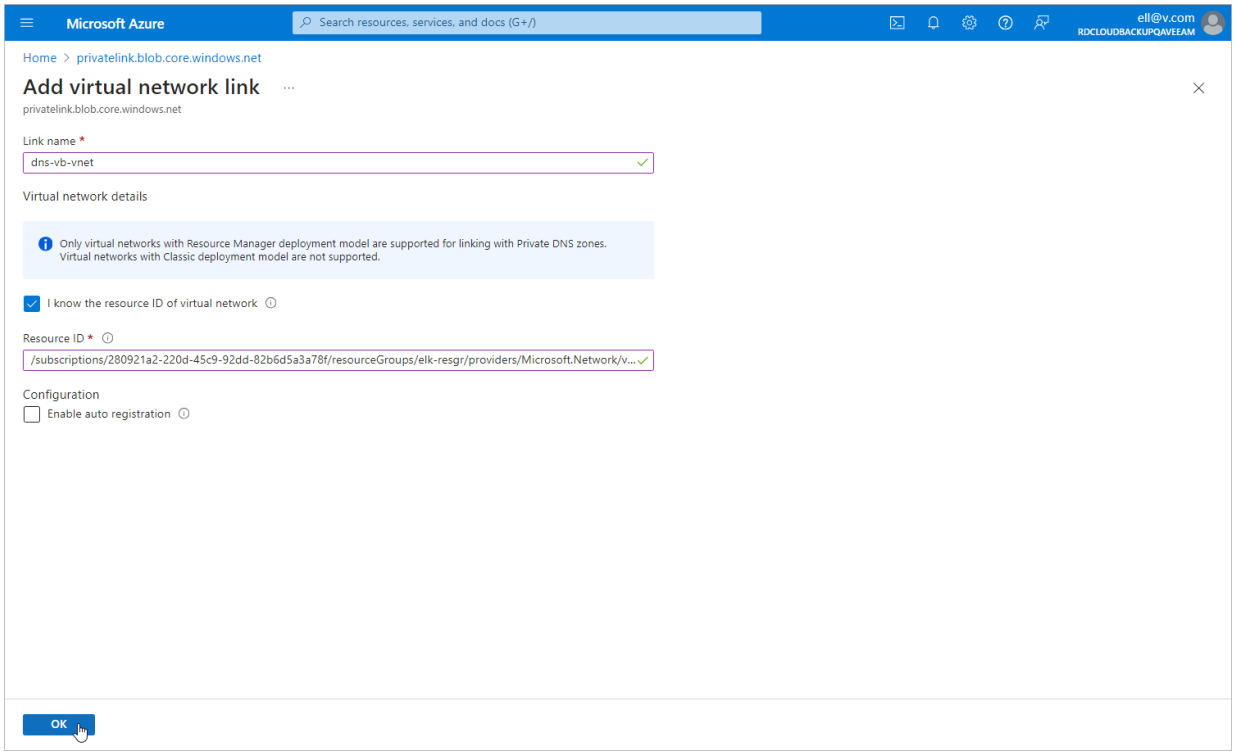
For Veeam Backup for Microsoft Azure to be able to launch worker instances in the private environment, create a worker configuration in the same Azure region where the protected VM resides, as described in section Adding Worker Configurations. When creating the configuration, make sure to select a VNet for the worker instances.

## Step 3. Add VNets to Private DNS Zones

To allow Veeam Backup for Microsoft Azure to perform backup operations in the private environment, you must add the VNet to which the backup appliance is connected and the VNet selected for the worker configuration created at step 2 to both DNS zones created at step 1.

To add a VNet to a DNS zone, do the following:

1. Log in to the Microsoft Azure portal.
2. Open the **Resource group** page.
3. In the **Resource** list, locate and click the necessary VNet. The **Virtual network** page will open.
4. Navigate to **JSON view**. In the **Resource JSON** window, navigate to the **Resource ID** field and copy the ID to the clipboard.
5. Back to the **Resource group** page, in the **Resource** list, locate the private DNS zones created at step 1 and click one of them.
6. On the **Private DNS zone** page, navigate to **Settings** > **Virtual network links** and click **Add**.
7. In the **Add virtual network link** window, create a link to the VNet:
   a. In the **Link name** field, specify a name for the link.
   b. In the **Virtual network details** section, select the **I know the resource ID of virtual network** check box.
   c. In the **Resource ID** field, paste the ID of the VNet.
   d. Click **OK**.



## Step 4. Configure Network Settings for Backup Appliance

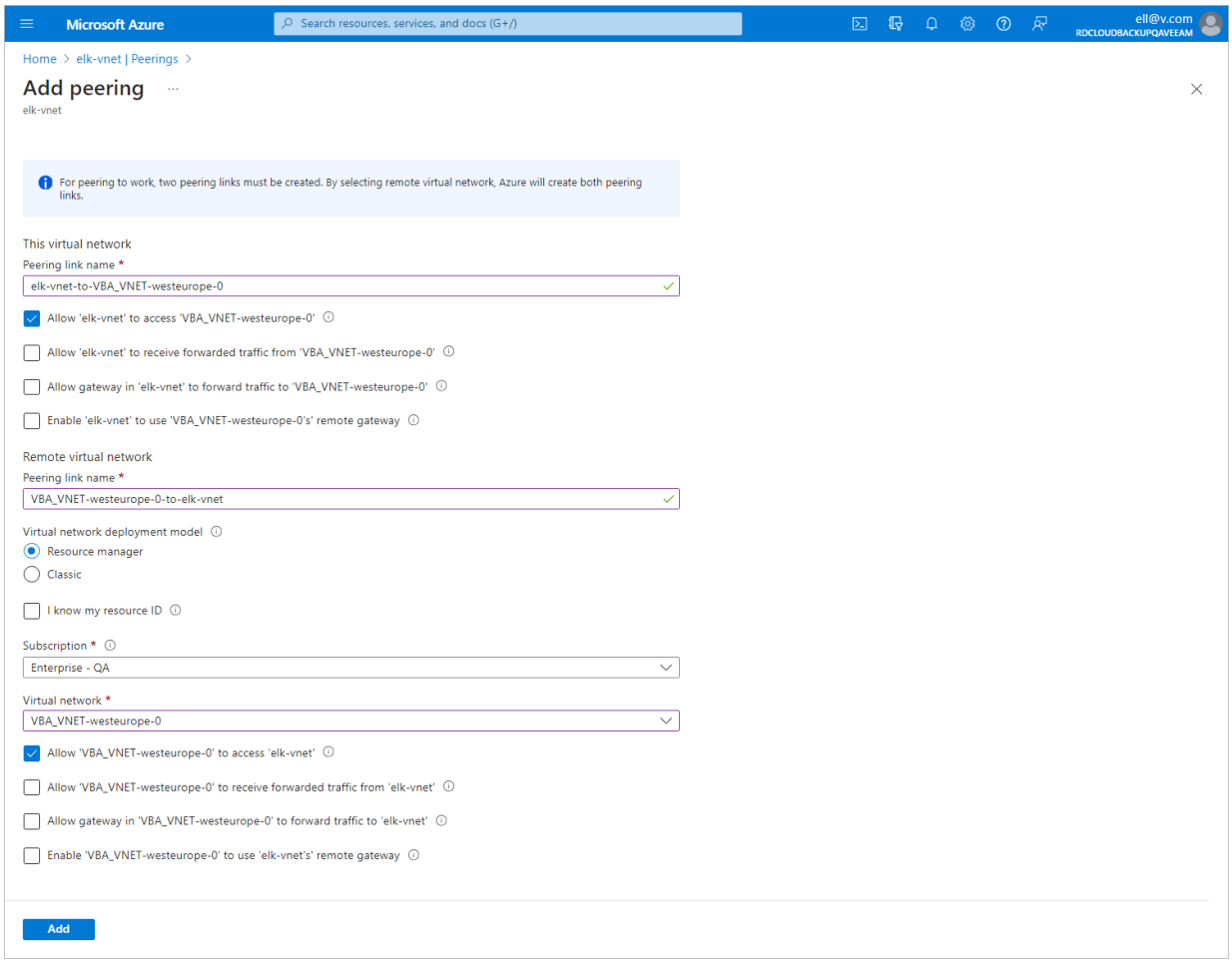
To allow Veeam Backup for Microsoft Azure components to communicate in the private environment, you must configure peering connections between the following VNets:

- The VNet to which the backup appliance is connected and the VNet to which worker instances are connected
- [Applies only if you plan to enable application-aware processing or to perform file-level recovery to the original location] The VNet to which the backup appliance is connected and the VNet to which the protected VM is connected
- [Applies only if you plan to enable backup to repository] The VNet to which the backup appliance is connected and the VNet to which the repository private endpoint is connected

To create a peering connection, perform the following steps:

1. Log in to the Microsoft Azure portal.
2. Open the **Resource group** page.
3. In the **Resource** list, locate and click the VNet to which the backup appliance is connected. The **Virtual network** page will open.
4. Navigate to **Settings** > **Peerings**.
5. Click **Add** to open the **Add peering** page.
6. On the **Add peering** page, specify the following settings:
    a. In the **This virtual network** section, specify a name for the peering link that will be added to the VNet to which the backup appliance is connected. Leave the default settings for the other options in this section.
    b. In the **Remote virtual network** section, specify a name for the peering link that will be added to the target VNet. Leave the default settings for the other options in this section.
    c. From the **Subscription** drop-down list, select an Azure subscription to which worker instances belong.
    d. From the **Virtual networks** drop-down list, select the virtual network to which worker instances are connected.

e. Click **Add**.


Microsoft Azure
Search resources, services, and docs (G+/)
ell@v.com
RDCLOUDBACKUPQAVEEAM
Home > elk-vnet | Peerings >
Add peering
elk-vnet
For peering to work, two peering links must be created. By selecting remote virtual network, Azure will create both peering links.
This virtual network
Peering link name *
elk-vnet-to-VBA_VNET-westeurope-0
Allow 'elk-vnet' to access 'VBA_VNET-westeurope-0'
Allow 'elk-vnet' to receive forwarded traffic from 'VBA_VNET-westeurope-0'
Allow gateway in 'elk-vnet' to forward traffic to 'VBA_VNET-westeurope-0'
Enable 'elk-vnet' to use 'VBA_VNET-westeurope-0's' remote gateway
Remote virtual network
Peering link name *
VBA_VNET-westeurope-0-to-elk-vnet
Virtual network deployment model
Resource manager
Classic
I know my resource ID
Subscription *
Enterprise - QA
Virtual network *
VBA_VNET-westeurope-0
Allow 'VBA_VNET-westeurope-0' to access 'elk-vnet'
Allow 'VBA_VNET-westeurope-0' to receive forwarded traffic from 'elk-vnet'
Allow gateway in 'VBA_VNET-westeurope-0' to forward traffic to 'elk-vnet'
Enable 'VBA_VNET-westeurope-0' to use 'elk-vnet's' remote gateway
Add

## Step 5. Create and Launch Backup Policy

To allow Veeam Backup for Microsoft Azure to protect Azure VMs in the private environment, create and launch a schedule-based backup policy as described in section Performing VM Backup.

Consider that the backup policy is launched at this step only to automatically create and configure Veeam storage accounts and private endpoints that will further be used for backup operations. As soon as Veeam Backup for Microsoft Azure performs the necessary configuration steps, the policy will fail as some additional manual configuration actions with the private endpoints will still be required. For more information, see Configuring Private Endpoints.

## Step 6. Configure Private Endpoints

For Veeam Backup for Microsoft Azure to be able to establish private connections with the protected Azure VMs, you must configure DNS settings for private endpoints that Veeam Backup for Microsoft Azure automatically created in Microsoft Azure at step 5. Private endpoints are network interfaces that use private IP addresses from VNets. For more information on private endpoints, see Microsoft Docs.

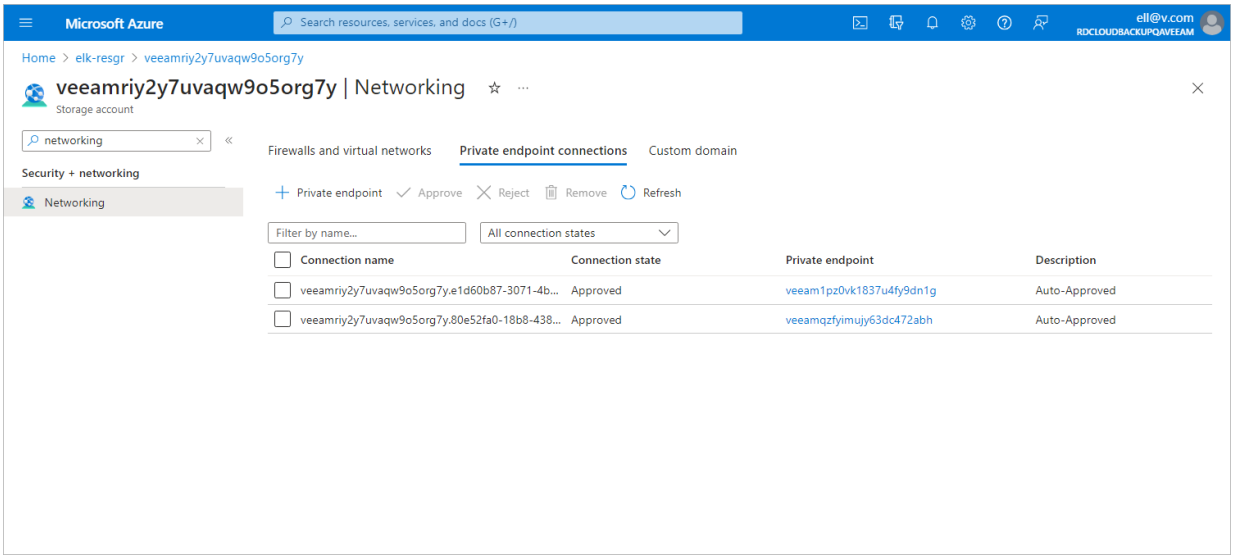
To configure DNS settings for private endpoints, perform the following steps:

1. Locate private endpoints for your Veeam storage account in Microsoft Azure.
2. Configure the private endpoint for Azure Blob Storage.
3. Configure private endpoint for Azure Queue Storage.

## Step 6a. Locate Private Endpoints

To locate private endpoints automatically created by Veeam Backup for Microsoft Azure, do the following:

1. Log in to the Microsoft Azure portal.
2. Click **More services** and select **Resource groups** on the **All services** page.
3. On the **Resource groups** page, select the resource group to which the necessary storage account belongs. The resource group page will open.
4. In the **Resources** list, search for storage accounts that are assigned the *Veeam backup appliance ID* tag.
5. Click the necessary storage account. The **Storage account** page will open.
6. Navigate to **Security + networking** > **Networking** and switch to the **Private endpoint connections** tab.



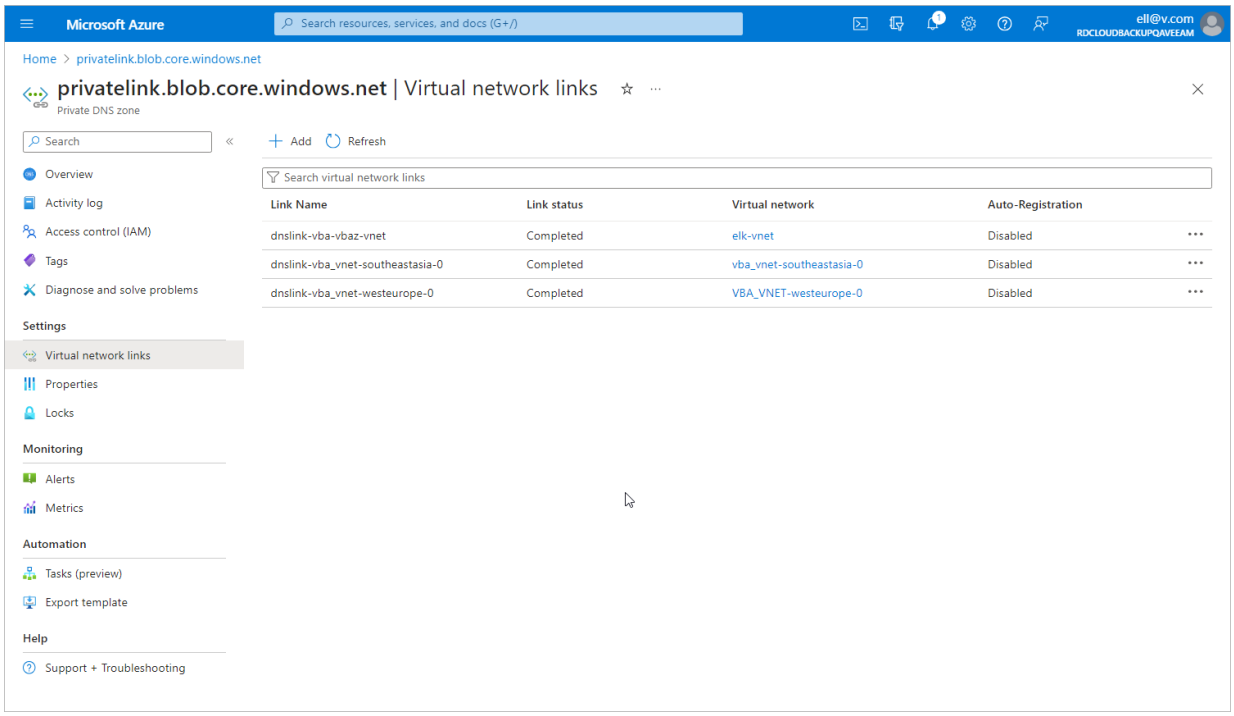
## Step 6b. Configure Private Endpoint for Azure Blob Storage

To configure DNS settings for the private endpoint that Veeam Backup for Microsoft Azure automatically created for Azure Blob Storage, do the following:

1. In the **Private endpoint connections** tab of the **Networking** window of the Veeam storage account selected at step 6a, locate the private endpoint created for Azure Blob Storage. To do that, click the link in the **Private endpoint** column. The private endpoint for Azure Blob Storage will have the *blob* value set in the **Target sub-resource** field.
2. In the **Private endpoint** window, navigate to **Settings** > **DNS Configuration** and click **Add configuration**.
3. In the **Add DNS zone configuration** window, do the following:
   a. From the **Subscription** drop-down list, select the subscription where the DNS zones created at step 1 reside.
   b. From the **Private DNS zone** drop-down list, select the pair of the *privatelink.blob.core.windows.net* name and the resource group in which the DNS zone was created. Leave the default settings for the other options in this window.
   c. Click **Add**.
4. In the private DNS zone, create an 'A' record for the added private endpoint as described in Microsoft Docs.
5. In the **DNS configuration** window, navigate to the newly created DNS configuration and click the in the **Private DNS zone** column.
6. In the **Private DNS zone** window, navigate to **DNS Management** > **Virtual network links** and click **Add**.
7. In the **Add virtual network link** window, add to the DNS zone both the link to the VNet to which the backup appliance is connected and the links to the VNets to which the worker instances are connected. To do that, perform the following steps for each VNet link:
   a. In the **Link name** field, specify a name for the link.
   b. From the **Subscription** drop-down list, select the subscription where the VNet resides.
   c. From the **Virtual network** drop-down list, select the necessary VNet.
   d. Click **OK**.

> **IMPORTANT**
>
> For application-aware processing, you must also add to the DNS zone the links to the VNets to which Azure VMs that you plan to protect are connected.

8. In the **Virtual network links** window, make sure that you have added links to all the necessary VNets.



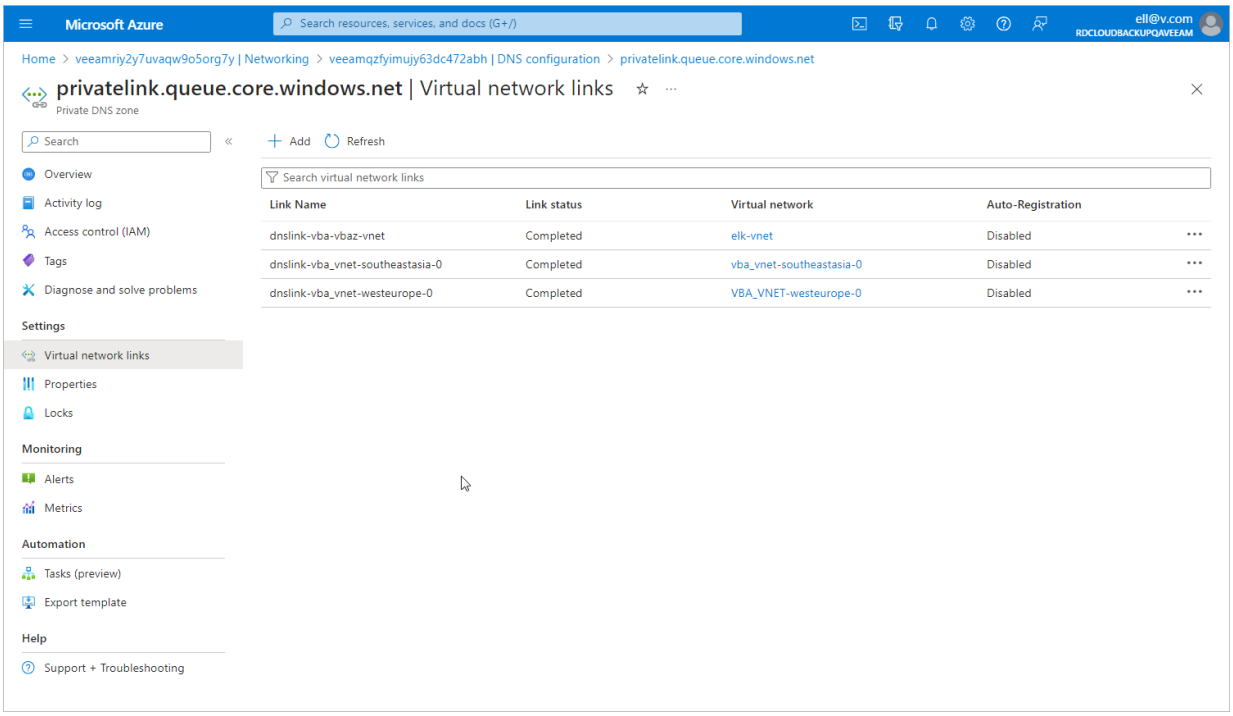
## Step 6c. Configure Private Endpoint for Azure Queue Storage

To configure DNS settings for the private endpoint that Veeam Backup for Microsoft Azure automatically created for Azure Queue Storage, do the following:

1. In the **Private endpoint connections** tab of the **Networking** window of the Veeam storage account selected at step 6a, locate the private endpoint created for Azure Queue Storage. To do that, click the link in the **Private endpoint** column. The private endpoint for Azure Queue Storage will have the *queue* value set in the **Target sub-resource** field.
2. In the **Private endpoint** window, navigate to **Settings** > **DNS Configuration** and click **Add configuration**.
3. In the **Add DNS zone configuration** window, do the following:
   a. From the **Subscription** drop-down list, select the subscription where the DNS zones created at step 1 reside.
   b. From the **Private DNS zone** drop-down list, select the pair of the *privatelink.queue.core.windows.net* name and the resource group in which the DNS zone was created. Leave the default settings for the other options in this window.
   c. Click **Add**.
4. In the private DNS zone, create an 'A' record for the added private endpoint as described in Microsoft Docs.
5. In the **DNS configuration** window, navigate to the newly created DNS configuration and click the in the **Private DNS zone** column.
6. In the **Private DNS zone** window, navigate to **DNS Management** > **Virtual network links** and click **Add**.
7. In the **Add virtual network link** window, add to the DNS zone links to the VNet to which the backup appliance is connected, and to VNets to which the worker instances are connected. To do that, perform the following steps for each VNet link:
   a. In the **Link name** field, specify a name for the link.
   b. From the **Subscription** drop-down list, select the subscription where the VNet resides.
   c. From the **Virtual network** drop-down list, select the name of the VNet.
   d. Click **OK**.

> **IMPORTANT**
>
> For application-aware processing, you must also add to the DNS zone links to the VNet to which Azure VMs that you plan to protect using application-aware processing are connected.

8. In the **Virtual network links** window, make sure that you have added links to all the necessary VNets.



## Step 7. Launch Backup Policy for Disk Access

To allow Veeam Backup for Microsoft Azure to finalize the private network deployment configuration, run the schedule-based backup policy created at step 5 once again.

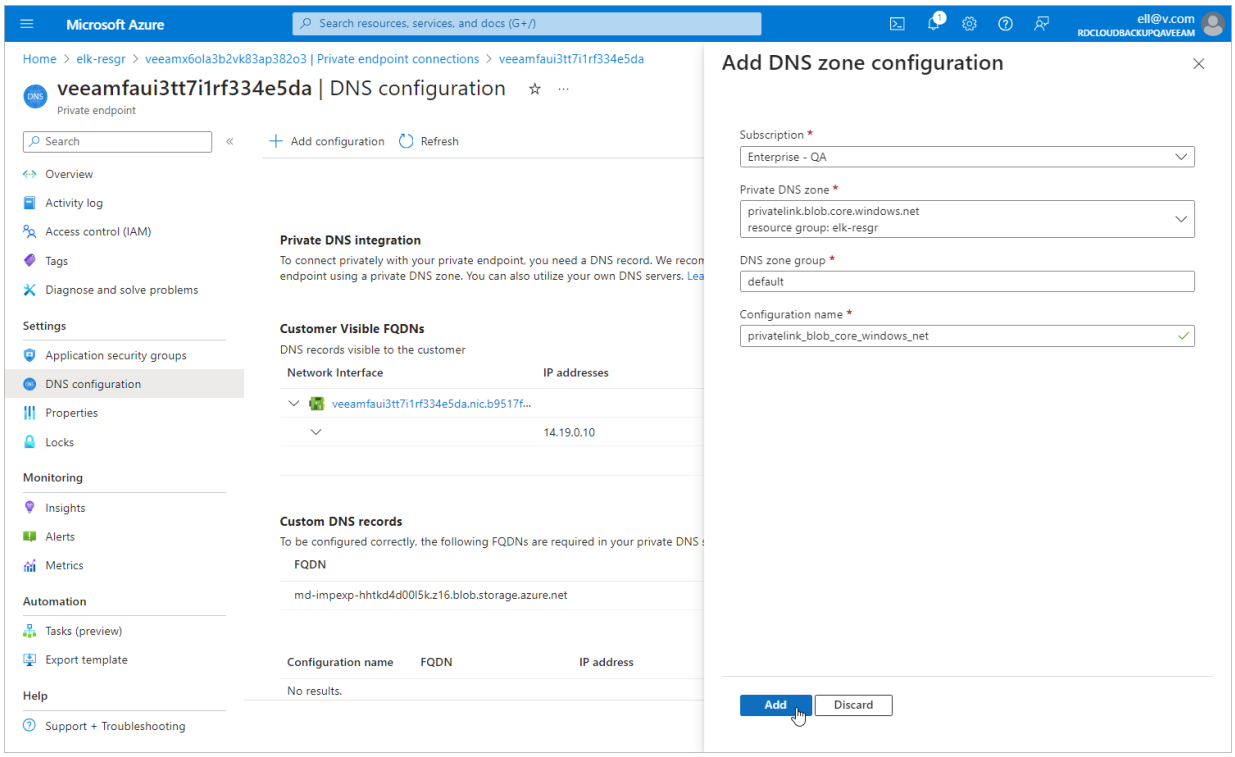
Consider that the backup policy is launched at this step only to automatically create and configure Veeam disk access resources that will further be used for backup operations. As soon as Veeam Backup for Microsoft Azure performs the necessary configuration steps, the policy will fail as some additional manual configuration actions with the disk access resources will still be required. For more information, see Configuring Disk Access Settings.

## Step 8. Configure Disk Access Settings

To allow worker instances to export the snapshot to the backup repository in the private environment, you must add the private endpoints of the disk access resources that Veeam Backup for Microsoft Azure automatically created at step 7 to the *privatelink.blob.core.windows.net* DNS zone created at step 1.

To add a private endpoint of a disk access resource to the DNS zone, do the following:

1. Log in to the Microsoft Azure portal.
2. Open the **Resource group** page.
3. In the **Resource** list, search for disk access resources that reside in the same region as your backup appliance and are assigned the *Veeam backup appliance ID* tag.
4. Click the necessary disk access resource. The **Disk Access** page will open.
5. Switch to the **Private endpoint connections** tab and locate the private endpoint created for disk access. To do that, click the link in the **Private endpoint** column. The private endpoint for disk access will have the *disks* value set in the **Target sub-resource** field.
6. Navigate to **DNS configuration** and click **Add configuration**.
7. In the **Add DNS zone configuration** window, do the following:
   a. From the **Subscription** drop-down list, select the subscription where the DNS zones created at step 1 reside.
   b. From the **Private DNS zone** drop-down list, select the pair of the *privatelink.blob.core.windows.net* name and the resource group in which the DNS zone was created. Leave the default settings for the other options in this window.
   c. Click **Add**.
8. In the DNS zone, create an 'A' record for the added private endpoint as described in Microsoft Docs.



### Step 9. Launch Test Backup Policy

To make sure that you have configured all the required settings correctly, launch the schedule-based backup policy created at step 5.

Consider that as soon as the backup policy completes successfully, Veeam Backup for Microsoft Azure will start regularly updating the worker instances. However, for Veeam Backup for Microsoft Azure to be able to install the updates, your worker instances will require public access to the online Ubuntu repositories listed in section Ports. If you do not want Veeam Backup for Microsoft Azure to update the worker instances, open a support case.

## Configuring Network Settings for SQL Servers

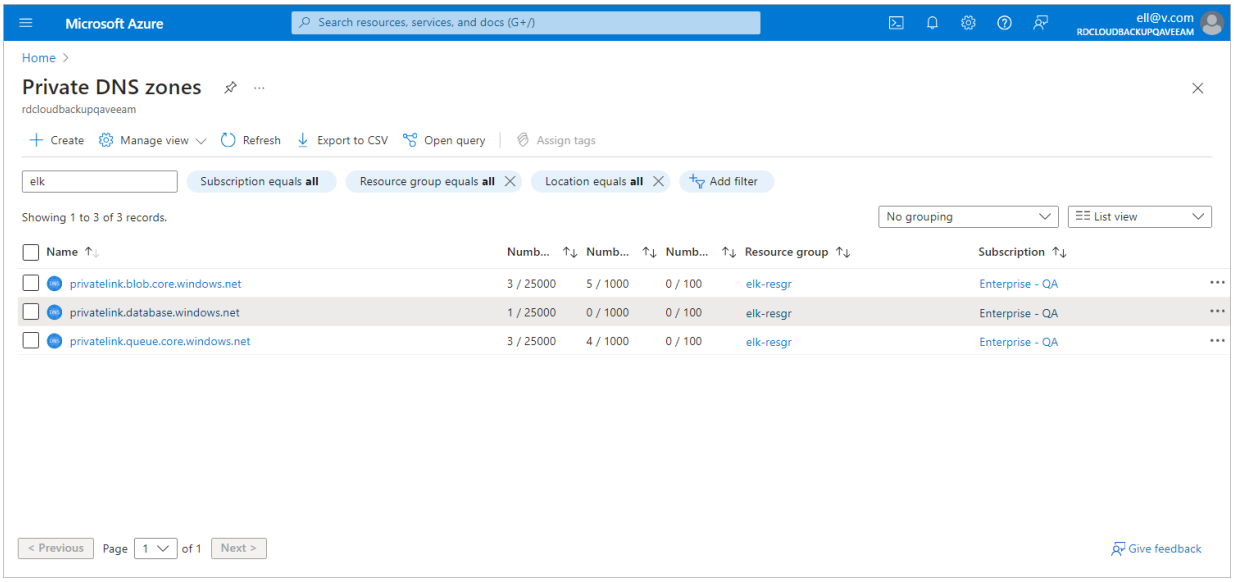
To allow Veeam Backup for Microsoft Azure to back up SQL Servers in a private environment, perform the following steps:

1. Create private DNS zones.
2. Add a custom worker configuration.
3. Add the VNets of the backup appliance and worker instances to the private DNS zones.
4. Configure network settings for backup appliance.
5. Create and run a backup policy to automatically create storage accounts and private endpoints.
6. Configure automatically created private endpoints.
7. Disable public access to the SQL Server.
8. Create a private endpoint for the SQL Server.
9. Configure the private endpoint created for the SQL Server.
10. Run the backup policy to check whether the configuration was successful.

## Step 1. Create Private DNS Zones

To create Azure private DNS zones that will allow Veeam Backup for Microsoft Azure to operate in the private environment, log in to the Microsoft Azure portal and create 3 Azure private DNS zones named *privatelink.blob.core.windows.net*, *privatelink.queue.core.windows.net* and *privatelink.database.windows.net* as described in Microsoft Docs. It is recommended that you create the DNS zones in the same resource group where the backup appliance resides, to simplify resource management.

> **IMPORTANT**
>
> Make sure that the names of the created private DNS zones are unique within the resource group in which they reside.



## Step 2. Add Worker Configuration

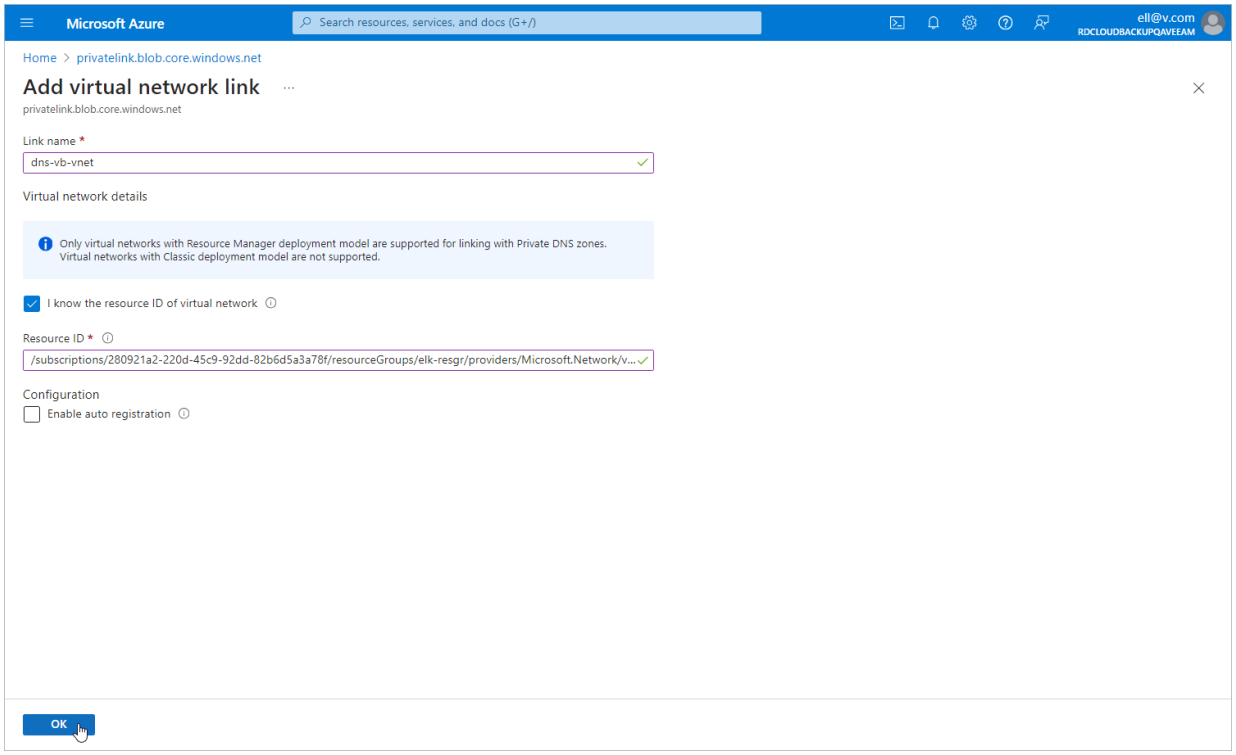
For Veeam Backup for Microsoft Azure to be able to launch worker instances in the private environment, create a worker configuration in the same Azure region where the protected SQL database resides, as described in section Adding Worker Configurations. When creating the configuration, make sure to select a VNet for the worker instances.

## Step 3. Add VNets to Private DNS Zones

To allow Veeam Backup for Microsoft Azure to perform backup operations in the private environment, you must add the VNet to which the backup appliance is connected and the VNet selected for the worker configuration created at step 2 to the DNS zones *privatelink.blob.core.windows.net* and *privatelink.queue.core.windows.net* created at step 1.

To add a VNet to a DNS zone, do the following:

1. Log in to the Microsoft Azure portal.
2. Open the **Resource group** page.
3. In the **Resource** list, locate and click the necessary VNet. The **Virtual network** page will open.
4. Navigate to **JSON view**. In the **Resource JSON** window, navigate to the **Resource ID** field and copy the ID to the clipboard.
5. Back to the **Resource group** page, in the **Resource** list, locate and click the necessary private DNS zone.
6. On the **Private DNS zone** page, navigate to **Settings** > **Virtual network links** and click **Add**.
7. In the **Add virtual network link** window, create a link to the VNet:
   a. In the **Link name** field, specify a name for the link.
   b. In the **Virtual network details** section, select the **I know the resource ID of virtual network** check box.
   c. In the **Resource ID** field, paste the ID of the VNet.
   d. Click **OK**.

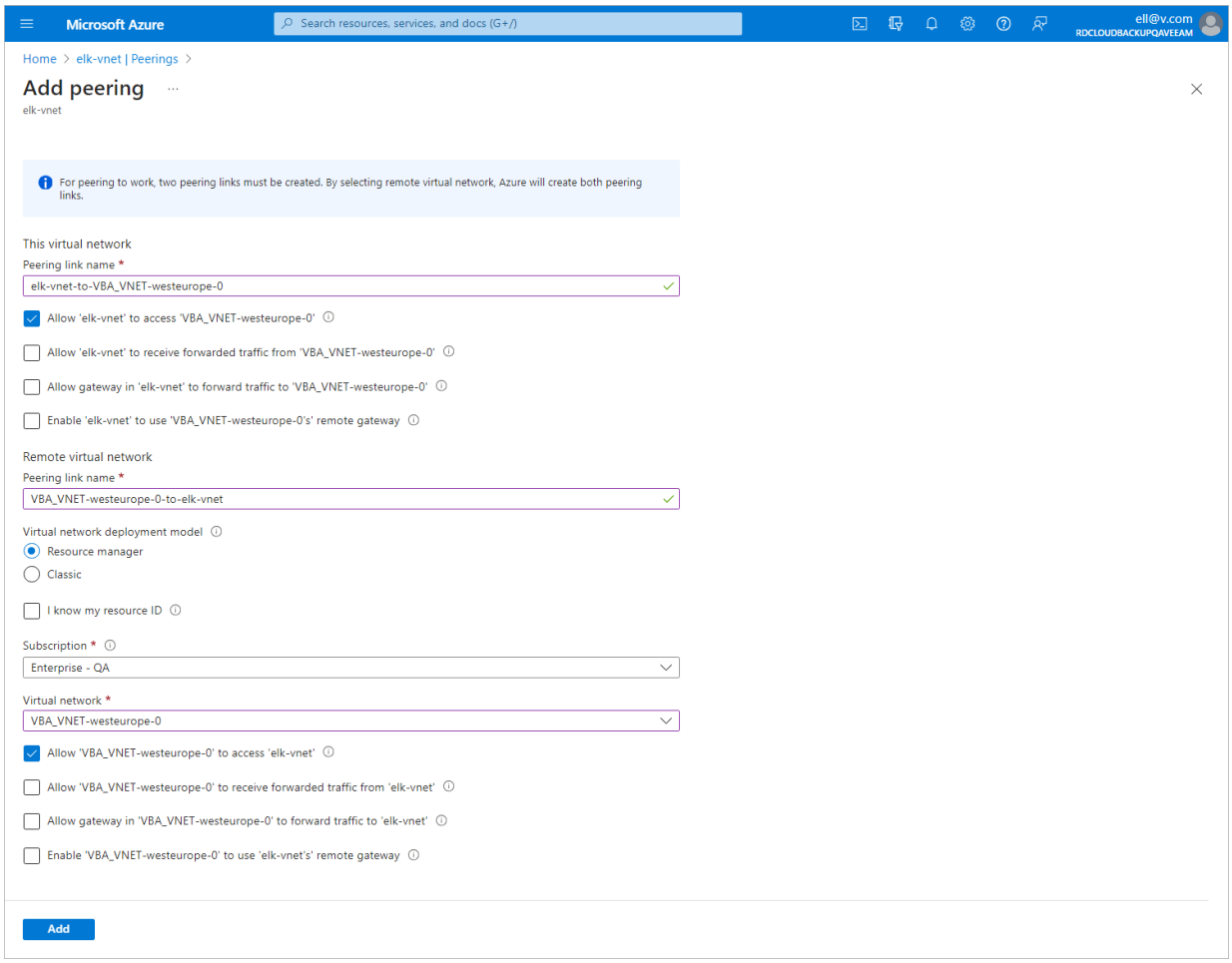


## Step 4. Configure Network Settings for Backup Appliance

To allow Veeam Backup for Microsoft Azure components to communicate in the private environment, you must configure a peering connection between the the VNet to which the backup appliance is connected and the VNet to which worker instances are connected. To do that, perform the following steps:

1. Log in to the Microsoft Azure portal.
2. Open the **Resource group** page.
3. In the **Resource** list, locate and click the VNet to which the backup appliance is connected. The **Virtual network** page will open.
4. Navigate to **Settings** > **Peerings**.
5. Click **Add** to open the **Add peering** page.
6. On the **Add peering** page, specify the following settings:
   a. In the **This virtual network** section, specify a name for the peering link that will be added to the VNet to which the backup appliance is connected. Leave the default settings for the other options in this section.
   b. In the **Remote virtual network** section, specify a name for the peering link that will be added to the target VNet. Leave the default settings for the other options in this section.
   c. From the **Subscription** drop-down list, select an Azure subscription to which worker instances belong.
   d. From the **Virtual networks** drop-down list, select the virtual network to which worker instances are connected.

e. Click **Add**.


Microsoft Azure
Search resources, services, and docs (G+/)
ell@v.com
RDCLOUDBACKUPQAVEEAM
Home > elk-vnet | Peerings >
Add peering
elk-vnet
For peering to work, two peering links must be created. By selecting remote virtual network, Azure will create both peering links.
This virtual network
Peering link name *
elk-vnet-to-VBA_VNET-westeurope-0
Allow 'elk-vnet' to access 'VBA_VNET-westeurope-0'
Allow 'elk-vnet' to receive forwarded traffic from 'VBA_VNET-westeurope-0'
Allow gateway in 'elk-vnet' to forward traffic to 'VBA_VNET-westeurope-0'
Enable 'elk-vnet' to use 'VBA_VNET-westeurope-0's' remote gateway
Remote virtual network
Peering link name *
VBA_VNET-westeurope-0-to-elk-vnet
Virtual network deployment model
Resource manager
Classic
I know my resource ID
Subscription *
Enterprise - QA
Virtual network *
VBA_VNET-westeurope-0
Allow 'VBA_VNET-westeurope-0' to access 'elk-vnet'
Allow 'VBA_VNET-westeurope-0' to receive forwarded traffic from 'elk-vnet'
Allow gateway in 'VBA_VNET-westeurope-0' to forward traffic to 'elk-vnet'
Enable 'VBA_VNET-westeurope-0' to use 'elk-vnet's' remote gateway
Add

## Step 5. Create and Launch Backup Policy

To allow Veeam Backup for Microsoft Azure to protect Azure SQL databases in the private environment, create and launch a backup policy as described in section Performing SQL Backup.

Consider that the backup policy is launched at this step only to automatically create and configure Veeam storage accounts and private endpoints that will further be used for backup operations. As soon as Veeam Backup for Microsoft Azure performs the necessary configuration steps, the policy will fail as some additional manual configuration actions with the private endpoints will still be required. For more information, see Configuring Automatically Created Private Endpoints.

## Step 6. Configure Automatically Created Private Endpoints

For Veeam Backup for Microsoft Azure to be able to establish private connections with the protected Azure VMs, you must configure DNS settings for private endpoints that Veeam Backup for Microsoft Azure automatically created in Microsoft Azure at step 5. Private endpoints are network interfaces that use private IP addresses from VNets. For more information on private endpoints, see Microsoft Docs.

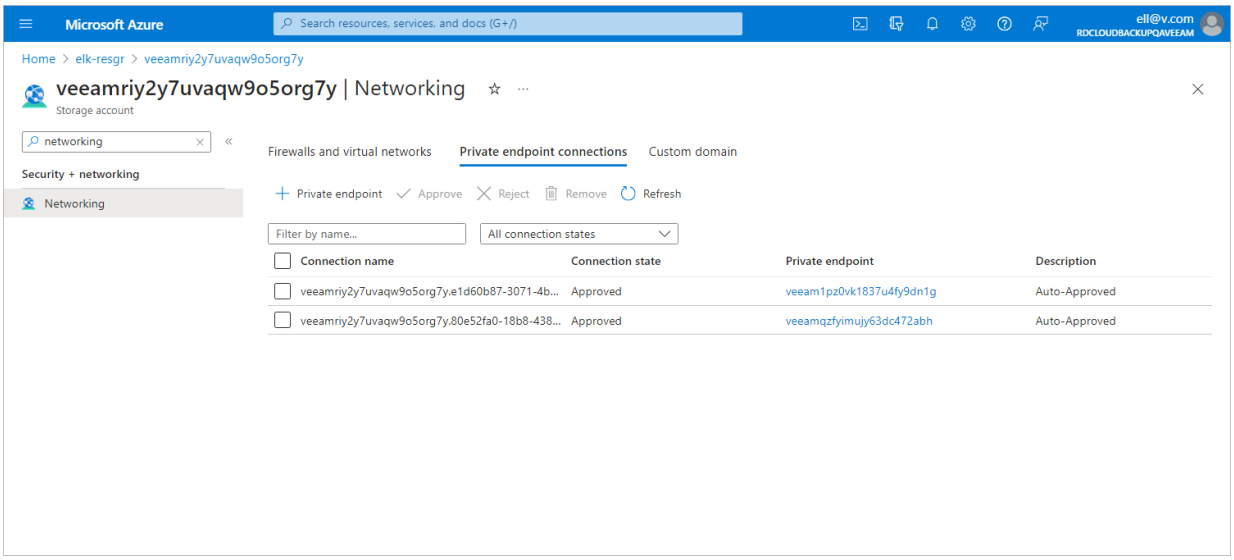
To configure DNS settings for private endpoints, perform the following steps:

1. Locate private endpoints for your Veeam storage account in Microsoft Azure.
2. Configure the private endpoint for Azure Blob Storage.
3. Configure private endpoint for Azure Queue Storage.

## Step 6a. Locate Private Endpoints

To locate the automatically created private endpoints, do the following:

1. Log in to the Microsoft Azure portal.
2. Click **More services** and select **Resource groups** on the **All services** page.
3. On the **Resource groups** page, select the resource group to which the necessary storage account belongs. The resource group page will open.
4. In the **Resources** list, search for storage accounts that are assigned the *Veeam backup appliance ID* tag.
5. Click the necessary storage account. The **Storage account** page will open.
6. Navigate to **Security + networking** > **Networking** and switch to the **Private endpoint connections** tab.

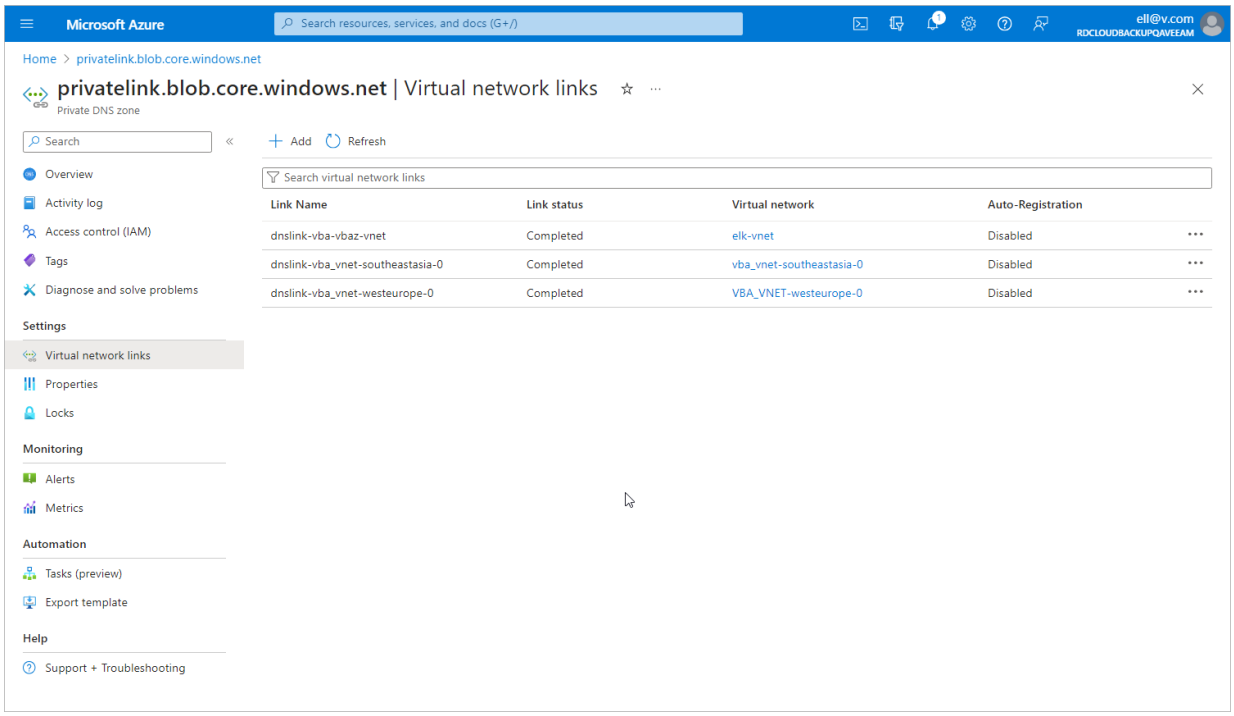


## Step 6b. Configure Private Endpoint for Azure Blob Storage

To configure DNS settings for the private endpoint that Veeam Backup for Microsoft Azure automatically created for Azure Blob Storage, do the following:

1. In the **Private endpoint connections** tab of the **Networking** window of the Veeam storage account selected at step 6a, locate the private endpoint created for Azure Blob Storage. To do that, click the link in the **Private endpoint** column. The private endpoint for Azure Blob Storage will have the *blob* value set in the **Target sub-resource** field.
2. In the **Private endpoint** window, navigate to **Settings** > **DNS Configuration** and click **Add configuration**.
3. In the **Add DNS zone configuration** window, do the following:
   a. From the **Subscription** drop-down list, select the subscription where the DNS zones created at step 1 reside.
   b. From the **Private DNS zone** drop-down list, select the pair of the *privatelink.blob.core.windows.net* name and the resource group in which the DNS zone was created. Leave the default settings for the other options in this window.
   c. Click **Add**.
4. In the private DNS zone, create an 'A' record for the added private endpoint as described in Microsoft Docs.
5. In the **DNS configuration** window, navigate to the newly created DNS configuration and click the link in the **Private DNS zone** column.
6. In the **Private DNS zone** window, navigate to **DNS Management** > **Virtual network links** and click **Add**.
7. In the **Add virtual network link** window, add to the DNS zone links to the VNet to which the backup appliance is connected, and to VNets to which the worker instances are connected. To do that, perform the following steps for each VNet link:
   a. In the **Link name** field, specify a name for the link.
   b. From the **Subscription** drop-down list, select the subscription where the VNet resides.
   c. From the **Virtual network** drop-down list, select the name of the VNet.
   d. Click **OK**.

8. In the **Virtual network links** window, make sure that you have added links to all the necessary VNets.

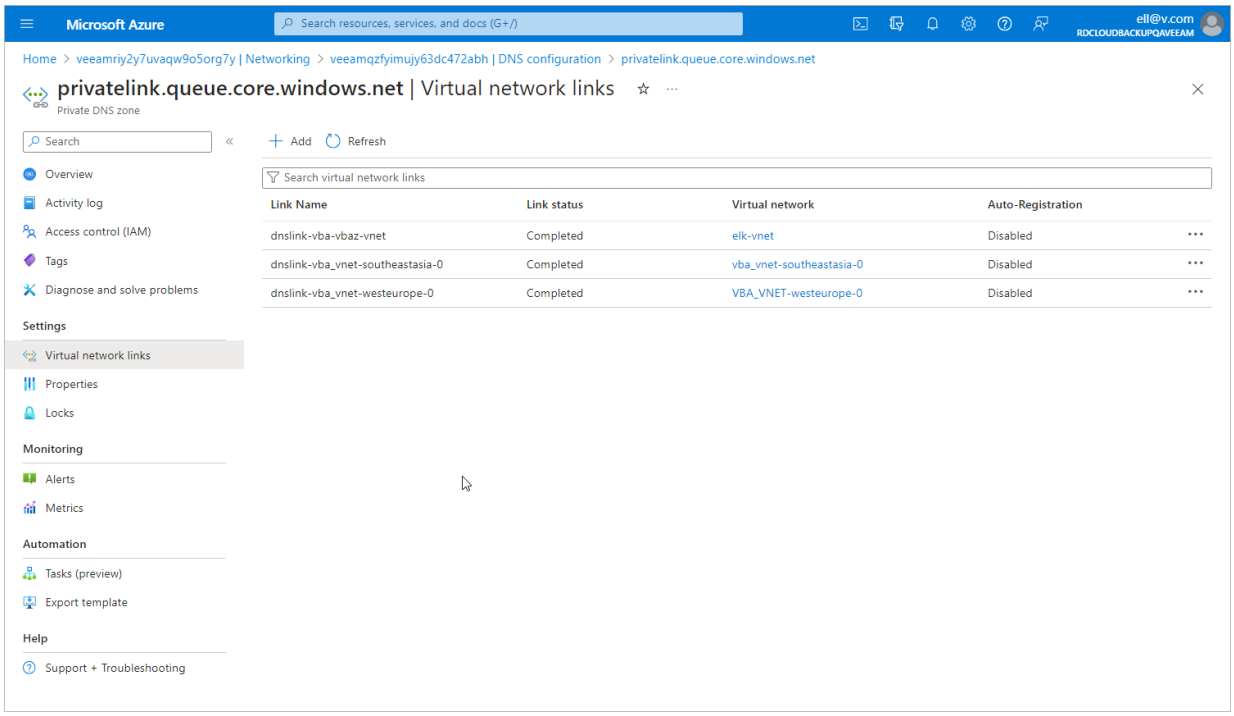


## Step 6c. Configure Private Endpoint for Azure Queue Storage

To configure DNS settings for the private endpoint that Veeam Backup for Microsoft Azure automatically created for Azure Queue Storage, do the following:

1. In the **Private endpoint connections** tab of the **Networking** window of the Veeam storage account selected at step 6a, locate the private endpoint created for Azure Queue Storage. To do that, click the link in the **Private endpoint** column. The private endpoint for Azure Queue Storage will have the *queue* value set in the **Target sub-resource** field.
2. In the **Private endpoint** window, navigate to **Settings** > **DNS Configuration** and click **Add configuration**.
3. In the **Add DNS zone configuration** window, do the following:
   a. From the **Subscription** drop-down list, select the subscription where the DNS zones created at step 1 reside.
   b. From the **Private DNS zone** drop-down list, select the pair of the *privatelink.queue.core.windows.net* name and the resource group in which the DNS zone was created. Leave the default settings for the other options in this window.
   c. Click **Add**.
4. In the private DNS zone, create an 'A' record for the added private endpoint as described in Microsoft Docs.
5. In the **DNS configuration** window, navigate to the newly created DNS configuration and click the link in the **Private DNS zone** column.
6. In the **Private DNS zone** window, navigate to **DNS Management** > **Virtual network links** and click **Add**.
7. In the **Add virtual network link** window, add to the DNS zone links to the VNet to which the backup appliance is connected, and to VNets to which the worker instances are connected. To do that, perform the following steps for each VNet link:
   a. In the **Link name** field, specify a name for the link.
   b. From the **Subscription** drop-down list, select the subscription where the VNet resides.
   c. From the **Virtual network** drop-down list, select the name of the VNet.
   d. Click **OK**.

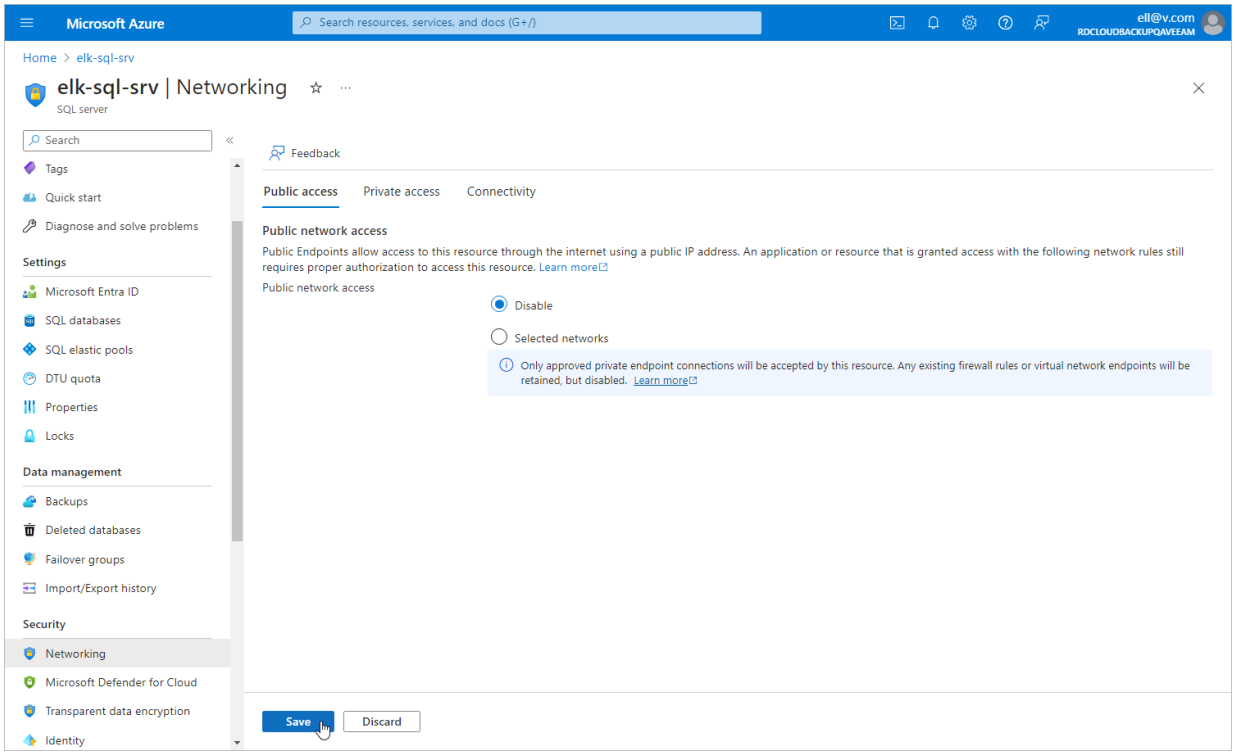
8. In the **Virtual network links** window, make sure that you have added links to all the necessary VNets.



## Step 7. Disable Public Access to SQL Server

For the SQL Server that you want to protect to be inaccessible through public network, you must disable public access to this SQL Server:

1. Log in to the Microsoft Azure portal.
2. Click **More services** and select **Resource groups** on the **All services** page.
3. On the **Resource groups** page, select the resource group to which the necessary SQL Server belongs. The resource group page will open.
4. In the **Resource** list, locate and click the SQL Server that you want to protect. The **SQL server** page will open.
5. Navigate to **Security** > **Networking**.
6. In the **Public access** tab, select the **Disable** option and click **Save**.



## Step 8. Create Private Endpoint for SQL Server

To allow Veeam Backup for Microsoft Azure access to the databases that you want to protect, you must create private endpoints for your SQL Server.

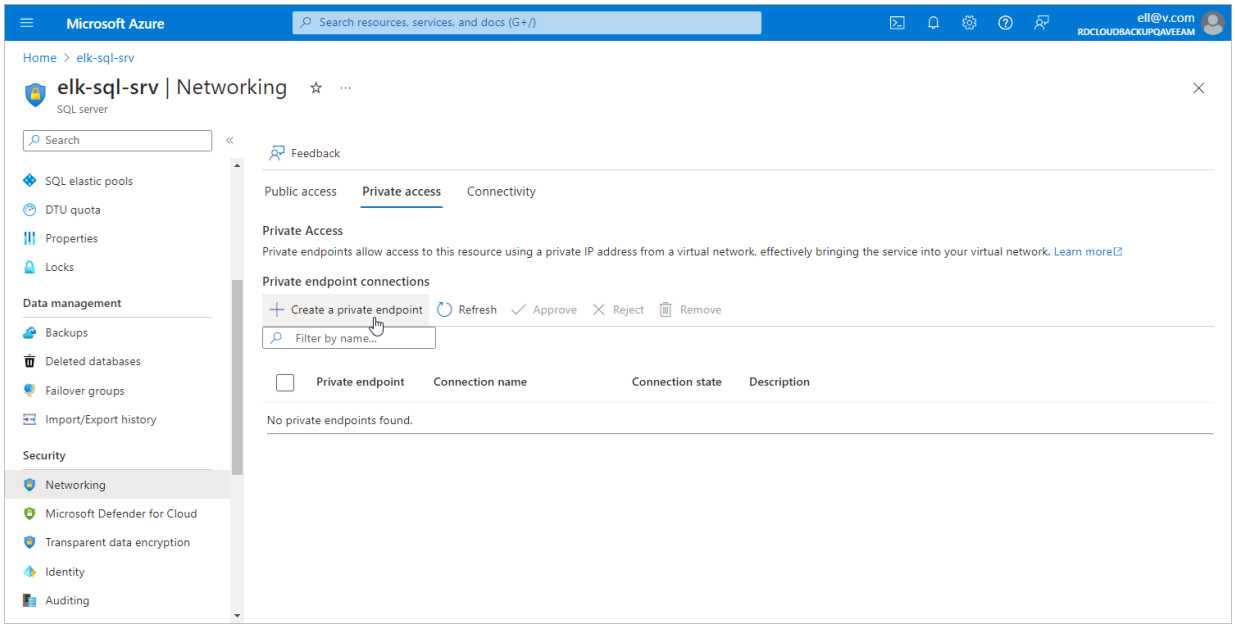
You must create a separate private endpoint for every VNet to which worker instances are connected. To create a private endpoint, complete the following steps:

1. Launch the Create a private endpoint wizard.
2. Configure private endpoint settings.
3. Specify resource settings.
4. Specify network settings.
5. Specify DNS settings.
6. Assign tags.
7. Finish working with the wizard.

## Step 8a. Launch Create a Private Endpoint Wizard

To launch the **Create a private endpoint** wizard for a SQL Server for which you want to create a private endpoint, do the following:

1. Log in to the Microsoft Azure portal.
2. Click **More services** and select **Resource groups** on the **All services** page.
3. On the **Resource groups** page, select the resource group to which the necessary SQL Server belongs. The resource group page will open.
4. In the **Resource** list, locate and click the SQL Server that you want to protect. The **SQL server** page will open.
5. Navigate to **Security** > **Networking**.
6. Switch to the **Private access** tab and click **Create a private endpoint**.

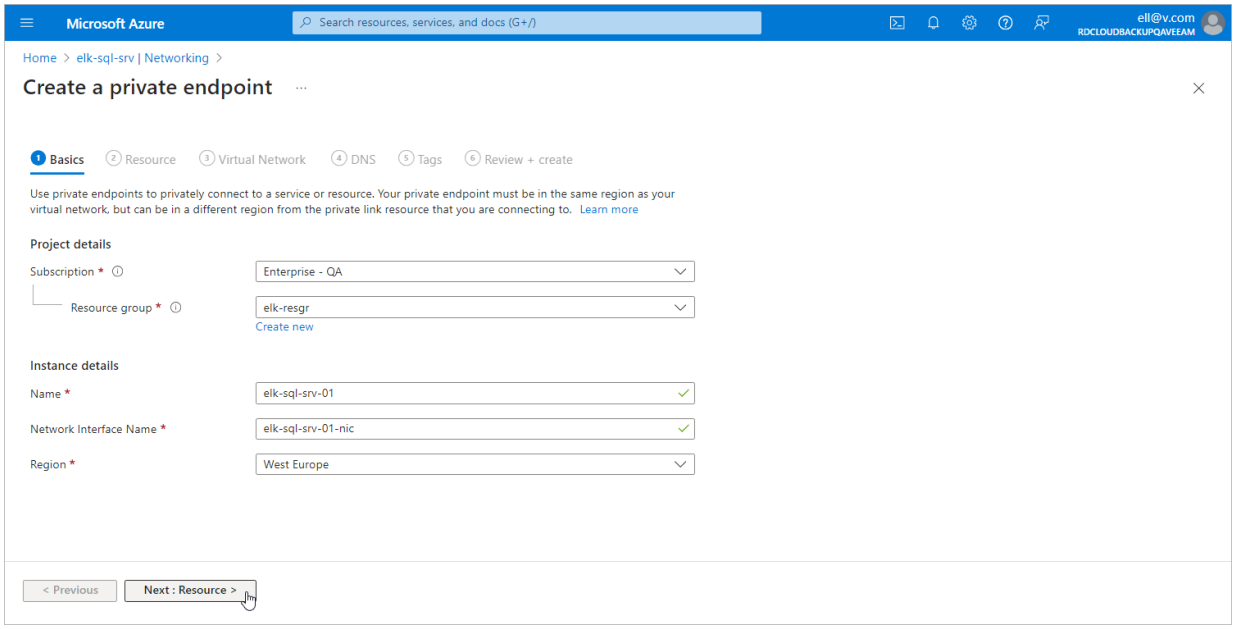


## Step 8b. Configure Private Endpoint Settings

At the **Basics** step of the **Create a private endpoint** wizard, do the following:

1. From the **Subscription** drop-down list, select an Azure subscription to which Azure VM hosting Veeam Backup for Microsoft Azure belongs.
2. From the **Resource group** drop-down list, select a resource group to which your newly created private endpoint will belong. You can either use an existing resource group or create a new one. For more information on creating and managing resource groups, see Microsoft Docs.
3. In the **Name** field, enter a name for the private endpoint.
4. From the **Region** drop-down list, select an Azure region of the virtual network to which worker instances are connected.

   For more information on the Azure regions, see Microsoft Docs.
5. Click **Next: Resource >**.



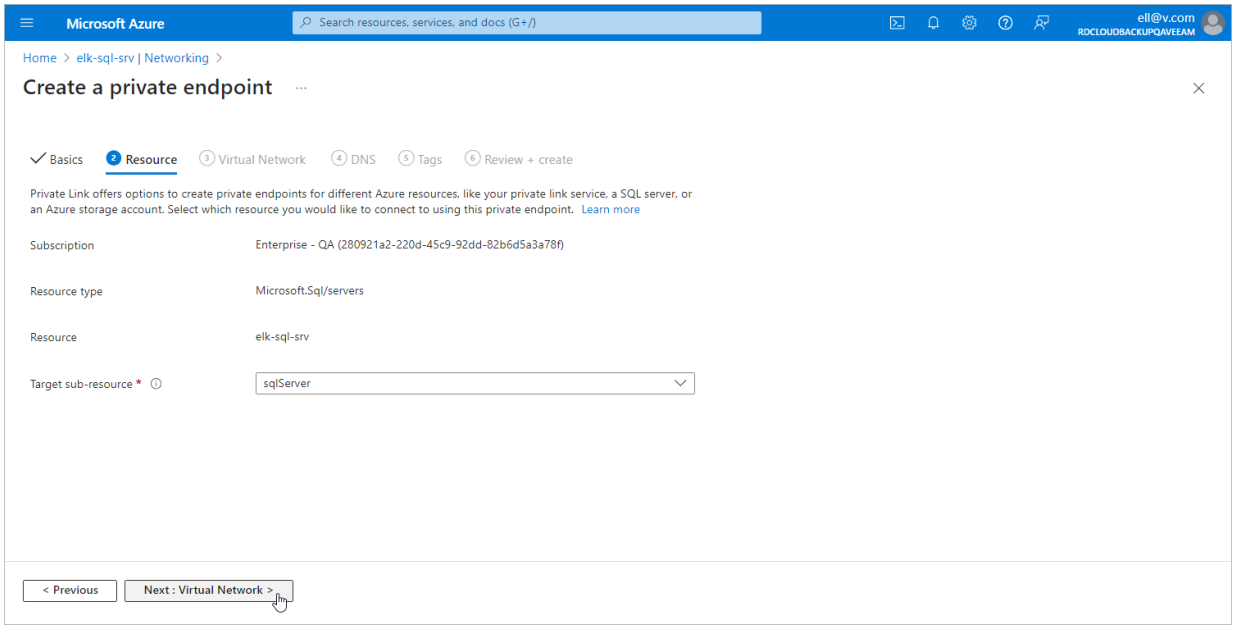
## Step 8c. Specify Resource Settings

At the **Resource** step of the **Create a private endpoint** wizard, do the following:

1. From the **Subscription** drop-down list, select an Azure subscription to which a SQL Server that you want to protect belongs.
2. From the **Resource type** drop-down list, select the *Microsoft.Sql/servers* type.
3. From the **Resource** drop-down list, select the SQL Server that you want to protect.

> **IMPORTANT**
>
> If you plan to back up SQL databases using a staging server, you must select the SQL Server that will be used as a staging one. To learn how to use staging servers, see Performing Backup.

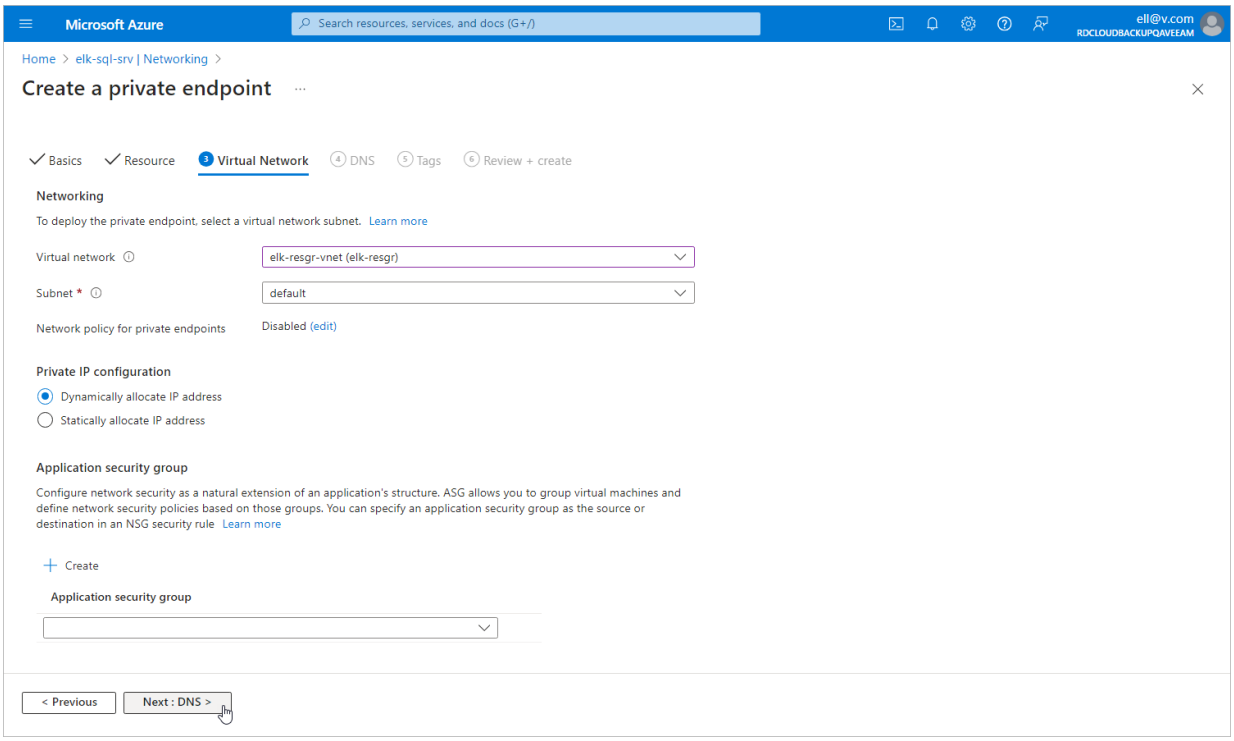
4. From the **Target sub-resource** drop-down list, select *sqlServer*.
5. Click **Next: Virtual Network >**.



## Step 8d. Specify Virtual Network Settings

At the **Virtual Network** step of the **Create a private endpoint** wizard, do the following:

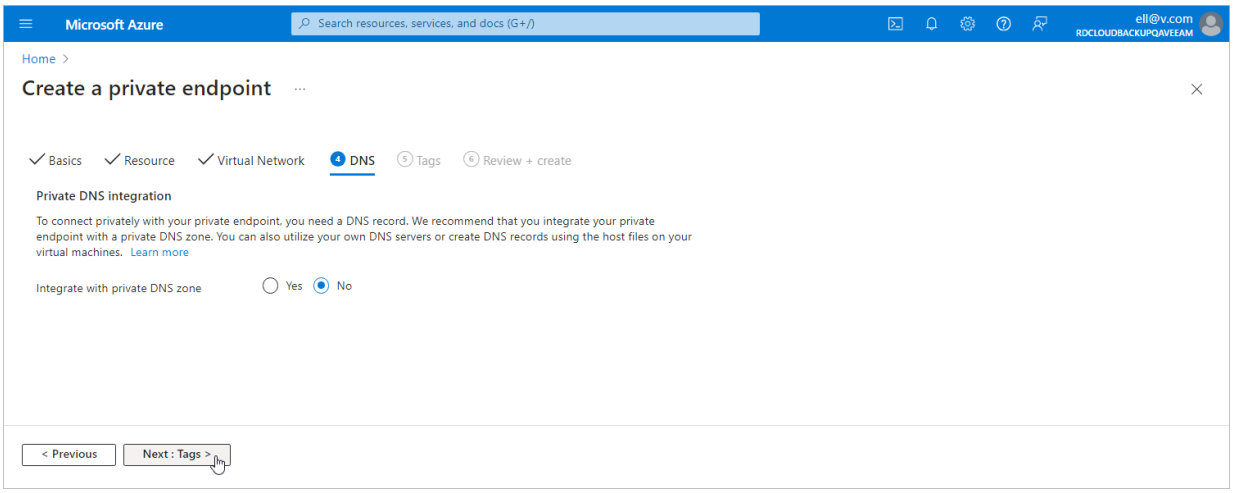
1. From the **Virtual network** drop-down list, select a virtual network to which worker instances are connected.
2. From the **Subnet** drop-down list, select a subnet to which worker instances are connected. For a subnet to be displayed in the list, it must be created within the selected virtual network as described in Microsoft Docs.
3. Click **Next: DNS >**.



## Step 8e. Specify DNS Settings

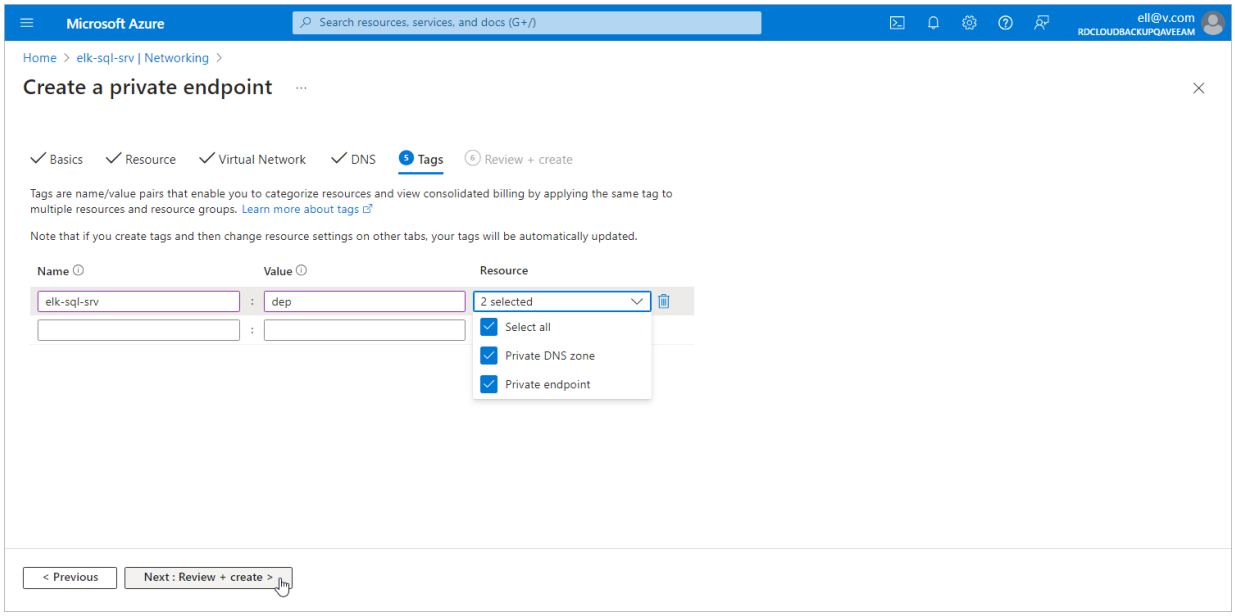
At the **DNS** step of the **Create a private endpoint** wizard, do the following:

1. In the **Private DNS integration** section, navigate to the **Integrate with private DNS zone** field and click **No**.
2. Click **Next: Tags >**.



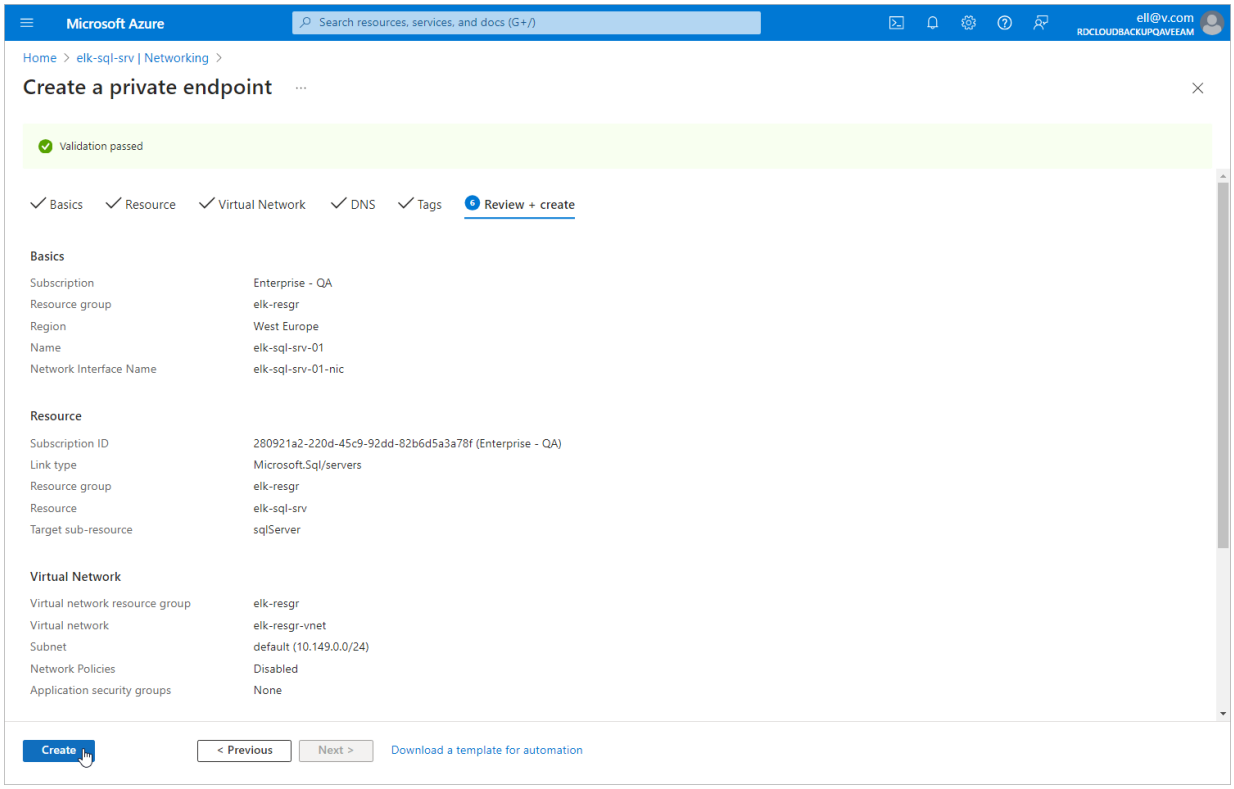
## Step 8f. Assign Tags

At the **Targets** step of the **Create a private endpoint** wizard, you can assign tags to the newly created private endpoint and private DNS zone if needed.



## Step 8g. Finish Working with Wizard

At the **Review + create** step of the **Create a private endpoint** wizard, review configured settings and click **Create**.

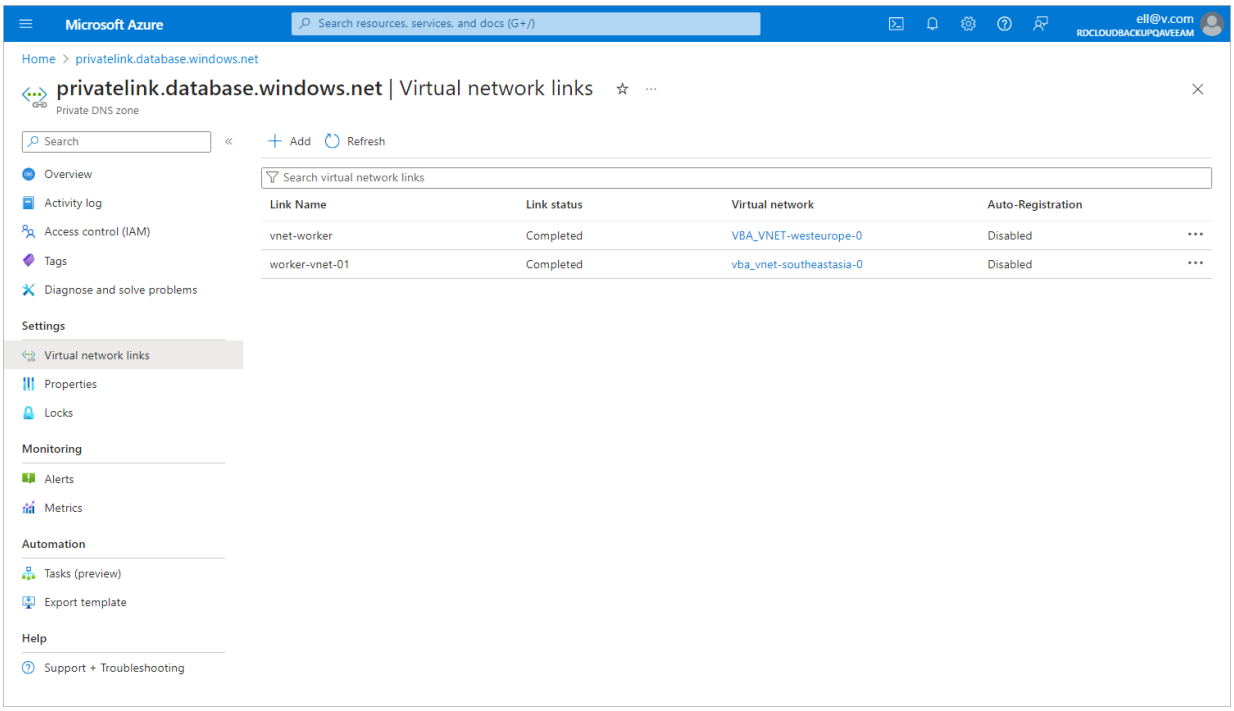


## Step 9. Configure Private Endpoint for SQL Server

To configure DNS settings for the private endpoint created at step 8, do the following:

1. Log in to the Microsoft Azure portal.
2. Click **More services** and select **Resource groups** on the **All services** page.
3. On the **Resource groups** page, select the resource group to which the necessary SQL Server belongs. The resource group page will open.
4. In the **Resource** list, locate and click the SQL Server that you want to protect. The **SQL Server** page will open.
5. Navigate to **Security** > **Networking**.
6. In the **Private access** tab, navigate to the **Private endpoint connections** section and click the private endpoint created at step 8.
7. In the **Private endpoint** window, navigate to **Settings** > **DNS Configuration** and click **Add configuration**.
8. In the **Add DNS zone configuration** window, do the following:
   a. From the **Subscription** drop-down list, select the subscription where the DNS zones created at step 1 reside.
   b. From the **Private DNS zone** drop-down list, select the pair of the *privatelink.database.windows.net* name and the resource group in which the DNS zone was created. Leave the default settings for the other options in this window.
   c. Click **Add**.
9. In the private DNS zone, create an 'A' record for the private endpoint as described in Microsoft Docs.
10. In the **DNS configuration** window, navigate to the newly created DNS configuration and click the link in the **Private DNS zone** column.
11. In the **Private DNS zone** window, navigate to **DNS Management** > **Virtual network links** and click **Add**.
12. In the **Add virtual network link** window, add to the DNS zone links to the VNets to which the worker instances are connected. To do that, perform the following steps for each VNet link:
    a. In the **Link name** field, specify a name for the link.
    b. From the **Subscription** drop-down list, select the subscription where the VNet resides.
    c. From the **Virtual network** drop-down list, select the name of the VNet.
    d. Click **OK**.

13. In the **Virtual network links** window, make sure that you have added links to all the necessary VNets.



### Step 10. Launch Test Backup Policy

To make sure that all configuration steps were performed correctly, run the backup policy created at step 5.

Consider that worker instances will need public access to the Ubuntu repositories to install updates as described in section Ports. If you do not want Veeam Backup for Microsoft Azure to update worker instances, open a support case.

## Configuring Network Settings for SQL Managed Instances

> **IMPORTANT**
>
> Before you configure network settings for a SQL Managed Instance, disable the public endpoint for this SQL Managed Instance as described in Microsoft Docs.

To allow Veeam Backup for Microsoft Azure to back up a SQL Managed Instance, you must configure the peering connection between the VNet to which worker instances are connected and the VNet to which a SQL Managed Instance is connected. To do that, perform the following steps:

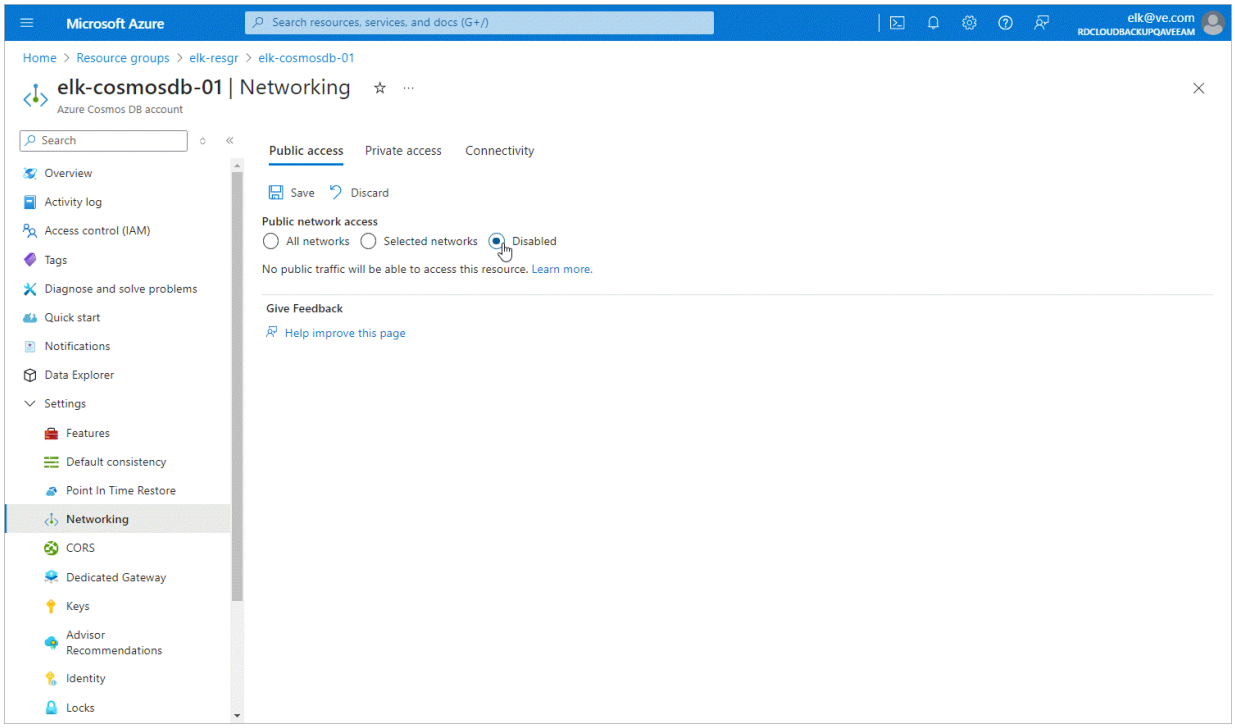
1. Log in to the Microsoft Azure portal.
2. Open the **Resource group** page.
3. In the **Resource** list, locate and click a virtual network to which the SQL Managed Instance is connected. The **Virtual network** page will open.
4. Navigate to **Settings** > **Peering**.
5. Click **Add** to open the **Add peering** page.
6. On the **Add peering** page, specify the following settings:
   a. In the **This virtual network** section, specify a name for the peering link that will be added to the VNet to which the SQL Managed Instance is connected. Leave the default settings for the other options in this section.
   b. In the **Remote virtual network** section, specify a name for the peering link that will be added to the VNet to which worker instances are connected. Leave the default settings for the other options in this section.
   c. From the **Subscription** drop-down list, select an Azure subscription to which worker instances belong.
   d. From the **Virtual networks** drop-down list, select the virtual network to which worker instances are connected.
   e. Click **Add**.

## Configuring Networking Settings for Cosmos DB Accounts

To allow Veeam Backup for Microsoft Azure to back up a Cosmos DB account in a private environment, you must disable public access to this account:

1. Log in to the Microsoft Azure portal.
2. Click **More services** and select **Resource groups** on the **All services** page.
3. On the **Resource groups** page, select the resource group to which the necessary Cosmos DB account belongs. The resource group page will open.

4. In the **Resource** list, locate and click the Cosmos DB account that you want to protect. The **Azure Cosmos DB account** page will open.
5. Navigate to **Settings** > **Networking**.
6. In the **Public access** tab, navigate to **Public network access** and select the **Disabled** option.




# Backup to Repository

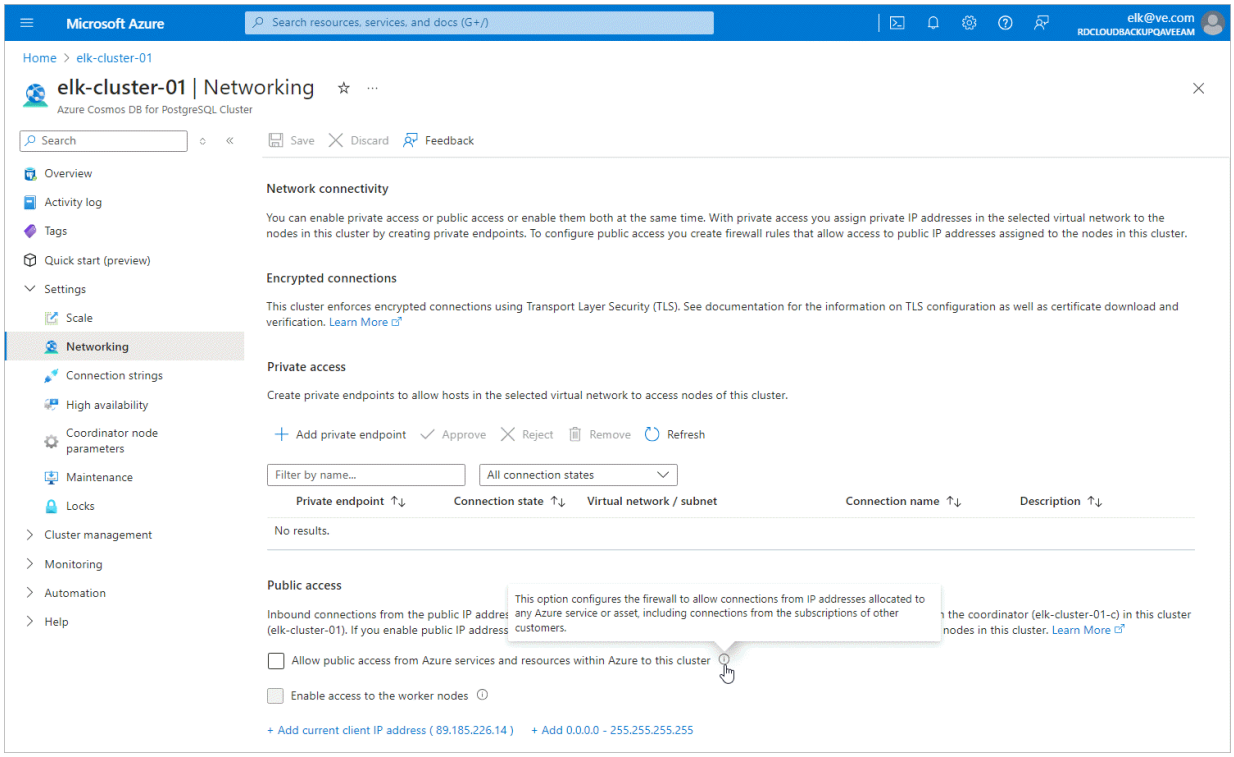
If you enable backup to a repository, you must perform the following steps:

1. Disable public access to the Cosmos DB for PostgreSQL account.
2. Create private endpoints for the Cosmos DB for PostgreSQL account.
3. Configure network settings for the private endpoints.

## Step 1. Disable Public Access Cosmos DB Account

For the Cosmos DB for PostgreSQL account that you want to protect to be inaccessible through public network, you must disable public access to this account:

1. Log in to the Microsoft Azure portal.
2. Click **More services** and select **Resource groups** on the **All services** page.
3. On the **Resource groups** page, select the resource group to which the necessary Cosmos DB for PostgreSQL cluster belongs. The resource group page will open.
4. In the **Resource** list, locate and click the cluster that you want to protect. The **Azure Cosmos DB for PostgreSQL Cluster** page will open.
5. Navigate to **Settings** > **Networking**.
6. In the **Public access** section, make sure the **Allow public access from Azure services and resources within Azure to this cluster** check box is not selected.



## Step 2. Create Private Endpoints for Cosmos DB Account

To allow Veeam Backup for Microsoft Azure access to the databases that you want to protect, you must create private endpoints for your Cosmos DB for PostgreSQL account.

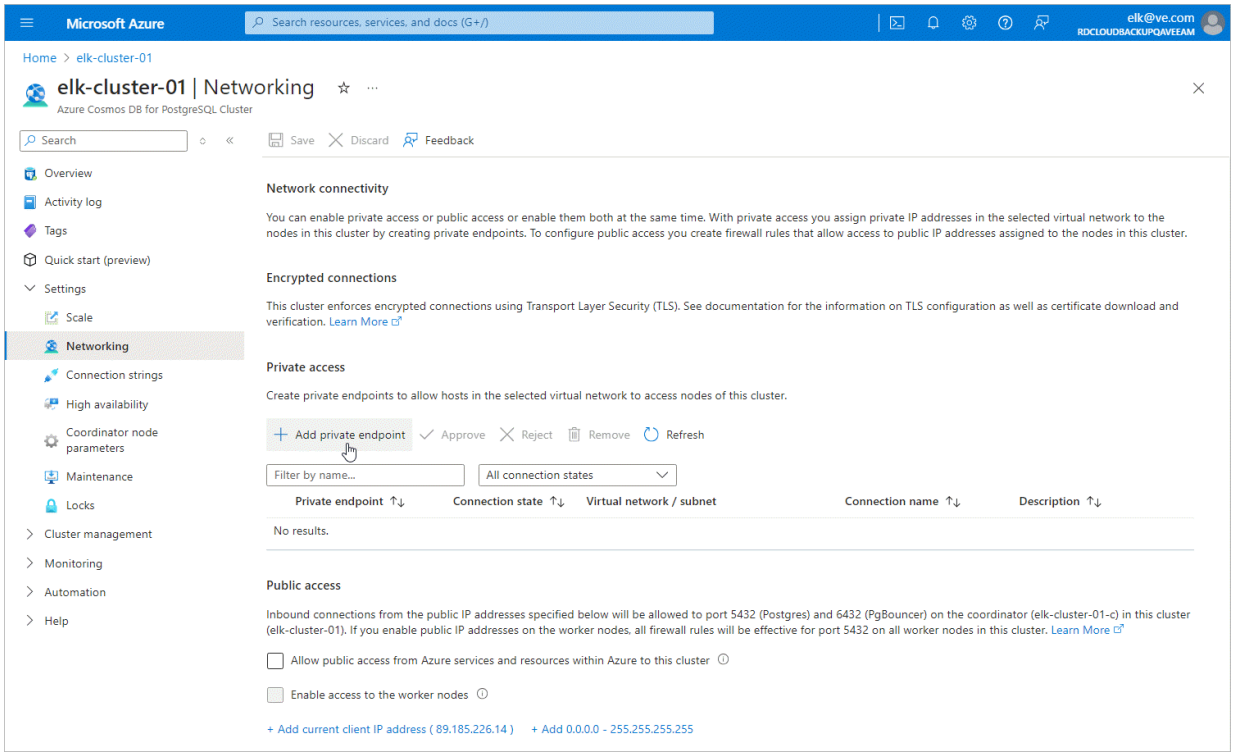
You must create a separate private endpoint for every VNet to which worker instances are connected. To create a private endpoint, complete the following steps:

1. Launch the Create a private endpoint wizard.
2. Configure private endpoint settings.
3. Specify resource settings.
4. Specify network settings.
5. Specify DNS settings.
6. Assign tags.
7. Finish working with the wizard.

## Step 2a. Launch Create a Private Endpoint Wizard

To launch the **Create a private endpoint** wizard for a Cosmos DB for PostgreSQL account for which you want to create a private endpoint, do the following:

1. Log in to the Microsoft Azure portal.
2. Click **More services** and select **Resource groups** on the **All services** page.
3. On the **Resource groups** page, select the resource group to which the necessary Cosmos DB for PostgreSQL cluster belongs. The resource group page will open.
4. In the **Resource** list, locate and click the cluster that you want to protect. The **Azure Cosmos DB for PostgreSQL Cluster** page will open.
5. Navigate to **Settings** > **Networking**.
6. In the **Private access** section, click **Add private endpoint**.

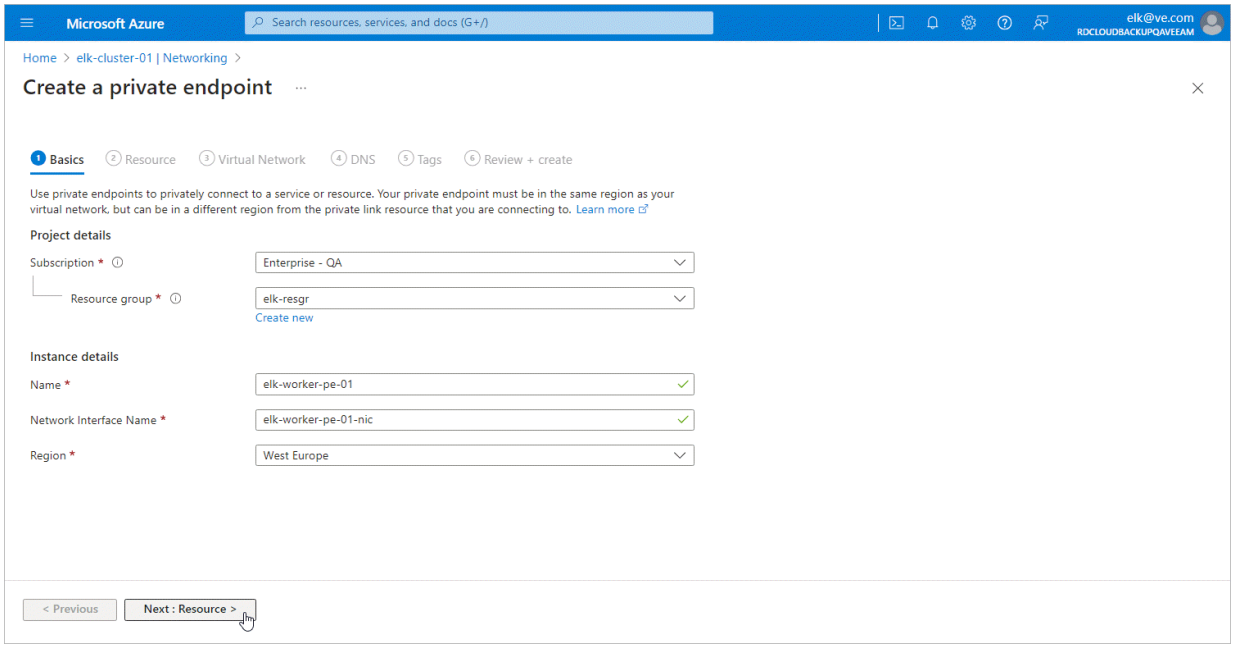


## Step 2b. Configure Private Endpoint Settings

At the **Basics** step of the **Create a private endpoint** wizard, do the following:

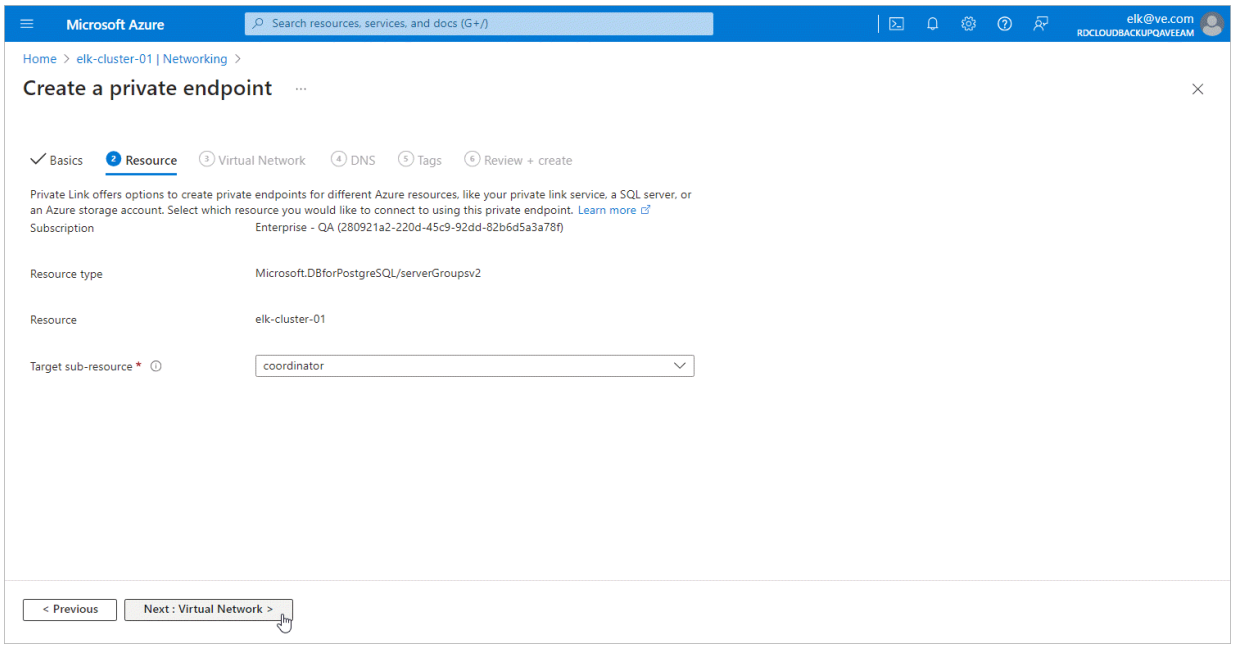
1. From the **Subscription** drop-down list, select an Azure subscription to which Azure VM hosting Veeam Backup for Microsoft Azure belongs.
2. From the **Resource group** drop-down list, select a resource group to which your newly created private endpoint will belong. You can either use an existing resource group or create a new one. For more information on creating and managing resource groups, see Microsoft Docs.
3. In the **Name** field, enter a name for the private endpoint.
4. From the **Region** drop-down list, select an Azure region of the virtual network to which the backup appliance or worker instances are connected.

   For more information on the Azure regions, see Microsoft Docs.
5. Click **Next: Resource >**.



## Step 2c. Specify Resource Settings

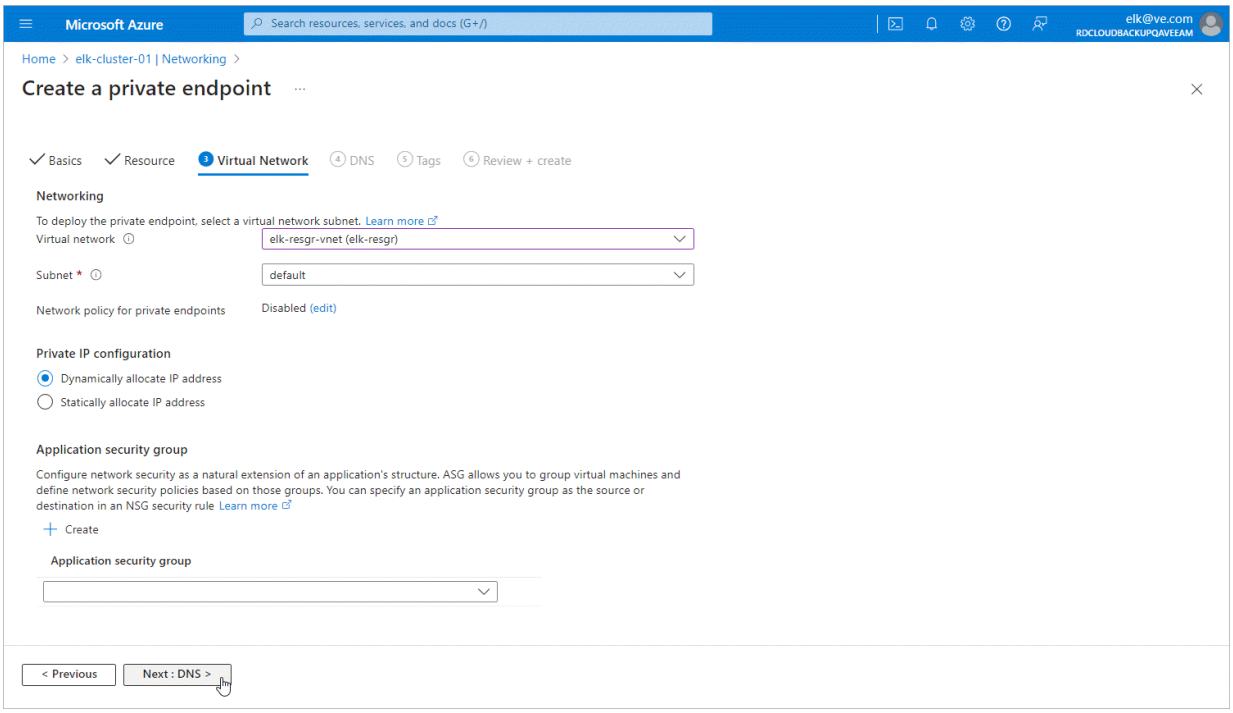
At the **Resource** step of the **Create a private endpoint** wizard, select *coordinator* from the **Target sub-resource** drop-down list and click **Next: Virtual Network >**.



## Step 2d. Specify Virtual Network Settings

At the **Virtual Network** step of the **Create a private endpoint** wizard, do the following:

1. From the **Virtual network** drop-down list, select a virtual network to which worker instances are connected.
2. From the **Subnet** drop-down list, select a subnet to which the backup appliance or worker instances are connected. For a subnet to be displayed in the list, it must be created within the selected virtual network as described in Microsoft Docs.
3. Click **Next: DNS >**.

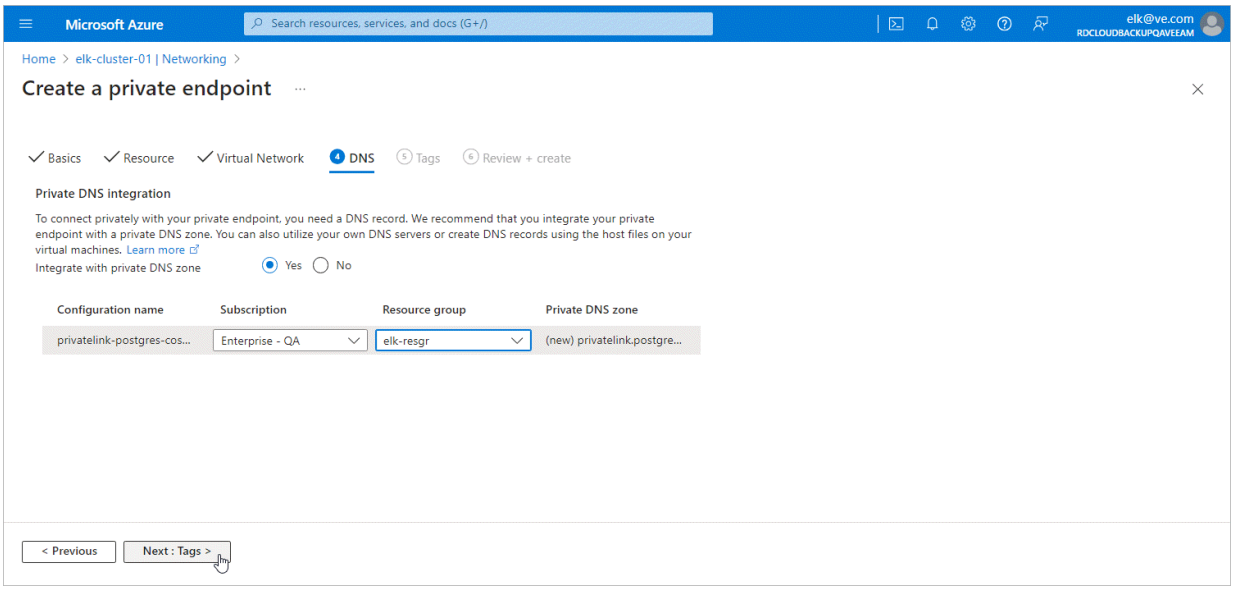


## Step 2e. Specify DNS Settings

At the **DNS** step of the **Create a private endpoint** wizard, do the following:

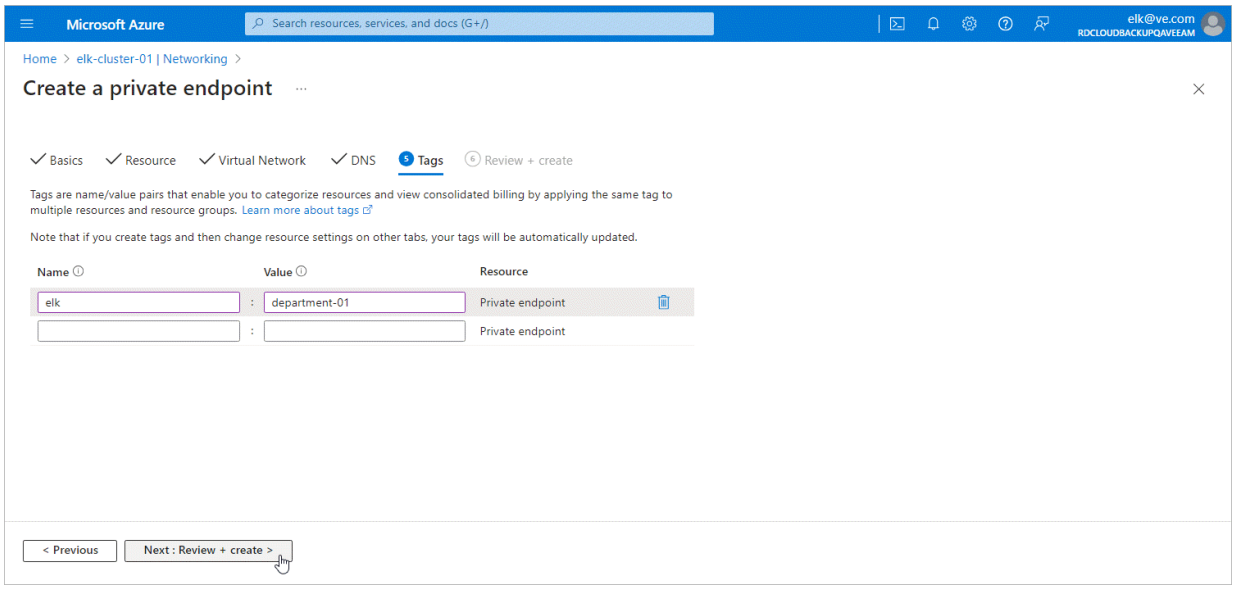
1. In the **Private DNS integration** section, navigate to the **Integrate with private DNS zone** field and click **Yes**.
2. From the **Subscription** and the **Resource group** drop-down lists, select the subscription and the resource group in which the private DNS zone will be created.

   It is recommended that you create the DNS zones in the same resource group where the backup appliance resides, to simplify resource management.
3. Click **Next: Tags >**.



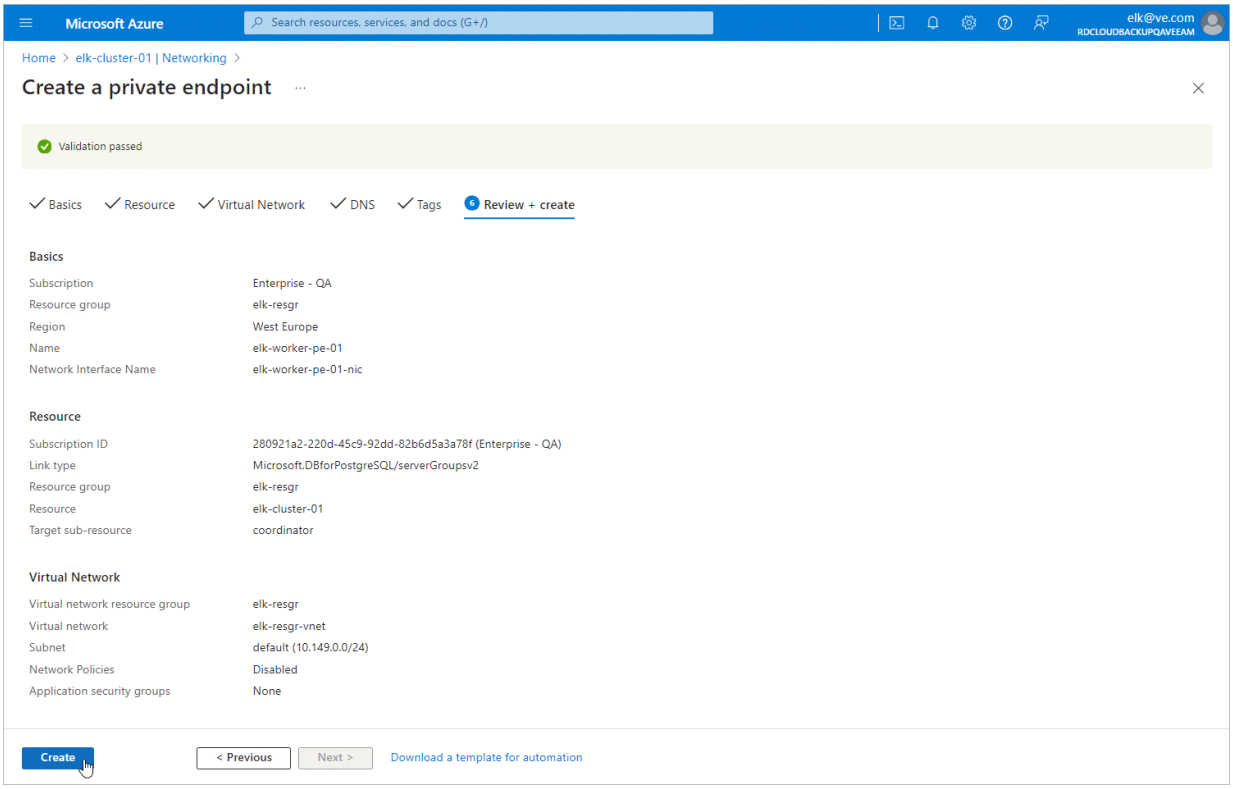
## Step 2f. Assign Tags

At the **Targets** step of the **Create a private endpoint** wizard, you can assign tags to the newly created private endpoint and private DNS zone if needed. Then, click **Review + create >**.



## Step 2g. Finish Working with Wizard

At the **Review + create** step of the **Create a private endpoint** wizard, review configured settings and click **Create**.

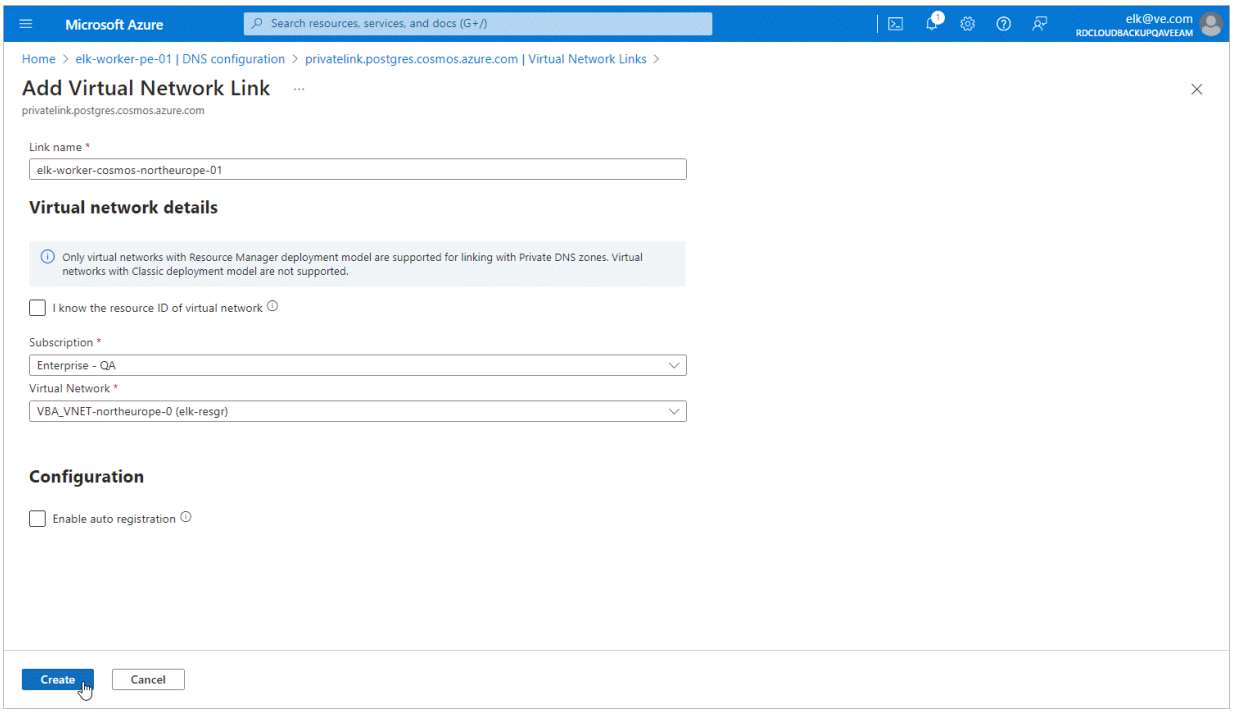


## Step 3. Configure Private Endpoints

To configure DNS settings for the private endpoints created at step 2, do the following:

1. In the **Private access** section of the **Networking** window of the Cosmos DB for PostgreSQL account for which you created the private endpoints, locate the private endpoint that you want to configure and click the link in the **Private endpoint** column.
2. In the **Private endpoint** window, navigate to **Settings** > **DNS Configuration** and click **Add configuration**.
3. In the **Add DNS zone configuration** window, do the following:
   a. From the **Subscription** drop-down list, select the subscription where the DNS zone created at step 2e resides.
   b. From the **Private DNS zone** drop-down list, select the pair of the *privatelink.postgres.cosmos.azure.com* name and the resource group in which the DNS zone was created. Leave the default settings for the other options in this window.
   c. Click **Add**.
4. In the private DNS zone, create an 'A' record for the private endpoint as described in Microsoft Docs.
5. In the **DNS configuration** window, navigate to the newly created DNS configuration and click the in the **Private DNS zone** column.
6. In the **Private DNS zone** window, navigate to **DNS Management** > **Virtual network links** and click **Add**.
7. In the **Add virtual network link** window, add to the DNS zone links to VNets to which the worker instances are connected. To do that, perform the following steps for each VNet link:
   a. In the **Link name** field, specify a name for the link.
   b. From the **Subscription** drop-down list, select the subscription where the VNet resides.
   c. From the **Virtual network** drop-down list, select the name of the VNet.
   d. Click **OK**.

8. In the **Virtual network links** window, make sure that you have added links to all the necessary VNets.




# Configuring Network Settings for Storage Accounts

By default, Veeam Backup for Microsoft Azure uses public access to communicate with Azure storage accounts. However, you can instruct Veeam Backup for Microsoft Azure to access the storage accounts without public IPv4 addresses in the following cases:

- You want Veeam Backup for Microsoft Azure to create and manage backup repositories within a private network.
- You plan to back up unmanaged Azure VMs in a private environment.
- You plan to back up Azure Files in a private environment.

To do that, in a storage account where your repositories or resources reside, you can either add firewall rules that will grant access to specific VNets, or create private endpoints that will be used to connect to the resources.

## Configuring Firewall Settings

To configure firewall rules for a storage account in which Azure resources that you want to protect reside, do the following:

1. Log in to the Microsoft Azure portal.
2. Click **More services** and select **Resource groups** on the **All services** page.
3. On the **Resource groups** page, select the resource group to which the necessary storage account belongs. The resource group page will open.
4. In the **Resource** list, locate and click the storage account. The **Storage account** page will open.
5. Navigate to **Security + networking** > **Networking**.
6. On the **Firewalls and virtual networks** tab, choose the **Enabled from selected virtual networks and IP addresses** option and click **Add existing virtual network**.

7. In the **Add networks** window:
   a. From the **Subscription** drop-down list, select an Azure subscription to which Azure VM hosting Veeam Backup for Microsoft Azure belongs.
   b. From the **Virtual networks** drop-down list, select check boxes next to necessary virtual networks:
      - To allow Veeam Backup for Microsoft Azure to manage backup repositories and to back up Azure VMs, select VNets to which the backup appliance and worker instances are connected.
      - To allow Veeam Backup for Microsoft Azure to back up Azure file shares, select the VNet to which the backup appliance is connected.
   c. From the **Subnets** drop-down list, select check boxes next to subnets to which the backup appliance or worker instances are connected.

> **NOTE**
>
> To allow access from virtual networks to storage accounts, Microsoft Azure uses virtual network service endpoints. If any of the selected networks do not have virtual network service endpoints enabled for *Microsoft.Storage.Global*, Microsoft Azure will raise a warning. In this case, click **Enable** and wait for the process to complete. For more information on virtual network service endpoints, see Microsoft Docs.

   d. Click **Add**.
8. Click **Save**.

## Creating Private Endpoints

If the backup appliance resides in another region than the resources that you want to back up, or you do not want to add firewall rules, you can create private endpoints for your storage account to allow Veeam Backup for Microsoft Azure access to the resources.

You must create a separate private endpoint for every VNet to which the backup appliance or worker instances are connected. To create a private endpoint, perform the following steps:

1. Launch the Create a private endpoint wizard.
2. Configure general settings for the private endpoint.
3. Specify resource settings.
4. Specify virtual network settings.
5. Specify DNS settings.
6. Assign tags.
7. Finish working with the wizard.
8. Configure network settings of the newly created private endpoint.

## Step 1. Launch Create a Private Endpoint Wizard

To launch the **Create a private endpoint** wizard for a storage account in which you want to create a private endpoint, do the following:

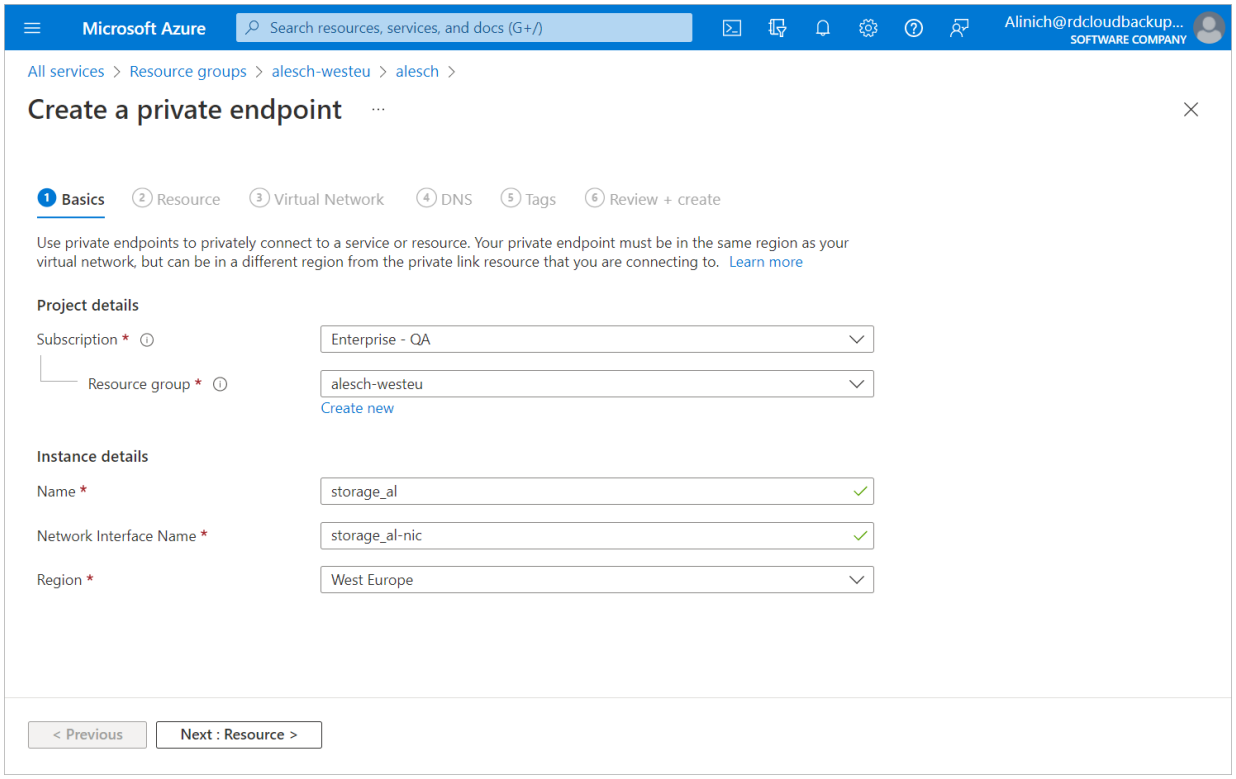
1. Log in to the Microsoft Azure portal.
2. Click **More services** and select **Resource groups** on the **All services** page.
3. On the **Resource groups** page, select the resource group to which the necessary storage account belongs. The resource group page will open.
4. In the **Resources** list, select the storage account. The **Storage account** page will open.
5. Navigate to **Security + networking** > **Networking**.
6. Switch to the **Private endpoint connections** tab and click **Private endpoint**.

## Step 2. Configure Private Endpoint General Settings

At the **Basics** step of the **Create a private endpoint** wizard, do the following:

1. From the **Subscription** drop-down list, select an Azure subscription to which your virtual network belongs.
2. From the **Resource group** drop-down list, select a resource group to which your newly created private endpoint will belong. You can either use an existing resource group or create a new one. For more information on creating and managing resource groups, see Microsoft Docs.
3. In the **Name** field, enter a name for the private endpoint.
4. From the **Region** drop-down list, select an Azure region of the virtual network to which the backup appliance or worker instances are connected.

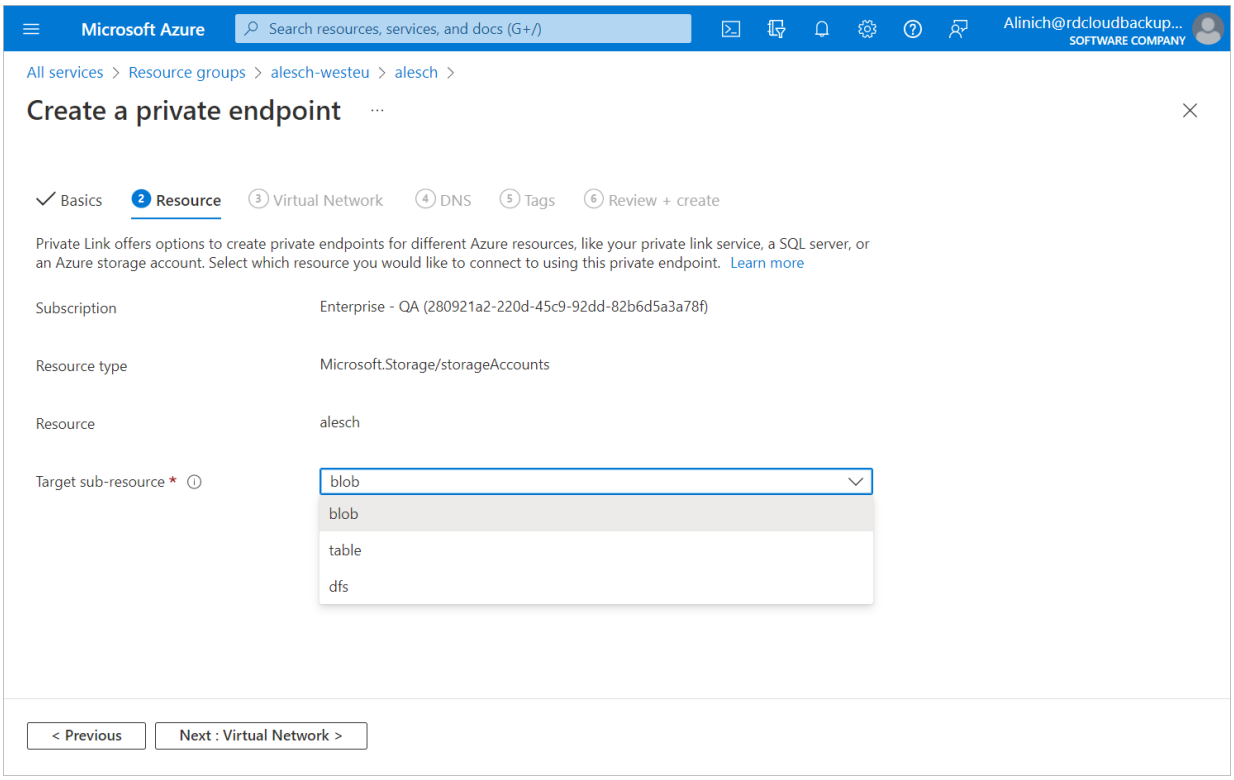
   For more information on the Azure regions, see Microsoft Docs.
5. Click **Next: Resource >**.



## Step 3. Specify Resource Settings

At the **Resource** step of the **Create a private endpoint** wizard, do the following:

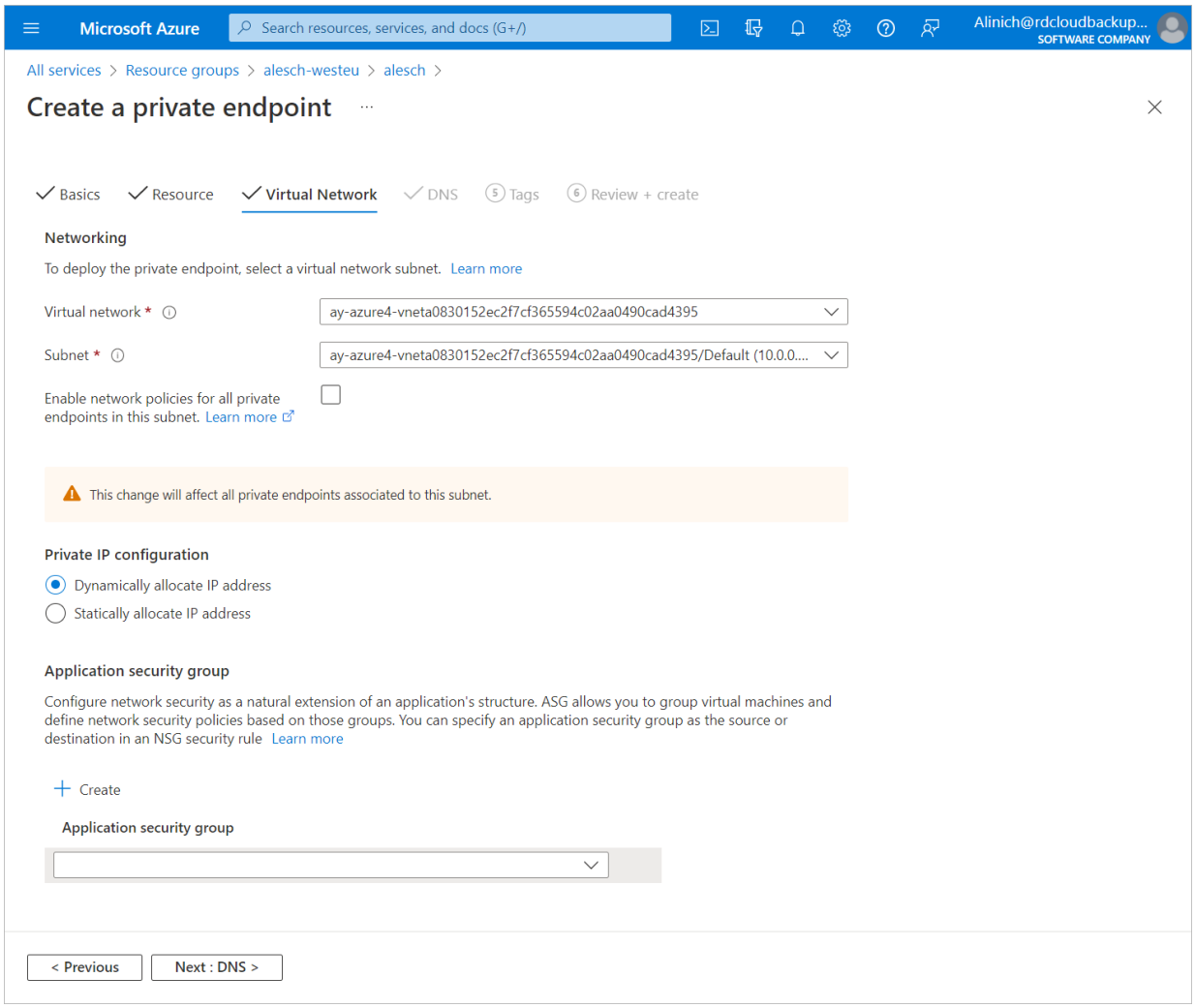
1. From the **Target sub-resource** drop-down list, select the type of the resource:
   - Select *blob* if you are creating a private endpoint to allow Veeam Backup for Microsoft Azure to manage backup repositories or back up Azure VMs.
   - Select *file* if you are creating a private endpoint to allow Veeam Backup for Microsoft Azure to back up Azure file shares.
2. Click **Next: Virtual Network >**.



## Step 4. Specify Virtual Network Settings

At the **Virtual Network** step of the **Create a private endpoint** wizard, do the following:

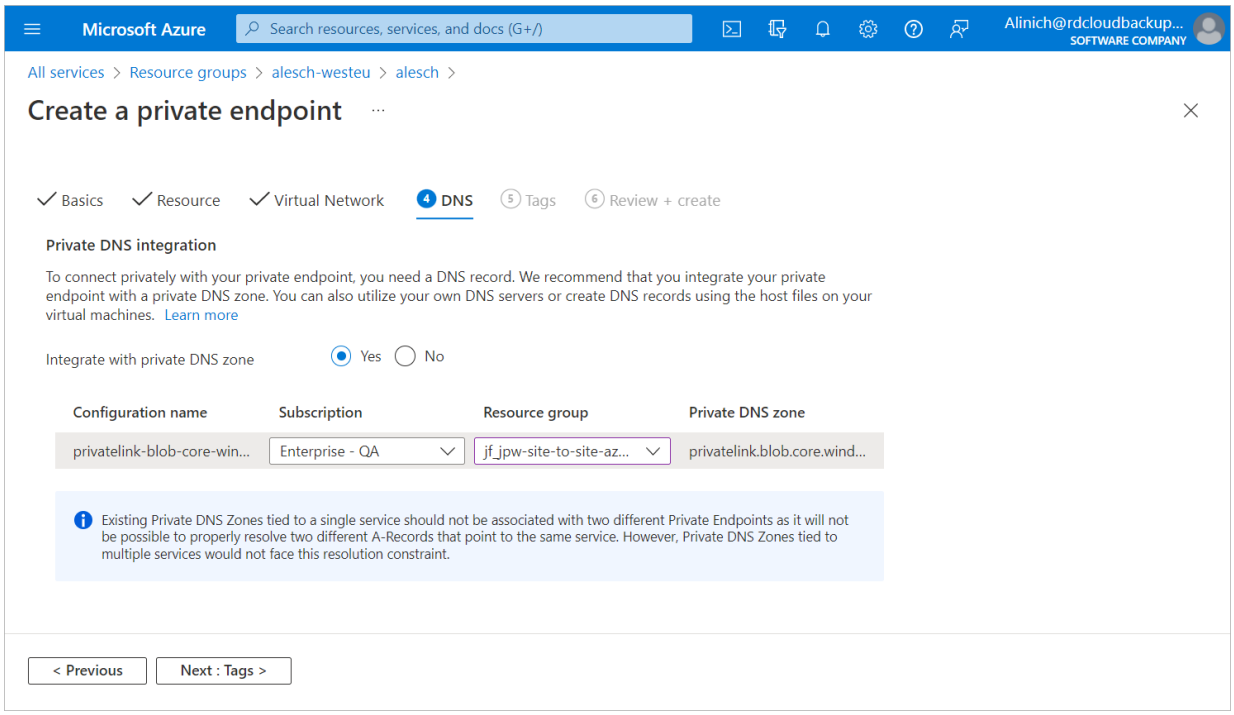
1. From the **Virtual network** drop-down list, select a virtual network to which the backup appliance or worker instances are connected.
2. From the **Subnet** drop-down list, select a subnet to which the backup appliance or worker instances are connected. For a subnet to be displayed in the list, it must be created within the selected virtual network as described in Microsoft Docs.
3. Click **Next: DNS >**.



## Step 5. Specify DNS Settings

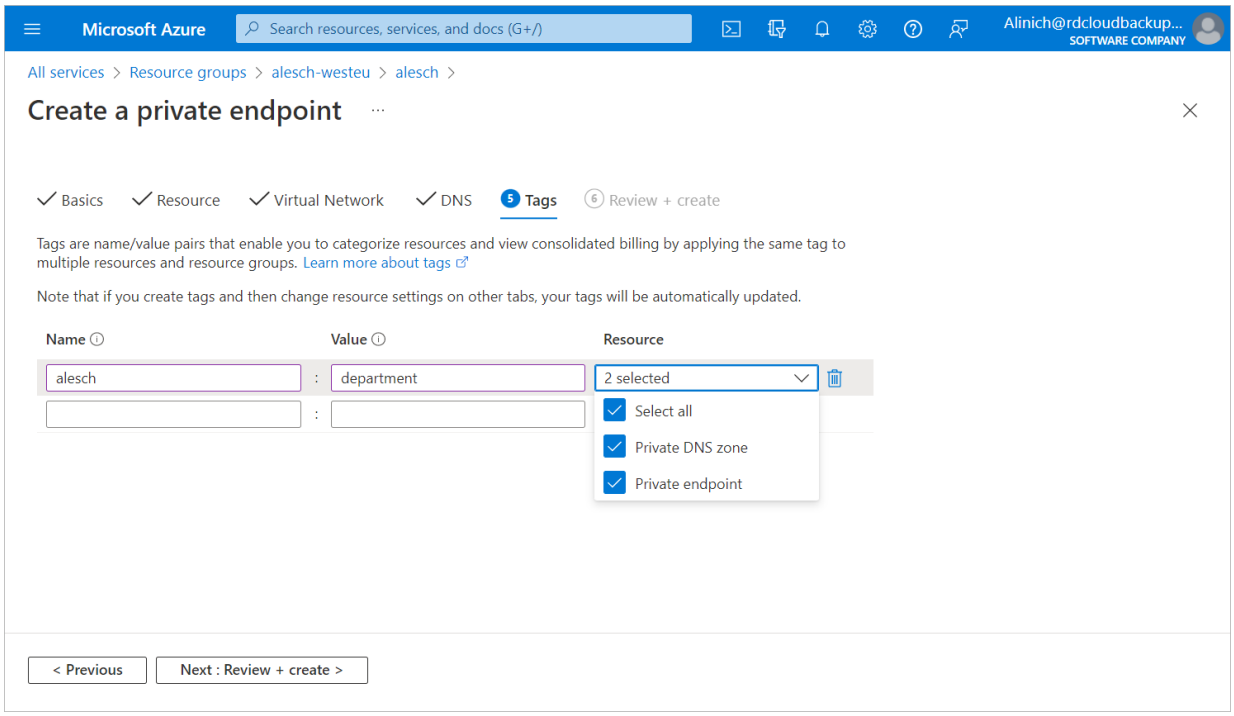
At the **DNS** step of the **Create a private endpoint** wizard, do the following:

1. In the **Private DNS integration** section, create a new DNS zone to override the DNS resolution from a public to private endpoint:
   a. To the right of the **Integrate with private DNS zone** field, click **Yes**.
   b. From the **Subscription** drop-down list, select a subscription to which the DNS zone will belong.
   c. From the **Resource group** drop-down list, select the resource group to which the DNS zone will belong.
2. Click **Next: Tags >**.



## Step 6. Assign Tags

At the **Targets** step of the **Create a private endpoint** wizard, you can assign tags to the newly created private endpoint and private DNS zone if needed.



### Step 7. Finish Working with Wizard

At the **Review + create** step of the **Create a private endpoint** wizard, review configured settings and click **Create**.

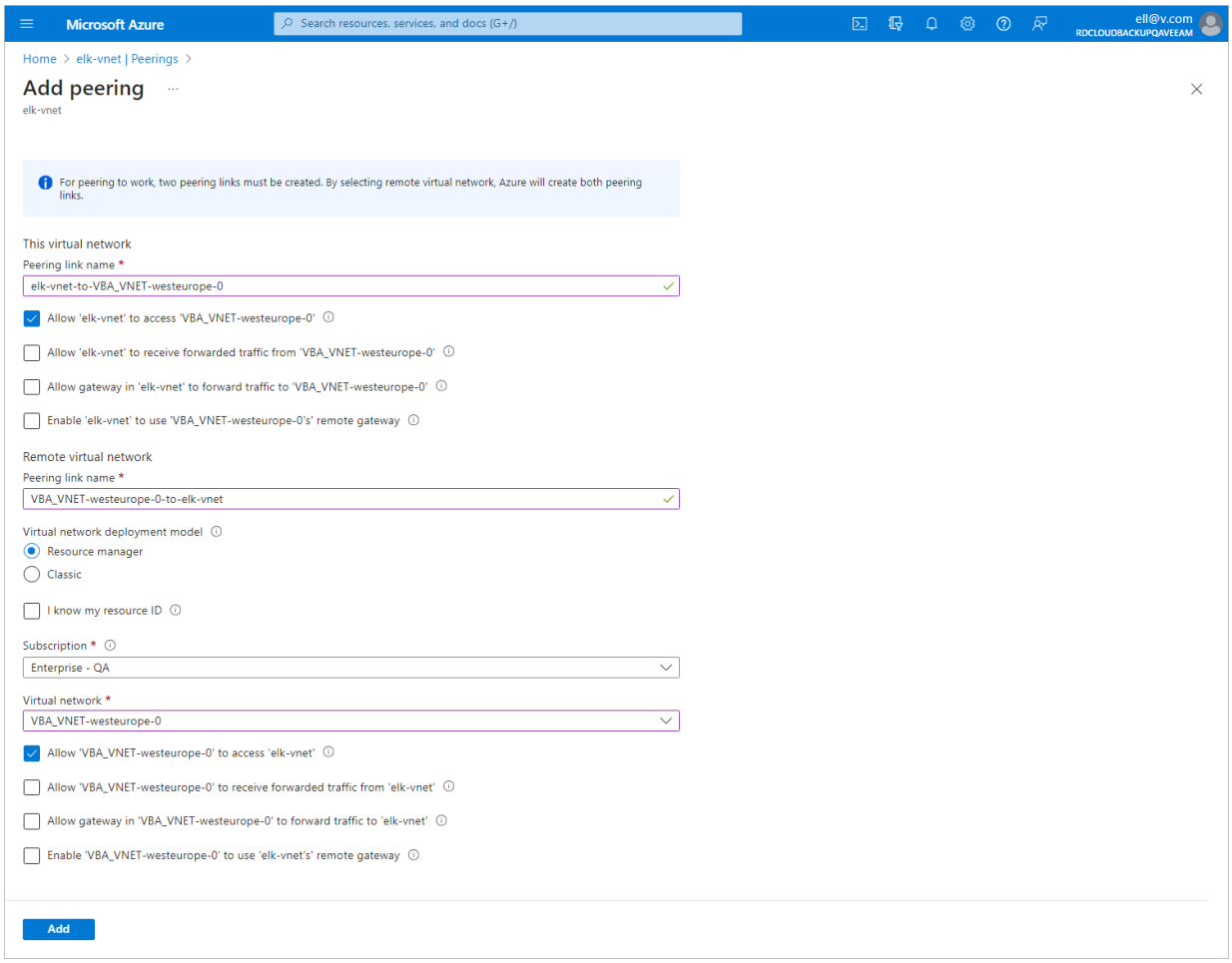
## Step 8. Configure Private Endpoint Network Settings

To allow Veeam Backup for Microsoft Azure components to communicate in private environment, you must configure peering connections between the VNet to which the backup appliance is connected and the VNet to which the newly created private endpoint is connected.

To create a peering, perform the following steps:

1. Log in to the Microsoft Azure portal.
2. Open the **Resource group** page.
3. In the **Resource** list, locate and click the VNet to which the backup appliance is connected. The **Virtual network** page will open.
4. Navigate to **Settings** > **Peerings**.
5. Click **Add** to open the **Add peering** page.
6. On the **Add peering** page, specify the following settings:
   a. In the **This virtual network** section, specify a name for the peering link that will be added to the VNet to which the backup appliance is connected. Leave the default settings for the other options in this section.
   b. In the **Remote virtual network** section, specify a name for the peering link that will be added to the target VNet. Leave the default settings for the other options in this section.
   c. From the **Subscription** drop-down list, select an Azure subscription to which worker instances belong.
   d. From the **Virtual networks** drop-down list, select the virtual network to which worker instances are connected.

e. Click **Add**.


Microsoft Azure
Search resources, services, and docs (G+/)
ell@v.com
RDCLOUDBACKUPQAVEEAM
Home > elk-vnet | Peerings >
Add peering
elk-vnet
For peering to work, two peering links must be created. By selecting remote virtual network, Azure will create both peering links.
This virtual network
Peering link name *
elk-vnet-to-VBA_VNET-westeurope-0
Allow 'elk-vnet' to access 'VBA_VNET-westeurope-0'
Allow 'elk-vnet' to receive forwarded traffic from 'VBA_VNET-westeurope-0'
Allow gateway in 'elk-vnet' to forward traffic to 'VBA_VNET-westeurope-0'
Enable 'elk-vnet' to use 'VBA_VNET-westeurope-0's' remote gateway
Remote virtual network
Peering link name *
VBA_VNET-westeurope-0-to-elk-vnet
Virtual network deployment model
Resource manager
Classic
I know my resource ID
Subscription *
Enterprise - QA
Virtual network *
VBA_VNET-westeurope-0
Allow 'VBA_VNET-westeurope-0' to access 'elk-vnet'
Allow 'VBA_VNET-westeurope-0' to receive forwarded traffic from 'elk-vnet'
Allow gateway in 'VBA_VNET-westeurope-0' to forward traffic to 'elk-vnet'
Enable 'VBA_VNET-westeurope-0' to use 'elk-vnet's' remote gateway
Add

# Configuring Global Retention Settings

You can configure global retention settings to specify for how long the following data will be retained in the configuration database:

- Obsolete snapshots and replicas
- Session records

## Configuring Retention Settings for Obsolete Snapshots

If an Azure resource (whether it is an Azure VM or an Azure file share) is no longer processed by a backup policy (for example, it was removed from the backup policy or the backup policy no longer exists), its cloud-native snapshots become obsolete. Retention policy settings configured when creating backup policies do not apply to obsolete snapshots — these snapshots are removed from the configuration database according to their own retention settings.

> **NOTE**
>
> Global retention settings apply to all cloud-native snapshots created by the Veeam backup service. If an Azure resource is still processed by a backup policy, but some of its cloud-native snapshots are older than the number of days (or months) specified in the global retention settings, these cloud-native snapshots will be removed from the configuration database.

To configure retention settings for obsolete snapshots, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **General** > **Retention**.
3. In the **Obsolete snapshots retention** section, select either of the following options:
   - Select the **Never** option if you do not want Veeam Backup for Microsoft Azure to remove obsolete snapshots.
   - Select the **After** option if you want to specify the number of days, months or years during which Veeam Backup for Microsoft Azure will keep obsolete snapshots in the configuration database. The number must be between 15 and 36135 for days, between 1 and 1188 for months and between 1 and 99 for years.

     If you select this option, Veeam Backup for Microsoft Azure will remove obsolete instance snapshots from the configuration database as soon as the specified period of time is over.
4. Click **Save**.

> **NOTE**
>
> When Veeam Backup for Microsoft Azure removes an obsolete snapshot from the configuration database, it also removes the snapshot from Microsoft Azure Storage.

# Configuring Retention Settings for Session Records

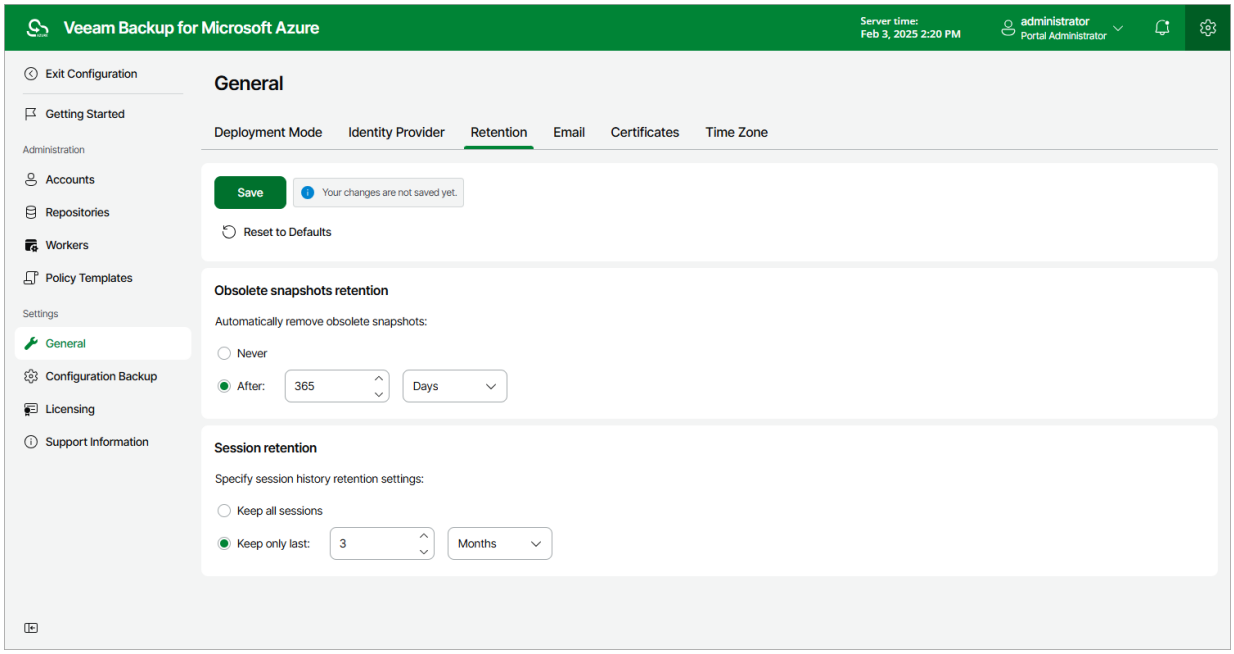
Veeam Backup for Microsoft Azure stores records for the login activity and all sessions of performed data protection and disaster recovery operations in the configuration database on the additional data disk attached to the backup appliance. The default retention period for the login activity records equals 3 months and cannot be modified. The session records are removed from the configuration database according to specific retention settings.

To configure retention settings for session records, do the following:

1. In the **Session retention** section, select either of the following options:
   - Select the **Keep all sessions** option if you do not want Veeam Backup for Microsoft Azure to remove session records.
   - Select the **Keep only last** option if you want to specify the number of days, months or years during which Veeam Backup for Microsoft Azure will keep session records in the configuration database.

     If you select this option, Veeam Backup for Microsoft Azure will remove all session records that are older than the specified time limit.
2. Click **Save**.

> **IMPORTANT**
>
> Retaining all session records in the configuration database may overload the data disk. By default, the disk comes with 32 GB of storage capacity. If you choose not to remove sessions records at all, consider increasing the disk space to avoid runtime problems.



# Replacing Security Certificates

To establish secure data communications between the backup appliance and web browsers running on user workstations, Veeam Backup for Microsoft Azure uses Transport Layer Security (TLS) certificates.

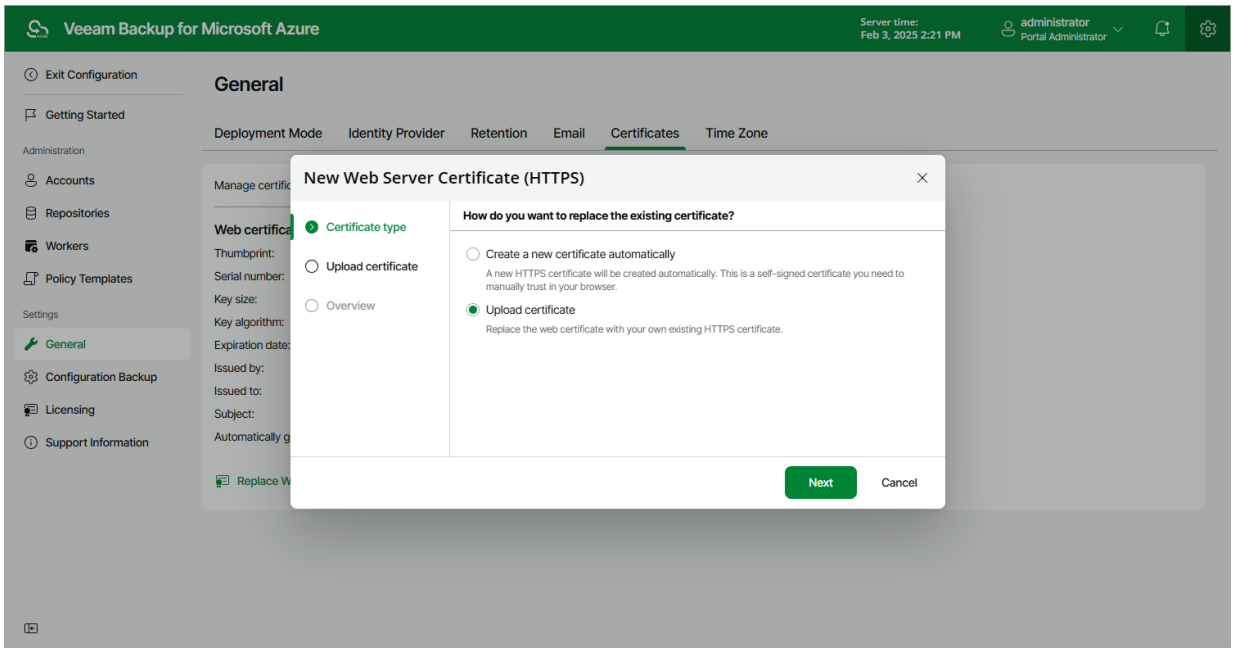
When you install Veeam Backup for Microsoft Azure, it automatically generates a default self-signed certificate. You can replace this default certificate with your own self-signed certificate or with a certificate obtained from a Certificate Authority (CA). To replace the currently used TLS certificate, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **General** > **Certificates**.
3. Click **Replace Web Certificate**.
4. Complete the **New Web Server Certificate (HTTPS)** wizard:
    a. At the **Certificate type** step of the wizard, do the following:
        - Select the **Create a new certificate automatically** option if you want to replace the existing certificate with a new self-signed certificate automatically generated by Veeam Backup for Microsoft Azure.
        - Select the **Upload certificate** option if you want to upload a certificate that you obtained from a CA or generated using a 3rd party tool.

    b. [Applies only if you have selected the **Upload certificate** option] At the **Upload certificate** step of the wizard, browse to the certificate that you want to install, and provide a password for the certificate file if required.

> **NOTE**
>
> Only .PFX and .P12 files are supported.

    c. At the **Summary** step of the wizard, review summary information and click **Finish**.



# Configuring Global Notification Settings

You can specify email notification settings for automated delivery of backup policy results and daily reports. Every daily report contains cumulative statistics for all backup policy and snapshot retention sessions run within the past 24-hour period.

To connect an email server that will be used for sending email notifications, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **General** > **Email**.
3. Select the **Enable email notifications** check box.
4. Click the link in the **Email server** field and configure email server settings.
5. In the **From** field, enter an email address of the notification sender. This email address will be displayed in the **From** field of notifications.
6. In the **To** field, enter an email address of a recipient. Use a semicolon to separate multiple recipient addresses.

   For each particular policy, you can configure specific notification settings. For more information on backup policies, see Performing Backup.

> **NOTE**
>
> If you specify the same email recipient in both backup policy notification and global notification settings, Veeam Backup for Microsoft Azure will override the configured global notification settings and will send each notification to this recipient only once to avoid notification duplicates.

7. In the **Subject** field, specify a subject for notifications. You can use the following runtime variables:
   - *%JobName%* — a backup policy name.
   - *%JobResult%* — a backup policy result.
   - *%ObjectCount%* — the number of Azure resources in a backup policy.
   - *%Issues%* — the number of Azure resources in a backup policy that encountered any issues (errors and warnings) while being processed.

   The default subject for email notifications is: *[%JobResult%] %JobName% (%ObjectCount% instances) %Issues%*.
8. In the **Notify me immediately about** section, choose whether you want to receive email notifications in case backup policies complete successfully, complete with warnings or complete with errors.
9. To receive daily reports, select the **Send daily report at** check box and specify the exact time when the reports will be sent.
10. Click **Save**.

> **TIP**
>
> Veeam Backup for Microsoft Azure allows you to send a test message to check whether you have configured all settings correctly. To do that, click **Send Test Email**. A test message will be sent to the specified email address.

# Configuring Email Server Settings

To configure email server settings, choose whether you want to employ Basic (SMTP) or Modern (OAuth 2.0) authentication for your email server.

## Using Basic Authentication

To employ the Basic authentication to connect to your email server, in the **Email Server Settings** window:

1. From the **Authentication** drop-down list, select *Basic*.
2. In the **Mail server name or address** field, enter a DNS name or an IP address of the SMTP server. All email notifications (including test messages) will be sent by this SMTP server.
3. In the **Port** field, specify a communication port for SMTP traffic. The default SMTP port is 25.
4. In the **Timeout** field, specify a connection timeout for responses from the SMTP server.
5. For an SMTP server with SSL/TLS support, select the **Connect using SSL** check box to enable SSL data encryption.
6. If your SMTP server requires authentication, select the **This server requires authentication** check box and choose an account that will be used when authenticating against the SMTP server from the **Connect as** drop-down list. Make sure the account you choose has the permissions to send emails as the notification sender specified in the **From** field.

   For an account to be displayed in the list of available accounts, it must be added to Veeam Backup for Microsoft Azure as described in section Adding SMTP and Database Accounts. If you have not added an account beforehand, click **Add** and complete the **Add Account** wizard.
7. Click **Save**.

## Using Modern Authentication

To employ the Modern authentication to connect to your mail service:

1. In **Email Server Settings** window, copy the URL from the **Redirect URL** field.
2. For Veeam Backup for Microsoft Azure to be able to use OAuth 2.0 to access Google Cloud or Microsoft Azure APIs, register a new client application either in the Google Cloud Console or in the Microsoft Azure portal.

   When registering the application, make sure that the redirect URI specified for the application matches the URL copied from the Veeam Backup for Microsoft Azure Web UI.

**IMPORTANT**

- If you plan to use a client application registered in the Microsoft Azure portal, you must grant it the *Mail.Send* Microsoft Graph application permission and the following Microsoft Graph delegated permissions: *email*, *offline_access*, *openid*, *User.Read*. For more information on Microsoft Graph permissions, see Microsoft Docs.
- If you plan to use a client application registered in a Google Cloud project with a Testing publishing status, keep in mind that authorization will be required every seven days from the time of consent.

3. Back to the Veeam Backup for Microsoft Azure Web UI, do the following in the **Email Server Settings** window:

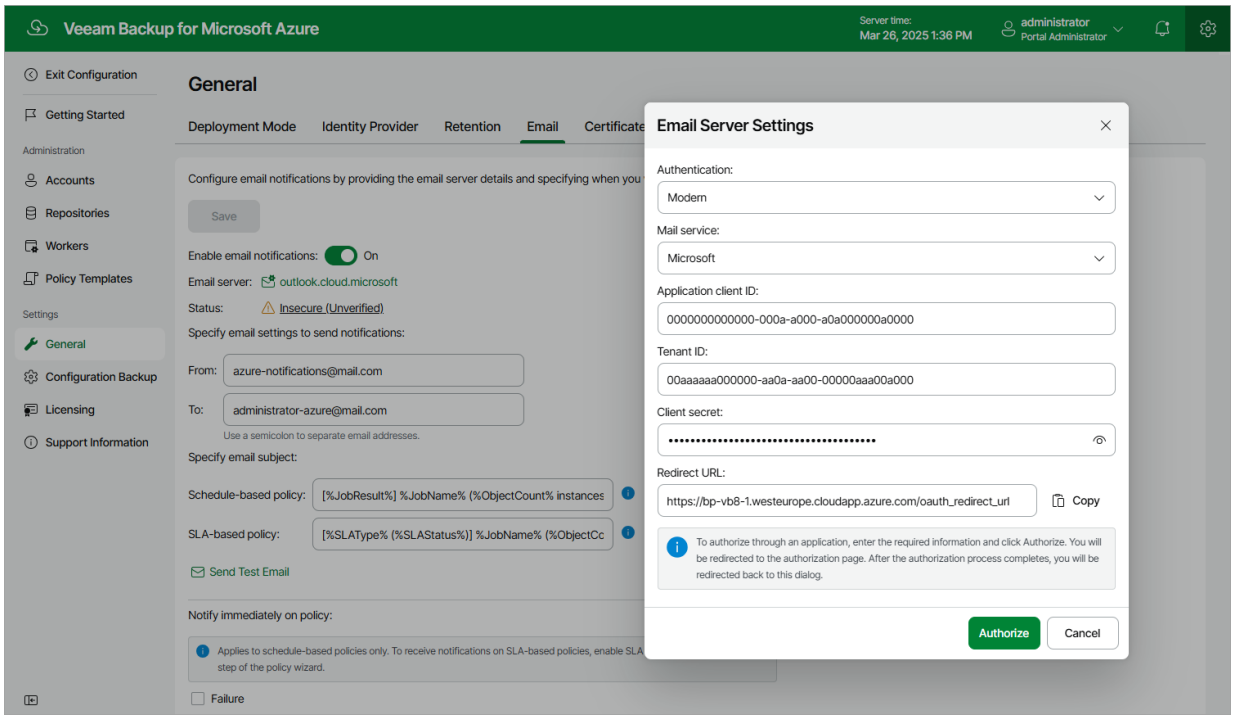
   a. From the **Authentication** drop-down list, select *Modern*.

b. Use the **Mail service** drop-down list to choose whether you want to use a *Google* or *Microsoft* mail service to send email notifications.

c. In the **Application client ID** and **Client secret** fields, provide the Client ID and Client secret created for the application as described in Google Cloud documentation or Microsoft Docs. Make sure the client whose data you provide has the permissions to send emails as the notification sender specified in the **From** field.

d. [Applies only if you have selected the **Microsoft** option] In the **Tenant ID** field, provide the ID of an Microsoft Entra tenant in which the application has been registered.

e. Click **Authorize**. You will be redirected to the authorization page. Sign in using a Google or Microsoft Azure account to validate the configured settings.



# Changing Time Zone

Veeam Backup for Microsoft Azure runs daily reports and performs all data protection and disaster recovery operations according to the time zone set on the backup appliance.

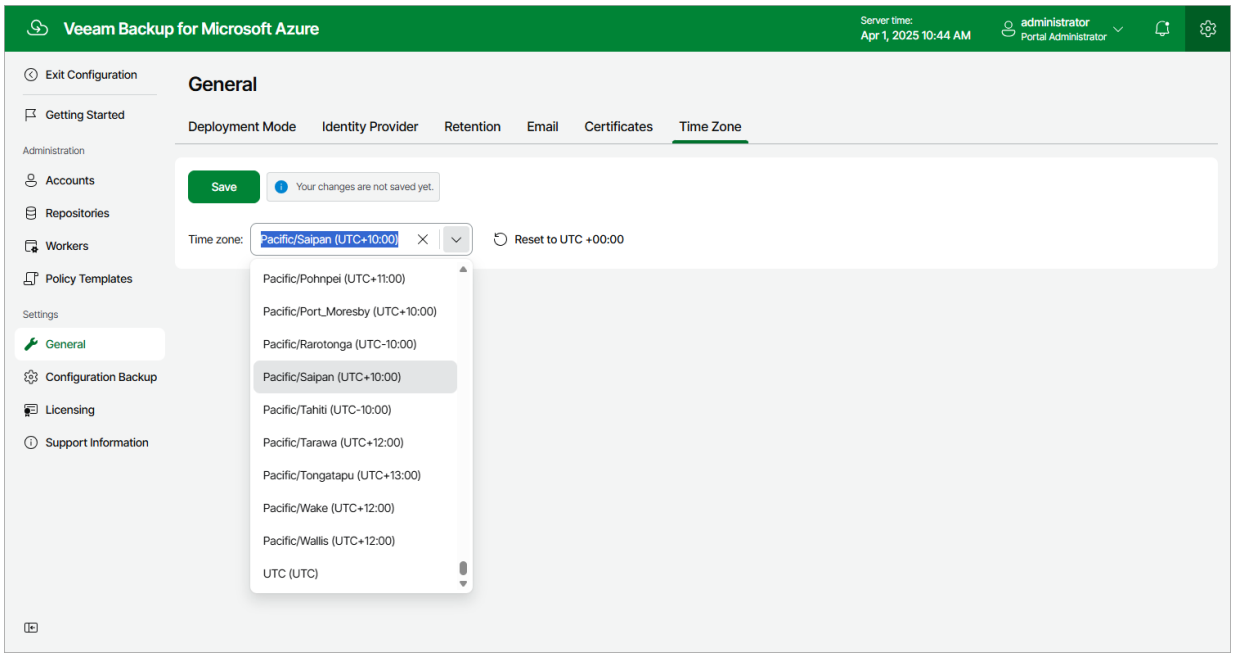
> **IMPORTANT**
>
> If Daylight Saving Time (DST) is used in the time zone set on the backup appliance, consider the following:
>
> - When DST starts (clocks are set one hour forward), all policy sessions scheduled to launch at the skipped hour on this day do not run. You can run the policies manually as described in section Starting and Stopping Backup Policies.
> - When DST ends (clocks are set one hour back), all policy sessions scheduled to launch at the duplicated hour on this day run only once.

Since the backup appliance is deployed on an Azure VM in Microsoft Azure, the time zone is set to Coordinated Universal Time (UTC) by default. However, you can change the time zone if required. For example, you may want the time on the backup appliance to match the time on the workstation from which you access Veeam Backup for Microsoft Azure.

To change the time zone set on the backup appliance:

1. Switch to the **Configuration** page.
2. Navigate to **General** > **Time Zone**.
3. Select the necessary time zone from the **Time zone** drop-down list.
4. Click **Save**.

> **NOTE**
>
> It is not recommended that you change the time zone if any backup policy is currently running. Wait for all the running policies to complete or stop them manually — and then try changing the time zone again.



# Configuring SSO Settings

Veeam Backup for Microsoft Azure supports single sign-on (SSO) authentication based on the SAML 2.0 protocol. SSO authentication scheme allows a user to log in to different software systems with the same credentials using the identity provider service. For Veeam Backup for Microsoft Azure to be able to authenticate users whose identity has been received from an identity provider, you must perform a number of configuration actions both in the Veeam Backup for Microsoft Azure Web UI and on the identity provider side.

> **TIP**
>
> The configuration actions you perform vary on the identity provider you use. This guide covers actions performed for Microsoft Entra ID only. If you need to obtain instructions for another identity provider, open a support case.

## Configuring SSO Settings for Microsoft Entra ID

For Veeam Backup for Microsoft Azure to be able to use Microsoft Entra ID as an identity provider, you must perform the following steps to configure SSO settings:

1. Obtain the service provider authentication settings on the Veeam Backup for Microsoft Azure side.
2. Configure the SAML single sign-on method for your Microsoft Entra application.
3. Forward the service provider authentication settings to your Microsoft Entra application.
4. Create a custom claim for your Microsoft Entra application.
5. Obtain a file with the identity provider settings.
6. Import the identity provider settings into the Veeam Backup for Microsoft Azure configuration database.
7. [Optional] Add SSO users that will be able to access Veeam Backup for Microsoft Azure.

## Step 1. Obtain Service Provider Settings

To obtain the service provider authentication settings, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **General** > **Identity Provider**.
3. In the **Identity provider configuration** section, click **Download** in the **Application configuration** section. Veeam Backup for Microsoft Azure will download a metadata file with the service provider authentication settings to your local machine.

   Alternatively, you can copy the service provider settings manually:

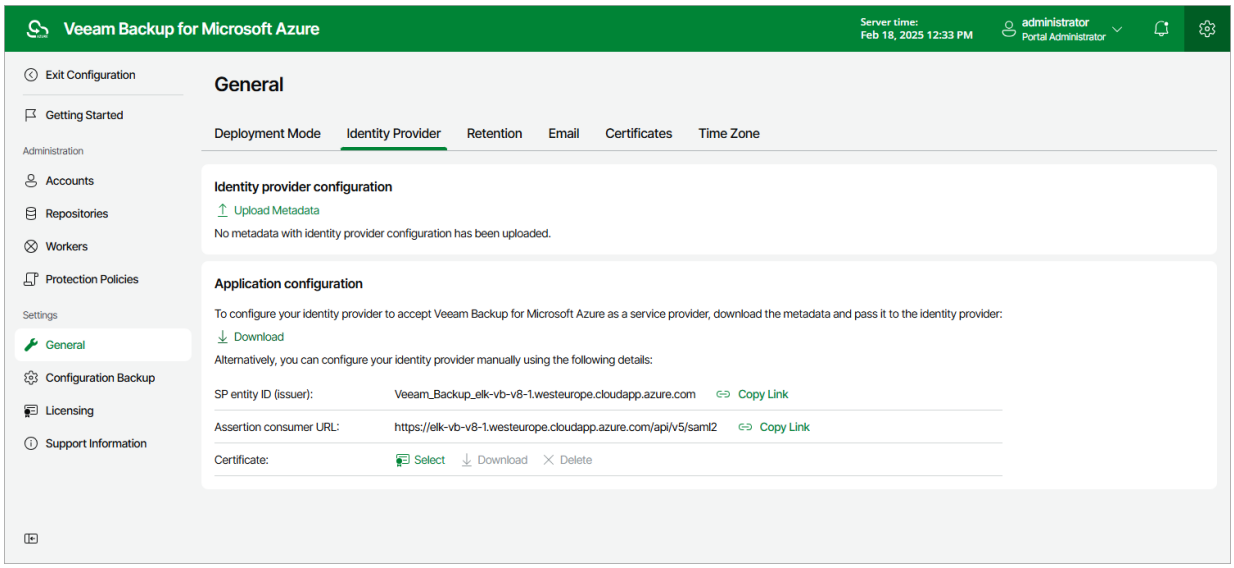
   a. Click **Copy Link** in the **SP entity ID (issuer)** field.

   b. Click **Copy Link** in the **Assertion consumer URL** field.

**TIP**

If you want to sign and encrypt authentication requests sent from Veeam Backup for Microsoft Azure to the identity provider, select a certificate with a private key that will be used to sign and encrypt the requests:

1. In the **Application configuration** section, click **Select** in the **Certificate** field.
2. In the **Upload Security Certificate** window, click **Browse** to locate the certificate file. In the **Password** field, specify a password used to open the file.
3. Click **Upload**.

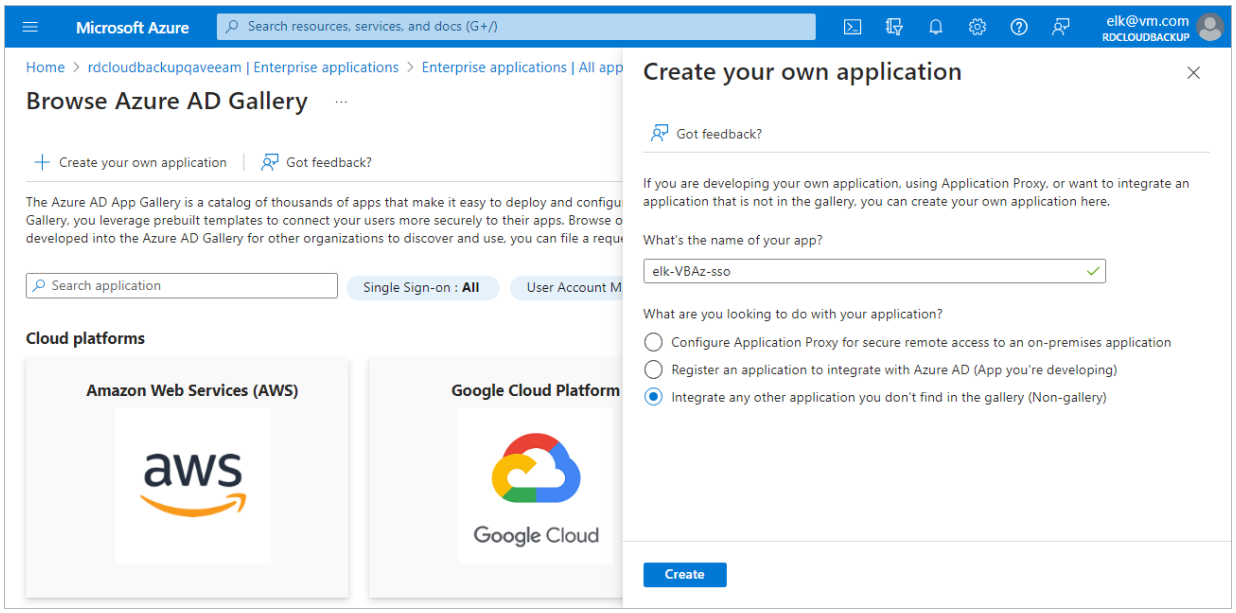



# Step 2. Set up SSO with SAML for Microsoft Entra application

To set up single sign-on with SAML in your Microsoft Entra ID, do the following:

1. Log in to the Microsoft Azure portal.
2. Select the Microsoft Entra ID to which the backup appliance belongs.
3. Navigate to **Enterprise applications** and click **New application** > **Create your own application**.
4. In the **Create your own application** window, specify a name for your Microsoft Entra application and select the **Integrate any other application you don't find in the gallery (Non-gallery)** option.

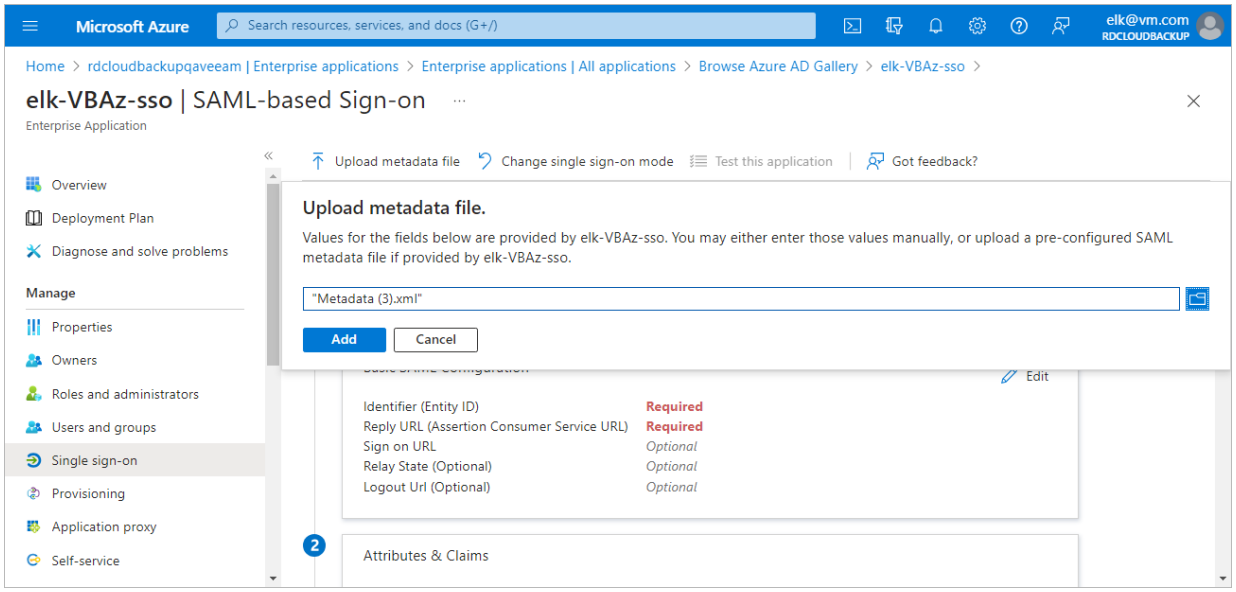
5. In the newly created application, navigate to **Single sign-on** and click **SAML**.




# Step 3. Forward Service Provider Settings to Microsoft Entra ID

To forward the service provider authentication settings to your Microsoft Entra ID, do the following:

1. In the **Single sign-on** window of your Microsoft Entra application, click **Upload metadata file**.
2. In the **Upload metadata file** window, click the folder icon to locate the file with the service provider settings downloaded at step 1.
3. Click **Add**.
4. In the **Basic SAML Configuration** window, click **Save**.

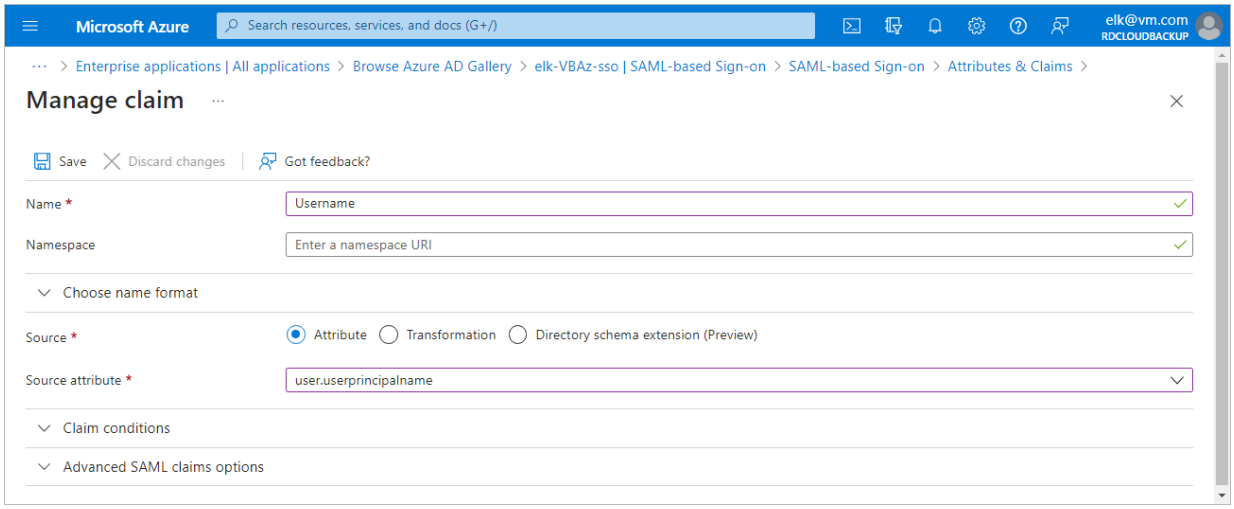


# Step 4. Create Claim for Microsoft Entra application

To authenticate a user whose identity is received from the identity provider, Veeam Backup for Microsoft Azure redirects the user to the identity provider portal. After the user logs in to the portal, the identity provider sends a SAML authentication response to Veeam Backup for Microsoft Azure. The SAML response must contain an attribute whose value will be used by Veeam Backup for Microsoft Azure to identify the user. The attribute value must match the user name that you specify when creating the user account.

For the identity provider to send the required attribute in the SAML authentication response, you must create a claim on the identity provider side and specify username as the outgoing claim name:

1. In the **Single sign-on** window of your Microsoft Entra application, locate the **Attributes & Claims** section and click **Edit**.
2. Click **Add new claim**.
3. In the **Manage claim** window, specify the following settings:
   a. In the **Name** field, enter *Username*.
   b. In the **Choose name format** section, select the **Attribute** option. In the **Source attribute** field, enter *user.userprincipalname*.
   c. Click **Save**.

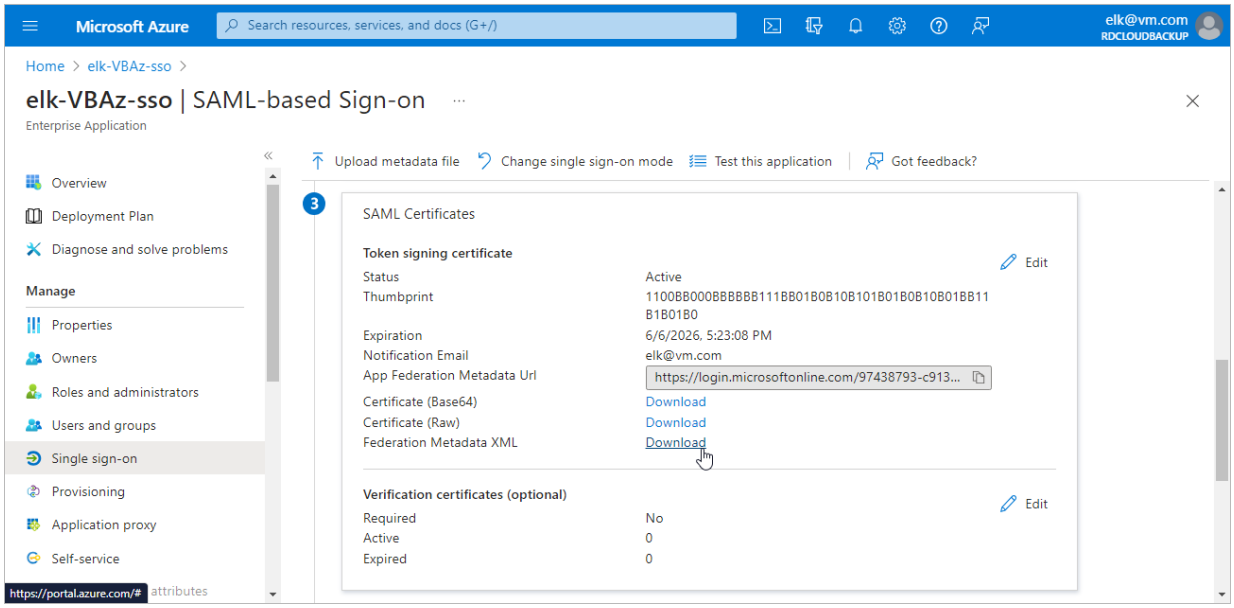



# Step 5. Obtain Microsoft Entra ID Metadata

To obtain the Microsoft Entra ID identity provider settings, do the following:

1. In the **Single sign-on** window of your Microsoft Entra application, locate the **Federation Metadata XML** field in the **SAML Certificates** section.

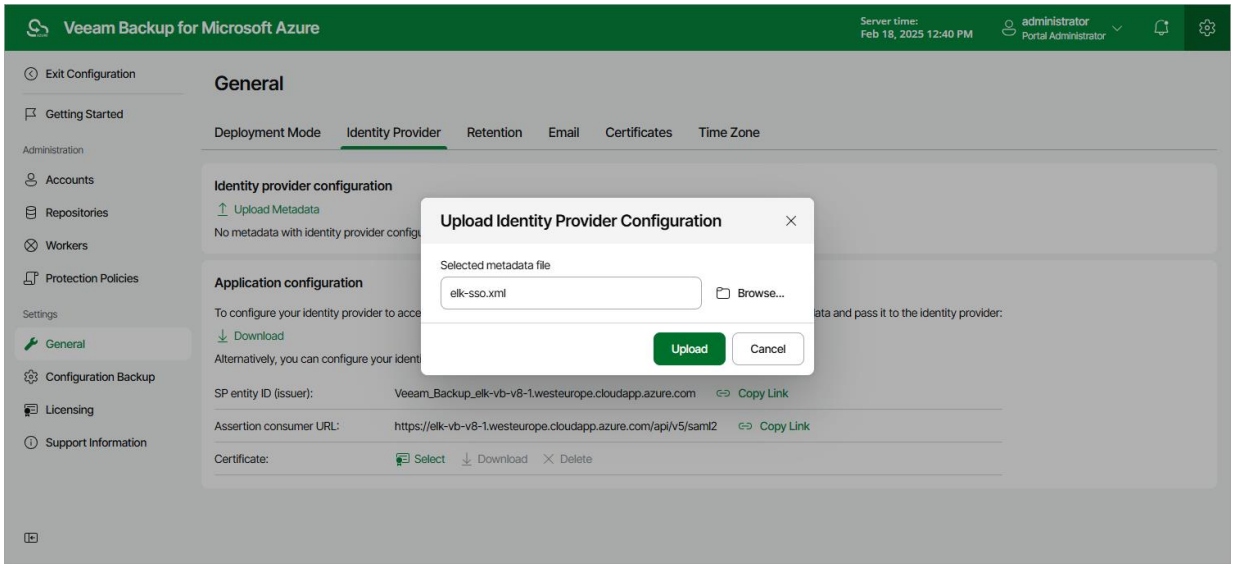
2. Click **Download**.




# Step 6. Import Microsoft Entra ID Metadata

To import the obtained Microsoft Entra ID identity provider settings, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **General** > **Identity Provider**.
3. In the **Identity provider configuration** section:
   a. Click **Upload Metadata**.
   b. In the **Upload Identity Provider Configuration** window, click **Browse** to locate the file with the identity provider settings.
   c. Click **Upload**.



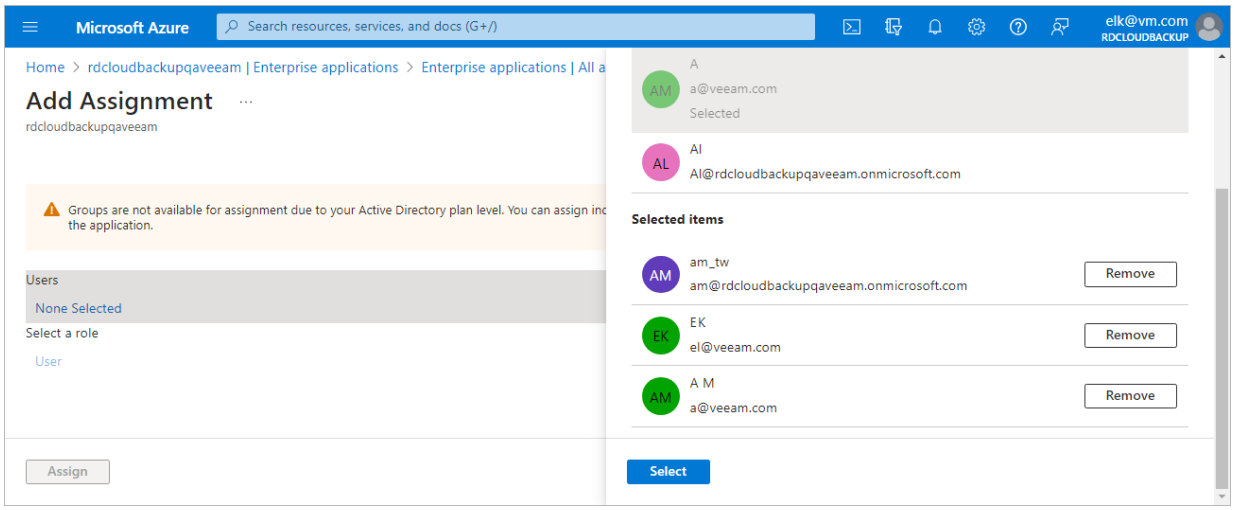
# [Optional] Step 7. Add SSO Users

To add users that will be able to access Veeam Backup for Microsoft Azure using single sign-on, do the following:

1. In the **Single sign-on** window of your Microsoft Entra application, navigate to **Users and groups**.
2. Click **Add user/group**.
3. In the **Add assignment** window, click **None selected** and select users in the **Users** list.

**IMPORTANT**

- Make sure that emails of the selected users match user names of their user accounts added to Veeam Backup for Microsoft Azure.
- You can only select users to access Veeam Backup for Microsoft Azure using single sign-on — groups are not supported.



# Performing Configuration Backup and Restore

You can back up and restore the configuration database that stores data collected from a backup appliance configuration for the existing backup policies, protected Azure VMs, Azure SQL databases, Cosmos DB accounts, Azure file shares, virtual network configurations, worker instance configurations, logged session records and so on. If the backup appliance goes down for some reason, you can reinstall it and quickly restore its configuration from a configuration backup. You can also use a configuration backup to migrate the configuration of one backup appliance to another appliance in Microsoft Azure.

It is recommended that you regularly perform configuration backup for every backup appliance added to the backup infrastructure. Periodic configuration backups reduce the risk of data loss and minimize the administrative overhead costs in case any problems with the backup appliance occur.

You can run configuration backup manually on demand, or instruct Veeam Backup for Microsoft Azure to do it automatically on a regular basis.

# Performing Configuration Backup

During the configuration backup, Veeam Backup & Replication exports data from the configuration database of an appliance and saves it to a backup file in a repository. The configuration database contains the following information: the existing backup policies, protected Azure VMs, Azure SQL databases, Cosmos DB accounts, Azure file shares, virtual network configurations, worker instance configurations, logged session records and so on.

## Performing Configuration Backup Using Console

When Veeam Backup & Replication performs configuration backup, it backs up the configuration of the backup server and also configurations of all backup appliances added to the backup infrastructure. The results of every configuration backup session are displayed in the **History** view under the **System** node.

You can perform configuration backup manually or instruct Veeam Backup & Replication to do it automatically on a regular basis:

- To perform configuration backup manually, follow the instructions provided in the Veeam Backup & Replication User Guide, section Running Configuration Backups Manually.
- To instruct Veeam Backup & Replication to perform configuration backup automatically, follow the instructions provided in the Veeam Backup & Replication User Guide, section Scheduling Configuration Backups.

> **IMPORTANT**
>
> For Veeam Backup & Replication to be able to back up configurations of managed backup appliances, you must enable backup file encryption in the configuration backup settings.

## Before You Begin

If you plan to back up the configuration of a managed backup appliance, keep in mind the following limitations and considerations:

- You must enable backup file encryption in the configuration backup settings. Otherwise, Veeam Backup & Replication will back up only the backup server configuration.

  To learn how to create encrypted configuration backups, see the Veeam Backup & Replication User Guide, section Creating Encrypted Configuration Backups.

- You cannot store configuration backups in scale-out backup repositories and external repositories.
- For Veeam Backup & Replication to be able to back up the appliance configuration, the backup appliance must be available and must run a Veeam Backup for Microsoft Azure version that is compatible with the Veeam Backup & Replication version.

  For the list of compatible versions, see System Requirements.

- During configuration backup, Veeam Backup & Replication can process only 3 appliances at once — the appliances exceeding this limit are queued.
- To enable data loss protection in case you lose or forget the password used for data encryption, you can use Veeam Backup Enterprise Manager to decrypt backup files.

  To learn how to let Veeam Backup & Replication encrypt and decrypt data with Enterprise Manager, see the Veeam Backup Enterprise Manager Guide, section Managing Encryption Keys.

# Configuration Backup Location

Veeam Backup & Replication stores configuration backups of backup appliances in a repository specified in the configuration backup settings. Backups are saved to the `\\VeeamConfigBackup\Azure` folder.

> **NOTE**
>
> Consider the following:
>
> - It is not recommended to store configuration backups on the backup server. Otherwise, you will not be able to restore the configurations of managed backup appliances in case the backup server goes down.
> - If the name of an appliance contains unsupported characters, these characters are replaced with the '_' underscore symbol in the name format for a subfolder and a backup files.

# Performing Configuration Backup Using Web UI

While performing configuration backup, Veeam Backup for Microsoft Azure exports data from the configuration database and saves it to a backup file in a backup repository. You can back up the configuration database of a backup appliance either manually or automatically.

> **IMPORTANT**
>
> If your backup appliance is managed by a Veeam Backup & Replication server, you will neither be able to perform manual or scheduled configuration backup of Veeam Backup for Microsoft Azure using the Web UI, nor to export the configuration data from the Web UI. In this case, you can perform configuration backup using the Veeam Backup & Replication console as described in section Performing Configuration Backup Using Console.

## Performing Snapshot-Based Configuration Backup

[Starting from version 6.0, this functionality has been deprecated and is available only for upgraded appliances that previously had the feature enabled]

You can instruct Veeam Backup for Microsoft Azure to automatically create snapshots of the backup appliance. You can then use these snapshots to restore the entire backup appliance to another Azure VM.

To configure the auto-backup settings, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **Configuration Backup**.
3. Switch to the **Snapshot-Based** tab.
4. Set the **Enable snapshot backup** toggle to *On*.
5. In the **Configure the snapshot settings and schedule** section, do the following:
   a. In the **Restore points to keep** field, specify the number of snapshots that you want to keep in the snapshot chain.

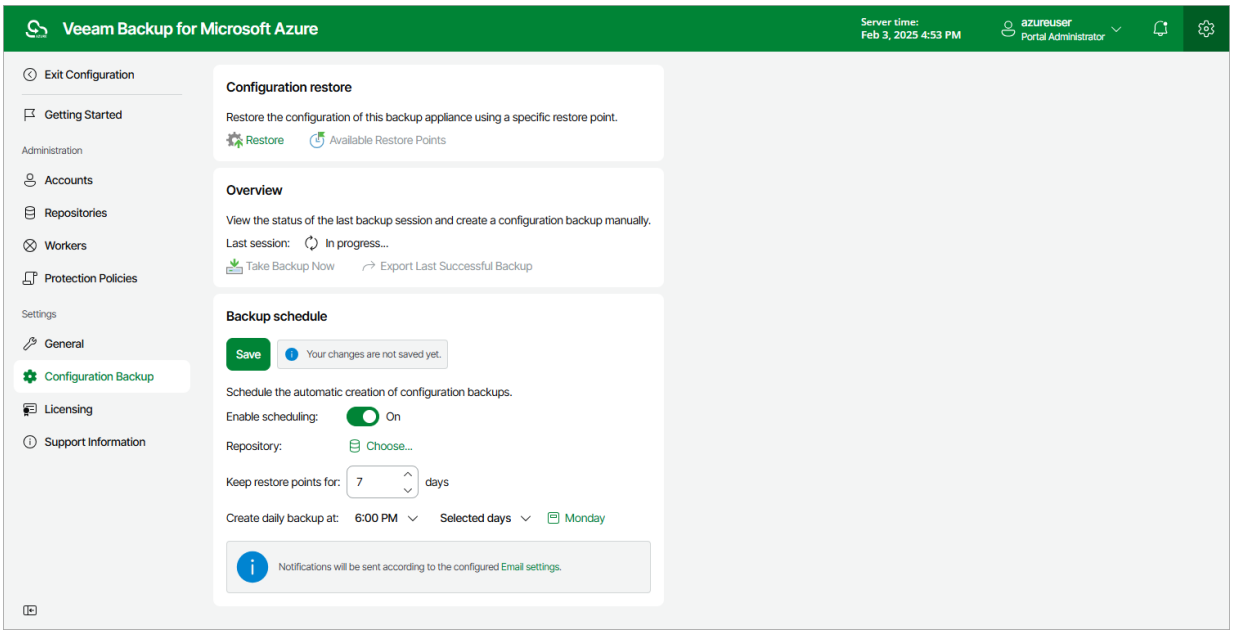
      If the snapshot limit is exceeded, Veeam Backup for Microsoft Azure removes the earliest snapshot from the chain. For more information, see sections VM Snapshot Retention and File Share Snapshot Retention.

b. In the **Schedule** section, choose whether you want to create snapshots daily, monthly or periodically:

- Select the **Daily at this time** option if you want Veeam Backup for Microsoft Azure to create snapshots once a day on defined days. You can choose whether snapshots will be created every day, on weekdays (Monday through Friday) or on specific days.
- Select the **Monthly at this time** option if you want Veeam Backup for Microsoft Azure to create snapshots once a month on a defined day.
- Select the **Periodically every** option if you want Veeam Backup for Microsoft Azure to create snapshots repeatedly throughout a day with a specific time interval. You can choose whether snapshots must be created every several hours or minutes. You can also instruct Veeam Backup for Microsoft Azure to create snapshots continuously, one after another.

> **TIP**
>
> If you choose to create snapshots once every several hours, you can also delay the snapshot creation by a defined amount of time within the specified interval. To do that, click **Schedule** and set the delay value (in minutes) in the **Start time within an hour** field.

6. Click **Save**.




# Performing Manual Configuration Backup

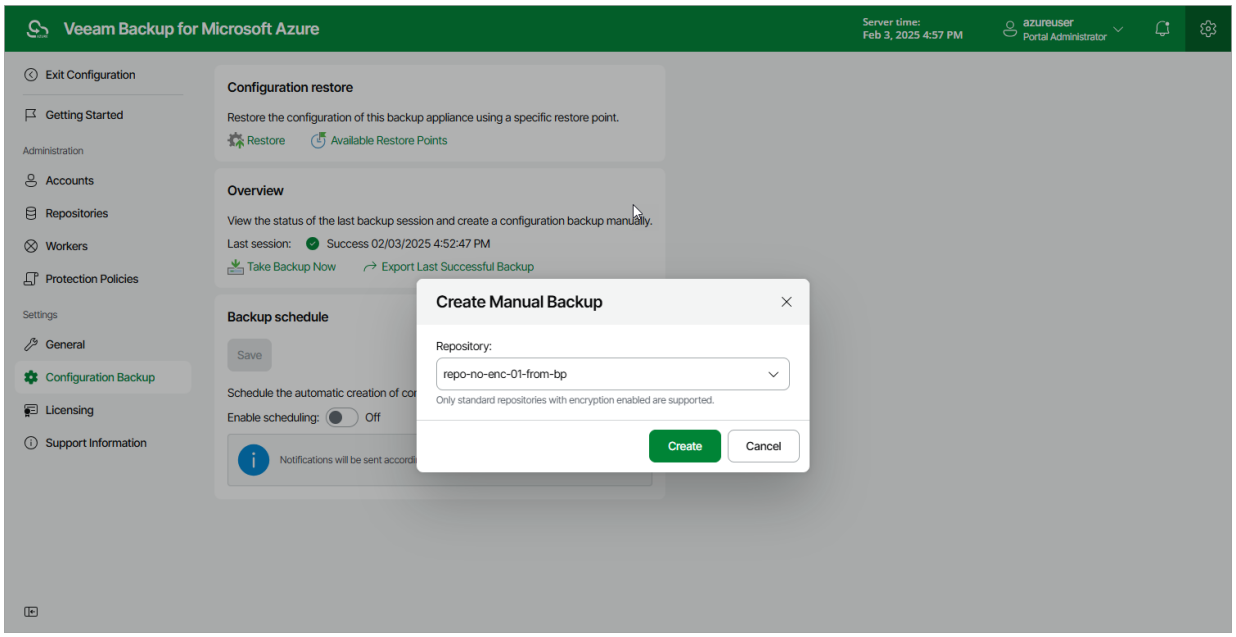
While performing configuration backup, Veeam Backup for Microsoft Azure exports data from the configuration database and saves it to a backup file in a backup repository. To back up the configuration database of the backup appliance manually, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **Configuration Backup**.
3. In the **Overview** section, click **Take Backup Now**.

4. In the **Create Manual Backup** window, select a repository where the configuration backup will be stored, and click **Create**.

   For a backup repository to be displayed in the **Repository** list, it must be added to Veeam Backup for Microsoft Azure as described in section Managing Backup Repositories. The **Repository** list shows only backup repositories that have encryption enabled and immutability disabled.

As soon as you click **Create**, Veeam Backup for Microsoft Azure will start creating a new backup in the selected repository. To track the progress, click **Go to Sessions** in the **Session Info** window to proceed to the Session Log page.




## Performing Scheduled Configuration Backup

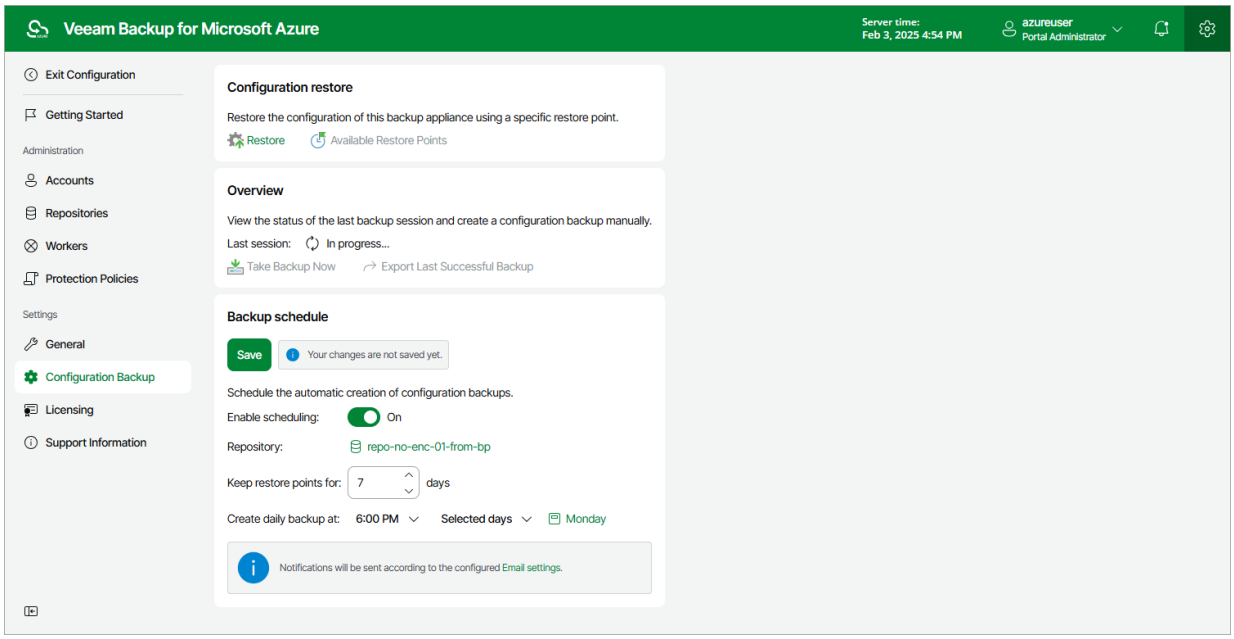
While performing configuration backup, Veeam Backup for Microsoft Azure exports data from the configuration database and saves it to a backup file in a backup repository. To instruct Veeam Backup for Microsoft Azure to back up the configuration database of the backup appliance automatically by schedule, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **Configuration Backup**.
3. In the **Backup schedule** section, set the **Enable scheduling** toggle to *On*.
4. Click **Choose** in the **Repository** field, and use the list of available repositories in the **Choose Repository** window to select a repository where configuration backups will be stored.

   For a backup repository to be displayed in the list of available repositories, it must be added to Veeam Backup for Microsoft Azure as described in section Adding Backup Repositories. The list shows only backup repositories that have encryption enabled and immutability disabled.
5. In the **Keep restore points for** field, specify the number of days for which you want to keep restore points in a backup chain in the selected backup repository.

   If a restore point is older than the specified time limit, Veeam Backup for Microsoft Azure removes the restore point from the chain. For more information, see VM Backup Retention, SQL Backup Retention and Cosmos DB Backup Retention .
6. In the **Create daily backup at** field, choose whether configuration backups will be created every day, on weekdays (Monday through Friday), or on specific days.

7. Click **Save**.



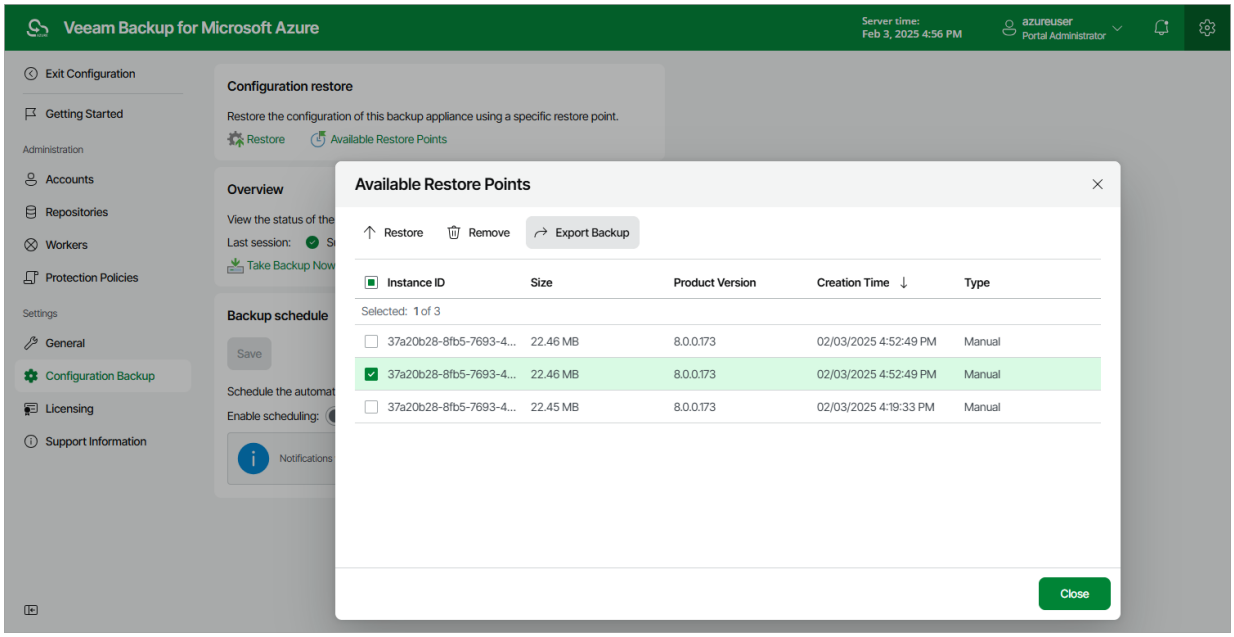

# Exporting Configuration Backup Data

Once Veeam Backup for Microsoft Azure creates a successful configuration backup, you can export the configuration backup file and use it to restore configuration data on another backup appliance.

To export the configuration backup file, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **Configuration Backup**.
3. Use either of the following options:
   - To export the last successful configuration backup:
     i. In the **Overview** section, click **Export Last Backup**.
     ii. In the **Export Last Backup** window, specify a password that will be used to encrypt the exported file, provide a hint for the specified password, and click **Export**.
   - To export a specific configuration backup file:
     i. In the **Configuration restore** section, click **Available Restore Points**.
     ii. In the **Available Restore Points** window, select the necessary backup and click **Export Backup**.
     iii. In the **Export Backup** window, specify a password that will be used to encrypt the exported file, provide a hint for the specified password, and click **Export**.

As soon as you click **Export**, Veeam Backup for Microsoft Azure will save the exported backup file to the default download directory on the local machine.



# Performing Configuration Restore

Veeam Backup for Microsoft Azure offers restore of the configuration database that can be helpful in the following situations:

- The configuration database got corrupted, and you want to recover data from a configuration backup.
- You want to roll back the configuration database to a specific point in time.
- The backup appliance got corrupted, and you want to recover its configuration from a configuration backup.
- The backup appliance went down, and you want to apply its configuration to a new backup appliance.

> **NOTE**
>
> Configuration restore to Veeam Backup for Microsoft Azure version 8 is supported from Veeam Backup for Microsoft Azure version 3.0 or later.

## Restoring Configuration Data Using Console

To restore the configuration database of a backup appliance using the Veeam Backup & Replication console, do the following:

1. Check prerequisites and limitations.
2. Launch the Configuration Restore wizard.
3. Choose a backup file.
4. Review the backup file info.
5. Specify a decryption password.
6. Choose restore options.
7. Specify a user whose credentials will be used to connect to the appliance.
8. Wait for the restore process to complete.
9. Finish working with the wizard.

### Limitations and Considerations

Before you restore configuration of a backup appliance, consider the following:

- Make sure there are no sessions currently running on the backup appliance. Also, make sure there are no backup policies scheduled to run during restore. Otherwise, backups created by these policies may be corrupted.
- If the backup appliance requires an upgrade, perform it before you start configuration restore. Otherwise, Veeam Backup & Replication will not be able to perform the restore operation. To learn how to upgrade appliances, see Updating Appliances Using Console.
- If you remove the backup appliance from the backup infrastructure, you will not be able to restore its configuration. However, you will be able to restore the configuration to another backup appliance currently added to the backup infrastructure.

- If you want to restore the configuration of the backup appliance to another one, you must remove the initial appliance from the backup infrastructure beforehand.
- Make sure that repositories added to the backup appliance are not managed by any other appliances. Otherwise, retention sessions running on different appliances may corrupt backup files stored in the repositories, which may result in unpredictable data loss.
- The appliance to which you restore the configuration preserves its TLS certificate.
- [Applies only if you restore the configuration of the backup appliance to another one] During restore, Veeam Backup & Replication removes the appliance and its repositories from the backup infrastructure. If the restore operation fails, re-add the appliance and its repositories to the backup infrastructure.

## Performing Configuration Restore

To restore the configuration database of a backup appliance, do the following:

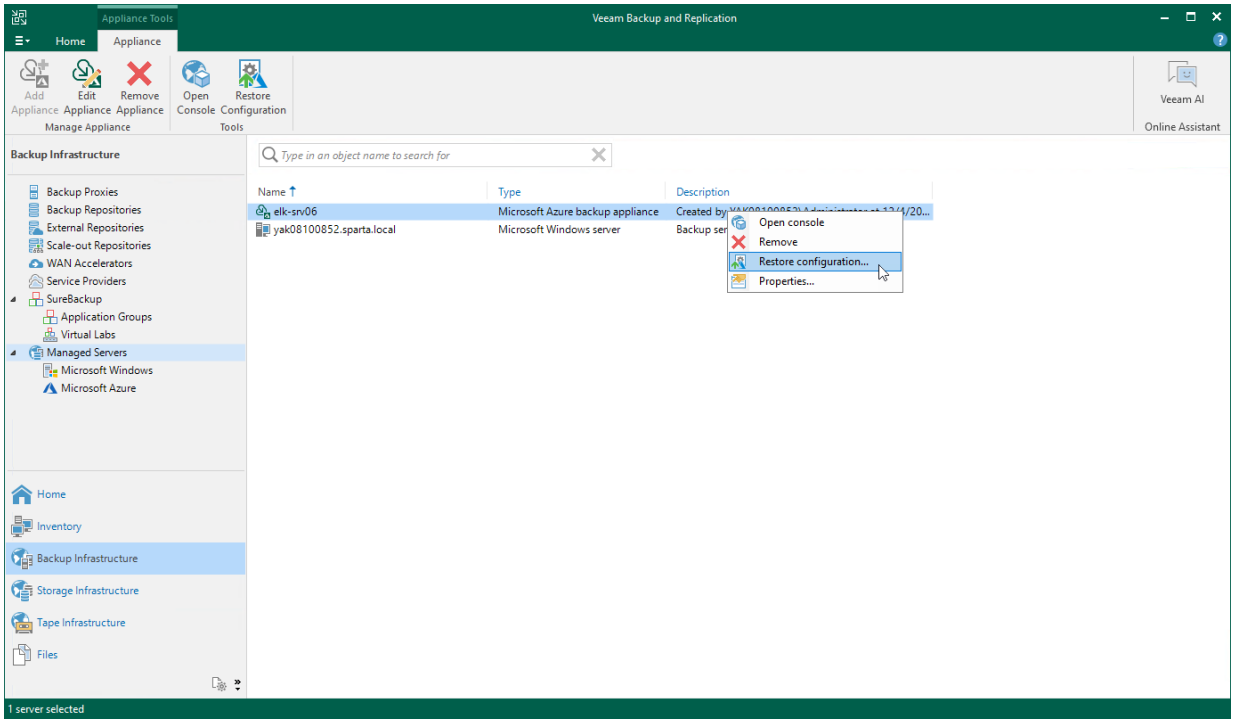
1. Launch the Configuration Restore wizard.
2. Choose a backup file.
3. Review the backup file info.
4. Specify a decryption password.
5. Choose restore options.
6. Specify a user whose credentials will be used to connect to the appliance.
7. Wait for the restore process to complete.
8. Finish working with the wizard.

## Step 1. Launch Configuration Restore Wizard

To launch the **Configuration Restore** wizard, do the following:

1. In the Veeam Backup & Replication console, open the **Backup Infrastructure** view.
2. Navigate to **Managed Servers** > **Microsoft Azure**.
3. Select a backup appliance for which you want to perform the restore operation, and click **Restore Configuration** on the ribbon.

   Alternatively, you can right-click the necessary appliance and select **Restore Configuration**.



## Step 2. Choose Backup File

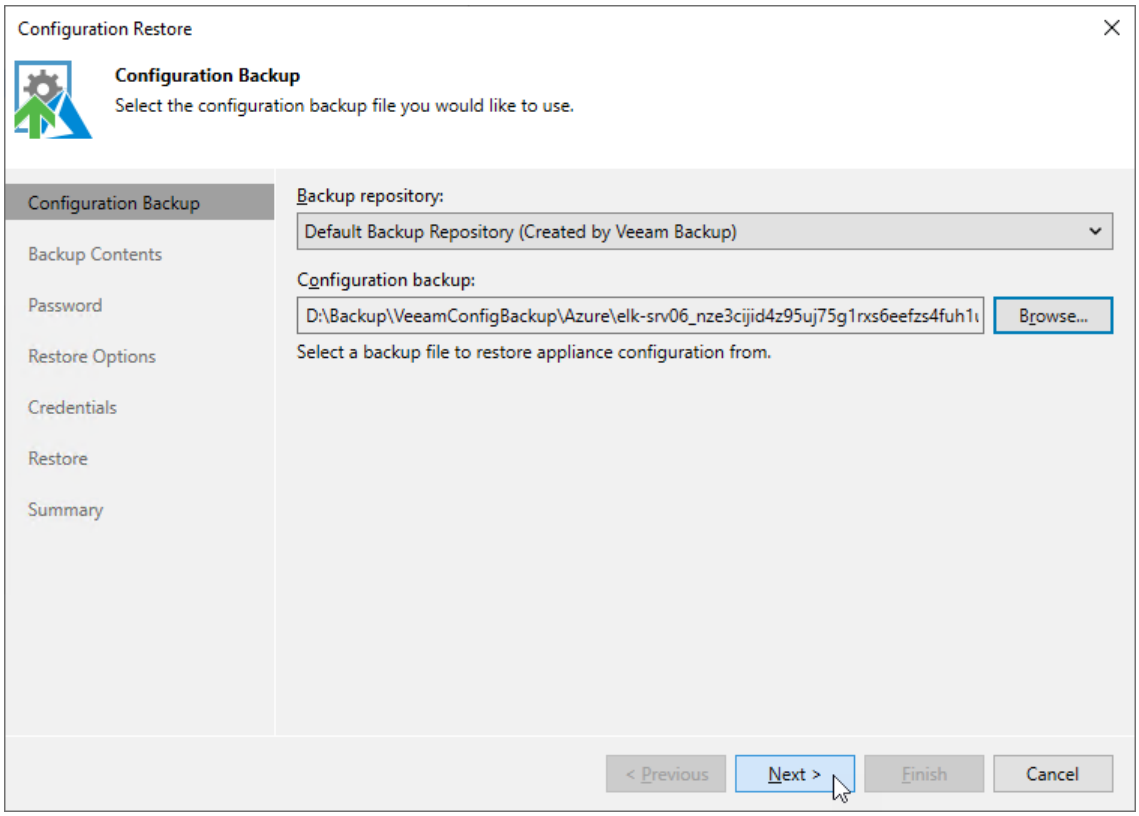
At the **Configuration backup** step of the wizard, do the following:

1. From the **Backup Repository** list, select a repository where the configuration backup file is stored.

   For a repository to be displayed in the list of available repositories, it must be added to the backup infrastructure as described Veeam Backup & Replication User Guide, section Adding Backup Repositories.

2. Click **Browse** and select the necessary file.

> **NOTE**
>
> If the selected configuration backup file is not stored on the backup server, Veeam Backup & Replication will copy the file to a temporary folder on the server and automatically delete it from the folder as soon as the restore process completes.

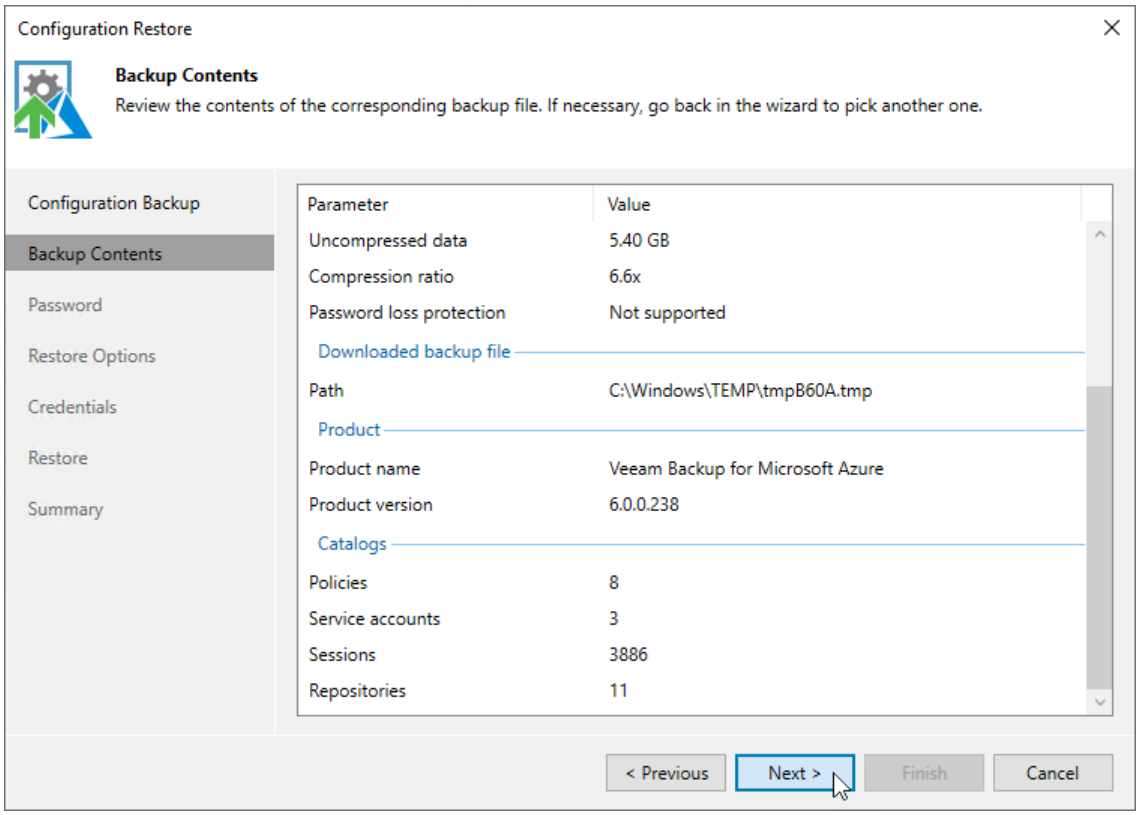


## Step 3. Review Backup File Info

At the **Backup Contents** step of the wizard, Veeam Backup & Replication will analyze the content of the selected backup and display the following information:

- Backup file — the data and time when the backup file was created, the size of the file, the file location and so on.
- [Applies if the configuration backup file selected at step 2 is not stored on the backup server] Downloaded backup file — the temporary location of the configuration backup file on the backup server.
- Product — the name of the product and its version that was installed on the initial appliance.
- Catalogs — configuration data saved in the file (such as the number of configured backup policies, added user accounts, created repositories, logged session records an so on).

At the **Backup Contents** step of the wizard, review the provided information and click **Next** to confirm that you want to use the selected file to restore the configuration data.

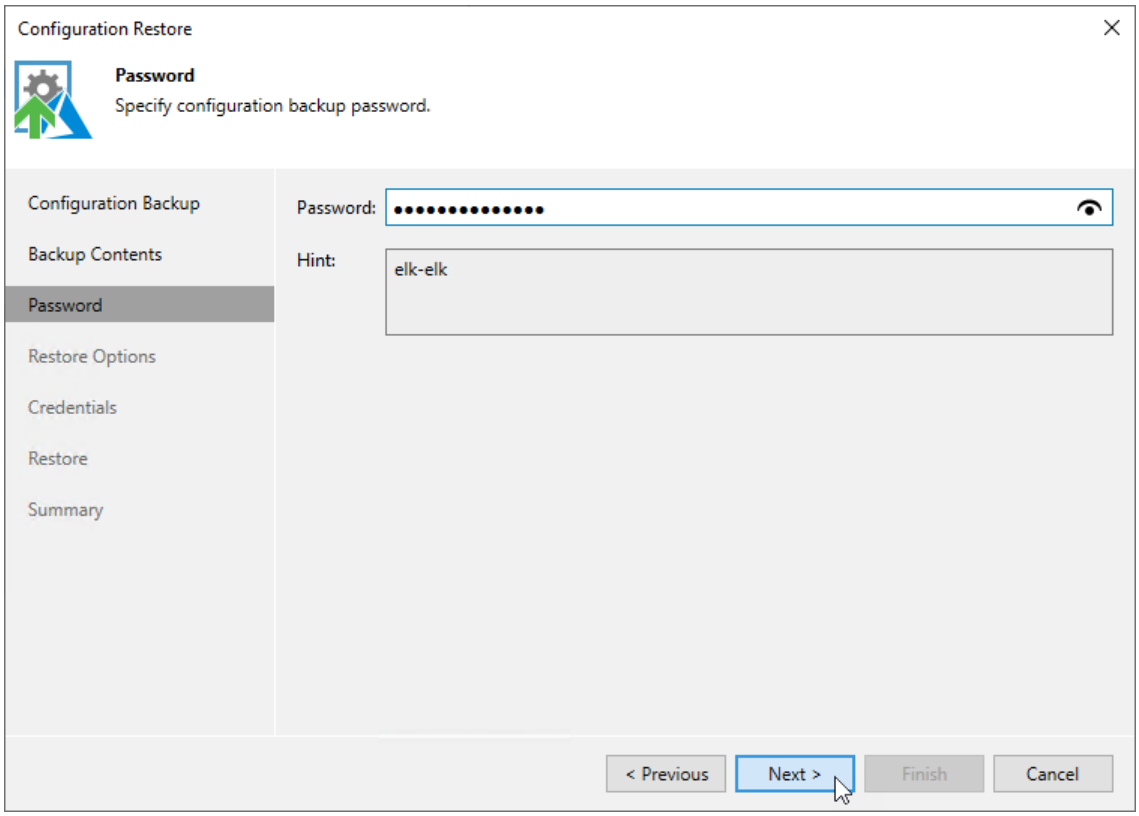


## Step 4. Specify Password

At the **Password** step of the wizard, specify the password used to encrypt the configuration backup file.

If you do not remember the password, you can restore configuration data without providing it. To do that, click the **I forgot the password** link and follow the instructions provided in the Veeam Backup & Replication User Guide, section Decrypting Data Without Password.

> **NOTE**
>
> To restore configuration data without a password, the following requirements must be met:
>
> - You must have either the Veeam Universal License or a legacy socket-based license (Enterprise edition or higher) installed on the backup server.
> - The backup server must be connected to Veeam Backup Enterprise Manager, and password loss protection must be enabled on the Veeam Backup Enterprise Manager side for the duration of both the backup and restore operations. For more information, see the Veeam Backup Enterprise Manager Guide.



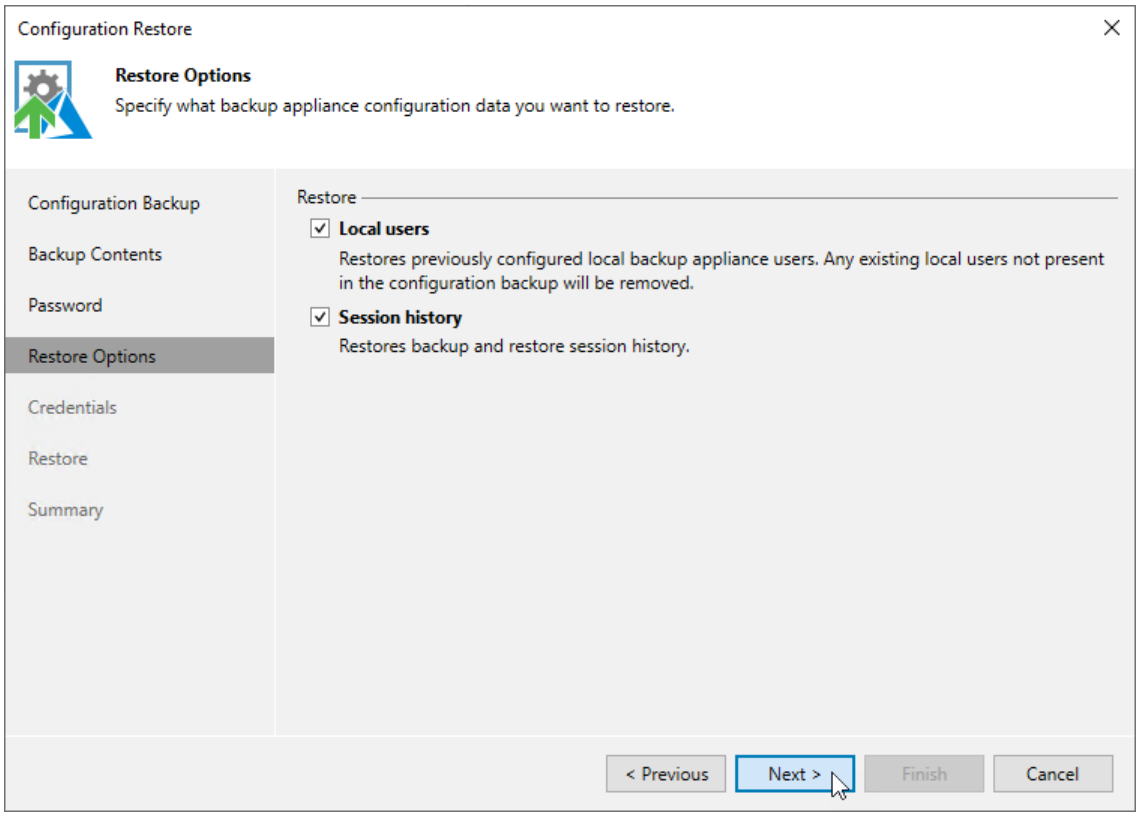
## Step 5. Choose Restore Options

By default, Veeam Backup & Replication restores configuration data for the existing infrastructure components, created backup policies, configured global settings.

At the **Restore options** step of the wizard, you can choose whether you want to restore session logs and portal users of the initial backup appliance as well.

If you select the **Local users** check box, Veeam Backup & Replication will restore all Portal Administrators, Portal Operators and Restore Operators saved to the configuration backup file — and overwrite the currently added portal users. If you select the **Session history** option, Veeam Backup & Replication will restore backup sessions, restore sessions, rescan sessions and service sessions — in this case, the restore process may take more to complete.

> **IMPORTANT**
>
> After you click **Next**, the restore process will start. You will not be able to halt the process or edit the restore settings.



## Step 6. Specify User Credentials

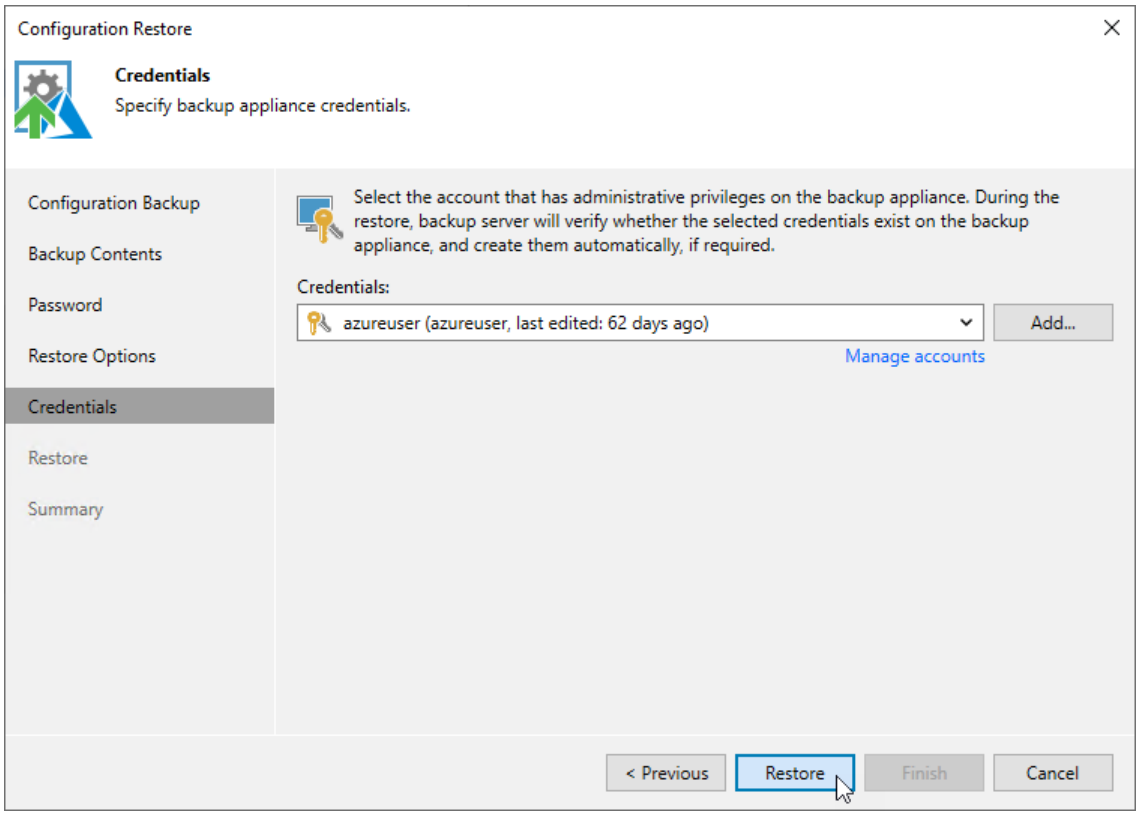
[This step applies only if you have selected the **Local users** option at the **Restore Options** step of the wizard]

After the configuration restore process completes, Veeam Backup & Replication will try to connect to the backup appliance using credentials of the user specified when adding the appliance to the backup infrastructure. However, since you have chosen to restore all users saved to the configuration backup file, this user may be overwritten and Veeam Backup & Replication will fail to connect to the appliance.

That is why at the **Credentials** step of the wizard, you will be prompted to specify a user whose credentials Veeam Backup & Replication will use to connect to the backup appliance. You can specify a new or an existing user. If you specify an existing user, the user must have been assigned the Portal Administrator role on the initial appliance and the credentials of the user must match the credentials saved in the configuration backup file.

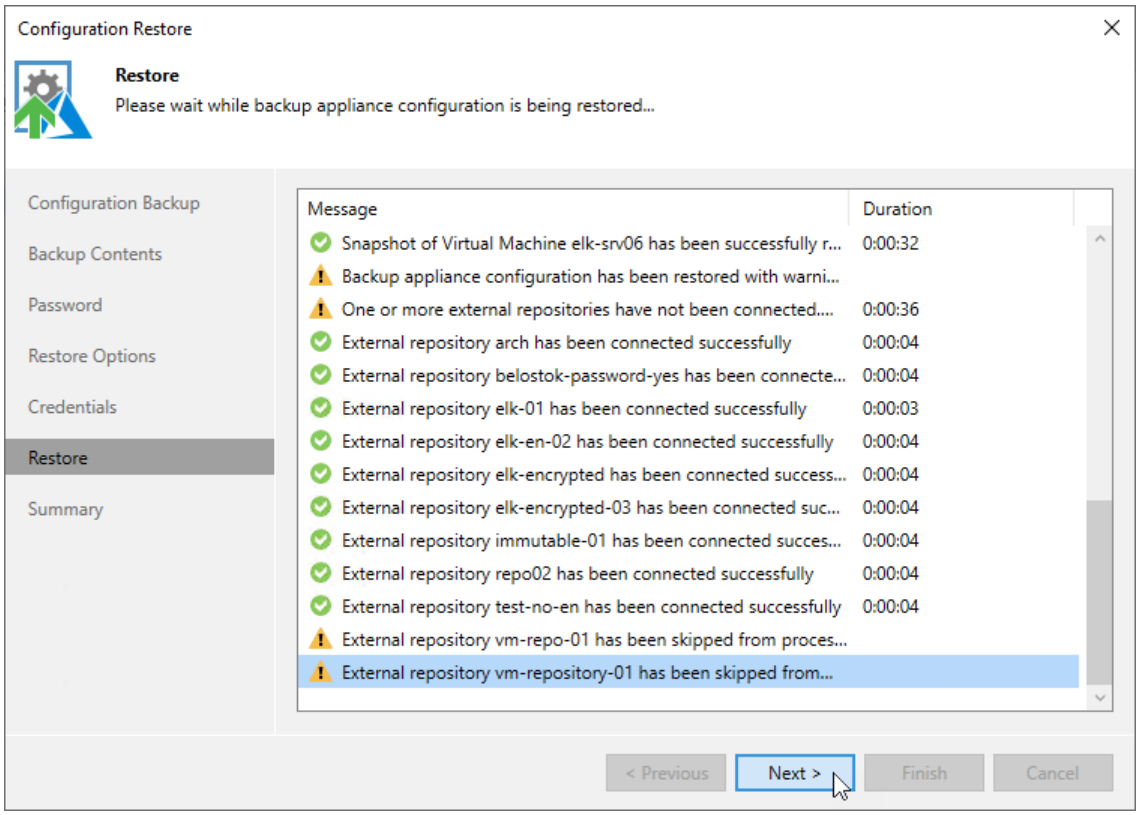
For a user to be displayed in the **Credentials** list, it must be added to the Credentials Manager as described in the Veeam Backup & Replication User Guide, section Standard Accounts. If you have not added the necessary user to the Credentials Manager beforehand, you can do it without closing the **Configuration Restore** wizard. To do that, click either the **Manage accounts** link or the **Add** button and specify the user name, password and description in the **Credentials** window.

> **IMPORTANT**
>
> After you click **Restore**, the restore process will start. You will not be able to halt the process or edit the restore settings.



## Step 7. Track Progress

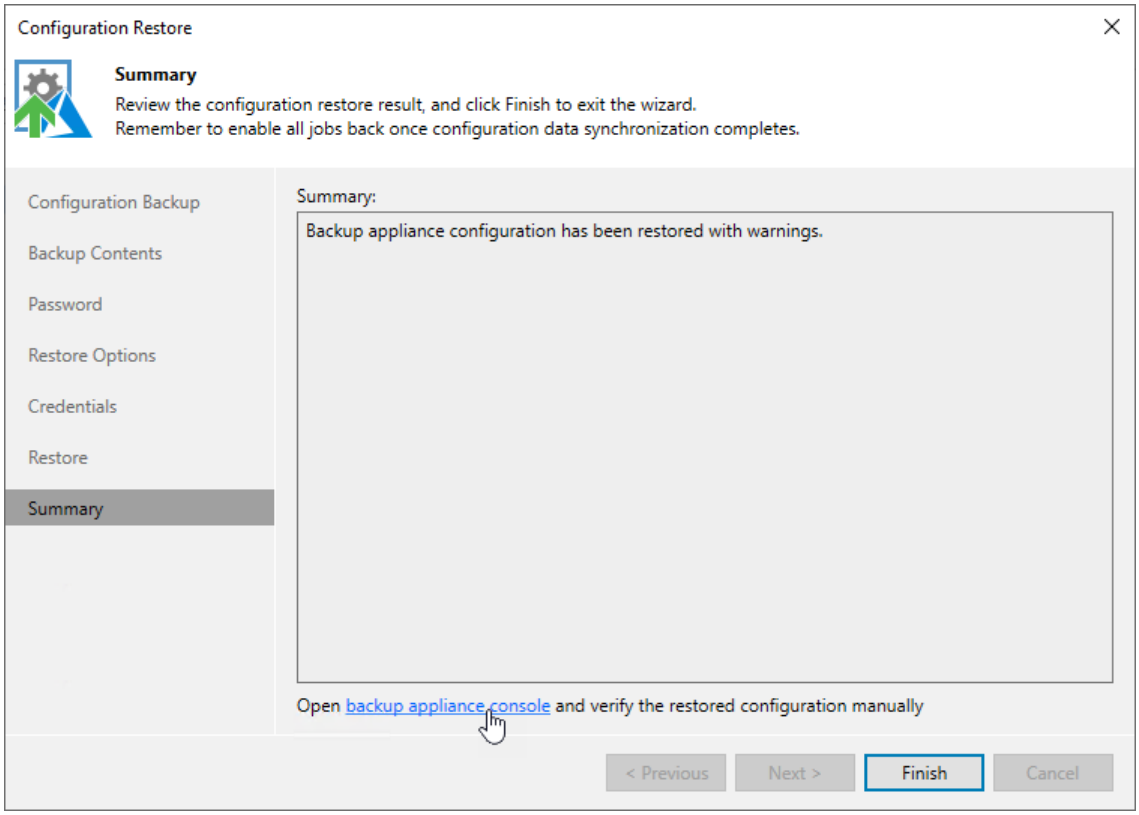
Veeam Backup & Replication will display the results of every step performed while executing the configuration restore. At the **Restore** step of the wizard, wait for the restore process to complete and click **Next**.



### Step 8. Finish Working with Wizard

At the **Summary** step of the wizard, click **Finish** to finalize the process of configuration data restore.

If Veeam Backup & Replication encounters an issue while performing configuration restore, the wizard will display the **Open backup appliance console and validate the restored configuration manually** link. This link redirects you to the Veeam Backup for Microsoft Azure Web UI where you can view the details on the occurred issues. To learn how to resolve issues, see section View Configuration Check Results.




# Restoring Configuration Data Using Web UI

To restore the configuration database of a backup appliance using the Veeam Backup for Microsoft Azure Web UI, do the following:

1. Launch the Configuration Restore wizard.
2. Choose a backup file.
3. Review the backup file info.
4. Choose restore options.
5. Track the restore progress.
6. View the results of verification steps.
7. Finish working with the wizard.

IMPORTANT

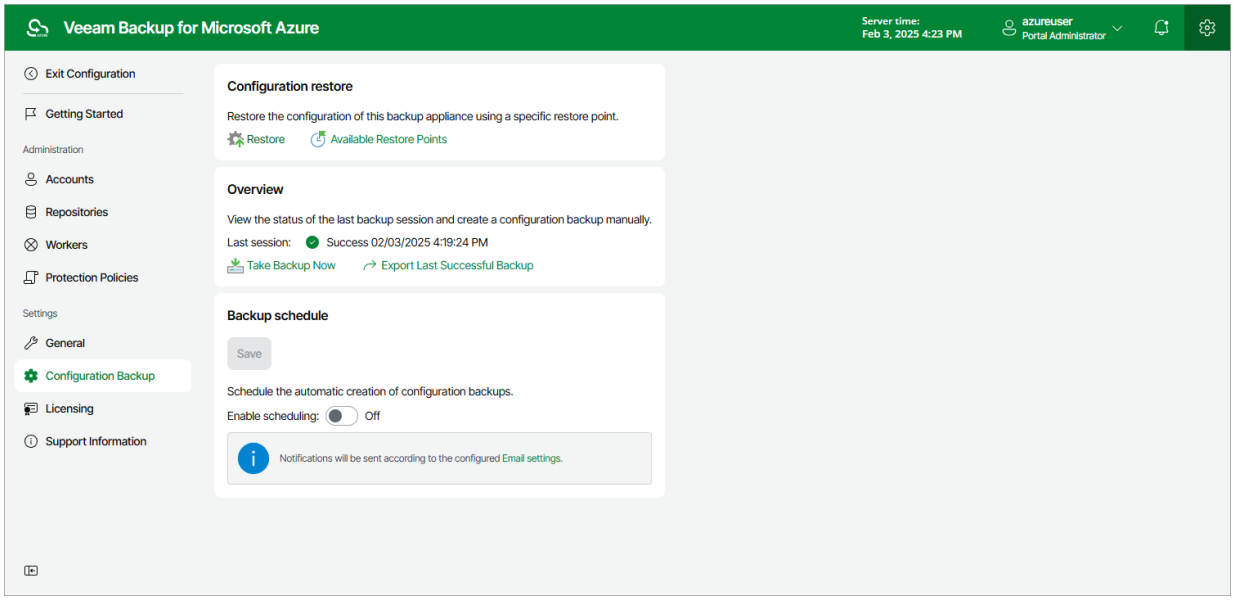
- Before you start the restore process, stop all policies that are currently running.
- If the backup appliance to which you plan to restore the configuration database is managed by a Veeam Backup & Replication server, you will not be able to restore the configuration of Veeam Backup for Microsoft Azure from the Web UI. In this case, you can perform configuration restore using the Veeam Backup & Replication console as described in section Restoring Configuration Data Using Console.
- If the backup appliance whose configuration database you plan to restore used the Azure Service Bus messaging service, you must switch to the Azure Queue Storage service immediately after the restore operation is complete. For more information, see Configuring Deployment Mode.

After Veeam Backup for Microsoft Azure performs configuration restore, it rescans the whole infrastructure to detect obsolete snapshots. These snapshots are then removed from the configuration database according to the specified global retention settings.

# Step 1. Launch Configuration Restore Wizard

To launch the **Configuration Restore** wizard, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **Configuration Backup**.
3. In the **Configuration restore** section, click **Restore**.



# Step 2. Choose Backup File

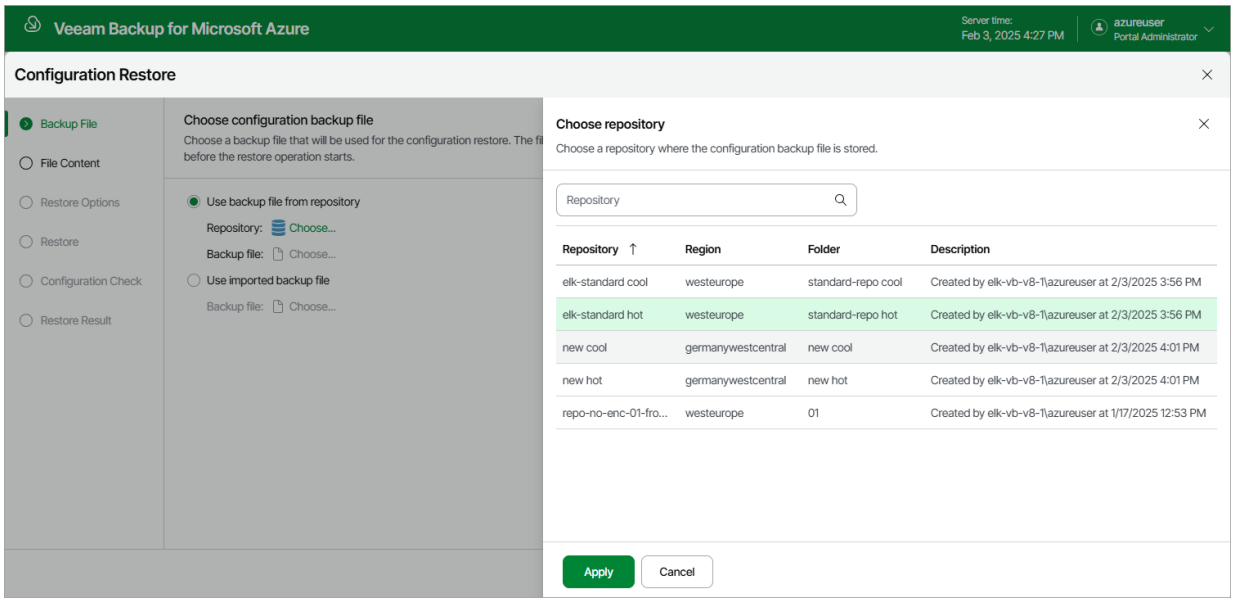
At the **Backup File** step of the wizard, choose whether you want to use an exported backup file or a backup file stored in a backup repository:

- If you want to use a file stored in a backup repository, select the **Use backup file from repository** option and do the following:
  a. Click **Choose** in the **Repository** field, and use the list of available repositories in the **Choose repository** window to select the repository where the necessary configuration backup file is stored.

     For a backup repository to be displayed in the **Repository** list, it must be added to Veeam Backup for Microsoft Azure as described in section Adding Backup Repositories. The list shows only backup repositories that have encryption enabled and immutability disabled.

  b. Click **Choose** in the **Backup file** field, and select the necessary file in the **Choose backup file** window.
- If you want to use a file that was exported from this or another backup appliance, select the **Use imported backup file** option and do the following:
  a. Click **Choose** in the **Backup file** field.
  b. In the **Import backup file** window, browse to the necessary backup file, provide the password that was used to encrypt the file, and click **Import**.

> **IMPORTANT**
>
> The size of an uploaded backup file must not exceed 10 GB. To upload a file of a bigger size, open a support case.



# Step 3. Review Backup File Info

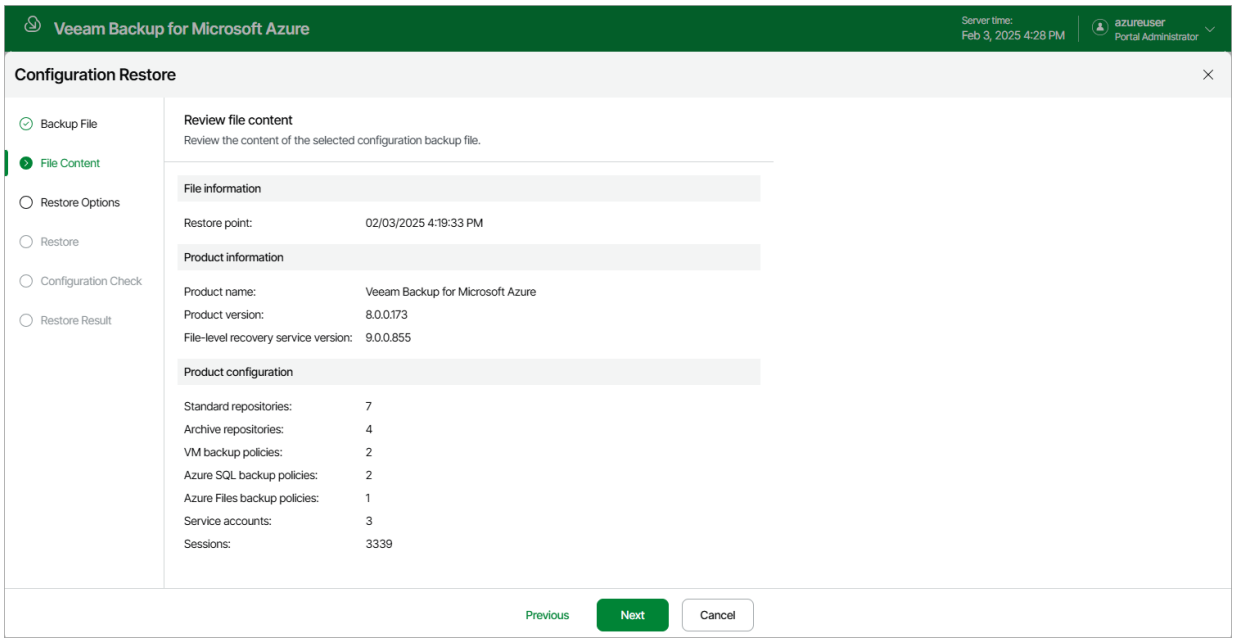
Veeam Backup for Microsoft Azure will analyze the content of the selected backup file and display the following information:

- File information — the date and time when the backup file was created.
- Product information — the version of Veeam Backup for Microsoft Azure that was installed on the initial backup appliance and the version of the File-level recovery service that was running on the appliance.

> **IMPORTANT**
>
> Consider that if the current version of Veeam Backup for Microsoft Azure installed on the backup appliance is later than the version saved in the configuration backup file, the configuration restore operation will not downgrade the backup appliance version.

- Product configuration — configuration data saved in the file (such as the number of configured backup policies, added user accounts, created backup repositories, logged session records and so on).

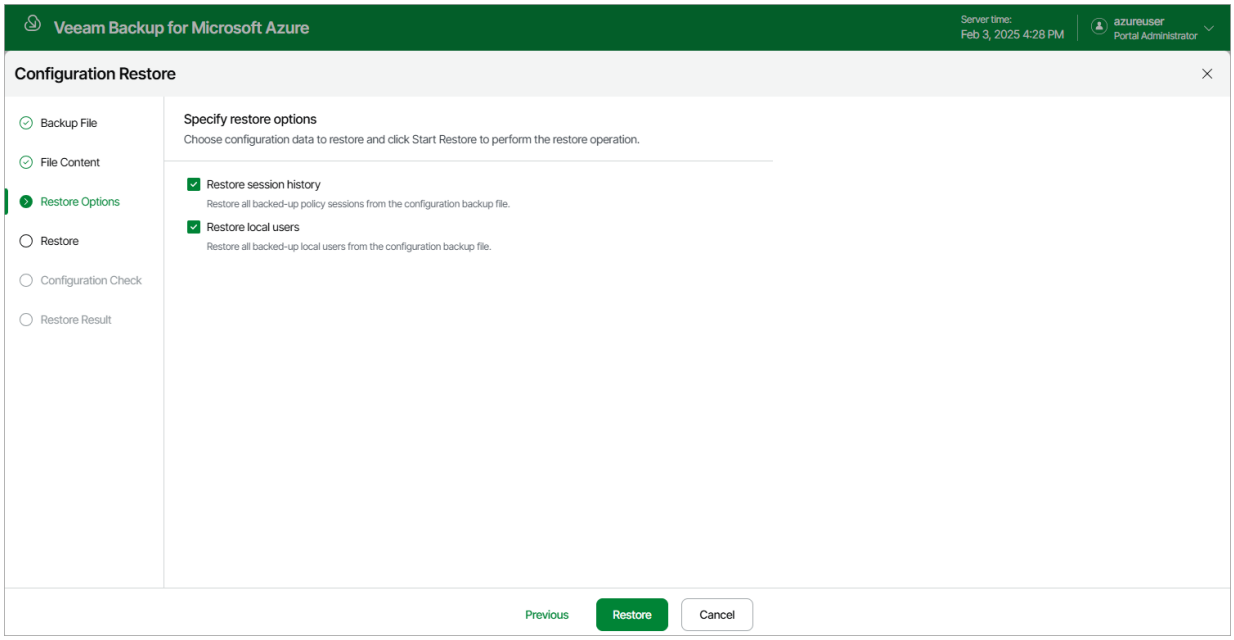
At the **File Content** step of the wizard, review the provided information and click **Next** to confirm that you want to use the selected file to restore the configuration data.



# Step 4. Choose Restore Options

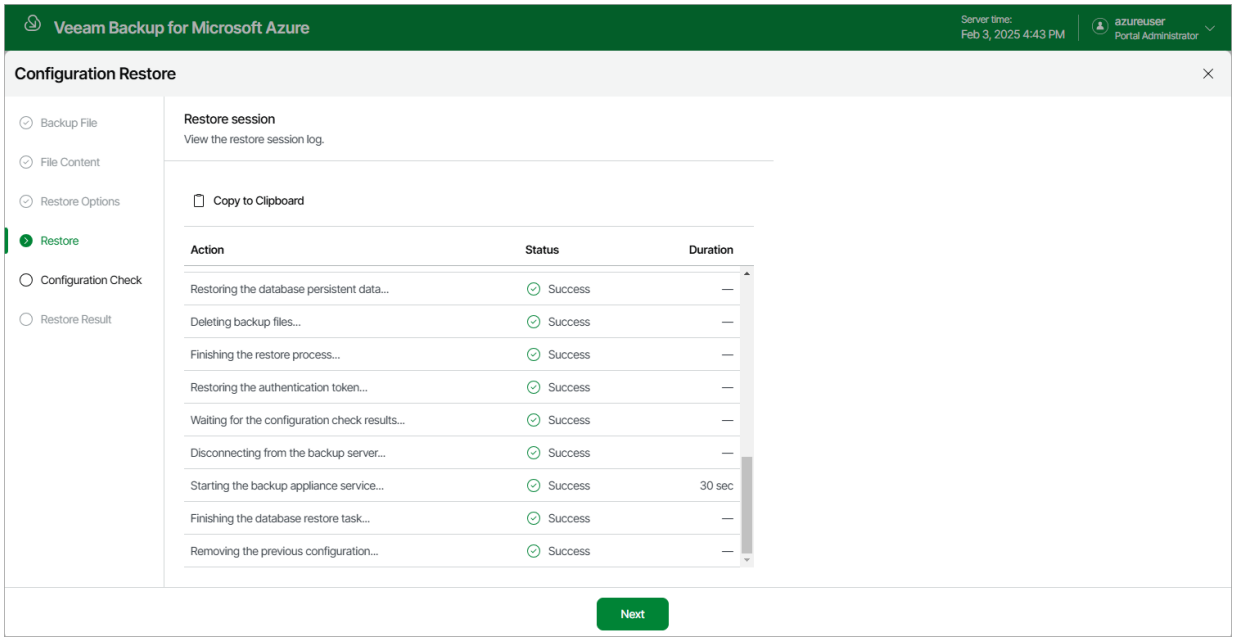
By default, Veeam Backup for Microsoft Azure restores only configuration data for the existing architecture components, created backup policies and configured global settings. At the **Restore Options** step of the wizard, you can choose whether you want to restore session logs and user accounts of the initial backup appliance as well.

> **IMPORTANT**
>
> After you click **Restore**, the restore process will start. You will not be able to halt the process or edit the restore settings.



# Step 5. Track Restore Progress

Veeam Backup for Microsoft Azure will display the results of every step performed while executing the configuration restore. At the **Restore** step of the wizard, wait for the restore process to complete and click **Next**.

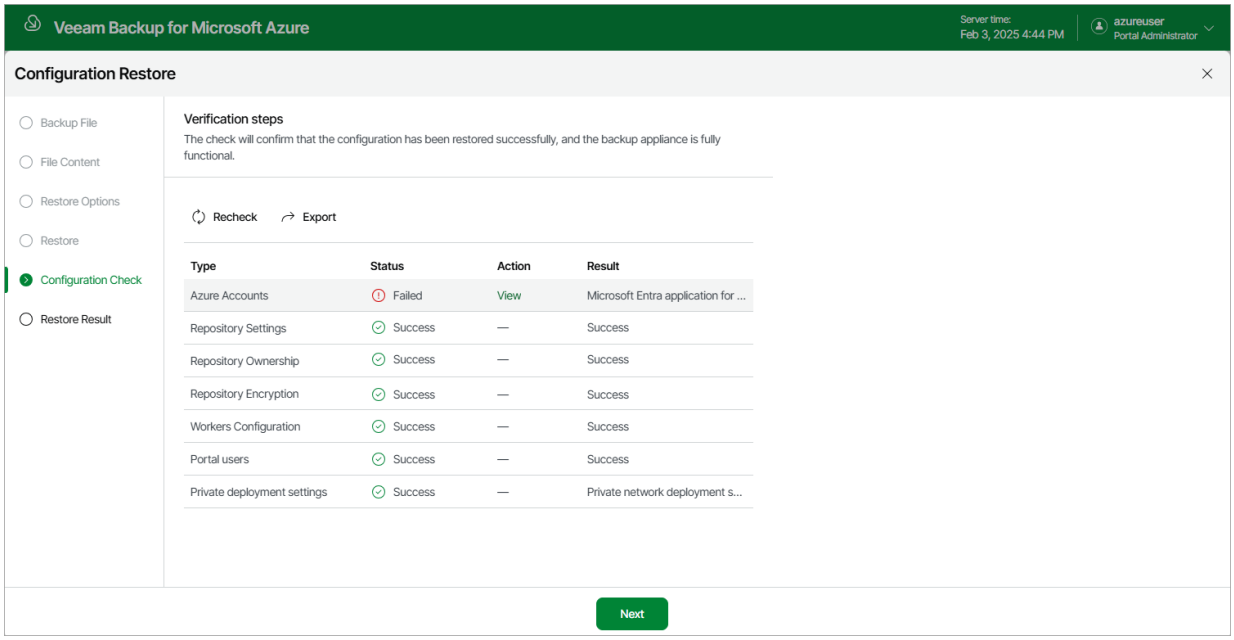


# Step 6. View Configuration Check Results

After the restore process is over, Veeam Backup for Microsoft Azure will run a number of verification checks to confirm that the configuration data has been restored successfully. At the **Configuration Check** step of the wizard, wait for the verification checks to complete and check whether Veeam Backup for Microsoft Azure encountered any configuration issues.

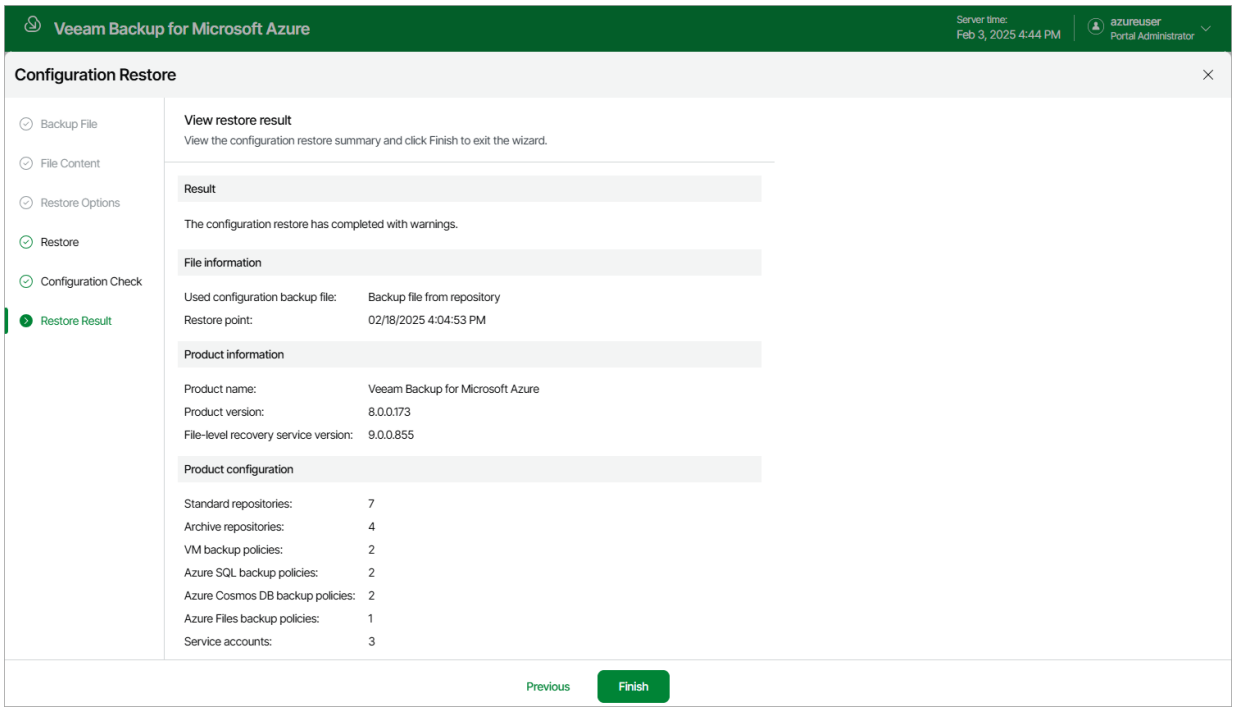
If Veeam Backup for Microsoft Azure encounters an issue while performing a verification check, the Result column will display a description of the issue, and the **Action** column will provide instructions on how to resolve it. After you resolve all issues, click **Recheck** to ensure the backup appliance is now fully functional, and click **Next**.

> **IMPORTANT**
>
> Restored repositories must not be managed by multiple backup appliances simultaneously — retention sessions running on different backup appliances may corrupt backup files stored in the repositories, which may result in unpredictable data loss. That is why Veeam Backup for Microsoft Azure verifies whether the restored backup repositories are managed by any backup appliances — but only for those repositories that were added to Veeam Backup for Microsoft Azure version 7.0 or later. If the backup repositories are already managed by any backup appliances, Veeam Backup for Microsoft Azure encounters an issue while performing a verification check. To resolve the issue, you must change the owner of these repositories to complete the restore session. To do that, in the **Action** column, click View in the **Repositories ownership** field. Then, click **Take Ownership** in the **Repository ownership** window.



# Step 7. Finish Working with Wizard

At the **Restore Result** step of the wizard, click **Finish** to finalize the process of configuration data restore.



# Viewing Available Resources

After you create a backup policy to protect a specific type of Azure resources (Azure VMs, Azure SQL databases, Cosmos DB accounts or Azure file shares), Veeam Backup for Microsoft Azure rescans Azure regions specified in the policy settings and populates the resource list on the **Resources** page with all resources of that type residing in these regions. If a region is no longer specified in any backup policy, Veeam Backup for Microsoft Azure removes resources residing in the region from the list of available resources.

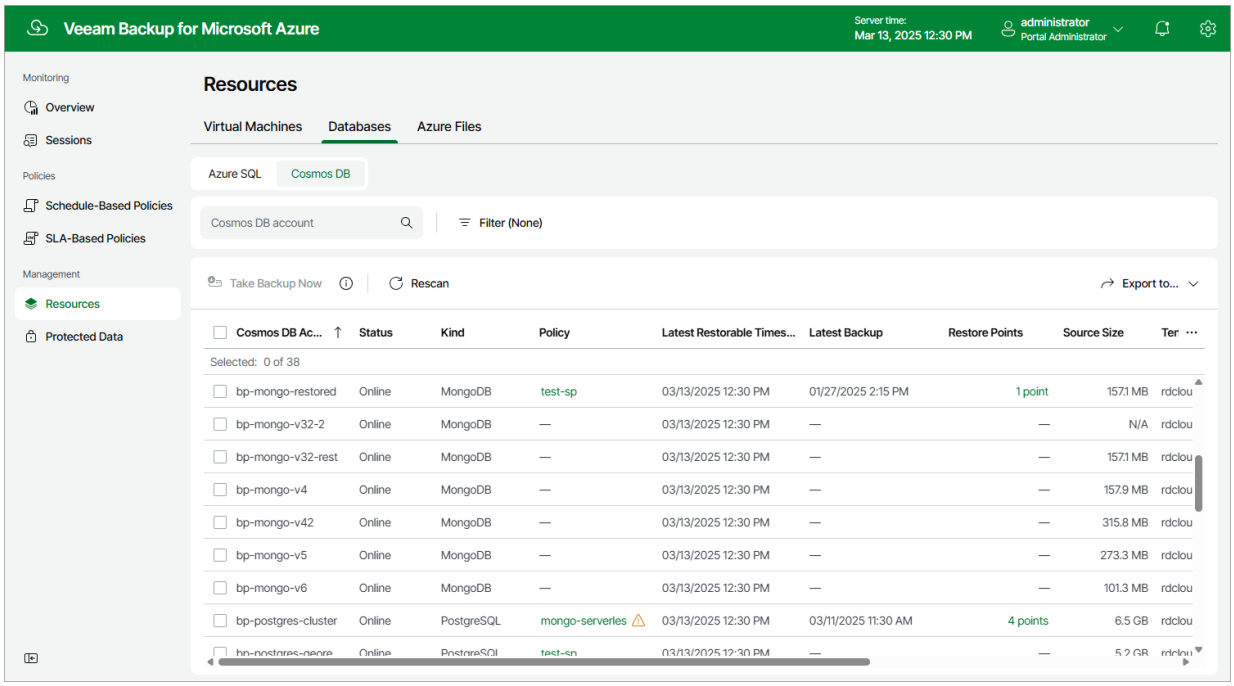
The **Resources** page displays Azure resources that can be protected by Veeam Backup for Microsoft Azure. Each resource is represented with a set of properties, such as:

- **Virtual Machine** or **Databases** (**Azure SQL** or **Cosmos DB**) or **File Share** – the name of the resource.
- **Policy** – the name of the backup policy that protects the resource (if any).
- **Region** – the region in which the resource resides.
- **Restore Points** – the number of restore points created for the resource (if any).
- **Latest Backup** – the date and time of the most recent backup policy (if any).

> **NOTE**
>
> Cosmos DB accounts that have the *Deleted* status cannot be added to a backup policy.

On the **Resources** page, you can also perform the following actions:

- Manually create backups of Azure SQL databases, Cosmos DB for PostgreSQL accounts and Cosmos DB for MongoDB accounts. For more information, see Performing SQL Backup and Performing Cosmos DB Backup.
- Manually create cloud-native snapshots of Azure VMs and Azure file shares. For more information, see sections Performing VM Backup and Performing Azure Files Backup.



# Performing Backup

With Veeam Backup for Microsoft Azure, you can protect data in the following ways:

- **Create cloud-native snapshots of Azure VMs**

  A cloud-native snapshot includes point-in-time snapshots of virtual disks attached to the processed Azure VM. Snapshots of virtual disks are taken using native Microsoft Azure capabilities.

- **Create image-level backups of Azure VMs**

  In addition to cloud-native snapshots, you can protect your Azure VMs with image-level backups. An image-level backup captures the whole image of the processed Azure VM (including OS data, application data and so on) at a specific point in time. The backup is saved as multiple files to a backup repository in the native Veeam format.

- **Create backups of Azure SQL databases**

  A backup of an Azure SQL database captures the whole image of the processed database (including tables, constraints, indexes and actual data) at a specific point of time. The backup is saved as multiple files to a backup repository in the native Veeam format.

- **Create backups of Cosmos DB accounts**

  To back up Cosmos DB accounts, Veeam Backup for Microsoft Azure uses the native Microsoft Azure continuous backup feature.

  For each processed Cosmos DB for PostgreSQL or Cosmos DB for MongoDB account, you can also choose to store backups in a repository. A backup of a Cosmos DB for PostgreSQL or Cosmos DB for MongoDB account stored in a repository includes user data contained in the database of this account. The backup is saved as a dump file to a backup repository in the native Veeam format.

- **Create cloud-native snapshots of Azure file shares**

  A cloud-native snapshot includes point-in-time snapshots of base files, metadata and files in the system properties of the processed Azure file share. Snapshots of these files are taken using native Microsoft Azure capabilities.

> **NOTE**
>
> Consider that if you delete a file share from Microsoft Azure, the snapshots of this file share will be deleted as well. To protect your snapshots from accidental deletion, you can use the file share soft delete option. For more information on the soft delete option for Azure file shares, see Microsoft Docs.

- **Create backups of your virtual network configuration**

  A virtual network configuration backup captures the whole image of a virtual network configuration of an Azure subscription (including multiple virtual network configuration settings and components) at a specific point in time. The virtual network configuration backup is stored in the Veeam Backup for Microsoft Azure database.

> **IMPORTANT**
>
> Veeam Backup for Microsoft Azure supports only the backup of the following virtual network configuration components: virtual networks, subnets, IP configurations, network security groups, route tables, network interfaces and virtual network peerings.

To schedule data protection tasks to run automatically, create backup policies. You will be able to run the backup policies on demand and manually perform backup of Azure VMs, Azure SQL databases, Cosmos DB accounts and Azure file shares. To learn how to perform backup manually, see sections Creating VM Snapshots Manually, Creating File Share Snapshots Manually, Creating SQL Backups Manually and Creating Cosmos DB Backups Manually.

> **TIP**
>
> You can perform advanced data protection operations with image-level backups from the Veeam Backup & Replication console. For more information, see the Veeam Backup & Replication User Guide, section External Repository.

# Performing Backup Using Console

Veeam Backup for Microsoft Azure runs backup policies for every data protection operation. A backup policy is a collection of settings that define the way backup operations are performed: what data to back up, where backups will be stored, when the backup process will start, and so on.

You can create multiple backup policies for Azure resources. One backup policy can be used to process multiple resources within different regions, but you can back up each resource with one backup policy at a time. For example, if an instance is added to more than one backup policy, it will be processed only by a backup policy that has the highest priority. Other backup policies will skip this instance from processing. For information on how to set a priority for a backup policy, see section Setting Backup Policy Priority.

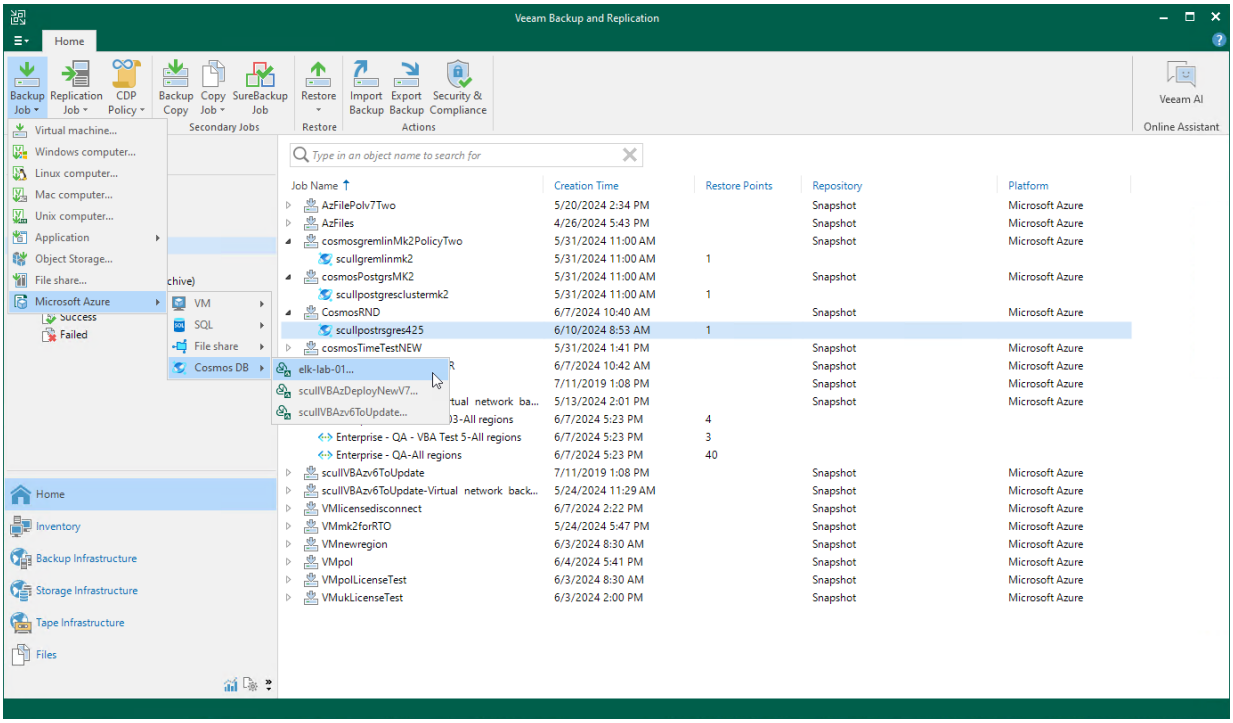
After you install Microsoft Azure Plug-in for Veeam Backup & Replication and add backup appliances to the backup infrastructure, you can manage backup policies directly from the Veeam Backup & Replication console.

# Creating Backup Policies

You can create backup policies in the Veeam Backup for Microsoft Azure Web UI only. However, you can launch the **Add Policy** wizard directly from the Veeam Backup & Replication console — to do that, use either of the following options:

- Switch to the **Home** tab, click **Backup Job** on the ribbon, navigate to **Microsoft Azure** > **VM**, **SQL**, **File share** or **Cosmos DB**, and select the backup appliance on which you want to create the backup policy.
- Open the **Home** view, right-click **Jobs**, navigate to **Backup** > **Microsoft Azure** > **VM**, **SQL**, **File share** or **Cosmos DB**, and select the backup appliance on which you want to create the backup policy.

Veeam Backup & Replication will open the **Add VM Policy**, **Add Azure SQL Policy**, **Add Azure Files Policy** or **Add Cosmos DB Policy** wizard in a web browser. Complete the wizard as described in sections Creating VM Backup Policies, Creating SQL Backup Policies, Creating Azure Files Backup Policies or Creating Cosmos DB Backup Policies.



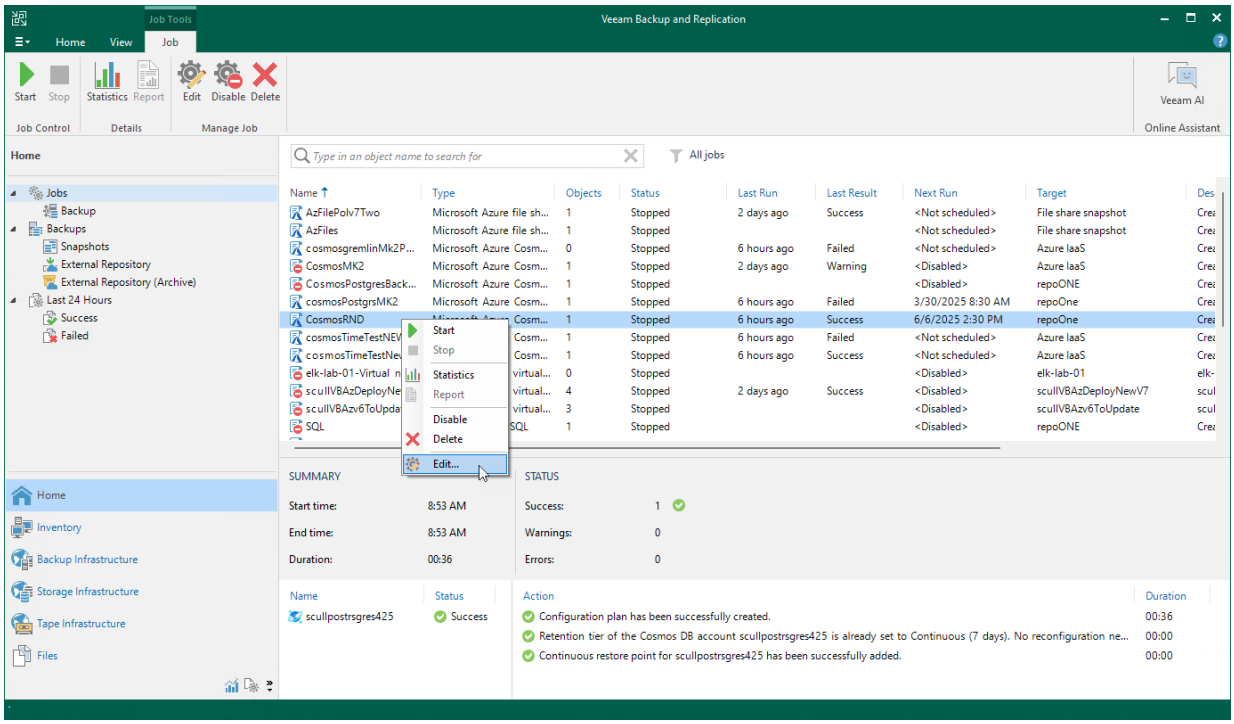
# Editing Backup Policy Settings

You can edit backup policy settings only in the Veeam Backup for Microsoft Azure Web UI. However, you can launch the edit policy wizard directly from the Veeam Backup & Replication console. To do that, do the following:

1. In the Veeam Backup & Replication console, open the **Home** view.
2. Navigate to **Jobs**.
3. Select the necessary backup policy and click **Edit** on the ribbon.

   Alternatively, you can right-click the policy and select **Edit**.

Veeam Backup & Replication will open the **Edit Policy** wizard in a web browser. Complete the wizard as described in section Creating VM Backup Policies, Creating SQL Backup Policies, Creating Azure Files Backup Policies or Editing Virtual Network Configuration Backup Policy.



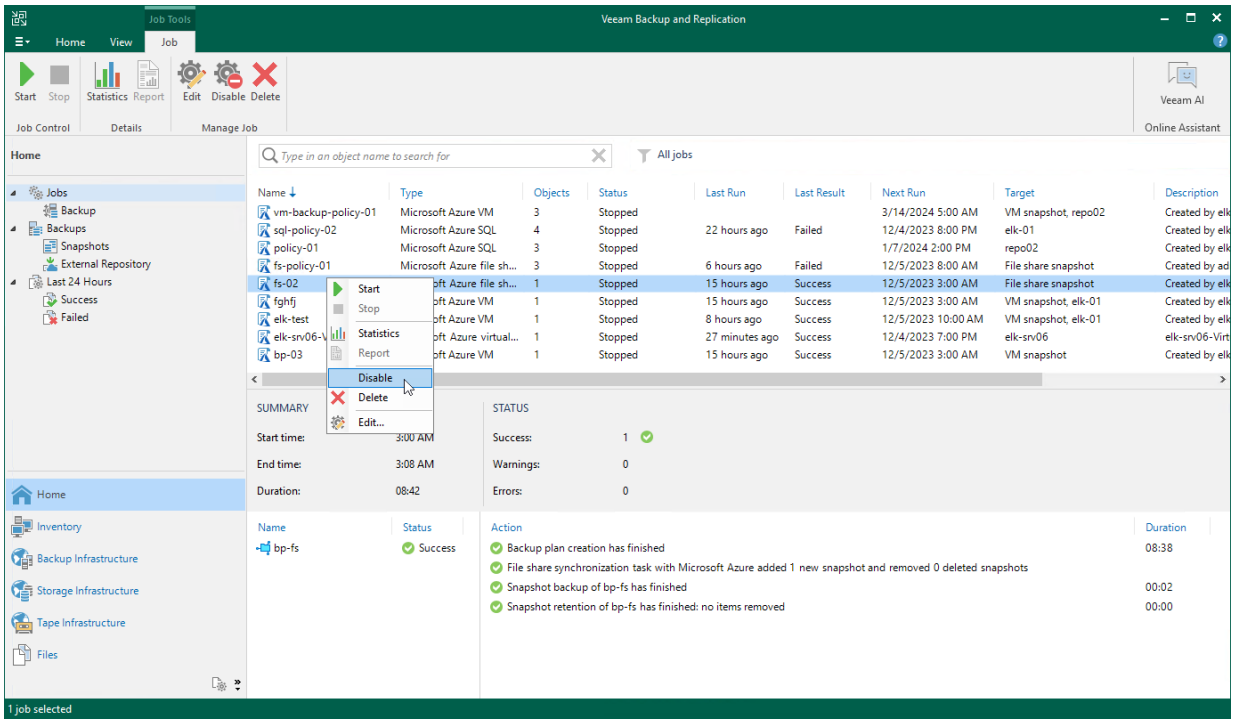
# Enabling and Disabling Backup Policies

By default, Veeam Backup for Microsoft Azure runs all created backup policies according to the specified schedules. However, you can temporarily disable a backup policy so that Veeam Backup for Microsoft Azure does not run the backup policy automatically. You will still be able to manually start or enable the disabled backup policy at any time you need.

To disable an enabled backup policy or to enable a disabled backup policy, do the following:

1. In the Veeam Backup & Replication console, open the **Home** view.
2. Navigate to **Jobs**.
3. Select the necessary backup policy and click **Disable** on the ribbon.

   Alternatively, you can right-click the necessary backup policy and select **Disable**.



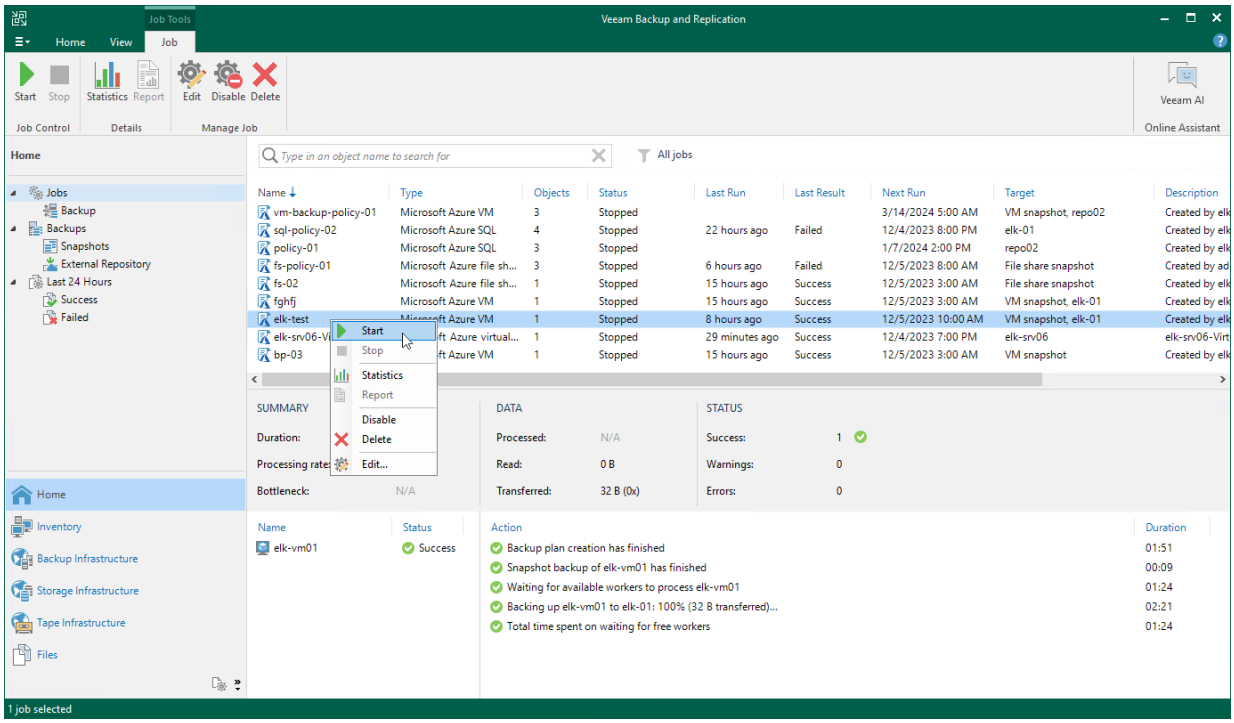
# Starting and Stopping Backup Policies

You can start a backup policy manually, for example, if you want to create an additional restore point in the snapshot or backup chain and do not want to modify the configured backup policy schedule. You can also stop a running backup policy if processing of a workload is about to take too long, and you do not want the policy to produce heavy load on the production environment during business hours.

To start or stop a backup policy, do the following:

1. In the Veeam Backup & Replication console, open the **Home** view.
2. Navigate to **Jobs**.
3. Select the necessary backup policy and click **Start** or **Stop** on the ribbon.

   Alternatively, you can right-click the selected backup policy and select **Start** or **Stop**.



# Deleting Backup Policies

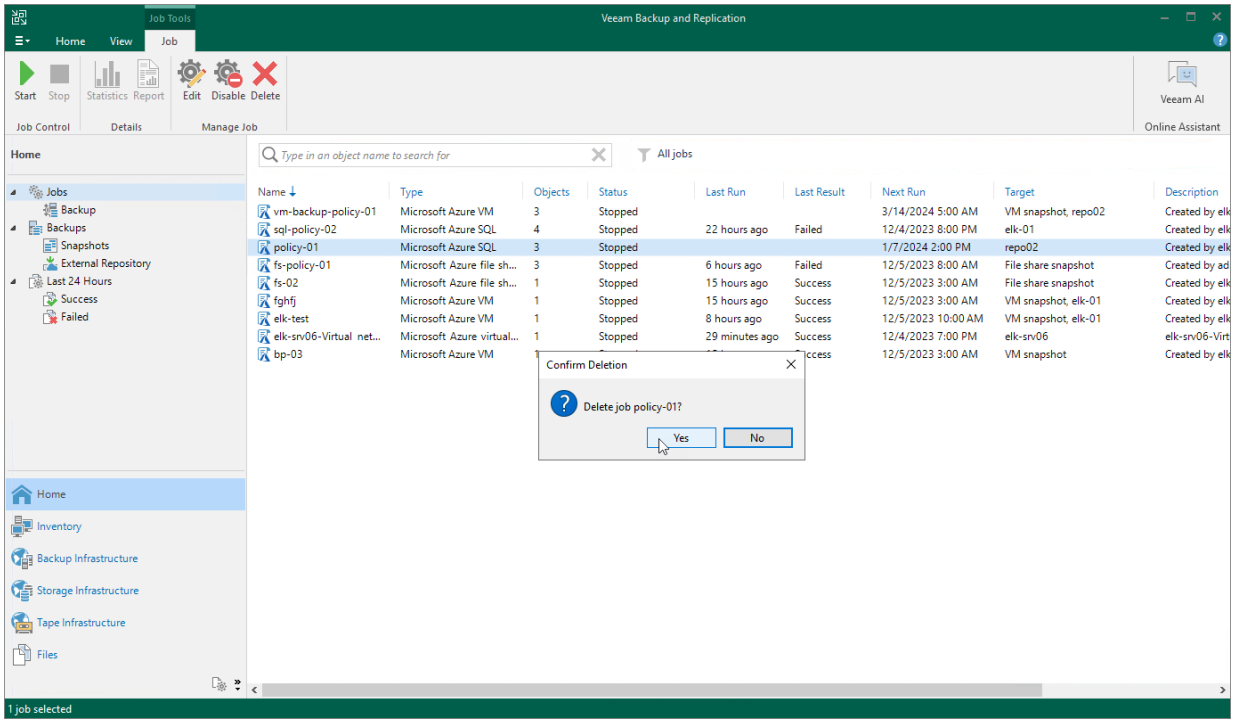
Veeam Backup & Replication allows you to permanently delete backup policies created by Veeam Backup for Microsoft Azure.

To delete a backup policy, do the following:

1. In the Veeam Backup & Replication console, open the **Home** view.
2. Navigate to **Jobs**.
3. Select the necessary backup policy and click **Delete** on the ribbon.

   Alternatively, right-click the necessary backup policy and select **Delete**.

> **IMPORTANT**
>
> When you delete a backup policy from Veeam Backup & Replication, the policy is automatically deleted from the backup appliance as well.



# Creating Backup Copy Jobs

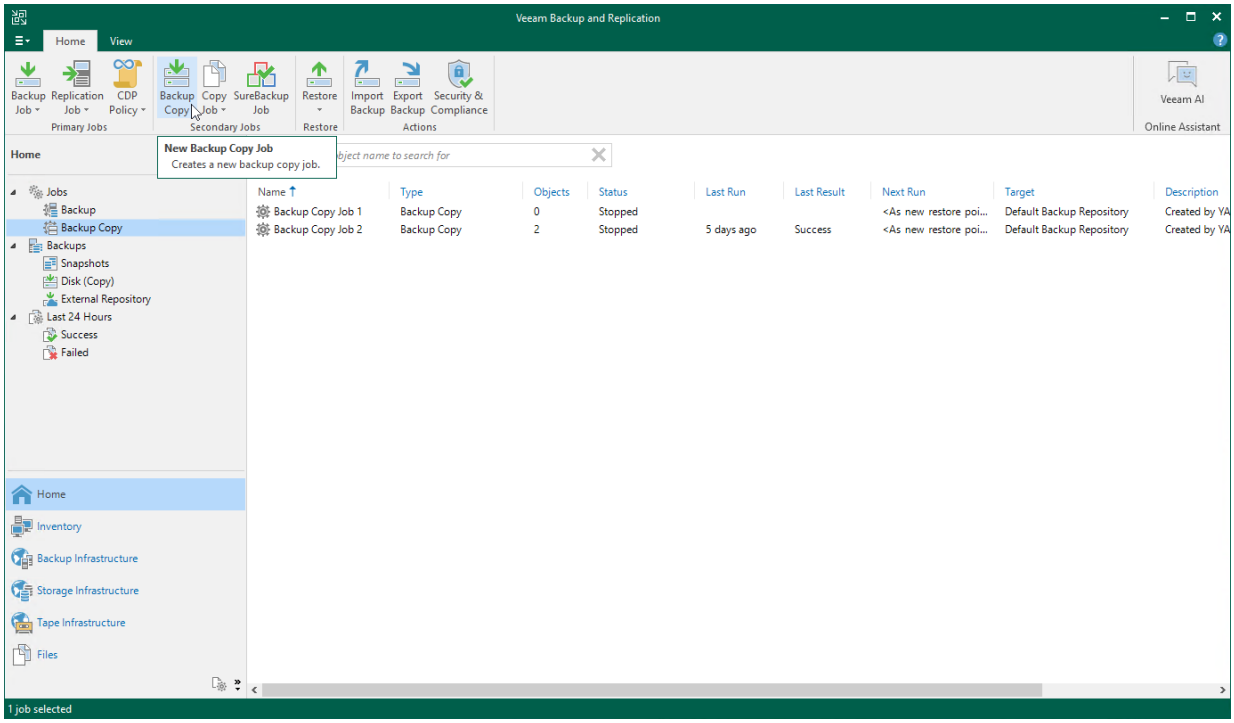
Backup copy is a technology that helps you copy and store backed-up data of Azure VMs in different locations. Storing data in different locations increases its availability and ensures that data can be recovered in case a disaster strikes.

Backup copy is a job-driven process. Veeam Backup & Replication fully automates the backup copy process and lets you specify retention settings to maintain the desired number of restore points, as well as full backups for archival purposes. For more information on the backup copy functionality, see the Veeam Backup & Replication User Guide, section Backup Copy.

> **IMPORTANT**
>
> Backup copy can be performed only using Azure VM backup files stored in standard repositories for which you have specified credentials of Microsoft Azure storage accounts where the target blob containers reside. To learn how to specify credentials for repositories, see sections Creating New Repositories and Connecting to Existing Appliances.

To create a backup copy job, do the following:

1. In the Veeam Backup & Replication console, open the **Home** view.
2. Click **Backup Copy** on the ribbon.
3. Complete the **New Backup Copy Job** wizard as described in the Veeam Backup & Replication User Guide, section Creating Backup Copy Jobs for VMs and Physical Machines.



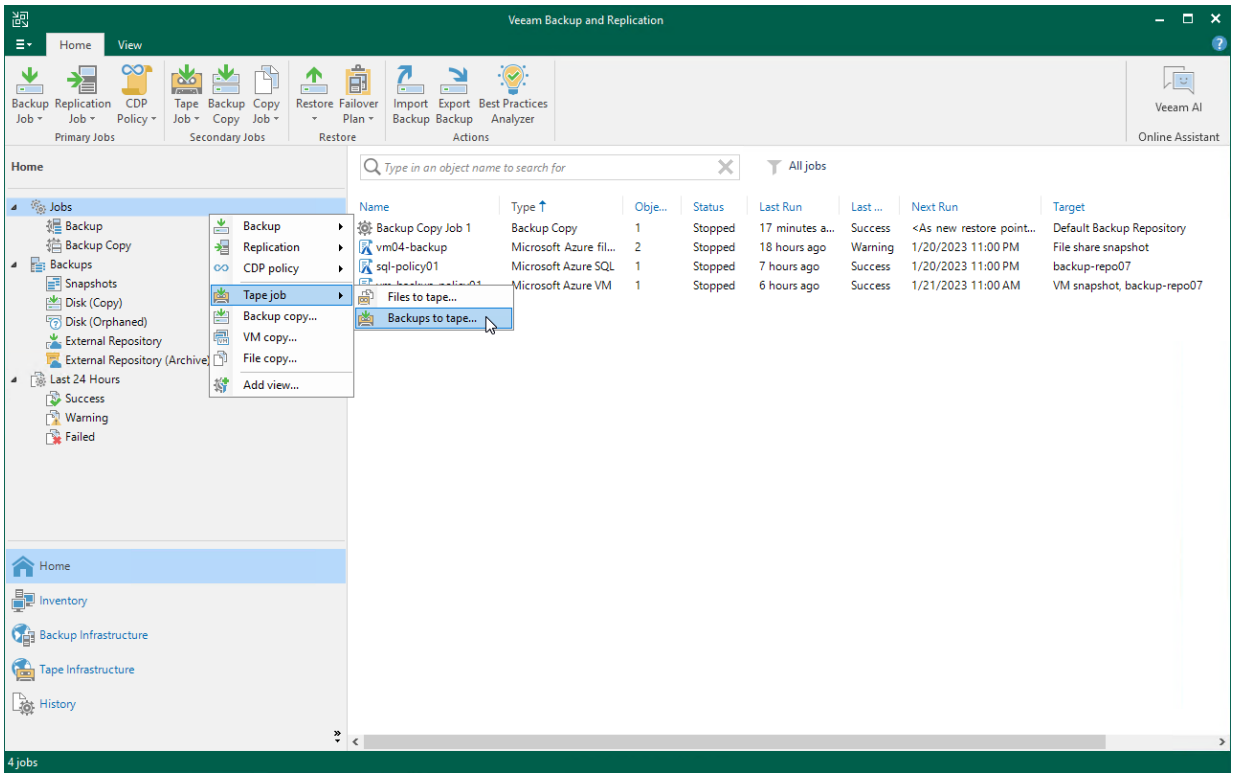
# Copying Backups to Tapes

Veeam Backup & Replication allows you to automate copying of image-level backups of Azure VMs to tape devices and lets you specify scheduling, archiving and media automation options. For more information on the supported tape libraries, see the Veeam Backup & Replication User Guide, section Tape Devices Support.

Before you start copying backup to tapes:

- Copy Azure VM backups to on-premises backup repositories. To learn how to copy backups, see the instructions provided in Creating Backup Copy Jobs.
- Connect tape devices to Veeam Backup & Replication as described in the Veeam Backup & Replication User Guide, section Tape Devices Deployment.
- Configure the tape infrastructure as described in the Veeam Backup & Replication User Guide, section Getting Started with Tapes (steps 1-3).

To copy Azure VM backups to tapes, create a backup to tape job as described in the Veeam Backup & Replication User Guide, section Creating Backup to Tape Jobs.



# Performing Backup Using Web UI

Veeam Backup for Microsoft Azure runs backup policies for every data protection operation. A backup policy is a collection of settings that define the way backup operations are performed: what data to back up, where to store backups, when to start the backup process, and so on.

One backup policy can be used to process multiple resources within different regions, but you can back up each resource with one backup policy at a time. For example, if an instance is added to more than one backup policy, it will be processed only by a backup policy that has the highest priority. For information on how to set a priority for a backup policy, see section Setting Backup Policy Priority. Other backup policies will skip this instance from processing.

# Performing VM Backup

One backup policy can be used to process one or more Azure VMs within one Microsoft Entra tenant. The scope of data that you can protect in a tenant is limited by permissions of a service account that is specified in the backup policy settings.

Before you create an Azure VM backup policy, keep in mind the following considerations:

- If you plan to create image-level backups of Azure VMs, backup infrastructure components that will take part in the backup process must be added to the backup infrastructure and configured properly. These include backup repositories and worker instances.
- If you plan to receive email notifications on backup policy results, configure email notification settings first. For more information, see Configuring Global Notification Settings.
- Configure policy templates that will be used by SLA-based backup policies. For more information, see Managing SLA and Storage Templates.

To schedule data protection tasks to run automatically, create backup policies. For each protected Azure file share, you can also take a cloud-native snapshot manually when needed.

## Creating Schedule-Based VM Backup Policies

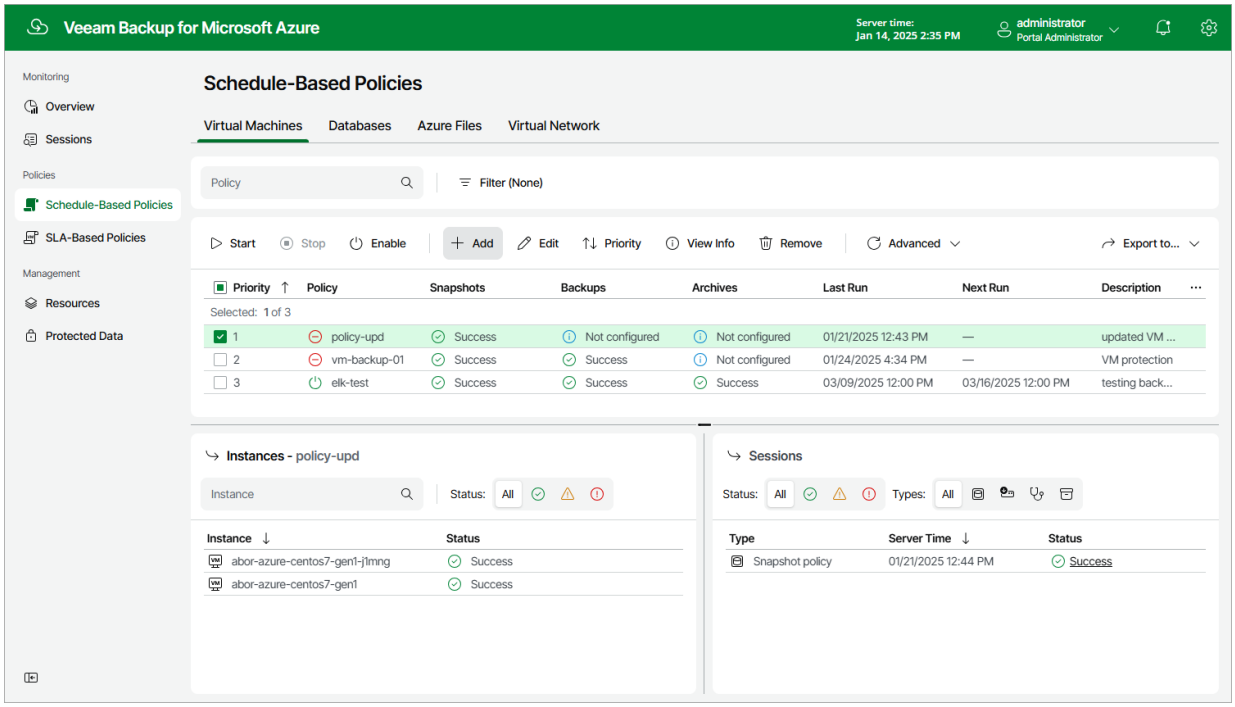
To create a schedule-based backup policy, do the following:

1. Launch the Add VM Policy wizard.
2. Specify a backup policy name and description.
3. Configure backup source settings.
4. Configure guest processing options.
5. Configure backup target settings.
6. Create a schedule for the backup policy.
7. Specify automatic retry, health check and notification settings for the backup policy.
8. Review the estimated cost of protecting the selected Azure VMs.
9. Finish working with the wizard.

# Step 1. Launch Add VM Policy Wizard

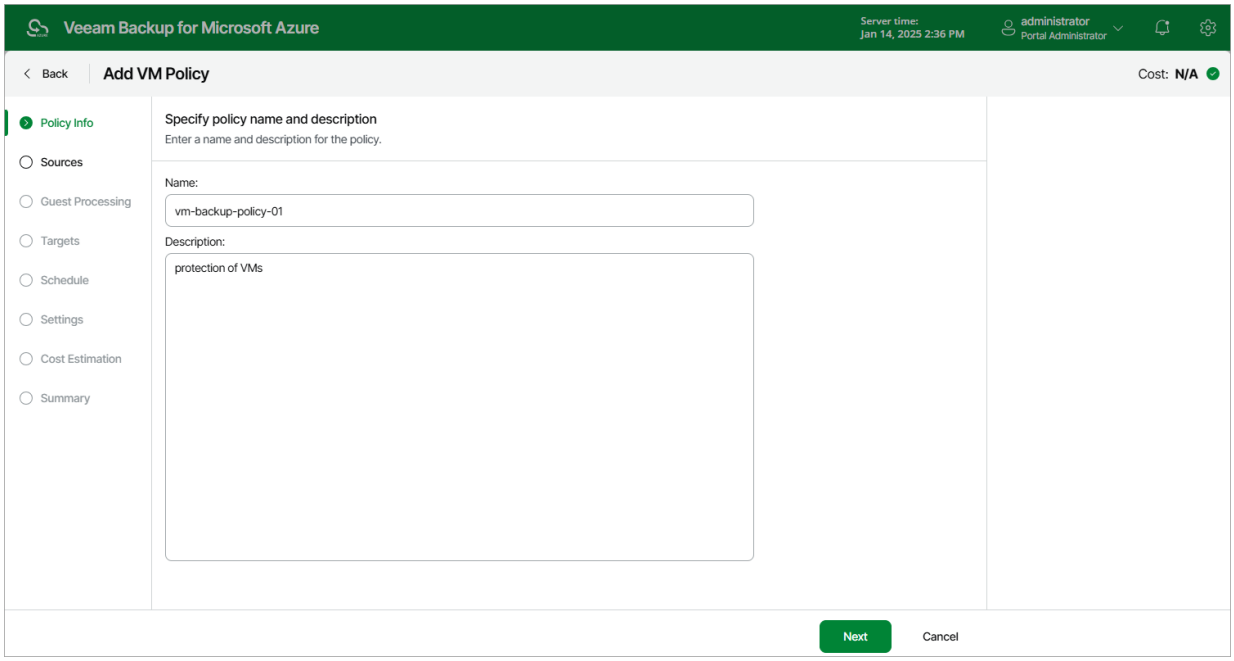
To launch the **Add VM Policy** wizard, do the following:

1. Navigate to **Schedule-Based Policies**.
2. Switch to **Virtual Machines**.
3. Click **Add**.



# Step 2. Specify Backup Policy Name

At the **Policy Info** step of the wizard, use the **Name** and **Description** fields to enter a name for the new backup policy and to provide a description for future reference. The maximum length of the name is 255 characters. The following characters are not supported: / \ " ' : | < > + = ; , ? ! * % # ^ @ & $ .



## Step 3. Configure Backup Source Settings

At the **Sources** step of the wizard, specify the following backup source settings:

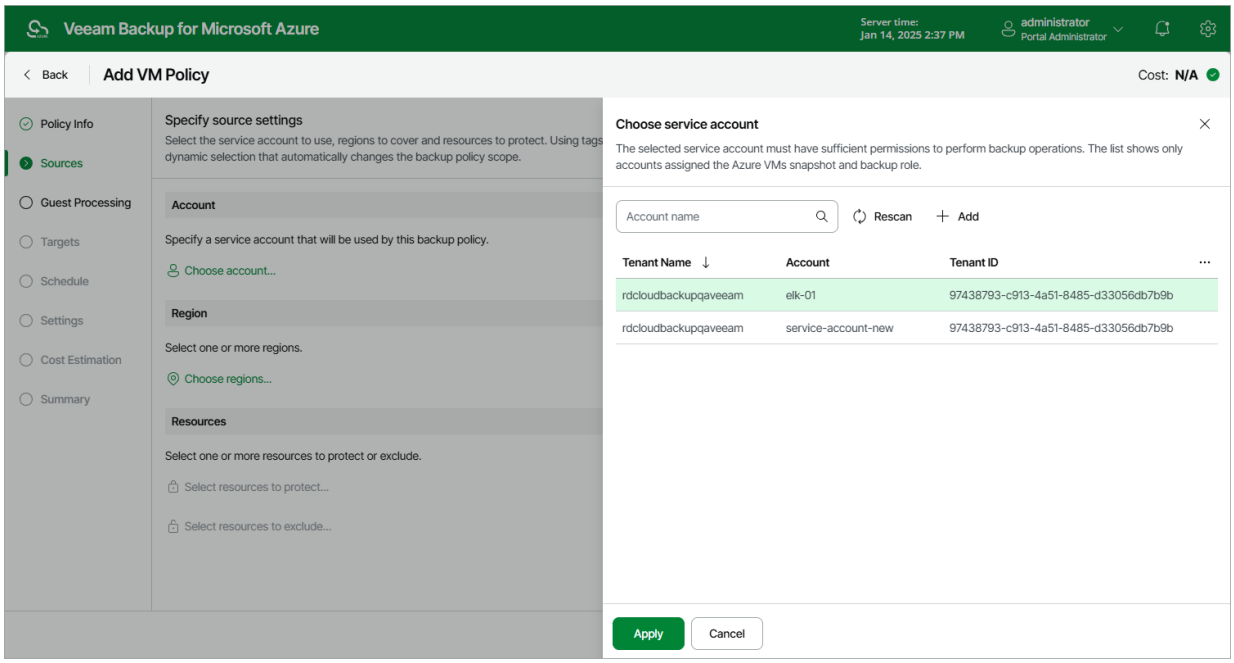
1. Select a service account whose permissions will be used to perform Azure VM backup.
2. Choose regions where Azure VMs that you want to back up reside.
3. Select resources to back up.

## Step 3a. Select Service Account

In the **Account** section of the **Sources** step of the wizard, specify a service account whose permissions will be used to access Azure services and resources, and to create cloud-native snapshots of Azure VMs.

1. Click **Choose account**.
2. In the **Choose service account** window, select the necessary service account from the available accounts list. The specified service account must belong to the Microsoft Entra tenant that contains the Azure VMs that you want to protect, and must be assigned permissions listed in section Azure VM Permissions.

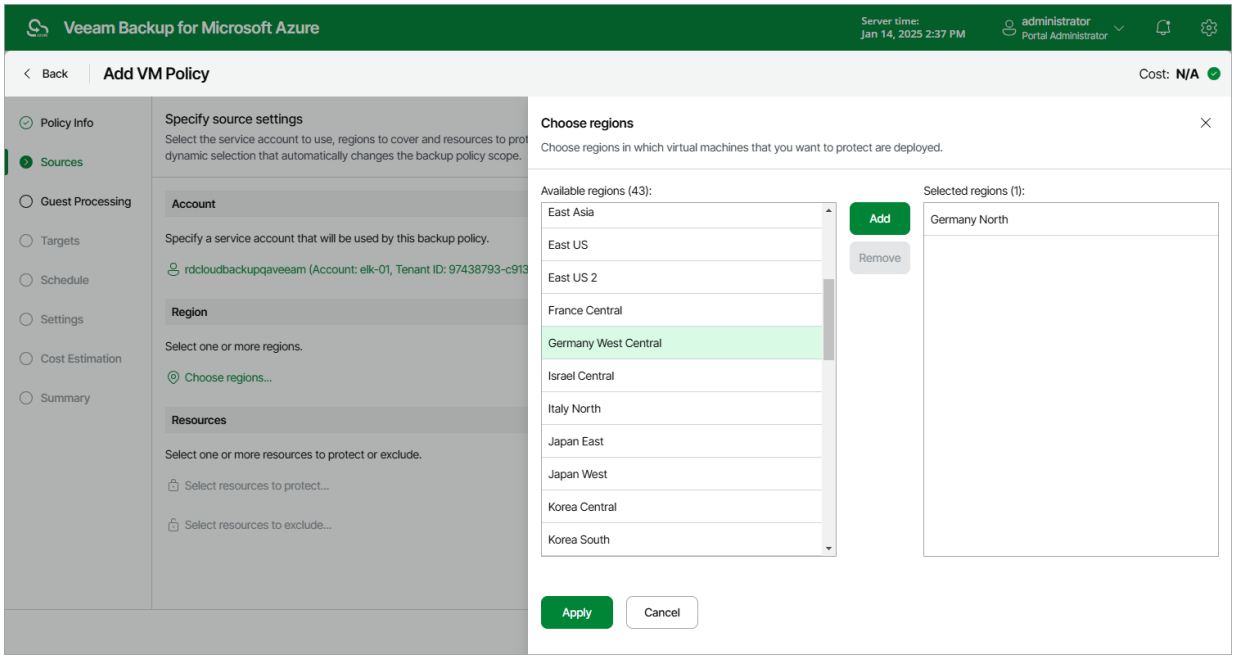
   For a service account to be displayed in the list of available accounts, it must be added to Veeam Backup for Microsoft Azure and assigned the *Azure VMs Snapshot and Backup* operational role as described in section Adding Service Accounts. If you have not added the necessary service account to Veeam Backup for Microsoft Azure beforehand, you can do it without closing the **Add VM Policy** wizard. To do that, click **Add** and complete the **Add Account** wizard.
3. To save changes made to the backup policy settings, click **Apply**.



## Step 3b. Select Regions

In the **Region** section of the **Sources** step of the wizard, select regions where Azure resources that you want to back up reside:

1. Click **Choose regions**.
2. In the **Choose regions** window, select the necessary regions from the **Available regions** list, and then click **Add**.
3. To save changes made to the backup policy settings, click **Apply**.



## Step 3c. Select Resources

In the **Resources** section of the **Sources** step of the wizard, specify the backup scope — select resources that Veeam Backup for Microsoft Azure will back up:

1. Click **Select resources to protect**.
2. In the **Choose resource protection options** window, choose whether you want to back up all Azure resources from the regions selected at step 3b, or only specific resources.

   If you select the **All resources** option, Veeam Backup for Microsoft Azure will regularly check for new Azure VMs launched in the selected regions and automatically update the backup policy settings to include these VMs in the backup scope.

   If you select the **Protect the following resources** option, you must also specify the resources explicitly:

   a. Use the **Resource type** drop-down list to select either of the following options:

      - *Subscription* — to back up Azure VMs managed by specific subscriptions.
      - *Resource group* — to back up Azure VMs that belong to specific resource groups.
      - *Tag* — to back up Azure VMs that have specific tags assigned.
      - *Virtual machine* — to back up only specific Azure VMs.

   b. Use the search field to the right of the **Resource type** list to find the necessary resource, and then click **Protect** to add the resource to the backup scope.

      For a resource to be displayed in the list of available resources, it must reside in an Azure region that has ever been specified in any backup policy. Otherwise, the only option to discover available resources is to click **Browse to select specific source from the global list** and wait for Veeam Backup for Microsoft Azure to populate the resource list.

      Note that your web browser zoom must not exceed 135% for the list of protected resources to be displayed correctly.

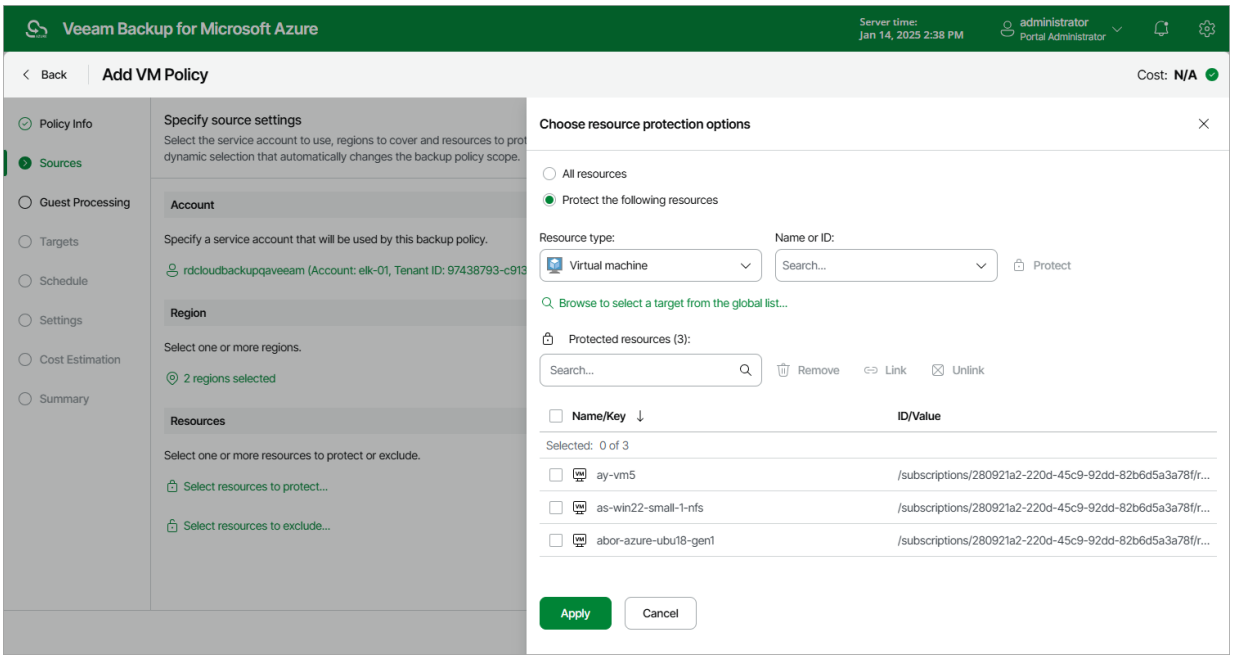
> **TIP**
>
> You can simultaneously add multiple resources to the backup scope. To do that, click **Browse to select specific source from the global list**, select check boxes next to the necessary items in the list of available resources, and then click **Protect**.
>
> If the list does not show the resources that you want to back up, click **Rescan** to launch the data collection process — as soon as the process is over, Veeam Backup for Microsoft Azure will update the resource list. If you still cannot find the necessary resources in the list, make sure that the *Microsoft.ManagedServices* provider is registered in the subscription to which the resources belong, return to step 3a and click **Rescan** in the **Choose service account** window. To learn how to register a resource provider, see Microsoft Docs.

   If you add a tag to the backup scope, Veeam Backup for Microsoft Azure will regularly check for new Azure VMs assigned the added tag and automatically update the backup policy settings to include these VMs in the scope. However, this applies only to Azure VMs from the regions selected at step 3b. If you select a tag assigned to Azure VMs from other regions, these VMs will not be protected by the backup policy. To work around the issue, either go back to step 3b and add the missing regions, or create a new backup policy.

4. To save changes made to the backup policy settings, click **Apply**.

> **TIP**
>
> As an alternative to selecting the **Protect the following resources** option and specifying the resources explicitly, you can select the **All resources** option and exclude a number of resources from the backup scope. To do that, click **Select resources to exclude** and specify Azure VMs or tags that you want to exclude from the backup scope — the procedure is the same as described for including resources in the backup scope.
>
> Consider that if a resource appears both in the list of included and excluded resources, Veeam Backup for Microsoft Azure will still not process the resource because the list of excluded resources has a higher priority.

When you add subscriptions, resource groups and tags to the backup scope, Veeam Backup for Microsoft Azure links all these resources using the OR operator. To instruct Veeam Backup for Microsoft Azure to use the AND operator, follow the instructions provided in section Configuring Conditions.




## Configuring Conditions

By default, Veeam Backup for Microsoft Azure uses the OR operator to link all the subscriptions, resource groups and tags that you include into the backup scope — meaning that all the related VMs will be protected by the policy. To narrow down the backup scope, you can configure conditions that will allow Veeam Backup for Microsoft Azure to link the selected resources using the AND operator.

When you configure a condition, Veeam Backup for Microsoft Azure composes a list of VMs to protect based on the resources that you add to this condition — meaning that an Azure VM will be protected by the policy only if this VM relates to all the linked resources. Keep in mind that one condition can link either multiple tags, a subscription with one or more tags, or a resource group with one or more tags.

To configure a condition, do the following in the **Resources** section of the **Sources** step of the wizard:

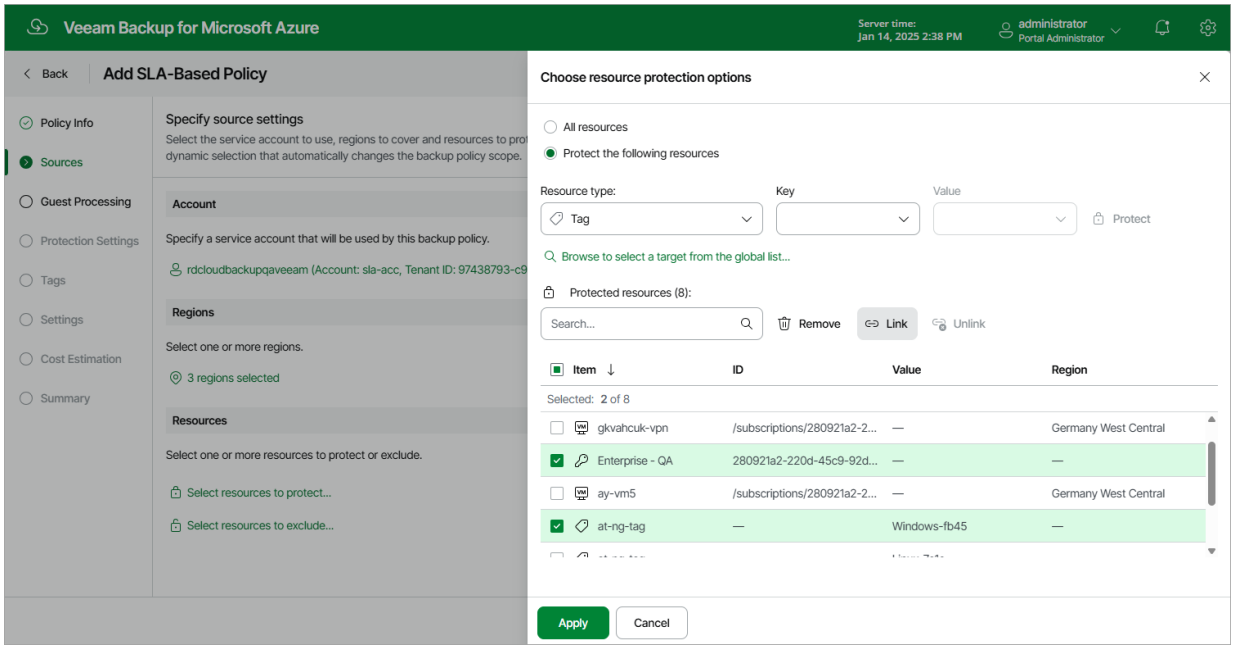
1. Click **Select resources to protect**.
2. In the **Choose resource protection options** window, select check boxes next to the items you want to include into the condition and click **Link**.

3. In the **Create Condition** window, provide a name for the condition and click **Apply**.

   The maximum length of the name is 64 characters.

When configuring conditions, you can add the same resource to the list of protected resources multiple times. For example, if you want to protect VMs that are managed by the *dept-01-sweden* subscription and that have either the *Veeam-01* tag or *Veeam-02* tag assigned (but not both tags at the same time), you must add this subscription to the list of protected resources twice and then configure 2 separate conditions: one condition will link the subscription with the *Veeam-01* tag, while another condition will link the subscription with the *Veeam-02* tag.

> **TIP**
>
> After you configure a condition, you will be able to modify the list of resources included into this condition, unlink all the resources, and remove the condition if you no longer need it. When performing these actions, keep in mind that:
>
> - If you exclude a resource from the condition, Veeam Backup for Microsoft Azure will re-add it to the list of protected resources as a single item.
> - If you unlink the condition, Veeam Backup for Microsoft Azure will re-add all resources that were included into this condition to the list of protected resources as single items, and will link these resources using the OR operator.
> - If you remove the condition, Veeam Backup for Microsoft Azure will remove all resources that were included into this condition from the backup scope.



## Step 4. Specify Guest Processing Settings

If you want to back up Azure VMs that are currently running, you can configure guest processing settings at the **Guest Processing** step of the wizard. These settings allow you to specify what actions Veeam Backup for Microsoft Azure will perform when communicating with the guest OSes.

Particularly, you can specify the following guest processing settings:

- Application-aware processing. For Windows-based Azure VMs running VSS-aware applications, you can enable application-aware processing to ensure that the applications will be able to recover successfully, without data loss.

  Application-aware processing is the Veeam technology based on Microsoft VSS. This option can be applied only to the Windows-based Azure VMs that support Microsoft VSS. For more information on Microsoft VSS, see Microsoft Docs.

- Guest scripting. You can instruct Veeam Backup for Microsoft Azure to run custom scripts on the processed Azure VM before and after the backup operation. For example, Veeam Backup for Microsoft Azure can execute a pre-snapshot script on the VM to quiesce these applications. This will allow Veeam Backup for Microsoft Azure to create a transactionally consistent snapshot while no write operations occur on the virtual disks. After the snapshot is created, a post-snapshot script can start the applications again.

# Limitations and Requirements

When creating transactionally consistent backups, Veeam Backup for Microsoft Azure uses the Azure Queue Storage service to stop and start applications running on the processed Windows-based Azure VMs. To ensure proper communication of the backup appliance and the guest OSes, all Windows-based Azure VMs for which you plan to enable guest processing must have the **443** network port opened.

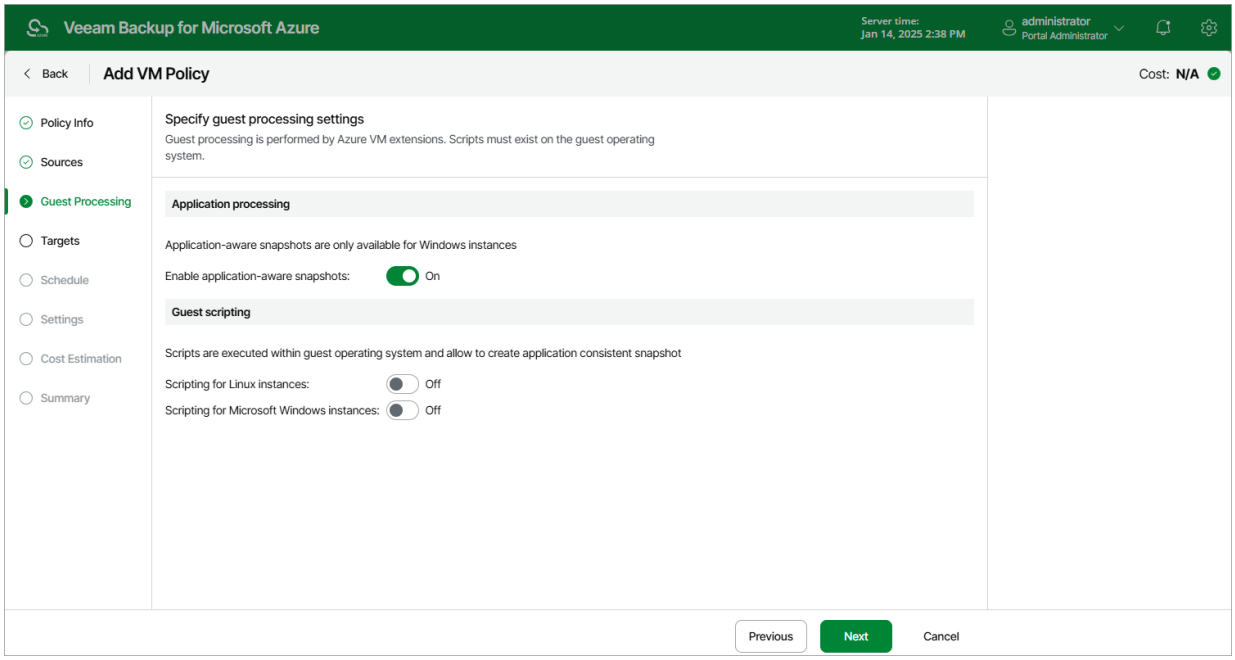
In case firewall rules configured for the Azure VMs do not allow outbound access using the **443** port, you must allow HTTPS traffic over **443** port for `<FQDN>.blob.core.windows.net` and `<FQDN>.queue.core.windows.net`, where *<FQDN>* is the name of the storage account used by the Veeam backup service.

## Enabling Application-Aware Processing

To enable application-aware processing, in the **Application Processing** section of the **Guest Processing** step of the wizard, set the **Enable application aware snapshots** toggle to *On*.

**IMPORTANT**

While creating application-aware snapshots, VSS Guest Agent uses the VSS Copy Backup type to create snapshots of the processed Azure VMs during the backup policy session. This type of VSS backup does not support truncation of transaction log. For more information on VSS Backup types, see Microsoft Docs.




# Limitation and Considerations

To enable application-aware processing, VSS agents must be installed on source Azure VMs. To install VSS agents, Veeam Backup for Microsoft Azure runs a specific PowerShell script on the source Azure VMs. That is why if you use PowerShell execution policies to control the conditions under which PowerShell loads configuration files and runs scripts on your source VMs, make sure that the **LocalMachine** scope is set to the *RemoteSigned* value. Otherwise, Veeam Backup for Microsoft Azure will not be able to run the script and application-aware processing will fail.

## Enabling Guest Scripting

To enable guest scripting, do the following at the **Guest Processing** step of the wizard:

- For Azure VMs running Linux OS, set the **Scripting for Linux instances** toggle to *On*.

  The **Specify scripting settings for Linux instances** window will open.

- For Azure VMs running Microsoft Windows OS, set the **Scripting for Microsoft Windows instances** toggle to *On*.

  The **Specify scripting settings for Windows instances** window will open.

**IMPORTANT**

When enabling guest scripting, consider the following:

- Veeam Backup for Microsoft Azure supports the EXE, BAT, CMD, WSF, JS, VBS and PS1 file formats for Windows-based Azure VMs, and the SH file format for Linux-based Azure VMs.
- To run custom scripts on Windows-based Azure VMs, Veeam Backup for Microsoft Azure uses the Run Command feature. For more information, see Microsoft Docs.

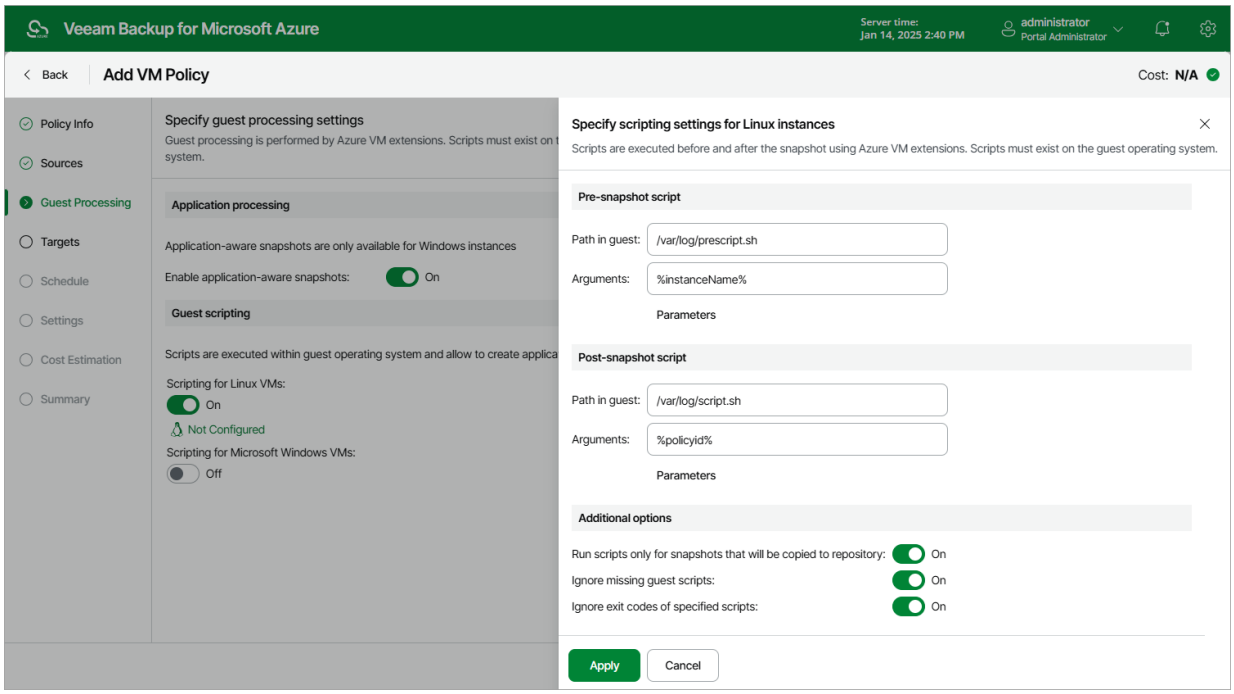
In the opened window, specify pre-snapshot and post-snapshot scripts that will be executed before and after the backup operation:

1. In the **Pre-snapshot script** section, do the following:
   a. In the **Path in guest** field, specify a path to the directory on an Azure VM where the pre-snapshot script file resides.
   b. In the **Arguments** field, specify additional arguments that will be passed to the script when the script is executed.

      You can use runtime variables as arguments for the script. To see the list of available variables, click **Parameters**.

> **IMPORTANT**
>
> Veeam Backup for Microsoft Azure will try to run a script residing in the specified directory for all Azure VMs added to the backup policy. If you want to execute different scripts for different Azure VMs, ensure that script files uploaded to these VMs have the same path and name.

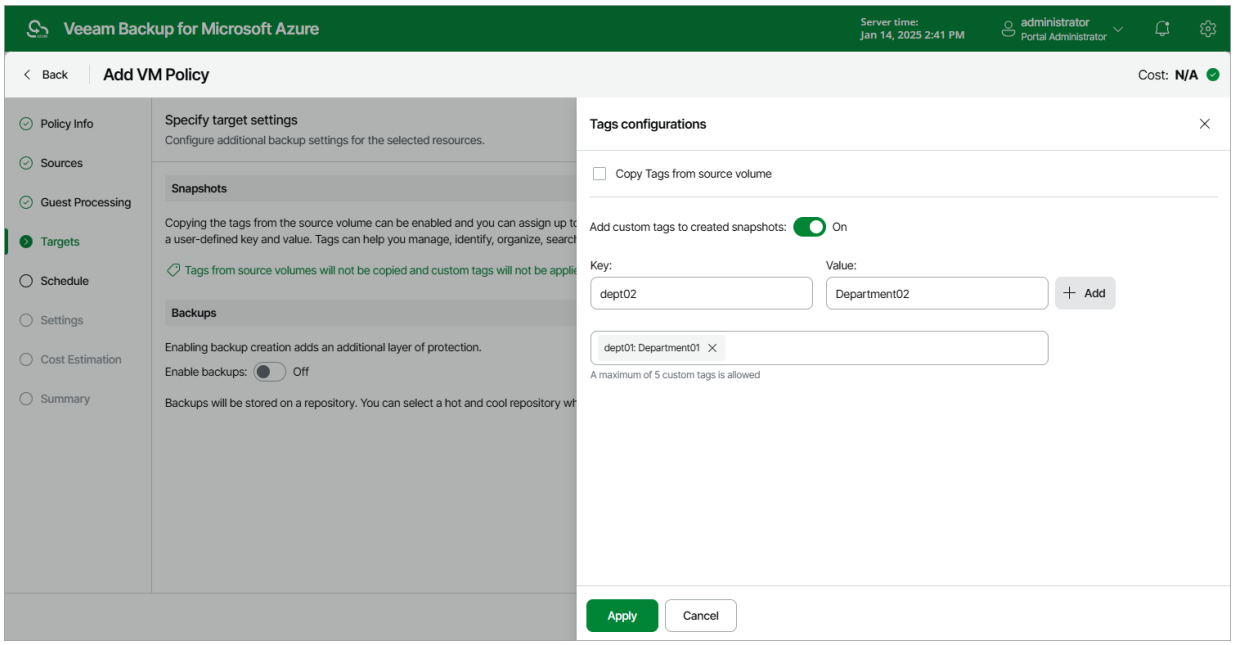
2. Repeat step 1 for the post-snapshot scripts in the **Post-snapshot script** section.
3. In the **Additional Options** section, choose whether you want to run scripts only while creating repository snapshots, to proceed with snapshot creation even though scripts are missing on some of the processed instances, and to ignore exit codes returned while executing the scripts.
4. Click **Apply**.



# Step 5. Configure Backup Target Settings

By default, backup policies create only cloud-native snapshots of processed Azure VMs. At the **Targets** step of the wizard, you can enable the following additional data protection scenarios:

- In the **Snapshot** section, you can assign tags to cloud-native snapshots of the selected Azure VMs:
  a. Click **Tags from source volumes will not be copied and custom tags will not be applied**.
  b. In the **Tags configurations** window, choose whether you want to assign tags to the created snapshots.
     - To assign already existing tags from the source virtual disks, select the **Copy Tags from source volume** check box.
     - To assign your own custom tags, set the **Add custom tags to created snapshots** toggle to *On*, and specify the tags explicitly. Click **Apply**. Note that you cannot add more than 5 custom tags.
- In the **Backups** section, set the **Enable backups** toggle to *On* to instruct Veeam Backup for Microsoft Azure to create image-level backups.



# Step 6. Specify Policy Scheduling Options

You can instruct Veeam Backup for Microsoft Azure to start the backup policy automatically according to a specific backup schedule. The backup schedule defines how often data of the Azure VMs added to the backup policy will be backed up.

To help you implement a comprehensive backup strategy, Veeam Backup for Microsoft Azure allows you to create schedules of the following types:

- Daily — the backup policy will create restore points repeatedly throughout a day on specific days.
- Weekly — the backup policy will create restore points once a day on specific days.
- Monthly — the backup policy will create restore points once a month on a specific day.
- Yearly — the backup policy will create restore points once a year on a specific day.

Combining multiple schedule types together allows you to retain restore points for longer periods of time — for more information, see Enabling Harmonized Scheduling. Combining multiple schedule types together also allows you to archive backups — for more information, see Enabling Backup Archiving.

## Specifying Daily Schedule

To create a daily schedule for the backup policy, at the **Schedule** step of the wizard, do the following:

1. Set the **Daily retention** toggle to *On* and click **Edit Daily Settings**.
2. In the **Daily schedule** window, select hours when the backup policy will create cloud-native snapshots and image-level backups. Use the **Run at** drop-down list to choose whether you want the backup policy to run every day, on weekdays (Monday through Friday) or on specific days.

   If you want to protect Azure VM data more frequently, you can instruct the backup policy to create multiple cloud-native snapshots per hour. To do that, click the link to the right of the **Snapshots** hour selection area, and specify the number of cloud-native snapshots that the backup policy will create within an hour.

> **NOTE**
>
> Consider the following:
>
> - Veeam Backup for Microsoft Azure does not create image-level backups independently from cloud-native snapshots. That is why when you select hours for image-level backups, the same hours are automatically selected for cloud-native snapshots. To learn how Veeam Backup for Microsoft Azure performs backup operations, see Protecting Azure VMs.
> - Since Veeam Backup for Microsoft Azure runs retention sessions at 12:15 AM according to the time zone set on the backup appliance, it is not recommended that you schedule backup policies to execute at 12:15 AM. Otherwise, Veeam Backup for Microsoft Azure will not be able to run the retention sessions.

3. In the **Daily retention** section, configure retention policy settings for the daily schedule:
   - For cloud-native snapshots, specify the number of restore points that you want to keep in a snapshot chain.

     If the restore point limit is exceeded, Veeam Backup for Microsoft Azure removes the earliest restore point from the chain. For more information, see VM Snapshot Retention.

**IMPORTANT**

To allow the CBT mechanism to be used when processing Azure VM data, you must keep at least one snapshot in the snapshot chain. However, by design, Veeam Backup for Microsoft Azure permanently retains 2 cloud-native snapshots in the chain due to the CBT mechanism limitations. To learn how the CBT mechanism works, see Changed Block Tracking.

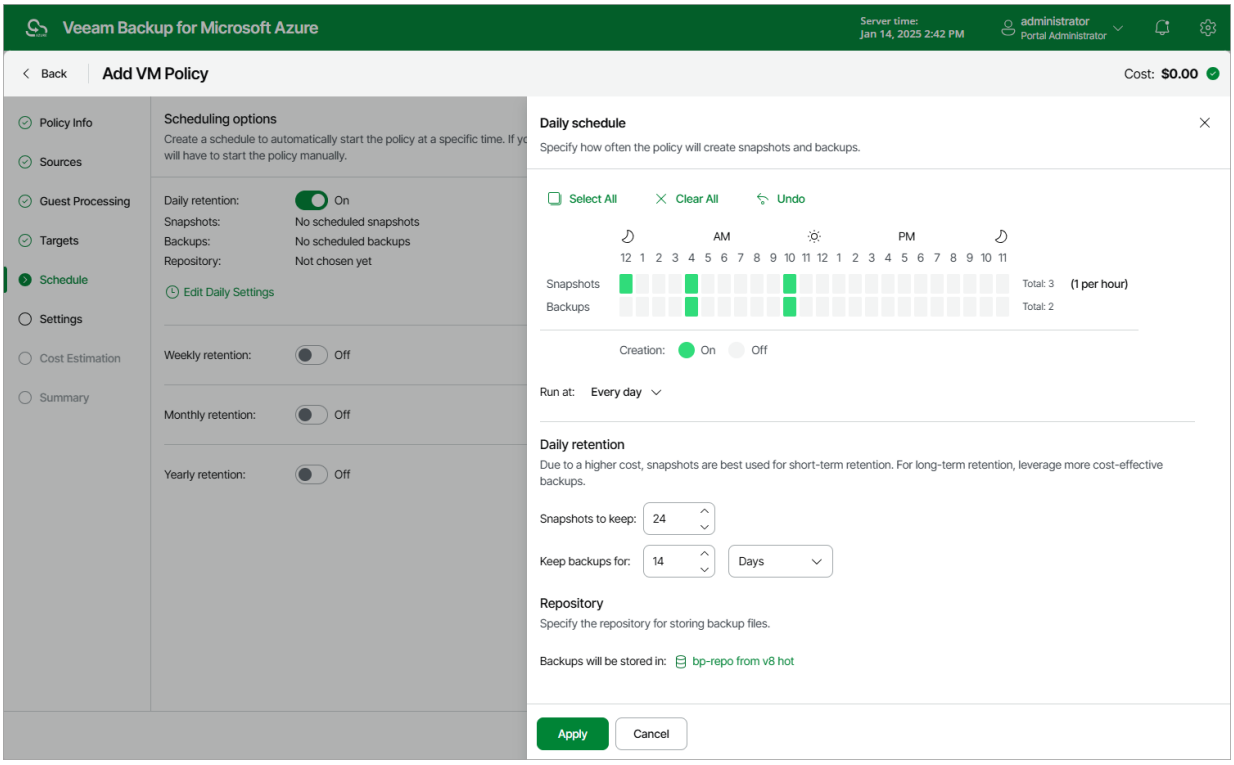
- For image-level backups, specify the number of days (or months) for which you want to keep restore points in a backup chain.

  If a restore point is older than the specified time limit, Veeam Backup for Microsoft Azure removes the restore point from the chain. For more information, see VM Backup Retention.

5. In the **Repository** section, select a backup repository where the created image-level backups will be stored.

   For a backup repository to be displayed in the **Repository** list, it must be added to Veeam Backup for Microsoft Azure as described in section Adding Backup Repositories.

6. To save changes made to the backup policy settings, click **Apply**.




## Specifying Weekly Schedule

To create a weekly schedule for the backup policy, at the **Schedule** step of the wizard, do the following:

1. Set the **Weekly retention** toggle to *On* and click **Edit Weekly Settings**.
2. In the **Weekly schedule** window, select days of the week when the backup policy will create cloud-native snapshots and image-level backups. Use the Create **restore points at** drop-down list to schedule a specific time for the backup policy to run.

NOTE

Veeam Backup for Microsoft Azure does not create image-level backups independently from cloud-native snapshots. That is why when you select days for image-level backups, the same days are automatically selected for cloud-native snapshots. To learn how Veeam Backup for Microsoft Azure performs backup operations, see Protecting Azure VMs.

4. In the **Weekly retention** section, configure retention policy settings for the weekly schedule:
   - For cloud-native snapshots, specify the number of restore points that you want to keep in a snapshot chain.

     If the restore point limit is exceeded, Veeam Backup for Microsoft Azure removes the earliest restore point from the chain. For more information, see VM Snapshot Retention.

IMPORTANT

To allow the CBT mechanism to be used when processing Azure VM data, you must keep at least one snapshot in the snapshot chain. However, by design, Veeam Backup for Microsoft Azure permanently retains 2 cloud-native snapshots in the chain due to the CBT mechanism limitations. To learn how the CBT mechanism works, see Changed Block Tracking.

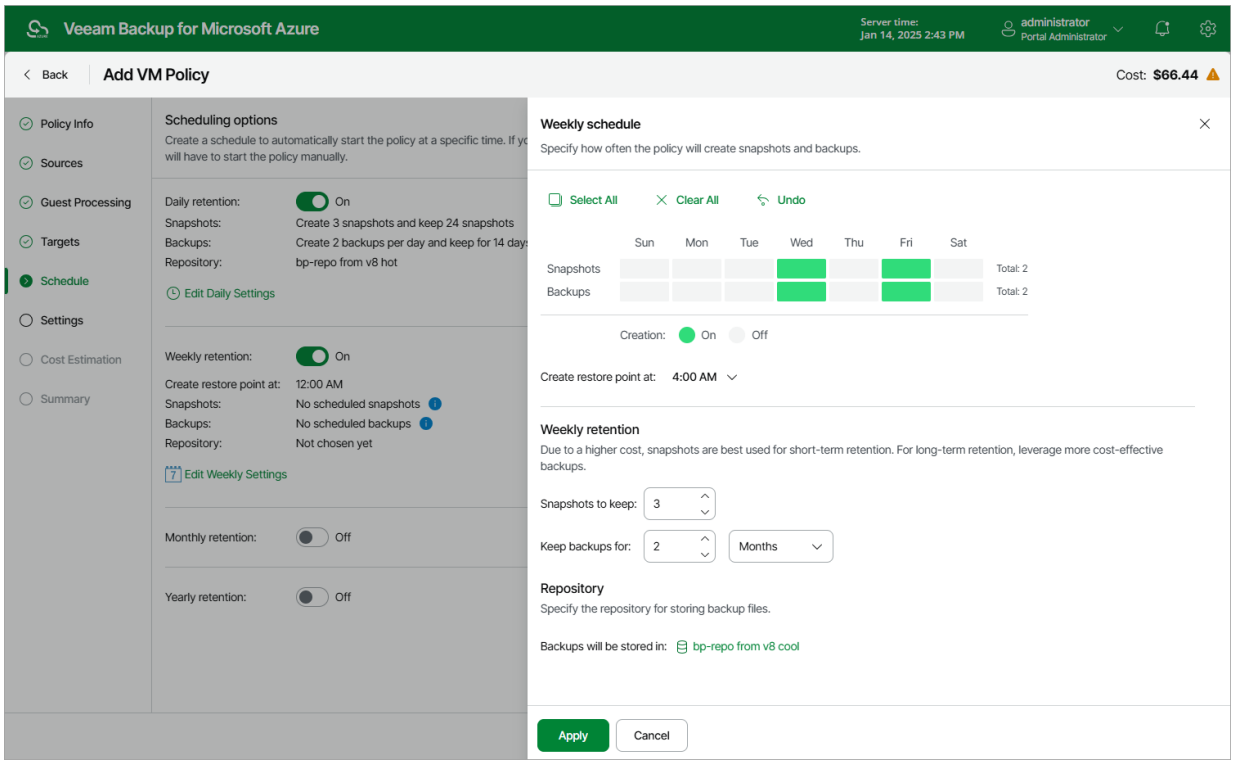
   - For image-level backups, specify the number of days (or months) for which you want to keep restore points in a backup chain.

     If a restore point is older than the specified time limit, Veeam Backup for Microsoft Azure removes the restore point from the chain. For more information, see VM Backup Retention.

5. In the **Repository** section, select a backup repository where the created image-level backups will be stored.

   For a backup repository to be displayed in the **Repository** list, it must be added to Veeam Backup for Microsoft Azure as described in section Adding Backup Repositories.

6. To save changes made to the backup policy settings, click **Apply**.




## Specifying Monthly Schedule

To create a monthly schedule for the backup policy, at the **Schedule** step of the wizard, do the following:

1. Set the **Monthly retention** toggle to *On* and click **Edit Monthly Settings**.
2. In the **Monthly schedule** window, select months when the backup policy will create cloud-native snapshots and image-level backups. Use the **Create restore points at** and **Run on** drop-down lists to schedule a specific time and day for the backup policy to run.

> **NOTE**
>
> Veeam Backup for Microsoft Azure does not create image-level backups independently from cloud-native snapshots. That is why when you select months for image-level backups, the same months are automatically selected for cloud-native snapshots. To learn how Veeam Backup for Microsoft Azure performs backup operations, see Protecting Azure VMs.

3. In the **Monthly retention** section, configure retention policy settings for the monthly schedule:
   - For cloud-native snapshots, specify the number of restore points that you want to keep in a snapshot chain.

     If the restore point limit is exceeded, Veeam Backup for Microsoft Azure removes the earliest restore point from the chain. For more information, see VM Snapshot Retention.

> **IMPORTANT**
>
> To allow the CBT mechanism to be used when processing Azure VM data, you must keep at least one snapshot in the snapshot chain. However, by design, Veeam Backup for Microsoft Azure permanently retains 2 cloud-native snapshots in the chain due to the CBT mechanism limitations. To learn how the CBT mechanism works, see Changed Block Tracking.

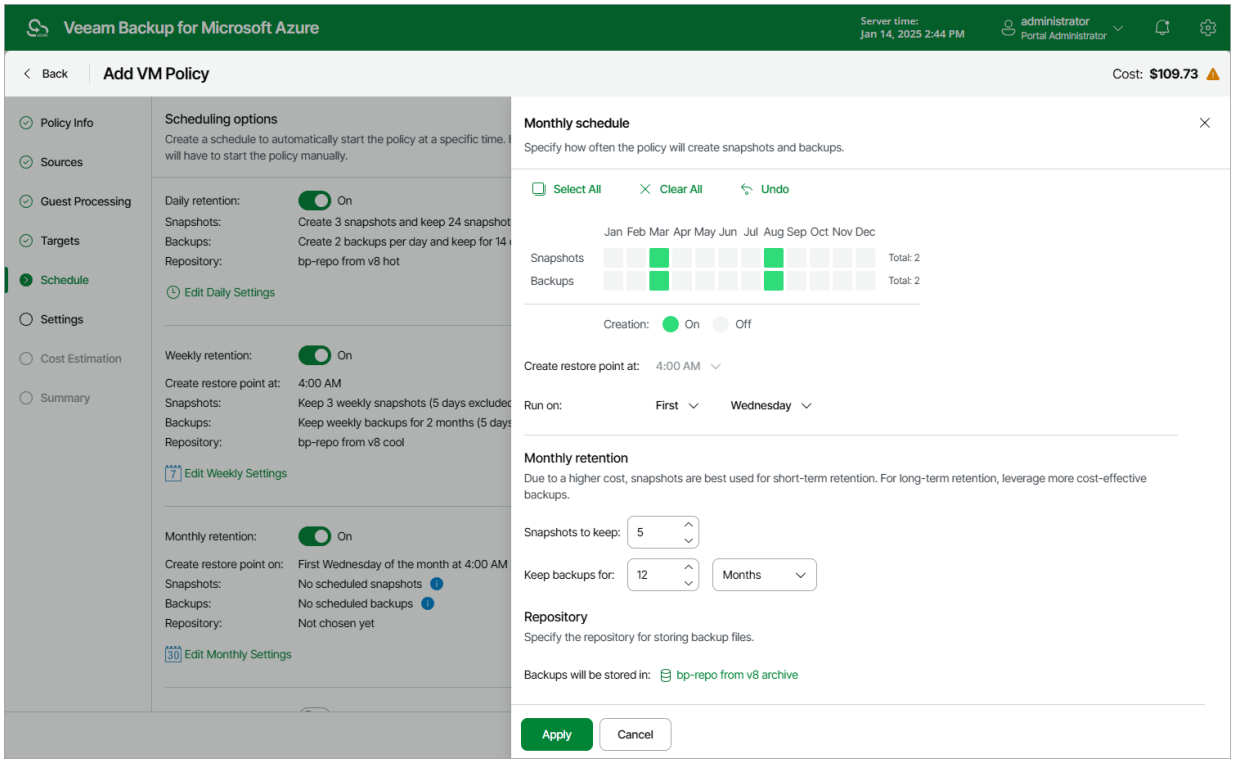
- For image-level backups, specify the number of days (or months) for which you want to keep restore points in a backup chain.

  If a restore point is older than the specified time limit, Veeam Backup for Microsoft Azure removes the restore point from the chain. For more information, see VM Backup Retention.

5. In the **Repository** section, select a backup repository where the created image-level backups will be stored.

   For a backup repository to be displayed in the **Repository** list, it must be added to Veeam Backup for Microsoft Azure as described in section Adding Backup Repositories.

6. To save changes made to the backup policy settings, click **Apply**.




## Specifying Yearly Schedule

[This step applies only if you have instructed Veeam Backup for Microsoft Azure to create image-level backups at the **Targets** step of the wizard]

To create a yearly schedule for the backup policy, at the **Schedule** step of the wizard, do the following:

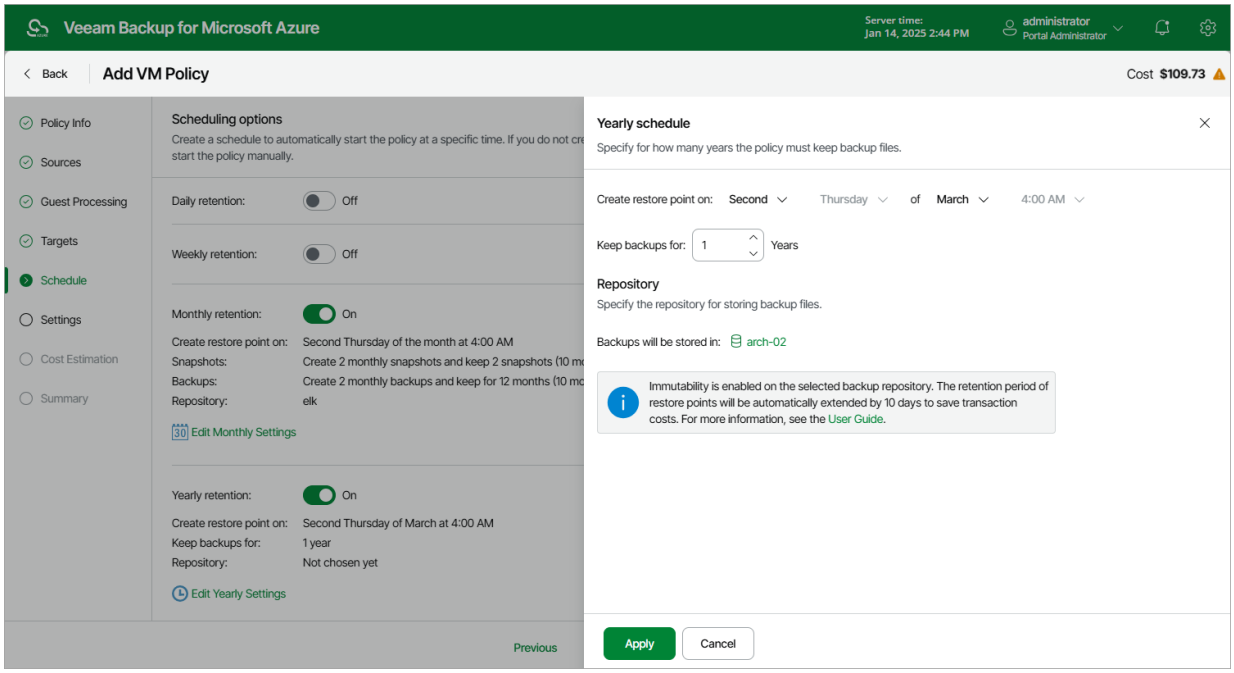
1. Set the **Yearly retention** toggle to *On* and click **Edit Yearly Settings**.
2. In the **Yearly schedule** window, specify a day, month and time when the backup policy will create image-level backups.
3. In the **Keep backups for** field, specify the number of years for which you want to keep restore points in a backup chain.

   If a restore point is older than the specified time limit, Veeam Backup for Microsoft Azure removes the restore point from the chain. For more information, see VM Backup Retention.

4. In the **Repository** section, select a backup repository where the created image-level backups will be stored.

   For a backup repository to be displayed in the **Repository** list, it must be added to Veeam Backup for Microsoft Azure as described in section Adding Backup Repositories.

5. To save changes made to the backup policy settings, click **Apply**.




## Enabling Harmonized Scheduling

When you combine multiple types of schedules, Veeam Backup for Microsoft Azure applies the harmonization mechanism that allows you to leverage restore points for long-term retentions instead of taking a new restore point every time. The mechanism simplifies the backup schedule, optimizes the backup performance and reduces the cost of storing restore points.

With harmonized scheduling, Veeam Backup for Microsoft Azure can keep restore points created according to a daily, weekly or monthly schedule for longer periods of time:

- Cloud-native snapshots can be kept for weeks and months.
- Image-level backups can be kept for weeks, months and years.

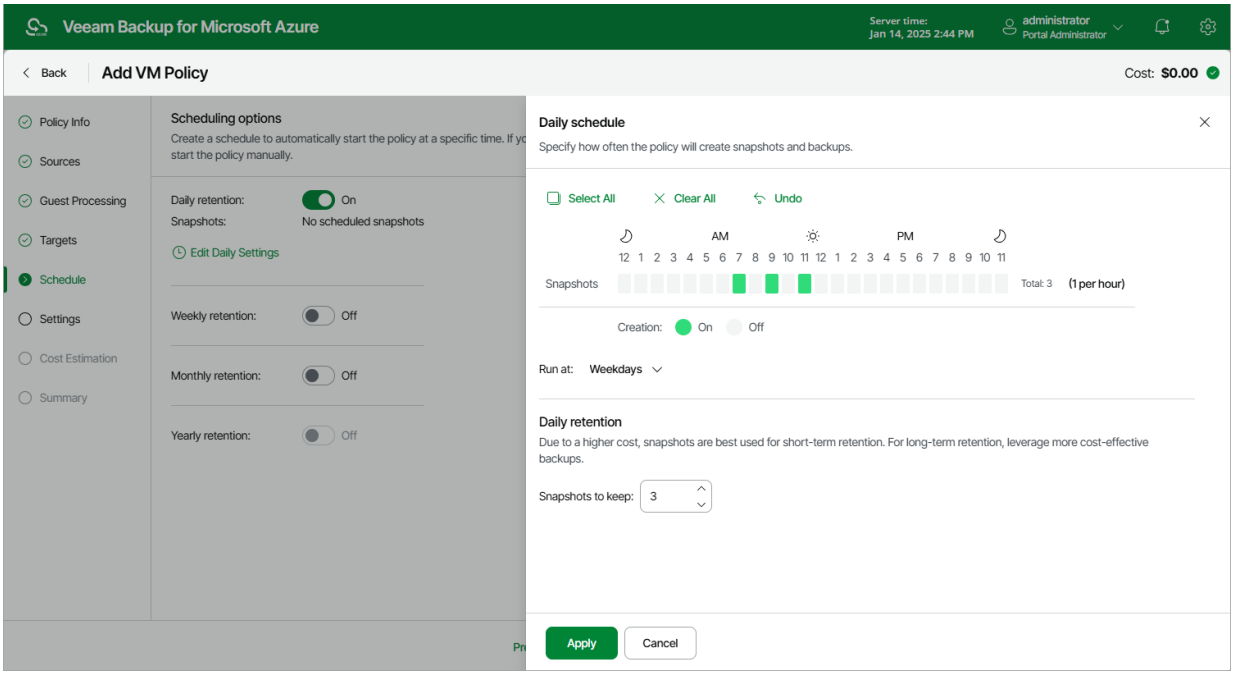
For Veeam Backup for Microsoft Azure to use the harmonization mechanism, there must be specified at least 2 different schedules: one schedule will control the regular creation of restore points, while another schedule will control the process of retaining restore points. In terms of harmonized scheduling, Veeam Backup for Microsoft Azure re-uses restore points created according to a more-frequent schedule (daily, weekly or monthly) to achieve the desired retention for less-frequent schedules (weekly, monthly and yearly). Each restore point is marked with a flag of the related schedule type: the (D) flag is used to mark restore points created daily, (W) — weekly, (M) — monthly, and (Y) — yearly. Veeam Backup for Microsoft Azure uses these flags to control the retention period for the created restore points. Once a flag of a less-frequent schedule is assigned to a restore point, this restore point can no longer be removed — it is kept for the period defined in the retention settings. When the specified retention period is over, the flag is unassigned from the restore point. If the restore point does not have any other flags assigned, it is removed according to the retention settings of a more-frequent schedule.

> **NOTE**
>
> Restore points created according to a more-frequent schedule and less-frequent schedules and stores in the same backup repository, compose a single backup or snapshot chain and uses the same backup repository. This means that regardless of flags assigned to restore points, Veeam Backup for Microsoft Azure adds the restore points to the chain as described in sections Backup Chain and Snapshot Chain.

Consider the following example. You want a backup policy to create cloud-native snapshots of your critical workloads 3 times a day, to keep 3 daily snapshots in the snapshot chain, and also to retain one of the created snapshots for 2 weeks. In this case, you create 2 schedules when configuring the backup policy settings — daily and weekly:

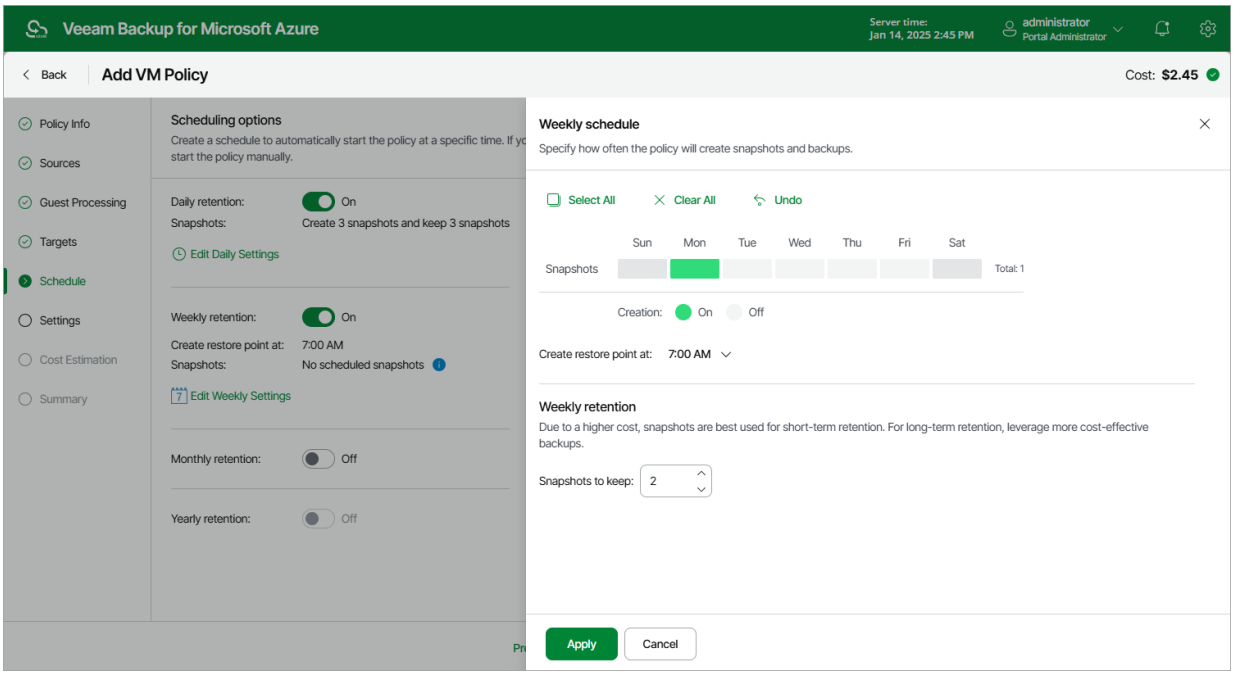
1. In the daily scheduling settings, you select hours and days when snapshots will be created (for example, *7:00 AM*, *9:00 AM*, and *11:00 AM*; *Weekdays*), and specify the number of daily restore points to retain (for example, *3*).

   Veeam Backup for Microsoft Azure will propagate these settings to the schedule with a lower frequency (which is the weekly schedule in our example).



2. In the weekly scheduling settings, you specify which one of the snapshots created by the daily schedule will be kept, and choose for how long you want to keep the selected snapshot.

   For example, if you want to keep the daily restore point created at 7:00 AM on Monday for 2 weeks, you select *7:00 AM*, *Monday* and specify *2* restore points to retain in the weekly schedule settings.

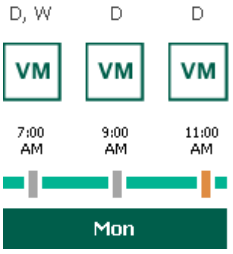



According to the specified scheduling settings, Veeam Backup for Microsoft Azure will create cloud-native snapshots in the following way:

1. On the first work day (Monday), a backup session will start at 7:00 AM to create the first restore point. The restore point will be marked with the (D) flag as it was created according to the daily schedule.

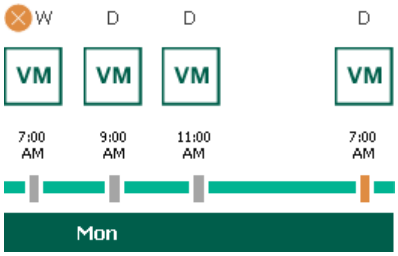
   Since *7:00 AM*, *Monday* is specified in the weekly scheduling settings, Veeam Backup for Microsoft Azure will assign the (W) flag to this restore point.

2. On the same day (Monday), after backup sessions run at 9:00 AM and 11:00 AM, the created restore points will be marked with the (D) flag.

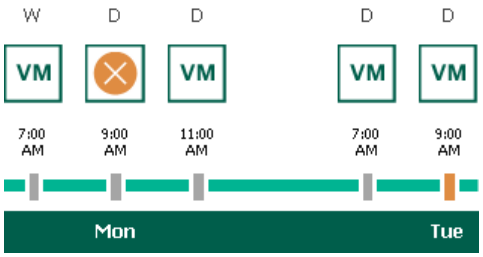


3. On the next work day (Tuesday), after a backup session runs at 7:00 AM, the created restore point will be marked with the (D) flag.

   At the moment the backup session completes, the number of restore points with the (D) flag will exceed the retention limit specified in the daily scheduling settings. However, Veeam Backup for Microsoft Azure will not remove the earliest restore point (*7:00 AM*, *Monday*) with the (D) flag from the snapshot chain as this restore point is also marked with a flag of a less-frequent schedule. Instead, Veeam Backup for Microsoft Azure will unassign the (D) flag from the restore point. This restore point will be kept for the retention period specified in the weekly scheduling settings (that is, for 2 weeks).

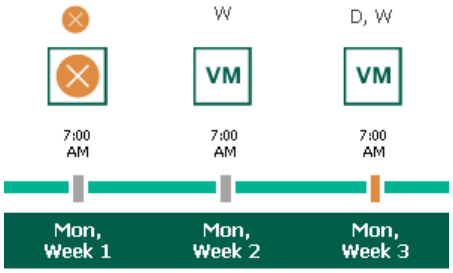



4. On the same day (Tuesday), after a backup session runs at 9:00 AM, the number of restore points with the (D) flag will exceed the retention limit once again. Veeam Backup for Microsoft Azure will remove from the snapshot chain the restore point created at 9:00 AM on Monday as no flags of a less-frequent schedule are assigned to this restore point.




5. Veeam Backup for Microsoft Azure will continue creating restore points for the next week in the same way as described in steps 1-4.

6. On week 3, after a backup session runs at 7:00 AM on Monday, the number of kept restore points will exceed the retention limit. Veeam Backup for Microsoft Azure will unassign the (W) flag from the earliest kept restore point. Since no other flags are assigned to this restore point, Veeam Backup for Microsoft Azure will remove this restore point from the snapshot chain.




## Enabling Backup Archiving

When you combine multiple types of schedules, you can enable the archiving mechanism to instruct Veeam Backup for Microsoft Azure to store backed-up data in the low-cost, long-term Archive access tier. The mechanism is the most useful in the following cases:

- Your data retention policy requires that you keep rarely accessed data in an archive.
- You want to reduce data-at-rest costs and to save space in the high-cost, short-term Hot and Cool access tiers.

> **NOTE**
>
> It is usually more expensive and takes more time to restore data from archived backups than from regular backups as it requires Veeam Backup for Microsoft Azure to retrieve the data from the Archive access tier. For more information, see Retrieving Data From Archive.

With backup archiving, Veeam Backup for Microsoft Azure can retain backups created according to a daily, weekly or monthly schedule for longer periods of time:

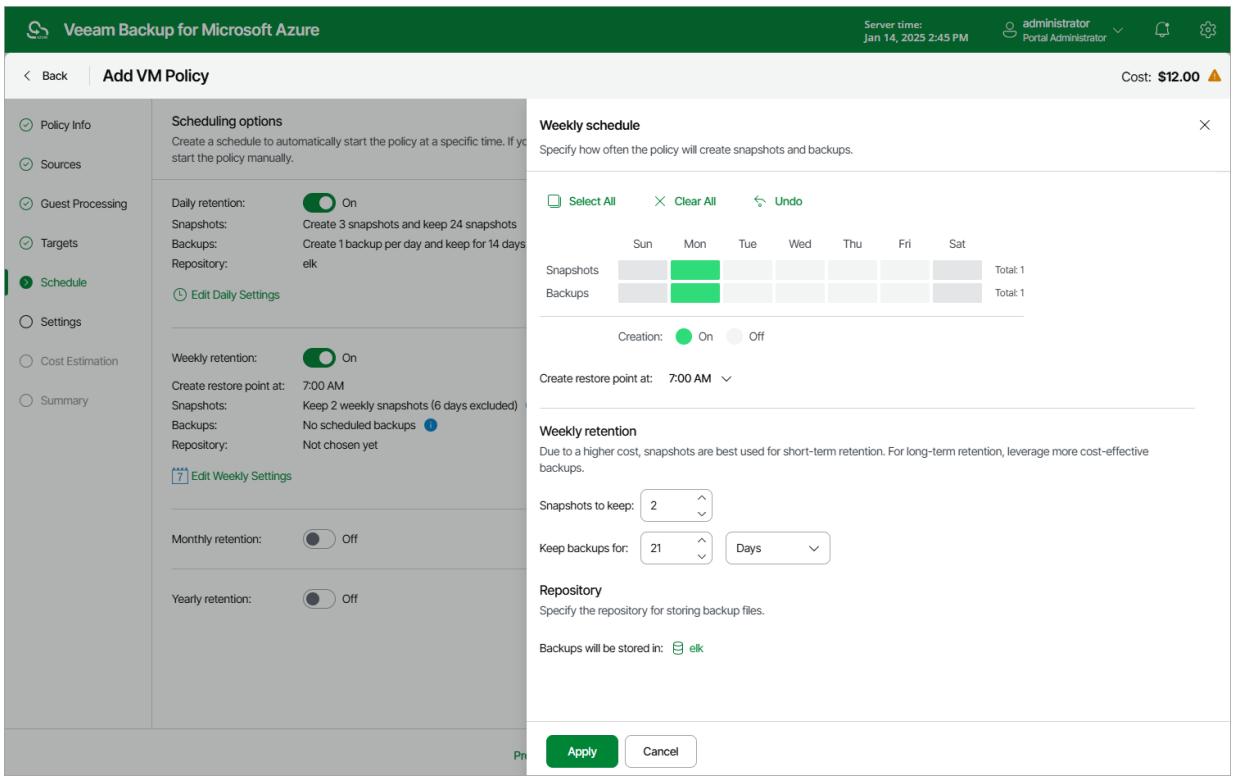
- To enable monthly archiving, you must configure a daily or a weekly schedule (or both).
- To enable yearly archiving, you must configure a daily, a weekly or a monthly schedule (or all three).

For Veeam Backup for Microsoft Azure to use the archiving mechanism, you must specify at least 2 different schedules: one schedule will control the regular creation of backups, while another schedule will control the process of copying backups to an archive repository. Backup chains created according to these two schedules will be completely different — for more information, see Backup Chain and Archive Backup Chain.

Consider the following example. You want a backup policy to create image-level backups of your critical workloads once a week, to keep the backed-up data in a backup repository for 3 weeks, and also to keep backups created once in 2 months in an archive repository for a year. In this case, you create 2 schedules when configuring the backup policy settings — weekly and monthly:

1. In the weekly scheduling settings, you do the following:
   a. Specify hours and days when backups will be created (for example, *7:00 AM, Monday*), and specify the number of days for which Veeam Backup for Microsoft Azure will retain backups (for example, *21 days*).
   b. Select a repository of the Hot or Cool access tier that will store regular backups.

   Veeam Backup for Microsoft Azure will propagate these settings to the archive schedule (which is the monthly schedule in our example).



2. In the monthly scheduling settings, you do the following:

   a. Specify when Veeam Backup for Microsoft Azure will create archive backups, and choose for how long you want to retain the created backups (for example, *January, March, May, July, September, November, 12 months* and *First Monday*).

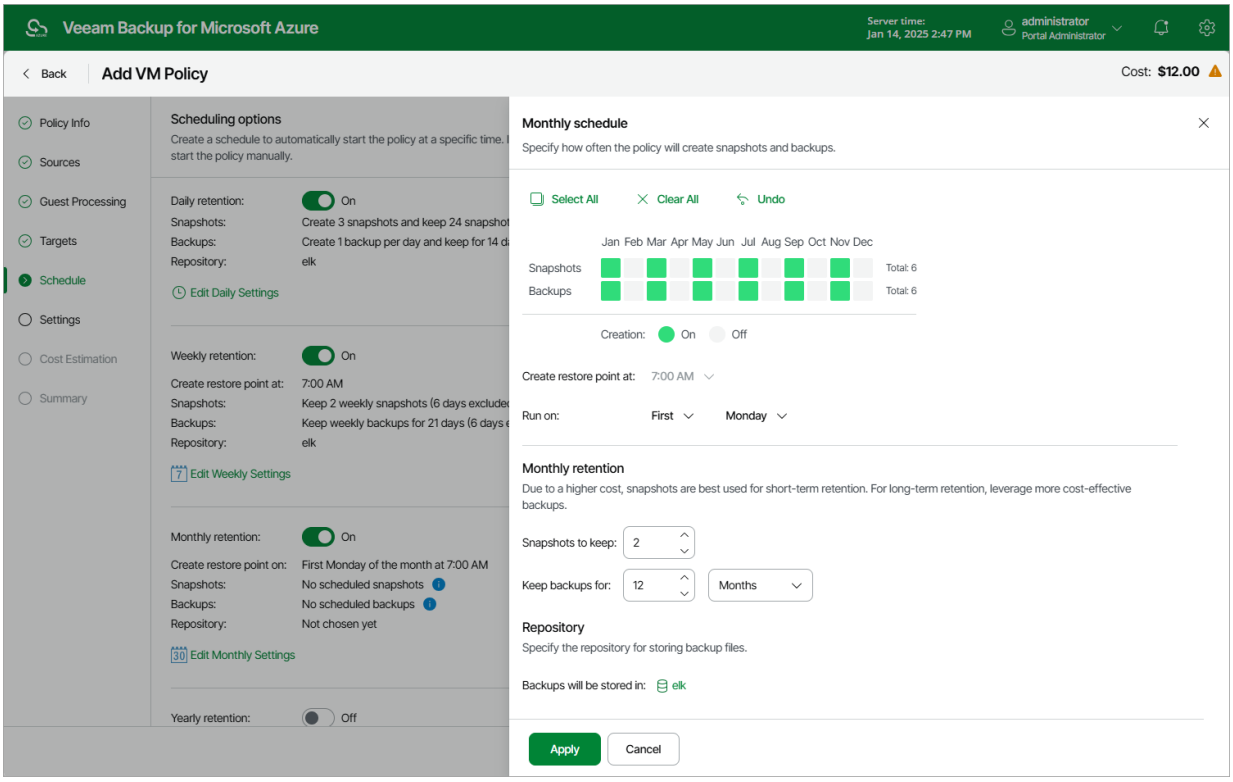
   b. Enable the archiving mechanism by selecting a repository of the Archive access tier that will store archive backups.

      Note that when you enable backup archiving, you become no longer able to create a schedule of the same frequency for regular backups. By design, these two functionalities are mutually exclusive.

**IMPORTANT**

If you enable backup archiving, consider the following:

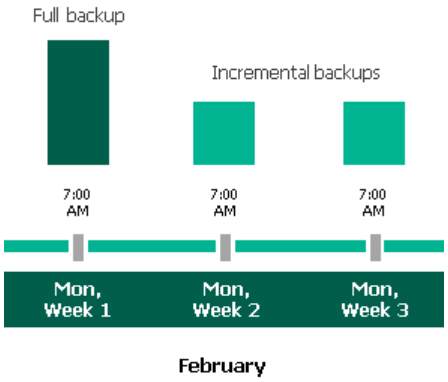
- It is recommended that you set the **Snapshots to keep** value to *0*, to reduce unexpected snapshot charges.
- It is recommended that you set the **Keep backups for** value to at least *6 months* (or *180 days*), since the minimum storage duration of the Archive access tier is 180 days.
- If you select the **On Day** option, harmonized scheduling cannot be guaranteed. Plus, to support the **On Day** option, Veeam Backup for Microsoft Azure will require to create an additional temporary restore point if there are no other schedules planned to run on that day. However, the temporary restore point will be removed during the *Backup Retention* process from Microsoft Azure Storage in approximately 24 hours, to reduce unexpected infrastructure charges.




According to the specified scheduling settings, Veeam Backup for Microsoft Azure will create image-level backups in the following way:

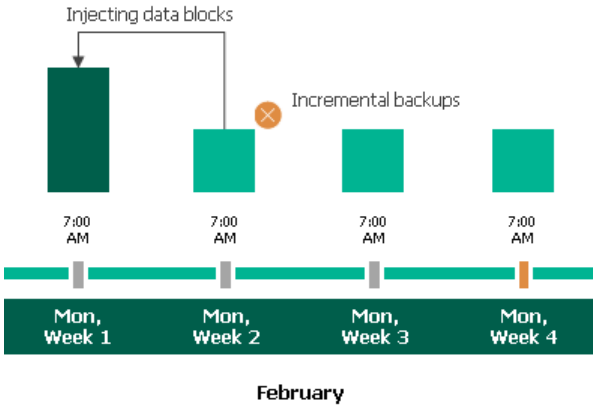
1. On the first Monday of February, a backup session will start at 7:00 AM to create the first restore point in the regular backup chain. Veeam Backup for Microsoft Azure will store this restore point as a full backup in the backup repository.

2. On the second and third Mondays of February, Veeam Backup for Microsoft Azure will create restore points at 7:00 AM and add them to the regular backup chain as incremental backups in the backup repository.



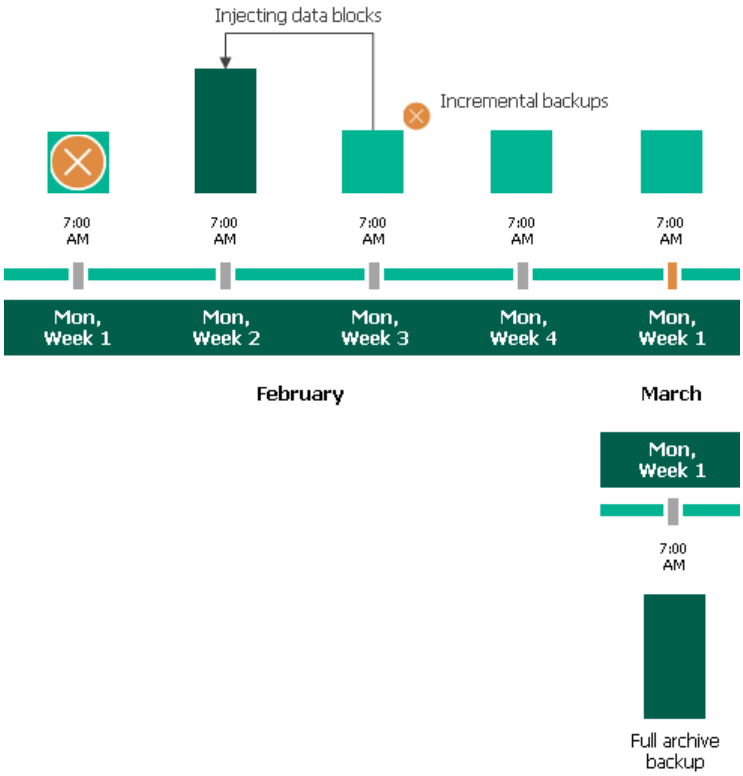

3. On the fourth Monday of February, Veeam Backup for Microsoft Azure will create a new restore point at 7:00 AM. By the moment the backup session completes, the earliest restore point in the regular backup chain will get older than the specified retention limit. That is why Veeam Backup for Microsoft Azure will rebuild the full backup and remove from the chain the restore point created on the first Monday.

   For more information on how Veeam Backup for Microsoft Azure transforms regular backup chains, see VM Backup Retention.



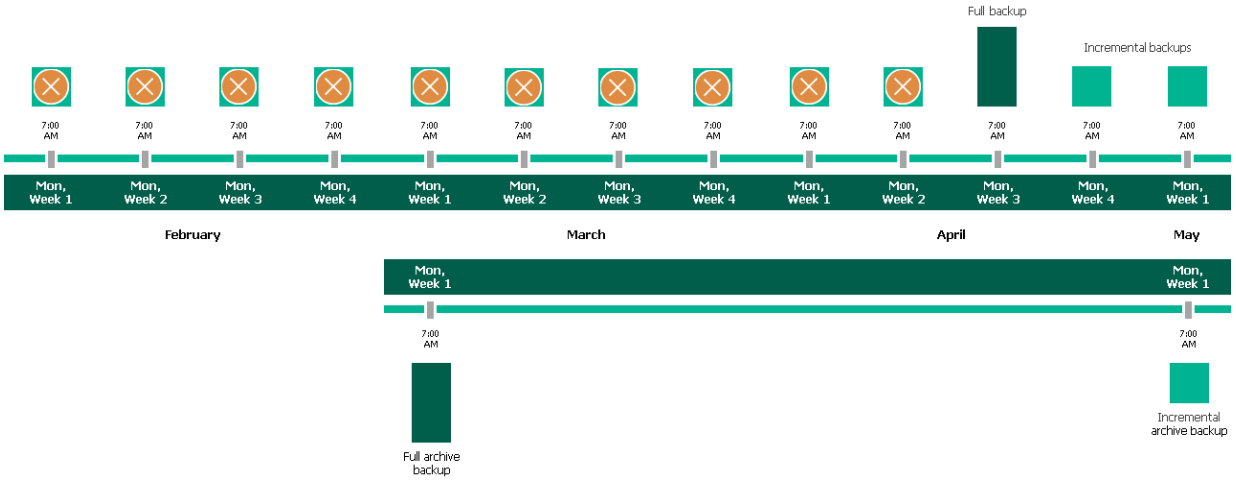
4. On the first Monday of March, a backup session will start at 7:00 AM to create another restore point in the regular backup chain. At the same time, the earliest restore point in the regular backup chain will get older than the specified retention limit again. That is why Veeam Backup for Microsoft Azure will rebuild the full backup again and remove from the chain the restore point created on the second Monday.

   After the backup session completes, an archive session will create a restore point with all data from the regular backup chain. Veeam Backup for Microsoft Azure will copy this restore point as a full archive backup to the archive repository.




5. Up to May, Veeam Backup for Microsoft Azure will continue adding new restore points to the regular backup chain and deleting outdated backups from the backup repository, according to the specified weekly scheduling settings.

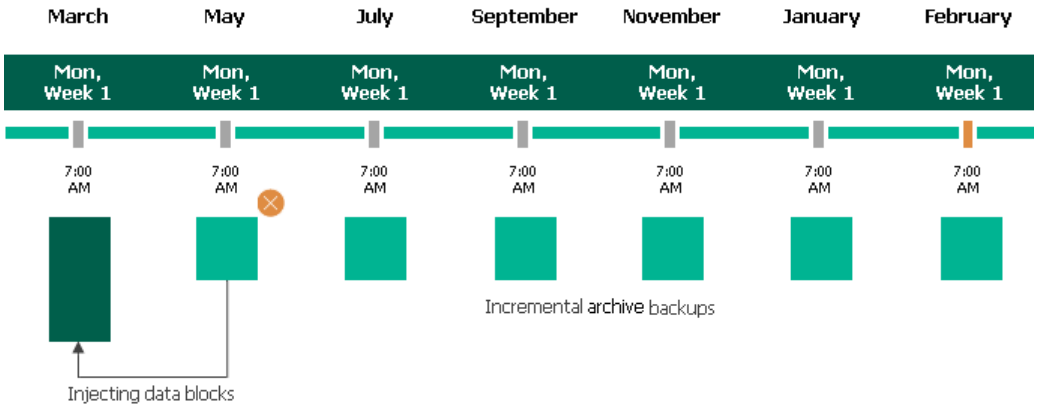
   On the first Monday of May, an archive session will create a restore point with only that data that has changed since the previous archive session in March. Veeam Backup for Microsoft Azure will copy this restore point as an incremental archive backup to the archive repository.



6. Up to the first Monday of February of the next year, Veeam Backup for Microsoft Azure will continue adding new restore points to the regular backup chain and deleting outdated backups from the backup repository, according to the specified weekly scheduling settings. Veeam Backup for Microsoft Azure will also continue adding new restore points to the archive backup chain, according to the specified monthly settings.

   By the moment the archive session completes, the earliest restore point in the archive backup chain will get older than the specified retention limit. That is why Veeam Backup for Microsoft Azure will rebuild the full archive backup and remove from the chain the restore point created on the first Monday of March of the previous year.

   For more information on how Veeam Backup for Microsoft Azure transforms archive backup chains, see Retention Policy for Archived Backups.




Consider that data encryption must be either enabled or disabled for both backup and archive backup repositories selected within the same backup archiving configuration. For example, you cannot select an encrypted standard backup repository and an unencrypted archive backup repository to store backups. However, you can select repositories with different data encryption configurations in one backup policy. That is, you can select an encrypted standard backup repository, an encrypted archive backup repository, an unencrypted standard backup repository and an unencrypted archive backup repository. In this case, backups created in the encrypted standard backup repository will be copied to the encrypted archive backup repository, and backups created in the unencrypted standard backup repository will be copied to the unencrypted archive backup repository. Also, the selected repositories can have different encryption options (password and Azure Key Vault cryptographic key encryption).

## Step 7. Configure General Settings

At the **Settings** step of the wizard, you can enable automatic retries, schedule health checks and specify notification settings for the backup policy.

# Automatic Retry Settings

To instruct Veeam Backup for Microsoft Azure to run the backup policy again if it fails on the first try, do the following:

1. In the **Schedule** section of the step, select the **Automatic retry failed policy** check box.
2. In the field to the right of the check box, specify the maximum number of attempts to run the backup policy. The time interval between retries is 600 seconds.

When retrying backup policies, Veeam Backup for Microsoft Azure processes only those Azure VMs that failed to be backed up during the previous attempt.

> **NOTE**
>
> The automatic retry settings apply only to backup policies that run according to specific schedules — these settings do not apply to policies started manually.

# Health Check Settings

If you have enabled creation of image-level backups at step 5, you can instruct Veeam Backup for Microsoft Azure to periodically perform a health check for backup restore points created by the backup policy. During the health check, Veeam Backup for Microsoft Azure performs an availability check for data blocks in the whole regular backup chain, and a cyclic redundancy check (CRC) for metadata to verify its integrity. The health check helps you ensure that the restore points are consistent and that you will be able to restore data using these restore points. For more information on the health check, see How Health Check Works.

> **NOTE**
>
> During a health check, Veeam Backup for Microsoft Azure does not verify archived restore points created by the policy.

To instruct Veeam Backup for Microsoft Azure to perform a health check, do the following:

1. In the **Health check** section of the step, set the **Enable health check** toggle to *On*.
2. Use the **Run on** drop-down lists to schedule a specific day for the health check to run.

> **NOTE**
>
> Veeam Backup for Microsoft Azure performs the health check during the last policy session that runs on the day when the health check is scheduled. If another backup policy session runs on the same day, Veeam Backup for Microsoft Azure will not perform the health check during that session. For example, if the backup policy is scheduled to run multiple times on Saturday, and the health check is also scheduled to run on Saturday, the health check will only be performed during the last policy session on Saturday.

# Notification Settings

To instruct Veeam Backup for Microsoft Azure to send email notifications for the backup policy, do the following:

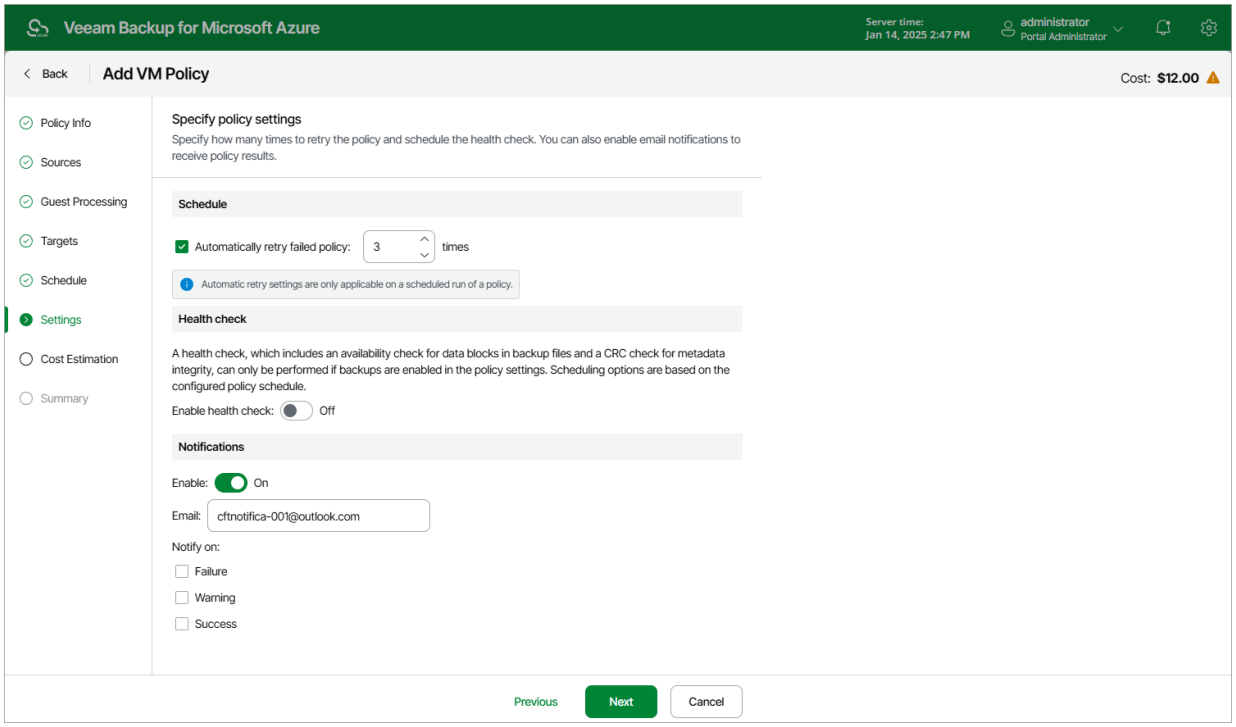
1. In the **Notifications** section of the step, set the **Enabled** toggle to *On*.

   If you set the toggle to *Off*, Veeam Backup for Microsoft Azure will not send any notifications for this backup policy — regardless of the configured global notification settings.

2. In the **Email** field, specify an email address of a recipient. Use a semicolon to separate multiple recipient addresses.

3. Use the **Notify on** list to choose whether you want Veeam Backup for Microsoft Azure to send email notifications in case the backup policy completes successfully, completes with warnings or completes with errors.

> **NOTE**
>
> If you specify the same email recipient in both backup policy notification and global notification settings, Veeam Backup for Microsoft Azure will override the configured global notification settings and will send each notification to this recipient only once to avoid notification duplicates.




## How Health Check Works

When Veeam Backup for Microsoft Azure saves a new backup restore point to a backup repository, it calculates CRC values for metadata in the backup chain and saves these values to the chain metadata, together with the instance data. When performing a health check, Veeam Backup for Microsoft Azure verifies the availability of data blocks and uses the saved values to ensure that the restore points being verified are consistent.

If you have enabled health checks for the backup policy, Veeam Backup for Microsoft Azure performs the following operations at the day scheduled for a health check to run:

1. As soon as a backup policy session completes successfully, Veeam Backup for Microsoft Azure starts the health check as a new session. For each restore point in the standard backup chain, Veeam Backup for Microsoft Azure calculates CRC values for backup metadata and compares them to the CRC values that were previously saved to the restore point. Veeam Backup for Microsoft Azure also checks whether data blocks that are required to rebuild the restore point are available.

   If the backup policy session completes with an error, Veeam Backup for Microsoft Azure tries to run the backup policy again, taking into account the maximum number of retries specified in the automatic retry settings. After the first successful retry (or after the last one out of the maximum number of retries), Veeam Backup for Microsoft Azure starts the health check.

2. If Veeam Backup for Microsoft Azure does not detect data inconsistency, the health check session completes successfully. Otherwise, the session completes with an error.

   Depending on the detected data inconsistency, Veeam Backup for Microsoft Azure performs the following operations:

   - If the health check detects corrupted metadata in a full or incremental restore point, Veeam Backup for Microsoft Azure marks the backup chain as corrupted in the configuration database. During the next backup policy session, Veeam Backup for Microsoft Azure copies the full instance image, creates a full restore point in the backup repository and starts a new backup chain in the backup repository.

> **NOTE**
>
> Veeam Backup for Microsoft Azure does not support metadata check for encrypted backup chains.

   - If the health check detects corrupted disk blocks in a full or an incremental restore point, Veeam Backup for Microsoft Azure marks the restore point that includes the corrupted data blocks and all subsequent incremental restore points as incomplete in the configuration database. During the next backup policy session, Veeam Backup for Microsoft Azure copies not only those data blocks that have changed since the previous backup session but also data blocks that have been corrupted, and saves these data blocks to the latest restore point that has been created during the current session.

## Step 8. Review Estimated Cost

[This step applies only if you have created a schedule for the backup policy at the **Schedule** step of the wizard]

At the **Cost Estimation** step of the wizard, review the approximate monthly cost of Azure services that Veeam Backup for Microsoft Azure will require to protect the Azure VMs added to the backup policy. The total estimated cost includes the following:

- The cost of creating and maintaining snapshots of the Azure VMs.

  For each Azure VM included in the backup policy, Veeam Backup for Microsoft Azure takes into account the total size of virtual disks attached, the number of restore points to be kept in the snapshot chain, and the configured scheduling settings.

- The cost of creating and maintaining image-level backups of the Azure VMs.

  For each Azure VM included in the backup policy, Veeam Backup for Microsoft Azure takes into account the total size of virtual disks attached, the number of restore points to be kept in the backup chain, and the configured scheduling settings.

- The cost of transferring Azure VM data between Azure regions during data protection operations (for example, if a protected Azure VM and the target storage account reside in different regions).

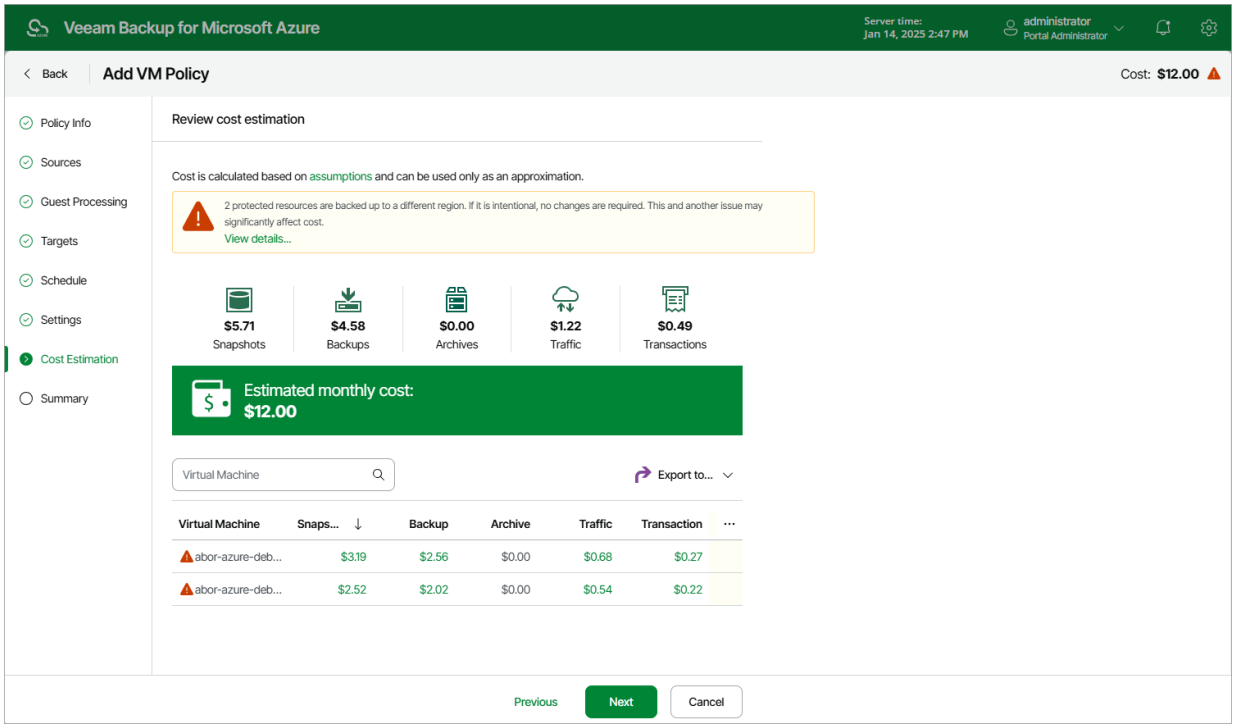
  If you get a warning message regarding additional costs associated with cross-region data transfer, you can click **View details** to see available cost-effective options.

- The cost of making API requests to Microsoft Azure during data protection operations.

> **NOTE**
>
> To calculate the estimated cost, Veeam Backup for Microsoft Azure uses the capabilities of the Azure Pricing Calculator that estimates the cost of services in USD only. This calculator is intended for informational and estimation purposes only.

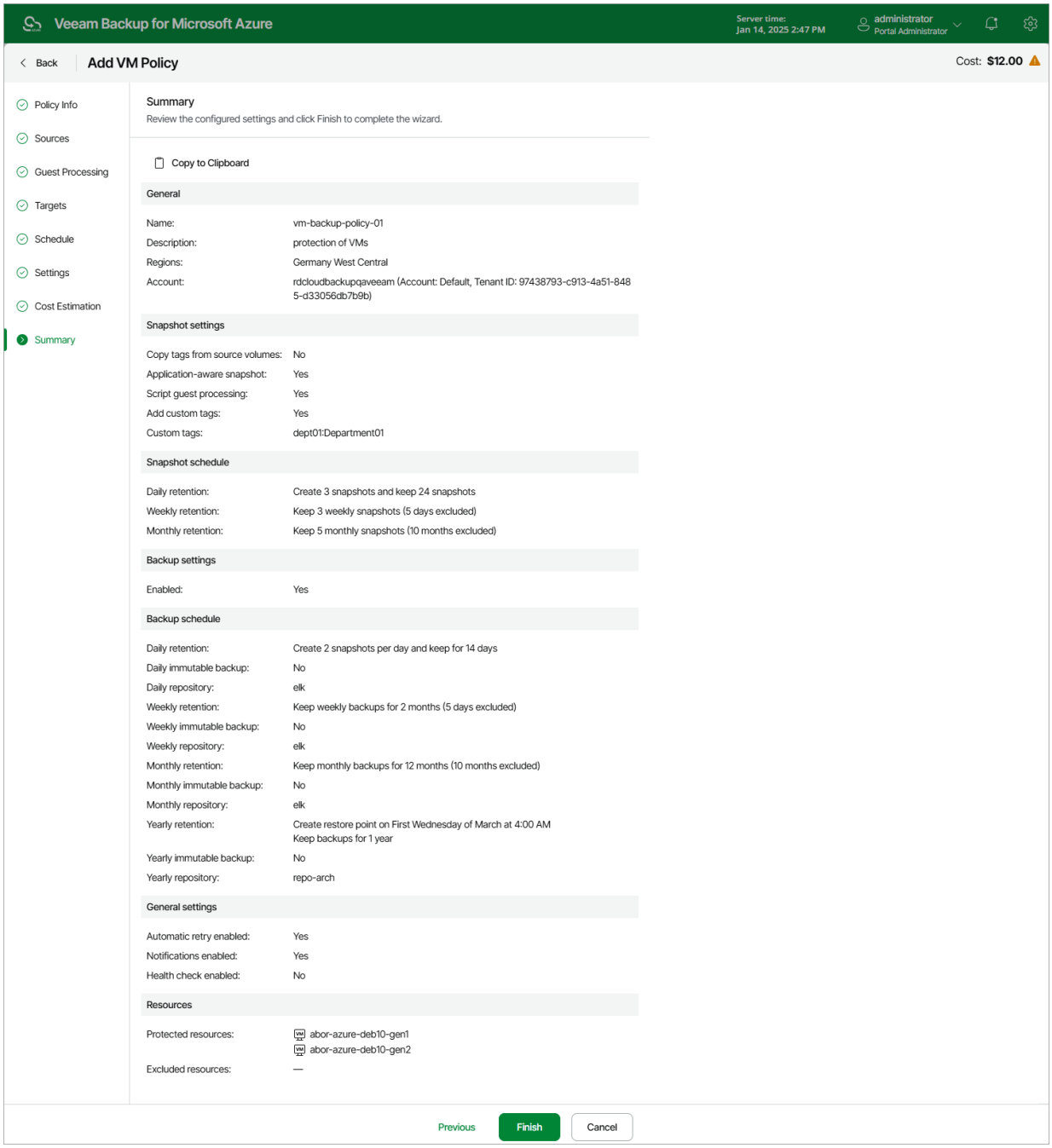
The estimated cost may occur to be significantly higher due to the backup frequency, cross-region data transfer and snapshot charges. To reduce the cost, you can try the following workarounds:

- To avoid additional costs related to cross-region data transfer, select a backup repository that resides in the same region as Azure VMs that you plan to back up.
- To reduce high snapshot charges, adjust the snapshot retention settings to keep less restore points in the snapshot chain.
- To optimize the cost of storing backups, modify the scheduling settings to run the backup policy less frequently, or specify an archive repository for long-term retention of restore points.


Veeam Backup for Microsoft Azure
Server time:
Jan 14, 2025 2:47 PM
administrator
Portal Administrator
Back
Add VM Policy
Cost: $12.00
Policy Info
Sources
Guest Processing
Targets
Schedule
Settings
Cost Estimation
Summary
Review cost estimation
Cost is calculated based on assumptions and can be used only as an approximation.
2 protected resources are backed up to a different region. If it is intentional, no changes are required. This and another issue may significantly affect cost.
View details...
$5.71
Snapshots
$4.58
Backups
$0.00
Archives
$1.22
Traffic
$0.49
Transactions
Estimated monthly cost:
$12.00
Virtual Machine
Export to...
Virtual Machine
Snaps...
Backup
Archive
Traffic
Transaction
abor-azure-deb...
$3.19
$2.56
$0.00
$0.68
$0.27
abor-azure-deb...
$2.52
$2.02
$0.00
$0.54
$0.22
Previous
Next
Cancel

## Step 9. Finish Working with Wizard

At the **Summary** step of the wizard, review summary information and click **Finish**.




# Creating SLA-Based VM Backup Policies

To create an SLA-based backup policy, do the following:

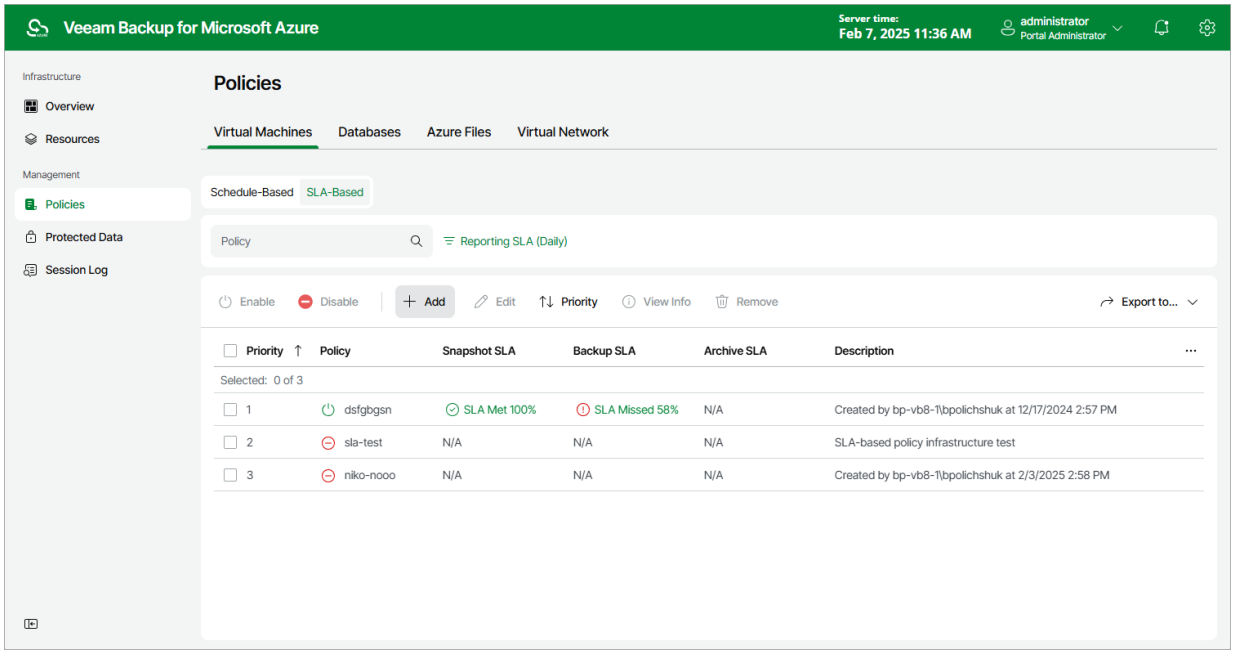
1. Launch the Add SLA-Based Policy wizard.
2. Specify a policy name and description.
3. Configure backup source settings.
4. Configure guest processing options.

5. Configure protection settings.
6. Configure tag settings.
7. Specify general settings for the policy.
8. Review the estimated cost of protecting the selected Azure VMs.
9. Finish working with the wizard.

# Step 1. Launch Add SLA-Based Policy Wizard

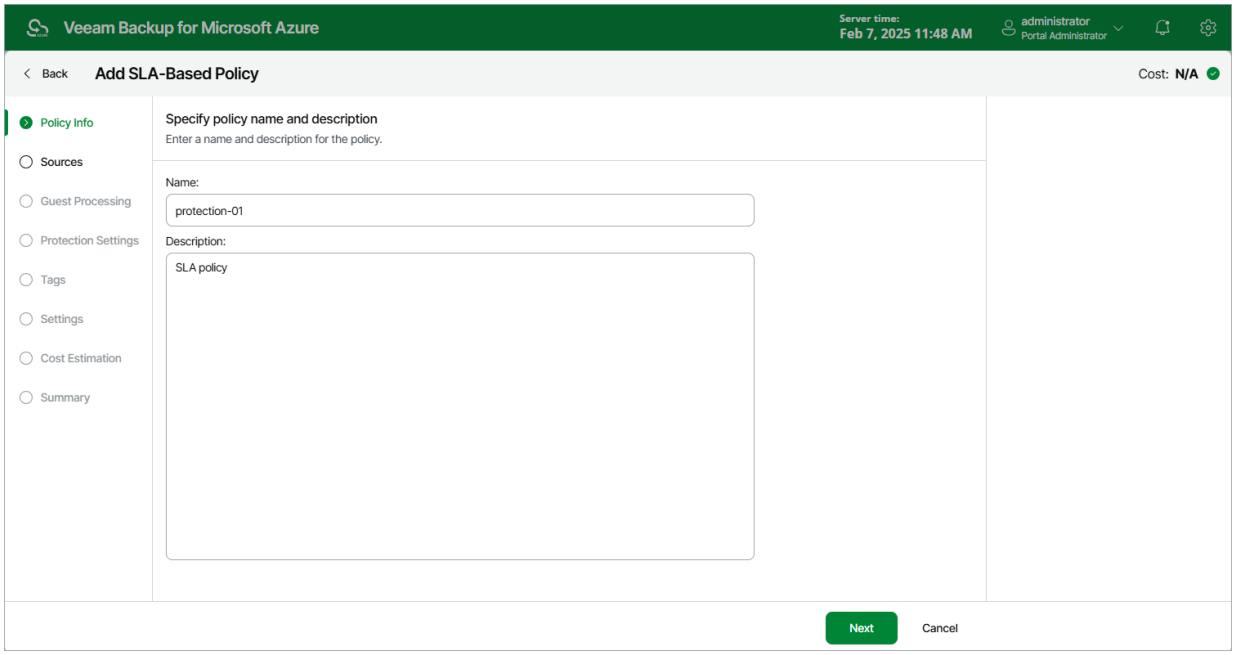
To launch the **Add SLA-Based Policy** wizard, do the following:

1. Navigate to **SLA-Based Policies**.
2. Click **Add**.



# Step 2. Specify Policy Name

At the **Policy Info** step of the wizard, use the **Name** and **Description** fields to enter a name for the new policy and to provide a description for future reference. The maximum length of the name is 255 characters. The following characters are not supported: / \ " ' : | < > + = ; , ? ! * % # ^ @ & $ .



## Step 3. Configure Backup Source Settings

At the **Sources** step of the wizard, specify the following backup source settings:

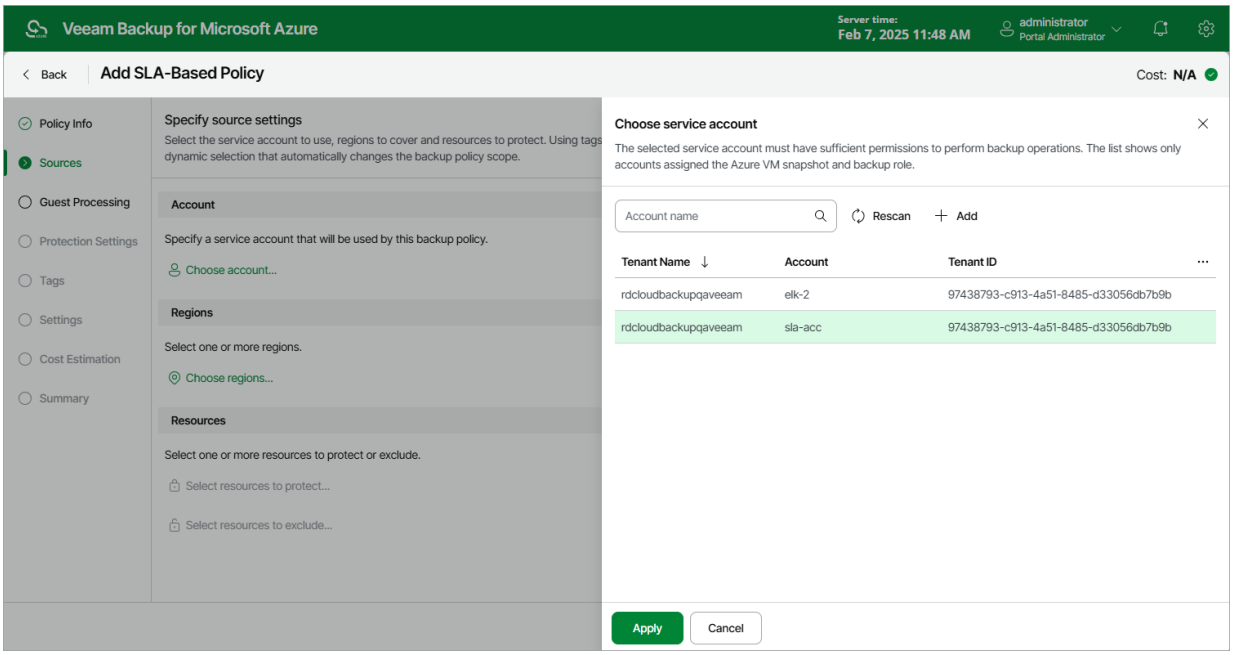
1. Select a service account whose permissions will be used to perform Azure VM backup.
2. Choose regions where Azure VMs that you want to back up reside.
3. Select resources to back up.

## Step 3a. Select Service Account

In the **Account** section of the **Sources** step of the wizard, specify a service account whose permissions will be used to access Azure services and resources, and to create cloud-native snapshots of Azure VMs.

1. Click **Choose account**.
2. In the **Choose service account** window, select the necessary service account from the available accounts list. The specified service account must belong to the Microsoft Entra tenant that contains the Azure VMs that you want to protect, and must be assigned permissions listed in section Azure VM Permissions.

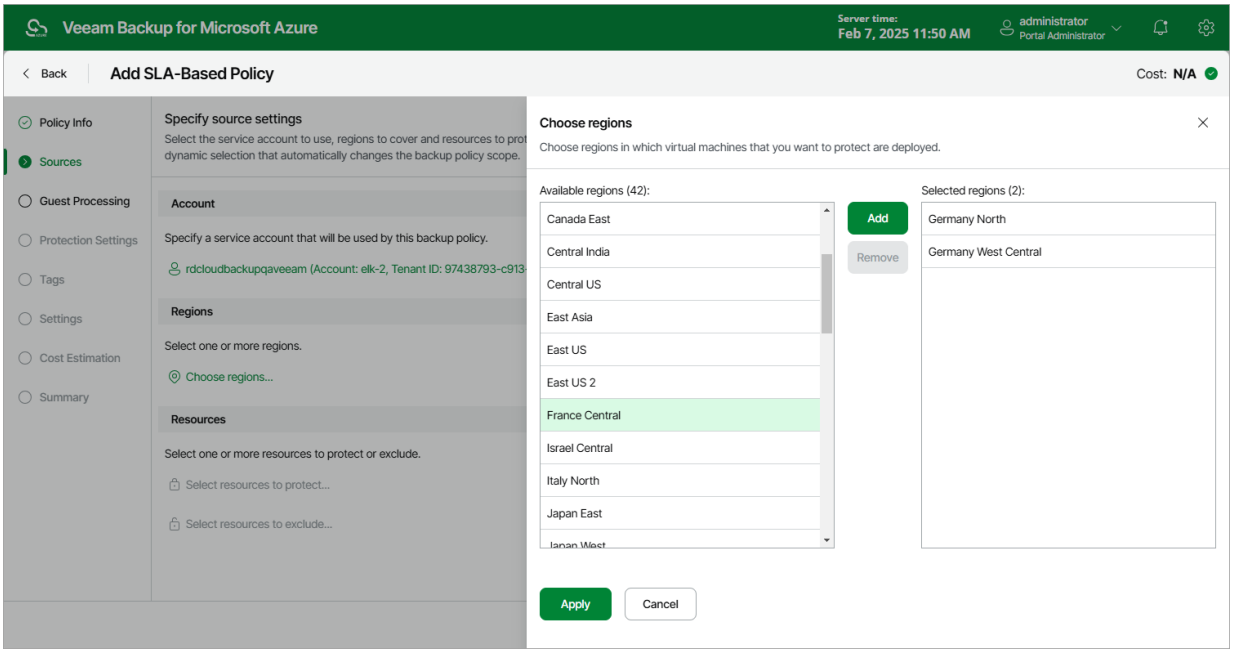
   For a service account to be displayed in the list of available accounts, it must be added to Veeam Backup for Microsoft Azure and assigned the *Azure VMs Snapshot and Backup* operational role as described in section Adding Service Accounts. If you have not added the necessary service account to Veeam Backup for Microsoft Azure beforehand, you can do it without closing the **Add VM Policy** wizard. To do that, click **Add** and complete the **Add Account** wizard.
3. To save changes made to the SLA-based backup policy settings, click **Apply**.



## Step 3b. Select Regions

In the **Region** section of the **Sources** step of the wizard, select regions where Azure resources that you want to back up reside:

1. Click **Choose regions**.
2. In the **Choose regions** window, select the necessary regions from the **Available regions** list, and then click **Add**.
3. To save changes made to the SLA-based backup policy settings, click **Apply**.



## Step 3c. Select Resources

In the **Resources** section of the **Sources** step of the wizard, specify the backup scope — select resources that Veeam Backup for Microsoft Azure will back up:

1. Click **Select resources to protect**.
2. In the **Choose resource protection options** window, choose whether you want to back up all Azure resources from the regions selected at step 3b, or only specific resources.

   If you select the **All resources** option, Veeam Backup for Microsoft Azure will regularly check for new Azure VMs launched in the selected regions and automatically update the SLA-based backup policy settings to include these VMs in the backup scope.

   If you select the **Protect the following resources** option, you must also specify the resources explicitly:

   a. Use the **Resource type** drop-down list to select either of the following options:

      - *Subscription* — to back up Azure VMs managed by specific subscriptions.
      - *Resource group* — to back up Azure VMs that belong to specific resource groups.
      - *Tag* — to back up Azure VMs that have specific tags assigned.
      - *Virtual machine* — to back up only specific Azure VMs.

   b. Use the search field to the right of the **Resource type** list to find the necessary resource, and then click **Protect** to add the resource to the backup scope.

      For a resource to be displayed in the list of available resources, it must reside in an Azure region that has ever been specified in any backup policy. Otherwise, the only option to discover available resources is to click **Browse to select specific source from the global list** and wait for Veeam Backup for Microsoft Azure to populate the resource list.

      Note that your web browser zoom must not exceed 135% for the list of protected resources to be displayed correctly.

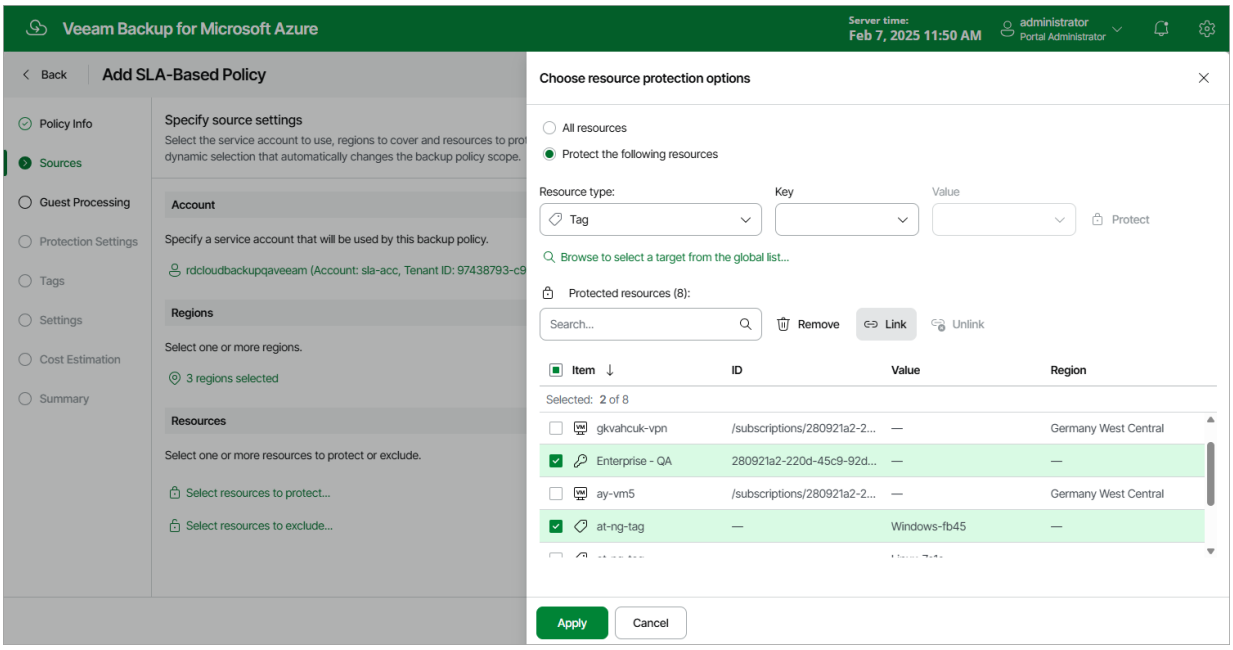
> **TIP**
>
> You can simultaneously add multiple resources to the backup scope. To do that, click **Browse to select specific source from the global list**, select check boxes next to the necessary items in the list of available resources, and then click **Protect**.
>
> If the list does not show the resources that you want to back up, click **Rescan** to launch the data collection process — as soon as the process is over, Veeam Backup for Microsoft Azure will update the resource list. If you still cannot find the necessary resources in the list, make sure that the *Microsoft.ManagedServices* provider is registered in the subscription to which the resources belong, return to step 3a and click **Rescan** in the **Choose service account** window. To learn how to register a resource provider, see Microsoft Docs.

   If you add a tag to the backup scope, Veeam Backup for Microsoft Azure will regularly check for new Azure VMs assigned the added tag and automatically update the SLA-based backup policy settings to include these VMs in the scope. However, this applies only to Azure VMs residing in the regions selected at step 3b. If you select a tag assigned to Azure VMs residing in other regions, these VMs will not be protected by the SLA-based backup policy. To work around the issue, either go back to step 3b and add the missing regions, or create a new SLA-based backup policy.

4. To save changes made to the SLA-based backup policy settings, click **Apply**.

> **TIP**
>
> As an alternative to selecting the **Protect the following resources** option and specifying the resources explicitly, you can select the **All resources** option and exclude a number of resources from the backup scope. To do that, click **Select resources to exclude** and specify Azure VMs or tags that you want to exclude from the backup scope — the procedure is the same as described for including resources in the backup scope.
>
> Consider that if a resource appears both in the list of included and excluded resources, Veeam Backup for Microsoft Azure will still not process the resource because the list of excluded resources has a higher priority.

When you add subscriptions, resource groups and tags to the backup scope, Veeam Backup for Microsoft Azure links all these resources using the OR operator. To instruct Veeam Backup for Microsoft Azure to use the AND operator, follow the instructions provided in section Configuring Conditions.




## Configuring Conditions

By default, Veeam Backup for Microsoft Azure uses the OR operator to link all the subscriptions, resource groups and tags that you include into the backup scope — meaning that all the related VMs will be protected by the policy. To narrow down the backup scope, you can configure conditions that will allow Veeam Backup for Microsoft Azure to link the selected resources using the AND operator.

When you configure a condition, Veeam Backup for Microsoft Azure composes a list of VMs to protect based on the resources that you add to this condition — meaning that an Azure VM will be protected by the policy only if this VM relates to all the linked resources. Keep in mind that one condition can link either multiple tags, a subscription with one or more tags, or a resource group with one or more tags.

To configure a condition, do the following in the **Resources** section of the **Sources** step of the wizard:

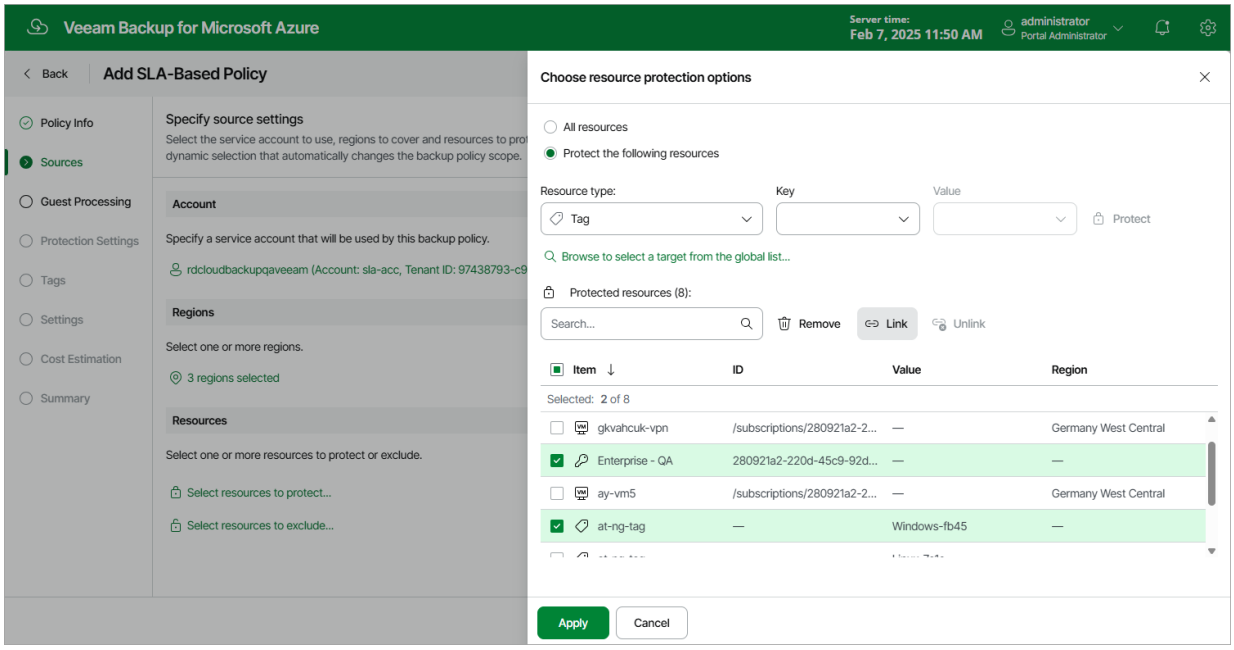
1. Click **Select resources to protect**.
2. In the **Choose resource protection options** window, select check boxes next to the items you want to include into the condition and click **Link**.

3. In the **Create Condition** window, provide a name for the condition and click **Apply**.

   The maximum length of the name is 64 characters.

When configuring conditions, you can add the same resource to the list of protected resources multiple times. For example, if you want to protect VMs that are managed by the *dept-01-sweden* subscription and that have either the *Veeam-01* tag or *Veeam-02* tag assigned (but not both tags at the same time), you must add this subscription to the list of protected resources twice and then configure 2 separate conditions: one condition will link the subscription with the *Veeam-01* tag, while another condition will link the subscription with the *Veeam-02* tag.

> **TIP**
>
> After you configure a condition, you will be able to modify the list of resources included into this condition, unlink all the resources, and remove the condition if you no longer need it. When performing these actions, keep in mind that:
>
> - If you exclude a resource from the condition, Veeam Backup for Microsoft Azure will re-add it to the list of protected resources as a single item.
> - If you unlink the condition, Veeam Backup for Microsoft Azure will re-add all resources that were included into this condition to the list of protected resources as single items, and will link these resources using the OR operator.
> - If you remove the condition, Veeam Backup for Microsoft Azure will remove all resources that were included into this condition from the backup scope.



## Step 4. Specify Guest Processing Settings

If you want to back up Azure VMs that are currently running, you can configure guest processing settings at the **Guest Processing** step of the wizard. These settings allow you to specify what actions Veeam Backup for Microsoft Azure will perform when communicating with the guest OSes.

Particularly, you can specify the following guest processing settings:

- Application-aware processing. For Windows-based Azure VMs running VSS-aware applications, you can enable application-aware processing to ensure that the applications will be able to recover successfully, without data loss.

  Application-aware processing is the Veeam technology based on Microsoft VSS. This option can be applied only to the Windows-based Azure VMs that support Microsoft VSS. For more information on Microsoft VSS, see Microsoft Docs.

- Guest scripting. You can instruct Veeam Backup for Microsoft Azure to run custom scripts on the processed Azure VM before and after the backup operation. For example, Veeam Backup for Microsoft Azure can execute a pre-snapshot script on the VM to quiesce these applications. This will allow Veeam Backup for Microsoft Azure to create a transactionally consistent snapshot while no write operations occur on the virtual disks. After the snapshot is created, a post-snapshot script can start the applications again.

> **NOTE**
>
> Only users with the *Portal Administrator* role can edit guest scripting settings.

# Limitations and Requirements

When creating transactionally consistent backups, Veeam Backup for Microsoft Azure uses the Azure Queue Storage service to stop and start applications running on the processed Windows-based Azure VMs. To ensure proper communication of the backup appliance and the guest OSes, all Windows-based Azure VMs for which you plan to enable guest processing must have the **443** network port opened.

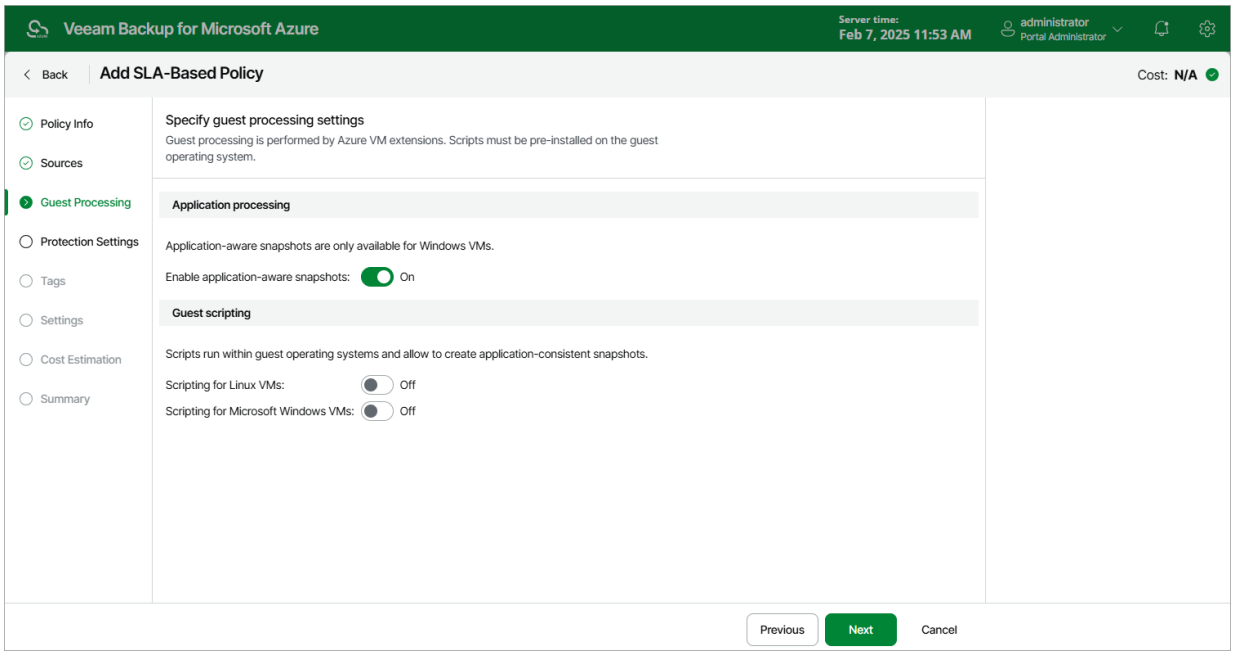
In case firewall rules configured for the Azure VMs do not allow outbound access using the **443** port, you must allow HTTPS traffic over **443** port for `<FQDN>.blob.core.windows.net` and `<FQDN>.queue.core.windows.net`, where *<FQDN>* is the name of the storage account used by the Veeam backup service.

## Enabling Application-Aware Processing

To enable application-aware processing, set the **Enable application aware snapshots** toggle to *On* in the **Application Processing** section of the **Guest Processing** step of the wizard.

**IMPORTANT**

While creating application-aware snapshots, VSS Guest Agent uses the VSS Copy Backup type to create snapshots of the processed Azure VMs during the SLA-based backup policy session. This type of VSS backup does not support truncation of transaction log. For more information on VSS Backup types, see Microsoft Docs.




# Limitation and Considerations

To enable application-aware processing, VSS agents must be installed on source Azure VMs. To install VSS agents, Veeam Backup for Microsoft Azure runs a specific PowerShell script on the source Azure VMs. That is why if you use PowerShell execution policies to control the conditions under which PowerShell loads configuration files and runs scripts on your source VMs, make sure that the **LocalMachine** scope is set to the *RemoteSigned* value. Otherwise, Veeam Backup for Microsoft Azure will not be able to run the script and application-aware processing will fail.

## Enabling Guest Scripting

[Applies for users that have the Portal Administrator role only]

To enable guest scripting, do the following at the **Guest Processing** step of the wizard:

- For Azure VMs running Linux OS, set the **Scripting for Linux instances** toggle to *On*.

  The **Specify scripting settings for Linux instances** window will open.

- For Azure VMs running Microsoft Windows OS, set the **Scripting for Microsoft Windows instances** toggle to *On*.

  The **Specify scripting settings for Windows instances** window will open.

**IMPORTANT**

When enabling guest scripting, consider the following:

- Veeam Backup for Microsoft Azure supports the EXE, BAT, CMD, WSF, JS, VBS and PS1 file formats for Windows-based Azure VMs, and the SH file format for Linux-based Azure VMs.
- To run custom scripts on Windows-based Azure VMs, Veeam Backup for Microsoft Azure uses the Run Command feature. For more information, see Microsoft Docs.

In the opened window, specify pre-snapshot and post-snapshot scripts that will be executed before and after the backup operation:

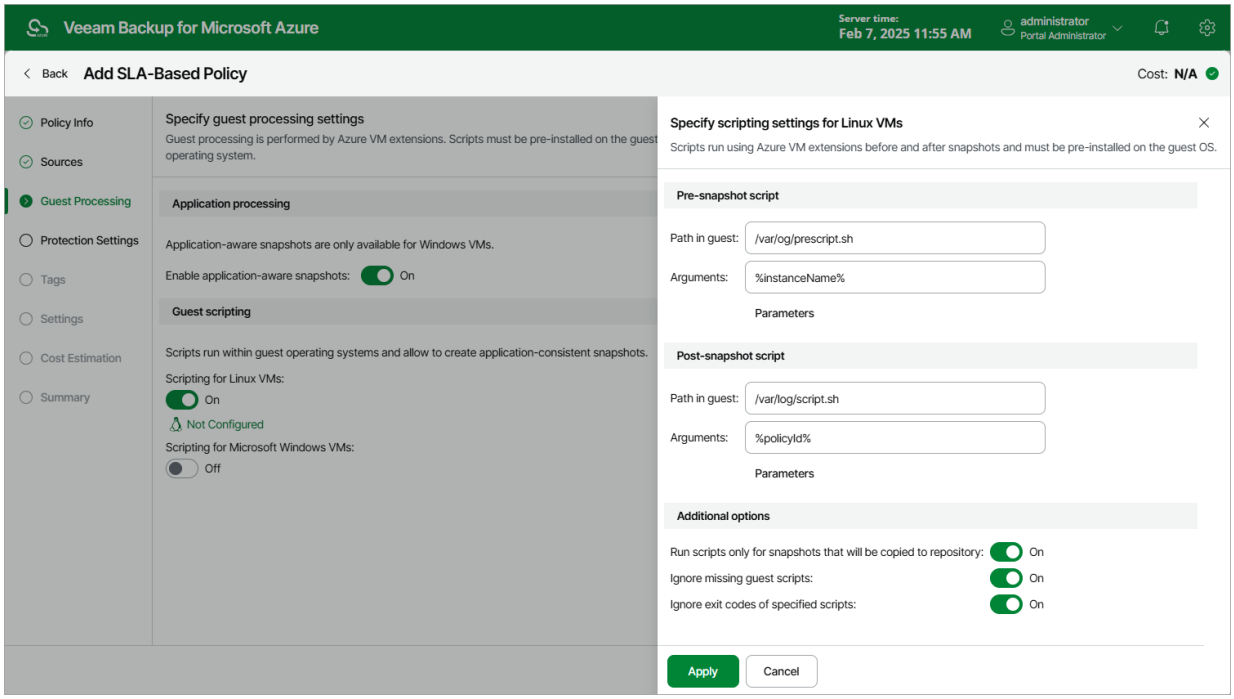
1. In the **Pre-snapshot script** section, do the following:
   a. In the **Path in guest** field, specify a path to the directory on an Azure VM where the pre-snapshot script file resides.
   b. In the **Arguments** field, specify additional arguments that will be passed to the script when the script is executed.

      You can use runtime variables as arguments for the script. To see the list of available variables, click **Parameters**.

**IMPORTANT**

Veeam Backup for Microsoft Azure will try to run a script residing in the specified directory for all Azure VMs added to the SLA-based backup policy. If you want to execute different scripts for different Azure VMs, ensure that script files uploaded to these VMs have the same path and name.

2. Repeat step 1 for the post-snapshot scripts in the **Post-snapshot script** section.
3. In the **Additional Options** section, choose whether you want to run scripts only while creating repository snapshots, to proceed with snapshot creation even though scripts are missing on some of the processed instances, and to ignore exit codes returned while executing the scripts.
4. Click **Apply**.



## Step 5. Configure Protection Settings

At the **Protection Settings** step of the wizard, select an SLA and a storage template that will be assigned to the policy:

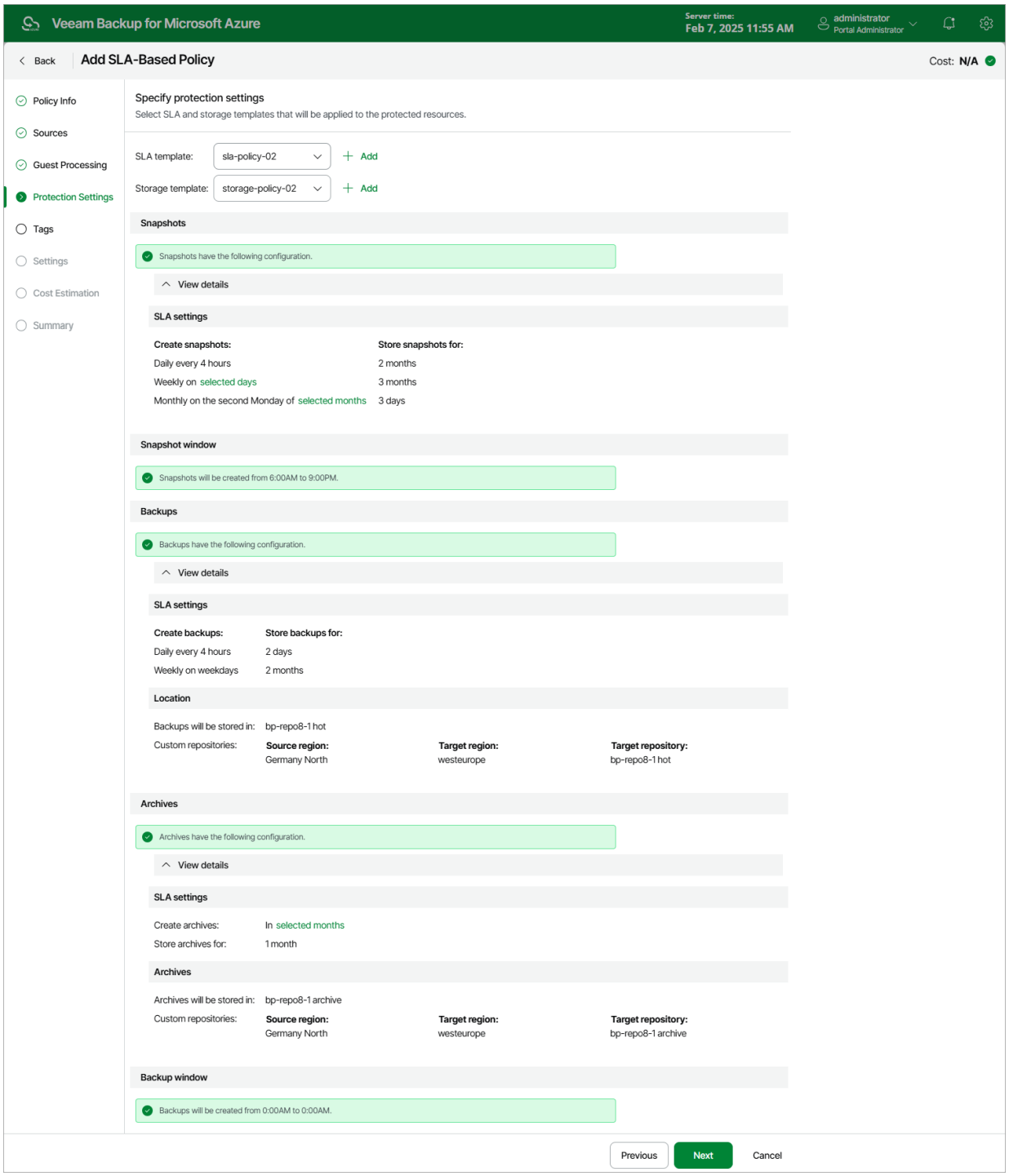
1. From the **SLA template** list, select an SLA template whose snapshot, backup and archived backup settings the policy will use to protect workloads specified at step 3c.

   For an SLA template to be displayed in the list, it must be added to Veeam Backup for Microsoft Azure as described in section Adding SLA Templates. If you have not added the necessary SLA template to Veeam Backup for Microsoft Azure beforehand, you can do it without closing the **SLA-Based Policy** wizard. To do that, click **Add** and complete the **Add SLA Template** wizard.

2. From the **Storage template** list, select a storage template whose target location settings the policy will use to store backed-up data.

   For a storage template to be displayed in the list, it must be added to Veeam Backup for Microsoft Azure as described in section Adding Storage Templates. If you have not added the necessary storage template to Veeam Backup for Microsoft Azure beforehand, you can do it without closing the **SLA-Based Policy** wizard. To do that, click **Add** and complete the **Add Storage Template** wizard.

> **IMPORTANT**
>
> The snapshot, backup and archived backup settings configured for the selected SLA template must match the target location settings configured for the selected storage template. That is, if backups are configured for the selected SLA template, make sure you configured backup location settings for the storage template, and if archive backups are configured for the selected SLA template, make sure you configured archived backup location settings for the storage template.


Veeam Backup for Microsoft Azure
Server time:
Feb 7, 2025 11:55 AM
administrator
Portal Administrator
Back
Add SLA-Based Policy
Cost: N/A
Policy Info
Sources
Guest Processing
Protection Settings
Tags
Settings
Cost Estimation
Summary
Specify protection settings
Select SLA and storage templates that will be applied to the protected resources.
SLA template:
sla-policy-02
Add
Storage template:
storage-policy-02
Add
Snapshots
Snapshots have the following configuration.
View details
SLA settings
Create snapshots:
Daily every 4 hours
Weekly on selected days
Monthly on the second Monday of selected months
Store snapshots for:
2 months
3 months
3 days
Snapshot window
Snapshots will be created from 6:00AM to 9:00PM.
Backups
Backups have the following configuration.
View details
SLA settings
Create backups:
Daily every 4 hours
Weekly on weekdays
Store backups for:
2 days
2 months
Location
Backups will be stored in:
bp-repo8-1 hot
Custom repositories:
Source region:
Germany North
Target region:
westeurope
Target repository:
bp-repo8-1 hot
Archives
Archives have the following configuration.
View details
SLA settings
Create archives:
In selected months
Store archives for:
1 month
Archives
Archives will be stored in:
bp-repo8-1 archive
Custom repositories:
Source region:
Germany North
Target region:
westeurope
Target repository:
bp-repo8-1 archive
Backup window
Backups will be created from 0:00AM to 0:00AM.
Previous
Next
Cancel

# Step 6. Enable Azure Tags Assigning

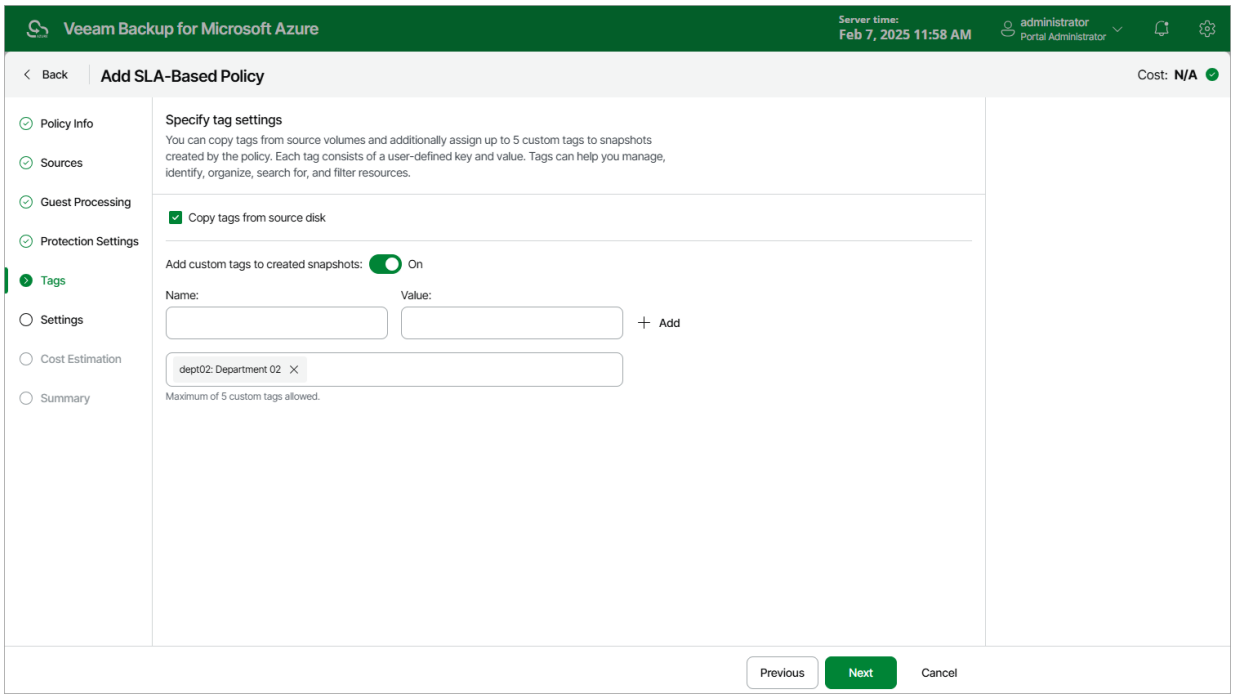
At the **Tags** step of the wizard, you can instruct Veeam Backup for Microsoft Azure to assign Azure tags to cloud-native snapshots of the selected Azure VMs:

1. To assign already existing Azure tags from the virtual disks of the processed Azure VM, select the **Copy tags from source disk** check box.

   If you choose to copy tags from the source disks, Veeam Backup for Microsoft Azure will first create a cloud-native snapshot of the Azure VM and will assign to the created snapshot Azure tags with Veeam metadata, then Veeam Backup for Microsoft Azure will copy tags from the disks of the processed VM and, finally, assign the copied tags to the snapshot.

2. To assign your own custom Azure tags, set the **Add custom tags to created snapshots** toggle to *On* and specify the tags explicitly. To do that, use the **Name** and **Value** fields to specify a name and value for the new custom tag, and then click **Add**. Note that you cannot add more than 5 custom Azure tags.

   If you choose to add custom tags to the created snapshots, Veeam Backup for Microsoft Azure will assign the specified tags right after it creates a cloud-native snapshot.



## Step 7. Configure General Settings

At the **Settings** step of the wizard, you can enable automatic retries and specify notification settings for the SLA-based backup policy policy.

# Automatic Retry Settings

To instruct Veeam Backup for Microsoft Azure to run a policy session again if it fails on the first try, do the following:

1. In the **Session retries** section of the step, select the **Automatic retry failed sessions** check box.
2. In the field to the right of the check box, specify the maximum number of attempts to run the policy sessions. The time interval between retries is 600 seconds.

When retrying policy sessions, Veeam Backup for Microsoft Azure processes only those Azure VMs that failed to be backed up during the previous attempt.

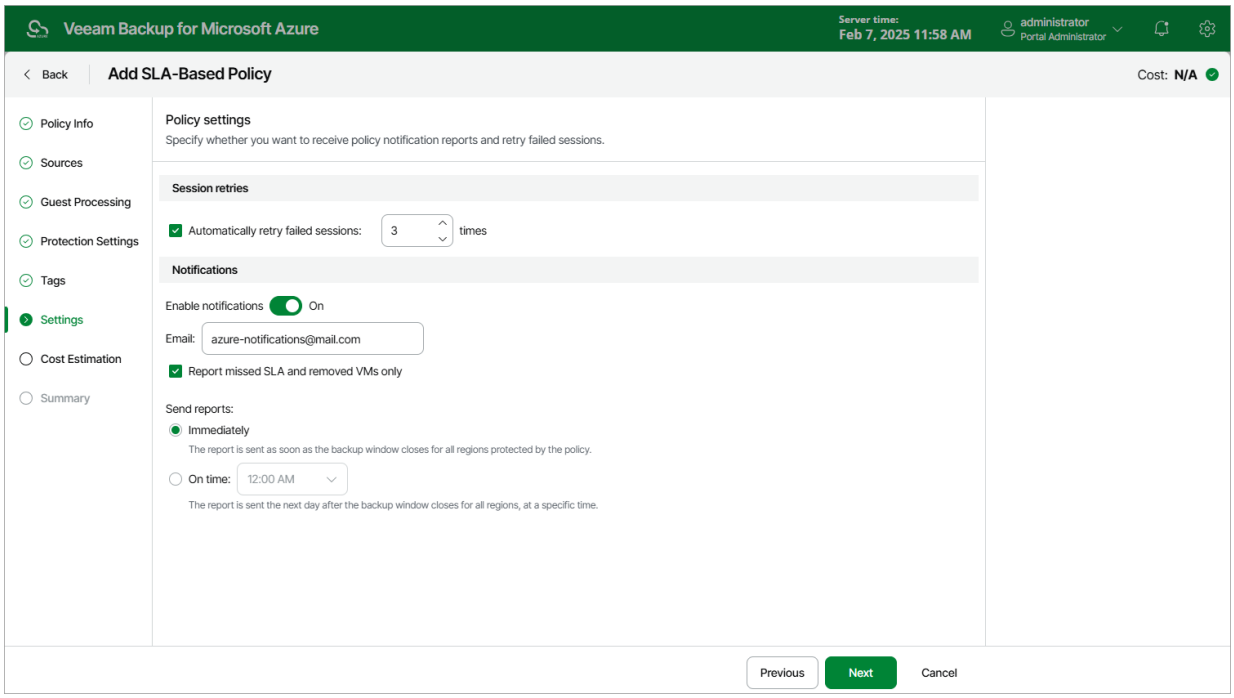
# Notification Settings

To instruct Veeam Backup for Microsoft Azure to send email notifications for the policy, do the following:

1. In the **Notifications** section of the step, set the **Enable notifications** toggle to *On*.

   If you set the toggle to *Off*, Veeam Backup for Microsoft Azure will not send any notifications for this backup policy — regardless of the configured global notification settings.
2. In the **Email** field, specify an email address of a recipient. Use a semicolon to separate multiple recipient addresses.
3. Select the **Report missed SLA and removed VMs only** check box if you want Veeam Backup for Microsoft Azure to send email notifications only in case the backup policy fails to meet SLA target value, or if any Azure VMs added to the policy are considered removed from Microsoft Azure.
4. Use the **Send reports** setting to define whether you want Veeam Backup for Microsoft Azure to send email notifications immediately after it finalizes the backup window specified for the policy in all regions added to the policy and completes calculating SLA compliance ratio, or at a specific time after Veeam Backup for Microsoft Azure finalizes the backup window specified for the policy in all regions added to the policy and completes calculating SLA compliance ratio.

> **NOTE**
>
> If you specify the same email recipient in both backup policy notification and global notification settings, Veeam Backup for Microsoft Azure will override the configured global notification settings and will send each notification to this recipient only once to avoid notification duplicates.


Veeam Backup for Microsoft Azure
Server time:
Feb 7, 2025 11:58 AM
administrator
Portal Administrator
Back
Add SLA-Based Policy
Cost: N/A
Policy Info
Sources
Guest Processing
Protection Settings
Tags
Settings
Cost Estimation
Summary
Policy settings
Specify whether you want to receive policy notification reports and retry failed sessions.
Session retries
Automatically retry failed sessions:
3
times
Notifications
Enable notifications
On
Email:
azure-notifications@mail.com
Report missed SLA and removed VMs only
Send reports:
Immediately
The report is sent as soon as the backup window closes for all regions protected by the policy.
On time:
12:00 AM
The report is sent the next day after the backup window closes for all regions, at a specific time.
Previous
Next
Cancel

## Step 8. Review Estimated Cost

[This step applies only if you have created a schedule for the SLA-based backup policy at the **Schedule** step of the wizard]

At the **Cost Estimation** step of the wizard, review the approximate monthly cost of Azure services that Veeam Backup for Microsoft Azure will require to protect the Azure VMs added to the SLA-based backup policy. The total estimated cost includes the following:

- The cost of creating and maintaining snapshots of the Azure VMs.

  For each Azure VM included in the SLA-based backup policy, Veeam Backup for Microsoft Azure takes into account the total size of virtual disks attached, the number of restore points to be kept in the snapshot chain, and the configured scheduling settings.

- The cost of creating and maintaining image-level backups of the Azure VMs.

  For each Azure VM included in the SLA-based backup policy, Veeam Backup for Microsoft Azure takes into account the total size of virtual disks attached, the number of restore points to be kept in the backup chain, and the configured scheduling settings.

- The cost of transferring Azure VM data between Azure regions during data protection operations (for example, if a protected Azure VM and the target storage account reside in different regions).

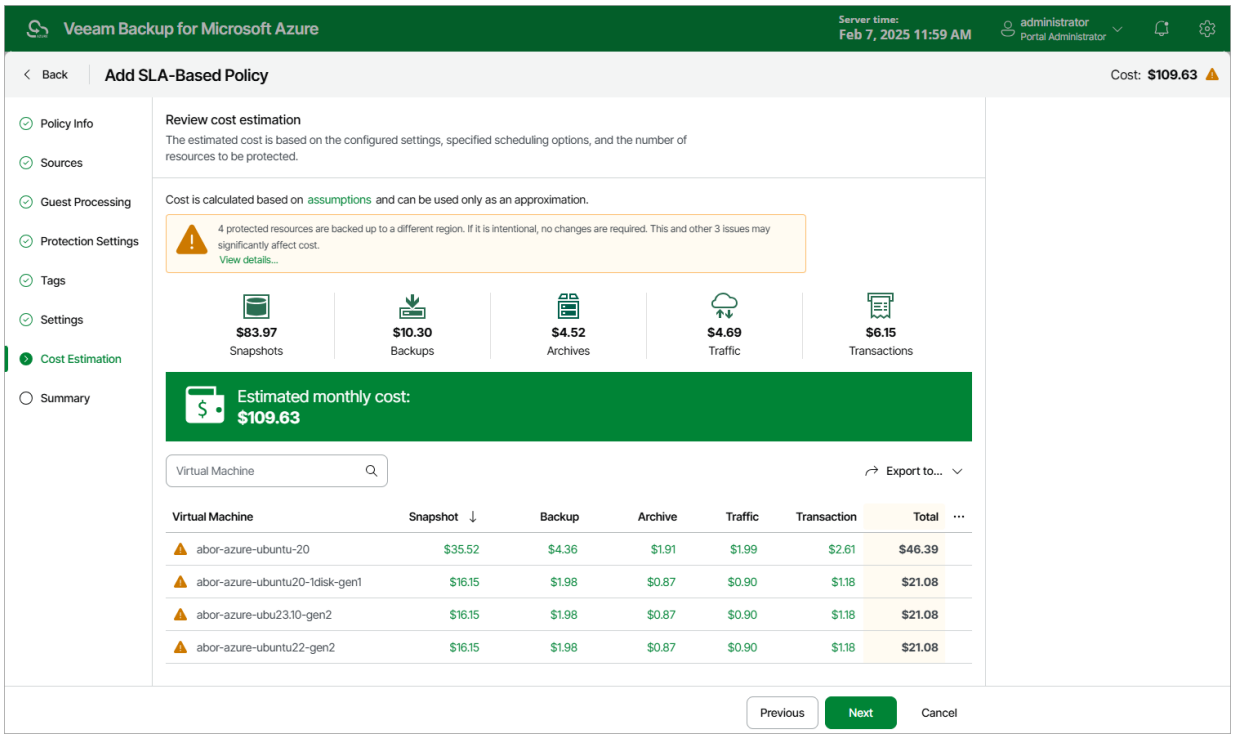
  If you get a warning message regarding additional costs associated with cross-region data transfer, you can click **View details** to see available cost-effective options.

- The cost of making API requests to Microsoft Azure during data protection operations.

> **NOTE**
>
> To calculate the estimated cost, Veeam Backup for Microsoft Azure uses the capabilities of the Azure Pricing Calculator that estimates the cost of services in USD only. This calculator is intended for informational and estimation purposes only.

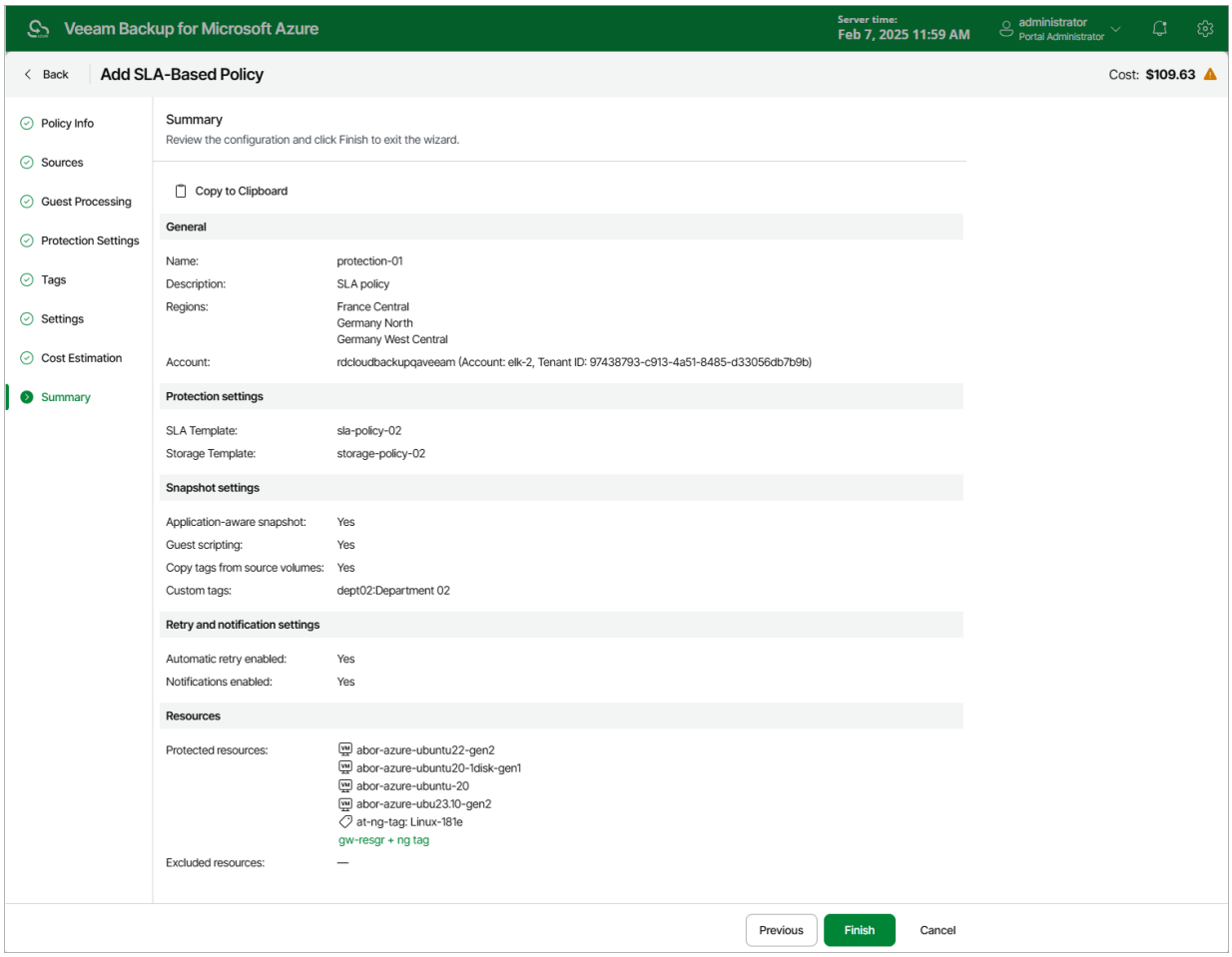
The estimated cost may occur to be significantly higher due to the backup frequency, cross-region data transfer and snapshot charges. To reduce the cost, you can try the following workarounds:

- To avoid additional costs related to cross-region data transfer, select a backup repository that resides in the same region as Azure VMs that you plan to back up.
- To reduce high snapshot charges, adjust the snapshot retention settings to keep less restore points in the snapshot chain.
- To optimize the cost of storing backups, modify the scheduling settings to run the SLA-based backup policy less frequently, or specify an archive repository for long-term retention of restore points.


Veeam Backup for Microsoft Azure
Server time:
Feb 7, 2025 11:59 AM
administrator
Portal Administrator
Back
Add SLA-Based Policy
Cost: $109.63
Policy Info
Sources
Guest Processing
Protection Settings
Tags
Settings
Cost Estimation
Summary
Review cost estimation
The estimated cost is based on the configured settings, specified scheduling options, and the number of resources to be protected.
Cost is calculated based on assumptions and can be used only as an approximation.
4 protected resources are backed up to a different region. If it is intentional, no changes are required. This and other 3 issues may significantly affect cost.
View details...
$83.97
Snapshots
$10.30
Backups
$4.52
Archives
$4.69
Traffic
$6.15
Transactions
Estimated monthly cost:
$109.63
Virtual Machine
Export to...
Virtual Machine
Snapshot
Backup
Archive
Traffic
Transaction
Total
abor-azure-ubuntu-20
$35.52
$4.36
$1.91
$1.99
$2.61
$46.39
abor-azure-ubuntu20-1disk-gen1
$16.15
$1.98
$0.87
$0.90
$1.18
$21.08
abor-azure-ubu23.10-gen2
$16.15
$1.98
$0.87
$0.90
$1.18
$21.08
abor-azure-ubuntu22-gen2
$16.15
$1.98
$0.87
$0.90
$1.18
$21.08
Previous
Next
Cancel

## Step 9. Finish Working with Wizard

At the **Summary** step of the wizard, review summary information and click **Finish**.




# Creating VM Snapshots Manually

Veeam Backup for Microsoft Azure allows you to manually create snapshots of Azure VMs. Each snapshot is saved to the same Azure region in which the protected Azure VM resides.

> **NOTE**
>
> Veeam Backup for Microsoft Azure does not include snapshots created manually in the snapshot chain and does not apply the configured retention policy settings to these snapshots. This means that the snapshots are kept in your Microsoft Azure environment unless you remove them manually, as described in section Managing VM Data.

To manually create a cloud-native snapshot of an Azure VM, do the following:

1. Navigate to **Resources** > **Virtual Machines**.
2. Select the check box next to the necessary Azure VM and click **Take Snapshot Now**.

   For an Azure VM to be displayed in the list of available resources, it must reside in any of the regions included in a backup policy as described in section Creating VM Schedule-Based Backup Policies (step 3c) or in section Creating VM SLA-Based Backup Policies (step 3c).

3. Complete the **Take Manual Snapshot** wizard:

   a. At the **Service account** step of the wizard, select a service account whose permissions Veeam Backup for Microsoft Azure will use to create a snapshot.

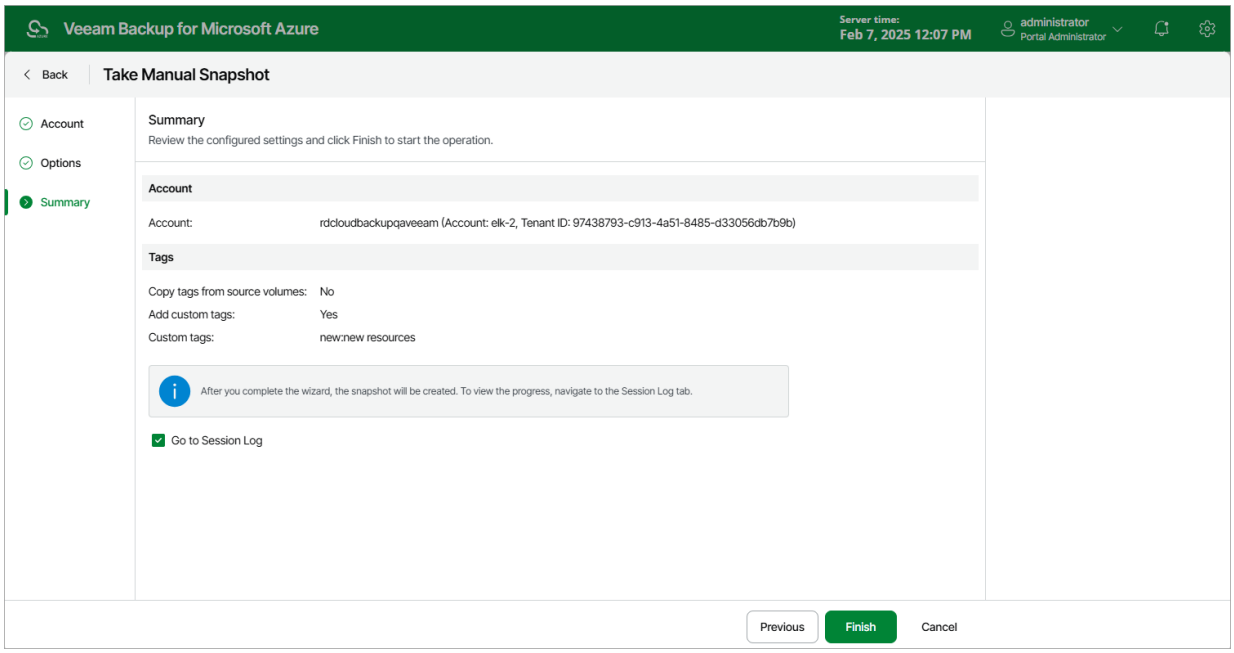
      For an account to be displayed in the accounts list, it must be added to Veeam Backup for Microsoft Azure as described in section Adding Service Accounts.

   b. At the **Options** step of the wizard, click **Tags from source volumes will not be copied and custom tags will not be applied** to assign tags to cloud-native snapshots.

   c. In the **Tags configurations** window, choose whether you want to assign tags to the created snapshot.

      - To assign already existing tags from the source virtual disks, select the **Copy Tags from source volume** check box.
      - To assign your own custom tags, set the **Add custom tags to created snapshots** toggle to *On*, and specify the tags explicitly. To do that, use the **Key** and **Value** fields to specify a key and a value for the new custom tag, and then click **Apply**.

   d. At the **Summary** step of the wizard, review configuration information, choose whether you want to proceed to the Session Log page to track the progress of snapshot creation, and click **Finish**.



# Performing SQL Backup

One backup policy can be used to process one or more Azure SQL databases within one Microsoft Entra tenant. The scope of data that you can protect in a tenant is limited by permissions of a service account that is specified in the backup policy settings.

Before you create an Azure SQL backup policy, check the following prerequisites:

- If you plan to create backups of Azure SQL databases, backup infrastructure components that will take part in the backup process must be added to the backup infrastructure and configured properly. These include backup repositories and worker instances.
- If you plan to receive email notifications on backup policy results, configure email notification settings first. For more information, see Configuring Global Notification Settings.

To schedule data protection tasks to run automatically, create backup policies. For each protected Azure SQL database, you can also take a backup manually when needed.

> **IMPORTANT**
>
> Veeam Backup for Microsoft Azure does not allow you to protect databases hosted by Azure Arc-enabled SQL Managed Instances and SQL Servers on Azure Arc-enabled servers.

## Creating SQL Backup Policies

> **IMPORTANT**
>
> SQL backup policies can protect only Azure SQL databases running on SQL Servers and databases located on SQL Managed Instances. If you want to protect a database hosted by a SQL Server on Azure VM, create an Azure VM backup policy. Note that in this case, you will not be able to restore a single database without restoring the entire VM.

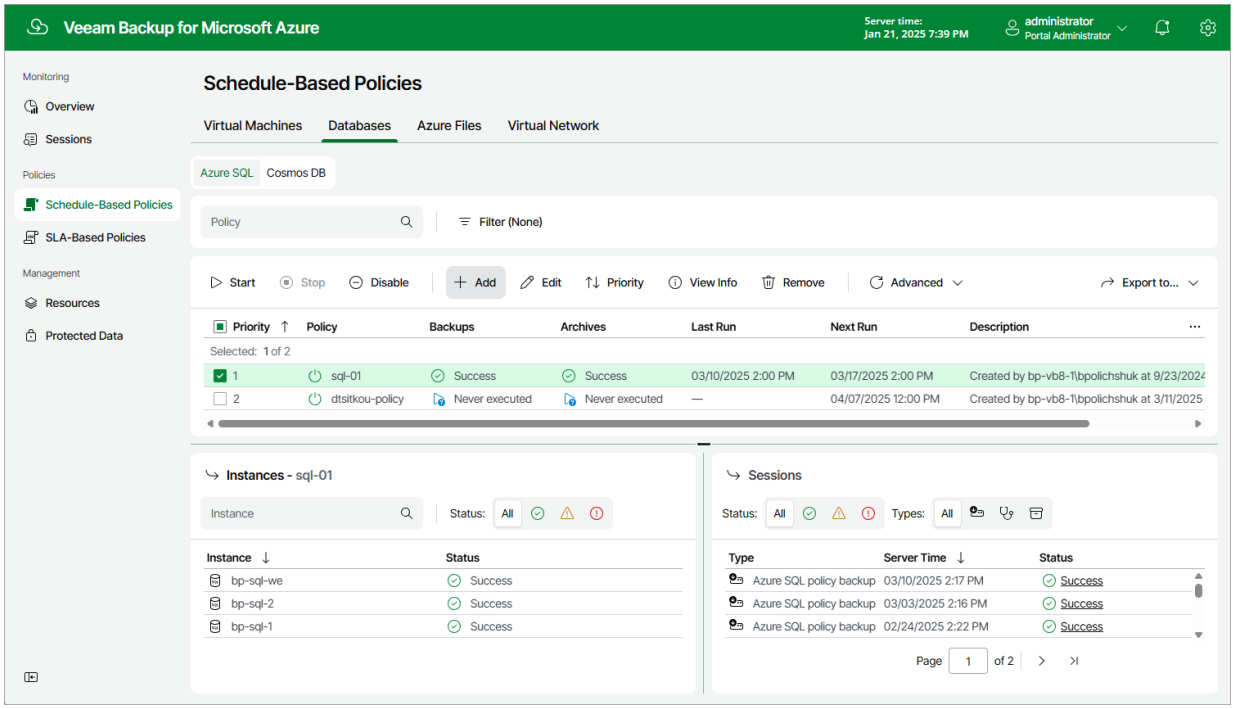
To create a backup policy, do the following:

1. Launch the Add Azure SQL Policy wizard.
2. Specify a backup policy name and description.
3. Configure backup source settings.
4. Configure processing options.
5. Create a schedule for the backup policy.
6. Specify automatic retry, health check and notification settings for the backup policy.
7. Review the estimated cost of protecting the selected Azure SQL databases.
8. Finish working with the wizard.

# Step 1. Launch Add Azure SQL Policy Wizard

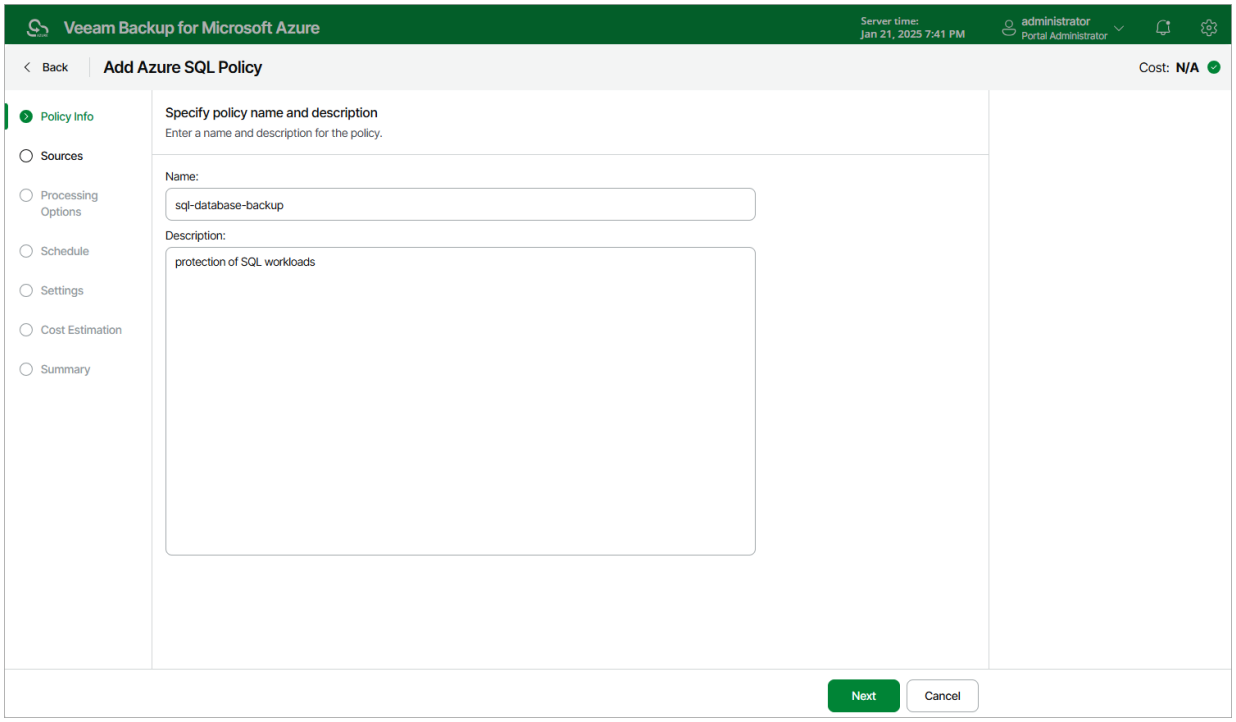
To launch the **Add Azure SQL Policy** wizard, do the following:

1. Navigate to **Schedule-Based Policies**.
2. Switch to **Databases** > **Azure SQL**.
3. Click **Add**.



# Step 2. Specify Backup Policy Name

At the **Policy Info** step of the wizard, use the **Name** and **Description** fields to enter a name for the new backup policy and to provide a description for future reference. The maximum length of the name is 255 characters. The following characters are not supported: / \ " ' : | < > + = ; , ? ! * % # ^ @ & $ .



## Step 3. Configure Backup Source Settings

At the **Sources** step of the wizard, specify the following backup source settings:

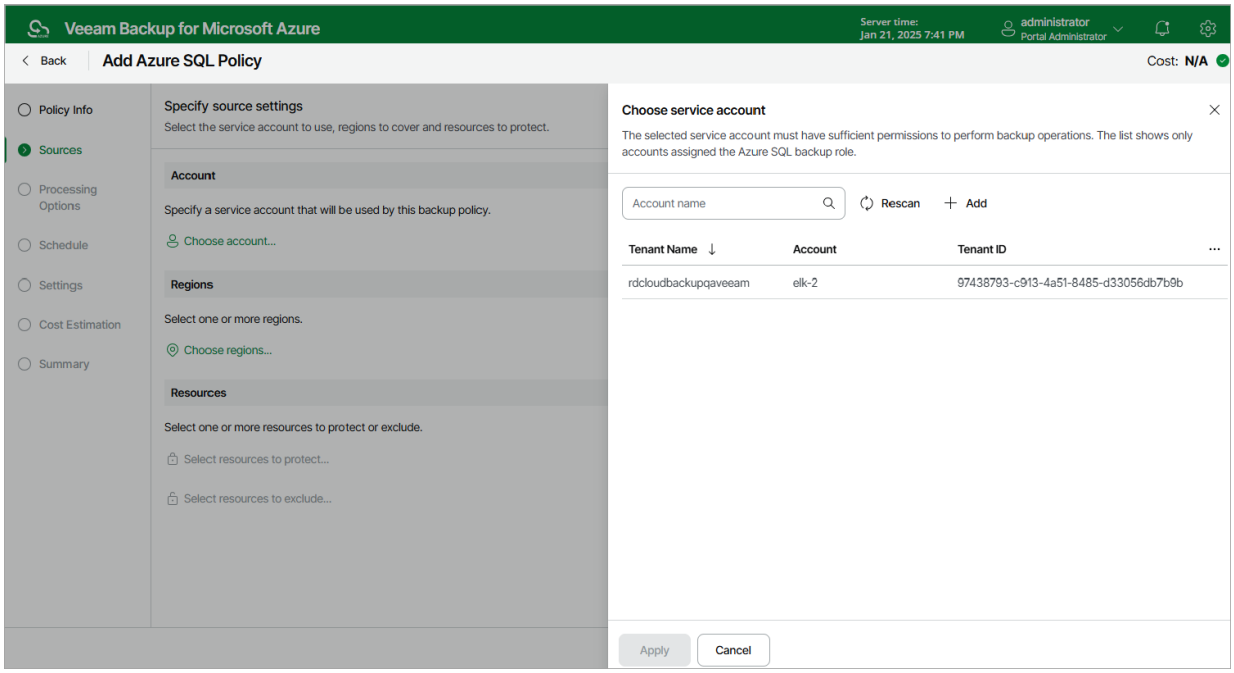
1. Select a service account whose permissions will be used to perform SQL backup.
2. Choose regions where Azure SQL Servers and databases that you want to back up reside.
3. Select resources to back up.

## Step 3a. Select Service Account

In the **Account** section of the **Sources** step of the wizard, specify a service account whose permissions will be used to access Azure services and resources, and to create backups of Azure SQL Servers and databases.

1. Click **Choose account**.
2. In the **Choose service account** window, select the necessary service account from the available accounts list. The specified service account must belong to the Microsoft Entra tenant that contains the Azure SQL Servers and databases that you want to protect, and must be assigned permissions listed in section Azure SQL Permissions.

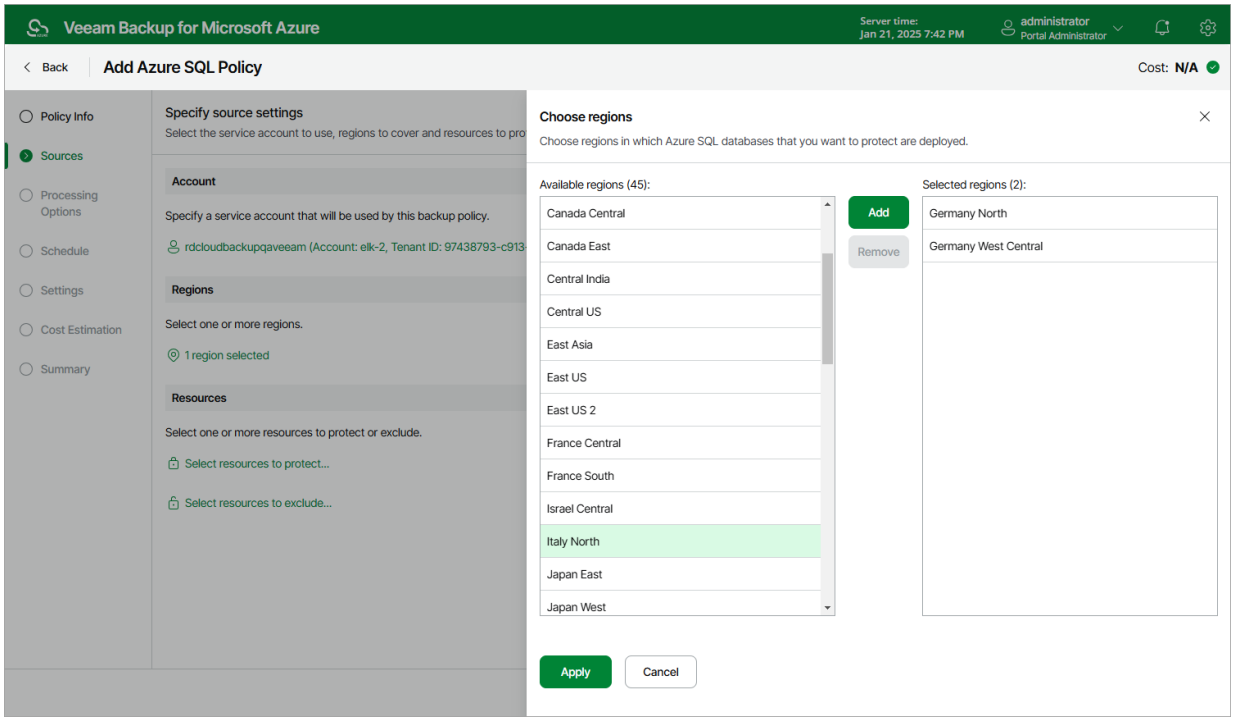
   For a service account to be displayed in the list of available accounts, it must be added to Veeam Backup for Microsoft Azure and assigned the *Azure SQL Backup* operational role as described in section Adding Service Accounts. If you have not added the necessary service account to Veeam Backup for Microsoft Azure beforehand, you can do it without closing the **Add Azure SQL Policy** wizard. To do that, click **Add** and complete the **Add Account** wizard.
3. Click **Apply**.



## Step 3b. Select Regions

In the **Region** section of the **Sources** step of the wizard, select regions where Azure resources that you want to back up reside.

1. Click **Choose regions**.
2. In the **Choose regions** window, select the necessary regions from the **Available regions** list, and then click **Add**.
3. Click **Apply**.



## Step 3c. Select Resources

In the **Resources** section of the **Sources** step of the wizard, specify the backup scope — select resources that Veeam Backup for Microsoft Azure will back up:

1. Click **Select resources to protect**.
2. In the **Choose resource protection options** window, choose whether you want to back up all Azure resources from the regions selected at step 3b, or only specific resources.

   If you select the **All resources** option, Veeam Backup for Microsoft Azure will regularly check for new Azure SQL databases created in the selected regions and automatically update the backup policy settings to include these databases in the backup scope.

   If you select the **Protect the following resources** option, you must also specify the resources explicitly:

   a. Use the **Resource type** drop-down list to select either of the following options:

      - *Database* — to back up only specific Azure SQL databases.
      - *SQL server* — to back up all Azure SQL databases that are located on a specific SQL Server.

   b. Use the search field to the right of the **Resource type** list to find the necessary resource, and then click **Protect** to add the resource to the backup scope.

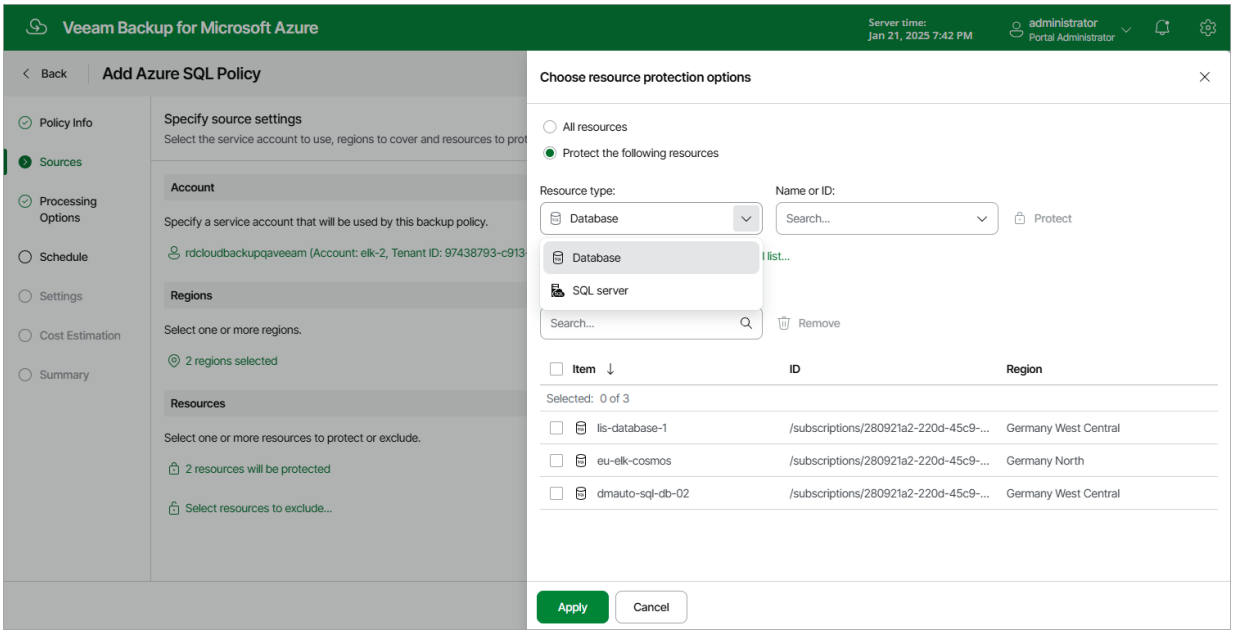
      For a resource to be displayed in the list of available resources, it must reside in an Azure region that has ever been specified in any backup policy. Otherwise, the only option to discover available resources is to click **Browse to select specific source from the global list** and wait for Veeam Backup for Microsoft Azure to populate the resource list.

      Note that your web browser zoom must not exceed 135% for the list of protected resources to be displayed correctly.

> **TIP**
>
> You can simultaneously add multiple resources to the backup scope. To do that, click **Browse to select specific source from the global list**, select check boxes next to the necessary items in the list of available resources, and then click **Protect**.
>
> If the list does not show the resources that you want to back up, click **Rescan** to launch the data collection process — as soon as the process is over, Veeam Backup for Microsoft Azure will update the resource list. If you still cannot find the necessary resources in the list, make sure that the *Microsoft.ManagedServices* provider is registered in the subscription to which the resources belong, return to the step 3a and click **Rescan** in the **Choose service account** window. To learn how to register a resource provider, see Microsoft Docs.

4. To save changes made to the backup policy settings, click **Apply**.

> **TIP**
>
> As an alternative to selecting the **Protect the following resources** option and specifying the resources explicitly, you can select the **All resources** option and exclude a number of resources from the backup scope. To do that, click **Select resources to exclude** and specify the Azure SQL databases that you do not want to back up — the procedure is the same as described for including resources in the backup scope.
>
> Consider that if a resource appears both in the list of included and excluded resources, Veeam Backup for Microsoft Azure will still not process the resource because the list of excluded resources has a higher priority.


Veeam Backup for Microsoft Azure
Server time:
Jan 21, 2025 7:42 PM
administrator
Portal Administrator
Back
Add Azure SQL Policy
Policy Info
Sources
Processing Options
Schedule
Settings
Cost Estimation
Summary
Specify source settings
Select the service account to use, regions to cover and resources to prot
Account
Specify a service account that will be used by this backup policy.
rdcloudbackupqaveeam (Account: elk-2, Tenant ID: 97438793-c913
Regions
Select one or more regions.
2 regions selected
Resources
Select one or more resources to protect or exclude.
2 resources will be protected
Select resources to exclude...
Choose resource protection options
All resources
Protect the following resources
Resource type:
Database
Name or ID:
Search...
Protect
Database
SQL server
l list...
Search...
Remove
Item
ID
Region
Selected: 0 of 3
lis-database-1
/subscriptions/280921a2-220d-45c9-...
Germany West Central
eu-elk-cosmos
/subscriptions/280921a2-220d-45c9-...
Germany North
dmauto-sql-db-02
/subscriptions/280921a2-220d-45c9-...
Germany West Central
Apply
Cancel

## Step 4. Configure Processing Options

At the **Processing Options** step of the wizard, choose whether you want to use a staging server to perform backup. To learn how Veeam Backup for Microsoft Azure uses staging servers to protect Azure SQL databases, see SQL Backup.

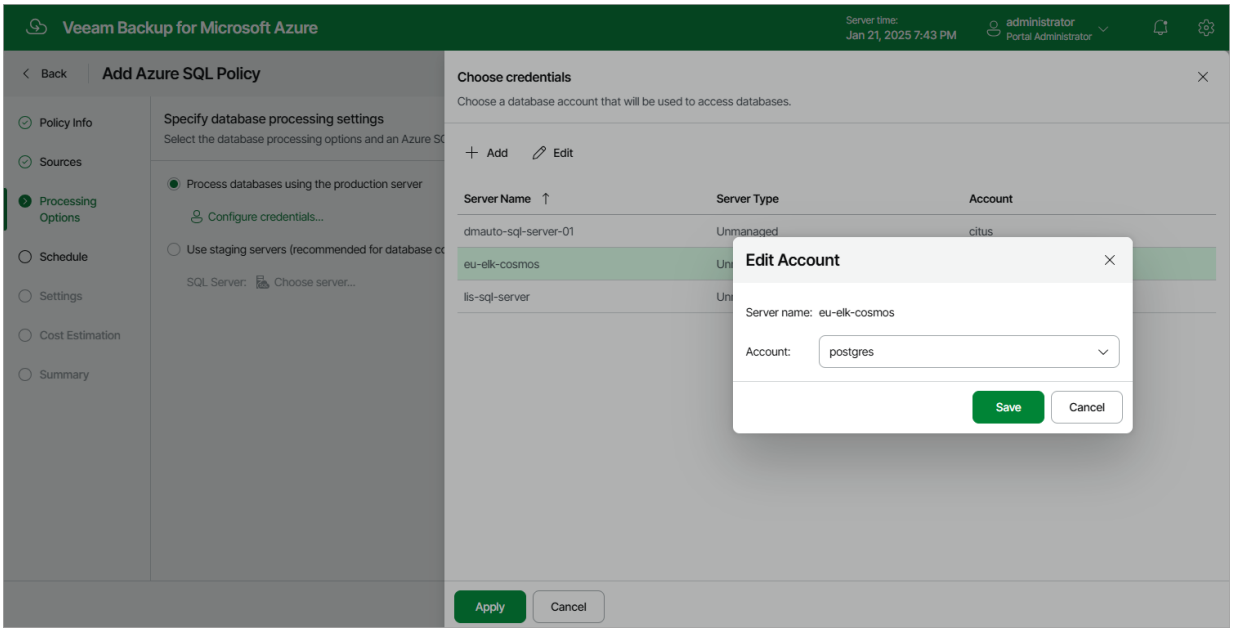
# Protecting Databases Without Staging Server

To back up the selected databases without a staging server, do the following:

1. Select the **Process databases using the production server** option.
2. Click **Configure Credentials**.
3. In the **Choose a SQL account** window:
   a. For each SQL Server added to the policy, specify an Azure SQL account whose permissions Veeam Backup for Microsoft Azure will use to authenticate against the server. To do that, select the server and click **Edit**. Then, in the **Edit Account** window, select the necessary account and click **Save**.

      For an account to be displayed in the **Account** list, it must be added to Veeam Backup for Microsoft Azure as described in section Adding SMTP and Database Accounts. If you have not added the necessary Azure SQL account to Veeam Backup for Microsoft Azure beforehand, you can do it without closing the **Add Azure SQL Policy** wizard. To do that, click **Add** and complete the Add Account wizard.

   b. Click **Apply**.




# Protecting Databases Using Staging Server

To back up the selected databases using a staging server, do the following:

1. Select the **Use staging servers** option.
2. Click **Choose server**.

3. In the **Choose staging server** window:

   a. From the **Staging server** drop-down list, select a SQL Server that will be used to copy the databases. If you plan to back up a database located on an Azure SQL Managed Instance, you must specify the source SQL Server as a staging server.

      For a server to be displayed in the **Staging server** list, it must be added to the Microsoft Azure environment as described in Microsoft Docs.

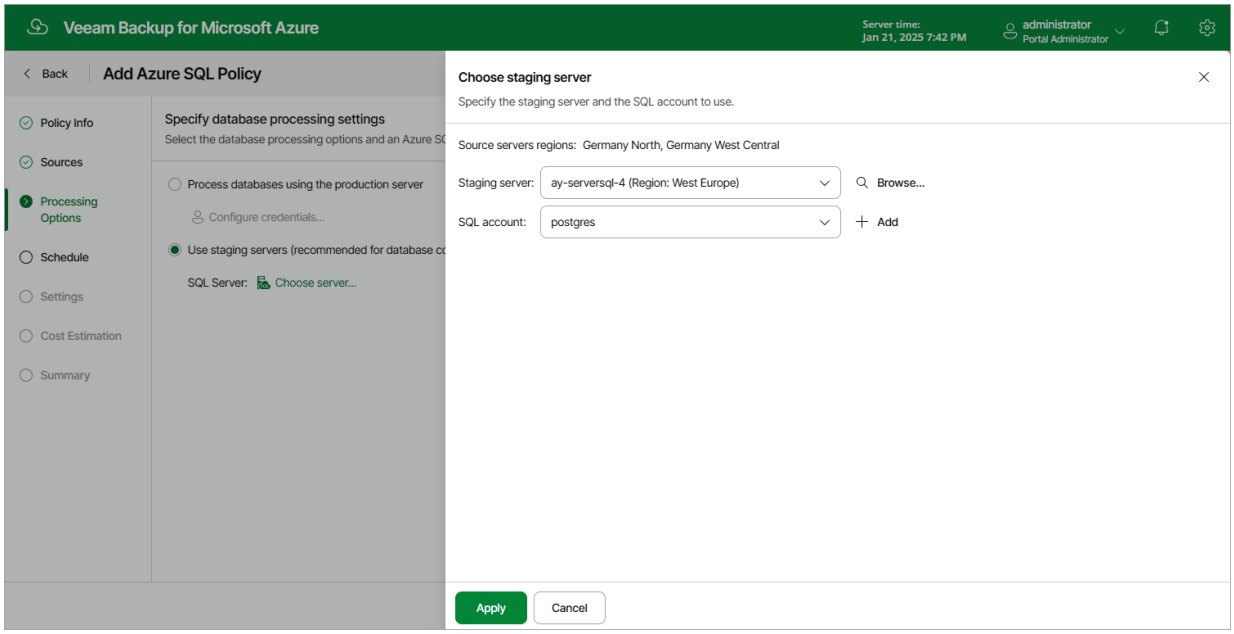
> **IMPORTANT**
>
> If you use custom Transparent Data Encryption (TDE) to protect SQL Server data, consider that the same Azure Key Vault cryptographic key must be used to encrypt the source and the staging SQL Servers to allow Veeam Backup for Microsoft Azure to perform backup using the **Use staging servers** option.

   b. From the **SQL account** drop-down list, select an Azure SQL account whose permissions Veeam Backup for Microsoft Azure will use to authenticate against the staging server.

      For an account to be displayed in the **Account** list, it must be added to Veeam Backup for Microsoft Azure as described in section Adding SMTP and Database Accounts. If you have not added the necessary Azure SQL account to Veeam Backup for Microsoft Azure beforehand, you can do it without closing the **Add Azure SQL Policy** wizard. To do that, click **Add** and complete the Add Account wizard.

> **NOTES**
>
> - To perform backup with a staging server, Veeam Backup for Microsoft Azure uses the service account specified at step 3 of the wizard to send REST API requests to the SQL Servers processed by the backup policy. That is why there is no need to specify credentials for each SQL Server.
> - If the Azure SQL account you use to authenticate against the staging server does not have the *sysadmin* server-level role assigned, you can only use the source SQL Server as a staging server — otherwise, the backup operation will fail.

   c. Click **Apply**.



## Step 5. Specify Policy Scheduling Options

You can instruct Veeam Backup for Microsoft Azure to start the backup policy automatically according to a specific backup schedule. The backup schedule defines how often data of the Azure SQL databases added to the backup policy will be backed up.

To help you implement a comprehensive backup strategy, Veeam Backup for Microsoft Azure allows you to create schedules of the following types:

- Daily — the backup policy will create restore points repeatedly throughout a day on specific days.
- Weekly — the backup policy will create restore points once a day on specific days.
- Monthly — the backup policy will create restore points once a month on a specific day.
- Yearly — the backup policy will create restore points once a year on a specific day.

Combining multiple schedule types together allows you to retain restore points for longer periods of time — for more information, see Enabling Harmonized Scheduling. Combining multiple schedule types together also allows you to archive backups — for more information, see Enabling Backup Archiving.

### Specifying Daily Schedule

To create a daily schedule for the backup policy, at the **Schedule** step of the wizard, do the following:

1. Set the **Daily retention** toggle to *On* and click **Edit Daily Settings**.
2. In the **Daily schedule** window, select hours when the backup policy will create backups.

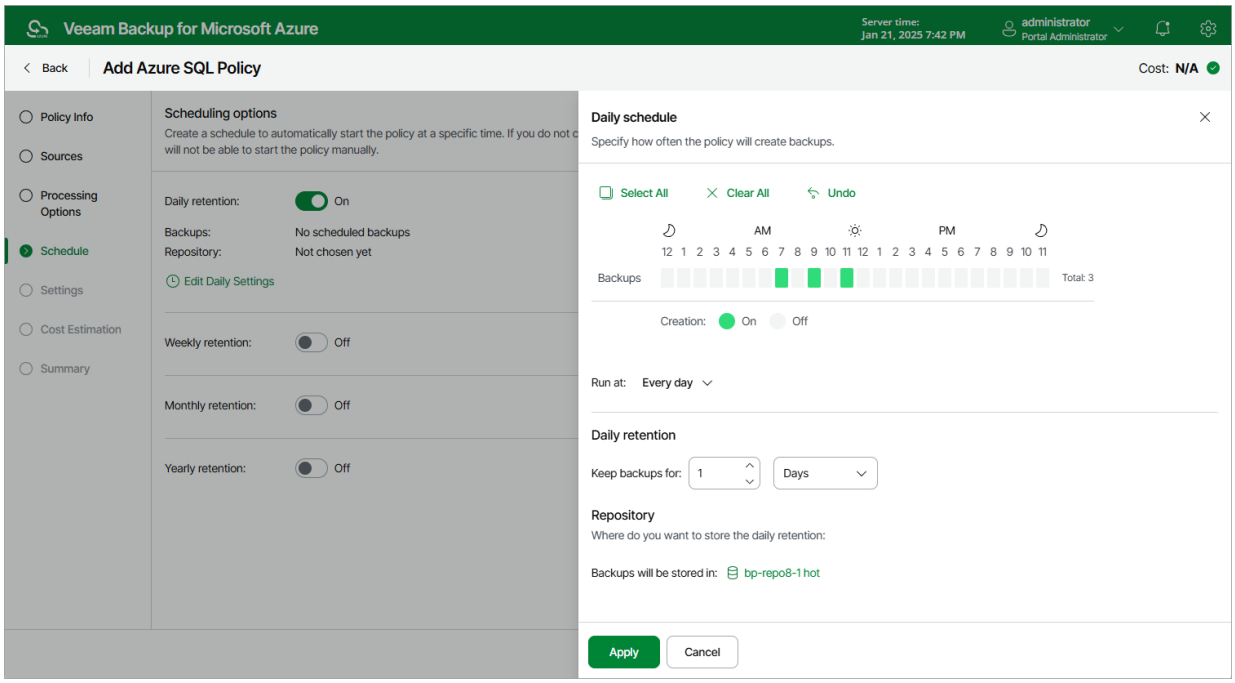
> **NOTE**
>
> Since Veeam Backup for Microsoft Azure runs retention sessions at 12:15 AM according to the time zone set on the backup appliance, it is not recommended that you schedule backup policies to execute at 12:15 AM. Otherwise, Veeam Backup for Microsoft Azure will not be able to run the retention sessions.

3. Use the **Run at** drop-down list to choose whether you want the backup policy to run every day, on weekdays (Monday through Friday) or on specific days.
4. In the **Daily retention** section, specify the number of days (or months) for which you want to keep restore points in a backup chain.

   If a restore point is older than the specified time limit, Veeam Backup for Microsoft Azure removes the restore point from the chain. For more information, see SQL Backup Retention.
5. In the **Repository** section, select a backup repository where the created backups will be stored.

   For a backup repository to be displayed in the **Repository** list, it must be added to Veeam Backup for Microsoft Azure as described in section Adding Backup Repositories.

6. To save changes made to the backup policy settings, click **Apply**.




## Specifying Weekly Schedule

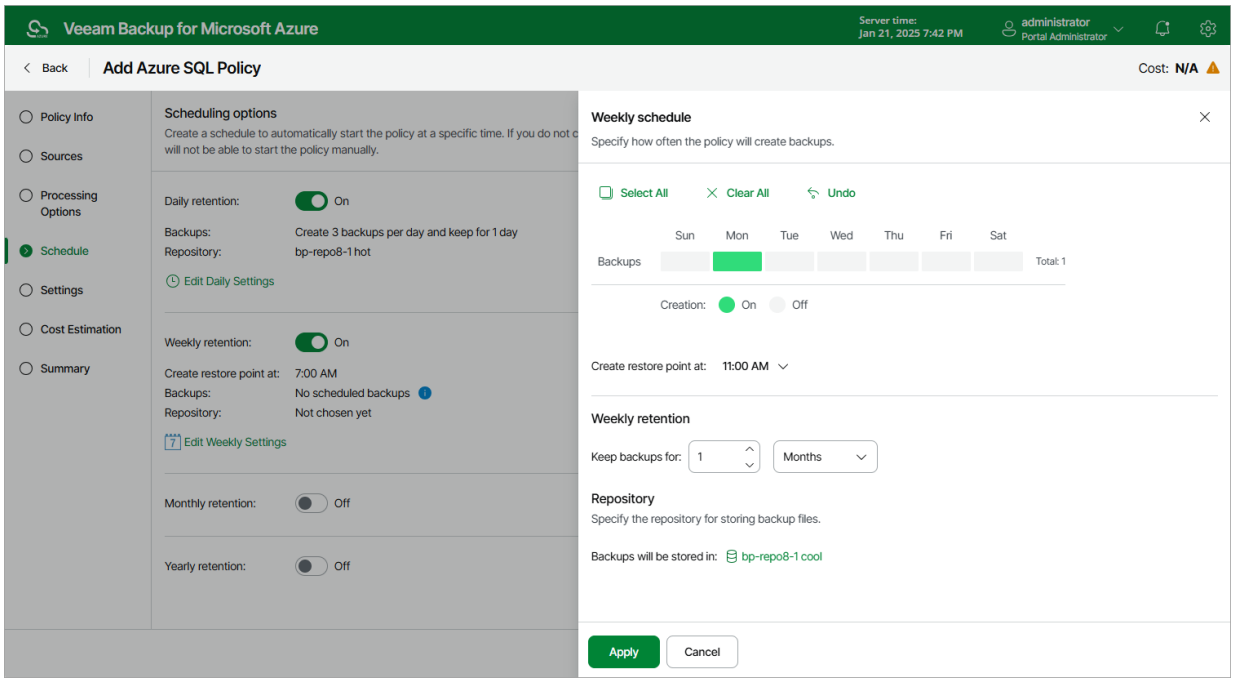
To create a weekly schedule for the backup policy, at the **Schedule** step of the wizard, do the following:

1. Set the **Weekly retention** toggle to *On* and click **Edit Weekly Settings**.
2. In the **Weekly schedule** window, select days of the week when the backup policy will create backups.
3. Use the **Create restore points at** drop-down list to schedule a specific time for the backup policy to run.
4. In the **Weekly retention** section, specify the number of days (or months) for which you want to keep restore points in a backup chain.

   If a restore point is older than the specified time limit, Veeam Backup for Microsoft Azure removes the restore point from the chain. For more information, see SQL Backup Retention.
5. In the **Repository** section, select a backup repository where the created backups will be stored.

   For a backup repository to be displayed in the **Repository** list, it must be added to Veeam Backup for Microsoft Azure as described in section Adding Backup Repositories.

6. To save changes made to the backup policy settings, click **Apply**.




## Specifying Monthly Schedule

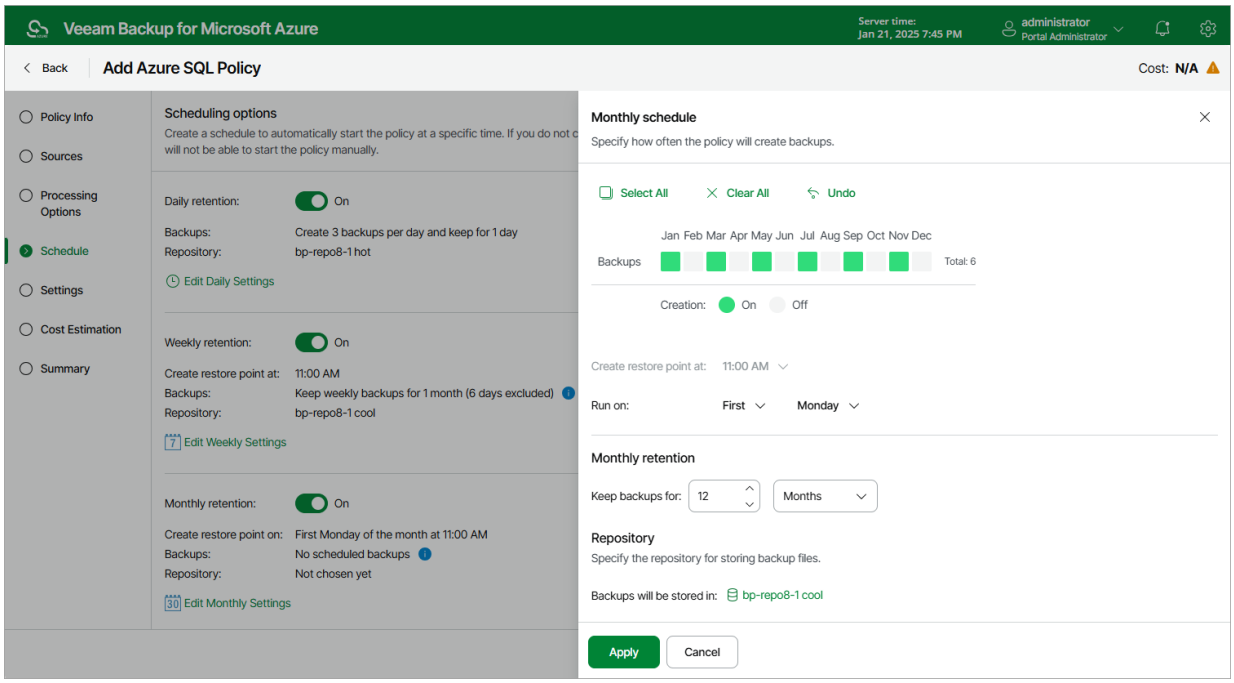
To create a monthly schedule for the backup policy, at the **Schedule** step of the wizard, do the following:

1. Set the **Monthly retention** toggle to *On* and click **Edit Monthly Settings**.
2. In the **Monthly schedule** window, select months when the backup policy will create backups.
3. Use the **Create restore points at** and **Run on** drop-down lists to schedule a specific time and day for the backup policy to run.
4. In the **Monthly retention** section, specify the number of days (or months) for which you want to keep restore points in a backup chain.

   If a restore point is older than the specified time limit, Veeam Backup for Microsoft Azure removes the restore point from the chain. For more information, see SQL Backup Retention.
5. In the **Repository** section, select a backup repository where the created backups will be stored.

   For a backup repository to be displayed in the **Repository** list, it must be added to Veeam Backup for Microsoft Azure as described in section Adding Backup Repositories.

6. To save changes made to the backup policy settings, click **Apply**.




## Specifying Yearly Schedule

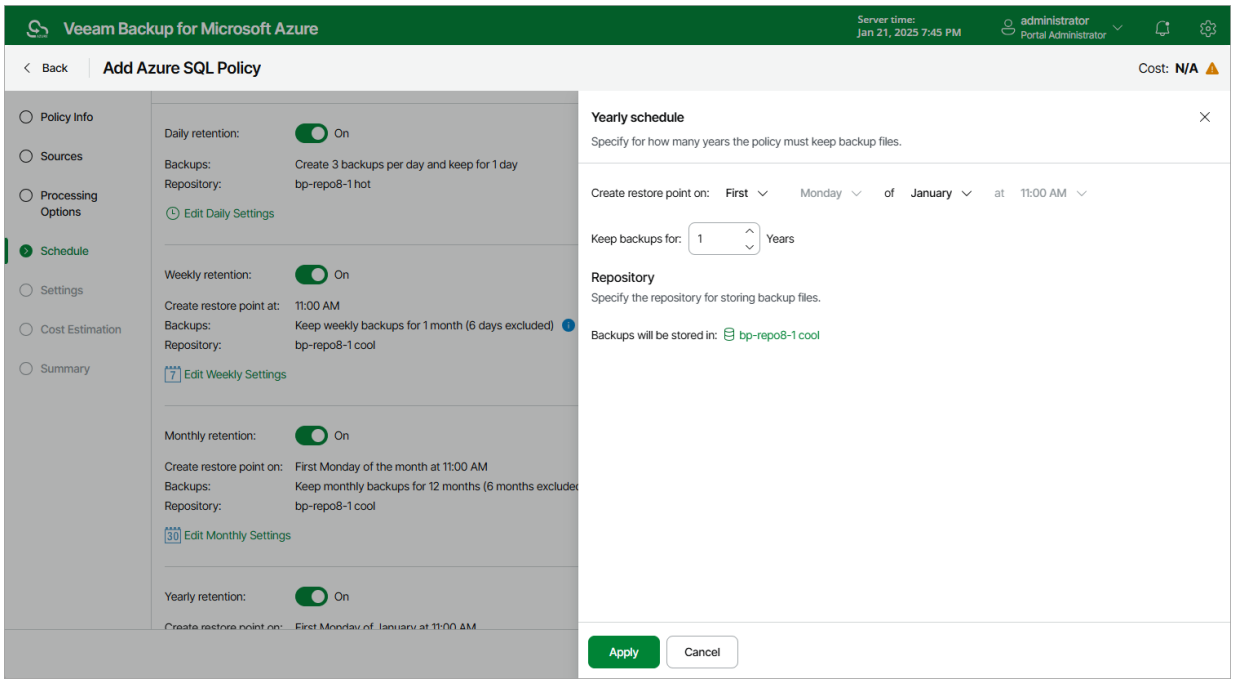
To create a yearly schedule for the backup policy, at the **Schedule** step of the wizard, do the following:

1. Set the **Yearly retention** toggle to *On* and click **Edit Yearly Settings**.
2. In the **Yearly schedule** window, specify a day, month and time when the backup policy will create backups.
3. In the **Keep backups for** field, specify the number of years for which you want to keep restore points in a backup chain.

   If a restore point is older than the specified time limit, Veeam Backup for Microsoft Azure removes the restore point from the chain. For more information, see SQL Backup Retention.
4. In the **Repository** section, select a backup repository where the created backups will be stored.

   For a backup repository to be displayed in the **Repository** list, it must be added to Veeam Backup for Microsoft Azure as described in section Adding Backup Repositories.

5. To save changes made to the backup policy settings, click **Apply**.




## Enabling Harmonized Scheduling

When you combine multiple types of schedules, Veeam Backup for Microsoft Azure applies the harmonization mechanism that allows you to leverage restore points for long-term retentions instead of taking a new restore point every time. The mechanism simplifies the backup schedule, optimizes the backup performance and reduces the cost of storing restore points in backup repositories.

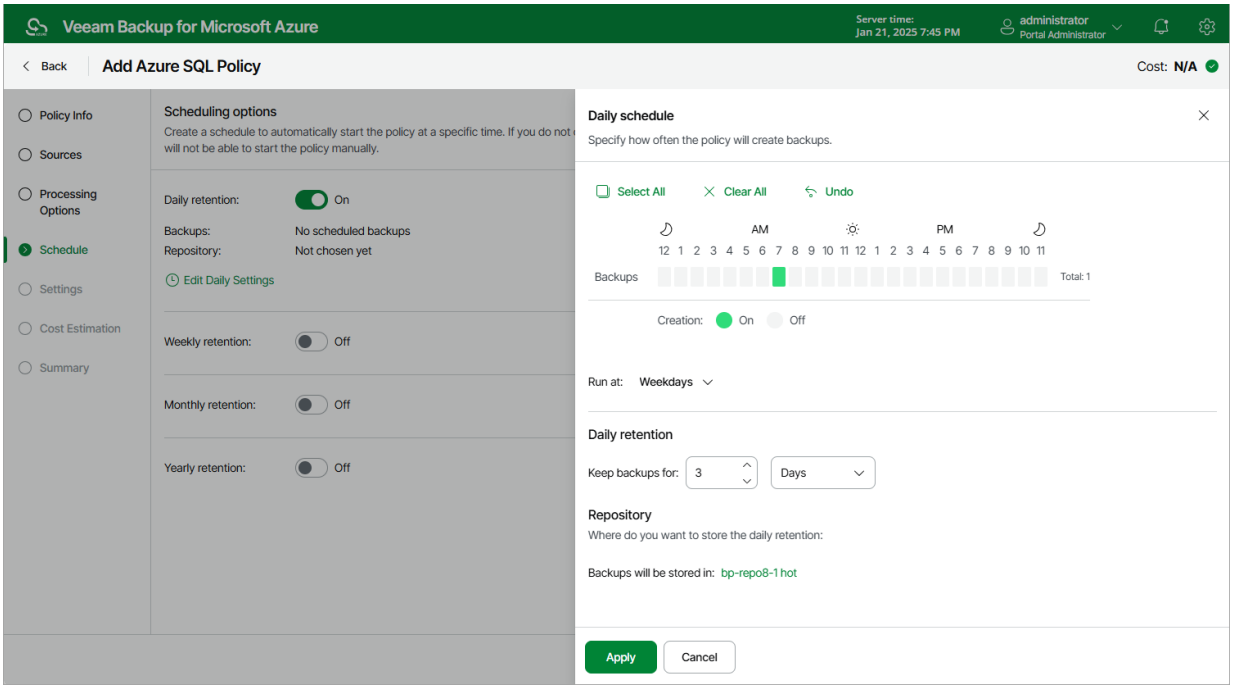
With harmonized scheduling, Veeam Backup for Microsoft Azure can keep restore points created according to a daily, weekly or monthly schedule for longer periods of time (for weeks, months and years).

For Veeam Backup for Microsoft Azure to use the harmonization mechanism, there must be specified at least 2 different schedules: one schedule will control the regular creation of restore points, while another schedule will control the process of retaining restore points. In terms of harmonized scheduling, Veeam Backup for Microsoft Azure re-uses restore points created according to a more-frequent schedule (daily, weekly or monthly) to achieve the desired retention for less-frequent schedules (weekly, monthly and yearly). Each restore point is marked with a flag of the related schedule type: the (Daily) flag is used to mark restore points created daily, (Weekly) — weekly, (Monthly) — monthly, and (Yearly) — yearly. Veeam Backup for Microsoft Azure uses these flags to control the retention period for the created restore points. Once a flag of a less-frequent schedule is assigned to a restore point, this restore point can no longer be removed — it is kept for the period defined in the retention settings. When the specified retention period is over, the flag is unassigned from the restore point. If the restore point does not have any other flags assigned, it is removed according to the retention settings of a more-frequent schedule.

Consider the following example. You want a backup policy to create backups of your critical workloads once a day, to keep 3 daily backups in the backup chain, and also to keep one of the created backups for 2 weeks. In this case, you create 2 schedules when configuring the backup policy settings — daily and weekly:

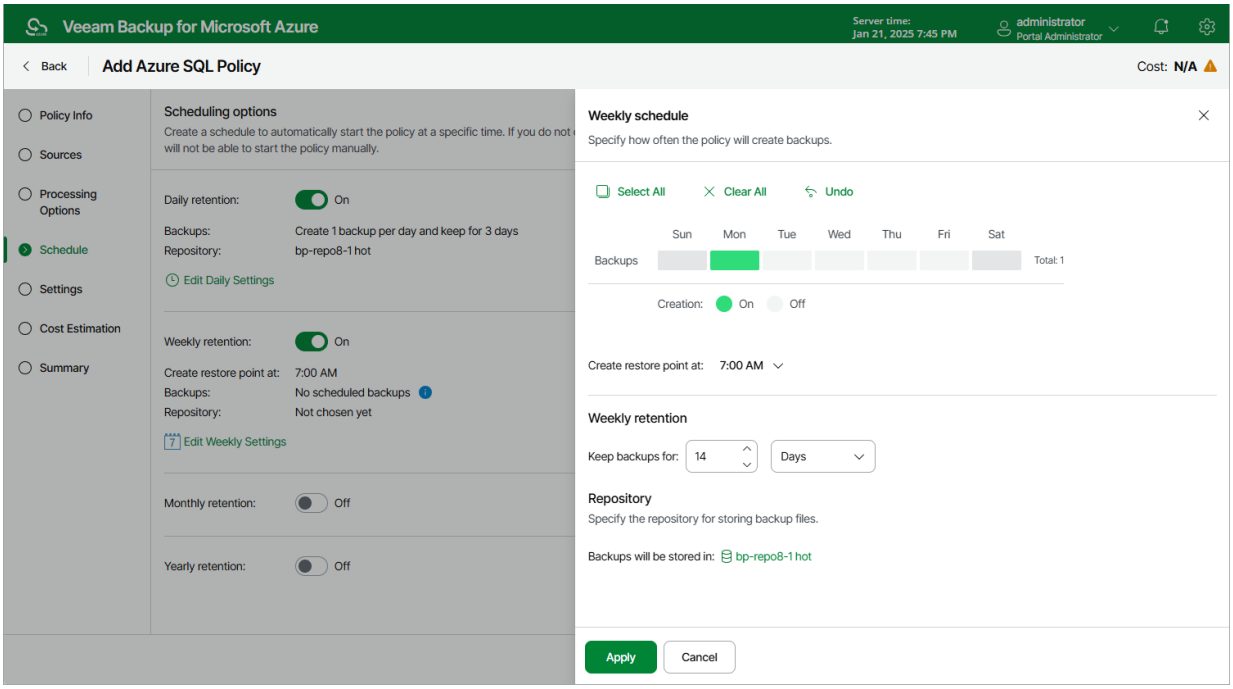
1. In the daily scheduling settings, you select hours and days when backups will be created (for example, *7:00 AM*; *Weekdays*), and specify the number of days for which you want to retain daily restore points in a backup chain (for example, *3*).

   Veeam Backup for Microsoft Azure will propagate these settings to the schedule with a lower frequency (which is the weekly schedule in our example).




2. In the weekly scheduling settings, you specify which one of the backups created by the daily schedule will be retained for a longer period, and choose for how long you want to keep the selected backup.

   For example, if you want to keep the daily restore point created on Monday for 2 weeks, you select *7:00 AM*, *Monday* and specify *14 days* in the weekly schedule settings.

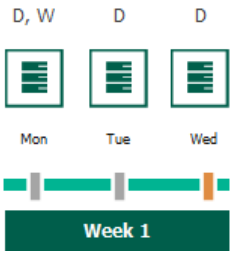


According to the specified scheduling settings, Veeam Backup for Microsoft Azure will create image-level backups in the following way:

1. On the first work day (Monday), a backup session will start at 7:00 AM to create the first restore point. The restore point will be marked with the (D) flag as it was created according to the daily schedule.

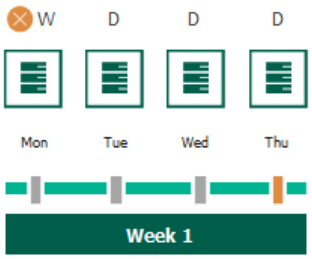
   Since *7:00 AM*, *Monday* is specified in weekly schedule settings, Veeam Backup for Microsoft Azure will assign the (W) flag to this restore point.

2. On the same week, after backup sessions run on Tuesday and Wednesday, the created restore points will be marked with the (D) flag.



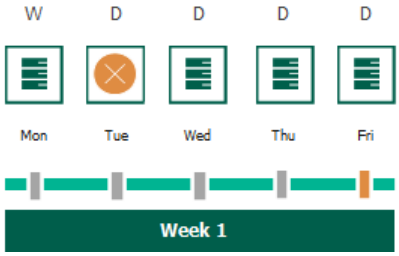

3. On the fourth work day (Thursday), after a backup session runs at 7:00 AM, the created restore point will be marked with the (D) flag.

   By this moment, the earliest restore point in the backup chain will get older than the specified retention limit. However, Veeam Backup for Microsoft Azure will not remove the earliest restore point (*7:00 AM*, *Monday*) with the (D) flag from the backup chain as this restore point is also marked with a flag of a less-frequent schedule. Instead, Veeam Backup for Microsoft Azure will unassign the (D) flag from the restore point. This restore point will be kept for the retention period specified in the weekly scheduling settings (that is, for 2 weeks).



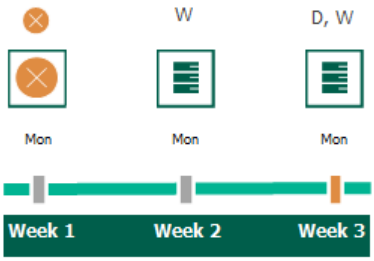

4. On the fifth working day (Friday), after a backup session runs at 7:00 AM, the created restore point will be marked with the (D) flag.

   By this moment, the restore point created on Tuesday with the (D) flag will get older than the specified retention limit. Veeam Backup for Microsoft Azure will remove from the backup chain the restore point created at 7:00 AM on Tuesday as no flags of a less-frequent schedule are assigned to this restore point.




5. Veeam Backup for Microsoft Azure will continue creating restore points for the next week in the same way as described in steps 1-4.

6. On week 3, after a backup session runs at 7:00 AM on Monday, the earliest weekly restore point in the backup chain will get older than the specified retention limit. Veeam Backup for Microsoft Azure will unassign the (W) flag from the earliest weekly restore point. Since no other flags are assigned to this restore point, Veeam Backup for Microsoft Azure will remove this restore point from the backup chain.




> **NOTE**
>
> This section does not explain how Veeam Backup for Microsoft Azure rebuilds the backup chain when applying the configured retention policy settings — it focuses on the harmonization mechanism itself only. To learn what types of backups Veeam Backup for Microsoft Azure includes in the backup chain and how it transforms the chain when removing outdated restore points, see sections Backup Chain and SQL Backup Retention.

## Enabling Backup Archiving

When you combine multiple types of schedules, you can enable the archiving mechanism to instruct Veeam Backup for Microsoft Azure to store backed-up data in the low-cost, long-term Archive access tier. The mechanism is the most useful in the following cases:

- Your data retention policy requires that you keep rarely accessed data in an archive.
- You want to reduce data-at-rest costs and to save space in the high-cost, short-term Hot and Cool access tiers.

> **NOTE**
>
> Restoring from an archived backup is longer and more expensive than restoring from a regular backup as it is required to retrieve data from the archive repository. For more information, see Retrieving Data From Archive.

With backup archiving, Veeam Backup for Microsoft Azure can retain backups created according to a daily, weekly or monthly schedule for longer periods of time:

- To enable monthly archiving, you must configure a daily or a weekly schedule (or both).
- To enable yearly archiving, you must configure a daily, a weekly or a monthly schedule (or all three).

For Veeam Backup for Microsoft Azure to use the archiving mechanism, there must be specified at least 2 different schedules: one schedule will control the regular creation of backups, while another schedule will control the process of copying backups to an archive repository. Backup chains created according to these two schedules will be completely different — for more information, see Backup Chain and Archive Backup Chain.

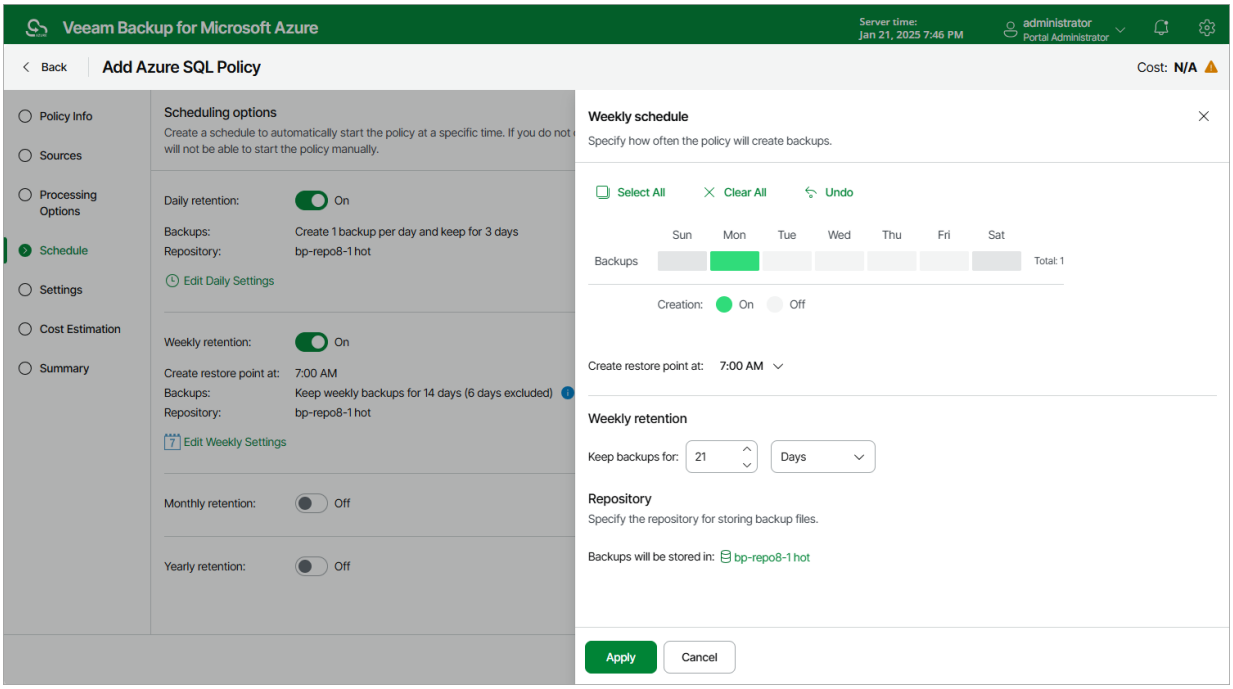
Consider the following example. You want a backup policy to create backups of your critical workloads once a week, to keep the backed-up data in a backup repository for 3 weeks, and also to keep backups created once in 2 months in an archive repository for a year. In this case, you create 2 schedules when configuring the backup policy settings — weekly and monthly:

1. In the weekly scheduling settings, you do the following:

   a. Specify hours and days when backups will be created (for example, *7:00 AM, Monday*), and specify the number of days for which Veeam Backup for Microsoft Azure will retain backups (for example, *21 days*).

   b. Select a repository of the Hot or Cool access tier that will store regular backups.

   Veeam Backup for Microsoft Azure will propagate these settings to the archive schedule (which is the monthly schedule in our example).




2. In the monthly scheduling settings, you do the following:

   a. Specify when Veeam Backup for Microsoft Azure will create archive backups, and choose for how long you want to retain the created backups (for example, *January, March, May, July, September, November, 12 months* and *First Monday*).

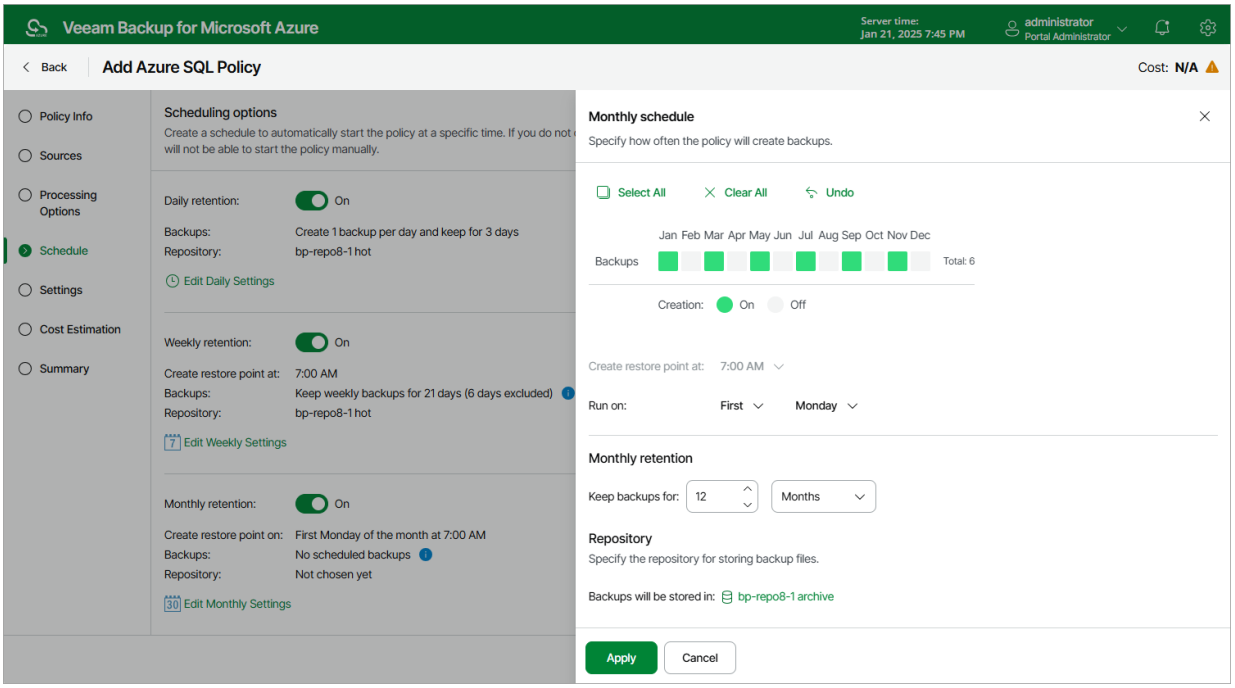
   b. Enable the archiving mechanism by selecting a repository of the Archive access tier that will store archived data.

   Note that when you enable backup archiving, you become no longer able to create a schedule of the same frequency for regular backups. By design, these two functionalities are mutually exclusive.

**IMPORTANT**

If you enable backup archiving, consider the following:

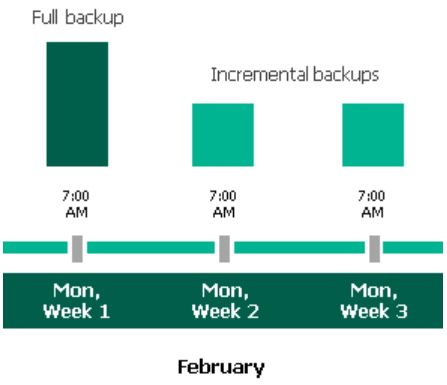
- It is recommended that you set the **Keep backups for** value to at least *6 months* (or *180 days*), since the minimum storage duration of the Archive access tier is 180 days.
- If you select the **On Day** option, harmonized scheduling cannot be guaranteed. Plus, to support the **On Day** option, Veeam Backup for Microsoft Azure will require to create an additional temporary restore point if there are no other schedules planned to run on that day. However, the temporary restore point will be removed during the *Backup Retention* process from Microsoft Azure Storage in approximately 24 hours, to reduce unexpected infrastructure charges.




According to the specified scheduling settings, Veeam Backup for Microsoft Azure will create image-level backups in the following way:

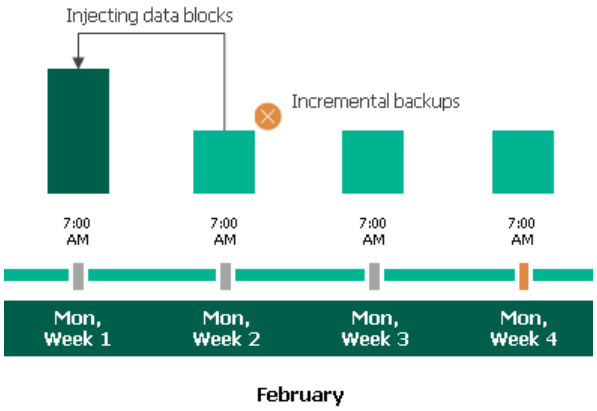
1. On the first Monday of February, a backup session will start at 7:00 AM to create the first restore point in the regular backup chain. Veeam Backup for Microsoft Azure will store this restore point as a full backup in the backup repository.

2. On the second and third Mondays of February, Veeam Backup for Microsoft Azure will create restore points at 7:00 AM and add them to the regular backup chain as incremental backups in the backup repository.



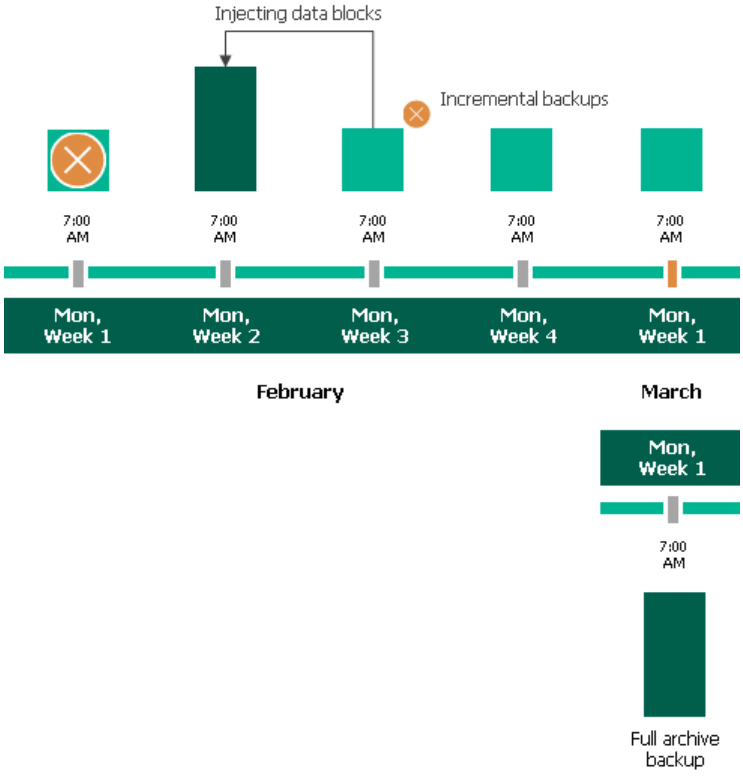
3. On the fourth Monday of February, Veeam Backup for Microsoft Azure will create a new restore point at 7:00 AM. By the moment the backup session completes, the earliest restore point in the regular backup chain will get older than the specified retention limit. That is why Veeam Backup for Microsoft Azure will rebuild the full backup and remove from the chain the restore point created on the first Monday.

   For more information on how Veeam Backup for Microsoft Azure transforms regular backup chains, see SQL Backup Retention.



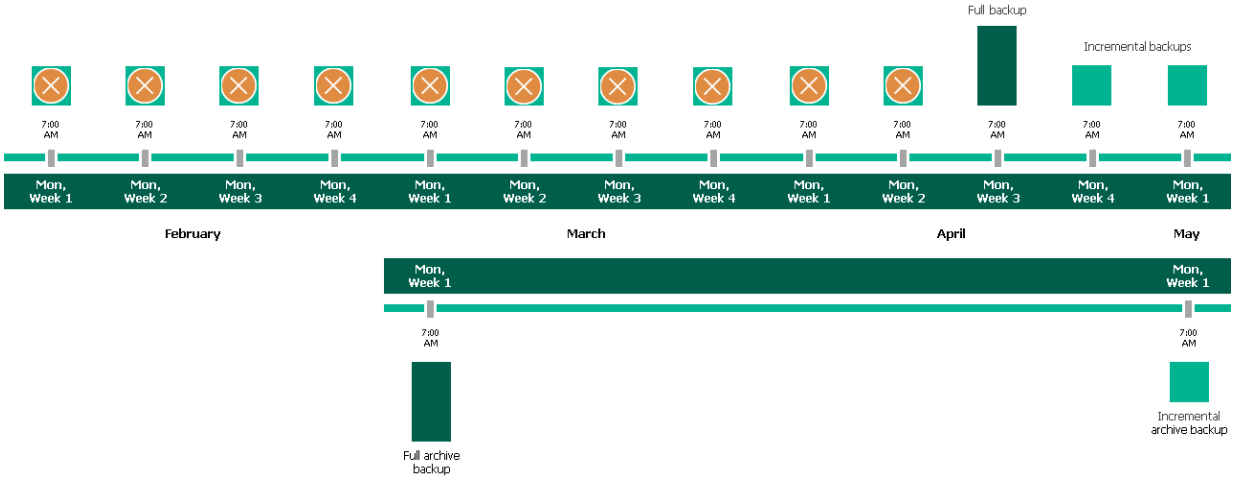

4. On the first Monday of March, a backup session will start at 7:00 AM to create another restore point in the regular backup chain. At the same time, the earliest restore point in the regular backup chain will get older than the specified retention limit again. That is why Veeam Backup for Microsoft Azure will rebuild the full backup again and remove from the chain the restore point created on the second Monday.

   After the backup session completes, an archive session will create a restore point with all data from the regular backup chain. Veeam Backup for Microsoft Azure will copy this restore point as a full archive backup to the archive repository.



5. Up to May, Veeam Backup for Microsoft Azure will continue adding new restore points to the regular backup chain and deleting outdated backups from the backup repository, according to the specified weekly scheduling settings.

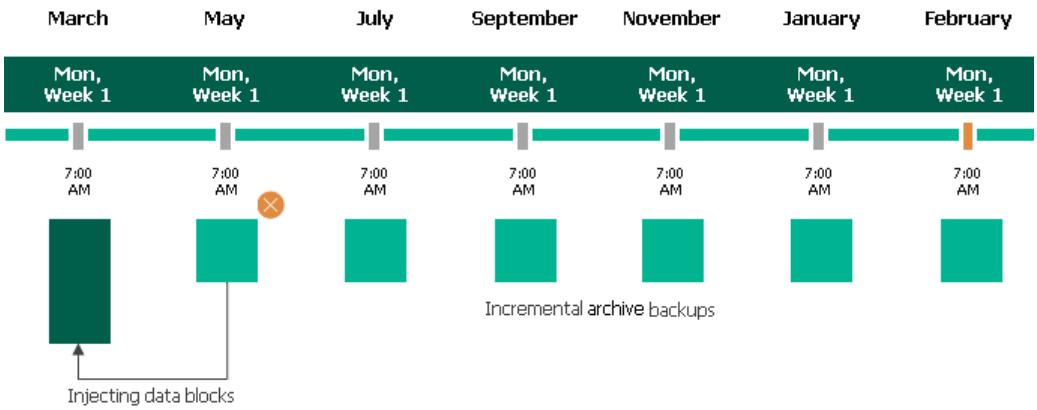
   On the first Monday of May, an archive session will create a restore point with only that data that has changed since the previous archive session in March. Veeam Backup for Microsoft Azure will copy this restore point as an incremental archive backup to the archive repository.




6. Up to the first Monday of February of the next year, Veeam Backup for Microsoft Azure will continue adding new restore points to the regular backup chain and deleting outdated backups from the backup repository, according to the specified weekly scheduling settings. Veeam Backup for Microsoft Azure will also continue adding new restore points to the archive backup chain, according to the specified monthly settings.

   By the moment the archive session completes, the earliest restore point in the archive backup chain will get older than the specified retention limit. That is why Veeam Backup for Microsoft Azure will rebuild the full archive backup and remove from the chain the restore point created on the first Monday of March of the previous year.

   For more information on how Veeam Backup for Microsoft Azure transforms archive backup chains, see Retention Policy for Archived Backups.



Data encryption must be either enabled or disabled for both backup and archive backup repositories selected within the same backup archiving configuration. This means that, for example, you cannot select an encrypted standard backup repository and an unencrypted archive backup repository to store backups. However, you can select repositories with different data encryption configuration in one backup policy. That is, you can select an encrypted standard backup repository, an encrypted archive backup repository, an unencrypted standard backup repository and an unencrypted archive backup repository — in this case, backups created in the encrypted standard backup repository, will be copied to the encrypted archive backup repository, and backups created in the unencrypted standard backup repository, will be copied to the unencrypted archive backup repository. Also, the selected repositories can have different encryption options (password and Azure Key Vault cryptographic key encryption).

## Step 6. Configure General Settings

At the **Settings** step of the wizard, you can enable automatic retries, schedule health checks and specify notification settings for the backup policy.

# Automatic Retry Settings

To instruct Veeam Backup for Microsoft Azure to run the backup policy again if it fails on the first try, do the following:

1. In the **Schedule** section of the step, select the **Automatic retry failed policy** check box.
2. In the field to the right of the check box, specify the maximum number of attempts to run the backup policy. The time interval between retries is 600 seconds.

When retrying backup policies, Veeam Backup for Microsoft Azure processes only those Azure SQL databases that failed to be backed up during the previous attempt.

> **NOTE**
>
> The automatic retry settings apply only to backup policies that run according to specific schedules — these settings do not apply to policies started manually.

# Health Check Settings

Veeam Backup for Microsoft Azure can periodically perform a health check for all restore points created by the backup policy. During the health check, Veeam Backup for Microsoft Azure performs an availability check for data blocks in the whole regular backup chain, and a cyclic redundancy check (CRC) for metadata to verify its integrity. The health check helps you ensure that the restore points are consistent and that you will be able to restore data using these restore points. For more information on the health check, see How Health Check Works.

> **NOTE**
>
> During a health check, Veeam Backup for Microsoft Azure does not verify archived restore points created by the policy.

To instruct Veeam Backup for Microsoft Azure to perform a health check, do the following:

1. In the **Health check** section of the step, set the **Enable health check** toggle to *On*.
2. Use the **Run on** drop-down lists to schedule a specific day for the health check to run.

> **NOTE**
>
> Veeam Backup for Microsoft Azure performs the health check during the last policy session that runs on the day when the health check is scheduled. If another backup policy session runs on the same day, Veeam Backup for Microsoft Azure will not perform the health check during that session. For example, if the backup policy is scheduled to run multiple times on Saturday, and the health check is also scheduled to run on Saturday, the health check will only be performed during the last policy session on Saturday.

# Notification Settings

To instruct Veeam Backup for Microsoft Azure to send email notifications for the backup policy, do the following:

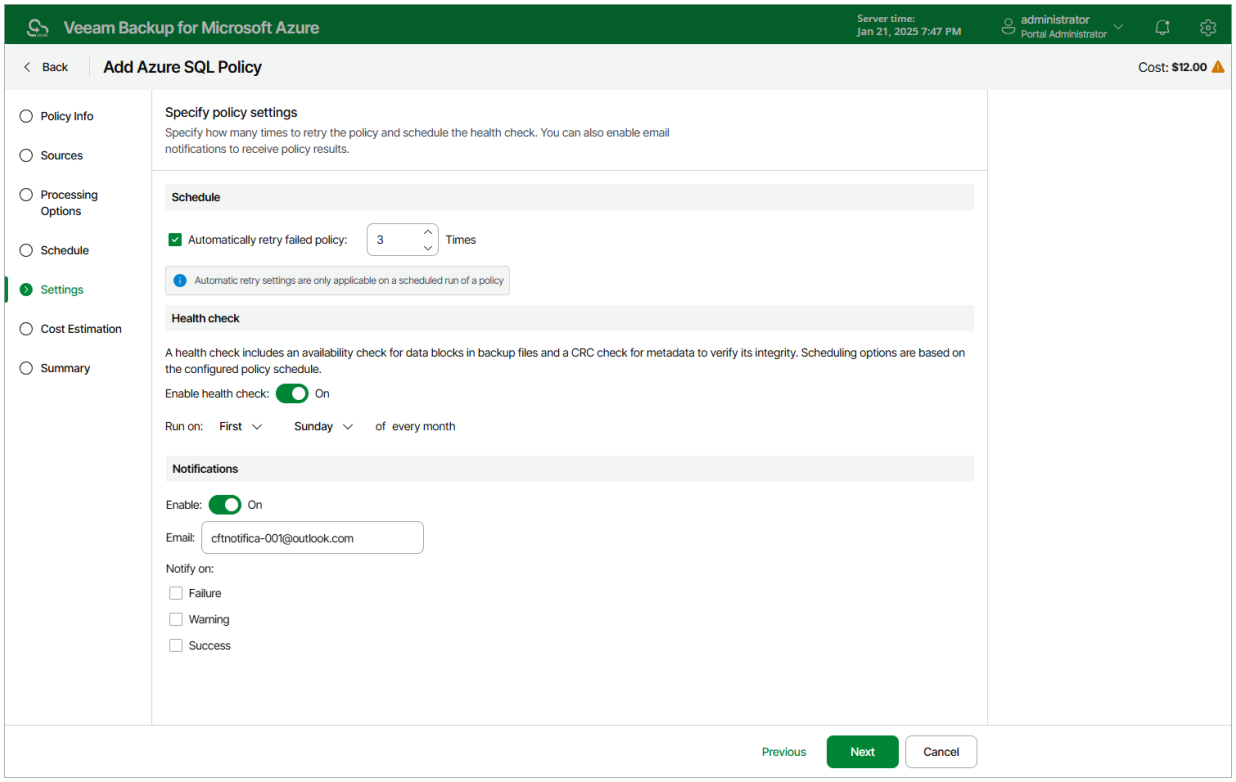
1. In the **Notifications** section of the step, set the **Enabled** toggle to *On*.

   If you set the toggle to *Off*, Veeam Backup for Microsoft Azure will not send any notifications for this backup policy — regardless of the configured global notification settings.

2. In the **Email** field, specify an email address of a recipient. Use a semicolon to separate multiple recipient addresses.

3. Use the **Notify on** list to choose whether you want Veeam Backup for Microsoft Azure to send email notifications in case the backup policy completes successfully, completes with warnings or completes with errors.

> **NOTE**
>
> If you specify the same email recipient in both backup policy notification and global notification settings, Veeam Backup for Microsoft Azure will override the configured global notification settings and will send each notification to this recipient only once to avoid notification duplicates.




## How Health Check Works

When Veeam Backup for Microsoft Azure saves a new backup restore point to a backup repository, it calculates CRC values for metadata in the backup chain and saves these values to the chain metadata, together with the instance data. When performing a health check, Veeam Backup for Microsoft Azure verifies the availability of data blocks and uses the saved values to ensure that the restore points being verified are consistent.

If you have enabled health checks for the backup policy, Veeam Backup for Microsoft Azure performs the following operations at the day scheduled for a health check to run:

1. As soon as a backup policy session completes successfully, Veeam Backup for Microsoft Azure starts the health check as a new session. For each restore point in the standard backup chain, Veeam Backup for Microsoft Azure calculates CRC values for backup metadata and compares them to the CRC values that were previously saved to the restore point. Veeam Backup for Microsoft Azure also checks whether data blocks that are required to rebuild the restore point are available.

   If the backup policy session completes with an error, Veeam Backup for Microsoft Azure tries to run the backup policy again, taking into account the maximum number of retries specified in the automatic retry settings. After the first successful retry (or after the last one out of the maximum number of retries), Veeam Backup for Microsoft Azure starts the health check.

2. If Veeam Backup for Microsoft Azure does not detect data inconsistency, the health check session completes successfully. Otherwise, the session completes with an error.

   Depending on the detected data inconsistency, Veeam Backup for Microsoft Azure performs the following operations:

   - If the health check detects corrupted metadata in a full or incremental restore point, Veeam Backup for Microsoft Azure marks the backup chain as corrupted in the configuration database. During the next backup policy session, Veeam Backup for Microsoft Azure copies the full instance image, creates a full restore point in the backup repository and starts a new backup chain in the backup repository.

> **NOTE**
>
> Veeam Backup for Microsoft Azure does not support metadata check for encrypted backup chains.

   - If the health check detects corrupted disk blocks in a full or an incremental restore point, Veeam Backup for Microsoft Azure marks the restore point that includes the corrupted data blocks and all subsequent incremental restore points as incomplete in the configuration database. During the next backup policy session, Veeam Backup for Microsoft Azure copies not only those data blocks that have changed since the previous backup session but also data blocks that have been corrupted, and saves these data blocks to the latest restore point that has been created during the current session.

# Step 7. Review Estimated Cost

At the **Cost Estimation** step of the wizard, review the approximate monthly cost of Azure services that Veeam Backup for Microsoft Azure will require to protect the Azure SQL databases added to the backup policy. The total estimated cost includes the following:

- The cost of creating and maintaining backups of the Azure SQL databases.

  For each Azure SQL database included in the backup policy, Veeam Backup for Microsoft Azure takes into account the size of the database and the configured scheduling settings.

- The cost of transferring Azure SQL database data between Azure regions during data protection operations (for example, if a protected Azure SQL database and the target storage account reside in different regions).

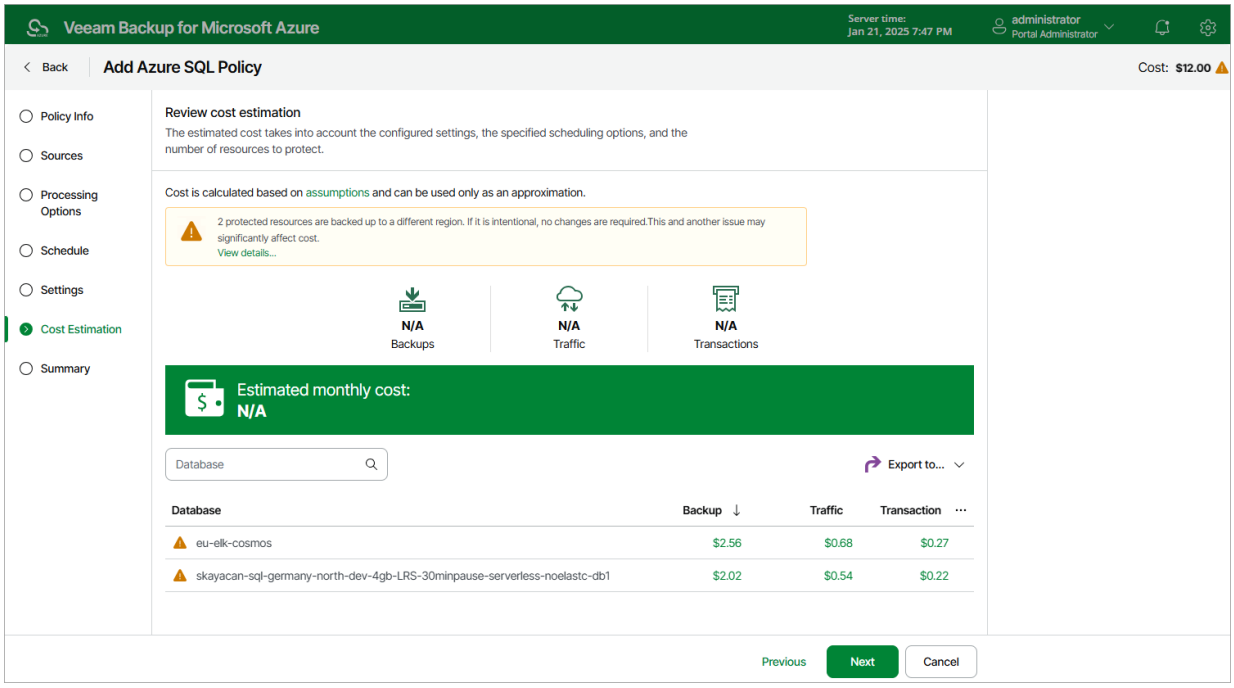
  If you get a warning message regarding additional costs associated with cross-region data transfer, you can click **View details** to see available cost-effective options.

- The cost of making API requests to Microsoft Azure during data protection operations.

> **NOTE**
>
> To calculate the estimated cost, Veeam Backup for Microsoft Azure uses the capabilities of the Azure Pricing Calculator that estimates the cost of services in USD only. This calculator is intended for informational and estimation purposes only.

The estimated cost may occur to be significantly higher due to the backup frequency and cross-region data transfer. To reduce the cost, you can try the following workarounds:

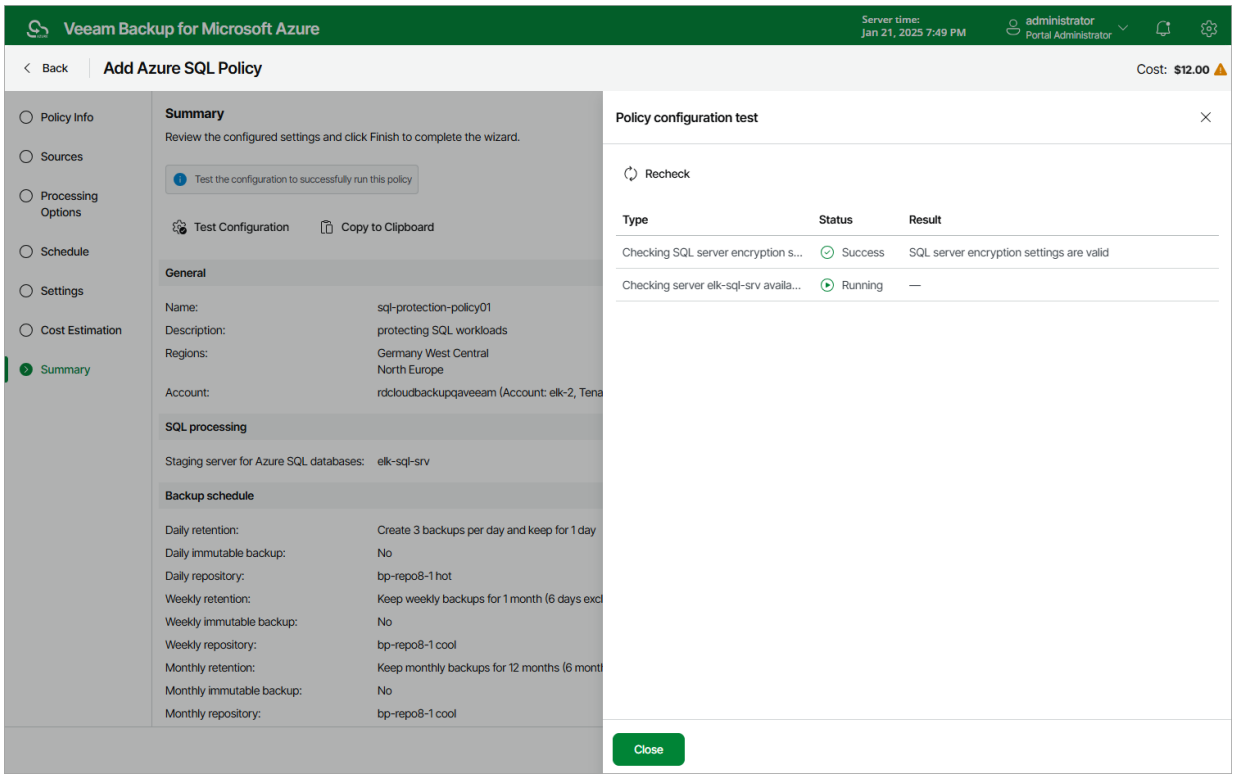
- To avoid additional costs related to cross-region data transfer, select a backup repository that resides in the same region as Azure SQL databases that you plan to back up.
- To optimize the cost of storing backups, modify the scheduling settings to run the backup policy less frequently, or specify an archive repository for long-term retention of restore points.



# Step 8. Finish Working with Wizard

At the **Summary** step of the wizard, it is recommended that you run the backup policy configuration check before you click **Finish**.

The configuration check will verify whether the specified accounts have all the required permissions, and networks settings are configured properly to launch worker instances. To run the configuration check, click **Test Configuration**. Veeam Backup for Microsoft Azure will display the **Policy configuration test** window where you can view the progress and results of the performed check. If the account permissions are insufficient or worker instance settings are not configured properly, the check will complete with errors.




If the configuration check discovers that network settings are not configured properly, Veeam Backup for Microsoft Azure will not be able to launch worker instances and thus perform the backup. To fix the network issues, do the following:

1. Close the **Policy configuration test** window, and then click **Finish** to close the **Add Azure SQL Policy** wizard.

   Veeam Backup for Microsoft Azure will save the configured backup policy.

2. To prevent the backup policy from failing, disable it as described in section Enabling and Disabling Backup Policies.

3. Depending on the error message received during the configuration check, do the following:

   - Make sure that network settings are configured for each Azure region selected at step 3b. For information on how to configure network settings for Azure regions, see Managing Worker Instances.
   - Make sure that the virtual networks specified in the network settings for the Azure regions have access to the required Azure services. For more information on the required Azure services, see Azure Services.

4. After the network issues are fixed, you can enable the backup policy as described in section Enabling and Disabling Backup Policies.

# Creating SQL Backups Manually

Veeam Backup for Microsoft Azure allows you to manually create backups of Azure SQL databases.

> **NOTE**
>
> Veeam Backup for Microsoft Azure does not include backups of Azure SQL databases created manually in the backup chain and does not apply the configured retention policy settings to these backups. This means that the backups are kept in the backup repository unless you remove them manually, as described in section Managing SQL Data.

To manually create a backup of an Azure SQL database, do the following:

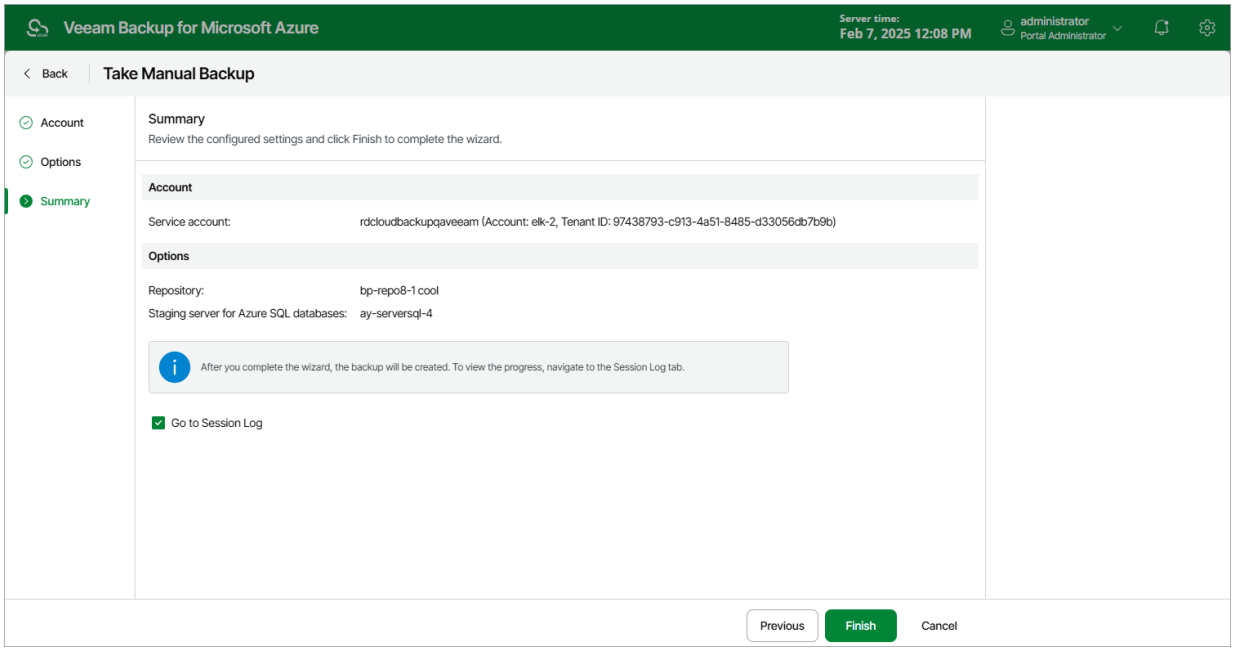
1. Navigate to **Resources** > **Databases** > **Azure SQL**.
2. Select the check box next to the necessary Azure SQL database and click **Take Backup Now**.

   For an Azure SQL database to be displayed in the list of available resources, it must reside in any region included in a backup policy as described in section Creating Backup Policies (step 3c).
3. Complete the **Take Manual Backup** wizard:
   a. At the **Account** step of the wizard, select a service account whose permissions Veeam Backup for Microsoft Azure will use to create a backup.

      For an account to be displayed in the accounts list, it must be added to Veeam Backup for Microsoft Azure as described in section Adding Service Accounts.
   b. At the **Options** step of the wizard, do the following:
      i. In the **Backup target** section, click **Choose backup repository**.

         In the **Specify the backup repository** window, select a backup repository where the created backup will be stored. For a backup repository to be displayed in the **Repository** list, it must be added to Veeam Backup for Microsoft Azure, must have the Hot or Cool access tier assigned and must have immutability disabled, as described in section Adding Backup Repositories.
      ii. In the **Specify database processing settings** section, choose whether you want to use a staging server to perform backup. For more information, see Configure Processing Options.

c. At the **Summary** step of the wizard, review configuration information, choose whether you want to proceed to the Session Log page to track the progress of backup creation, and click **Finish**.



# Performing Cosmos DB Backup

> **IMPORTANT**
>
> Cosmos DB backup is available only for backup appliances managed by a Veeam Backup & Replication server. To unlock the full functionality, you must install Microsoft Azure Plug-in for Veeam Backup & Replication on the server and add your appliances to the backup infrastructure.

One backup policy can be used to process one or more Cosmos DB accounts within one Microsoft Entra tenant. The scope of data that you can protect in a tenant is limited by permissions of a service account that is specified in the backup policy settings.

Before you create an Cosmos DB backup policy, check the following prerequisites:

- If you plan to enable backup to repository, backup infrastructure components that will take part in the backup process must be added to the backup infrastructure and configured properly. These include backup repositories and worker instances.
- If you plan to receive email notifications on backup policy results, configure email notification settings first. For more information, see Configuring Global Notification Settings.

To schedule data protection tasks to run automatically, create backup policies. For each protected Cosmos DB for PostgreSQL or Cosmos DB for MongoDB account, you can also take a backup to a repository manually when needed.

> **IMPORTANT**
>
> Consider the following:
>
> - Veeam Backup for Microsoft Azure allows you to protect only Cosmos DB accounts created using the following APIs: NoSQL, MongoDB RU-based, Apache Gremlin, Table and PostgreSQL.
> - Veeam Backup for Microsoft Azure does not support protecting Cosmos DB accounts that have periodic backup or multi-region writes enabled.

## Creating Cosmos DB Backup Policies

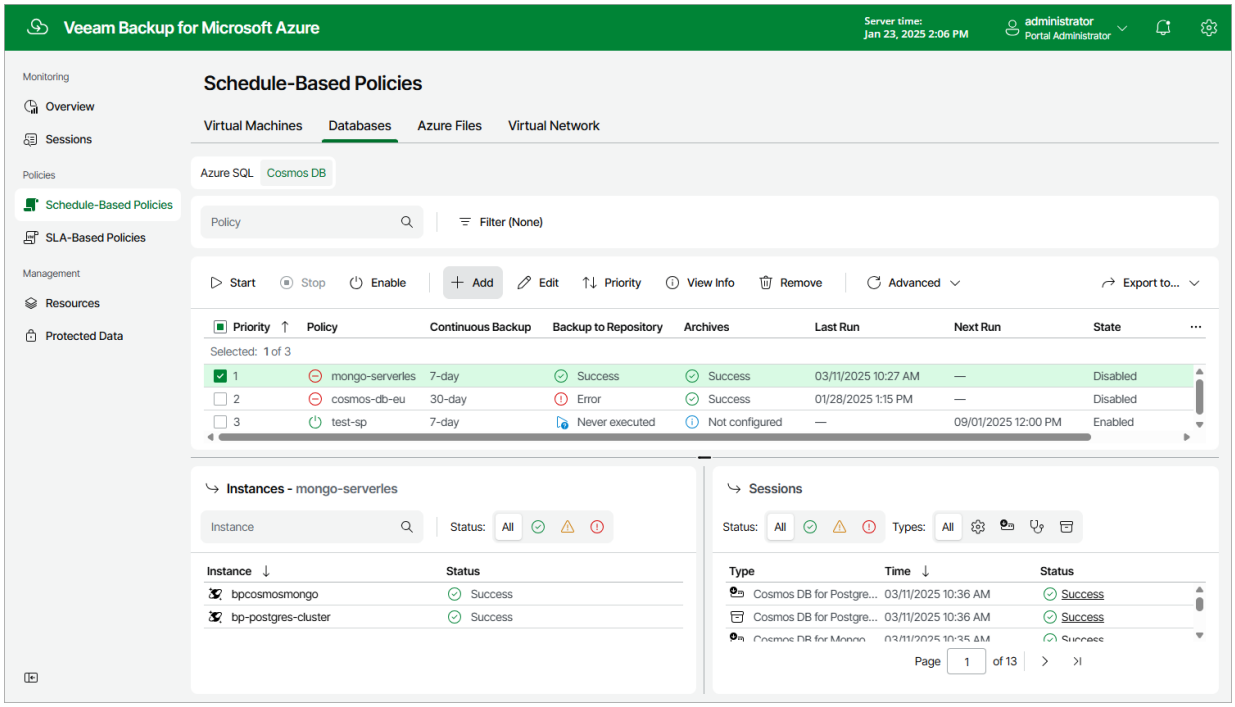
To create a backup policy, do the following:

1. Launch the Add Cosmos DB Policy wizard.
2. Specify a backup policy name and description.
3. Configure backup source settings.
4. Configure backup target settings.
5. Configure processing options.
6. Create a schedule for the backup policy.
7. Review the estimated cost of protecting the selected Cosmos DB accounts and databases.
8. Specify automatic retry, health check and notification settings for the backup policy.
9. Finish working with the wizard.

# Step 1. Launch Add Cosmos DB Policy Wizard

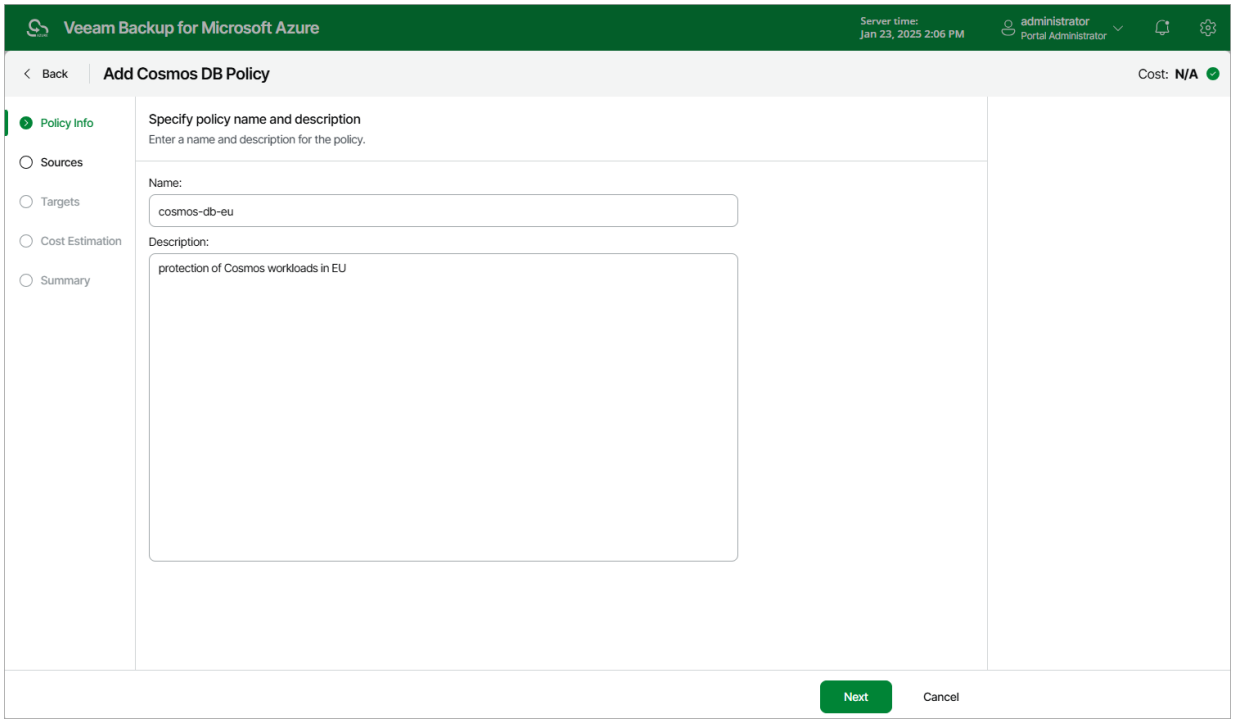
To launch the **Add Cosmos DB Policy** wizard, do the following:

1. Navigate to **Schedule-Based Policies**.
2. Switch to **Databases** > **Cosmos DB**.
3. Click **Add**.



# Step 2. Specify Backup Policy Name

At the **Policy Info** step of the wizard, use the **Name** and **Description** fields to enter a name for the new backup policy and to provide a description for future reference. The maximum length of the name is 255 characters. The following characters are not supported: / \ " ' : | < > + = ; , ? ! * % # ^ @ & $ .



## Step 3. Configure Backup Source Settings

At the **Sources** step of the wizard, specify the following backup source settings:

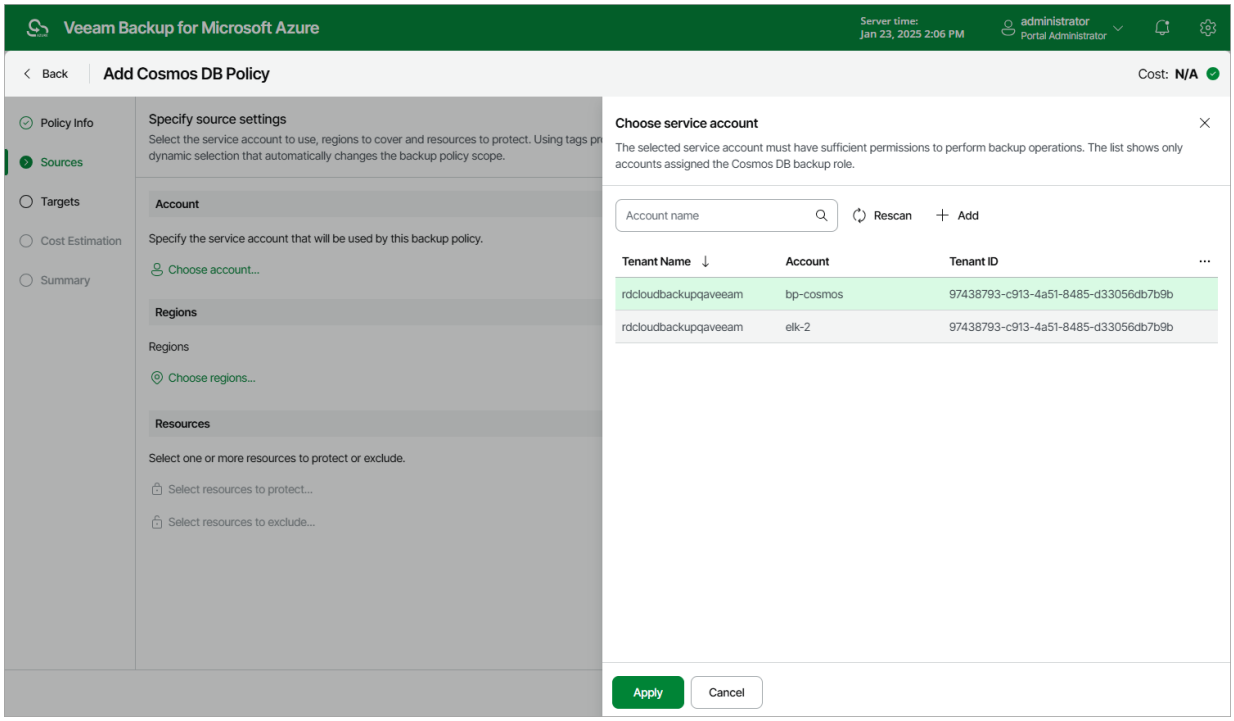
1. Select a service account whose permissions will be used to perform Cosmos DB backup.
2. Choose regions where Cosmos DB accounts that you want to back up reside.
3. Select resources to back up.

## Step 3a. Select Service Account

In the **Account** section of the **Sources** step of the wizard, specify a service account whose permissions will be used to access Azure services and resources, and to create backups of Cosmos DB accounts.

1. Click **Choose account**.
2. In the **Choose service account** window, select the necessary service account from the available accounts list. The specified service account must belong to the Microsoft Entra tenant that contains the Cosmos DB accounts that you want to protect, and must be assigned permissions listed in section Cosmos DB Permissions.

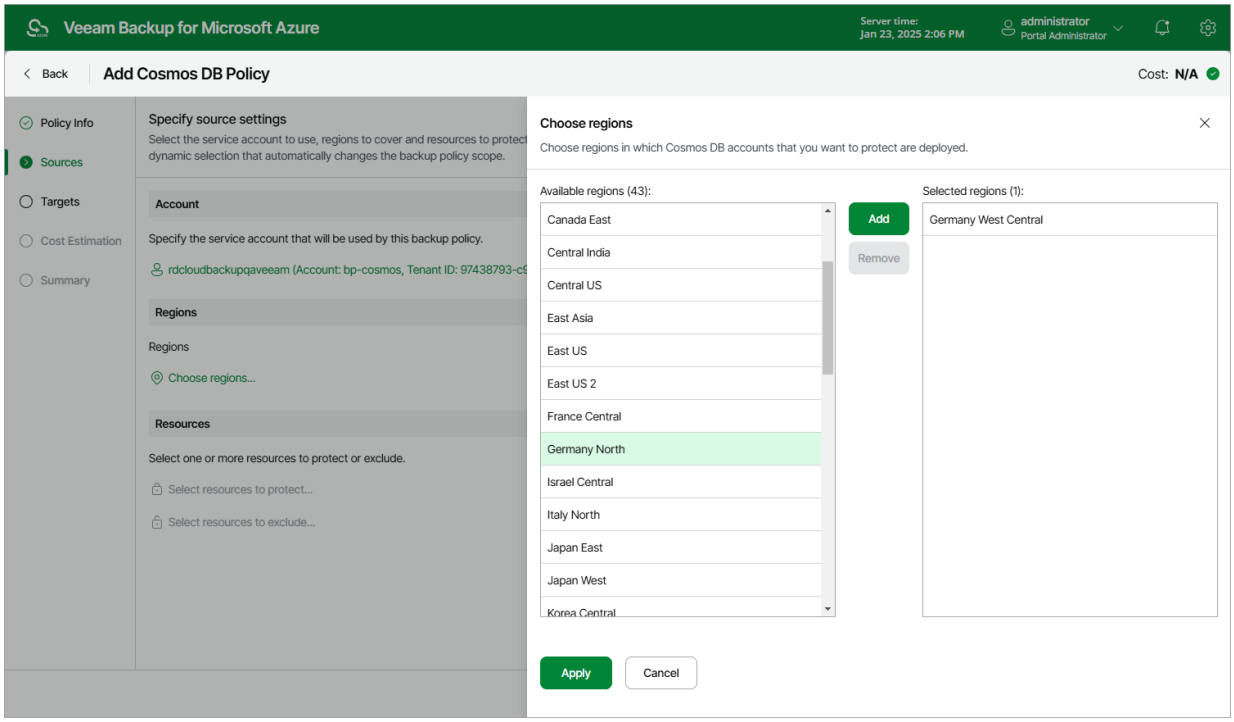
   For a service account to be displayed in the list of available accounts, it must be added to Veeam Backup for Microsoft Azure and assigned the *Cosmos DB Backup* operational role as described in section Adding Service Accounts. If you have not added the necessary service account to Veeam Backup for Microsoft Azure beforehand, you can do it without closing the **Add Cosmos DB Policy** wizard. To do that, click **Add** and complete the **Add Account** wizard.
3. Click **Apply**.



## Step 3b. Select Regions

In the **Region** section of the **Sources** step of the wizard, select regions where Azure resources that you want to back up reside.

1. Click **Choose regions**.
2. In the **Choose regions** window, select the necessary regions from the **Available regions** list, and then click **Add**.
3. Click **Apply**.



## Step 3c. Select Resources

In the **Resources** section of the **Sources** step of the wizard, specify the backup scope — select resources that Veeam Backup for Microsoft Azure will back up:

1. Click **Select resources to protect**.
2. In the **Choose resource protection options** window, choose whether you want to back up all Azure resources from the regions selected at step 3b, or only specific resources.

   If you select the **All resources** option, Veeam Backup for Microsoft Azure will regularly check for new Cosmos DB accounts created in the selected regions and automatically update the backup policy settings to include these databases in the backup scope.

   If you select the **Protect the following resources** option, you must also specify the resources explicitly:

   a. Use the **Resource type** drop-down list to select either of the following options:

      - *Subscription* — to back up Cosmos DB accounts managed by specific subscriptions.
      - *Resource group* — to back up Cosmos DB accounts that reside in a specific Azure resource group.
      - *Tag* — to back up Cosmos DB accounts with specific tags.
      - *Cosmos DB Account* — to back up only specific Cosmos DB accounts.

   b. Use the search field to the right of the **Resource type** list to find the necessary resource, and then click **Protect** to add the resource to the backup scope.

      For a resource to be displayed in the list of available resources, it must reside in an Azure region that has ever been specified in any backup policy. Otherwise, the only option to discover available resources is to click **Browse to select specific source from the global list** and wait for Veeam Backup for Microsoft Azure to populate the resource list.

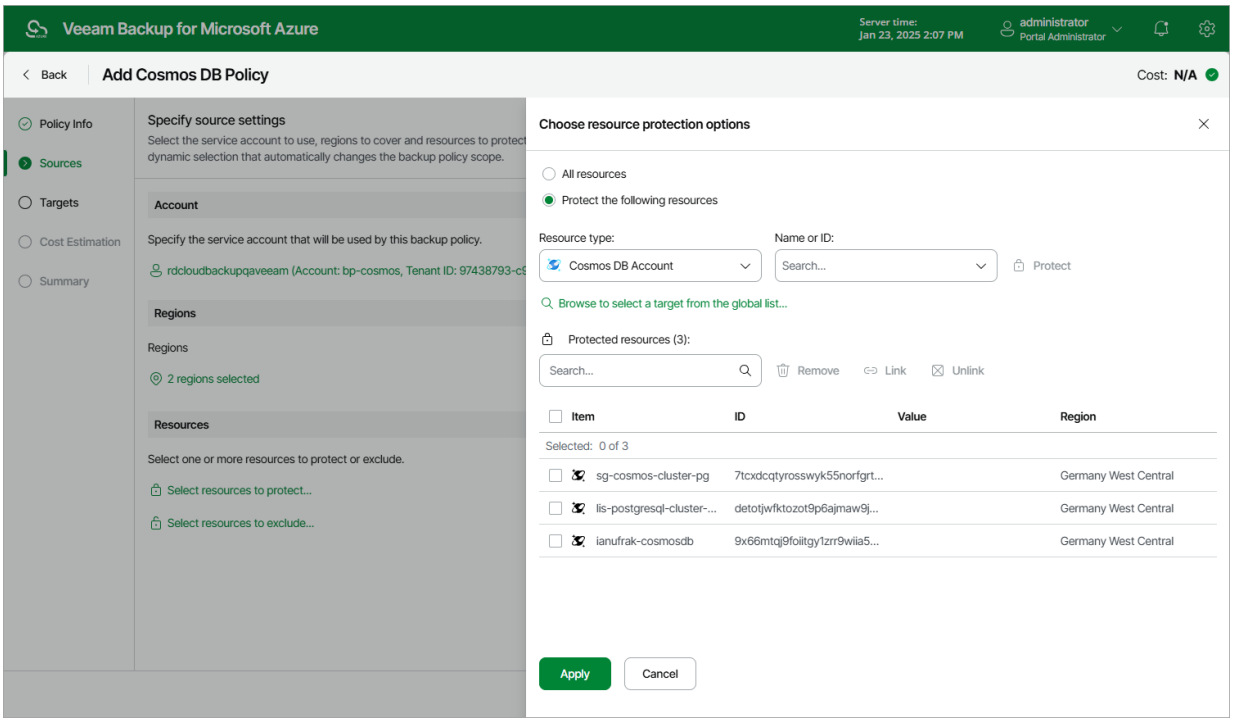
      Note that your web browser zoom must not exceed 135% for the list of protected resources to be displayed correctly.

> **TIP**
>
> You can simultaneously add multiple resources to the backup scope. To do that, click **Browse to select specific source from the global list**, select check boxes next to the necessary items in the list of available resources, and then click **Protect**.
>
> If the list does not show the resources that you want to back up, click **Rescan** to launch the data collection process — as soon as the process is over, Veeam Backup for Microsoft Azure will update the resource list. If you still cannot find the necessary resources in the list, make sure that the *Microsoft.ManagedServices* provider is registered in the subscription to which the resources belong, return to the step 3a and click **Rescan** in the **Choose service account** window. To learn how to register a resource provider, see Microsoft Docs.

4. To save changes made to the backup policy settings, click **Apply**.

> **TIP**
>
> As an alternative to selecting the **Protect the following resources** option and specifying the resources explicitly, you can select the **All resources** option and exclude a number of resources from the backup scope. To do that, click **Select resources to exclude** and specify Cosmos DB accounts or tags that you want to exclude from the backup scope — the procedure is the same as described for including resources in the backup scope.
>
> Consider that if a resource appears both in the list of included and excluded resources, Veeam Backup for Microsoft Azure will still not process the resource because the list of excluded resources has a higher priority.

When you add subscriptions, resource groups and tags to the backup scope, Veeam Backup for Microsoft Azure links all these resources using the OR operator. To instruct Veeam Backup for Microsoft Azure to use the AND operator, follow the instructions provided in section Configuring Conditions.




## Configuring Conditions

By default, Veeam Backup for Microsoft Azure uses the OR operator to link all the subscriptions, resource groups and tags that you include into the backup scope — meaning that all the related Cosmos DB accounts will be protected by the policy. To narrow down the backup scope, you can configure conditions that will allow Veeam Backup for Microsoft Azure to link the selected resources using the AND operator.

When you configure a condition, Veeam Backup for Microsoft Azure composes a list of Cosmos DB accounts to protect based on the resources that you add to this condition — meaning that a Cosmos DB account will be protected by the policy only if this account relates to all the linked resources. Keep in mind that one condition can link either multiple tags, a subscription with one or more tags, or a resource group with one or more tags.

To configure a condition, do the following in the **Resources** section of the **Sources** step of the wizard:

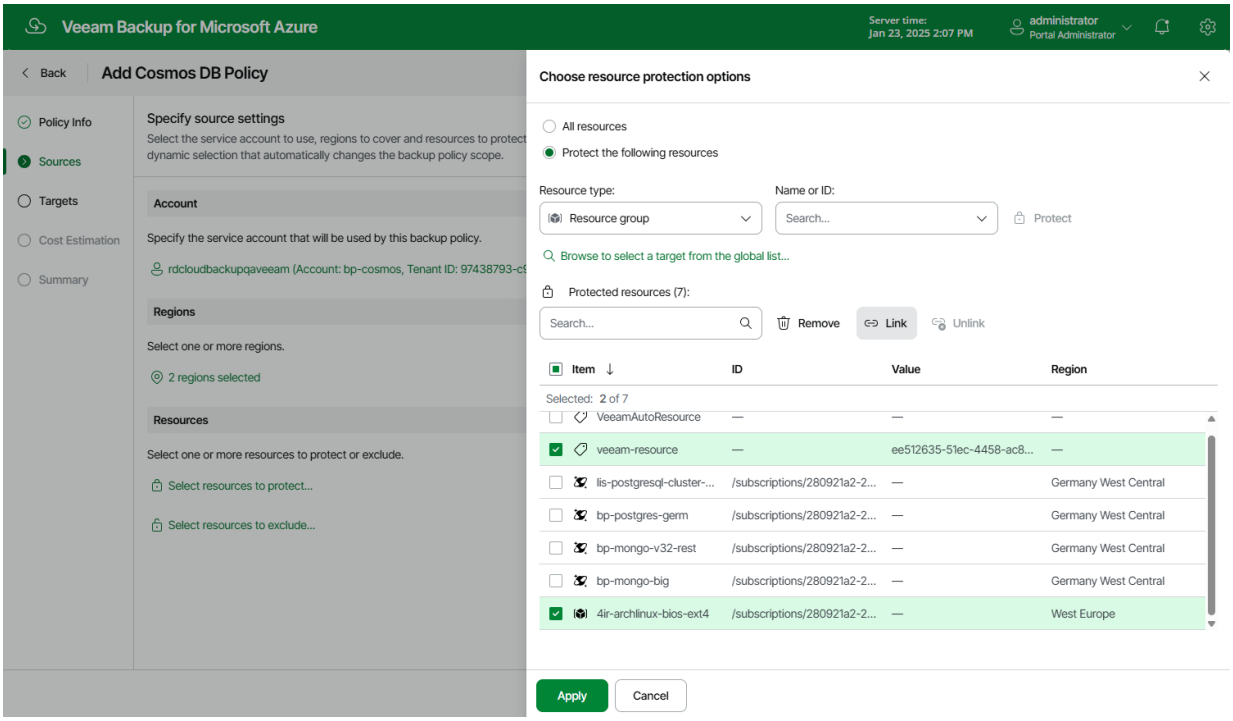
1. Click **Select resources to protect**.
2. In the **Choose resource protection options** window, select check boxes next to the items you want to include into the condition and click **Link**.

3. In the **Create Condition** window, provide a name for the condition and click **Apply**.

   The maximum length of the name is 64 characters.

When configuring conditions, you can add the same resource to the list of protected resources multiple times. For example, if you want to protect Cosmos DB accounts that are managed by the *dept-01-sweden* subscription and that have either the *Veeam-01* tag or *Veeam-02* tag assigned (but not both tags at the same time), you must add this subscription to the list of protected resources twice and then configure 2 separate conditions: one condition will link the subscription with the *Veeam-01* tag, while another condition will link the subscription with the *Veeam-02* tag.

> **TIP**
>
> After you configure a condition, you will be able to modify the list of resources included into this condition, unlink all the resources, and remove the condition if you no longer need it. When performing these actions, keep in mind that:
>
> - If you exclude a resource from the condition, Veeam Backup for Microsoft Azure will re-add it to the list of protected resources as a single item.
> - If you unlink the condition, Veeam Backup for Microsoft Azure will re-add all resources that were included into this condition to the list of protected resources as single items, and will link these resources using the OR operator.
> - If you remove the condition, Veeam Backup for Microsoft Azure will remove all resources that were included into this condition from the backup scope.



## Step 4. Configure Backup Target Settings

By default, Veeam Backup for Microsoft Azure protects Cosmos DB accounts using continuous backup — a native Microsoft Azure capability that allows you to eliminate consumption of extra provisioned throughput without affecting the database performance and availability. The backups are created in Azure regions in which source Cosmos DB accounts reside and are kept for a specific retention period. At the **Targets** step of the wizard, you can configure that period and also choose to store backups of Cosmos DB for PostgreSQL or Cosmos DB for MongoDB accounts in a repository.

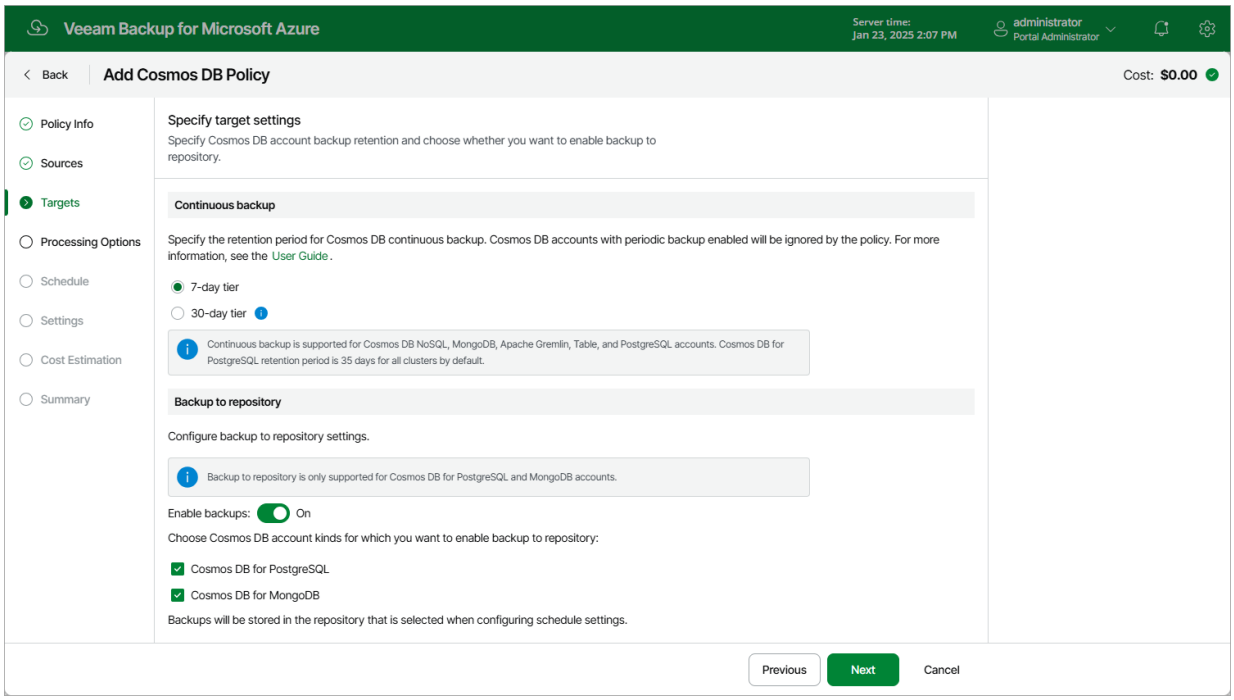
> **IMPORTANT**
>
> Consider the following:
>
> - Veeam Backup for Microsoft Azure does not support protecting Cosmos DB accounts that have periodic backup or multi-region writes enabled. If such an account is included in the backup scope, Veeam Backup for Microsoft Azure will not process it. If you want Veeam Backup for Microsoft Azure to protect this account, provision the account with continuous backup and point-in-time restore in Microsoft Azure as described in Microsoft Docs.
> - Storing backups in a repository is supported for Cosmos DB for PostgreSQL accounts and Cosmos DB for MongoDB accounts of MongoDB versions 3.6 and later.

The default retention period for continuous backup is 7 days. To change the retention period, select the *30-day tier* option in the **Continuous backup** section. Note that changing the retention period will cause additional infrastructure charges. For more information on Cosmos DB pricing, see Microsoft Docs.

> **NOTE**
>
> Regardless of the specified retention period for continuous backup, backups of Cosmos DB for PostgreSQL accounts are kept for 35 days.

As soon as you start the backup policy, Veeam Backup for Microsoft Azure will run a configuration session to check the continuous backup retention period defined in Microsoft Azure for all the Cosmos DB accounts added to the backup scope; if the retention period differs from the retention period specified in the backup policy settings, Veeam Backup for Microsoft Azure will redefine the retention period in Microsoft Azure. To track the progress of the configuration session, navigate to the Session Log page.

> **TIP**
>
> Veeam Backup for Microsoft Azure will keep running configuration sessions every 8 hours. If you want to adjust the frequency, open a support case.


Veeam Backup for Microsoft Azure
Server time:
Jan 23, 2025 2:07 PM
administrator
Portal Administrator
Back
Add Cosmos DB Policy
Cost: $0.00
Policy Info
Sources
Targets
Processing Options
Schedule
Settings
Cost Estimation
Summary
Specify target settings
Specify Cosmos DB account backup retention and choose whether you want to enable backup to repository.
Continuous backup
Specify the retention period for Cosmos DB continuous backup. Cosmos DB accounts with periodic backup enabled will be ignored by the policy. For more information, see the User Guide.
7-day tier
30-day tier
Continuous backup is supported for Cosmos DB NoSQL, MongoDB, Apache Gremlin, Table, and PostgreSQL accounts. Cosmos DB for PostgreSQL retention period is 35 days for all clusters by default.
Backup to repository
Configure backup to repository settings.
Backup to repository is only supported for Cosmos DB for PostgreSQL and MongoDB accounts.
Enable backups:
On
Choose Cosmos DB account kinds for which you want to enable backup to repository:
Cosmos DB for PostgreSQL
Cosmos DB for MongoDB
Backups will be stored in the repository that is selected when configuring schedule settings.
Previous
Next
Cancel

## Step 5. Configure Processing Options

[This step applies only if you set the **Backup to repository** toggle to *On* at the **Targets** step of the wizard]

At the **Processing Options** step of the wizard, review the authentication method used to process Cosmos DB for MongoDB accounts and select credentials for processing Cosmos DB for PostgreSQL clusters.

# Cosmos DB For MongoDB Account Authentication

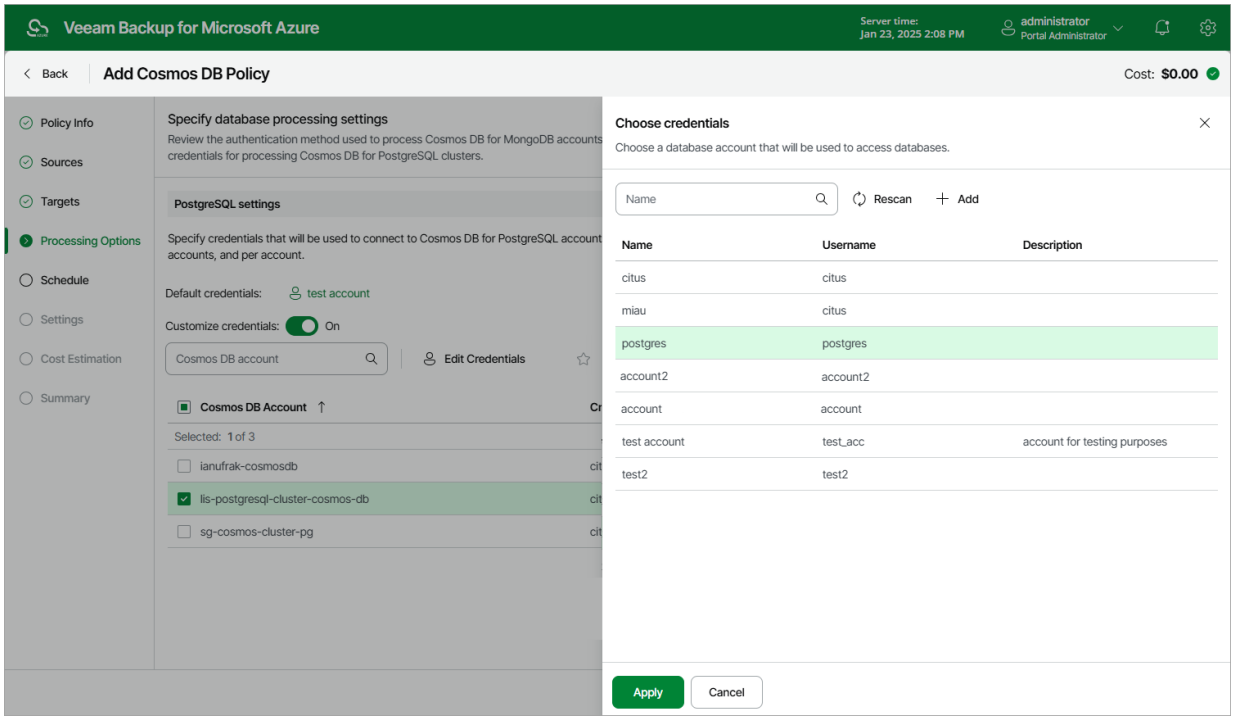
To access Cosmos DB for MongoDB accounts and to back up database data, Veeam Backup for Microsoft Azure uses the read-only primary/secondary keys. For more information, see Microsoft Docs.

# Cosmos DB For PostgreSQL Account Authentication

In the **PostgreSQL settings** section, select a database account whose credentials will be used to authenticate against databases of the Cosmos DB for PostgreSQL accounts added to the backup scope. For a database account to be displayed in the list of available accounts, it must be added to Veeam Backup for Microsoft Azure as described in section Adding SMTP and Database Accounts. If you have not added the necessary account to Veeam Backup for Microsoft Azure beforehand, you can do it without closing the **Add Cosmos DB Policy** wizard. To do that, click **Add** and complete the **Add Account** wizard.

By default, the selected database account will be used to access all databases of the Cosmos DB for PostgreSQL accounts added to the backup policy. You can also granularly specify credentials that Veeam Backup for Microsoft Azure will use to connect to specific databases. To do that, set the **Customize credentials** toggle to *On*, choose a database for which you want to specify the credentials and click **Edit Credentials**.

> **IMPORTANT**
>
> The selected account must have permissions required to perform database dumping operations, and access to all user databases of the processed Cosmos DB accounts — otherwise, the backup operation will fail to complete successfully.



## Step 6. Specify Policy Scheduling Options

[This step applies only if you set the **Backup to repository** toggle on the **Targets** step of the wizard to *On*]

You can instruct Veeam Backup for Microsoft Azure to start the backup policy automatically according to a specific backup schedule. The backup schedule defines how often data of the Cosmos DB for PostgreSQL and Cosmos DB for MongoDB accounts added to the backup policy will be backed up.

To help you implement a comprehensive backup strategy, Veeam Backup for Microsoft Azure allows you to create schedules of the following types:

- Daily — the backup policy will create restore points repeatedly throughout a day on specific days.
- Weekly — the backup policy will create restore points once a day on specific days.
- Monthly — the backup policy will create restore points once a month on a specific day.
- Yearly — the backup policy will create restore points once a year on a specific day.

Combining multiple schedule types together allows you to retain restore points for longer periods of time — for more information, see Enabling Harmonized Scheduling. Combining multiple schedule types together also allows you to archive backups — for more information, see Enabling Backup Archiving.

> **NOTE**
>
> When scheduling backup policies, it is recommended that you take into account the load in your Cosmos DB clusters since a large number of backup operations may affect the overall cluster performance.

### Specifying Daily Schedule

To create a daily schedule for the backup policy, at the **Schedule** step of the wizard, do the following:

1. Set the **Daily retention** toggle to *On* and click **Edit Daily Settings**.
2. In the **Daily schedule** window, select hours when the backup policy will create backups.

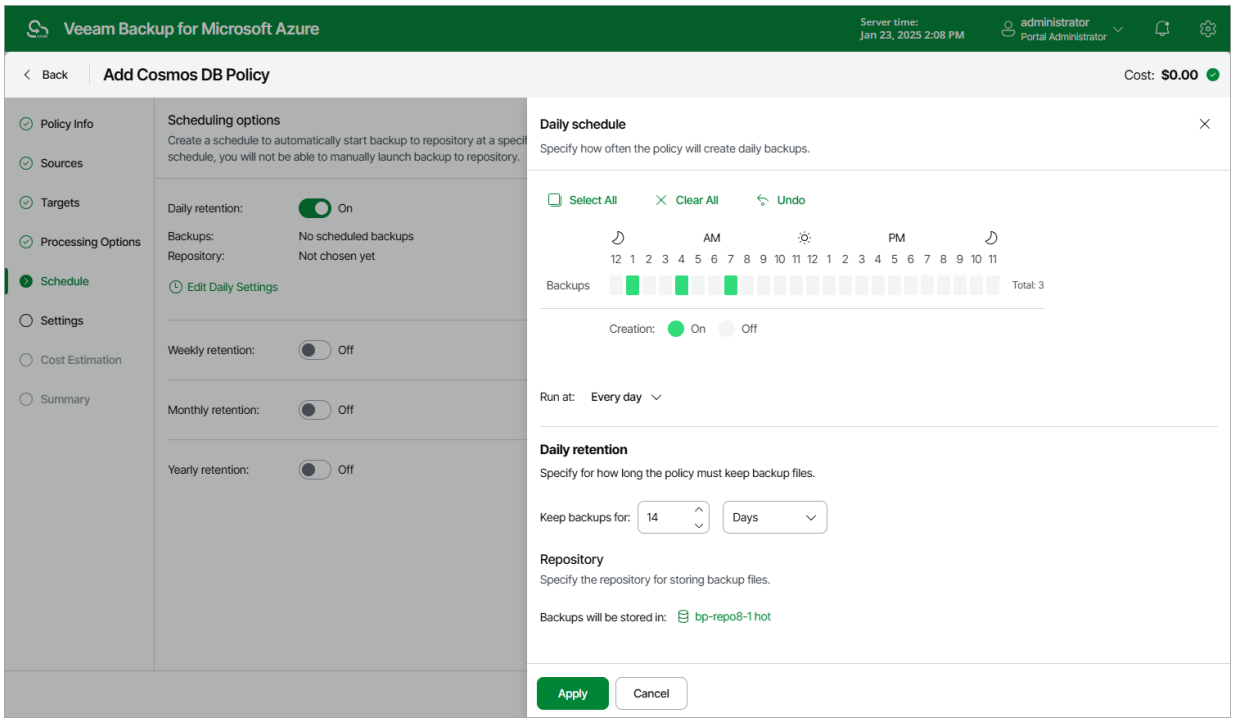
> **NOTE**
>
> Since Veeam Backup for Microsoft Azure runs retention sessions at 12:15 AM according to the time zone set on the backup appliance, it is not recommended that you schedule backup policies to execute at 12:15 AM. Otherwise, Veeam Backup for Microsoft Azure will not be able to run the retention sessions.

3. Use the **Run at** drop-down list to choose whether you want the backup policy to run every day, on weekdays (Monday through Friday) or on specific days.
4. In the **Daily retention** section, specify the number of days (or months) for which you want to keep restore points in a backup chain.

   If a restore point is older than the specified time limit, Veeam Backup for Microsoft Azure removes the restore point from the chain. For more information, see Cosmos DB Backup Retention.
5. In the **Repository** section, select a backup repository where the created backups will be stored.

   For a backup repository to be displayed in the **Repository** list, it must be added to Veeam Backup for Microsoft Azure as described in section Adding Backup Repositories.

6. To save changes made to the backup policy settings, click **Apply**.




## Specifying Weekly Schedule

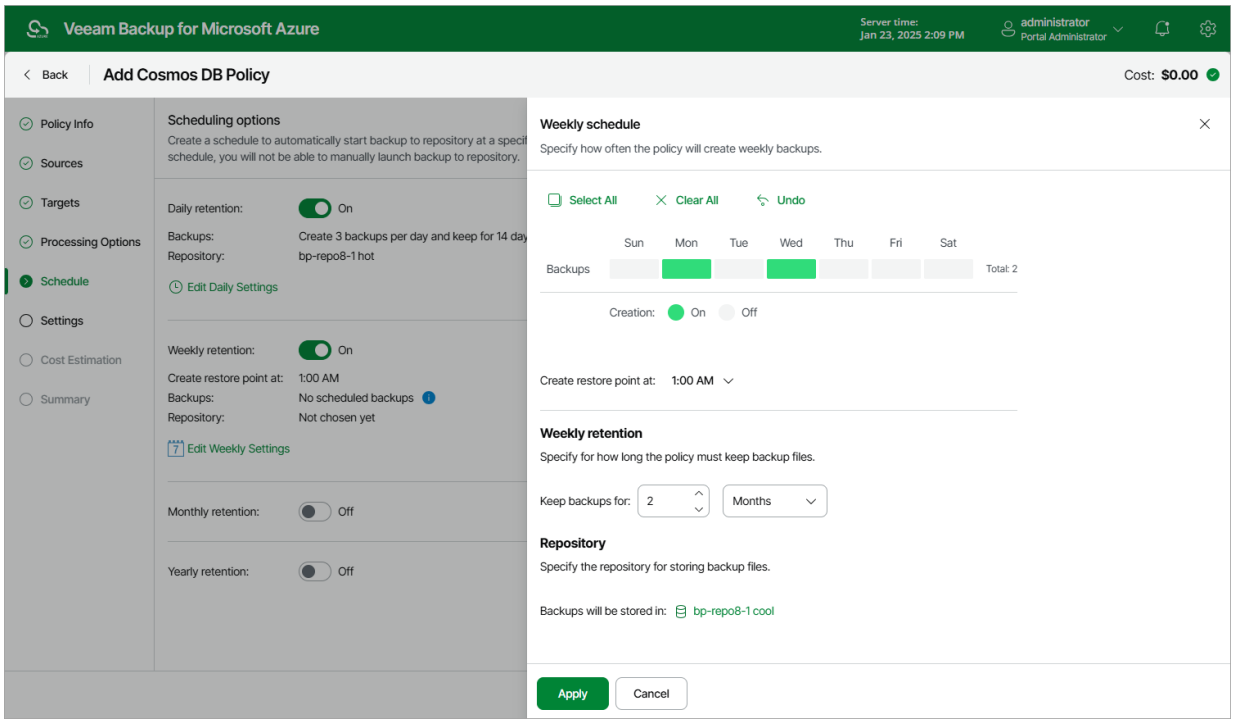
To create a weekly schedule for the backup policy, at the **Schedule** step of the wizard, do the following:

1. Set the **Weekly retention** toggle to *On* and click **Edit Weekly Settings**.
2. In the **Weekly schedule** window, select days of the week when the backup policy will create backups.
3. Use the **Create restore points at** drop-down list to schedule a specific time for the backup policy to run.
4. In the **Weekly retention** section, specify the number of days (or months) for which you want to keep restore points in a backup chain.

   If a restore point is older than the specified time limit, Veeam Backup for Microsoft Azure removes the restore point from the chain. For more information, see Cosmos DB Backup Retention.
5. In the **Repository** section, select a backup repository where the created backups will be stored.

   For a backup repository to be displayed in the **Repository** list, it must be added to Veeam Backup for Microsoft Azure as described in section Adding Backup Repositories.

6. To save changes made to the backup policy settings, click **Apply**.




## Specifying Monthly Schedule

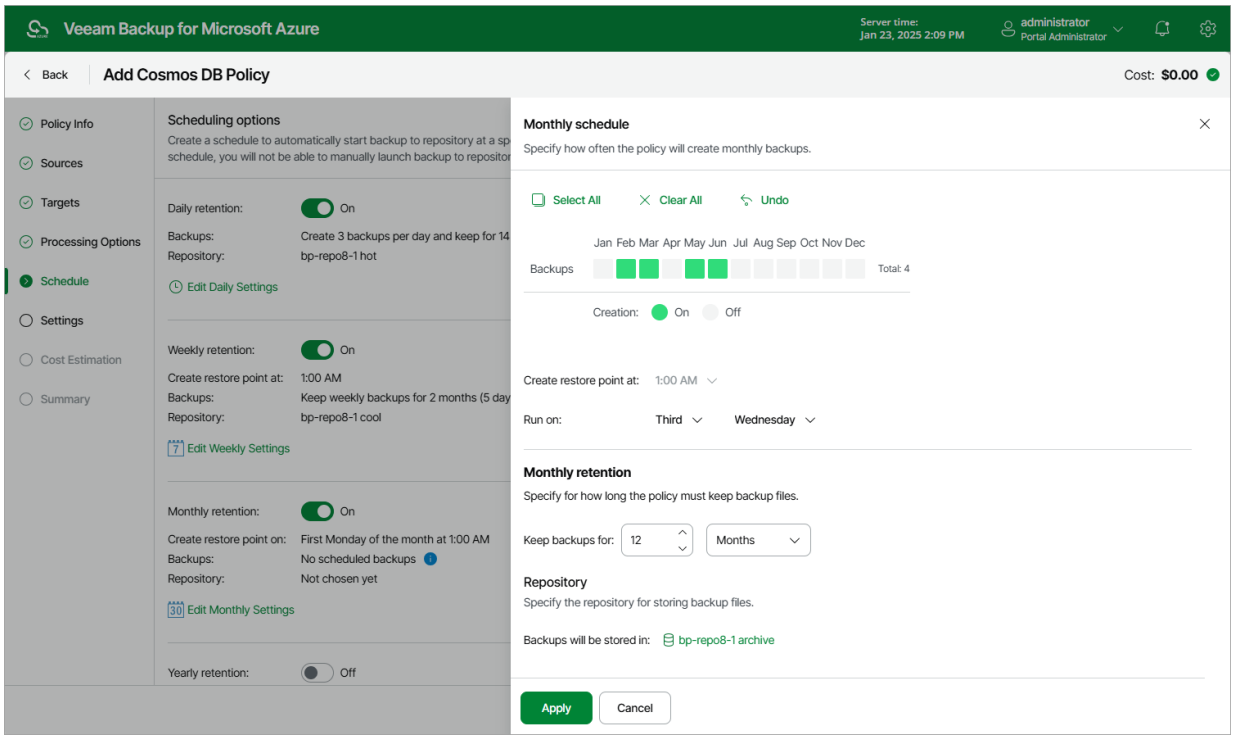
To create a monthly schedule for the backup policy, at the **Schedule** step of the wizard, do the following:

1. Set the **Monthly retention** toggle to *On* and click **Edit Monthly Settings**.
2. In the **Monthly schedule** window, select months when the backup policy will create backups.
3. Use the **Create restore points at** and **Run on** drop-down lists to schedule a specific time and day for the backup policy to run.
4. In the **Monthly retention** section, specify the number of days (or months) for which you want to keep restore points in a backup chain.

   If a restore point is older than the specified time limit, Veeam Backup for Microsoft Azure removes the restore point from the chain. For more information, see Cosmos DB Backup Retention.
5. In the **Repository** section, select a backup repository where the created backups will be stored.

   For a backup repository to be displayed in the **Repository** list, it must be added to Veeam Backup for Microsoft Azure as described in section Adding Backup Repositories.

6. To save changes made to the backup policy settings, click **Apply**.




## Specifying Yearly Schedule

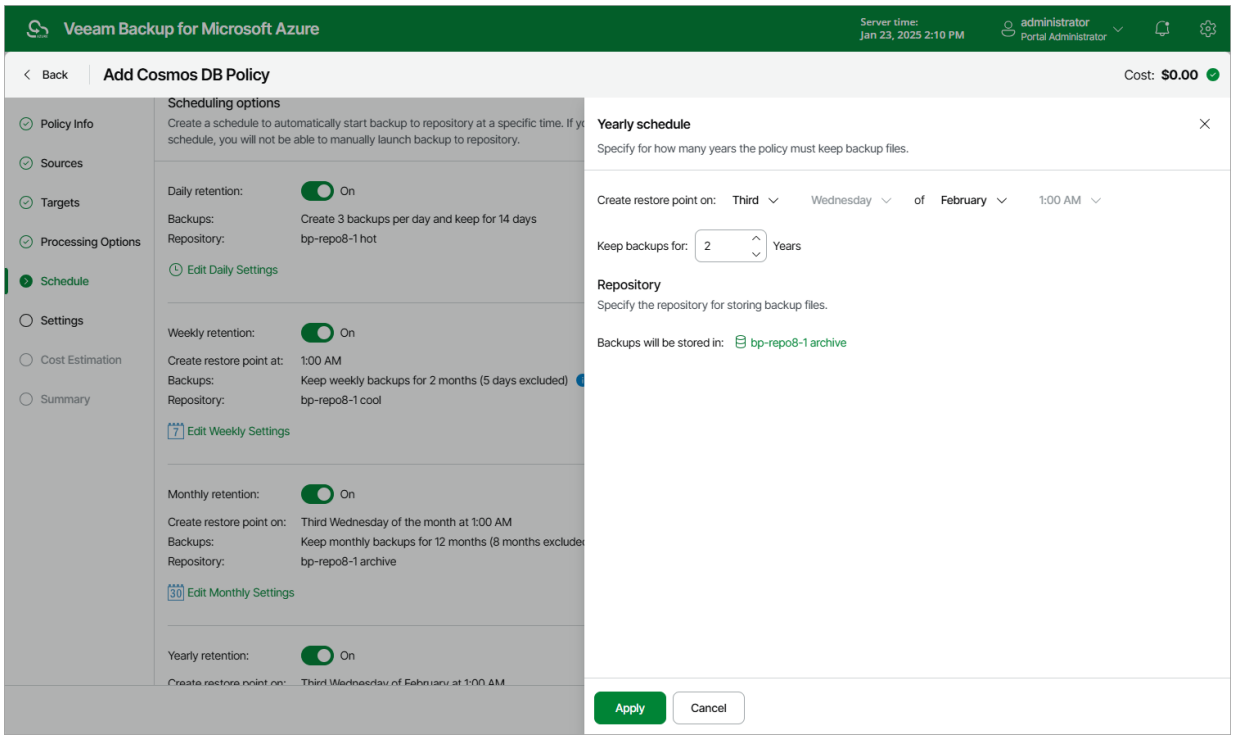
To create a yearly schedule for the backup policy, at the **Schedule** step of the wizard, do the following:

1. Set the **Yearly retention** toggle to *On* and click **Edit Yearly Settings**.
2. In the **Yearly schedule** window, specify a day, month and time when the backup policy will create backups.
3. In the **Keep backups for** field, specify the number of years for which you want to keep restore points in a backup chain.

   If a restore point is older than the specified time limit, Veeam Backup for Microsoft Azure removes the restore point from the chain. For more information, see Cosmos DB Backup Retention.
4. In the **Repository** section, select a backup repository where the created backups will be stored.

   For a backup repository to be displayed in the **Repository** list, it must be added to Veeam Backup for Microsoft Azure as described in section Adding Backup Repositories.

5. To save changes made to the backup policy settings, click **Apply**.




## Enabling Harmonized Scheduling

When you combine multiple types of schedules, Veeam Backup for Microsoft Azure applies the harmonization mechanism that allows you to leverage restore points for long-term retentions instead of taking a new restore point every time. The mechanism simplifies the backup schedule, optimizes the backup performance and reduces the cost of storing restore points in backup repositories.

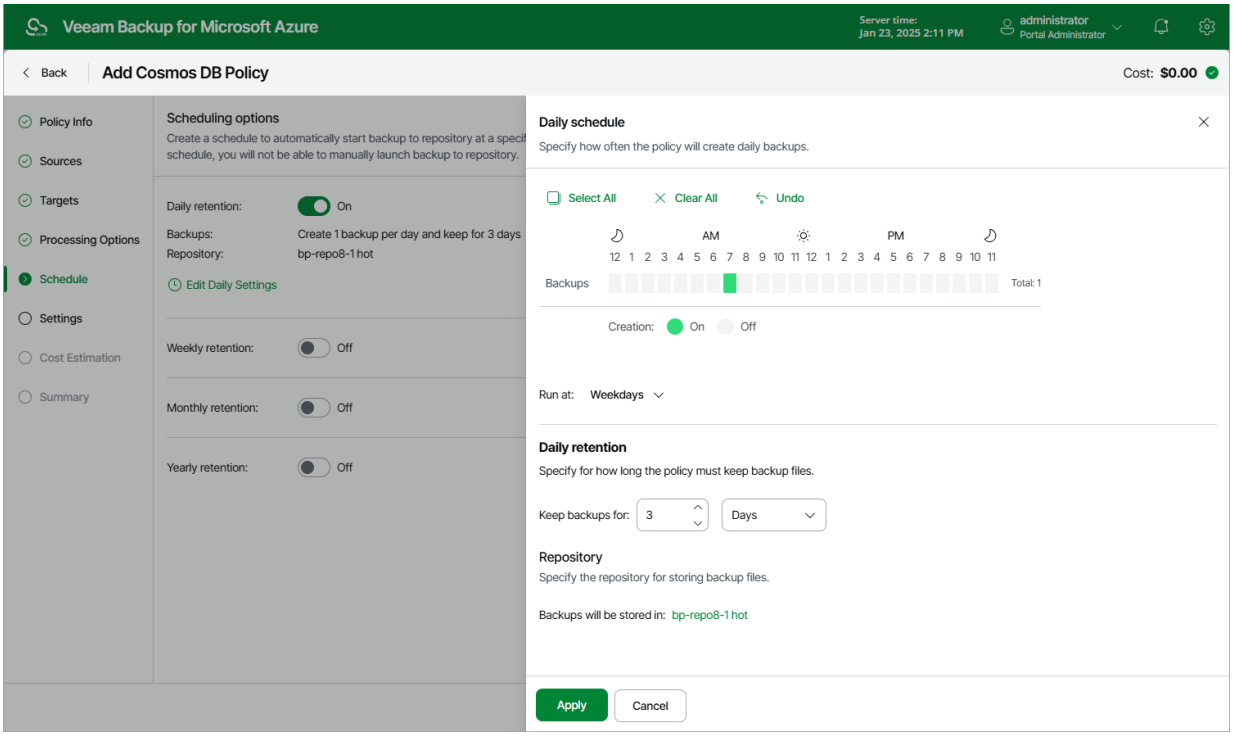
With harmonized scheduling, Veeam Backup for Microsoft Azure can keep restore points created according to a daily, weekly or monthly schedule for longer periods of time (for weeks, months and years).

For Veeam Backup for Microsoft Azure to use the harmonization mechanism, there must be specified at least 2 different schedules: one schedule will control the regular creation of restore points, while another schedule will control the process of retaining restore points. In terms of harmonized scheduling, Veeam Backup for Microsoft Azure re-uses restore points created according to a more-frequent schedule (daily, weekly or monthly) to achieve the desired retention for less-frequent schedules (weekly, monthly and yearly). Each restore point is marked with a flag of the related schedule type: the (Daily) flag is used to mark restore points created daily, (Weekly) — weekly, (Monthly) — monthly, and (Yearly) — yearly. Veeam Backup for Microsoft Azure uses these flags to control the retention period for the created restore points. Once a flag of a less-frequent schedule is assigned to a restore point, this restore point can no longer be removed — it is kept for the period defined in the retention settings. When the specified retention period is over, the flag is unassigned from the restore point. If the restore point does not have any other flags assigned, it is removed according to the retention settings of a more-frequent schedule.

Consider the following example. You want a backup policy to create backups of your critical workloads once a day, to keep 3 daily backups in the backup chain, and also to keep one of the created backups for 2 weeks. In this case, you create 2 schedules when configuring the backup policy settings — daily and weekly:

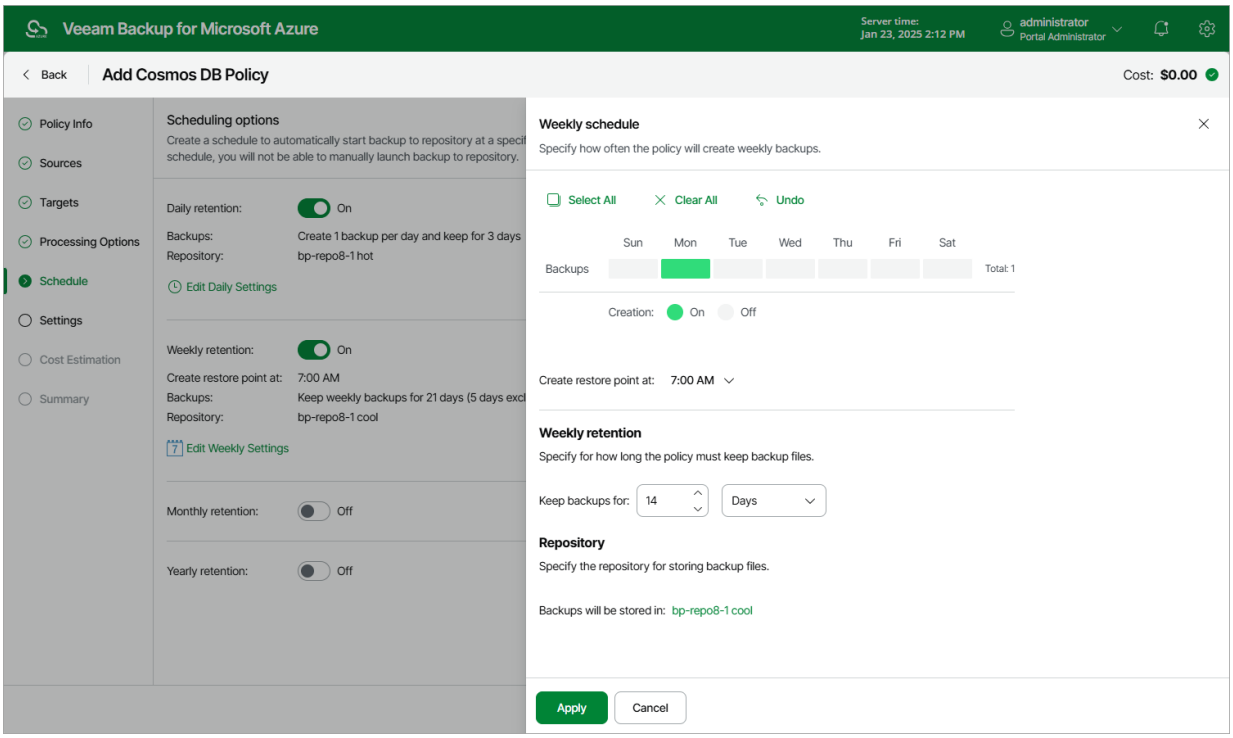
1. In the daily scheduling settings, you select hours and days when backups will be created (for example, *7:00 AM*; *Weekdays*), and specify the number of days for which you want to retain daily restore points in a backup chain (for example, *3*).

   Veeam Backup for Microsoft Azure will propagate these settings to the schedule with a lower frequency (which is the weekly schedule in our example).



2. In the weekly scheduling settings, you specify which one of the backups created by the daily schedule will be retained for a longer period, and choose for how long you want to keep the selected backup.

   For example, if you want to keep the daily restore point created on Monday for 2 weeks, you select *7:00 AM*, *Monday* and specify *14 days* in the weekly schedule settings.

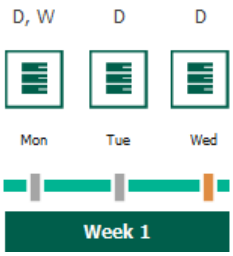



According to the specified scheduling settings, Veeam Backup for Microsoft Azure will create image-level backups in the following way:

1. On the first work day (Monday), a backup session will start at 7:00 AM to create the first restore point. The restore point will be marked with the (D) flag as it was created according to the daily schedule.

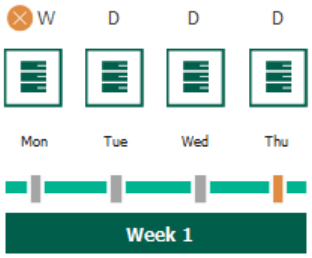
   Since *7:00 AM*, *Monday* is specified in weekly schedule settings, Veeam Backup for Microsoft Azure will assign the (W) flag to this restore point.

2. On the same week, after backup sessions run on Tuesday and Wednesday, the created restore points will be marked with the (D) flag.



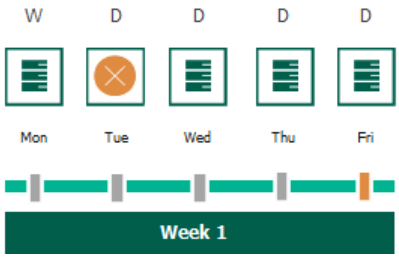
3. On the fourth work day (Thursday), after a backup session runs at 7:00 AM, the created restore point will be marked with the (D) flag.

   By this moment, the earliest restore point in the backup chain will get older than the specified retention limit. However, Veeam Backup for Microsoft Azure will not remove the earliest restore point (*7:00 AM, Monday*) with the (D) flag from the backup chain as this restore point is also marked with a flag of a less-frequent schedule. Instead, Veeam Backup for Microsoft Azure will unassign the (D) flag from the restore point. This restore point will be kept for the retention period specified in the weekly scheduling settings (that is, for 2 weeks).



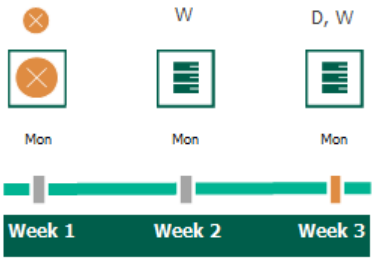

4. On the fifth working day (Friday), after a backup session runs at 7:00 AM, the created restore point will be marked with the (D) flag.

   By this moment, the restore point created on Tuesday with the (D) flag will get older than the specified retention limit. Veeam Backup for Microsoft Azure will remove from the backup chain the restore point created at 7:00 AM on Tuesday as no flags of a less-frequent schedule are assigned to this restore point.




5. Veeam Backup for Microsoft Azure will continue creating restore points for the next week in the same way as described in steps 1-4.

6. On week 3, after a backup session runs at 7:00 AM on Monday, the earliest weekly restore point in the backup chain will get older than the specified retention limit. Veeam Backup for Microsoft Azure will unassign the (W) flag from the earliest weekly restore point. Since no other flags are assigned to this restore point, Veeam Backup for Microsoft Azure will remove this restore point from the backup chain.




> **NOTE**
>
> This section does not explain how Veeam Backup for Microsoft Azure rebuilds the backup chain when applying the configured retention policy settings — it focuses on the harmonization mechanism itself only. To learn what types of backups Veeam Backup for Microsoft Azure includes in the backup chain and how it transforms the chain when removing outdated restore points, see sections Backup Chain and Cosmos DB Backup Retention.

## Enabling Backup Archiving

When you combine multiple types of schedules, you can enable the archiving mechanism to instruct Veeam Backup for Microsoft Azure to store backed-up data in the low-cost, long-term Archive access tier. The mechanism is the most useful in the following cases:

- Your data retention policy requires that you keep rarely accessed data in an archive.
- You want to reduce data-at-rest costs and to save space in the high-cost, short-term Hot and Cool access tiers.

> **NOTE**
>
> Restoring from an archived backup is longer and more expensive than restoring from a regular backup as it is required to retrieve data from the archive repository. For more information, see Retrieving Data From Archive.

With backup archiving, Veeam Backup for Microsoft Azure can retain backups created according to a daily, weekly or monthly schedule for longer periods of time:

- To enable monthly archiving, you must configure a daily or a weekly schedule (or both).
- To enable yearly archiving, you must configure a daily, a weekly or a monthly schedule (or all three).

For Veeam Backup for Microsoft Azure to use the archiving mechanism, there must be specified at least 2 different schedules: one schedule will control the regular creation of backups, while another schedule will control the process of copying backups to an archive repository. Backup chains created according to these two schedules will be completely different — for more information, see Backup Chain and Archive Backup Chain.

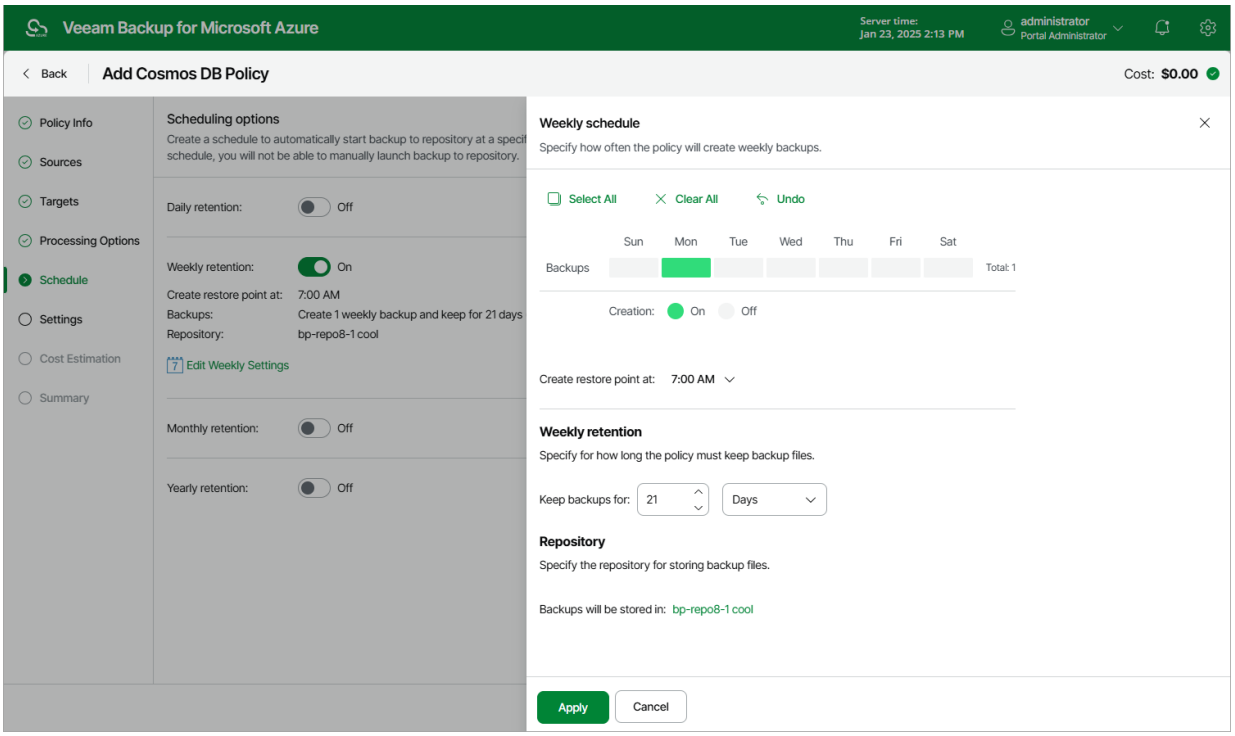
> **TIP**
>
> Copying backups to archive repositories is supported only from standard repositories with the same encryption settings (that is, data encryption must be either enabled or disabled). For example, if you instruct Veeam Backup for Microsoft Azure to store daily backups in a standard repository with encryption enabled, and monthly backups in an archive repository with encryption disabled, Veeam Backup for Microsoft Azure will not be able to archive these daily backups. However, data in the selected repositories can be encrypted differently (using a password or an Azure Key Vault cryptographic key).

Consider the following example. You want a backup policy to create backups of your critical workloads once a week, to keep the backed-up data in a standard repository for 3 weeks, and also to keep backups created once in 2 months in an archive repository for a year. In this case, you create 2 schedules when configuring the backup policy settings — weekly and monthly:

1. In the weekly scheduling settings, you do the following:
    a. Specify hours and days when backups will be created (for example, *7:00 AM, Monday*), and specify the number of days for which Veeam Backup for Microsoft Azure will retain backups (for example, *21 days*).

b. Select a repository of the Hot or Cool access tier that will store regular backups.

Veeam Backup for Microsoft Azure will propagate these settings to the archive schedule (which is the monthly schedule in our example).




2. In the monthly scheduling settings, you do the following:

   a. Specify when Veeam Backup for Microsoft Azure will create archive backups, and choose for how long you want to retain the created backups (for example, *January*, *March*, *May*, *July*, *September*, *November*, *12 months* and *First Monday*).

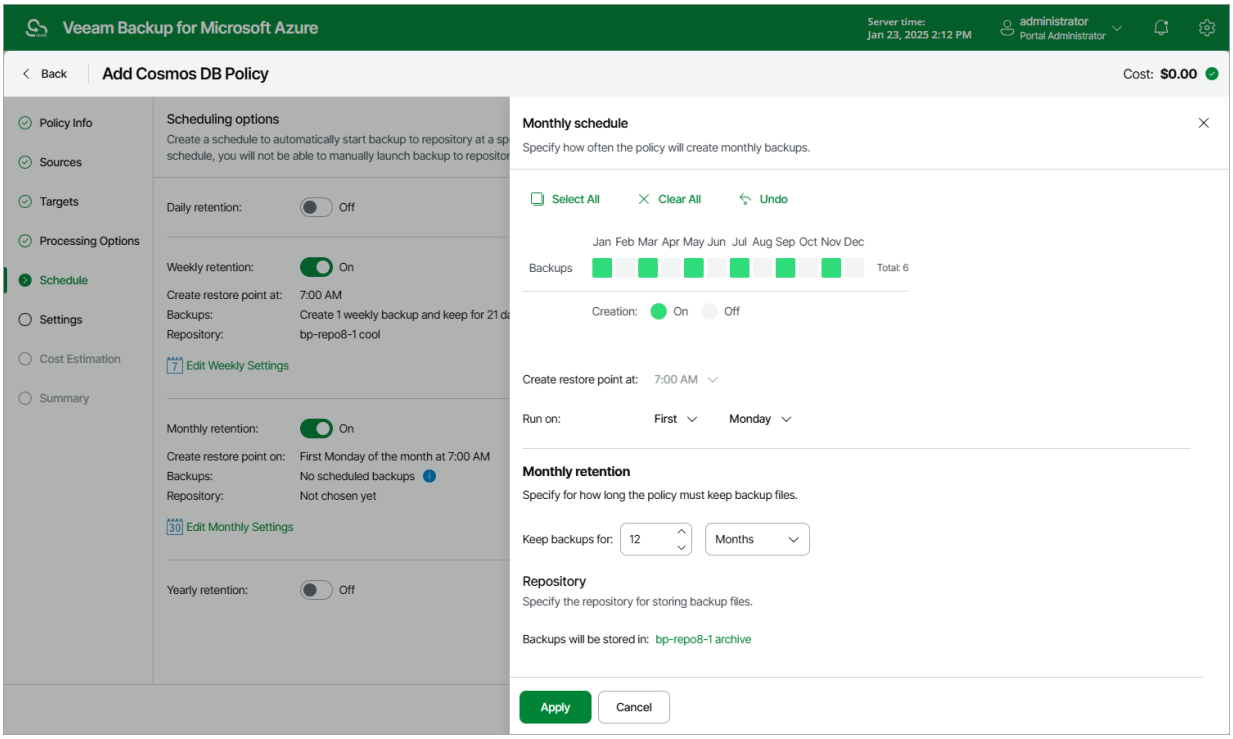
   b. Enable the archiving mechanism by selecting a repository of the Archive access tier that will store archived data.

      Note that when you enable backup archiving, you become no longer able to create a schedule of the same frequency for regular backups. By design, these two functionalities are mutually exclusive.

**IMPORTANT**

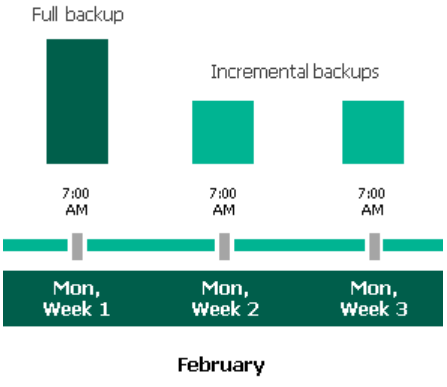
If you enable backup archiving, consider the following:

- It is recommended that you set the **Keep backups for** value to at least *6 months* (or *180 days*), since the minimum storage duration of the Archive access tier is 180 days.
- If you select the **On Day** option, harmonized scheduling cannot be guaranteed. Plus, to support the **On Day** option, Veeam Backup for Microsoft Azure will require to create an additional temporary restore point if there are no other schedules planned to run on that day. However, the temporary restore point will be removed during the *Backup Retention* process from Microsoft Azure Storage in approximately 24 hours, to reduce unexpected infrastructure charges.



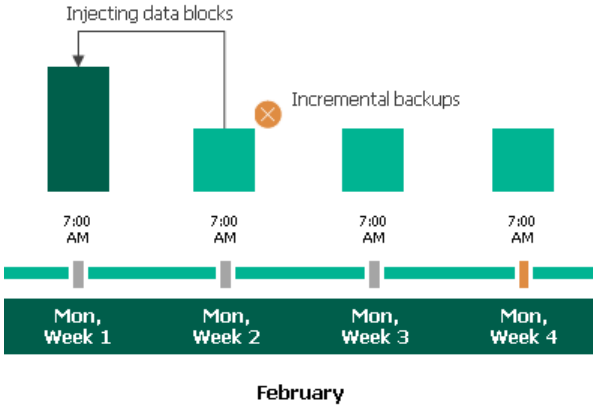

According to the specified scheduling settings, Veeam Backup for Microsoft Azure will create image-level backups in the following way:

1. On the first Monday of February, a backup session will start at 7:00 AM to create the first restore point in the regular backup chain. Veeam Backup for Microsoft Azure will store this restore point as a full backup in the backup repository.
2. On the second and third Mondays of February, Veeam Backup for Microsoft Azure will create restore points at 7:00 AM and add them to the regular backup chain as incremental backups in the backup repository.



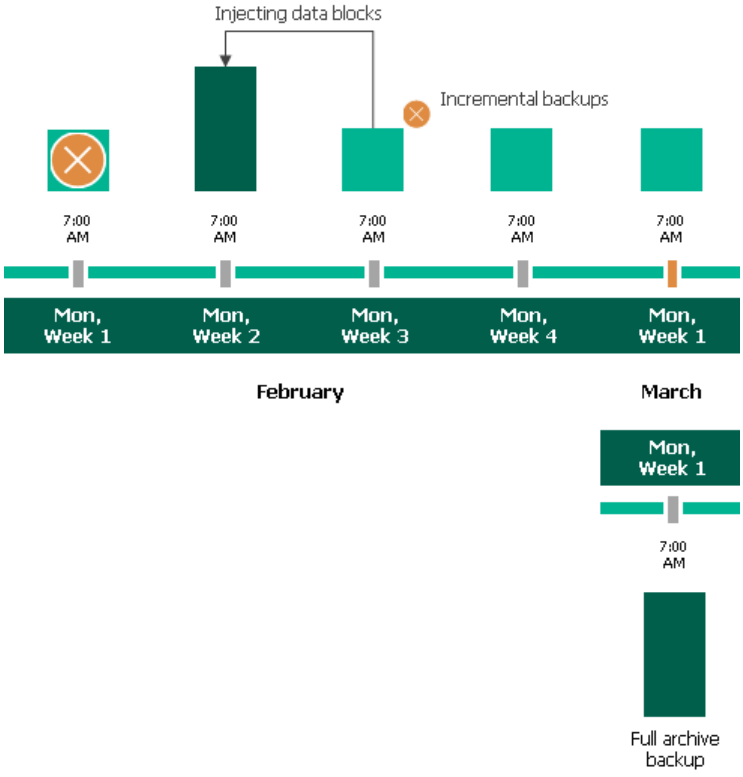
3. On the fourth Monday of February, Veeam Backup for Microsoft Azure will create a new restore point at 7:00 AM. By the moment the backup session completes, the earliest restore point in the regular backup chain will get older than the specified retention limit. That is why Veeam Backup for Microsoft Azure will rebuild the full backup and remove from the chain the restore point created on the first Monday.

   For more information on how Veeam Backup for Microsoft Azure transforms regular backup chains, see Cosmos DB Backup Retention.



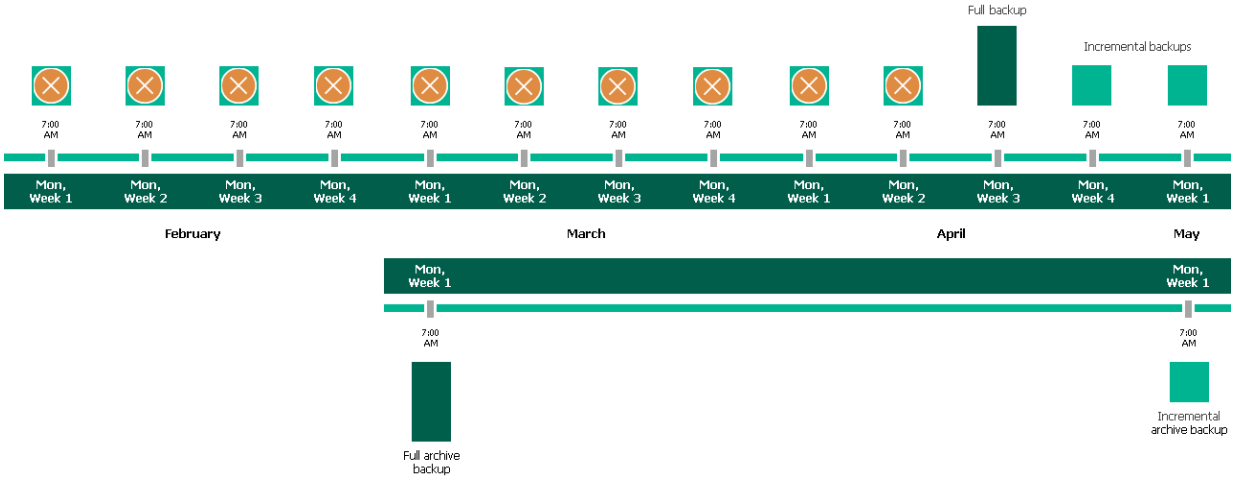

4. On the first Monday of March, a backup session will start at 7:00 AM to create another restore point in the regular backup chain. At the same time, the earliest restore point in the regular backup chain will get older than the specified retention limit again. That is why Veeam Backup for Microsoft Azure will rebuild the full backup again and remove from the chain the restore point created on the second Monday.

   After the backup session completes, an archive session will create a restore point with all data from the regular backup chain. Veeam Backup for Microsoft Azure will copy this restore point as a full archive backup to the archive repository.



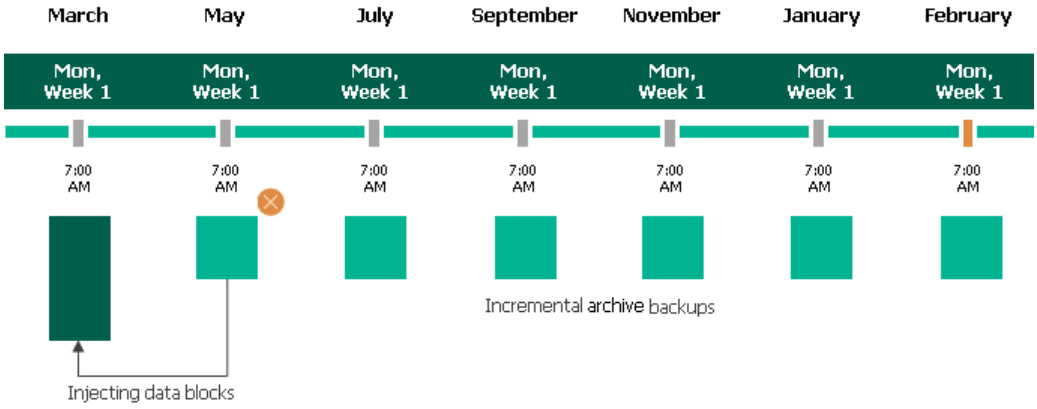
5. Up to May, Veeam Backup for Microsoft Azure will continue adding new restore points to the regular backup chain and deleting outdated backups from the backup repository, according to the specified weekly scheduling settings.

   On the first Monday of May, an archive session will create a restore point with only that data that has changed since the previous archive session in March. Veeam Backup for Microsoft Azure will copy this restore point as an incremental archive backup to the archive repository.




6. Up to the first Monday of February of the next year, Veeam Backup for Microsoft Azure will continue adding new restore points to the regular backup chain and deleting outdated backups from the backup repository, according to the specified weekly scheduling settings. Veeam Backup for Microsoft Azure will also continue adding new restore points to the archive backup chain, according to the specified monthly settings.

   By the moment the archive session completes, the earliest restore point in the archive backup chain will get older than the specified retention limit. That is why Veeam Backup for Microsoft Azure will rebuild the full archive backup and remove from the chain the restore point created on the first Monday of March of the previous year.



## Step 7. Configure General Settings

At the **Settings** step of the wizard, you can enable automatic retries, schedule health checks and specify notification settings for the backup policy.

# Automatic Retry Settings

To instruct Veeam Backup for Microsoft Azure to run the backup policy again if it fails on the first try, do the following:

1. In the **Schedule** section of the step, select the **Automatic retry failed policy** check box.
2. In the field to the right of the check box, specify the maximum number of attempts to run the backup policy. The time interval between retries is 600 seconds.

When retrying backup policies, Veeam Backup for Microsoft Azure processes only those Cosmos DB accounts that failed to be backed up during the previous attempt.

> **NOTE**
>
> The automatic retry settings apply only to backup policies that run according to specific schedules — these settings do not apply to policies started manually.

# Health Check Settings

Veeam Backup for Microsoft Azure can periodically perform a health check for all restore points created by the backup policy. During the health check, Veeam Backup for Microsoft Azure performs an availability check for data blocks in the whole regular backup chain, and a cyclic redundancy check (CRC) for metadata to verify its integrity. The health check helps you ensure that the restore points are consistent and that you will be able to restore data using these restore points. For more information on the health check, see How Health Check Works.

> **NOTE**
>
> During a health check, Veeam Backup for Microsoft Azure does not verify archived restore points created by the policy.

To instruct Veeam Backup for Microsoft Azure to perform a health check, do the following:

1. In the **Health check** section of the step, set the **Enable health check** toggle to *On*.
2. Use the **Run on** drop-down lists to schedule a specific day for the health check to run.

> **NOTE**
>
> Veeam Backup for Microsoft Azure performs the health check during the last policy session that runs on the day when the health check is scheduled. If another backup policy session runs on the same day, Veeam Backup for Microsoft Azure will not perform the health check during that session. For example, if the backup policy is scheduled to run multiple times on Saturday, and the health check is also scheduled to run on Saturday, the health check will only be performed during the last policy session on Saturday.

# Notification Settings

To instruct Veeam Backup for Microsoft Azure to send email notifications for the backup policy, do the following:

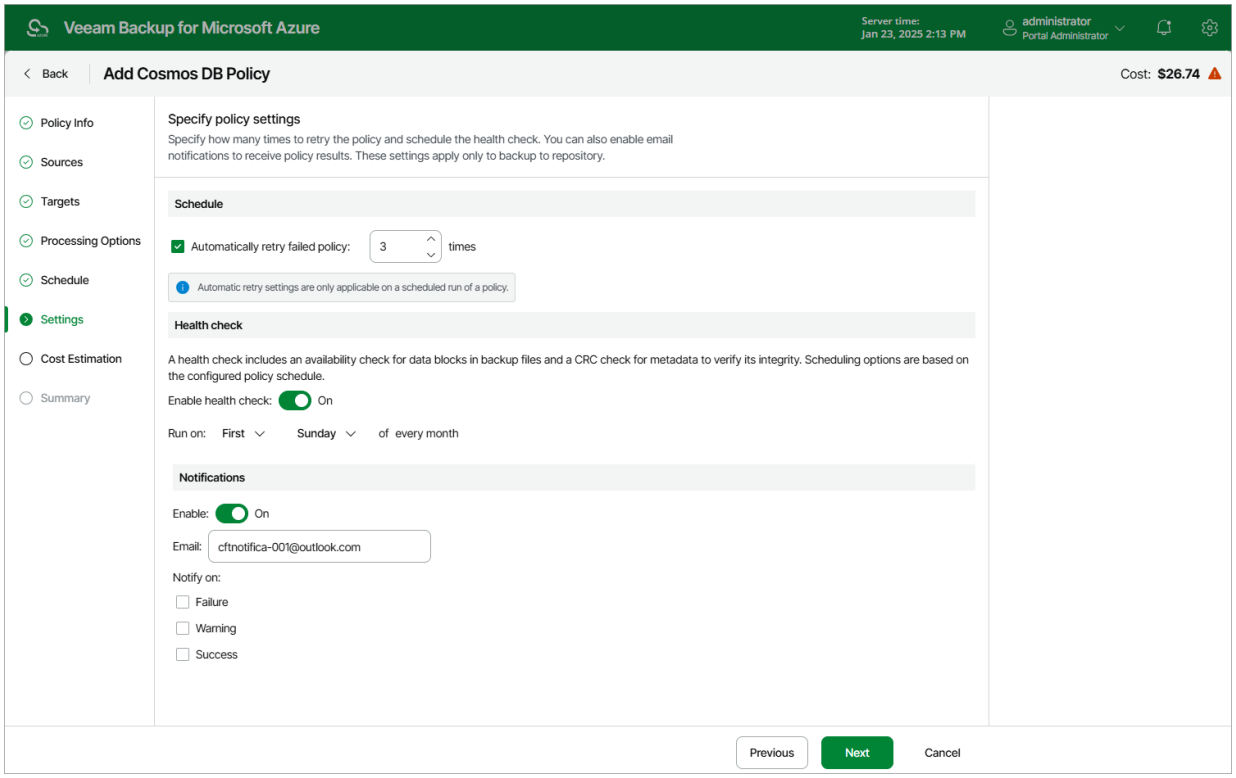
1. In the **Notifications** section of the step, set the **Enabled** toggle to *On*.

   If you set the toggle to *Off*, Veeam Backup for Microsoft Azure will not send any notifications for this backup policy — regardless of the configured global notification settings.

2. In the **Email** field, specify an email address of a recipient. Use a semicolon to separate multiple recipient addresses.

3. Use the **Notify on** list to choose whether you want Veeam Backup for Microsoft Azure to send email notifications in case the backup policy completes successfully, completes with warnings or completes with errors.

> **NOTE**
>
> If you specify the same email recipient in both backup policy notification and global notification settings, Veeam Backup for Microsoft Azure will override the configured global notification settings and will send each notification to this recipient only once to avoid notification duplicates.




## How Health Check Works

When Veeam Backup for Microsoft Azure saves a new backup restore point to a backup repository, it calculates CRC values for metadata in the backup chain and saves these values to the chain metadata, together with the instance data. When performing a health check, Veeam Backup for Microsoft Azure verifies the availability of data blocks and uses the saved values to ensure that the restore points being verified are consistent.

If you have enabled health checks for the backup policy, Veeam Backup for Microsoft Azure performs the following operations at the day scheduled for a health check to run:

1. As soon as a backup policy session completes successfully, Veeam Backup for Microsoft Azure starts the health check as a new session. For each restore point in the standard backup chain, Veeam Backup for Microsoft Azure calculates CRC values for backup metadata and compares them to the CRC values that were previously saved to the restore point. Veeam Backup for Microsoft Azure also checks whether data blocks that are required to rebuild the restore point are available.

   If the backup policy session completes with an error, Veeam Backup for Microsoft Azure tries to run the backup policy again, taking into account the maximum number of retries specified in the automatic retry settings. After the first successful retry (or after the last one out of the maximum number of retries), Veeam Backup for Microsoft Azure starts the health check.

2. If Veeam Backup for Microsoft Azure does not detect data inconsistency, the health check session completes successfully. Otherwise, the session completes with an error.

   Depending on the detected data inconsistency, Veeam Backup for Microsoft Azure performs the following operations:

   - If the health check detects corrupted metadata in a full or incremental restore point, Veeam Backup for Microsoft Azure marks the backup chain as corrupted in the configuration database. During the next backup policy session, Veeam Backup for Microsoft Azure copies the full instance image, creates a full restore point in the backup repository and starts a new backup chain in the backup repository.

> **NOTE**
>
> Veeam Backup for Microsoft Azure does not support metadata check for encrypted backup chains.

   - If the health check detects corrupted disk blocks in a full or an incremental restore point, Veeam Backup for Microsoft Azure marks the restore point that includes the corrupted data blocks and all subsequent incremental restore points as incomplete in the configuration database. During the next backup policy session, Veeam Backup for Microsoft Azure copies not only those data blocks that have changed since the previous backup session but also data blocks that have been corrupted, and saves these data blocks to the latest restore point that has been created during the current session.

## Step 8. Review Estimated Cost

At the **Cost Estimation** step of the wizard, review the approximate monthly cost of Azure services that Veeam Backup for Microsoft Azure will require to protect the Cosmos DB accounts added to the backup policy. The total estimated cost includes the following:

- The cost of creating, maintaining and retaining backups of the Cosmos DB accounts.

  For each Cosmos DB account included in the backup policy, Veeam Backup for Microsoft Azure takes into account the size of the database and the configured scheduling settings.

- The cost of transferring Cosmos DB account data between Azure regions during data protection operations (for example, if a protected Cosmos DB account and the target storage account reside in different regions).

  If you get a warning message regarding additional costs associated with cross-region data transfer, you can click **View details** to see available cost-effective options.

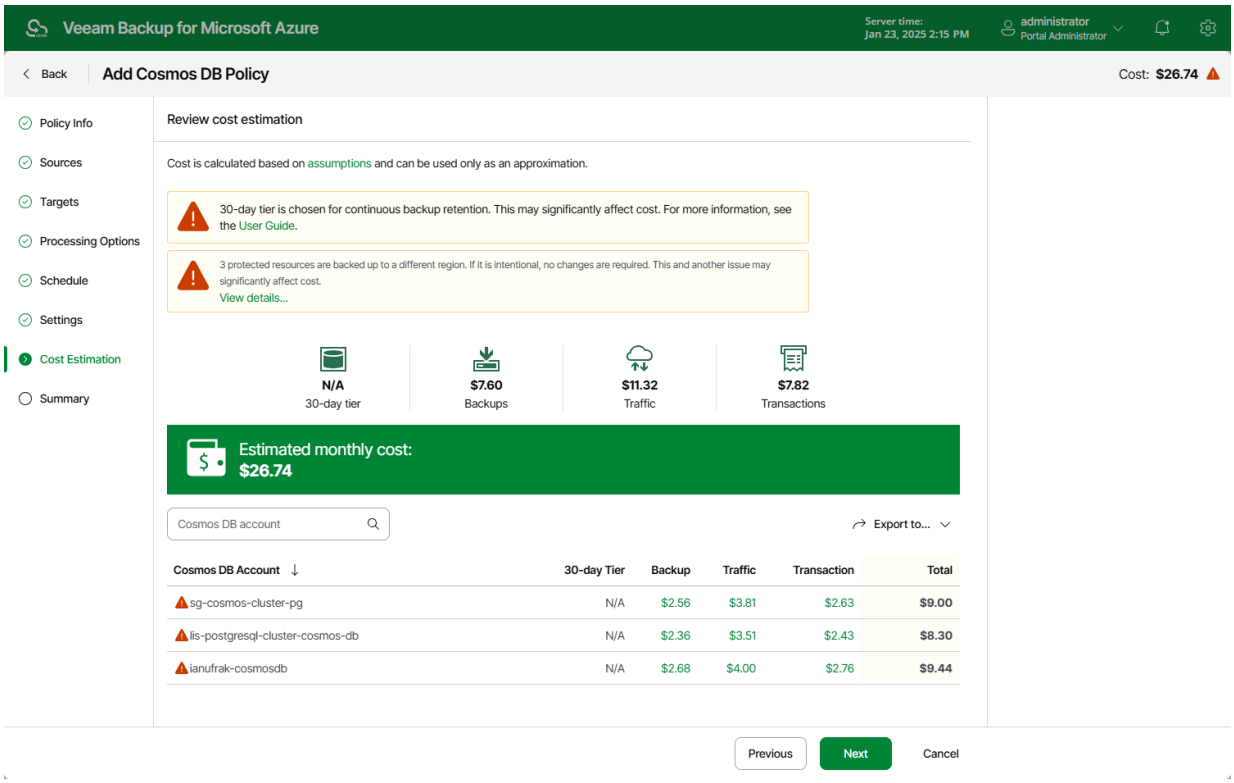
- The cost of making API requests to Microsoft Azure during data protection operations.

> **NOTES**
>
> - To calculate the estimated cost, Veeam Backup for Microsoft Azure uses the capabilities of the Azure Pricing Calculator that estimates the cost of services in USD only. This calculator is intended for informational and estimation purposes only.
> - When calculating the total cost, Veeam Backup for Microsoft Azure uses an assumption that the size of each backup is the same as the size of the source data (that is, the compression ratio is 1:1). However, this does not apply to Cosmos DB for PostgreSQL backups since the size of each Cosmos DB for PostgreSQL backup depends on the type of backed-up data — as a result, the size of this backup may occur to be significantly larger than the size of the source data. The latter may increase the cost of storing backed-up data in Microsoft Azure.

The estimated cost may occur to be significantly higher due to the backup frequency and cross-region data transfer. To reduce the cost, you can try the following workarounds:

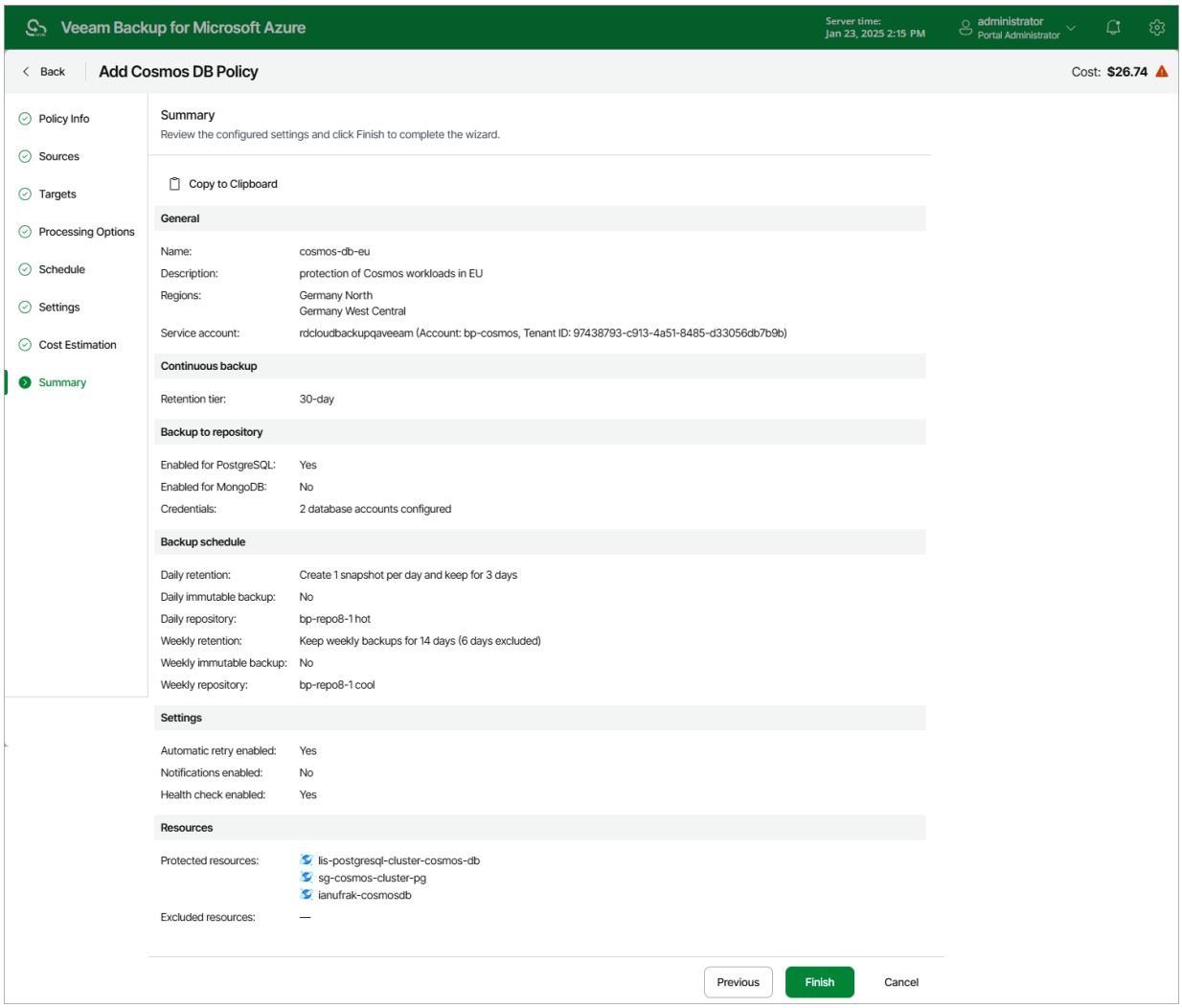
- To avoid additional costs related to cross-region data transfer, select a backup repository that resides in the same region as Cosmos DB accounts that you plan to back up.
- To optimize the cost of storing backups, modify the scheduling settings to run the backup policy less frequently, or specify an archive repository for long-term retention of restore points.
- To optimize the cost of retaining backups of Cosmos DB accounts protected using continuous backup, choose the default 7-day retention period. For more information on Cosmos DB pricing, see Microsoft Docs.

> **NOTE**
>
> If Veeam Backup for Microsoft Azure displays the total estimated cost equal to $0.00 for any Cosmos DB account, it means that the cost is less than $0.01. To view the exact value of this cost, click the link next to the account in the necessary column.


Veeam Backup for Microsoft Azure
Server time:
Jan 23, 2025 2:15 PM
administrator
Portal Administrator
Back
Add Cosmos DB Policy
Cost: $26.74
Policy Info
Sources
Targets
Processing Options
Schedule
Settings
Cost Estimation
Summary
Review cost estimation
Cost is calculated based on assumptions and can be used only as an approximation.
30-day tier is chosen for continuous backup retention. This may significantly affect cost. For more information, see the User Guide.
3 protected resources are backed up to a different region. If it is intentional, no changes are required. This and another issue may significantly affect cost.
View details...
N/A
30-day tier
$7.60
Backups
$11.32
Traffic
$7.82
Transactions
Estimated monthly cost:
$26.74
Cosmos DB account
Export to...
Cosmos DB Account
30-day Tier
Backup
Traffic
Transaction
Total
sg-cosmos-cluster-pg
N/A
$2.56
$3.81
$2.63
$9.00
lis-postgresql-cluster-cosmos-db
N/A
$2.36
$3.51
$2.43
$8.30
ianufrak-cosmosdb
N/A
$2.68
$4.00
$2.76
$9.44
Previous
Next
Cancel

## Step 9. Finish Working with Wizard

At the **Summary** step of the wizard, review summary information and click **Finish**.




# Creating Cosmos DB Backups Manually

Veeam Backup for Microsoft Azure allows you to manually create backups of Cosmos DB for PostgreSQL and Cosmos DB for MongoDB accounts.

> **NOTE**
>
> Veeam Backup for Microsoft Azure does not include backups of Cosmos DB accounts created manually in the backup chain and does not apply the configured retention policy settings to these backups. This means that the backups are kept in the backup repository unless you remove them manually, as described in section Cosmos DB Data.

To manually create backups of Cosmos DB for PostgreSQL and Cosmos DB for MongoDB accounts, do the following:

1. Navigate to **Resources** > **Databases** > **Cosmos DB**.

2. Select the check box next to the necessary Cosmos DB for PostgreSQL and Cosmos DB for MongoDB accounts and click **Take Backup Now**.

   For the accounts to be displayed in the list of available resources, they must reside in any region included in a backup policy as described in section Creating Backup Policies (step 3c).

3. Complete the **Take Manual Backup** wizard:

   a. At the **Account** step of the wizard, select a service account whose permissions Veeam Backup for Microsoft Azure will use to create backups.

      For an account to be displayed in the accounts list, it must be added to Veeam Backup for Microsoft Azure as described in section Adding Service Accounts.

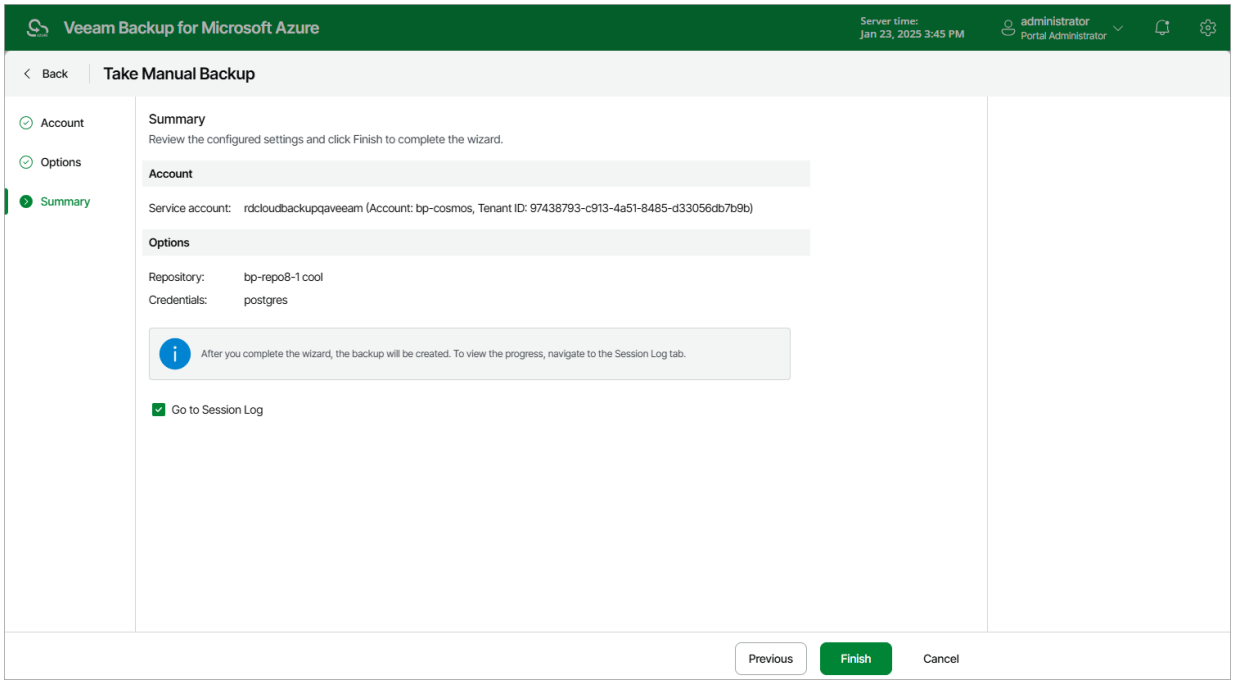
   b. At the **Options** step of the wizard, do the following:

      i. In the **Backup target** section, click **Choose repository**.

         In the **Choose repository** window, select a backup repository where the created backups will be stored. For a backup repository to be displayed in the **Repository** list, it must be added to Veeam Backup for Microsoft Azure, must have the Hot or Cool access tier assigned and must have immutability disabled, as described in section Adding Backup Repositories.

      ii. In the **Processing options** section, specify credentials that Veeam Backup for Microsoft Azure will use to connect to the processed Cosmos DB for PostgreSQL accounts. For more information, see Configure Processing Options.

   c. At the **Summary** step of the wizard, review summary information, choose whether you want to proceed to the **Session Log** page to track the progress of repository creation, and click **Finish**.



# Performing Azure Files Backup

One backup policy can be used to process one or more Azure file shares within one Microsoft Entra tenant. The scope of data that you can protect in a tenant is limited by permissions of a service account that is specified in the backup policy settings.

> **IMPORTANT**
>
> Before you create an Azure Files policy, make sure the **Allow storage account key access** option for Shared Key authorization is enabled for the storage accounts where the file shares you plan to protect reside — otherwise, backup operations will fail. For more information on Shared Key authorization, see Microsoft Docs.

To schedule data protection tasks to run automatically, create backup policies. For each protected Azure file share, you can also take a cloud-native snapshot manually when needed.

If you plan to receive email notifications on backup policy results, configure email notification settings first. For more information, see Configuring Global Notification Settings.

## Creating Azure Files Backup Policies

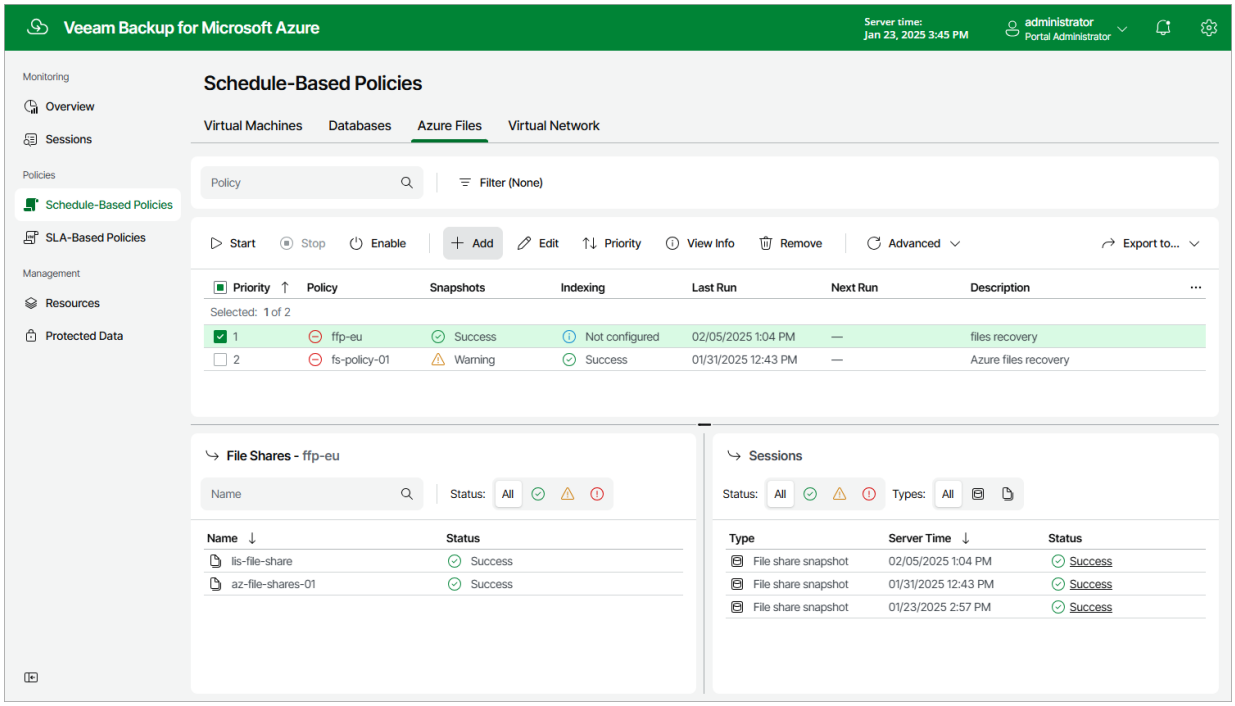
To create a backup policy, do the following:

1. Launch the Add Azure Files Policy wizard.
2. Specify a backup policy name and description.
3. Configure backup source settings.
4. Create a schedule for the backup policy.
5. Specify automatic retry settings and notification settings for the backup policy.
6. Review the estimated cost of protecting the selected Azure file shares.
7. Finish working with the wizard.

# Step 1. Launch Add Azure Files Policy Wizard

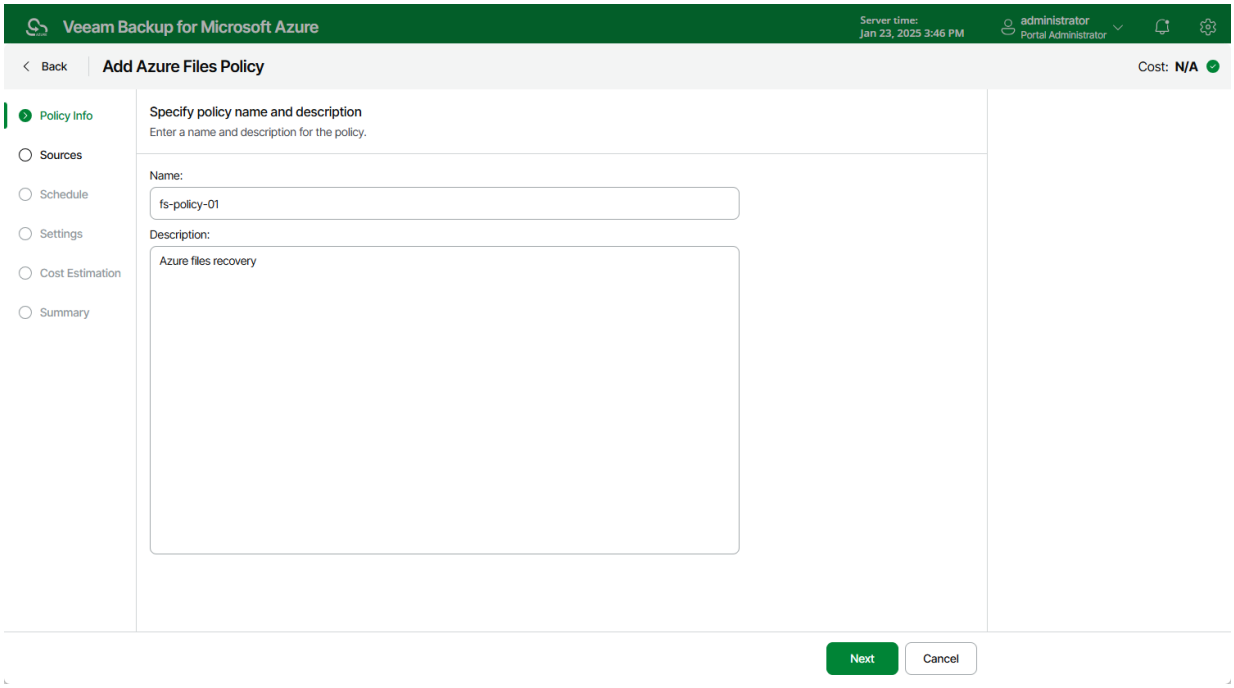
To launch the **Add Azure Files Policy** wizard, do the following:

1. Navigate to **Schedule-Based Policies**.
2. Switch to **Azure Files**.
3. Click **Add**.



# Step 2. Specify Backup Policy Name

At the **Info** step of the wizard, use the **Name** and **Description** fields to enter a name for the new backup policy and to provide a description for future reference. The maximum length of the name is 255 characters. The following characters are not supported: / \ " ' : | < > + = ; , ? ! * % # ^ @ & $ .



## Step 3. Configure Backup Source Settings

At the **Sources** step of the wizard, specify the following backup source settings:

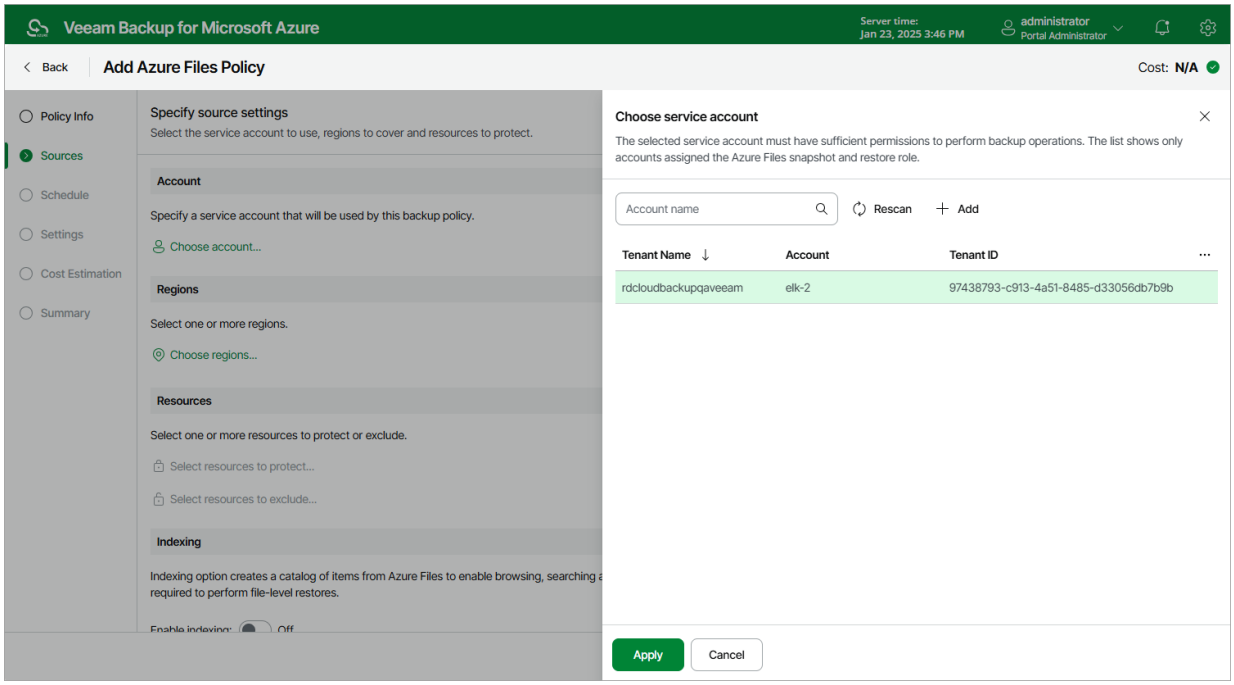
1. Select a service account whose permissions will be used to perform Azure Files backup.
2. Choose regions where Azure file shares that you want to protect reside.
3. Select resources to protect.
4. Enable Azure file share indexing.

## Step 3a. Select Service Account

In the **Account** section of the **Sources** step of the wizard, specify a service account whose permissions will be used to access Azure services and resources, and to create cloud-native snapshots of Azure file shares.

1. Click **Choose account**.
2. In the **Choose service account** window, select the necessary service account from the available accounts list. The specified service account must belong to the Microsoft Entra tenant that contains the Azure file shares that you want to protect, and must be assigned permissions listed in section Azure Files Permissions.

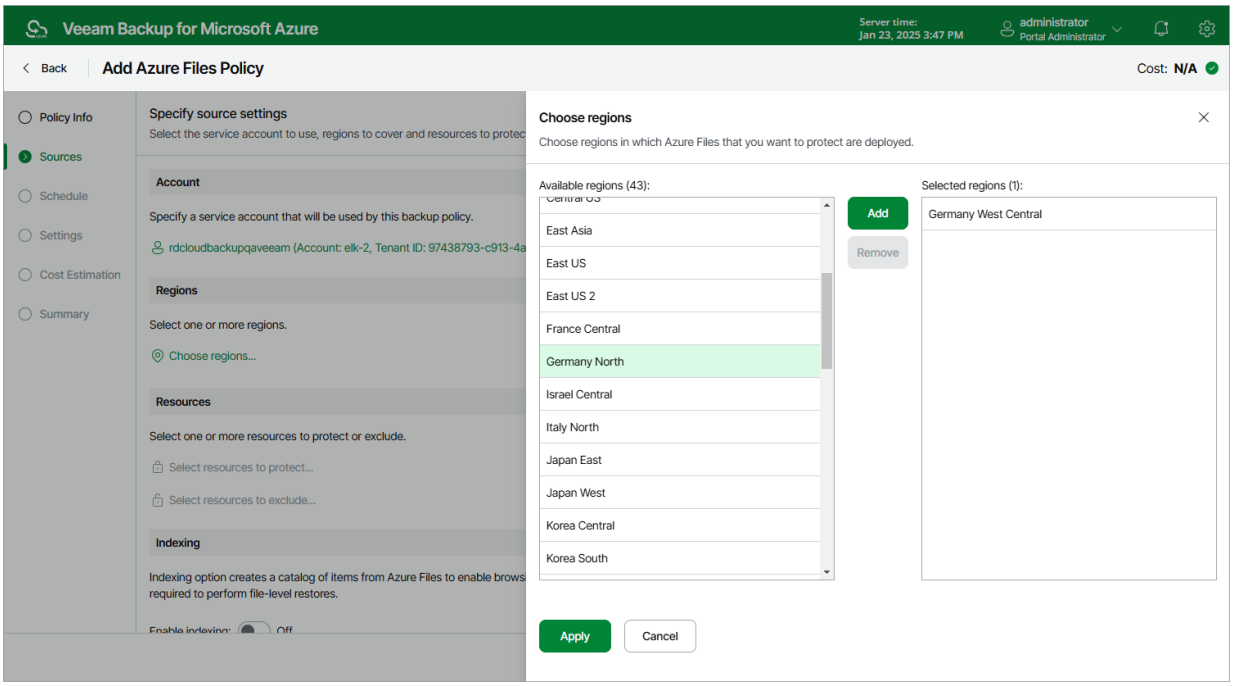
   For a service account to be displayed in the list of available accounts, it must be added to Veeam Backup for Microsoft Azure and assigned the *Azure Files Snapshot and Restore* operational role as described in section Adding Service Accounts. If you have not added the necessary service account to Veeam Backup for Microsoft Azure beforehand, you can do it without closing the **Add Azure Files Policy** wizard. To do that, click **Add** and complete the **Add Account** wizard.
3. Click **Apply**.



## Step 3b. Select Regions

In the **Region** section of the **Sources** step of the wizard, select regions where Azure resources that you want to protect reside.

1. Click **Choose regions**.
2. In the **Choose regions** window, select the necessary regions from the **Available regions** list, and then click **Add**.
3. Click **Apply**.



## Step 3c. Select Resources

In the **Resources** section of the **Sources** step of the wizard, specify the backup scope — select resources that Veeam Backup for Microsoft Azure will back up.

1. Click **Select resources to protect**.
2. In the **Choose resource protection options** window, choose whether you want to protect all Azure resources from the regions selected at step 3b, or only specific resources.

   If you select the **All resources** option, Veeam Backup for Microsoft Azure will regularly check for new Azure file shares created in the selected regions and automatically update the backup policy settings to include these file shares in the backup scope.

   If you select the **Protect the following resources** option, you must also specify the resources explicitly:

   a. Use the **Resource type** drop-down list to select either of the following options:

      - *Resource group* — to protect Azure file shares that belong to specific resource groups.
      - *File Share* — to protect only specific Azure file shares.
      - *Storage account* — to protect Azure file shares that reside in specific storage accounts.

   b. Use the search field to the right of the **Resource type** list to find the necessary resource, and then click **Protect** to add the resource to the backup scope.

      For a resource to be displayed in the list of available resources, it must reside in an Azure region that has ever been specified in any backup policy. Otherwise, the only option to discover available resources is to click **Browse to select a target from the global list** and wait for Veeam Backup for Microsoft Azure to populate the resource list.

      Note that your web browser zoom must not exceed 135% for the list of protected resources to be displayed correctly.

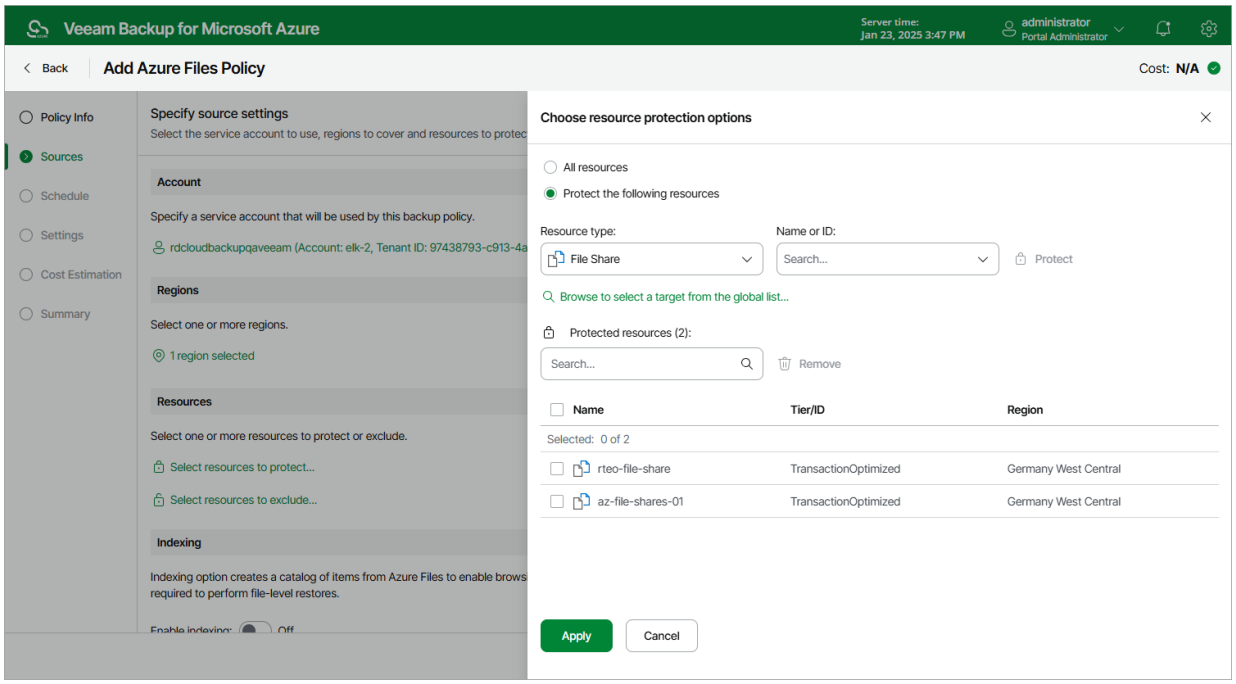
> **TIP**
>
> You can simultaneously add multiple resources to the backup scope. To do that, click **Browse to select a target from the global list**, select check boxes next to the necessary items in the list of available resources, and then click **Protect**.
>
> If the list does not show the resources that you want to protect, click **Rescan** to launch the data collection process — as soon as the process is over, Veeam Backup for Microsoft Azure will update the resource list. If you still cannot find the necessary resources in the list, make sure that the *Microsoft.ManagedServices* provider is registered in the subscription to which the resources belong, return to step 3a and click **Rescan** in the **Choose service account** window. To learn how to register a resource provider, see Microsoft Docs.

4. To save changes made to the backup policy settings, click **Apply**.

### TIP

As an alternative to selecting the **Protect the following resources** option and specifying the resources explicitly, you can select the **All resources** option and exclude a number of resources from the backup scope. To do that, click **Select resources to exclude** and specify Azure file shares that you do not want to protect — the procedure is the same as described for including resources in the backup scope.

Consider that if a resource appears both in the list of included and excluded resources, Veeam Backup for Microsoft Azure will still not process the resource because the list of excluded resources has a higher priority.



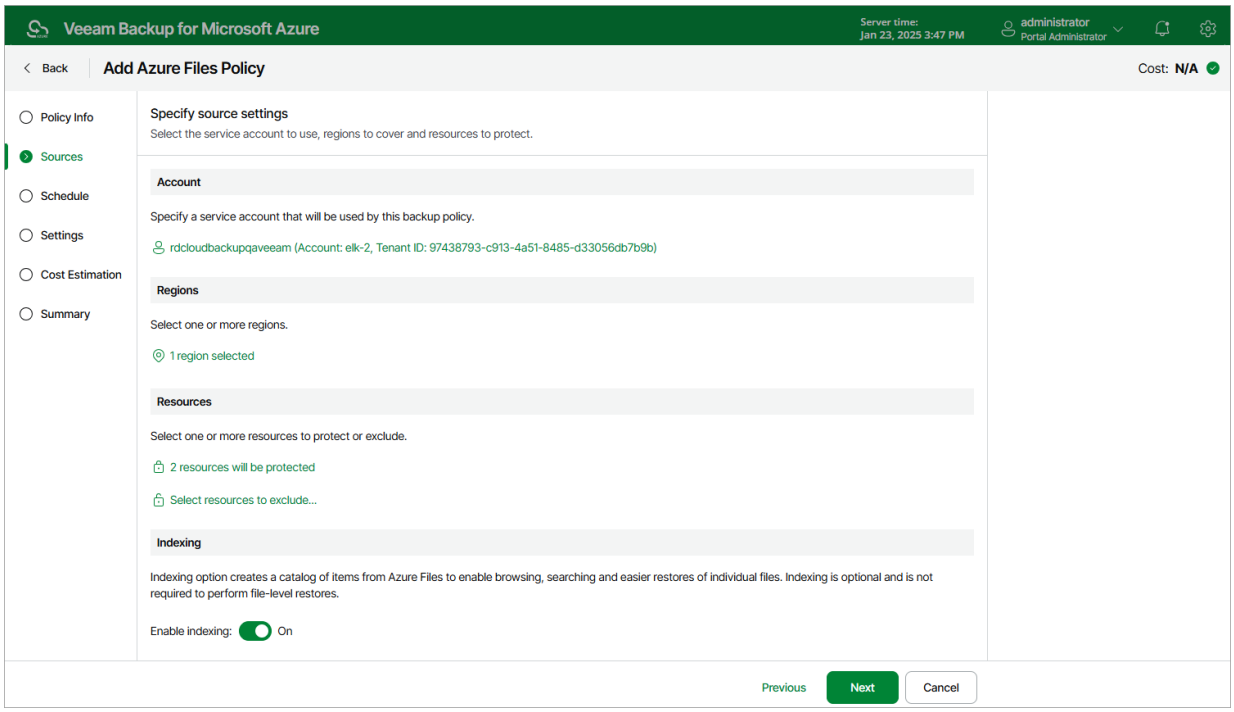
## Step 3d. Enable File Share Indexing

While performing Azure file share indexing for a file system, Veeam Backup for Microsoft Azure creates a catalog of all files and directories (that is, the index) and saves the index to the configuration database on the backup appliance. This index is further used to reproduce the file system structure and to enable browsing and searching for specific files across multiple restore points. To learn how indexing works, see Azure Files Backup.

> **IMPORTANT**
>
> When performing indexing operations, Veeam Backup for Microsoft Azure uses the Server Message Block (SMB) 3.0 and New Technology LAN Manager (NTLM) v2 protocols to authenticate against the processed file shares. That is why authentication using these protocols must be enabled on the file shares that you plan to index. Otherwise, indexing of the file shares will fail.
>
> For more information on Azure Files identity-based authentication options for SMB access, see Microsoft Docs.

In the **Indexing** section of the **Sources** step of the wizard, you can instruct Veeam Backup for Microsoft Azure to perform indexing of the processed Azure file shares. To do that, set the **Enable indexing** toggle to *On*.

> **NOTE**
>
> Azure file share indexing is not supported in the *Free* edition of Veeam Backup for Microsoft Azure. For more information on license editions, see Licensing.



## Step 4. Specify Policy Scheduling Options

You can instruct Veeam Backup for Microsoft Azure to start the backup policy automatically according to a specific backup schedule. The backup schedule defines how often data stored in file systems added to the backup policy will be backed up.

To help you implement a comprehensive backup strategy, Veeam Backup for Microsoft Azure allows you to create schedules of the following types:

- Daily — the backup policy will create restore points repeatedly throughout a day on specific days.
- Weekly — the backup policy will create restore points once a day on specific days.
- Monthly — the backup policy will create restore points once a month on a specific day.

Combining multiple schedule types together allows you to keep restore points for longer periods of time. For more information, see Enabling Harmonized Scheduling.

### Specifying Daily Schedule

To create a daily schedule for the backup policy, at the **Schedule** step of the wizard, do the following:

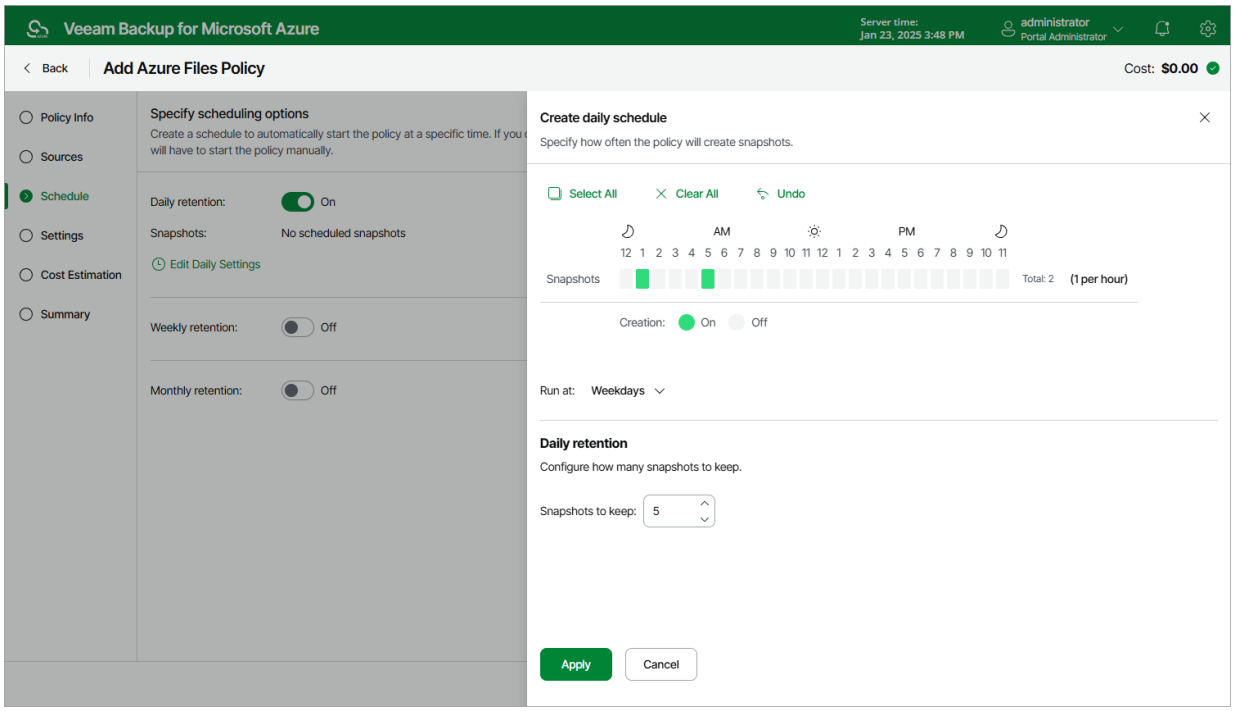
1. Set the **Daily retention** toggle to *On* and click **Edit Daily Settings**.
2. In the **Create daily schedule** window, select hours when Veeam Backup for Microsoft Azure will create snapshots.

> **NOTE**
>
> Since Veeam Backup for Microsoft Azure runs retention sessions at 12:15 AM according to the time zone set on the backup appliance, it is not recommended that you schedule backup policies to execute at 12:15 AM. Otherwise, Veeam Backup for Microsoft Azure will not be able to run the retention sessions.

3. Use the **Run at** drop-down list to choose whether you want the backup policy to run everyday, on weekdays (Monday through Friday) or on specific days.
4. In the **Daily retention** section, specify the number of restore points that you want to keep in a snapshot chain.

   If the restore point limit is exceeded, Veeam Backup for Microsoft Azure removes the earliest restore point from the chain. For more information, see File Share Snapshot Retention.

5. To save changes made to the backup policy settings, click **Apply**.



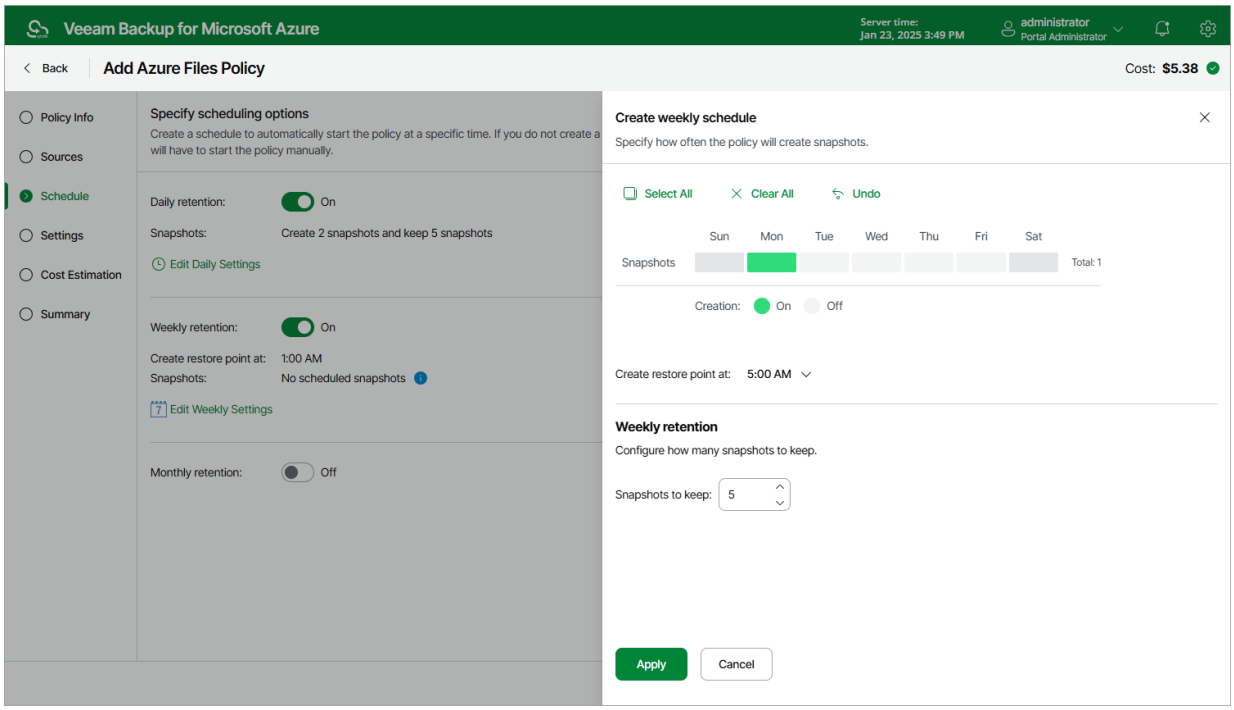

## Specifying Weekly Schedule

To create a weekly schedule for the backup policy, at the **Schedule** step of the wizard, do the following:

1. Set the **Weekly retention** toggle to *On* and click **Edit Weekly Settings**.
2. In the **Create weekly schedule** window, select days of the week when Veeam Backup for Microsoft Azure will create snapshots.
3. Use the **Create restore points at** drop-down list to schedule a specific time for the backup policy to run.
4. In the **Weekly retention** section, specify the number of restore points that you want to keep in a snapshot chain.

   If the restore point limit is exceeded, Veeam Backup for Microsoft Azure removes the earliest restore point from the chain. For more information, see File Share Snapshot Retention.

5. To save changes made to the backup policy settings, click **Apply**.



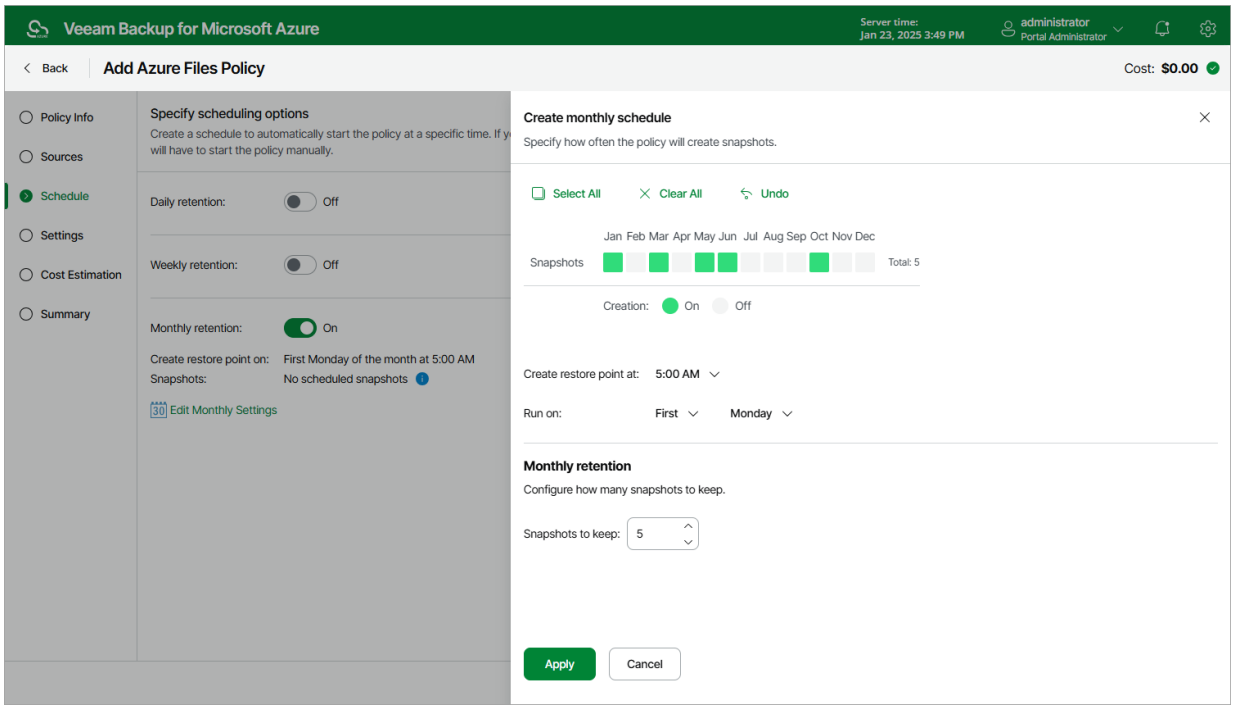

## Specifying Monthly Schedule

To create a monthly schedule for the backup policy, at the **Schedule** step of the wizard, do the following:

1. Set the **Monthly retention** toggle to *On* and click **Edit Monthly Settings**.
2. In the **Create monthly schedule** window, select months when the backup policy will create snapshots.
3. Use the **Create restore points at** and **Run on** drop-down lists to schedule a specific time and day for the backup policy to run.
4. In the **Monthly retention** section, specify the number of restore points that you want to keep in a snapshot chain.

   If the restore point limit is exceeded, Veeam Backup for Microsoft Azure removes the earliest restore point from the chain. For more information, see File Share Snapshot Retention.

5. To save changes made to the backup policy settings, click **Apply**.




## Enabling Harmonized Scheduling

When you combine multiple types of schedules, Veeam Backup for Microsoft Azure applies the harmonization mechanism that allows you to leverage restore points for long-term retentions instead of taking a new restore point every time. The mechanism simplifies the backup schedule, optimizes the backup performance and reduces the cost of storing restore points in backup repositories.

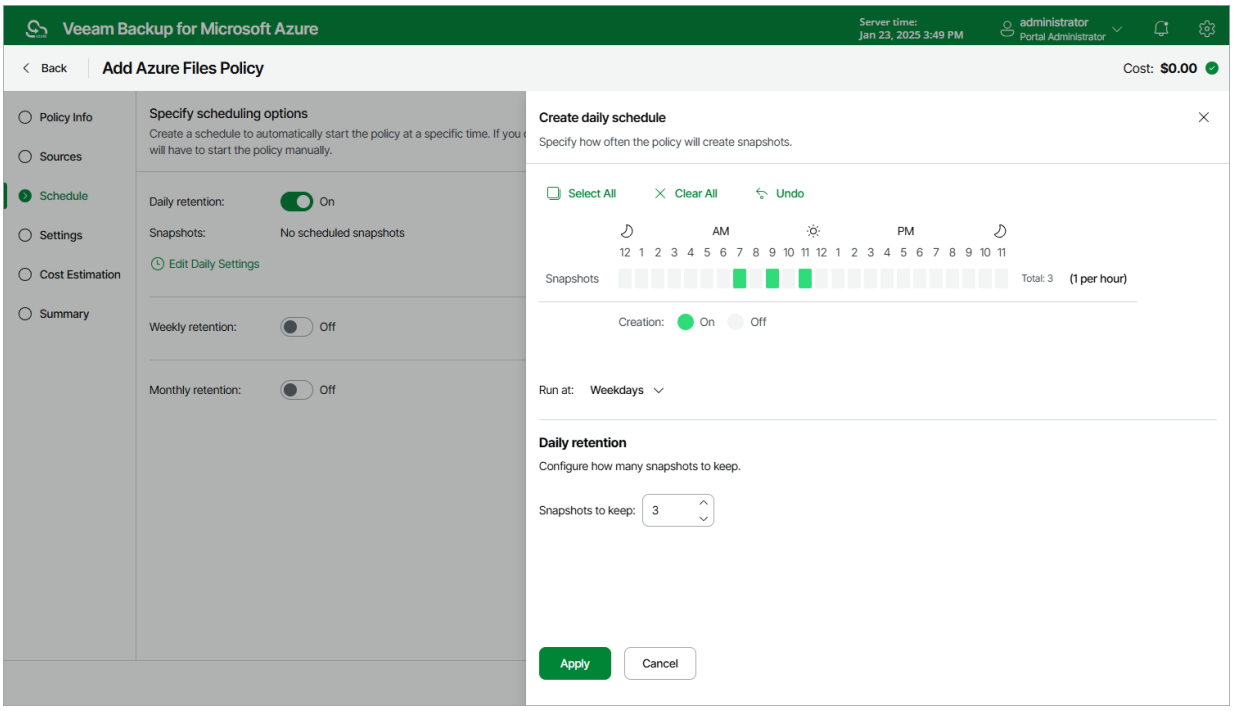
With harmonized scheduling, Veeam Backup for Microsoft Azure can keep restore points created according to a daily or weekly schedule for longer periods of time (for weeks and months).

For Veeam Backup for Microsoft Azure to use the harmonization mechanism, there must be specified at least 2 different schedules: one schedule will control the regular creation of restore points, while another schedule will control the process of retaining restore points. In terms of harmonized scheduling, Veeam Backup for Microsoft Azure re-uses restore points created according to a more-frequent schedule (daily or weekly) to achieve the desired retention for less-frequent schedules (weekly and monthly). Each restore point is marked with a flag of the related schedule type: the (Daily) flag is used to mark restore points created daily, (Weekly) — weekly, and (Monthly) — monthly. Veeam Backup for Microsoft Azure uses these flags to control the retention period for the created restore points. Once a flag of a less-frequent schedule is assigned to a restore point, this restore point can no longer be removed — it is kept for the period defined in the retention settings. When the specified retention period is over, the flag is unassigned from the restore point. If the restore point does not have any other flags assigned, it is removed according to the retention settings of a more-frequent schedule.

Consider the following example. You want a backup policy to create cloud-native snapshots of your critical workloads 3 times a day, to keep 3 daily snapshots in the snapshot chain, and also to retain one of the created snapshots for 2 weeks. In this case, you create 2 schedules when configuring the backup policy settings — daily and weekly:

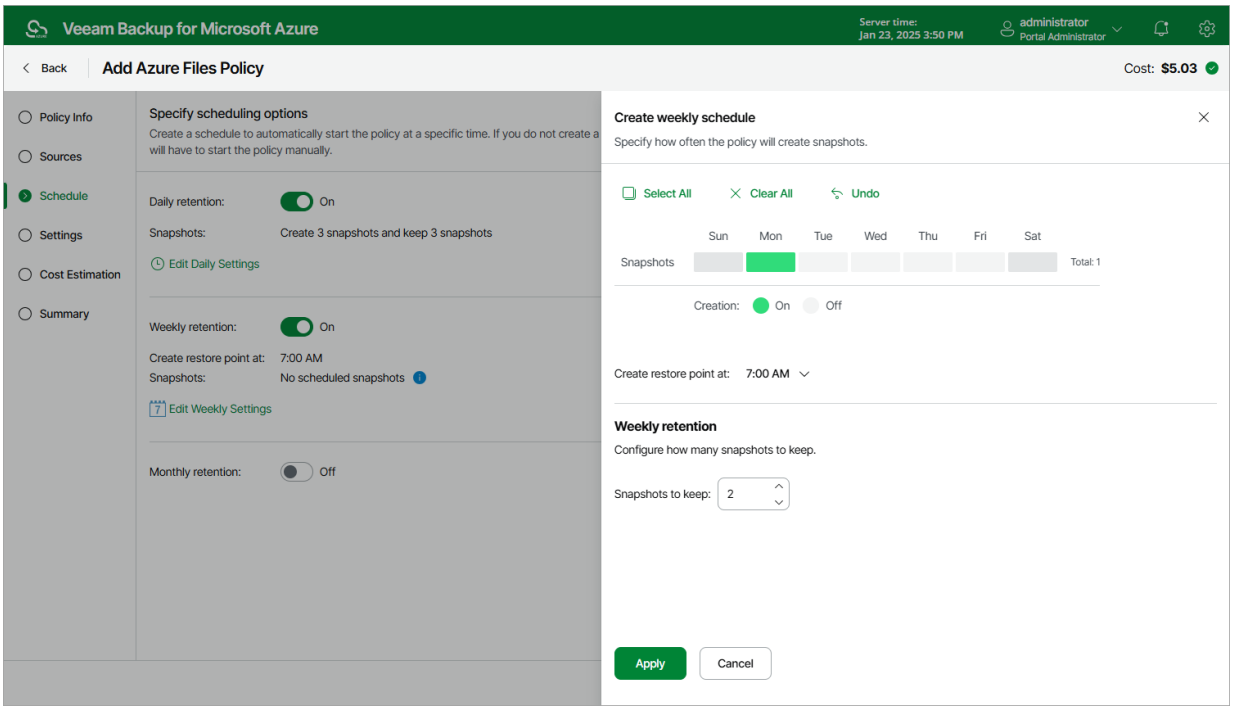
1. In the daily scheduling settings, you select hours and days when snapshots will be created (for example, *7:00 AM*, *9:00 AM*, and *11:00 AM*; *Weekdays*), and specify the number of daily restore points to retain (for example, *3*).

   Veeam Backup for Microsoft Azure will propagate these settings to the schedule with a lower frequency (which is the weekly schedule in our example).



2. In the weekly scheduling settings, you specify which one of the snapshots created by the daily schedule will be kept, and choose for how long you want to keep the selected snapshot.

   For example, if you want to keep the daily restore point created at 7:00 AM on Monday for 2 weeks, you select *7:00 AM*, *Monday* and specify *2* restore points to retain in the weekly schedule settings.

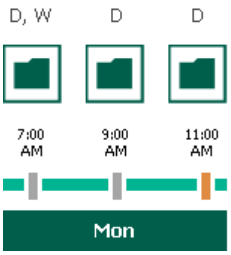



According to the specified scheduling settings, Veeam Backup for Microsoft Azure will create cloud-native snapshots in the following way:

1. On the first work day (Monday), a backup session will start at 7:00 AM to create the first restore point. The restore point will be marked with the (D) flag as it was created according to the daily schedule.

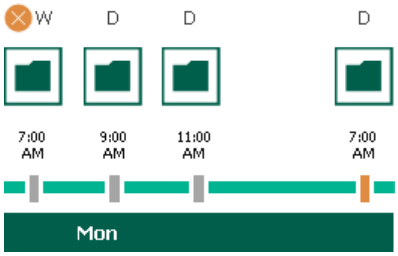
   Since *7:00 AM*, *Monday* is specified in the weekly scheduling settings, Veeam Backup for Microsoft Azure will assign the (W) flag to this restore point.

2. On the same day (Monday), after backup sessions run at 9:00 AM and 11:00 AM, the created restore points will be marked with the (D) flag.

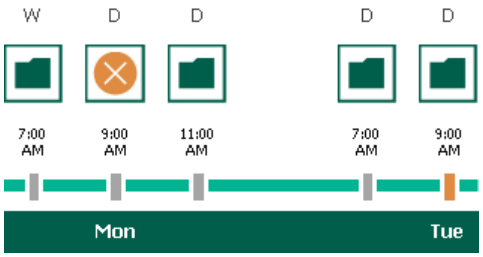


3. On the next work day (Tuesday), after a backup session runs at 7:00 AM, the created restore point will be marked with the (D) flag.

   At the moment the backup session completes, the number of restore points with the (D) flag will exceed the retention limit specified in the daily scheduling settings. However, Veeam Backup for Microsoft Azure will not remove the earliest restore point (*7:00 AM*, *Monday*) with the (D) flag from the snapshot chain as this restore point is also marked with a flag of a less-frequent schedule. Instead, Veeam Backup for Microsoft Azure will unassign the (D) flag from the restore point. This restore point will be kept for the retention period specified in the weekly scheduling settings (that is, for 2 weeks).

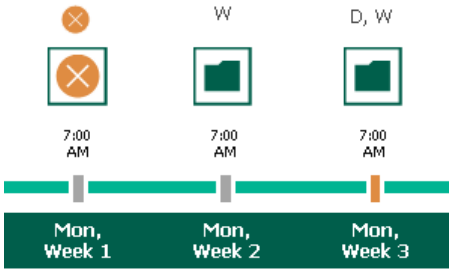



4. On the same day (Tuesday), after a backup session runs at 9:00 AM, the number of restore points with the (D) flag will exceed the retention limit once again. Veeam Backup for Microsoft Azure will remove from the snapshot chain the restore point created at 9:00 AM on Monday as no flags of a less-frequent schedule are assigned to this restore point.




5. Veeam Backup for Microsoft Azure will continue creating restore points for the next week in the same way as described in steps 1-4.

6. On week 3, after a backup session runs at 7:00 AM on Monday, the number of kept restore points will exceed the retention limit. Veeam Backup for Microsoft Azure will unassign the (W) flag from the earliest kept restore point. Since no other flags are assigned to this restore point, Veeam Backup for Microsoft Azure will remove this restore point from the snapshot chain.



## Step 5. Configure General Settings

At the **Settings** step of the wizard, you can enable automatic retries and specify notification settings for the backup policy.

# Automatic Retry Settings

To instruct Veeam Backup for Microsoft Azure to run the backup policy again if it fails on the first try, do the following:

1. In the **Schedule** section of the step, select the **Automatic retry failed policy** check box.
2. In the field to the right of the check box, specify the maximum number of attempts to run the backup policy. The time interval between retries is 600 seconds.

When retrying backup policies, Veeam Backup for Microsoft Azure processes only those Azure file shares that failed to be protected during the previous attempt.

> **NOTE**
>
> The automatic retry settings apply only to backup policies that run according to specific schedules — these settings do not apply to policies started manually.

# Notification Settings

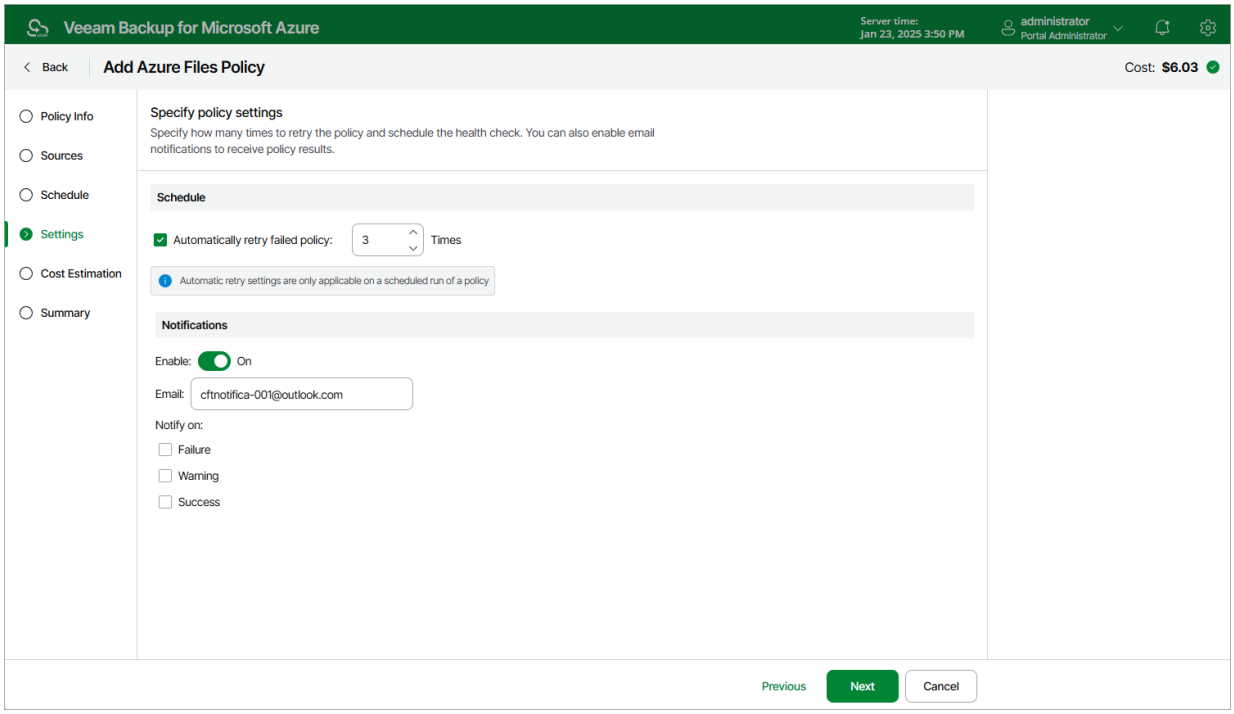
To instruct Veeam Backup for Microsoft Azure to send email notifications for the backup policy, do the following:

1. In the **Notifications** section of the step, set the **Enabled** toggle to *On*.

   If you set the toggle to *Off*, Veeam Backup for Microsoft Azure will not send any notifications for this backup policy — regardless of the configured global notification settings.
2. In the **Email** field, specify an email address of a recipient. Use a semicolon to separate multiple recipient addresses.
3. Use the **Notify on** list to choose whether you want Veeam Backup for Microsoft Azure to send email notifications in case the backup policy completes successfully, completes with warnings or completes with errors.

## NOTE

If you specify the same email recipient in both backup policy notification and global notification settings, Veeam Backup for Microsoft Azure will override the configured global notification settings and will send each notification to this recipient only once to avoid notification duplicates.



# Step 6. Review Estimated Cost

[This step applies only if you have created a schedule for the backup policy at the **Schedule** step of the wizard]

At the **Cost Estimation** step of the wizard, review the approximate monthly cost of Azure services that Veeam Backup for Microsoft Azure will require to protect the Azure file shares added to the backup policy. The total estimated cost includes the following:

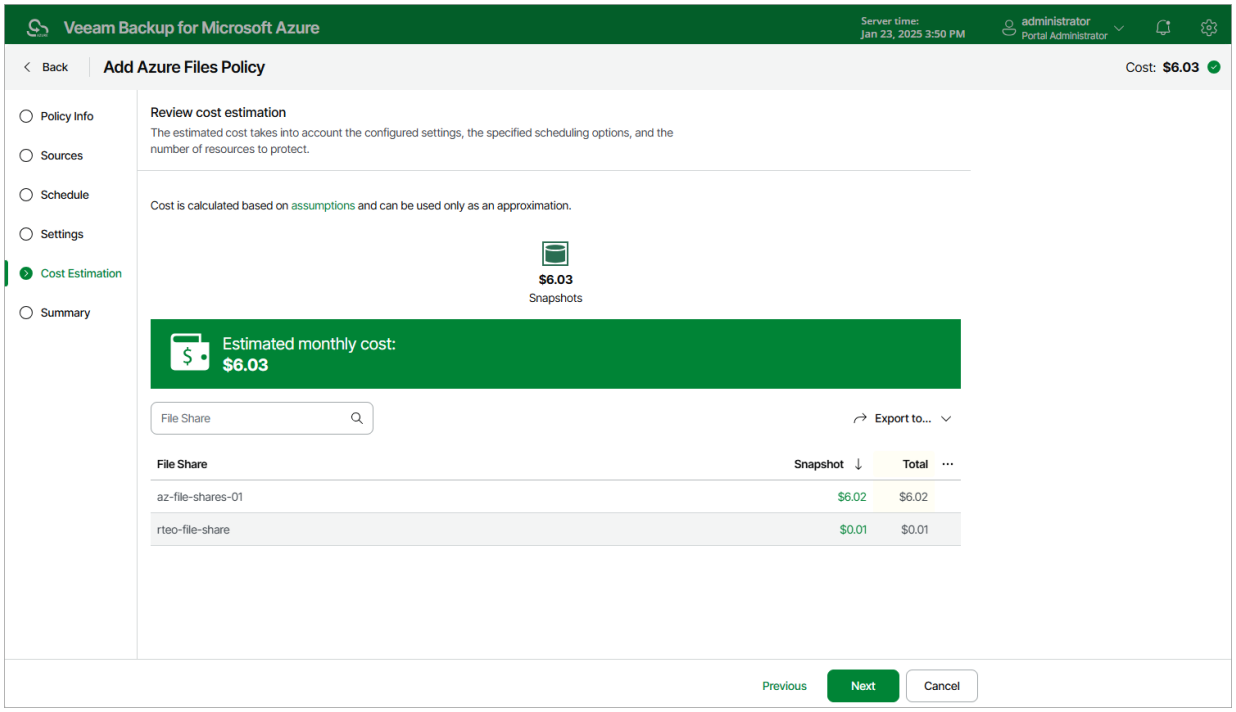
- The cost of creating and maintaining snapshots of the Azure file shares.

  For each Azure file share included in the backup policy, Veeam Backup for Microsoft Azure takes into account the number of restore points to be kept in the snapshot chain and the configured scheduling settings.

- The cost of making API requests to Microsoft Azure during data protection operations.

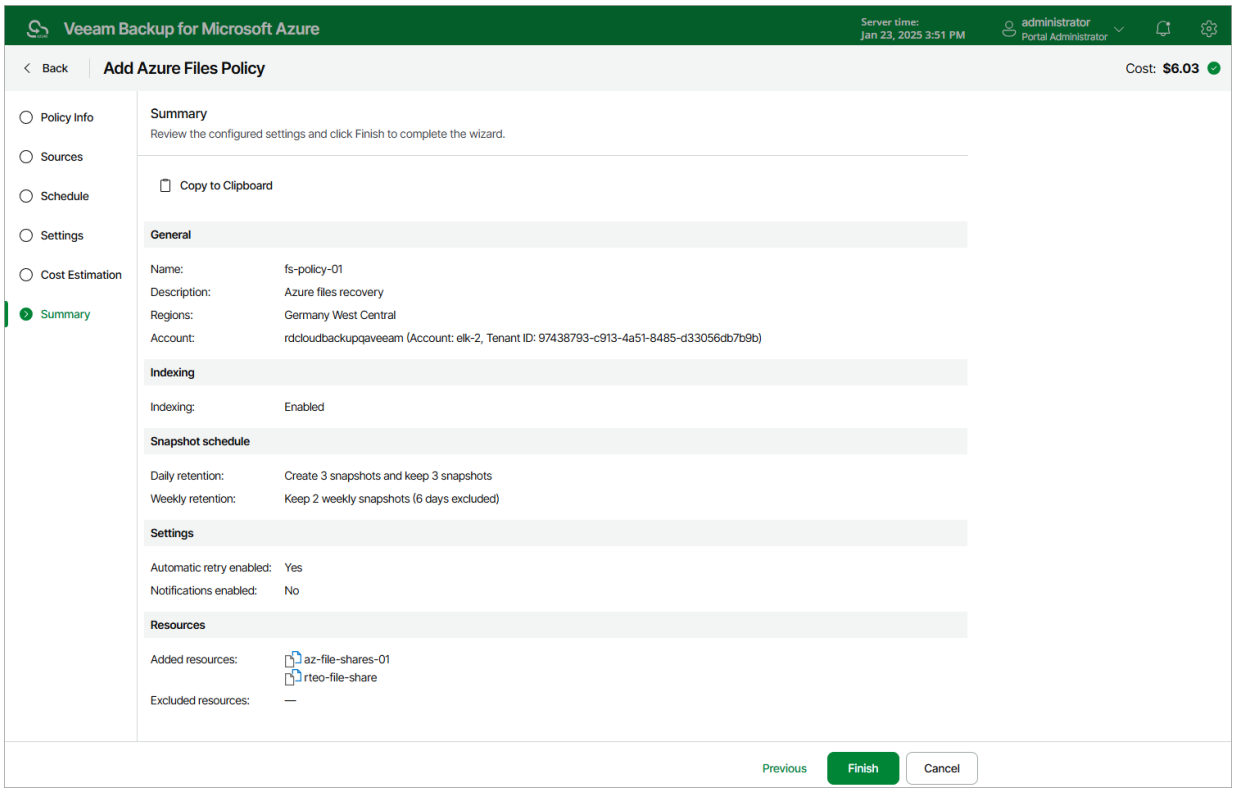
> **NOTE**
>
> To calculate the estimated cost, Veeam Backup for Microsoft Azure uses the capabilities of the Azure Pricing Calculator that estimates the cost of services in USD only. This calculator is intended for informational and estimation purposes only.

The estimated cost may occur to be significantly higher due to the backup frequency and snapshot charges. To reduce high snapshot charges, adjust the snapshot retention settings to keep less restore points in the snapshot chain.



## Step 7. Finish Working with Wizard

At the **Summary** step of the wizard, review summary information and click **Finish**.




# Creating File Share Snapshots Manually

Veeam Backup for Microsoft Azure allows you to manually create snapshots of Azure file shares. Each snapshot is saved to the same Azure region in which the protected Azure file share resides.

> **NOTE**
>
> Veeam Backup for Microsoft Azure does not include snapshots created manually in the snapshot chain and does not apply the configured retention policy settings to these snapshots. This means that the snapshots are kept in your Microsoft Azure environment unless you remove them manually, as described in section Azure Files Data.

To manually create a cloud-native snapshot of an Azure file share, do the following:

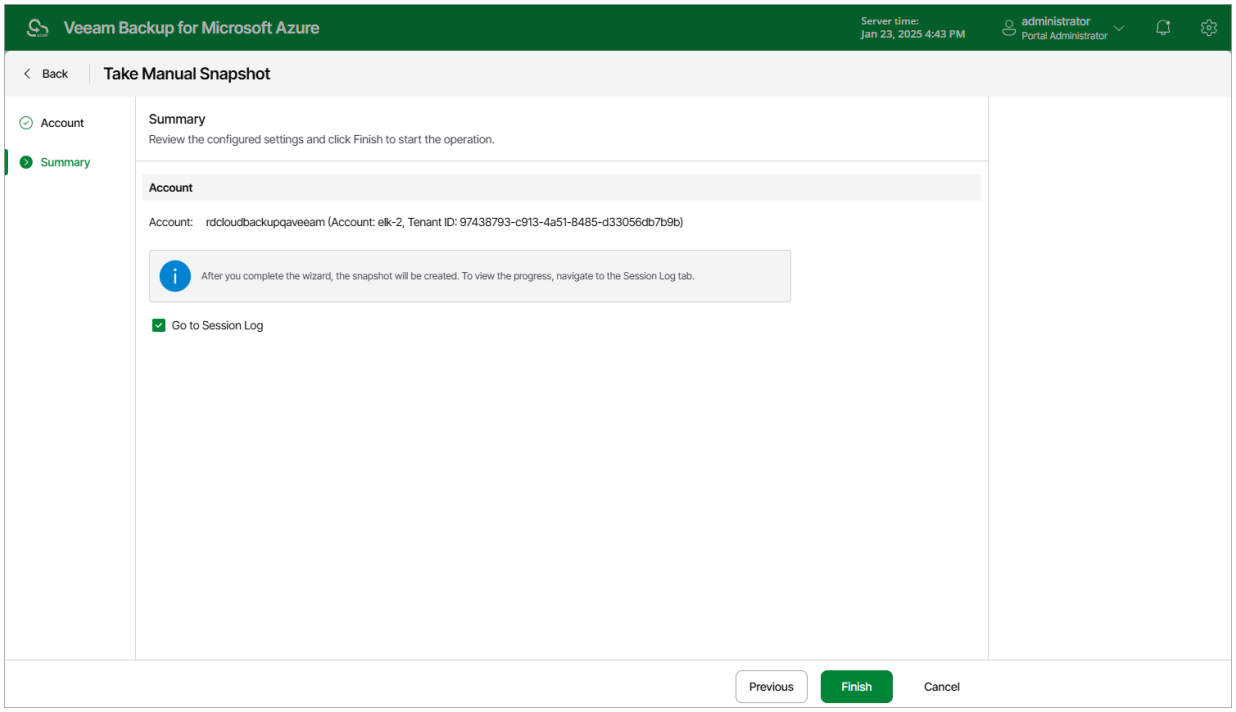
1. Navigate to **Resources** > **Azure Files**.
2. Select the check box next to the necessary Azure file share and click **Take Snapshot Now**.

   For an Azure file share to be displayed in the list of available resources, it must reside in any region included in a backup policy as described in section Creating Backup Policies (step 3c).
3. Complete the **Take Manual Snapshot** wizard:

   a. At the **Account** step of the wizard, select a service account whose permissions Veeam Backup for Microsoft Azure will use to create a snapshot.

   For an account to be displayed in the accounts list, it must be added to Veeam Backup for Microsoft Azure as described in section Adding Service Accounts.

b. At the **Summary** step of the wizard, review configuration information, choose whether you want to proceed to the Session Log page to track the progress of snapshot creation, and click **Finish**.



# Performing Virtual Network Configuration Backup

> **IMPORTANT**
>
> Virtual network configuration backup is available only for backup appliances managed by a Veeam Backup & Replication server. To unlock the full functionality, you must install Microsoft Azure Plug-in for Veeam Backup & Replication on the server and add your appliances to the backup infrastructure.

To protect the Azure virtual network configuration and settings, Veeam Backup for Microsoft Azure comes with a preconfigured Virtual Network Configuration Backup policy. With this policy, you can protect virtual network configurations of Azure subscriptions associated with your Microsoft Entra tenants.

Veeam Backup for Microsoft Azure supports backup of the following virtual network configuration components: virtual networks, subnets, IP configurations, network security groups, route tables, network interfaces and virtual network peerings.

The Virtual Network Configuration Backup policy is disabled by default. To start protecting your Azure virtual network configuration, edit backup policy settings and enable the policy.

## Editing Virtual Network Configuration Backup Policy

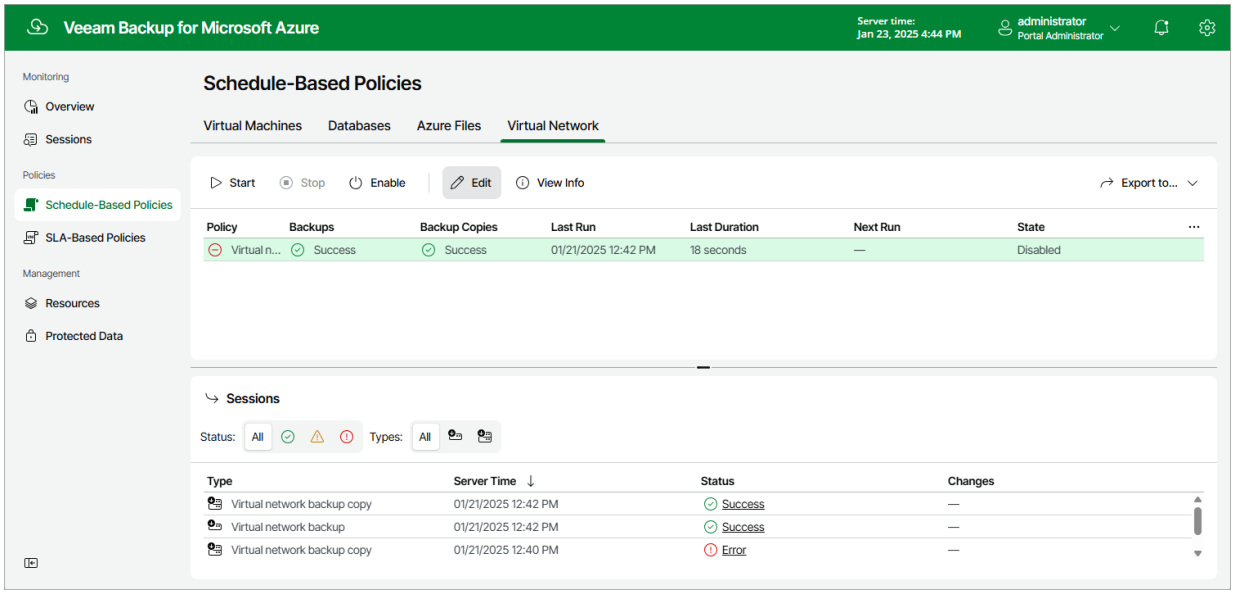
To configure the virtual network configuration backup policy settings, perform the following steps:

1. Launch the Virtual Network Configuration Backup wizard.
2. Select Azure subscriptions to protect.
3. Enable additional backup copy.
4. Configure retention settings for Azure virtual network configuration backups.
5. Specify automatic retry settings and notification settings.
6. Finish working with the wizard.

# Step 1. Launch Virtual Network Configuration Backup Wizard

To launch the **Virtual Network Configuration Backup** wizard, do the following:

1. Navigate to **Policies** > **Virtual Network**.
2. Click **Edit**.



## Step 2. Select Azure Subscriptions

At the **Subscriptions** step of the wizard, select Azure subscriptions whose virtual network configuration you want to back up.

Veeam Backup for Microsoft Azure allows you to automatically collect and back up virtual network configuration data for all Azure subscriptions selected for Azure VM, Azure SQL and Azure Files backup policies. To do that, enable automatic protection for Azure subscriptions. To retrieve virtual network configurations of all automatically protected Azure subscriptions, Veeam Backup for Microsoft Azure will use permissions of service accounts specified in the settings of backup policies that protect resources residing in these Azure subscriptions.

You can also configure the Virtual Network Configuration Backup policy to protect configuration data for Azure subscriptions that are not specified in the settings of any backup policy, or choose another service account whose permissions Veeam Backup for Microsoft Azure will use to collect the virtual network configuration data of the automatically protected Azure subscriptions. To do that, manually add Azure subscriptions to the Virtual Network Configuration Backup policy and configure backup settings for them.

### Enabling Automatic Protection

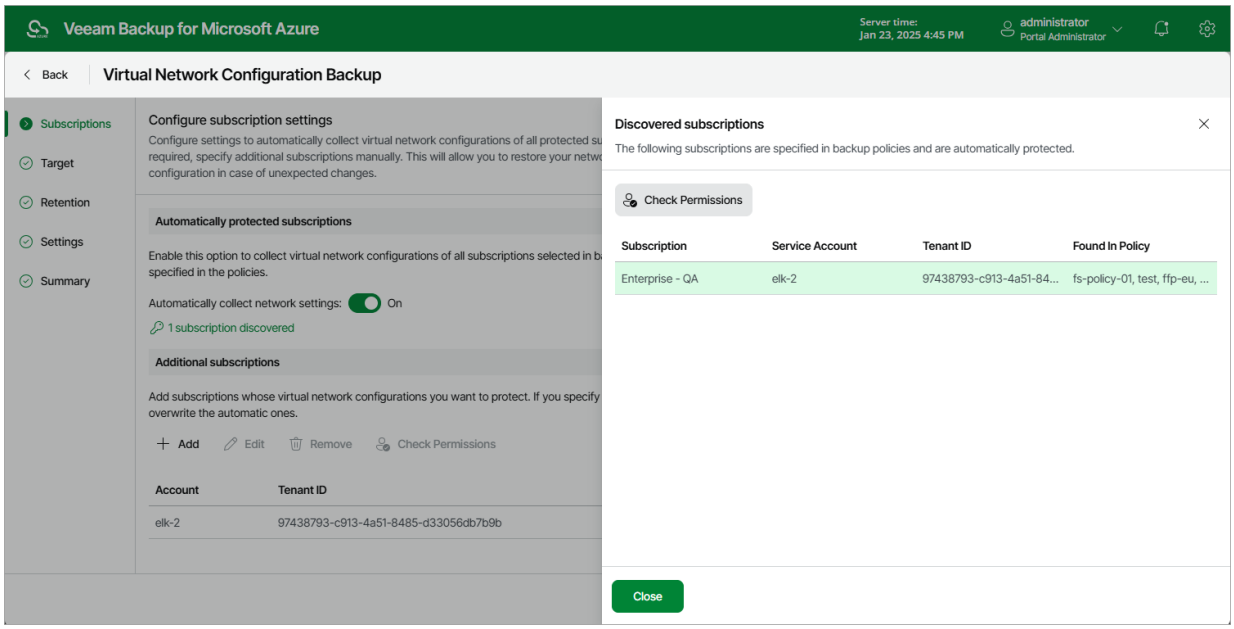
To instruct Veeam Backup for Microsoft Azure to protect the virtual network configuration of all Azure subscriptions specified in Azure VM, Azure SQL and Azure Files backup policy settings, in the **Automatically protected subscriptions** section, set the **Automatically collect network settings** toggle to *On*.

To retrieve virtual network configurations of all automatically protected Azure subscriptions, Veeam Backup for Microsoft Azure will use permissions of service accounts specified in the settings of backup policies that protect instances residing in these Azure subscriptions. It is recommended that you check whether service accounts whose permissions Azure VM, Azure SQL and Azure Files backup policies use to perform data protection operations have all the permissions required to perform Azure virtual network configuration backup. If the service account permissions are insufficient, the backup policy will fail.

To run the service account permission check:

1. In the **Automatically protected subscriptions** section, click the **Discovered subscriptions** link.
2. In the **Discovered subscriptions** window, select the service account whose permissions you want to check.
3. Click **Check Permissions**.

Veeam Backup for Microsoft Azure will display the **Permission Check** window where you can view the results of the performed check. If the service account permissions are insufficient, the check will complete with errors. You can view the list of permissions that must be granted to service accounts in the **Details** column. You can grant the missing permissions to service accounts as described in section Checking Service Account Permissions.



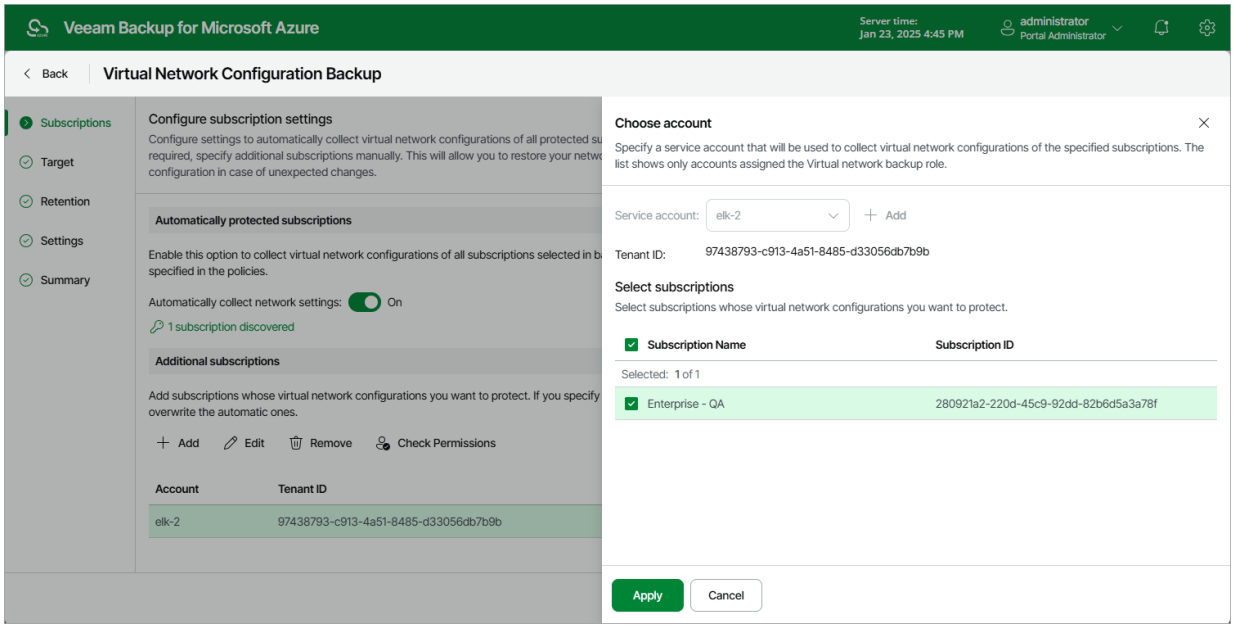

## Adding Azure Subscriptions Manually

To add an Azure subscription to the Virtual Network Configuration Backup policy, or to choose another service account for collecting virtual network configuration data, do the following:

1. In the **Additional subscriptions** section, click **Add**.
2. In the **Account settings** window, from the **Service account** drop-down list, select a service account whose permissions Veeam Backup for Microsoft Azure will use to perform virtual network configuration backup. The specified service account must belong to the Microsoft Entra tenant associated with the subscription whose virtual network configuration you want to protect, and must be assigned permissions listed in section Virtual Network Configuration Permissions.

   For a service account to be displayed in the list of available accounts, it must be added to Veeam Backup for Microsoft Azure and assigned the *Virtual Network Backup* operational role as described in section Adding Service Accounts. If you have not added the necessary service account to Veeam Backup for Microsoft Azure beforehand, you can do it without closing the **Virtual Network Configuration Backup** wizard. To do that, click **Add** and complete the **Add Account** wizard.
3. In the **Select subscriptions** section, select the necessary Azure subscriptions from the list.
4. To save changes made to the backup policy settings, click **Apply**.
5. To check whether the service account specified for the selected Azure subscriptions has all the permissions required to perform Azure virtual network configuration backup, in the **Additional subscriptions** section, click **Check Permissions**.

You can add, edit or remove additional Azure subscriptions from the Virtual Network Configuration Backup policy.



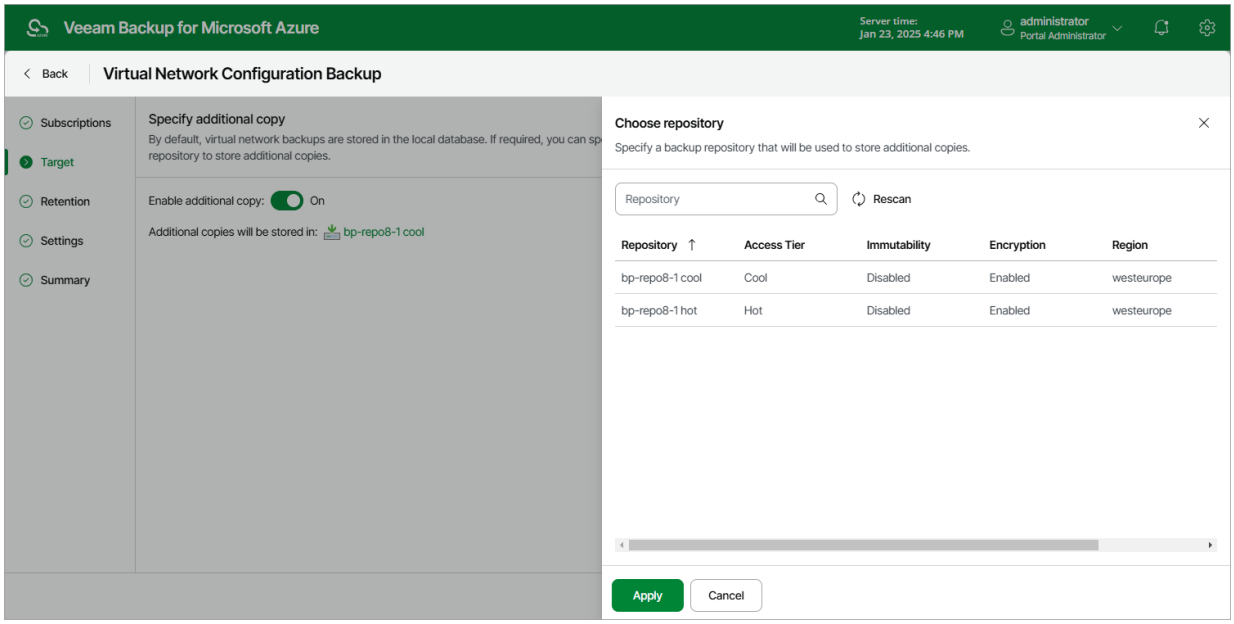
# Step 3. Enable Additional Backup Copy

By default, Veeam Backup for Microsoft Azure stores virtual network configuration backups in the local database. You can instruct Veeam Backup for Microsoft Azure to save additional backup copies to a backup repository. To do that:

1. At the **Target** step of the wizard, set the **Enable additional copy** toggle to *On*.
2. In the **Choose repository** window, select a backup repository that will be used to store the additional virtual network configuration backup copies.

   For a backup repository to be displayed in the list of available repositories, it must be added to Veeam Backup for Microsoft Azure as described in section Adding Backup Repositories. The list shows only backup repositories of the Hot and Cool access tiers.
3. To save changes made to the backup policy settings, click **Apply**.

> **NOTE**
>
> When choosing a backup repository, consider the following:
>
> - If you want to encrypt the backed-up virtual network configuration data, select a repository with encryption enabled.
> - If you want to make the backed-up virtual network configuration data immutable for the period specified in retention settings of the backup policy, select a repository with immutability enabled. Note that Veeam Backup for Microsoft Azure does not apply generations to virtual network configuration backups.
>
> For more information on encryption and immutability, see Adding Backup Repositories.

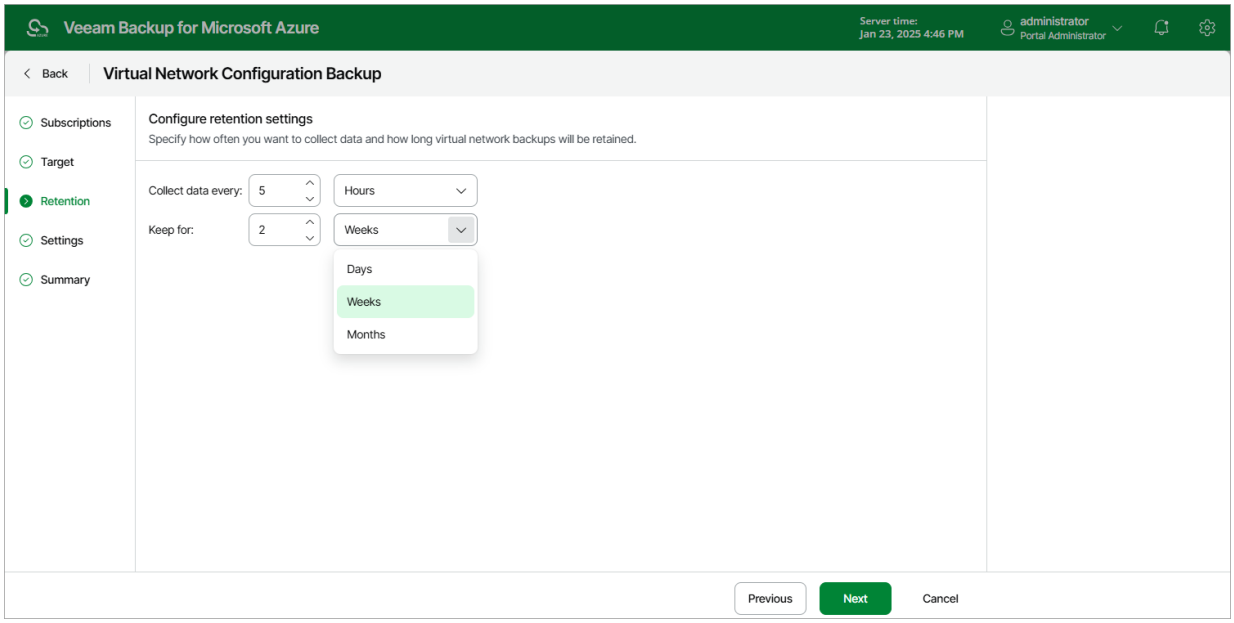


# Step 4. Configure Retention Settings

At the **Retention** step of the wizard, specify retention settings for virtual network configuration backups.

1. Click the **Collect data** link.
2. In the **Daily retention** window, specify how often the data will be backed up and for how long the backups will be stored in the Veeam Backup for Microsoft Azure configuration database.

   If a restore point is older than the specified time limit, Veeam Backup for Microsoft Azure removes the restore point from the backup chain. For more information, see Virtual Network Configuration Backup Retention.



# Step 5. Specify Email Notification Settings

At the **Settings** step of the wizard, you can specify email notification settings for the Virtual Network Configuration Backup policy.

> **NOTE**
>
> To be able to specify email notification settings for the Virtual Network Configuration Backup policy, you must configure global notification settings first. For more information, see Configuring Global Notification Settings.

To instruct Veeam Backup for Microsoft Azure to send email notifications for the backup policy, do the following:

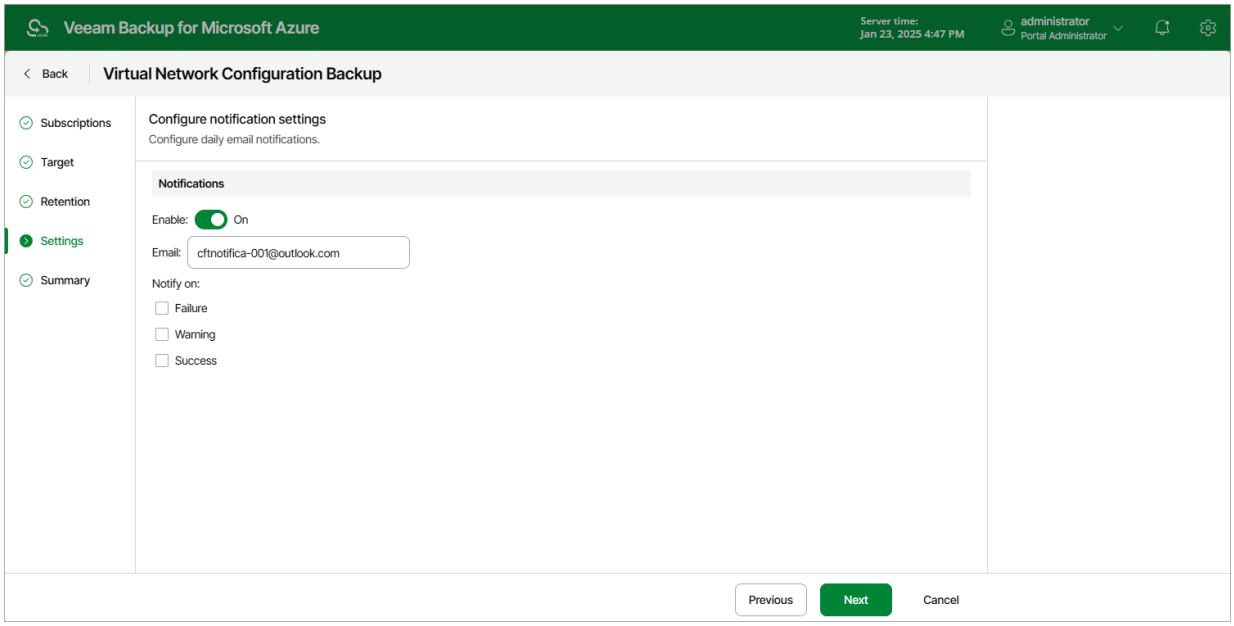
1. In the **Notifications** section, set the **Receive daily report** toggle to *On*.

   If you set the toggle to *Off*, Veeam Backup for Microsoft Azure will not send any notifications for this backup policy — regardless of the configured global notification settings.

2. In the **Email** field, specify an email address of a recipient. Use a semicolon to separate multiple recipient addresses.

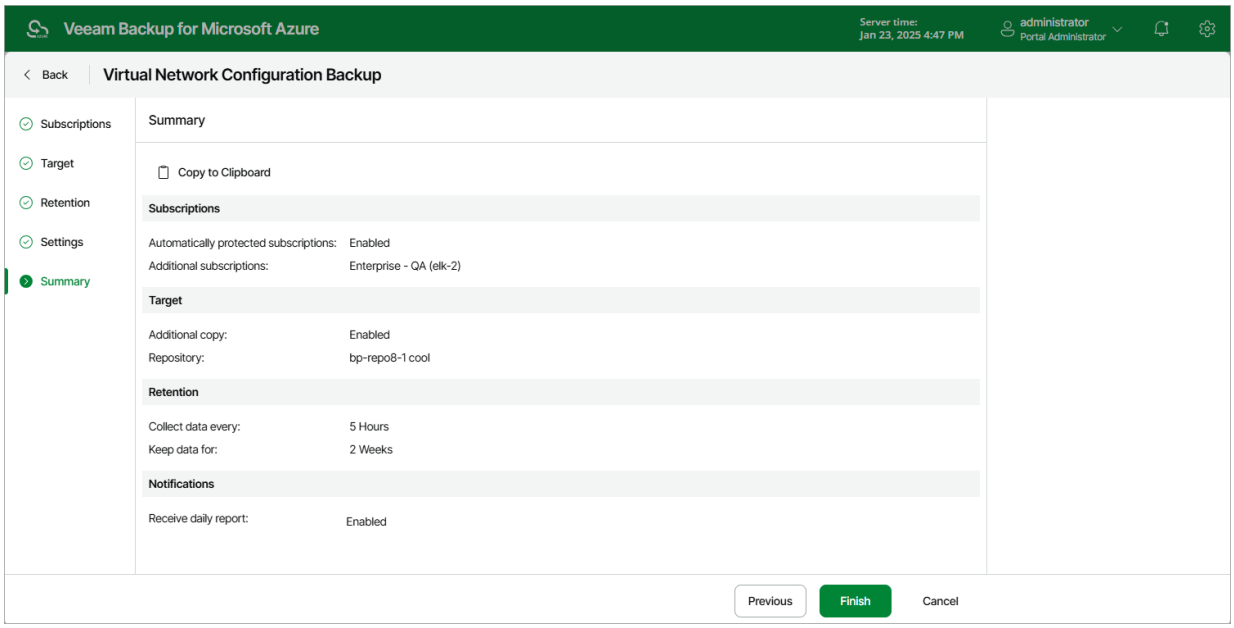
3. Use the **Notify on** list to choose whether you want Veeam Backup for Microsoft Azure to send email notifications in case the backup policy completes successfully, completes with warnings or completes with errors.

> **NOTE**
>
> If you specify the same email recipient in both backup policy notification and global notification settings, Veeam Backup for Microsoft Azure will override the configured global notification settings and will send each notification to this recipient only once to avoid notification duplicates.



## Step 6. Finish Working with Wizard

At the **Summary** step of the wizard, review configuration information and click **Finish**.

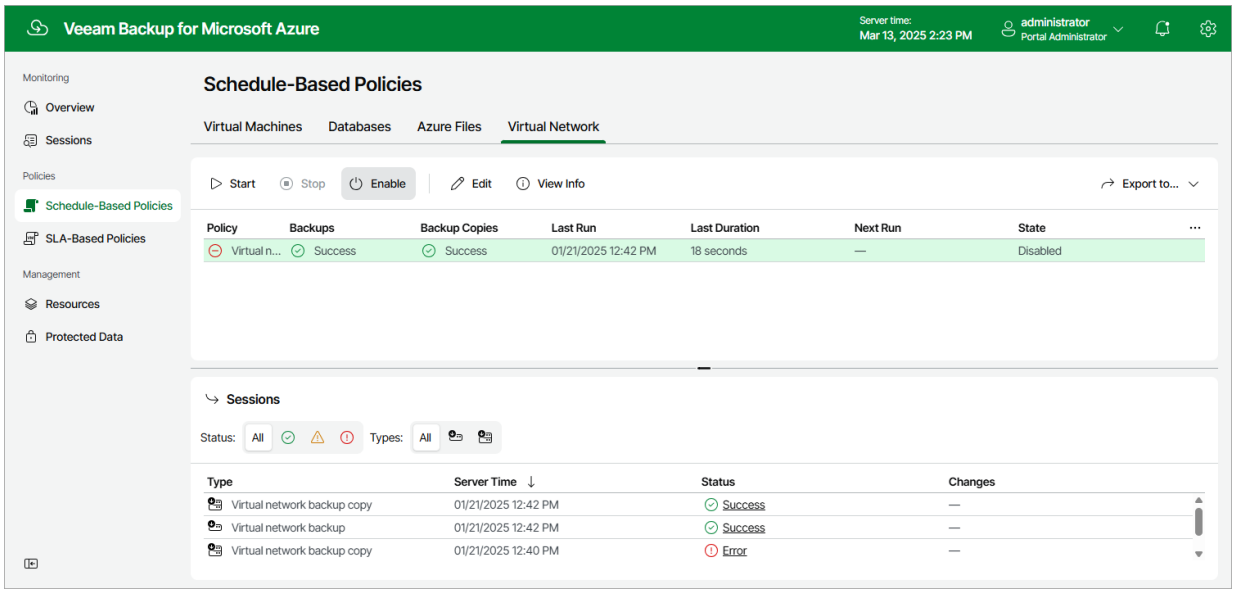



# Enabling and Disabling Virtual Network Configuration Backup Policy

By default, Veeam Backup for Microsoft Azure comes with the disabled Virtual Network Configuration Backup Policy. You can manually start or enable the disabled backup policy at any time you need.

To enable or disable the Virtual Network Configuration Backup policy, do the following:

1. Navigate to **Policies** > **Virtual Network**.
2. Click **Enable** or **Disable**.

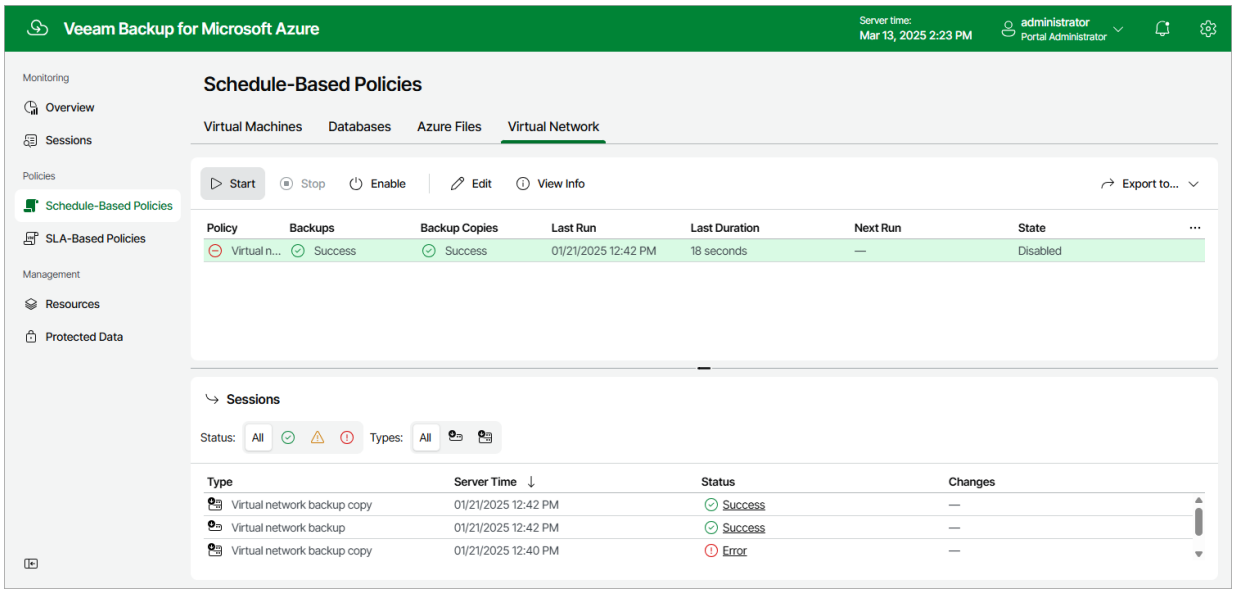


# Starting and Stopping Virtual Network Configuration Backup Policy

You can start the Virtual Network Configuration Backup policy manually, for example, if you want to create an additional restore point in the backup chain and do not want to modify the configured backup policy schedule. You can also stop a backup policy if the backup process is about to take long, and you do not want the policy to have an impact on the production environment during business hours.

To start or stop a backup policy, do the following:

1. Navigate to **Policies** > **Azure Virtual Network**.
2. Click **Start** or **Stop**.



# Managing Backup Policies

You can manage and edit created VM, SQL, Cosmos DB and Azure Files backup policies, and view the details of each backup policy in Veeam Backup for Microsoft Azure. You can also remove backup policies that you do not use anymore, as well as export existing and import new backup policies.

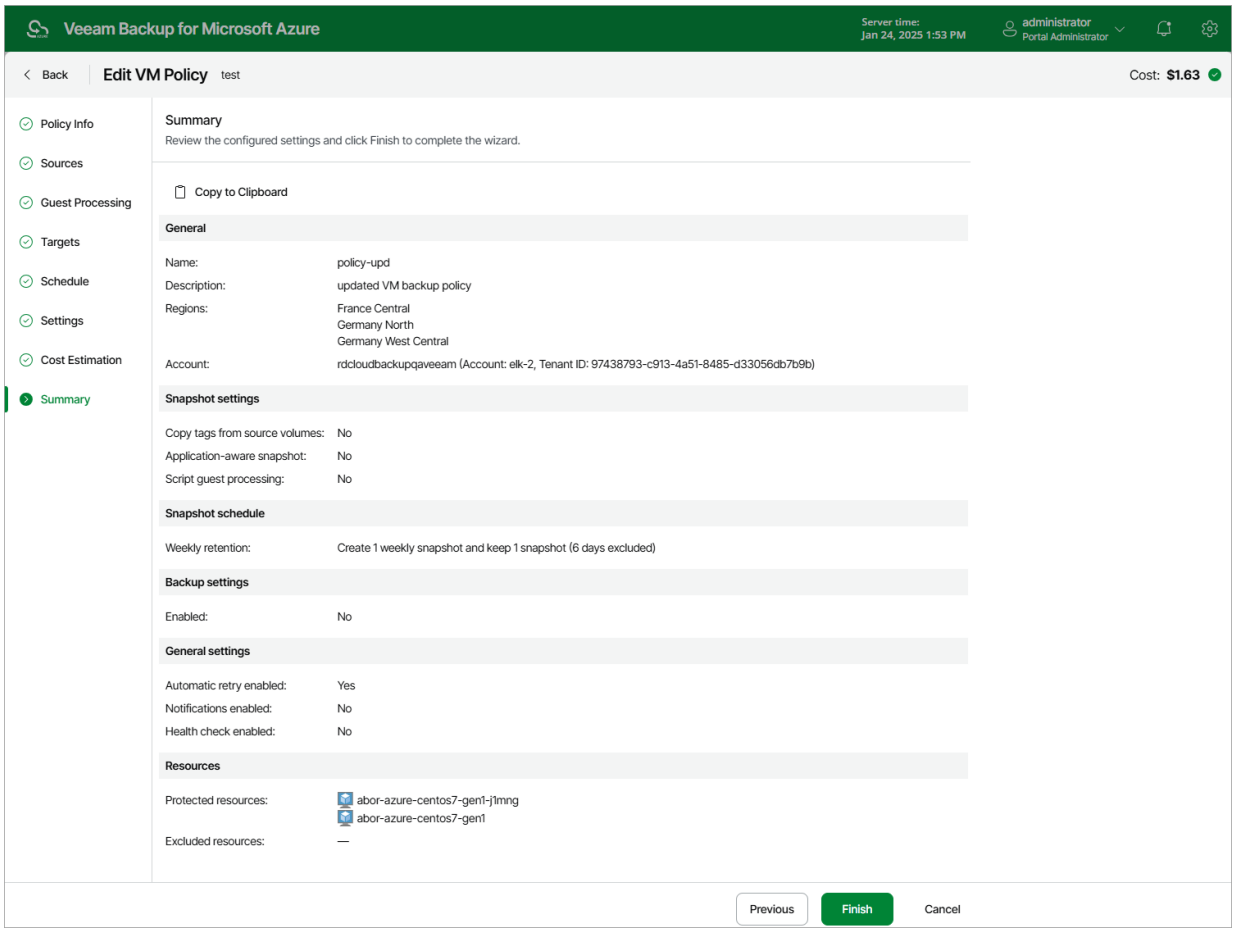
## Editing Backup Policy Settings

For each backup policy, you can modify settings configured while creating the policy:

1. Navigate to **Policies**.
2. Switch to the necessary tab and select the backup policy.
3. Click **Edit**.
4. Edit the backup policy settings as described in section Performing VM Backup, Performing SQL Backup, Performing Cosmos DB Backup, Performing Azure Files Backup or Performing Virtual Network Configuration Backup.

**IMPORTANT**

- Assigning another SLA template may cause Veeam Backup for Microsoft Azure to incorrectly calculate the SLA compliance ratio for the policy on the day when this modification is made. For more information on how Veeam Backup for Microsoft Azure estimates SLA compliance, see Viewing SLA-Based Backup Policy Details.
- Assigning another storage template will cause Veeam Backup for Microsoft Azure to start a new chain of restore points in the specified location. The old chain of restore points will be retained in the previous location until removed according to retention settings specified for the SLA template assigned to this SLA-based backup policy.



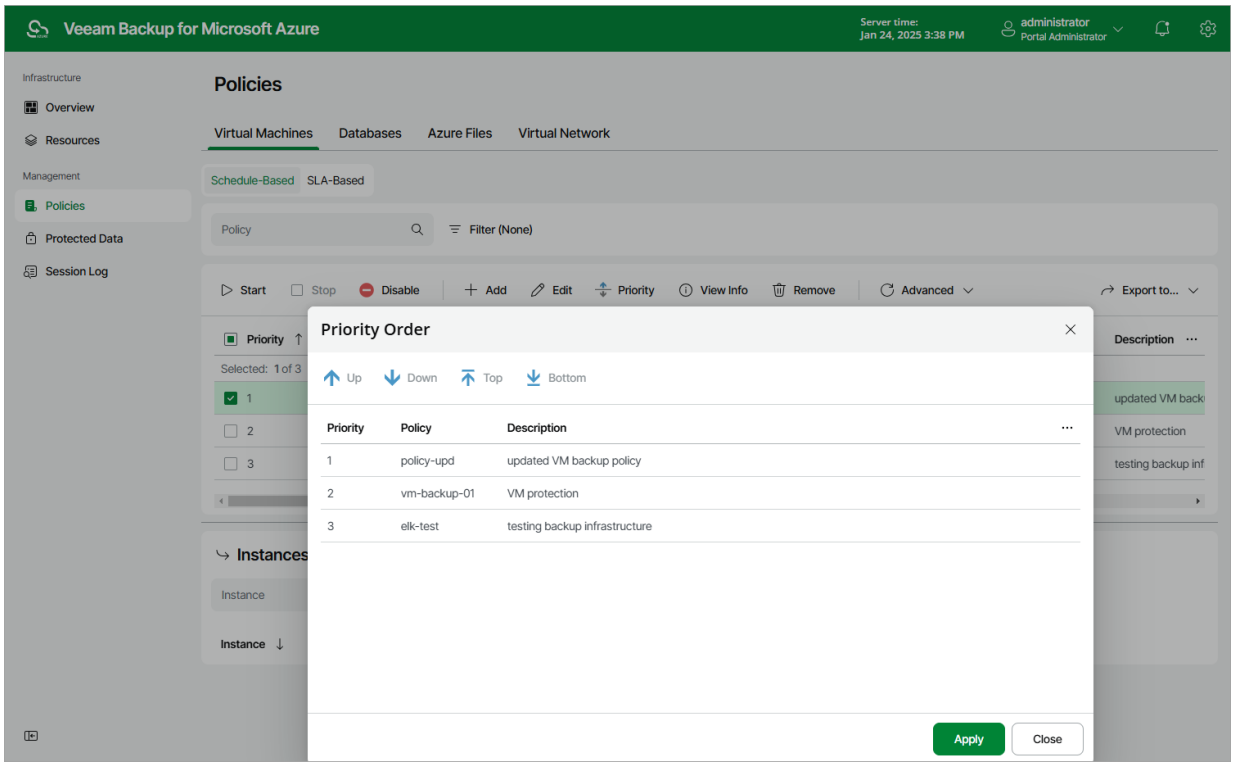

# Setting Backup Policy Priority

By default, Veeam Backup for Microsoft Azure runs backup policies in the order you create them. However, you can set the backup policy priority manually:

1. Navigate to **Policies**.
2. Switch to the necessary tab and click **Priority**.
3. In the **Priority Order** window, do the following:
   a. Select a backup policy in the list of existing policies.
   b. To move the policy up or down the list, use the **Up** and **Down** arrows.
   c. To save changes made to the priority order, click **Apply**.

NOTE

If an Azure resource is included into multiple backup policies, it will be processed only by the backup policy that has the highest priority.



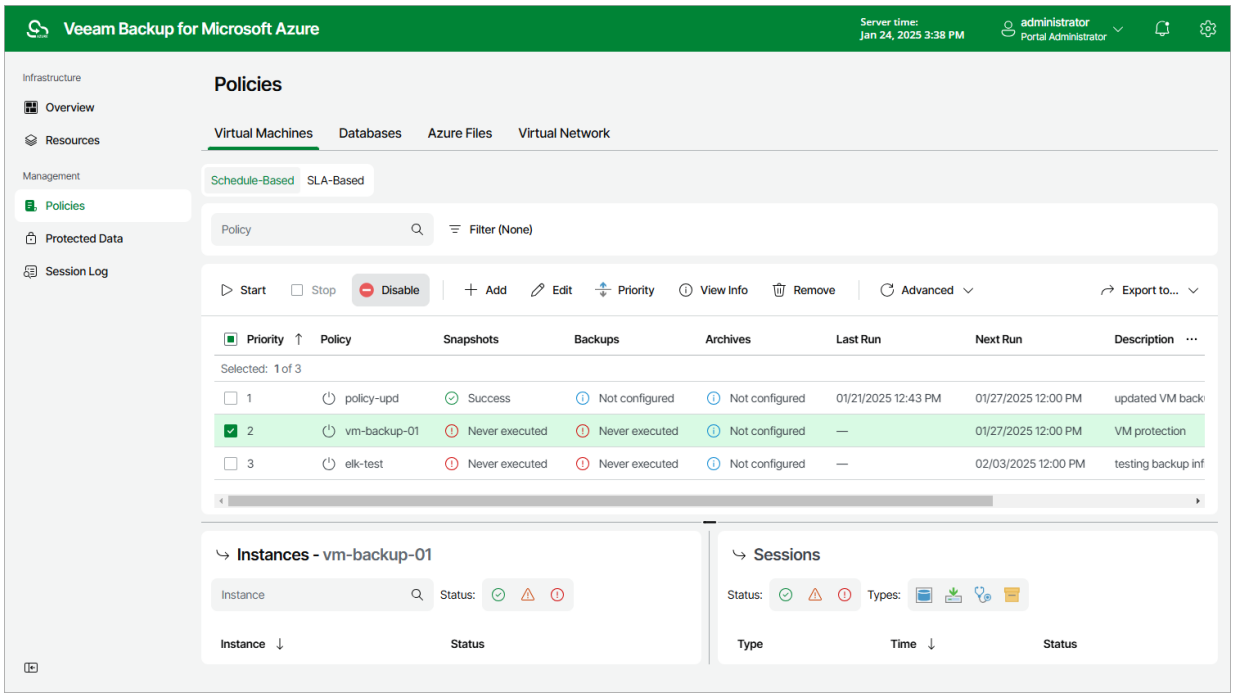

# Enabling and Disabling Backup Policies

By default, Veeam Backup for Microsoft Azure runs all created backup policies according to the specified schedules. However, you can temporarily disable a backup policy so that Veeam Backup for Microsoft Azure does not run the backup policy automatically. You will still be able to manually start or enable the disabled backup policy at any time you need.

To enable or disable a backup policy, do the following:

1. Navigate to **Policies**.
2. Switch to the necessary tab and select the backup policy.

3. Click **Enable** or **Disable**.




# Starting and Stopping Backup Policies

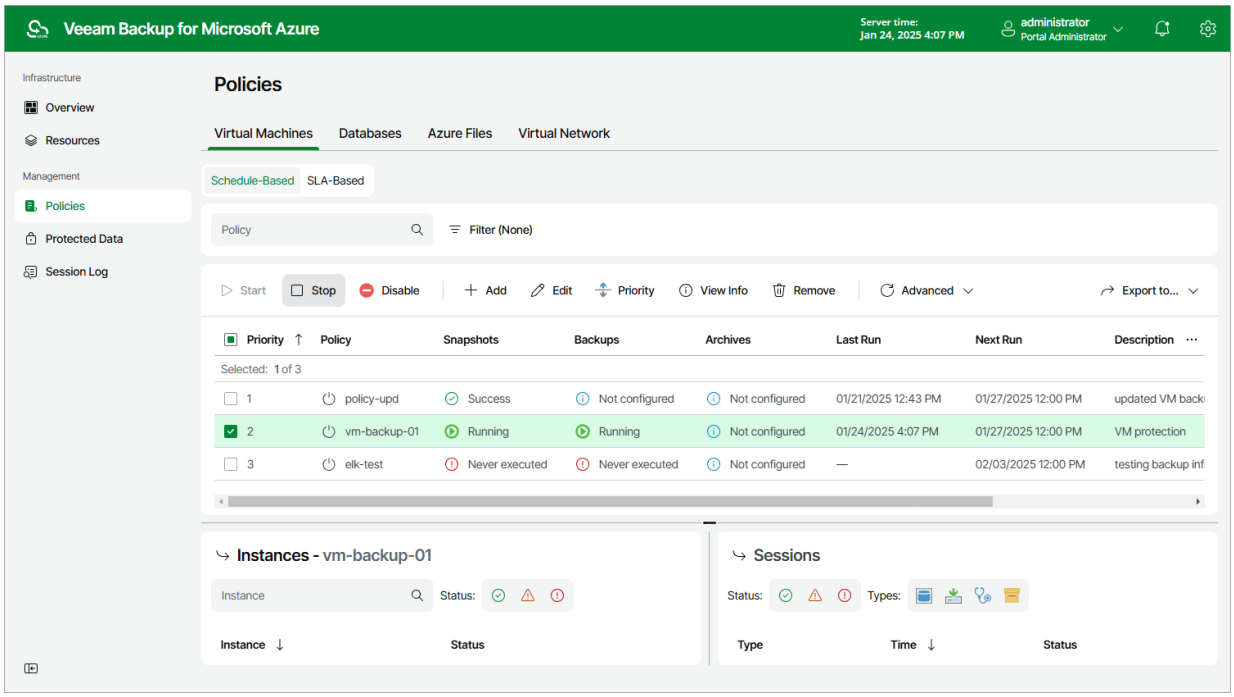
You can start a schedule-based backup policy manually, for example, if you want to create an additional restore point in the snapshot or backup chain and do not want to modify the configured policy schedule. You can also stop a schedule-based backup policy if processing of an Azure resource is about to take too long, and you do not want the policy to have an impact on the production environment during business hours.

> **IMPORTANT**
>
> In Veeam Backup for Microsoft Azure version 8, you cannot start or stop SLA-based backup policies manually — as a workaround, you can enable or disable the policy.

To start or stop a schedule-based backup policy, do the following:

1. Navigate to **Policies**.
2. Switch to the necessary tab and select the backup policy.

3. Click **Start** or **Stop**.




# Exporting and Importing Backup Policies

Veeam Backup for Microsoft Azure allows you to use settings of an existing schedule-based backup policy as a template for creating other policies. You can export a schedule-based backup policy to a .JSON file, modify the necessary settings in the file, and then import the policy to the same or a different backup appliance.

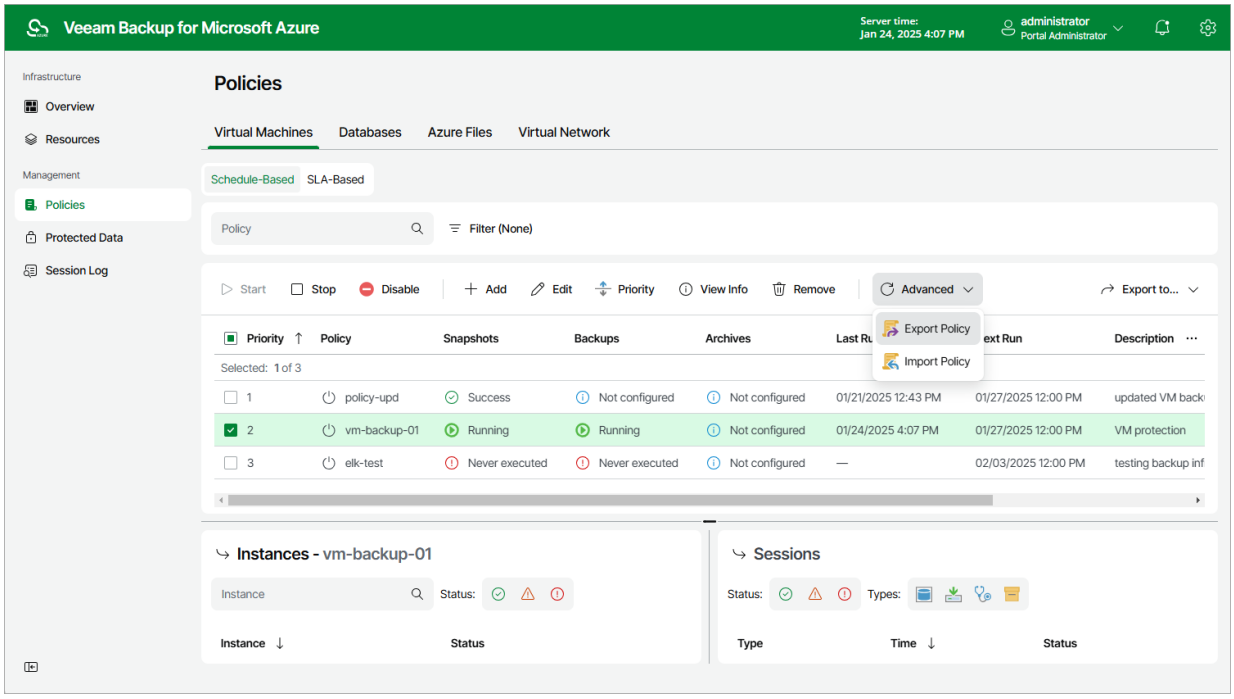
> **IMPORTANT**
>
> In Veeam Backup for Microsoft Azure version 8, you cannot export or import SLA-based backup policies.

# Exporting Backup Policies

To export a schedule-based backup policy to a .JSON file, do the following:

1. Navigate to **Policies**.
2. Switch to the necessary tab and select the backup policy.
3. Click **Advanced** > **Export Policy**.

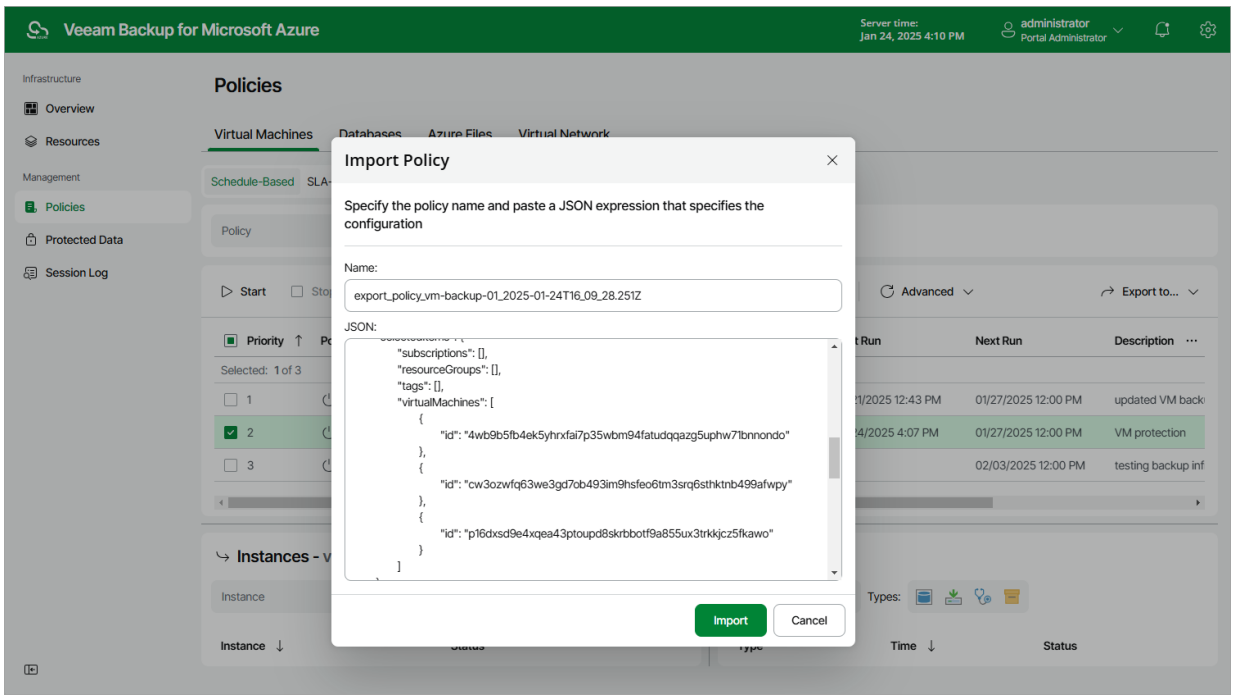
Veeam Backup for Microsoft Azure will save the schedule-based backup policy settings as a single .JSON file to the default download directory on the local machine.




# Importing Backup Policies

To import a backup policy from a .JSON file, do the following:

1. Click **Advanced** > **Import Policy**.
2. In the **Import Policy** window, specify a name for the imported backup policy, paste the content of the necessary .JSON file, and click **Import**.

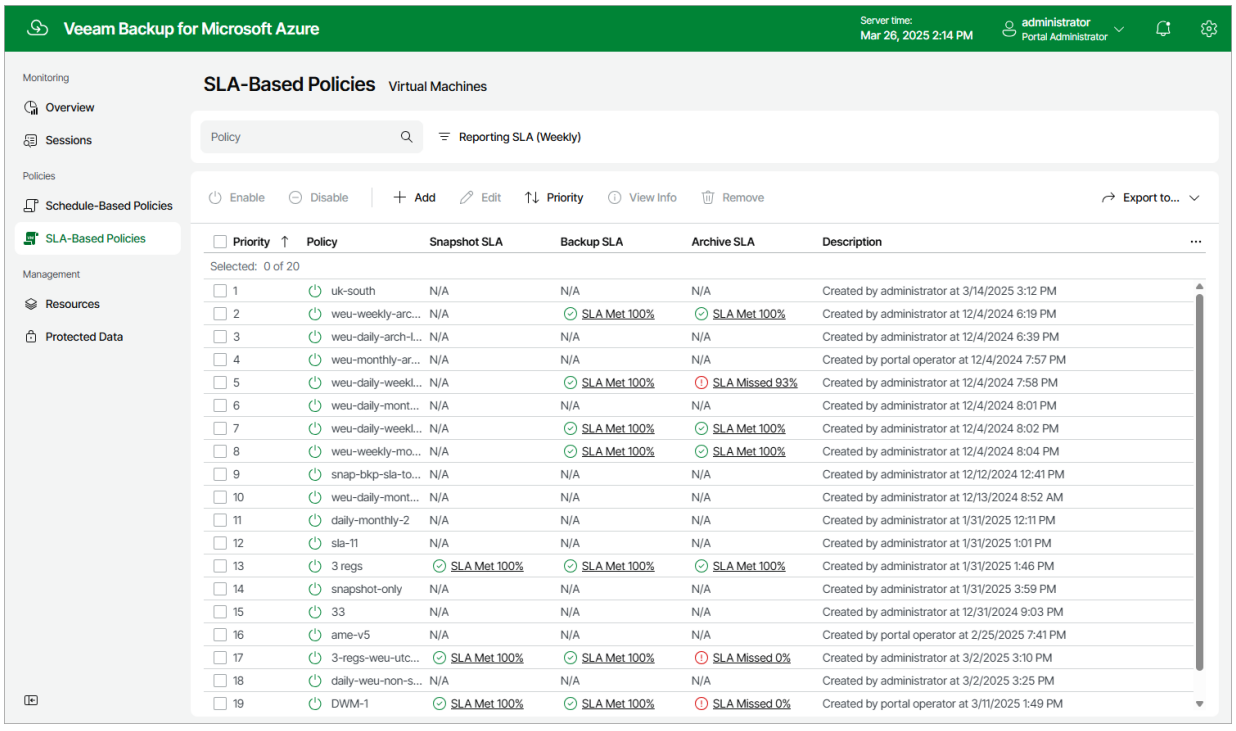


# Viewing SLA-Based Backup Policy Details

After you create an SLA-based backup policy, Veeam Backup for Microsoft Azure displays this policy on the **SLA-Based** tab of the **Policies** page. Each policy is described with the following set of properties:

- **Priority** – the priority of the policy.
- **Policy** – the name of the policy.
- **Description** – the reference information on the policy.
- **Snapshot SLA** – the most recent SLA compliance ratio calculated for all snapshots produced by the policy.
- **Backup SLA** – the most recent SLA compliance ratio calculated for all backups produced by the policy.
- **Archive SLA** – the most recent SLA compliance ratio calculated for all archived backups produced by the policy.

To see how the SLA compliance ratio has been changing over a specific period (daily, monthly or weekly) for each Azure VM protected by the policy, click the link in the **Snapshot SLA**, **Backup SLA** or **Archive SLA** column. For more information, see Monitoring SLA-Based Policy Performance.



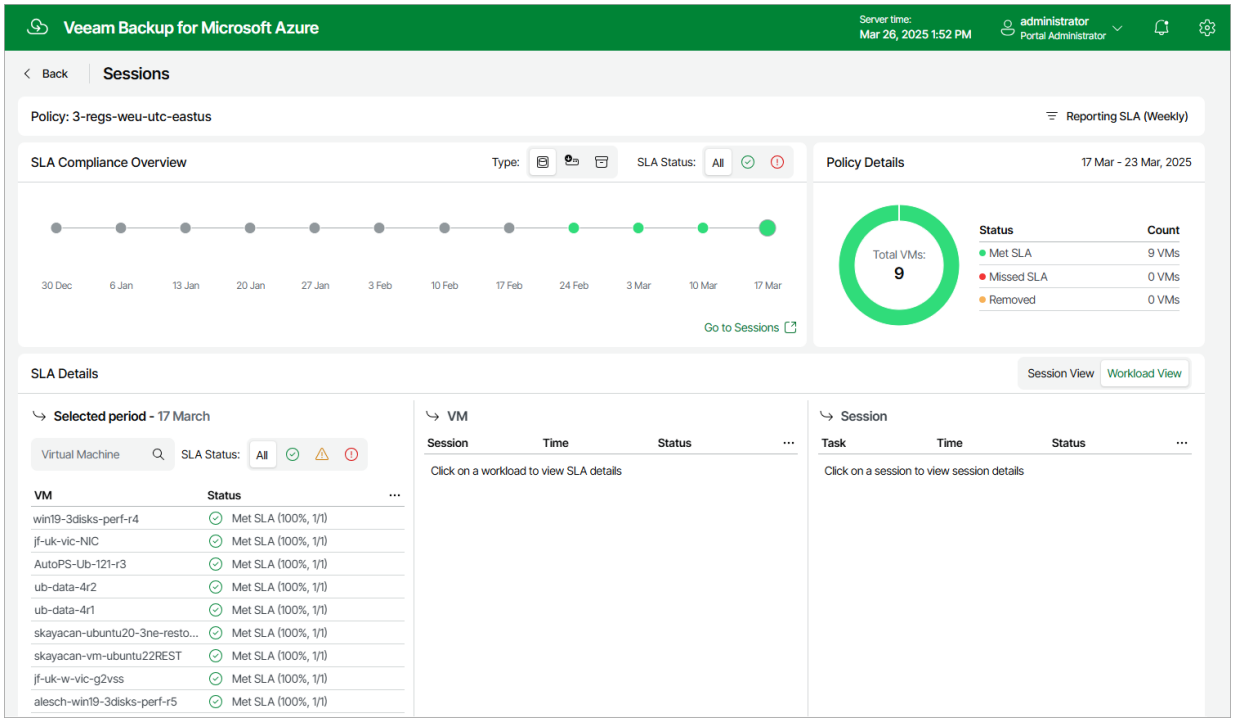

# Monitoring SLA-Based Policy Performance

Veeam Backup for Microsoft Azure allows you to monitor the protection status of all Azure VMs included into a specific SLA-based backup policy. As soon as Veeam Backup for Microsoft Azure finalizes the data protection window in all the protected regions, the SLA details for this window are automatically added to the SLA compliance overview on the **Sessions** page.

The number of entries on the **SLA Compliance Overview** chart depends on the filtering condition (daily, weekly or monthly) that you specify when proceeding to the **Sessions** page. That is, if you select the *Daily* condition, the chart will display 14 entries (the past 14 days); if you select the *Weekly* condition, the chart will display 12 entries (the past 12 weeks); if you select the *Monthly* condition, the chart will display 12 entries (the past 12 months). To switch between the filtering conditions, click **Reporting SLA**.

NOTES

- Since time zones of the protected regions may differ significantly, it may take Veeam Backup for Microsoft Azure up to 26 hours to add a new entry to the **SLA Compliance Overview** chart.
- By design, Veeam Backup for Microsoft Azure does not allow you to switch between filtering conditions for archived backups — it always displays SLA details for monthly archived backups only.




# How Veeam Backup for Microsoft Azure Estimates SLA Compliance

To estimate SLA compliance for an SLA-based backup policy, Veeam Backup for Microsoft Azure performs the following steps:

1. Calculates the SLA compliance ratio individually for each Azure VM added to the backup scope. The SLA compliance ratio equals a percentage of restore points successfully created for the VM out of the total number of restore points expected to be produced by the SLA-based backup policy for this VM.

   When calculating the SLA compliance ratio for daily, weekly and monthly restore points, Veeam Backup for Microsoft Azure takes into account snapshot and backup settings configured while creating the SLA template that is assigned to the SLA-based backup policy.

2. Uses the ratios calculated at step 1 to determine the average SLA compliance ratio for the policy.

3. Compares the target SLA value configured for the policy to the average SLA compliance ratio calculated at step 2. If the target SLA value equals or is less than the average SLA compliance ratio, Veeam Backup for Microsoft Azure marks this policy as meeting SLA standards.Impact of SLA Template Changes on SLA Compliance Estimation

Veeam Backup for Microsoft Azure estimates SLA compliance for each SLA-based backup policy based on the schedule settings configured for the SLA template that is assigned to this policy. When you modify snapshot or backup settings for an SLA template or assign another template to an SLA-based backup policy, this affects the SLA compliance ratio retrospectively — meaning that Veeam Backup for Microsoft Azure recalculates the SLA compliance ratio for all entries on the **SLA Compliance Overview** chart.

For example, if an SLA-based backup policy configured to produce daily snapshots every 2 hours between 10:00 AM and 2:00 PM successfully creates 2 snapshots on time, this means that the SLA compliance ratio will be 100%. If you reconfigure the policy to produce daily snapshots every 1 hour between 10:00 AM and 2:00 PM, and if the policy successfully creates 4 snapshots on time, this means that the SLA compliance ratio will change to 50% on the **SLA Compliance Overview** chart.

> **IMPORTANT**
>
> Modifying snapshot or backup settings for an SLA template or assigning another template to an SLA-based backup policy may cause Veeam Backup for Microsoft Azure to incorrectly calculate the SLA compliance ratio for the policy on the day when this modification is made. To learn how to edit SLA template settings, see Managing SLA Templates.

# Managing Backed-Up Data

The actions that you can perform with backed-up data depend on whether you access the data using the Veeam Backup & Replication console or the Veeam Backup for Microsoft Azure Web UI.

# Managing Backed-Up Data Using Console

To view and manage backed-up data, navigate to the **Backups** node of the **Home** view. The node displays information on all restore points created by backup appliances.

> **NOTE**
>
> You cannot remove created image-level backups and snapshots from the Veeam Backup & Replication console. To remove restore points of Azure VMs, Azure SQL databases, Cosmos DB accounts, Azure file shares and Azure virtual network configurations, open the backup appliance Web UI and follow the instructions provided in section Managing Backed-Up Data Using Web UI.

When you expand the **Backups** node in the working area, you can see the following icons:

| Icon | Protected Workload |
|---|---|
|  | Indicates that the protected workload is an Azure VM. |
|  | Indicates that the protected workload is an Azure SQL database. |
|  | Indicates that the protected workload is a Cosmos DB account. |
|  | Indicates that the protected workload is an Azure file share. |
|  | Indicates that the protected workload is a virtual network configuration. |

The **Backups** node contains 4 subnodes:

- The **Snapshots** subnode displays information on cloud-native snapshots of the protected Azure VMs, Azure file shares and Azure virtual network configurations and cloud-native backups of the protected Cosmos DB accounts:
  - *<appliance_name>* nodes show snapshots created manually on the backup appliance and snapshots imported to the appliance from Azure regions specified in the backup policy settings.
  - *<backup_policy_name>* nodes show snapshots and cloud-native backups created by the backup policy.

  To learn how Veeam Backup for Microsoft Azure creates cloud-native snapshots of Azure VMs, Azure file shares and Azure virtual network configurations, see sections Protecting Azure VMs, Protecting Azure Files and Protecting Virtual Network Configurations. To learn how Veeam Backup for Microsoft Azure creates cloud-native backups of Cosmos DB accounts, see section Protecting Cosmos DB Accounts.
- The **External Repository** subnode displays information on backups of the protected Azure VMs, Azure SQL databases and Cosmos DB accounts that are stored in standard repositories.

  To learn how Veeam Backup for Microsoft Azure creates image-level backups of the Azure VMs and backups of Azure SQL databases and Cosmos DB accounts, see sections Protecting Azure VMs, Protecting Azure SQL Databases and Protecting Cosmos DB Accounts.

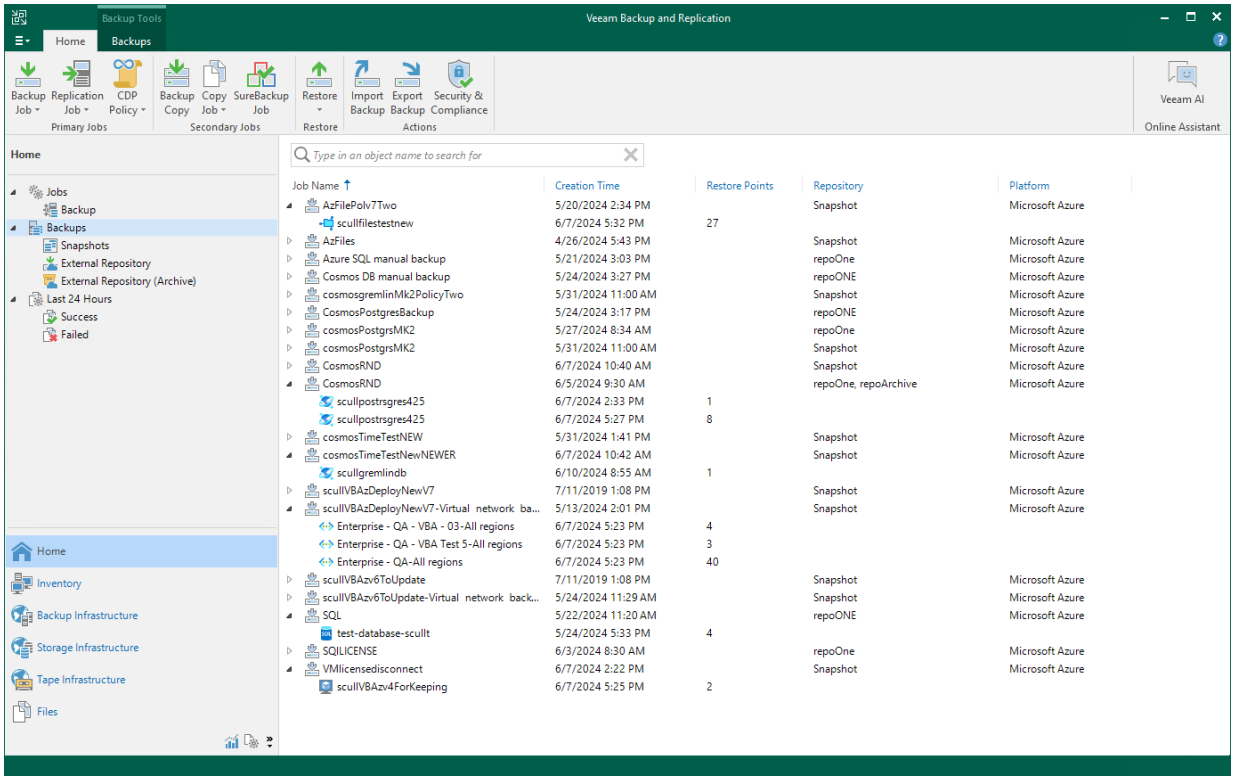
> **NOTE**
>
> If a backup chain was originally encrypted and then got decrypted by Veeam Backup & Replication, the backup chain will be marked with the **Key** icon.

- The **External Repository (Encrypted)** subnode displays information on encrypted image-level backups of Azure VMs that are stored in standard repositories and that have not been decrypted yet, which means either that you have not specified the decryption password or that the specified password is invalid.

  To learn how to decrypt backups, see Decrypting Backups.

- The **External Repository (Archive)** subnode displays information on backups of the protected Azure VMs and Azure SQL databases that are stored in archive repositories.

  To learn how Veeam Backup for Microsoft Azure creates archive backups, see section Archive Backup Chain.




# Decrypting Backups

Veeam Backup & Replication automatically decrypts backup files stored in repositories either using passwords that you specify when adding these repositories to the backup infrastructure or using Azure Key Vault cryptographic keys automatically detected by Veeam Backup & Replication. If you do not specify decryption passwords or Veeam Backup & Replication does not have permissions to access cryptographic keys, the backup files remain encrypted.

- To decrypt backup files encrypted using a cryptographic key, make sure that the service account specified when creating a new repository or adding an existing repository to the backup infrastructure is assigned permissions required to access Azure Key Vault cryptographic keys. For more information on the required permissions, see Plug-In Permissions.

- To decrypt backup files encrypted using a password, do the following:

  a. In the Veeam Backup & Replication console, open the **Home** view.

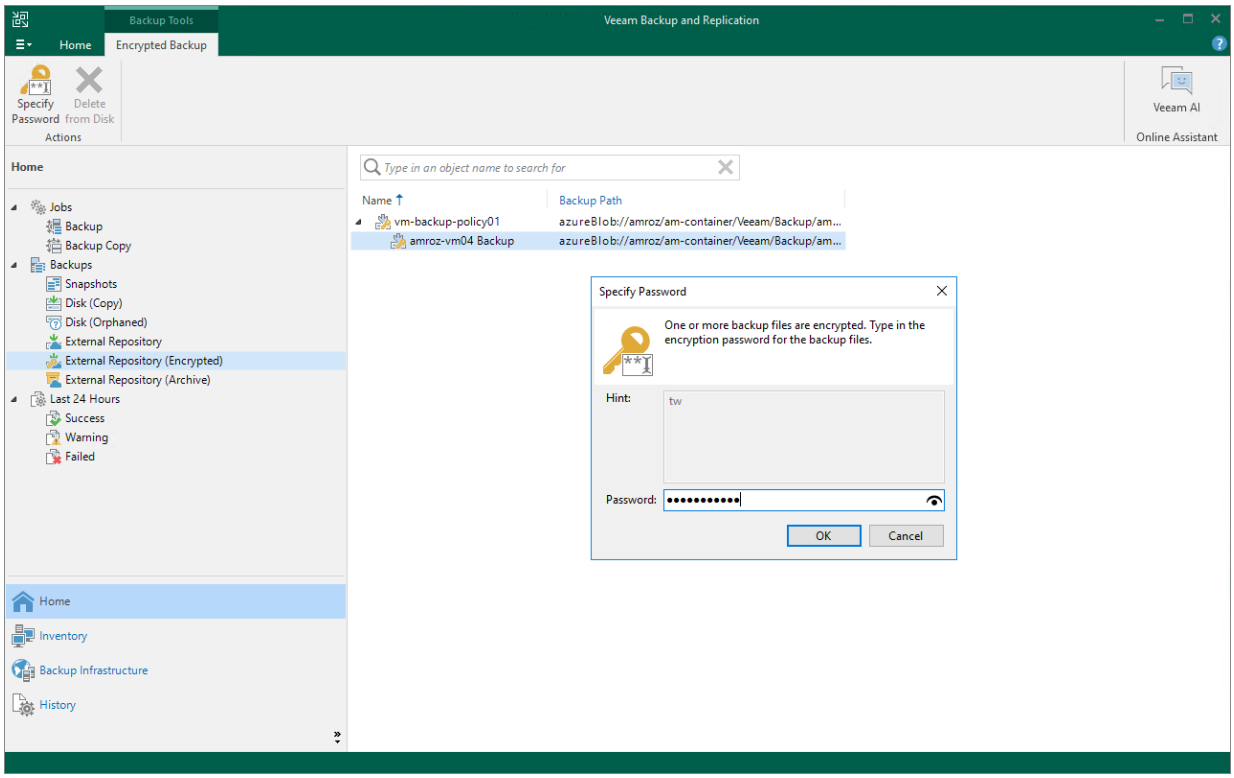
b. Navigate to **Backups** > **External Repository (Encrypted)**.

c. Expand the backup policy that protects an Azure VM whose image-level backups you want to decrypt, select the backup chain that belongs to the VM and click **Specify Password** on the ribbon.

   Alternatively, you can right-click the necessary backup chain and select **Specify password**.

> **TIP**
>
> To decrypt all backups created by a backup policy, right-click the policy and select **Specify Password**.

d. In the **Specify Password** window, enter a password that was used to encrypt the data stored in the target repository.



# Managing Backed-Up Data Using Web UI

Veeam Backup for Microsoft Azure stores information on all protected Azure resources in the configuration database. Even if a resource is no longer protected by any configured backup policy and even if the resource no longer exists in Microsoft Azure, information on the backed-up data will not be deleted from the database until Veeam Backup for Microsoft Azure automatically removes all restore points associated with this resource according to the retention settings saved in the backup metadata. You can also remove the restore points manually on the **Protected Data** page.

> **NOTE**
>
> Veeam Backup for Microsoft Azure does not include restore points created manually in backup and snapshot chains, and does not apply the configured retention policy settings to these restore points. This means that the restore points are kept in your Microsoft Azure environment unless you remove them manually, as described in sections Removing VM Backups and Snapshots, Removing SQL Backups, Removing Cosmos DB Backups, Removing File Share Snapshots and Removing Virtual Network Configuration Backups.

# Azure VM Data

After a backup policy successfully creates a restore point of an Azure VM according to the specified schedule, or after you create a snapshot of a VM manually, Veeam Backup for Microsoft Azure adds the VM to the resource list on the **Protected Data** page.

The **Protected Data** page displays Azure resources that are already protected by Veeam Backup for Microsoft Azure. Each resource is represented with a set of properties, such as:

- **Virtual Machine** — the name of the Azure VM.
- **Policy** — the name of the backup policy that protects the Azure VM.
- **Restore Points** — the number of restore points created for the Azure VM.

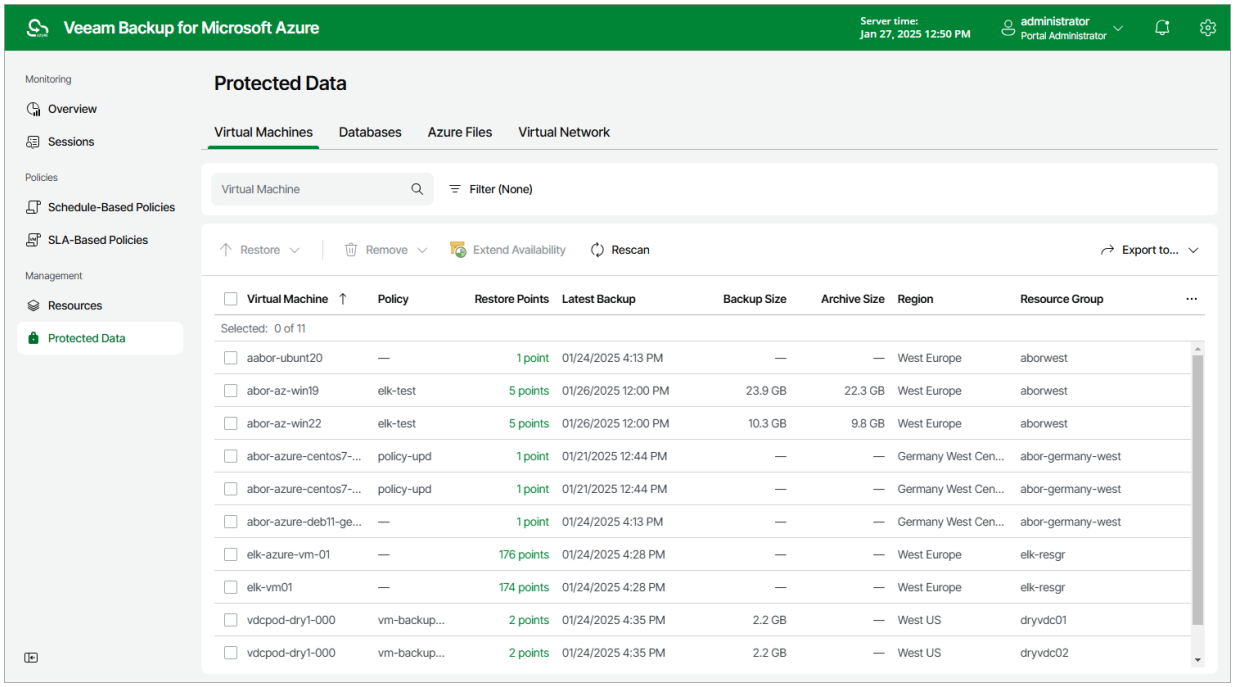
  To view the list of restore points, click the link in the **Restore Points** column. The **Available Restore Points** window will display information on each restore point, including the following: the date when the restore point was created, the access tier of the backup repository where the restore point is stored, and the configured retention policy settings (*D* — daily, *W* — weekly, *M* — monthly or *Y* — yearly).
- **Latest Backup** — the date and time of the most recent restore point created for the Azure VM.
- **Backup Size** — the total size of the standard VM backups.
- **Archive Size** — the total size of the Azure VM backups stored in archive repositories.
- **Region** — an Azure region in which the Azure VM resides.
- **Resource Group** — the resource group to which the Azure VM belongs.
- **VM Size** — the VM size of the Azure VM.
- **Operating System** — the operating system running on the Azure VM.
- **Data Retrieval** — the status of the backups retrieval from the archive repository.
- **File-level Recovery URL** — a link to the file-level recovery browser.

  The link appears when Veeam Backup for Microsoft Azure starts a restore session to perform file-level recovery. The link contains a public DNS name of the worker instance hosting the file-level recovery browser and authentication information used to access this worker instance.
- **Tenant ID** — the unique identification number of the Microsoft Entra tenant that contains the Azure VM.
- **Subscription ID** — the unique identification number of the Azure subscription that manages the Azure VM.

On the **Protected Data** page, you can also perform the following actions:

- Remove restore points if you no longer need them. For more information, see Removing Backups and Snapshots.

- Restore data of backed-up Azure VMs. For more information, see VM Restore.




# Removing VM Backups and Snapshots

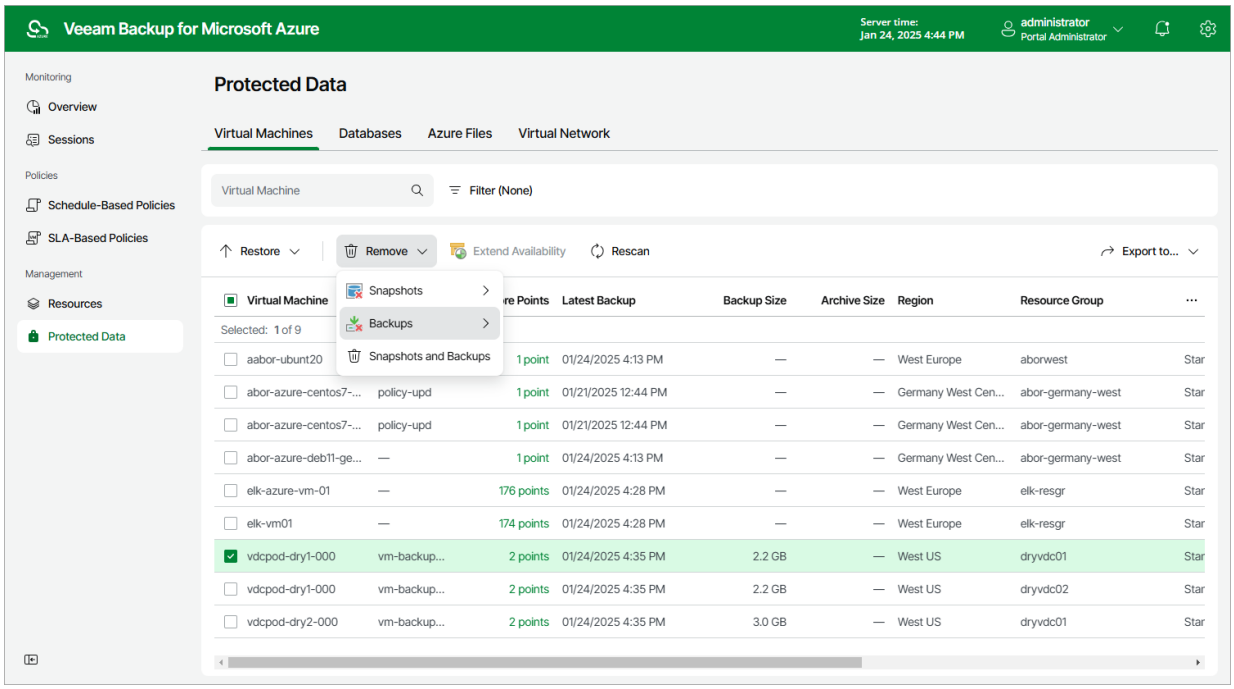
Veeam Backup for Microsoft Azure applies the configured retention policy settings to automatically remove cloud-native snapshots and image-level backups created for Azure VMs by backup policies. If necessary, you can also remove the backed-up data manually.

> **IMPORTANT**
>
> Do not delete backups from Microsoft Azure storage accounts in the Microsoft Azure portal. If some backup in a backup chain is missing, you will not be able to roll back Azure VM data to the necessary state.

To remove backed-up data manually, do the following:

1. Navigate to **Protected Data** > **Virtual Machines**.
2. Select Azure VMs whose data you want to remove.
3. Click **Remove** and select either of the following options:
   - **Snapshots** > **All** — to remove all cloud-native snapshots created for the selected Azure VMs both by backup policies and manually.
   - **Snapshots** > **Local** — to remove all cloud-native snapshots created for the selected Azure VMs by backup policies.
   - **Snapshots** > **Manual** — to remove all cloud-native snapshots created for the selected Azure VMs manually.
   - **Backups** > **All** — to remove all image-level backups created for the selected Azure VMs.
   - **Backups** > **Backup** — to remove all image-level backups created in backup repositories for the selected Azure VMs.
   - **Backups** > **Archive** — to remove all image-level backups created in archive repositories for the selected Azure VMs.

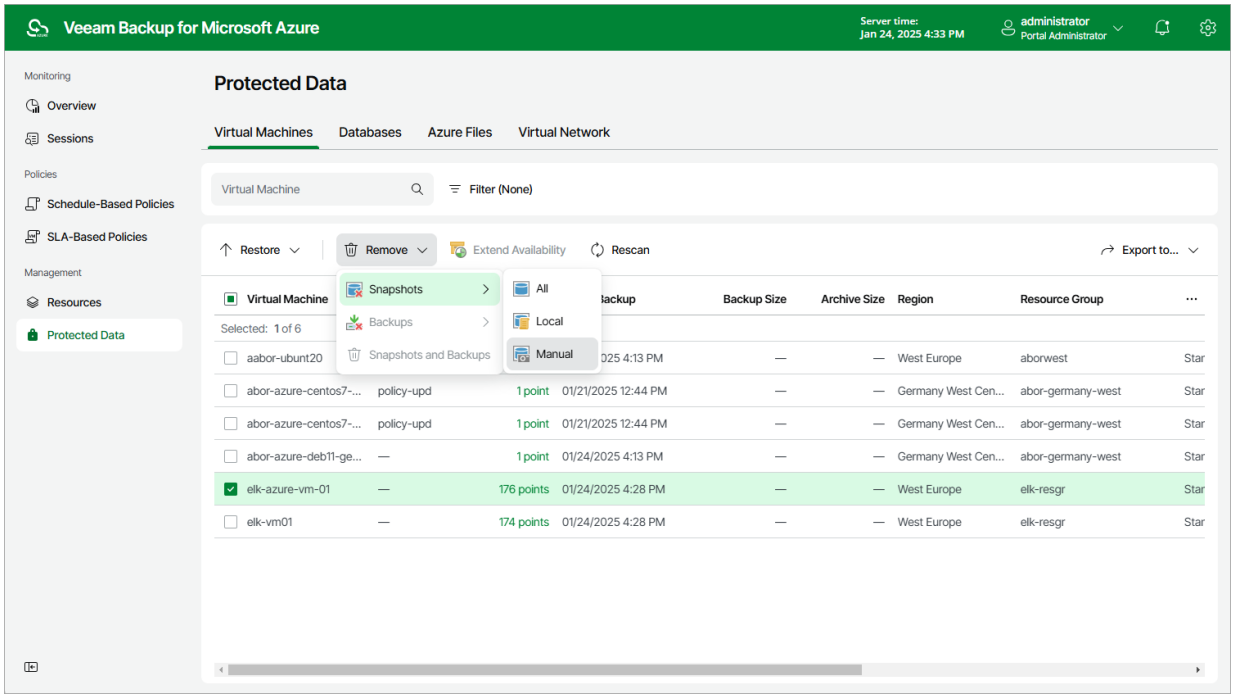
- **Snapshots and Backups** — to remove both cloud-native snapshots and image-level backups created for the selected Azure VMs.




# Removing VM Snapshots Created Manually

To remove all cloud-native snapshots created for an Azure VM manually, follow the instructions provided in Removing VM Backups and Snapshots. If you want to remove a specific cloud-native snapshot created manually, do the following:

1. Navigate to **Protected Data**.
2. Select the check box next to the necessary Azure VM, and click the link in the **Restore Points** column.
3. In the **Available Restore Points** window, select the necessary snapshot and click **Remove Manual Snapshot**.



# Retrieving Data from Archive

Backups stored in archive repositories are not immediately accessible. If you want to restore an Azure VM from a backup that is stored in a repository of the Archive access tier, you must first retrieve the archived data. During the data retrieval process, a temporary copy of the archived data is created in an Azure blob container where the repository is located. This copy is stored in the Hot access tier for a period of time that you specify when launching the data retrieval process. If the time period expires while a restore operation is still running, Veeam Backup for Microsoft Azure automatically extends the period to keep the retrieved data available for one more hour. You can also extend the availability period manually.

To retrieve archived data, you can launch the data retrieval process either from the Data Retrieval wizard before you begin a restore operation, or directly from the Restore Virtual Machines and Restore Disks wizards. When you retrieve archived data, you can choose one of the following priority options:

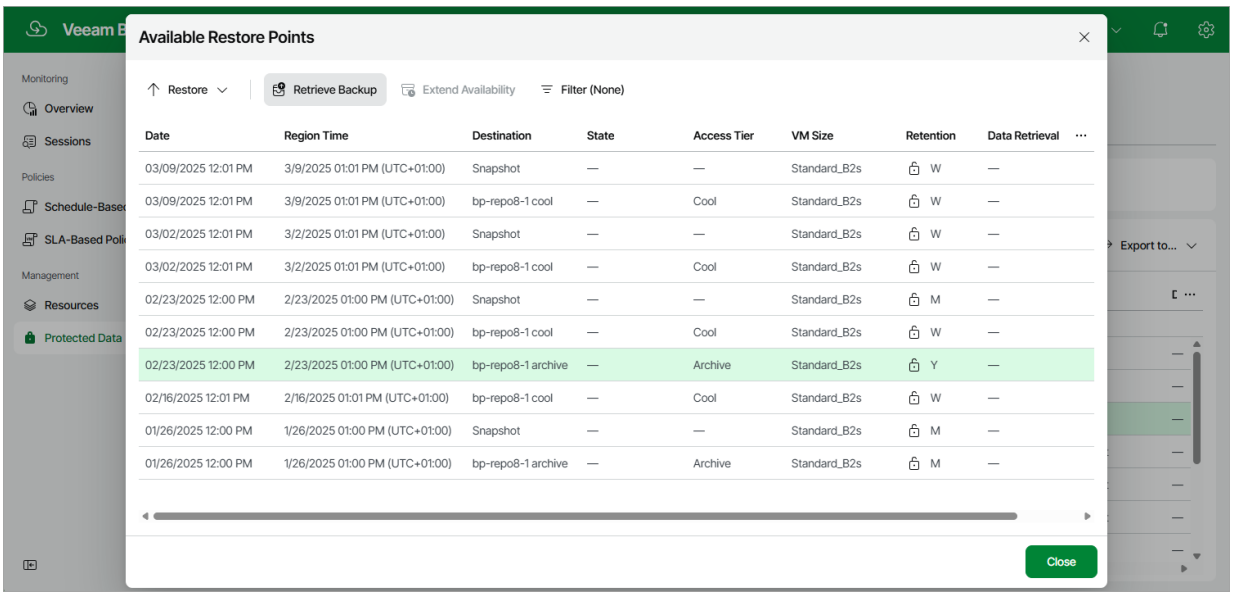
- **Standard Priority** — the default priority option. The retrieved data will be available within 15 hours.
- **High Priority** — the fastest but more expensive priority option. The retrieved data will be available within one hour if the size of the backup is less than 10 GB.

For more information on priority options, see Microsoft Docs

# Retrieving Data Manually

To retrieve archived data of an Azure VM, do the following:

1. Navigate to **Protected Data** > **Virtual Machines**.
2. Select the necessary Azure VM.
3. Click the link in the **Restore Points** column.
4. In the **Available Restore Points** window, select a restore point that contains archived data you want to retrieve, and click **Retrieve Backup**. The **Data Retrieval** wizard will open.

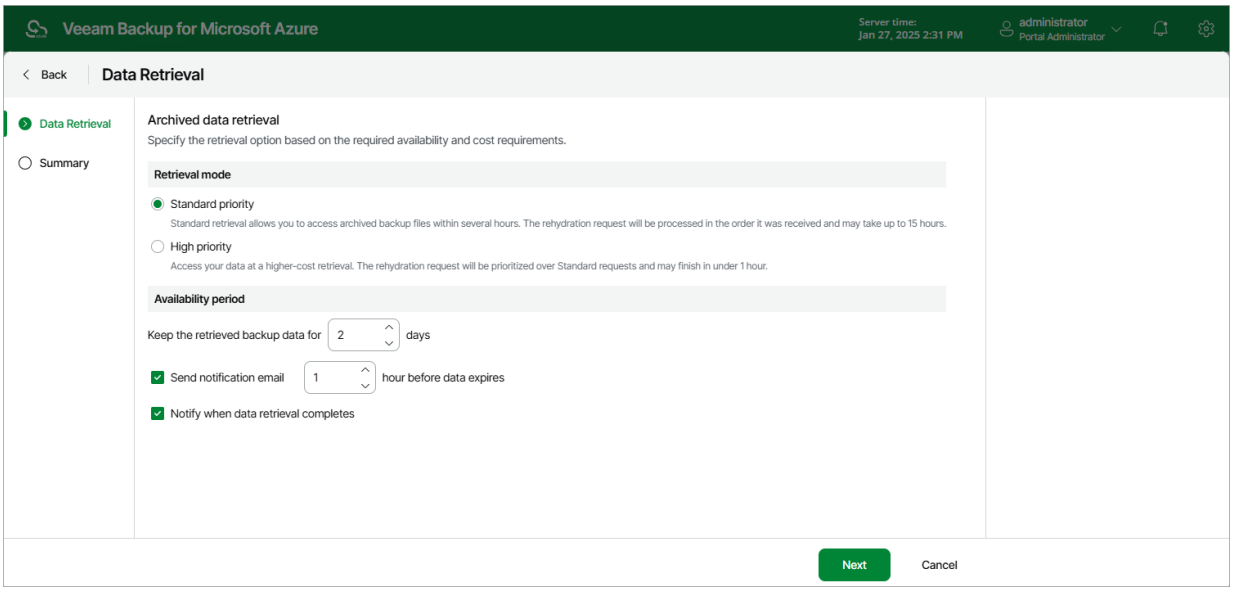



5. At the **Data Retrieval** step of the wizard, specify the following settings:
   a. In the **Retrieval mode** section, select the retrieval option that Veeam Backup for Microsoft Azure will use to retrieve the data.

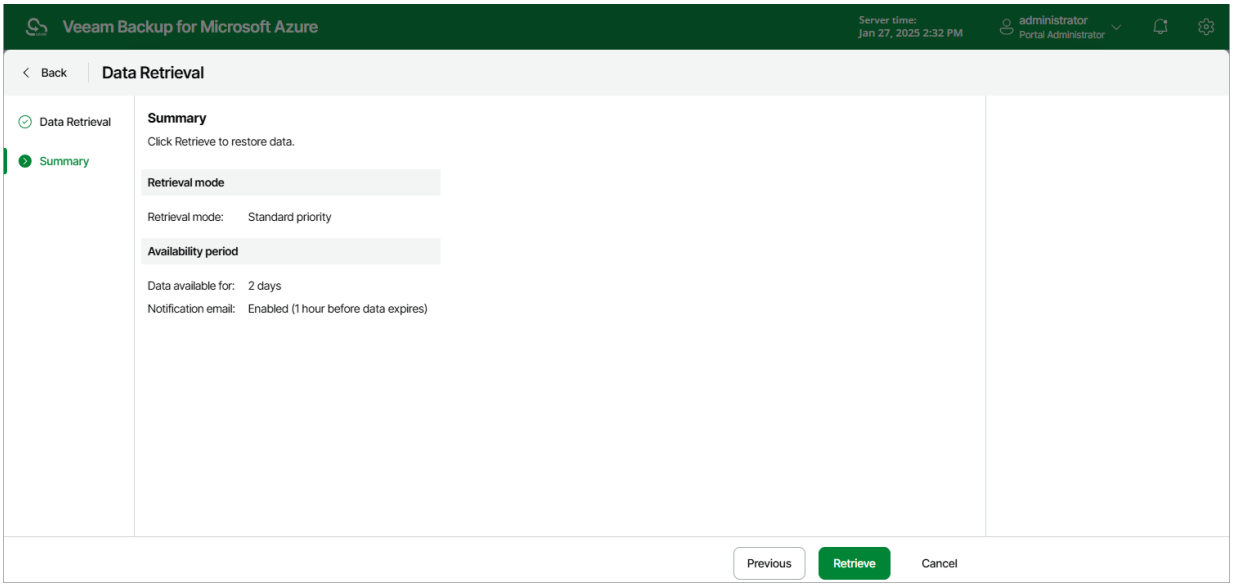
b. In the **Availability period** section, specify the number of days for which you want to keep the data available for restore operations.

You will be able to manually extend data availability later if required.

> **TIP**
>
> If you want to receive an email notification when the data availability period is about to expire, select the **Send notification email** check box, and specify the number of hours before the expiration time when the notification will be sent.




6. At the **Summary** step of the **Data Retrieval** wizard, review configuration information and click **Retrieve**.




# Extending Data Availability

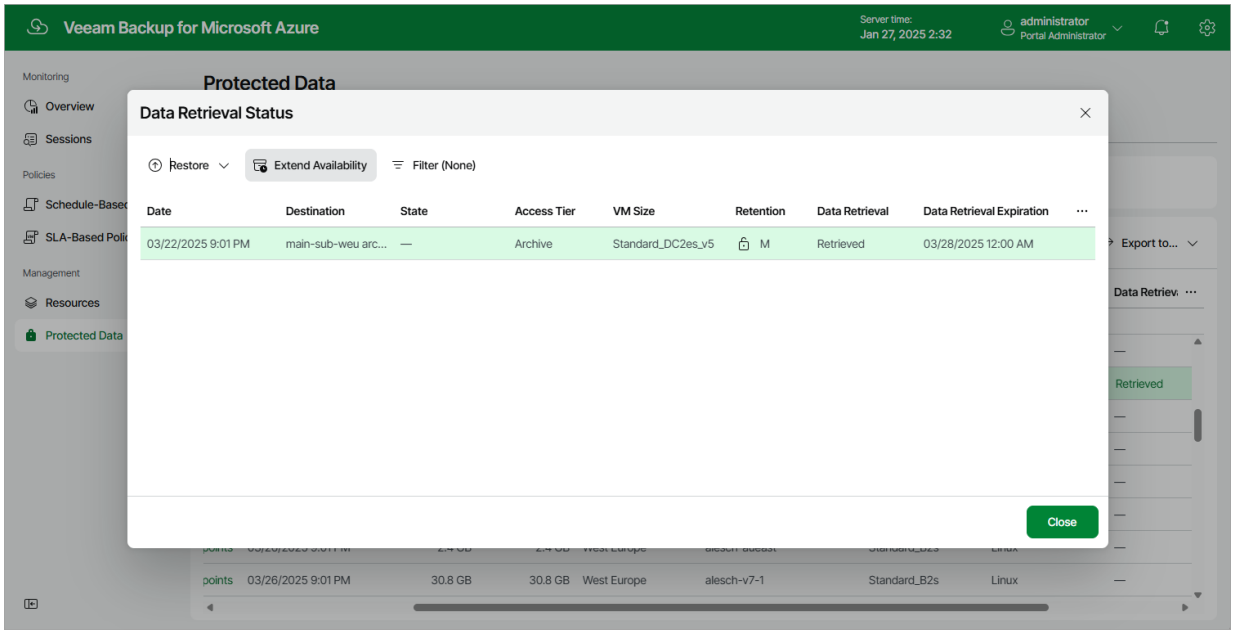
To extend time for which you want to keep retrieved data available for restore operations:

1. Select the Azure VM for which you want to extend availability of the retrieved data.

2. Click **Extend Availability**.

   Alternatively, click the link in the **Restore Points** column. In the **Data Retrieval** window, select the restore point that contains the retrieved data, and click **Extend Availability**.

3. In the **Extend Data Availability Period** window, specify the number of days for which you want to keep the data available for restore operations, and click **Extend**.



# Azure SQL Data

After a backup policy successfully creates a restore point of an Azure SQL database according to the specified schedule, or after you create a backup of a database manually, Veeam Backup for Microsoft Azure adds the database to the resource list on the **Protected Data** page.

The **Protected Data** page displays Azure resources that are already protected by Veeam Backup for Microsoft Azure. Each resource is represented with a set of properties, such as:

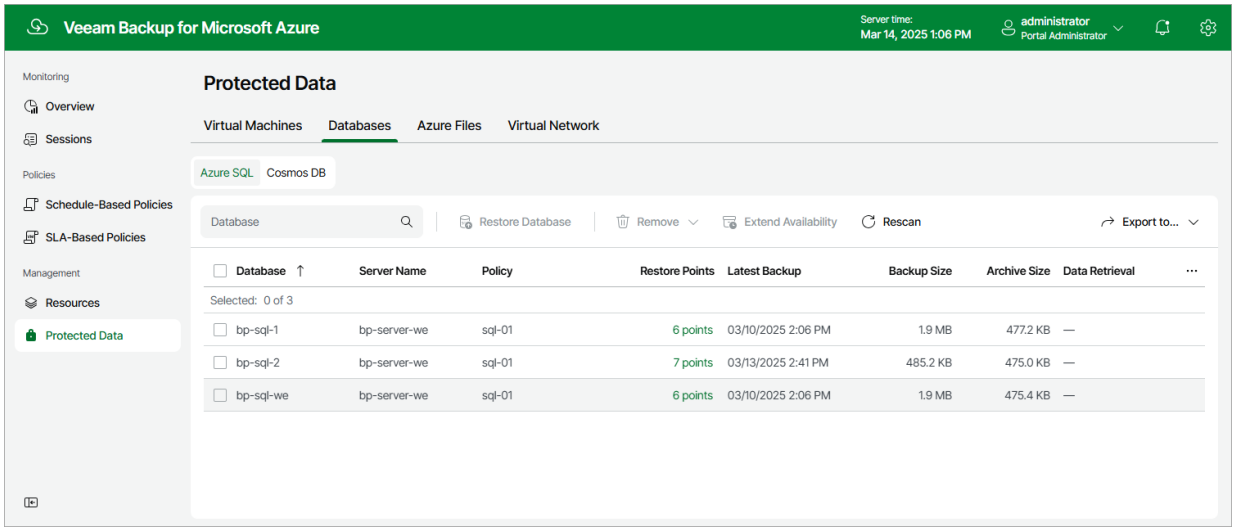
- **Database** — the name of the Azure SQL database.
- **Server Name** — the name of the SQL Server where the protected Azure SQL database is located.
- **Policy** — the name of the backup policy that protects the Azure SQL database.
- **Restore Points** — the number of restore points created for the Azure SQL database.

  To view the list of restore points, click the link in the **Restore Points** column. The **Available Restore Points** window will display information on each restore point, including the following: the date when the restore point was created, the access tier of the backup repository where the restore point is stored, and the configured retention policy settings (*D* — daily, *W* — weekly, *M* — monthly or *Y* — yearly).
- **Latest Backup** — the date and time of the most recent restore point created for the Azure SQL database.
- **Backup Size** — the total size of the standard Azure SQL database backups.
- **Archive Size** — the total size of the Azure SQL database backups stored in archive repositories.
- **Region** — an Azure region in which the Azure SQL database resides.
- **Resource Group** — the resource group to which the Azure SQL database belongs.
- **SQL Elastic Pool** — the name of the elastic pool to which the Azure SQL database is added.
- **Data Retrieval** — the status of the backups retrieval from the archive repository.
- **Tenant ID** — the unique identification number of the Microsoft Entra tenant that contains the Azure SQL database.
- **Subscription ID** — the unique identification number of the Azure subscription that manages the Azure SQL database.

On the **Protected Data** page, you can also perform the following actions:

- Remove restore points if you no longer need them. For more information, see Removing SQL Backups.

- Restore data of backed-up Azure SQL databases. For more information, see SQL Restore.




# Removing SQL Backups

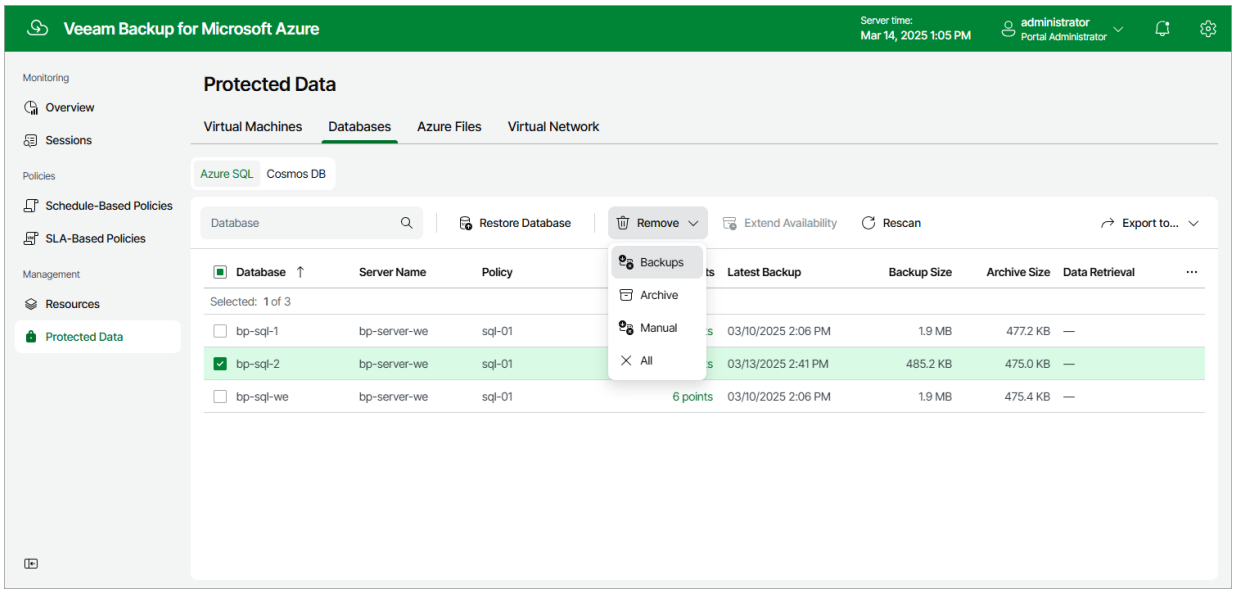
Veeam Backup for Microsoft Azure applies the configured retention policy settings to automatically remove backups created for SQL databases by backup policies. If necessary, you can also remove the backed-up data manually.

> **IMPORTANT**
>
> Do not delete backups from Microsoft Azure storage accounts in the Microsoft Azure portal. If some backup in a backup chain is missing, you will not be able to roll back Azure SQL database data to the necessary state.

To remove backed-up data manually, do the following:

1. Navigate to **Protected Data** > **Databases** > **Azure SQL**.
1. Select Azure SQL databases whose data you want to remove.
3. Click **Remove** and select either of the following options:
   - **All** — to remove all backups created for the selected Azure SQL databases both by backup policies and manually.
   - **Backups** — to remove all backups created in backup repositories for the selected Azure SQL databases.
   - **Archive** — to remove all backups created in archive repositories for the selected Azure SQL databases.

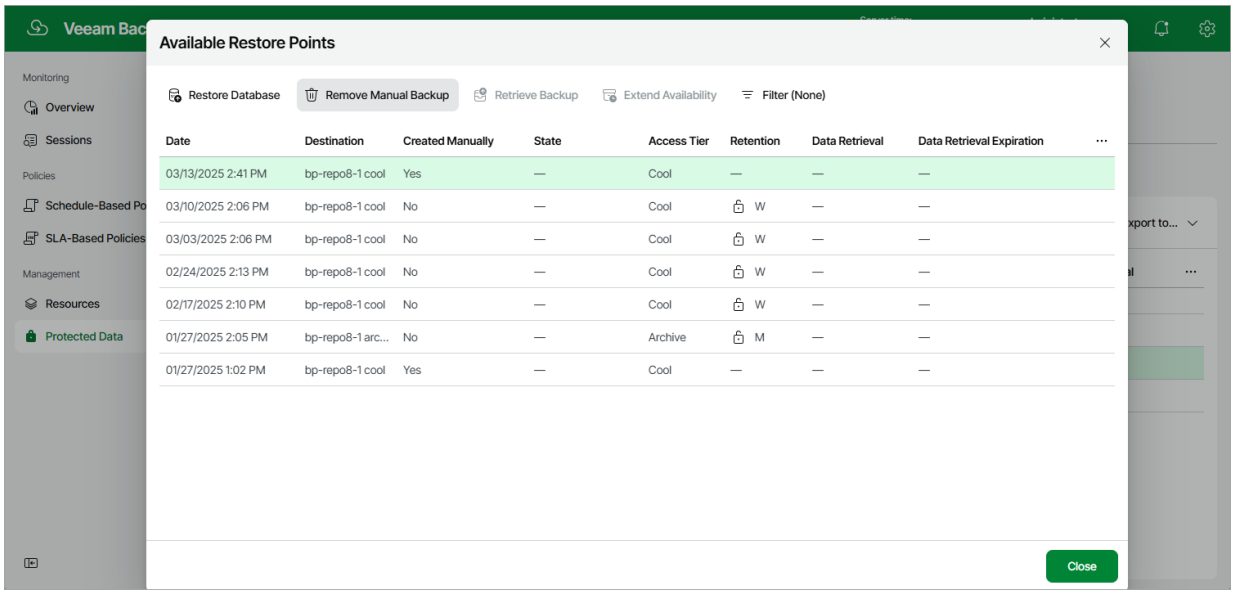
- **Manual** — to remove all backups created for the selected Azure SQL databases manually.




# Removing SQL Backups Created Manually

To remove all backups created for a SQL database manually, follow the instructions provided in Removing SQL Backups. If you want to remove a specific image-level backup created manually, do the following:

1. Navigate to **Protected Data** > **Databases** > **Azure SQL**.
2. Select the check box next to the necessary Azure SQL database, and click the link in the **Restore Points** column.
3. In the **Available Restore Points** window, select the necessary restore point and click **Remove Manual Backup**.



# Retrieving Data from Archive

Backups stored in archive repositories are not immediately accessible. If you want to restore an Azure SQL database from a backup that is stored in a repository of the Archive access tier, you must first retrieve the archived data. During the data retrieval process, a temporary copy of the archived data is created in an Azure blob container where the repository is located. This copy is stored in the Hot access tier for a period of time that you specify when launching the data retrieval process. If the time period expires while a restore operation is still running, Veeam Backup for Microsoft Azure automatically extends the period to keep the retrieved data available for one more hour. You can also extend the availability period manually.

To retrieve archived data, you can launch the data retrieval process either from the Data Retrieval wizard before you begin a restore operation, or directly from the SQL Database Restore wizard. When you retrieve archived data, you can choose one of the following priority options:

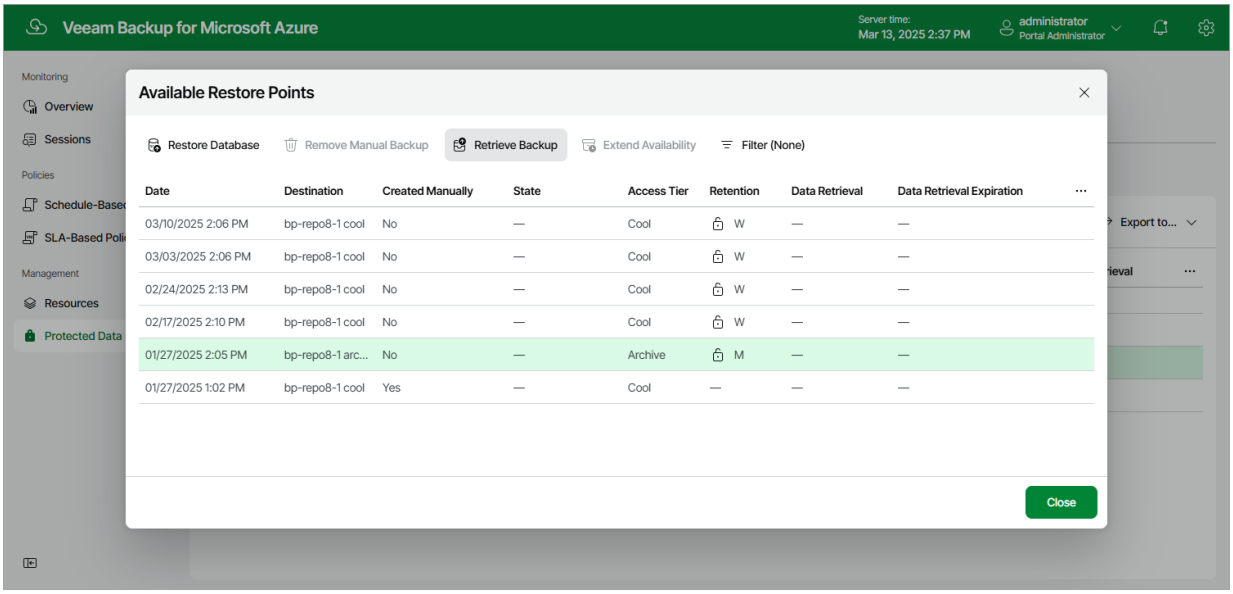
- **Standard Priority** — the default priority option. The retrieved data will be available within 15 hours.
- **High Priority** — the fastest but more expensive priority option. The retrieved data will be available within one hour if the size of the backup is less than 10 GB.

For more information on priority options, see Microsoft Docs

# Retrieving Data Manually

To retrieve archived data of an Azure SQL database, do the following:

1. Navigate to **Protected Data** > **Databases** > **Azure SQL**.
2. Select the necessary Azure SQL database.
3. Click the link in the **Restore Points** column.
4. In the **Available Restore Points** window, select a restore point that contains archived data you want to retrieve, and click **Retrieve Backup**. The **Data Retrieval** wizard will open.

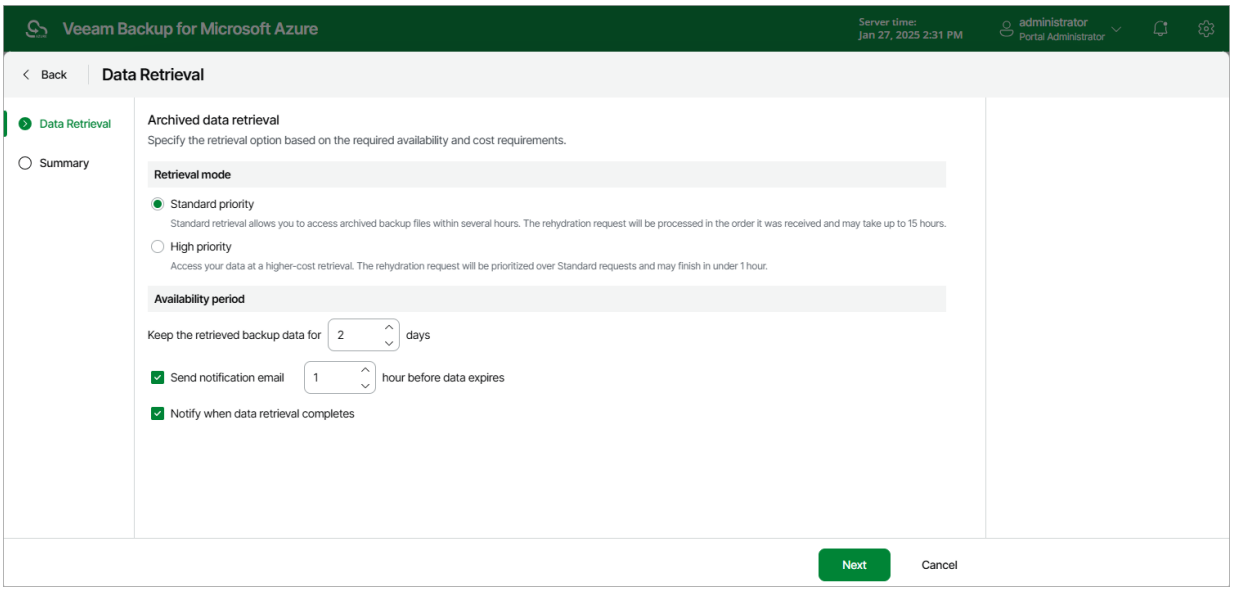



5. At the **Data Retrieval** step of the wizard, specify the following settings:
   a. In the **Retrieval mode** section, select the retrieval option that Veeam Backup for Microsoft Azure will use to retrieve the data.

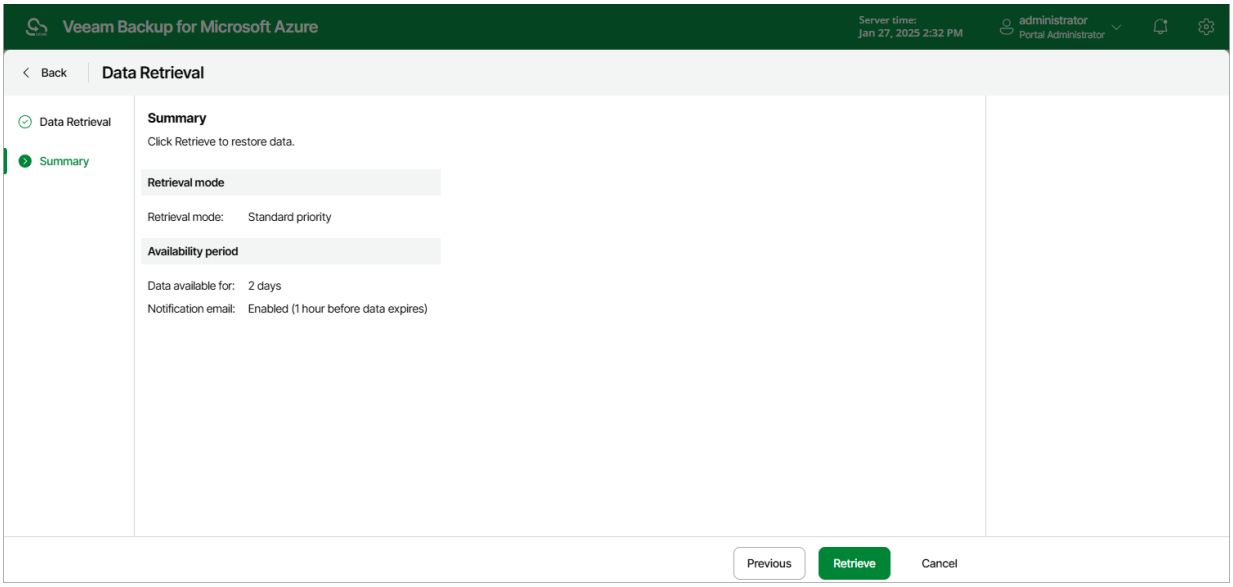
b. In the **Availability period** section, specify the number of days for which you want to keep the data available for restore operations.

You will be able to manually extend data availability later if required.

> **TIP**
>
> If you want to receive an email notification when data availability period is about to expire, select the **Send notification email** check box and choose when you want to be notified (that is, the number of hours remaining until data expiration).




6. At the **Summary** step of the **Data Retrieval** wizard, review configuration information and click **Retrieve**.




# Extending Data Availability

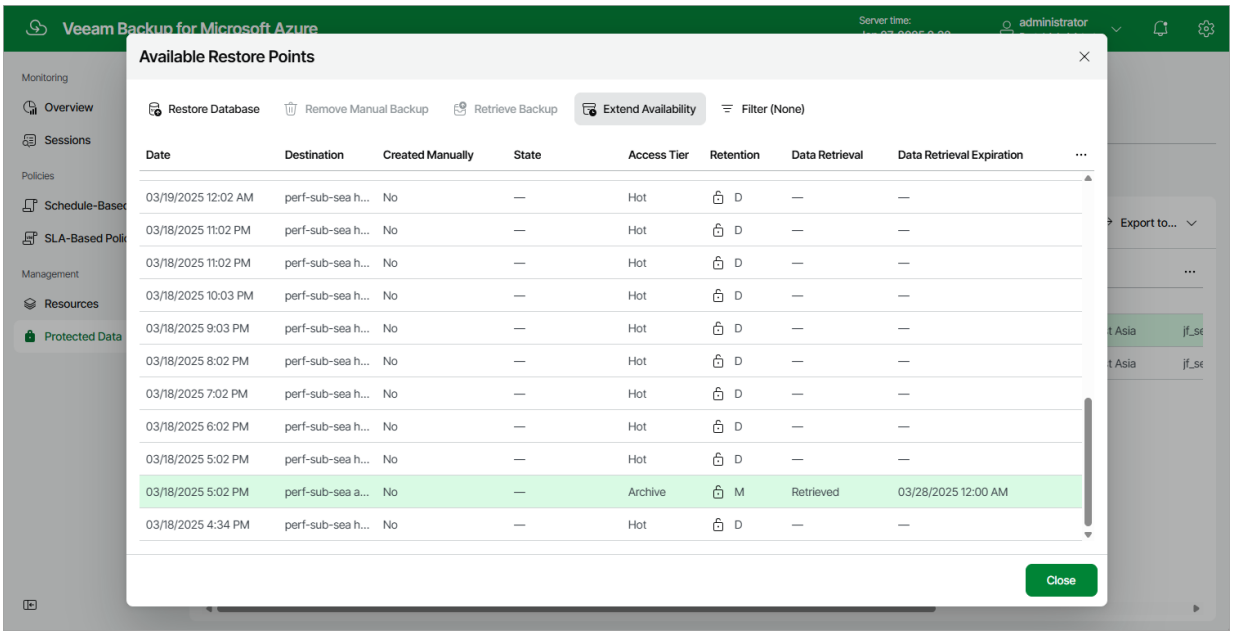
To extend time for which you want to keep retrieved data available for restore operations:

1. Select the Azure SQL database for which you want to extend availability of the retrieved data.

2. Click **Extend Availability**.

   Alternatively, click the link in the **Restore Points** column. In the **Data Retrieval** window, select the restore point that contains the retrieved data, and click **Extend Availability**.

3. In the **Extend Data Availability Period** window, specify the number of days for which you want to keep the data available for restore operations, and click **Extend**.



# Cosmos DB Data

After a backup policy successfully creates a restore point of a Cosmos DB account according to the specified schedule, after Veeam Backup for Microsoft Azure runs a configuration session, or after you create a backup of a Cosmos DB for PostgreSQL or a Cosmos DB for MongoDB account manually, Veeam Backup for Microsoft Azure adds the database to the resource list on the **Protected Data** page.

The **Protected Data** page displays Azure resources that are already protected by Veeam Backup for Microsoft Azure. Each resource is represented with a set of properties, such as:

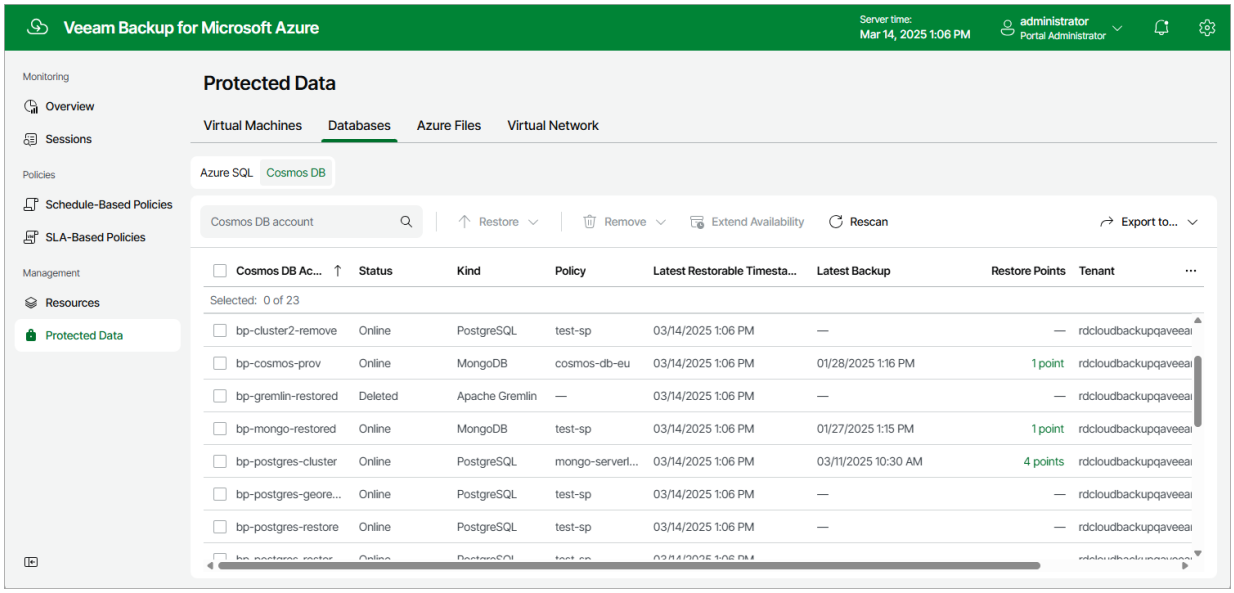
- **Cosmos DB Account** — the name of the protected Cosmos DB account.
- **Status** — the status of the protected Cosmos DB account.
- **Kind** — the API that was used to create the Cosmos DB account.
- **Policy** — the name of the backup policy that protects the Cosmos DB account.
- **Latest Restorable Timestamp** — the date and time of the most recent restorable timestamp created for the Cosmos DB account protected using the **Continuous backup** option.
- **Latest Backup** — the date and time of the most recent restore point created for the Cosmos DB for PostgreSQL or the Cosmos DB for MongoDB account protected using the **Backup to repository** option.
- **Restore Points** — a number of restore points created for the Cosmos DB for PostgreSQL or the Cosmos DB for MongoDB account protected using the **Backup to repository** option.

  To view the list of restore points, click the link in the **Restore Points** column. The **Available Restore Points** window will display information on each restore point, including the following: the date when the restore point was created, the access tier of the backup repository where the restore point is stored, and the configured retention policy settings (*D* — daily, *W* — weekly, *M* — monthly or *Y* — yearly).
- **Backup Size** — the total size of the standard Cosmos DB account backups.
- **Archive Size** — the total size of the Cosmos DB account backups stored in archive repositories.
- **Tenant** — the name and the ID of the Microsoft Entra tenant that contains the Cosmos DB account.
- **Subscription** — the name and the ID of the Azure subscription that manages the Cosmos DB account.
- **Resource Group** — the resource group to which the Cosmos DB account belongs.
- **Region** — an Azure region in which the Cosmos DB account resides.
- **Data Retrieval** — the status of the backups retrieval from the archive repository.

On the **Protected Data** page, you can also perform the following actions:

- Remove restore points if you no longer need them. For more information, see Removing Cosmos DB Backups.

- Restore data of backed-up Cosmos DB accounts. For more information, see Cosmos DB Restore.



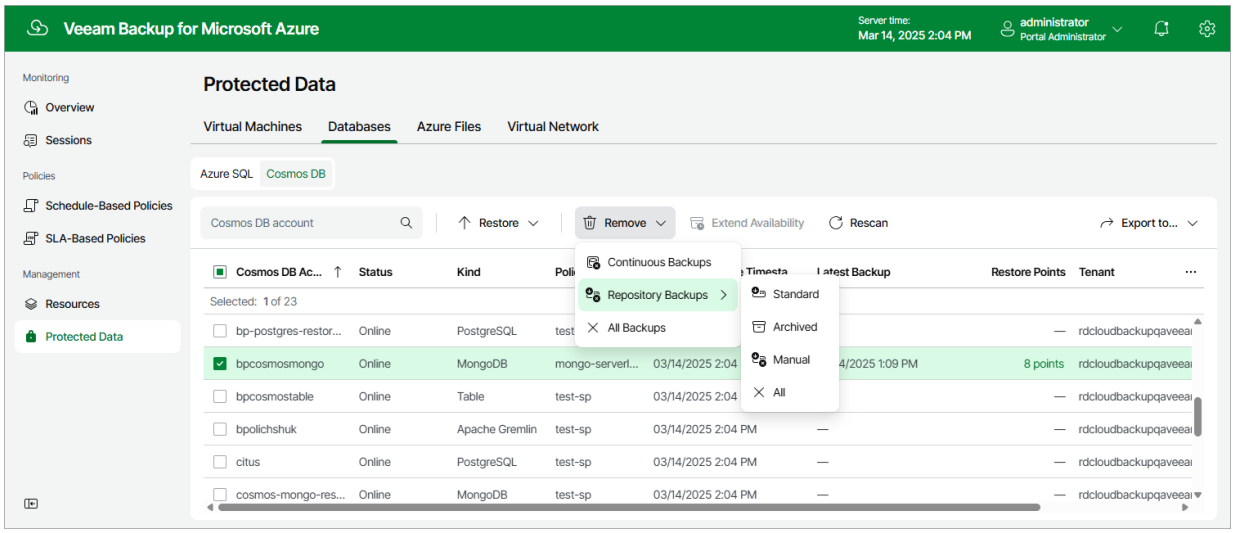

# Removing Cosmos DB Backups

Veeam Backup for Microsoft Azure applies the configured retention policy settings to automatically remove backups created for Cosmos DB accounts by backup policies. If necessary, you can also remove the backed-up data manually.

To remove backed-up data manually, do the following:

1. Navigate to **Protected Data** > **Databases** > **Cosmos DB**.
1. Select Cosmos DB accounts whose data you want to remove.
3. Click **Remove** and select either of the following options:
    - **All** — to remove all backups created for the selected Cosmos DB accounts both by backup policies and manually, including backups created using the **Continuous backup** option.
    - **Backups** — to remove all backups created in backup repositories for the selected Cosmos DB for PostgreSQL or Cosmos DB for MongoDB accounts protected using the **Backup to repository** option.
    - **Archive** — to remove all backups created in archive repositories for the selected Cosmos DB for PostgreSQL or Cosmos DB for MongoDB accounts protected using the **Backup to repository** option.
    - **Manual** — to remove all backups created for the selected Cosmos DB for PostgreSQL or Cosmos DB for MongoDB accounts manually.

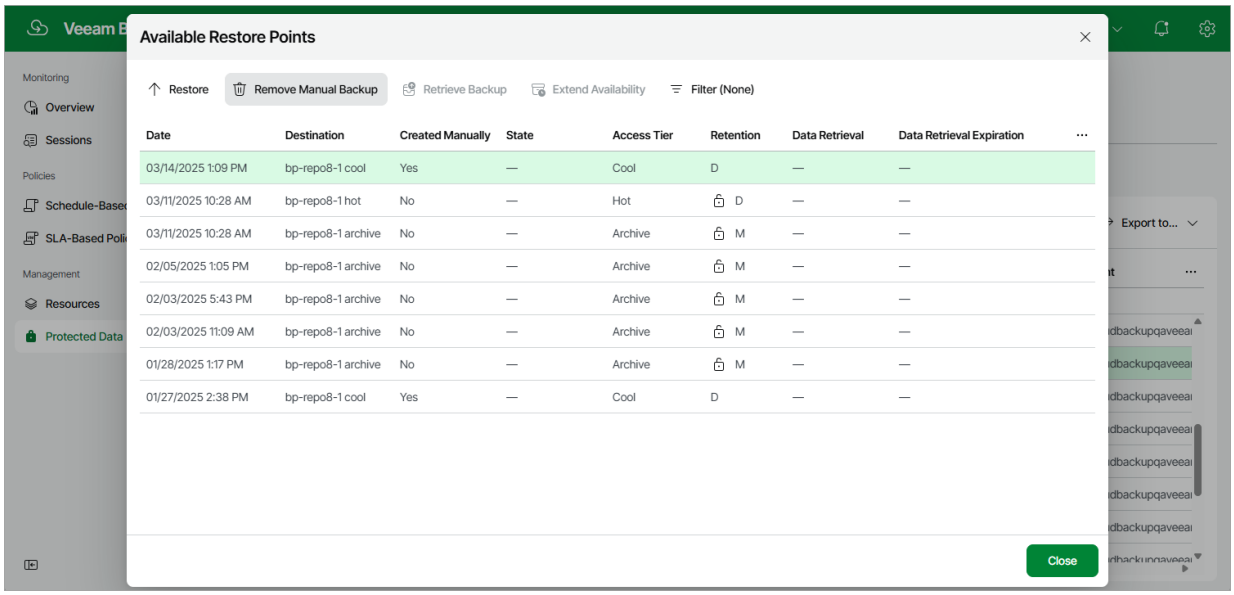
> **NOTE**
>
> When you select the **All** option, Veeam Backup for Microsoft Azure removes both backups created in backup repositories using the **Backup to repository** option and backups created in the configuration database using the **Continuous backup** option. However, the latter backups still remain in Microsoft Azure since they cannot be removed from the infrastructure on demand — Microsoft Azure removes these backups automatically upon expiration of the retention period. For more information, Microsoft Docs.




# Removing Cosmos DB Backups Created Manually

To remove all backups created for a Cosmos DB for PostgreSQL or Cosmos DB for MongoDB account manually, follow the instructions provided in Removing Cosmos DB Backups. If you want to remove a specific image-level backup created manually, do the following:

1. Navigate to **Protected Data** > **Databases** > **Cosmos DB**.
2. Select the check box next to the necessary Cosmos DB account, and click the link in the **Restore Points** column.
3. In the **Available Restore Points** window, select the necessary restore point and click **Remove Manual Backup**.



# Retrieving Data from Archive

Backups stored in archive repositories are not immediately accessible. If you want to restore a Cosmos DB account from a backup that is stored in a repository of the Archive access tier, you must first retrieve the archived data. During the data retrieval process, a temporary copy of the archived data is created in an Azure blob container where the repository is located. This copy is stored in the Hot access tier for a period of time that you specify when launching the data retrieval process. If the time period expires while a restore operation is still running, Veeam Backup for Microsoft Azure automatically extends the period to keep the retrieved data available for one more hour. You can also extend the availability period manually.

To retrieve archived data, you can launch the data retrieval process either from the Data Retrieval wizard before you begin a restore operation, or directly from the Cosmos DB Restore wizard. When you retrieve archived data, you can choose one of the following priority options:

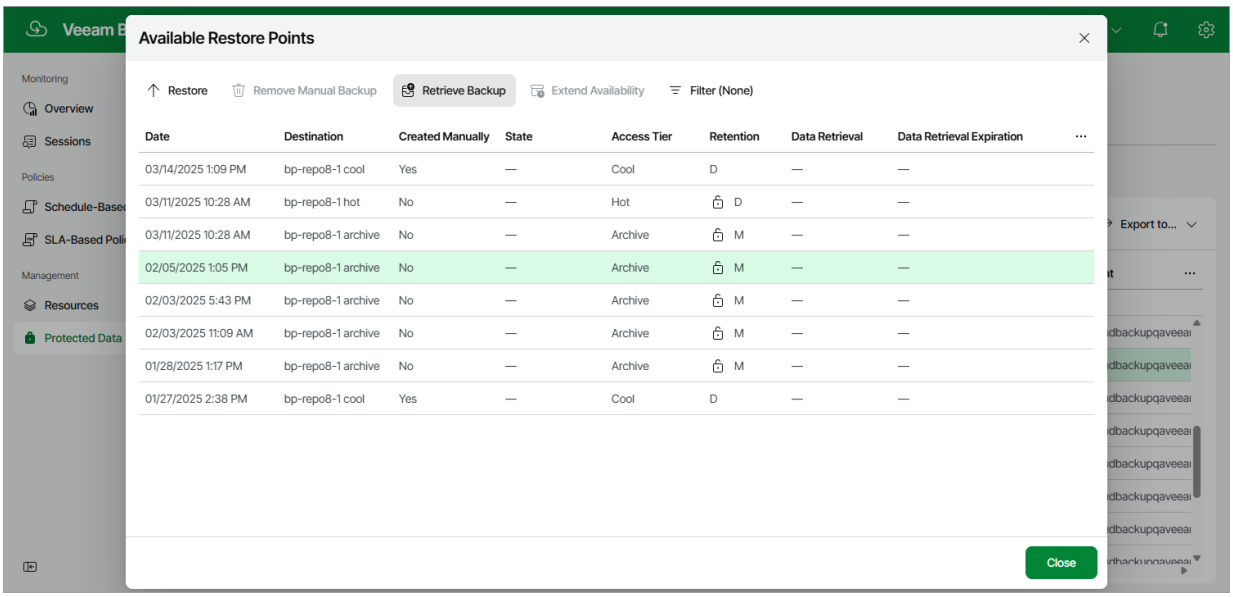
- **Standard Priority** — the default priority option. The retrieved data will be available within 15 hours.
- **High Priority** — the fastest but more expensive priority option. The retrieved data will be available within one hour if the size of the backup is less than 10 GB.

For more information on priority options, see Microsoft Docs

# Retrieving Data Manually

To retrieve archived data of a Cosmos DB account, do the following:

1. Navigate to **Protected Data** > **Databases** > **Cosmos DB**.
2. Select the necessary Cosmos DB account.
3. Click the link in the **Restore Points** column.
4. In the **Available Restore Points** window, select a restore point that contains archived data you want to retrieve, and click **Retrieve Backup**. The **Data Retrieval** wizard will open.

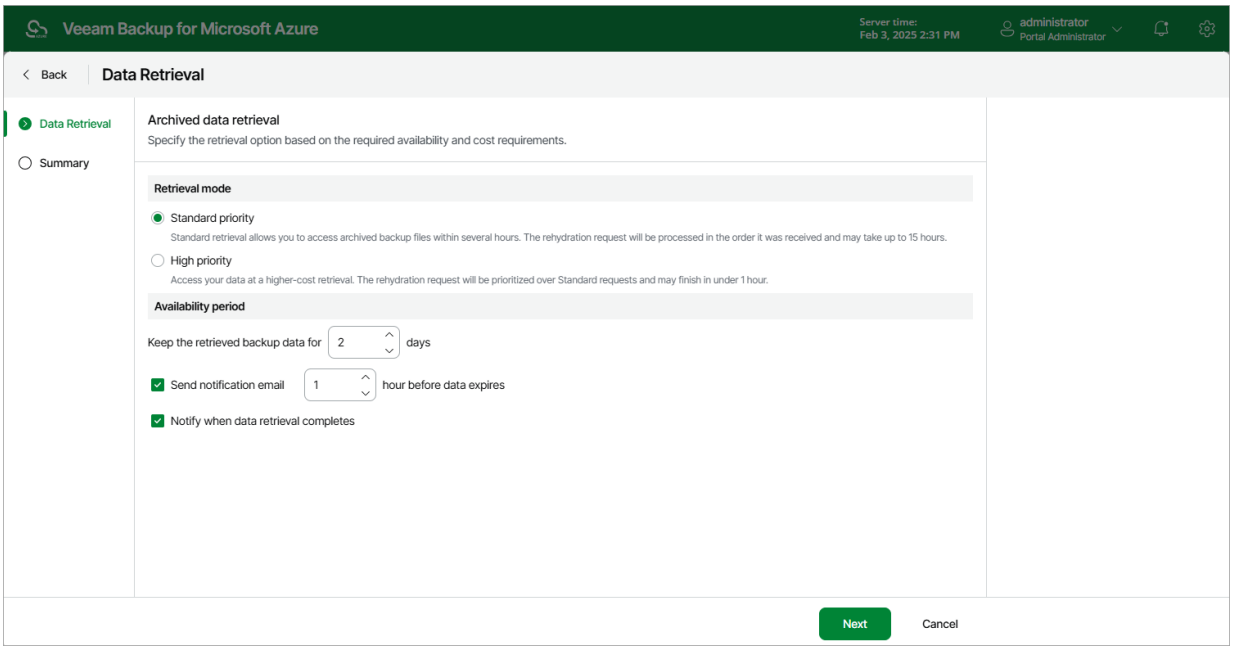



5. At the **Data Retrieval** step of the wizard, specify the following settings:
   a. In the **Retrieval mode** section, select the retrieval option that Veeam Backup for Microsoft Azure will use to retrieve the data.

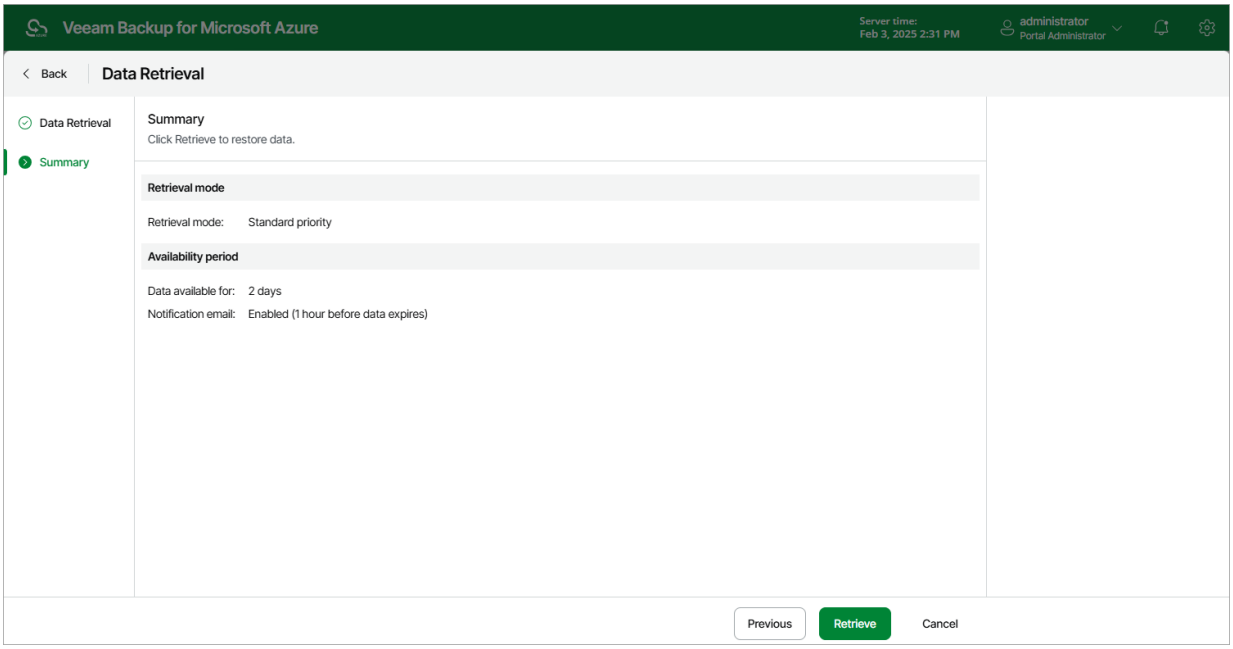
b. In the **Availability period** section, specify the number of days for which you want to keep the data available for restore operations.

You will be able to manually extend data availability later if required.

> **TIP**
>
> If you want to receive an email notification when data availability period is about to expire, select the **Send notification email** check box and choose when you want to be notified (that is, the number of hours remaining until data expiration).




6. At the **Summary** step of the **Data Retrieval** wizard, review configuration information and click **Retrieve**.

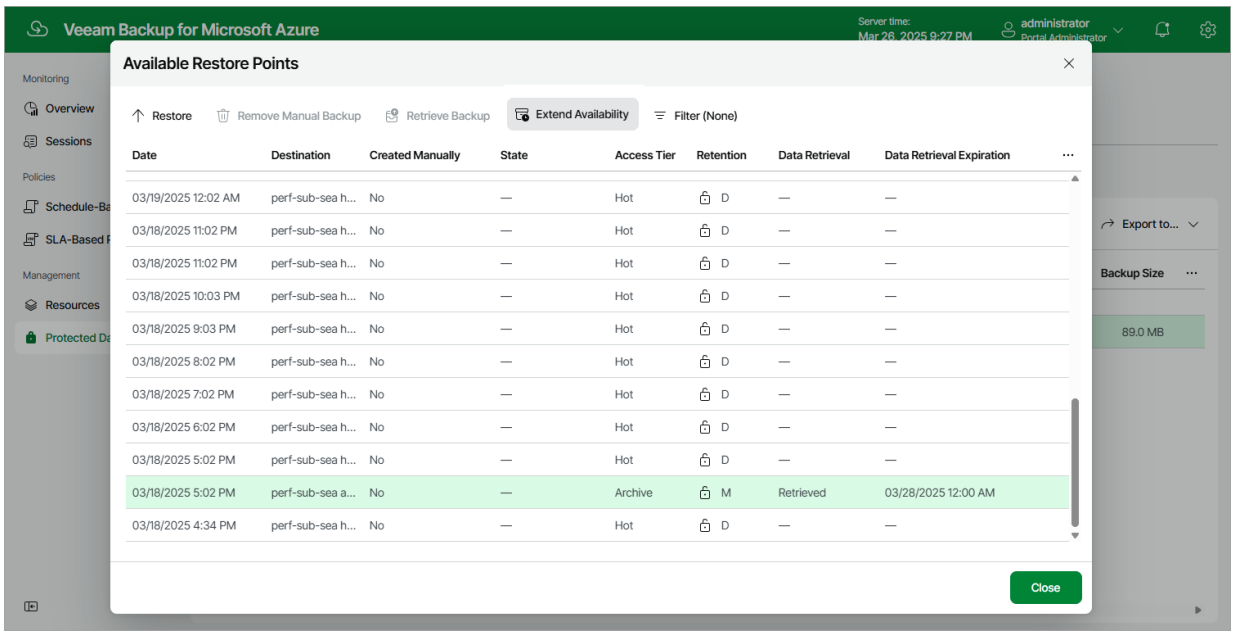


# Extending Data Availability

To extend time for which you want to keep retrieved data available for restore operations:

1. Select the Cosmos DB account for which you want to extend availability of the retrieved data.
2. Click **Extend Availability**.

   Alternatively, click the link in the **Restore Points** column. In the **Data Retrieval** window, select the restore point that contains the retrieved data, and click **Extend Availability**.
3. In the **Extend Data Availability Period** window, specify the number of days for which you want to keep the data available for restore operations, and click **Extend**.



# Azure Files Data

After a backup policy successfully creates a restore point of an Azure file share according to the specified schedule, or after you create a snapshot of a file share manually, Veeam Backup for Microsoft Azure adds the file share to the resource list on the **Protected Data** page.

The **Protected Data** page displays Azure resources that are already protected by Veeam Backup for Microsoft Azure. Each resource is represented with a set of properties, such as:

- **File Share** — the name of the Azure file share.
- **Policy** — the name of the backup policy that protects the Azure file share.
- **Restore Points** — a number of restore points created for the Azure file share.

  To view the list of restore points, click the link in the **Restore Points** column. The **Available Restore Points** window will display information on each restore point, including the following: the date when the restore point was created, the type of the restore point, and the configured retention policy settings (*D* — daily, *W* — weekly or *M* — monthly).

> **NOTE**
>
> Veeam Backup for Microsoft Azure displays all existing snapshots of Azure file share resources, not only snapshots created by the Veeam backup service. Azure file share snapshots created in Microsoft Azure Storage have the **External snapshot** type and cannot be deleted from the Veeam Backup for Microsoft Azure Web UI.

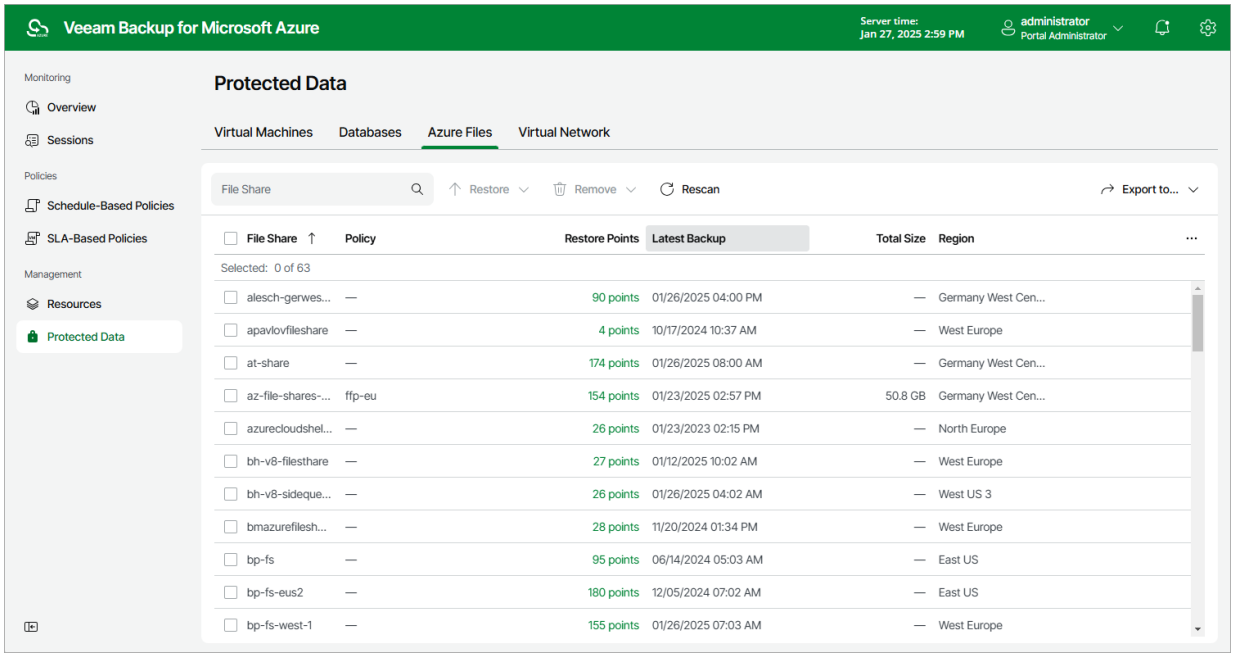
- **Latest Backup** — the date and time of the most recent restore point created for the Azure file share.
- **Total Size** — the total size of the Azure file share backups.
- **Region** — an Azure region in which the Azure file share resides.
- **Resource Group** — the resource group to which the Azure file share belongs.
- **Storage Account** — an Azure storage account in which the Azure file share resides.
- **File-level Recovery URL** — a link to the file-level recovery browser.

  The link appears when Veeam Backup for Microsoft Azure starts a restore session to perform file-level recovery.
- **Tenant ID** — the unique identification number of the Microsoft Entra tenant that contains the Azure file share.
- **Subscription ID** — the unique identification number of the Azure subscription that manages the Azure file share.

On the **Protected Data** page, you can also perform the following actions:

- Remove restore points if you no longer need them. For more information, see Removing File Share Snapshots.
- Restore data of backed-up Azure file shares. For more information, see File Share Restore.

> **NOTE**
>
> Consider that if you delete a file share from Microsoft Azure, the snapshots of this file share will be deleted as well. To protect your snapshots from accidental deletion, you can use the file share soft delete option. For more information on the soft delete option for Azure file shares, see Microsoft Docs.




# Removing File Share Snapshots

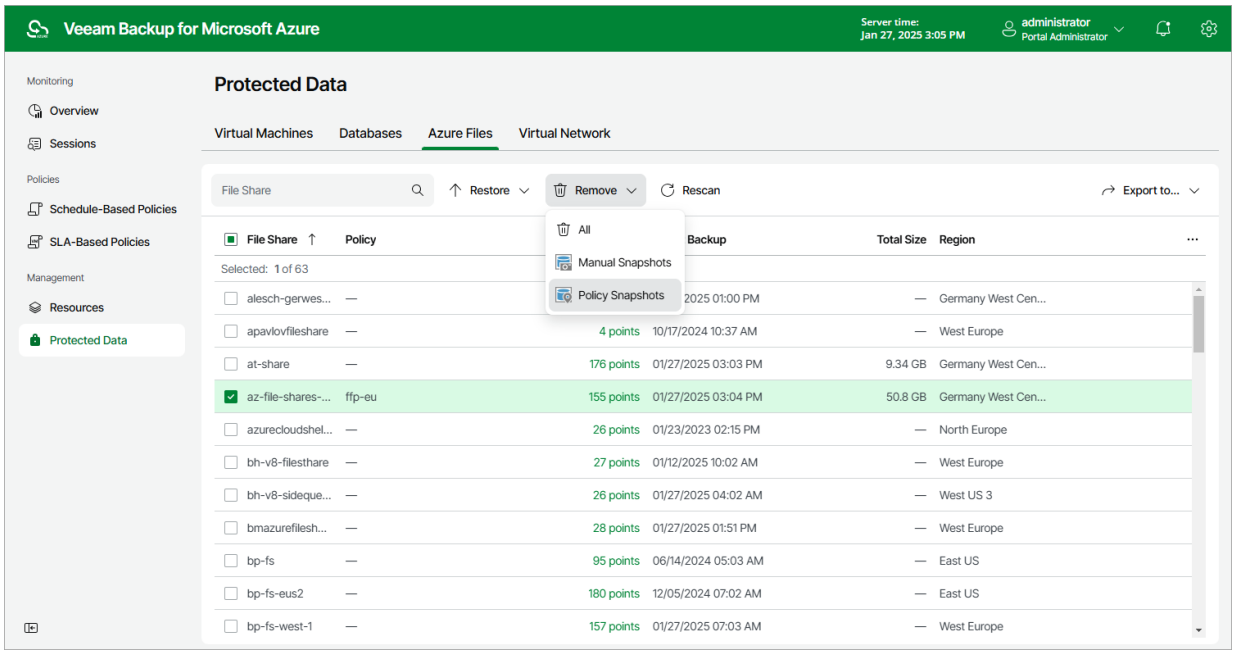
Veeam Backup for Microsoft Azure applies the configured retention policy settings to automatically remove cloud-native snapshots created by backup policies. If necessary, you can also remove the backed-up data manually.

> **NOTE**
>
> In Veeam Backup for Microsoft Azure, you can remove only snapshots created by the Veeam backup service. To delete **External snapshots**, use Microsoft Azure portal as described in Microsoft Docs.

To remove backed-up data manually, do the following:

1. Navigate to **Protected Data** > **Azure Files**.
2. Select Azure file shares whose data you want to remove.
3. Click **Remove** and select either of the following options:
   - **All** — to remove all cloud-native snapshots created for the selected Azure file shares both by backup policies and manually.
   - **Policy Snapshots** — to remove all cloud-native snapshots created for the selected Azure file shares by backup policies.

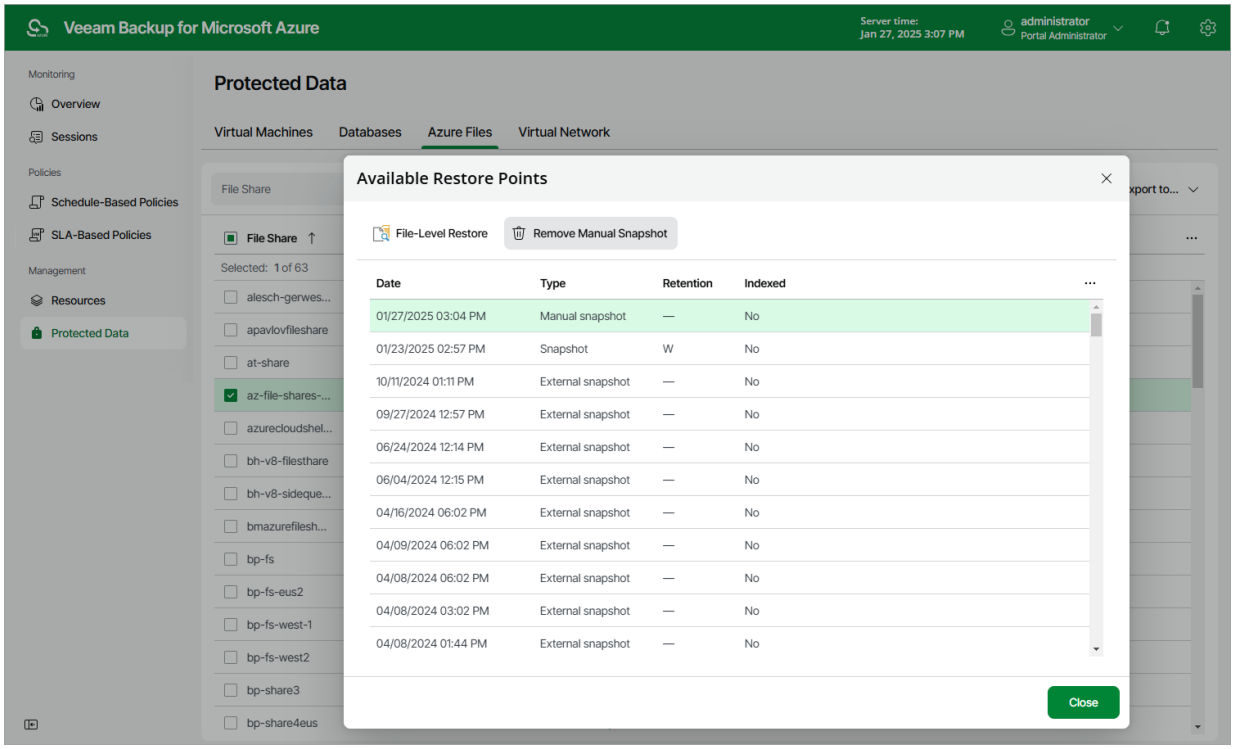
- **Manual Snapshots** — to remove all cloud-native snapshots created for the selected Azure file shares manually.




# Removing File Share Snapshots Created Manually

To remove all cloud-native snapshots created for a file share manually, follow the instructions provided in Removing File Share Snapshots. If you want to remove a specific cloud-native snapshot created manually, do the following:

1. Navigate to **Protected Data** > **Azure Files**.
2. Select the check box next to the necessary file share, and click the link in the **Restore Points** column.
3. In the **Available Restore Points** window, select the necessary snapshot and click **Remove Manual Snapshot**.



# Virtual Network Configuration Data

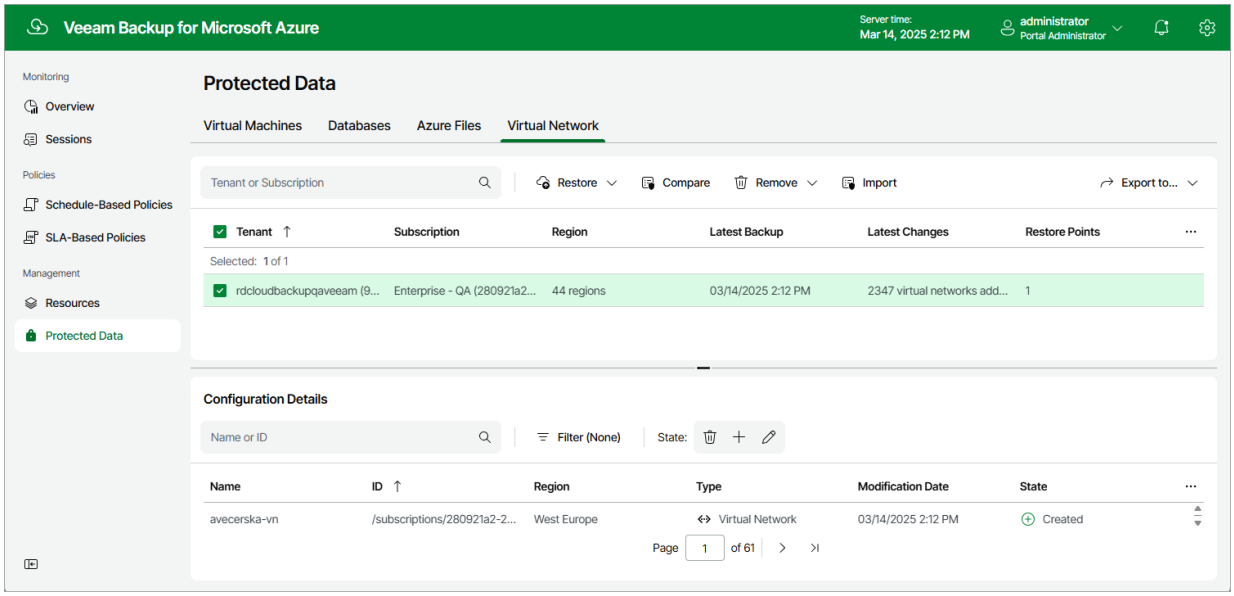
After the Virtual Network Configuration Backup policy successfully creates a restore point for the virtual network configuration of an Azure subscription within a Microsoft Entra tenant, the configuration record is automatically added to the resource list on the **Protected Data** page.

For each protected Azure subscription associated with the Microsoft Entra tenant, Veeam Backup for Microsoft Azure creates a configuration record in the database with the following set of properties:

- **Tenant** – a name of an Microsoft Entra tenant whose service account was used to collect the virtual network configuration data.
- **Subscription** – an Azure subscription whose virtual network configuration data is backed up.
- **Region** – a number of Azure regions in which the virtual network configuration data resides.
- **Latest Backup** – the date and time of the latest created restore point.
- **Latest Changes** – the summary of changes in the virtual network configuration in comparison with the previous restore point.
- **Restore Points** – a number of restore points created for the subscription.

On the **Protected Data** page, you can perform the following actions:

- Compare the items of the current virtual network configuration with the items stored in a backup. For more information, see Comparing Virtual Network Configuration Backups.
- Import all virtual network configuration backups stored in repositories to the Veeam Backup for Microsoft Azure database. For more information, see Importing Virtual Network Configuration Data.
- Remove restore points if you no longer need them. For more information, see Removing Virtual Network Configuration Backups.
- Restore data of backed-up virtual network configurations. For more information, see Performing Virtual Network Configuration Restore Using Web UI.



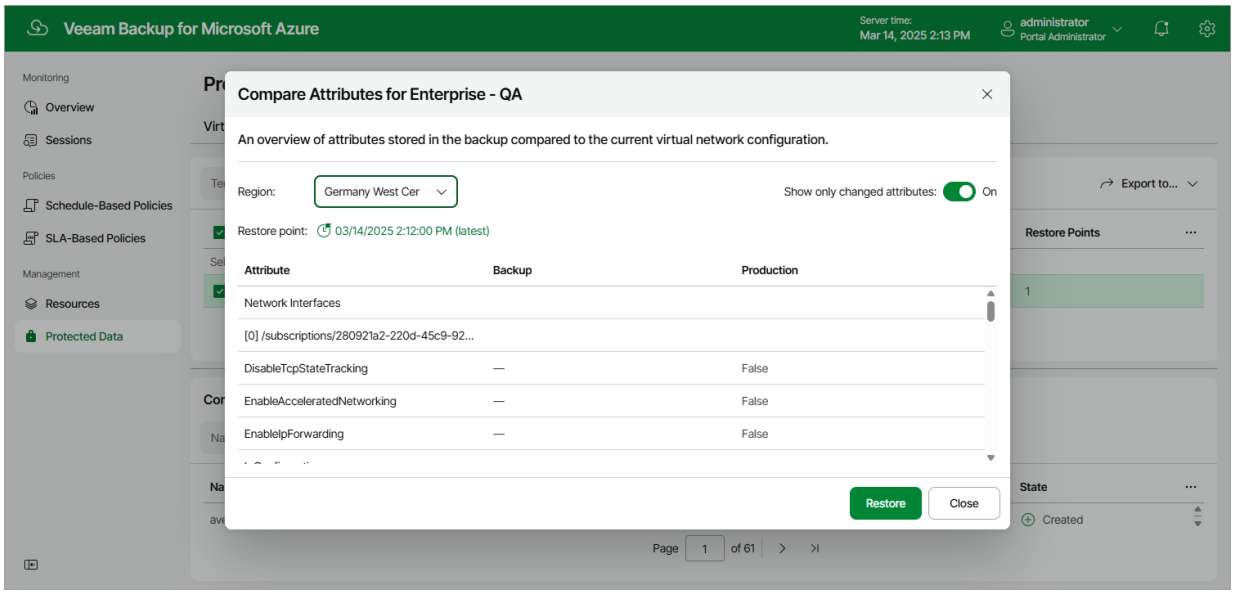
# Comparing Virtual Network Configuration Backups

You can compare the current Azure virtual network configuration of an Azure subscription to the virtual network configuration contained in any available restore point. To do that:

1. Navigate to **Protected Data** > **Virtual Network**.
2. Select the configuration record for an Azure subscription whose virtual network configuration you want to compare.
3. Click **Compare**.

By default, Veeam Backup for Microsoft Azure uses the most recent valid restore point. However, you can compare the virtual network configuration data to an earlier state. In the **Compare Attributes** window, click the link to the right of **Restore point** to select the necessary restore point.

If you want Veeam Backup for Microsoft Azure to display only backed-up virtual network configuration items that differ from the current virtual network configuration items, set the **Show only changed attributes** toggle to *On*.




# Importing Virtual Network Configuration Data

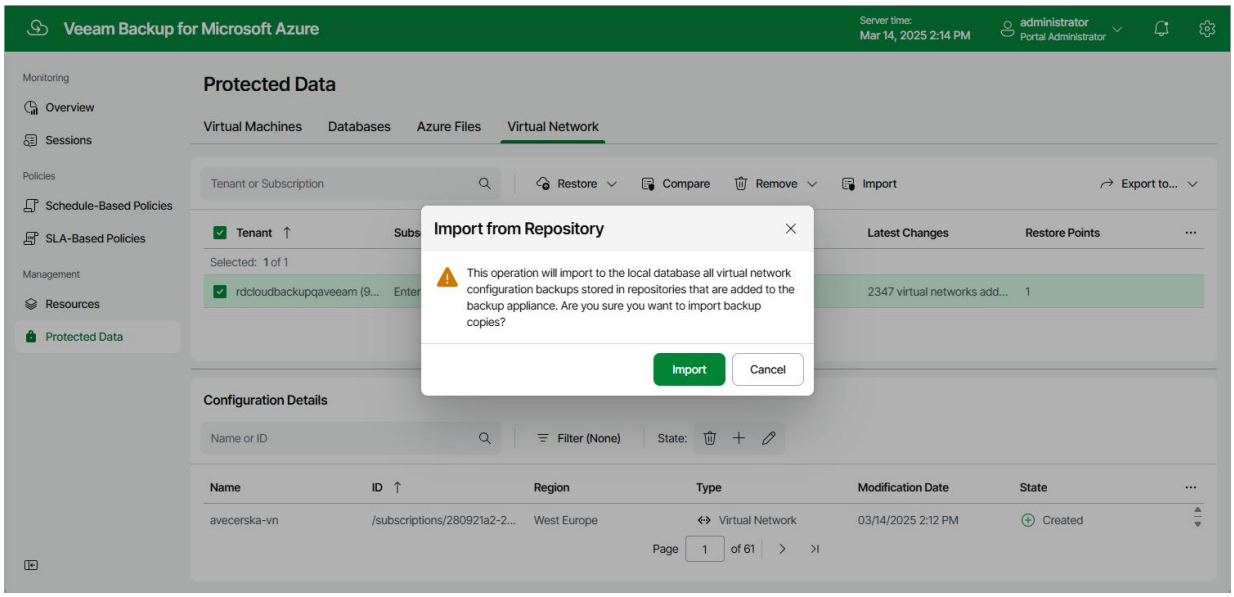
The **Protected Data** page only shows configuration records saved to the configuration database of the backup appliance. That is why you can restore virtual network configuration from these records only.

When you add a new repository to your backup appliance, Veeam Backup for Microsoft Azure checks whether any virtual network configuration backups are stored in this repository and then automatically imports all the detected restore points to the configuration database.

You can also manually import any deleted virtual network configuration backups to the local database, in case these backups are still stored in repositories added to the backup appliance. To do that:

1. Navigate to **Protected Data** > **Virtual Network**.

2. Click **Import**. Veeam Backup for Microsoft Azure will update the list of configuration records.




# Removing Virtual Network Configuration Backups

Veeam Backup for Microsoft Azure applies the configured retention policy settings to automatically remove virtual network configuration backups and backup copies created by the Virtual Network Configuration Backup policy. If necessary, you can also remove these backups manually — from the configuration database, from the repository or both. Keep in mind that:

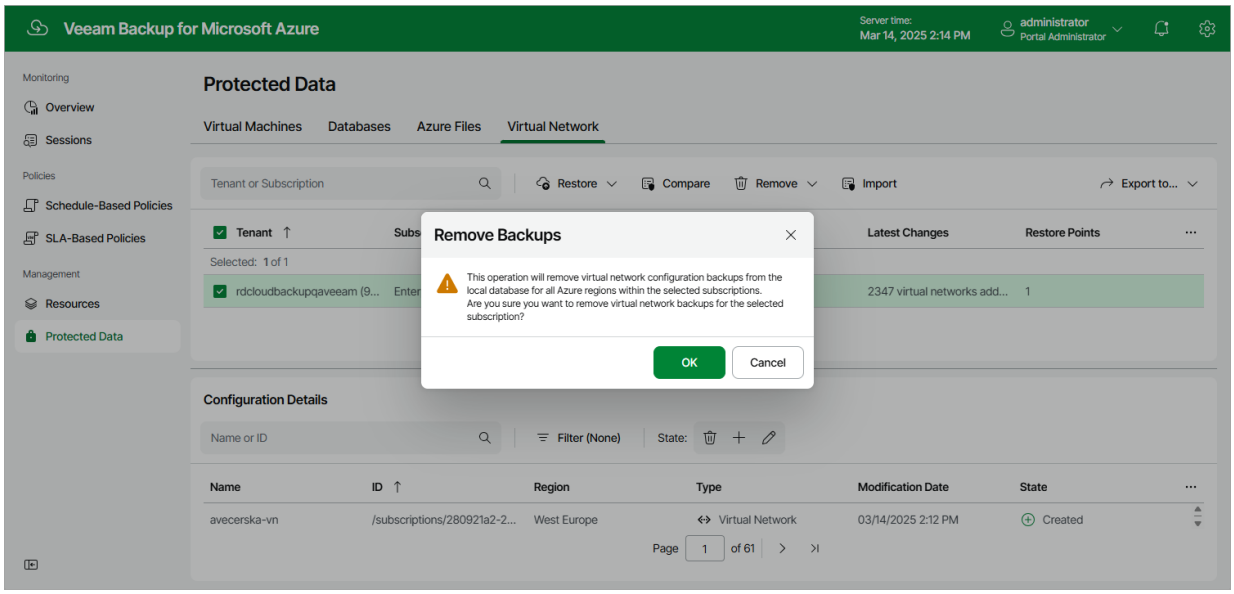
- If a backup is removed from both the configuration database and the repository, you will no longer be able to use this backup to restore the virtual network configuration data.
- If a backup is removed from the repository but still exists in the configuration database, you will be able to use this backup to restore the virtual network configuration data.
- If a backup is removed from the configuration database but still exists in the repository, you will be able to use this backup to restore the virtual network configuration data — but you will first have to import it to the database as described in section Importing Virtual Network Configuration Data.

To remove backed-up data manually, do the following:

1. Navigate to **Protected Data** > **Virtual Network**.
2. Select the configuration record for which you want to remove the backed-up data.

   Each configuration record contains a whole set of all virtual network configuration backups created for an Azure subscription. Note that you cannot remove individual virtual network configuration items or specific backups.
3. Click **Remove** and select one of the following options:
   - **Backups** — to remove all virtual network configuration backups for the selected configuration record from the Veeam Backup for Microsoft Azure database.
   - **Backup Copies** — to remove all virtual network configuration backups of an Azure subscription from all backup repositories.

- **All** – to remove all virtual network configuration backups for the selected configuration record.



# Performing Restore

In various disaster recovery scenarios, you can perform the following restore operations using backed-up data:

- Restore of Azure VMs — restore Azure VMs from cloud-native snapshots or image-level backups to the original location or to a new location.
- Restore of Azure SQL databases — restore Azure SQL databases from backups to the original or to a new location.
- Restore of Cosmos DB accounts — restore Cosmos DB accounts from restorable timestamps using native Microsoft Azure capabilities, or databases of Cosmos DB for PostgreSQL accounts from backups stored in Veeam repositories.
- Restore of Azure Files — restore files of file shares from cloud-native snapshots to the original location or to a new location.
- Restore of virtual network configurations — restore virtual network configurations from virtual network configuration backups to the original location or to a new location.
- Instant Recovery — immediately restore of Azure VMs from image-level backups to VMware vSphere and Hyper-V environments, and to Nutanix AHV clusters.
- Azure VM disk export — restore virtual disks and convert them to disks of the VMDK, VHD or VHDX format.
- Azure VM disk publish — publish point-in-time virtual disks and copy the necessary files and folders to the target server.
- Restore to AWS — restore Azure VMs from image-level backups to AWS as EC2 instances.
- Restore to Google Cloud — restore Azure VMs from image-level backups to Google Cloud as VM instances.
- Restore to Nutanix AHV — restore Azure VMs from image-level backups to Nutanix AHV as Nutanix AHV VMs.

> **NOTE**
>
> You can perform all recovery operations using restore points stored in standard repositories. For restore points stored in archive repositories, only restore of Azure VMs, Azure SQL databases, databases of Cosmos DB for PostgreSQL accounts and databases and collections of Cosmos DB for MongoDB accounts to Microsoft Azure is supported.

# VM Restore

The actions that you can perform with restore points of Azure VMs depend on whether you access the restore points using the Veeam Backup & Replication console or the Veeam Backup for Microsoft Azure Web UI.

# Performing VM Restore Using Console

Veeam Backup & Replication offers the following restore operations:

- Entire VM restore — restore an entire Azure VM from a restore point.
- Guest OS file recovery — restore individual files and folders of an Azure VM.
- Application restore — restore applications such as Microsoft Entra ID, Microsoft Exchange, Microsoft SharePoint, and Microsoft SQL Server.

You can restore VM data to the most recent state or to any available restore point.

## Performing Entire VM Restore

In case a disaster strikes, you can restore entire Azure VM from a cloud-native snapshot or an image-level backup. Veeam Backup & Replication allows you to restore one or more Azure VMs at a time, to the original location or to a new location.

## How Instance Restore Works

To restore Azure VMs from cloud-native snapshots, Veeam Backup & Replication uses native Azure capabilities. To restore VMs from image-level backups, Veeam Backup & Replication uses different algorithms depending on whether a backup appliance is added to the backup infrastructure:

- If a backup appliance is connected to the backup server, Veeam Backup & Replication uses the restore algorithm described in section Performing Entire VM Restore.
- If a backup appliance is not connected to the backup server, Veeam Backup & Replication uses the restore algorithm described in the Veeam Backup & Replication User Guide, section How Restore to Microsoft Azure Works.

## How to Perform VM Restore

To restore an entire VM, do the following:

1. Launch the Restore to Azure wizard.
2. Select a restore point.
3. Choose a restore mode.
4. Specify an Azure subscription and region.
5. Specify a new VM name and resource group.
6. Specify VM configuration settings.
7. Specify a VM size.
8. Configure network and security group settings.
9. Specify a restore reason.
10. Finish working with the wizard.

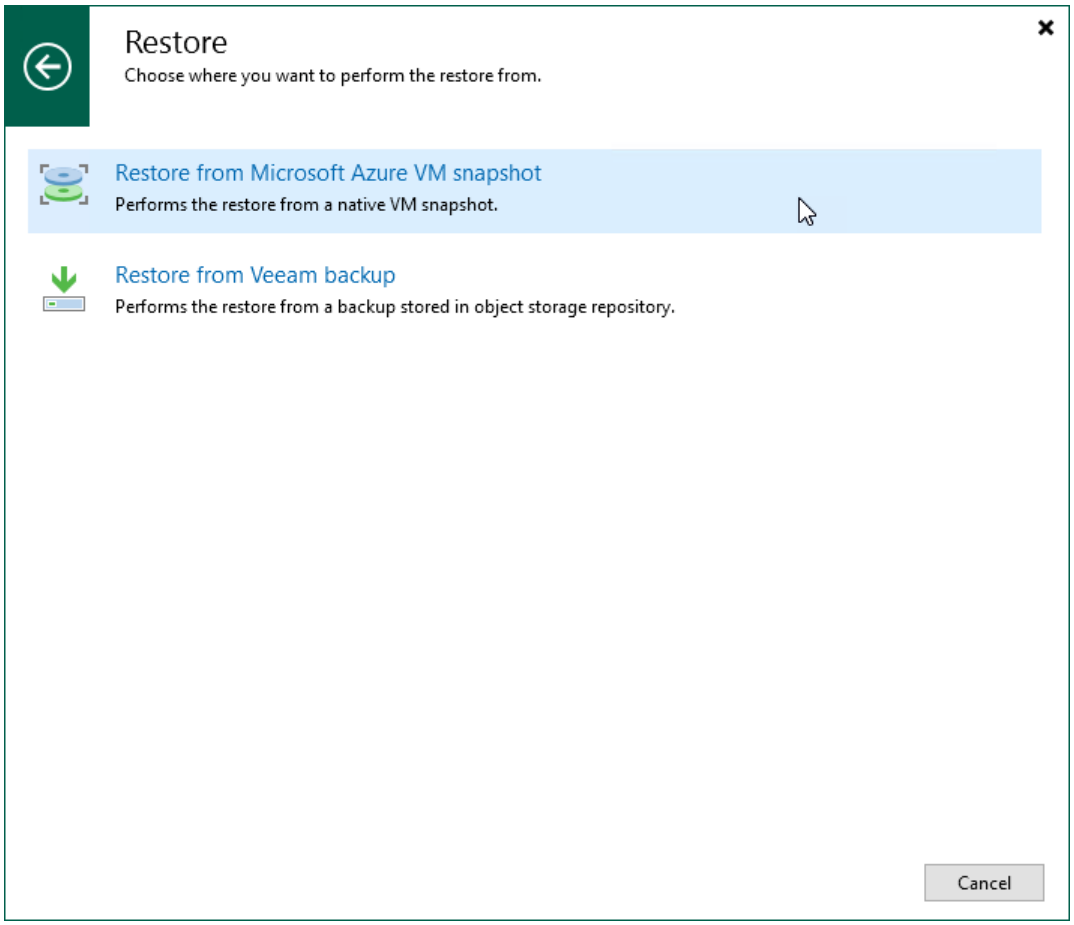
## Step 1. Launch Restore to Microsoft Azure Wizard

To launch the **Restore to Microsoft Azure** wizard, do the following:

1. In the Veeam Backup & Replication console, open the **Home** view.
2. Navigate to **Backups** > **Snapshots** if you want to restore from a cloud-native snapshot, or to **Backups** > **External Repository** if you want to restore from an image-level backup.
3. In the working area, expand the backup policy that protects an Azure VM that you want to restore, select the necessary VM and click **Microsoft Azure Iaas** on the ribbon.

   Alternatively, you can right-click the instance and select **Restore to Microsoft Azure Iaas**.

> **TIP**
>
> You can also launch the **Restore to Microsoft Azure** wizard from the **Home** tab. To do that, click **Restore** and select **Microsoft Azure**. Then, in the **Restore** window, select **Microsoft Azure Iaas** > **Entire machine restore** > **Restore to public cloud** > **Restore to Microsoft Azure** and, depending on whether you want to restore from a backup or a snapshot, click either **Restore from Microsoft Azure VM snapshot** or **Restore from Veeam backup**.



## Step 2. Select VM and Restore Point

At the **Virtual Machine** step of the wizard, choose a restore point that will be used to restore the selected Azure VM. By default, Veeam Backup & Replication uses the most recent valid restore point. However, you can restore the VM data to an earlier state.

To select a restore point, do the following:

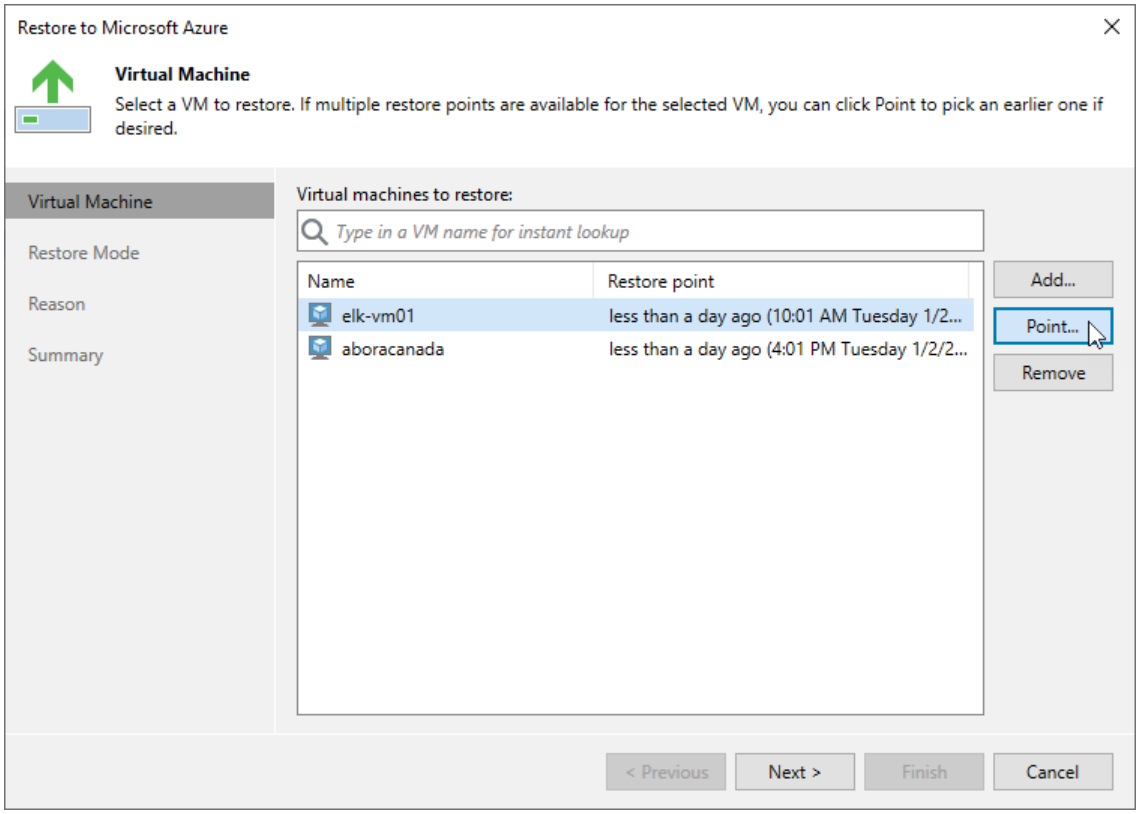
1. In the **Virtual machines to restore** list, select the Azure VM and click **Point**.
2. In the **Restore Points** window, expand the backup policy that protects the VM, select the necessary restore point and click **OK**.

   To help you choose a restore point, Veeam Backup & Replication provides the following information on each available restore point:

   - **Job** – the name of the backup policy that created the restore point and the date when the restore point was created.
   - **Type** – the type of the restore point.
   - **Location** – the region or repository where the restore point is stored.

> **TIP**
>
> You can use the wizard to restore multiple instances at a time. To do that, click **Add**, select more Azure VMs to restore and choose a restore point for each of them.

Note that if you want to restore an Azure VM from a backup that is stored in a repository of the Archive access tier, you must first retrieve the archived data. That is why Veeam Backup & Replication will open the **Retrieve Backup** wizard if the selected restore point is stored in an archive repository. To learn how to complete the wizard and retrieve the archived data, see Retrieving Data from Archive.



### Retrieving Data from Archive

Backups stored in archive repositories are not immediately accessible. If you want to restore an Azure VM from a backup that is stored in a repository of the Archive access tier, you must first retrieve the archived data.

During the data retrieval process, a temporary copy of the archived data is created in an Azure blob container where the repository is located. This copy is stored in the Hot or Cool access tier for a period of time that you specify when launching the data retrieval process. If the time period expires while a restore operation is still running, Veeam Backup for Microsoft Azure automatically extends the period to keep the retrieved data available for one more hour. You can also extend the availability period manually.

## Retrieving Data

To retrieve data from an archived restore point, complete the **Retrieve Backup** wizard:

1. At the **Retrieval Mode** step of the wizard, choose the retrieval mode that Veeam Backup & Replication will use to retrieve the archived data:
   - **Standard Priority** – the default priority mode. If you choose this mode, the retrieved data will be available within 15 hours.
   - **High Priority** – the faster but more expensive priority mode. If you choose this mode, the retrieved data will be available within one hour if the size of a backup file is less than 10 GB.

   For more information on priority options, see Microsoft Docs.
2. At the **Availability Period** step of the wizard, specify the number of days for which you want to keep the data available for restore operations.

   The data will be available during the day when the retrieval process completes plus the specified number of days. Each day starts at 12:00 AM and ends at 11:59 PM (in your appliance time zone). For example, if the data retrieval finished at 3:00 PM on June 6, and the availability period is set to 1 day, the data will be available till 11:59 PM on June 7.

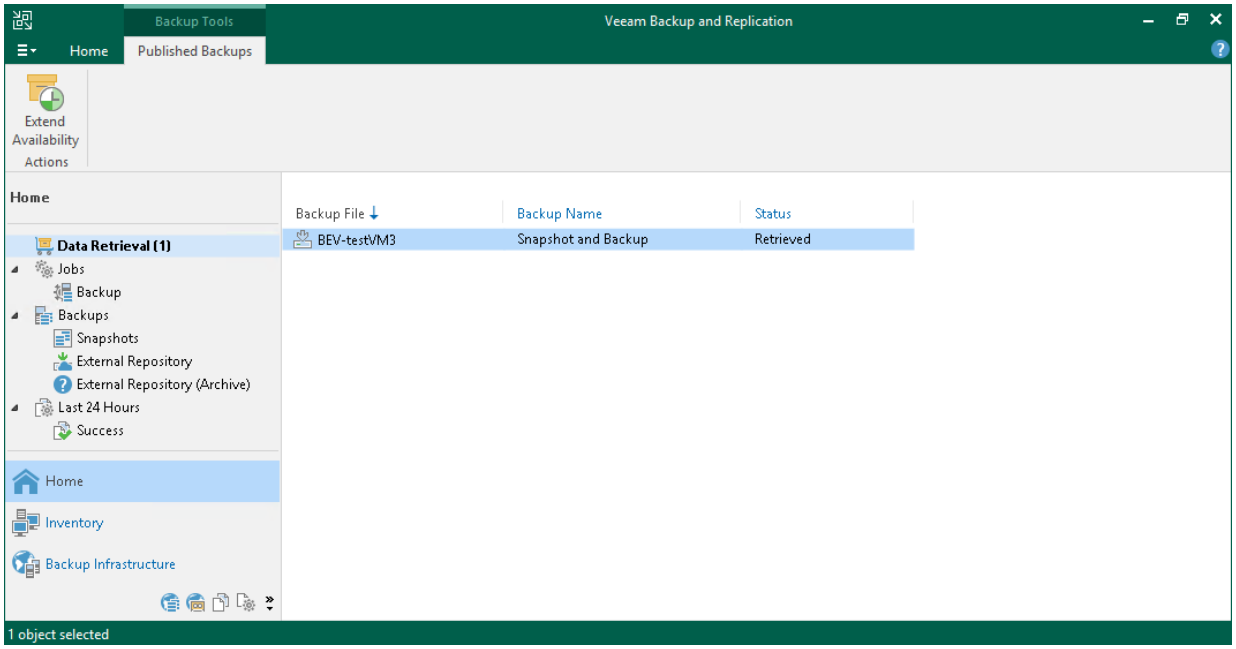
   You will be able to manually extend data availability later if required.

> **TIP**
>
> If you want to receive an email notification when the data availability period is about to expire, select the **Enable e-mail notifications** check box and choose when you want to be notified (that is, the number of hours remaining until data expiration).
>
> To learn how to configure global email notification settings, see the Veeam Backup & Replication User Guide, section Configuring Global Email Notification Settings.

3. At the **Summary** step of the wizard, review summary information and click **Finish**.

   The retrieved data will be displayed in the **Home** view under the **Data Retrieval** node.

After you complete the **Retrieve Backup** wizard, you will be able to proceed with the **Restore to Microsoft Azure** wizard. However, the restore process will start only after the data is retrieved.



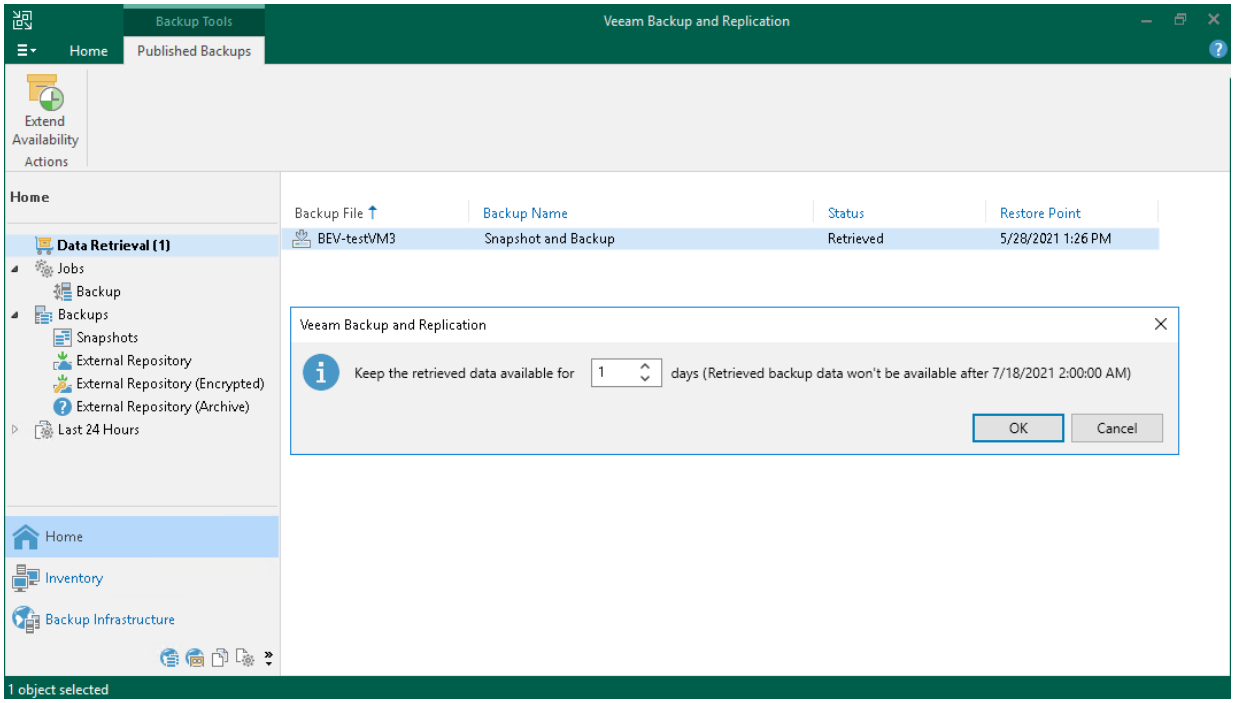

# Extending Data Availability

To extend time for which you want to keep retrieved data available for restore operations:

1. In the Veeam Backup & Replication console, open the **Home** view.
2. Navigate to **Data Retrieval** node.
3. Select an Azure VM for which you want to extend availability of the retrieved data and click **Extend Availability** on the ribbon.

   Alternatively, you can right-click the VM and click **Extend availability**.

4. In the opened window, specify the number of days for which you want to keep the data available for restore operations, and click **OK**.



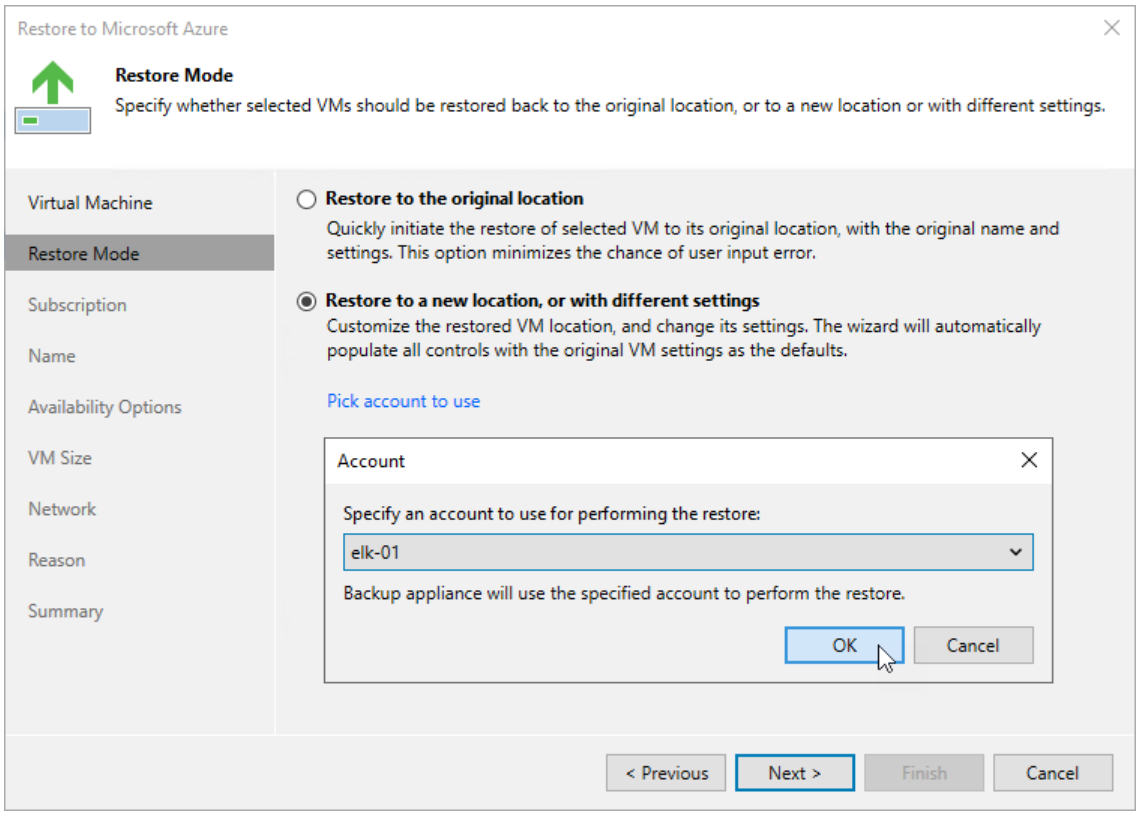
## Step 3. Choose Restore Mode

At the **Restore Mode** step of the wizard, do the following:

1. Choose whether you want to restore the selected Azure VM to the original or to a new location.
2. Click **Pick account to use** to select a service account whose permissions will be used to perform the restore operation. For more information on the required permissions, see Service Account Permissions.

   For a service account to be displayed in the list of available accounts, it must be added to Veeam Backup for Microsoft Azure and assigned the *Azure VM Restore* operational role as described in section Adding Service Accounts.

> **NOTE**
>
> To perform restore operations, Veeam Backup & Replication uses permissions of service accounts that belong to the tenants that contained original VMs. If none of the service accounts added to Veeam Backup for Microsoft Azure belong to these tenants, the **Restore to the original location** option will not be available.



# Step 4. Specify Azure Subscription and Region

[This step applies only if you have selected the **Restore to a new location, or with different settings** option at the **Restore Mode** step of the wizard]

At the **Subscription** step of the wizard, do the following:

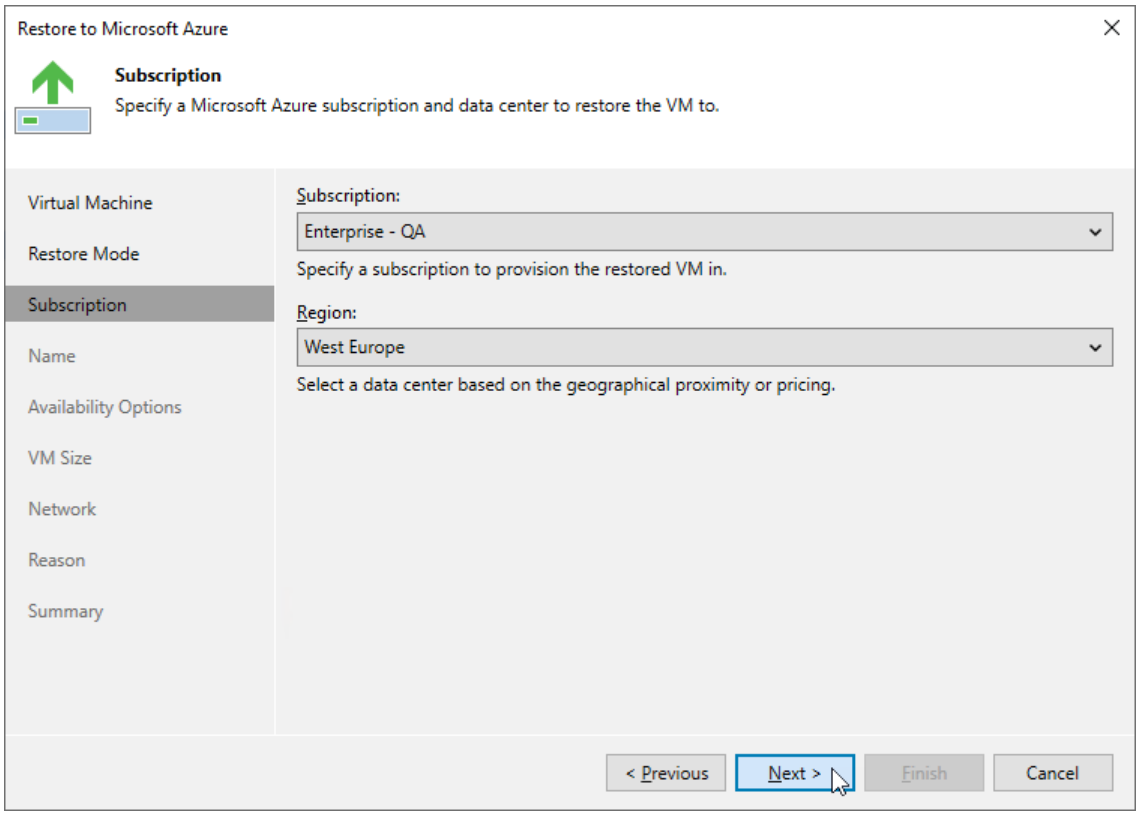
1. From the **Subscription** drop-down list, select an Azure subscription that will be used to manage the restored Azure VM.

   For a subscription to be displayed in the list of available subscriptions, it must be created in Microsoft Azure and associated with the Microsoft Entra tenant to which the service account specified at step 3 of the wizard belongs.

2. From the **Region** drop-down list, select the target region where the restored Azure VM will operate.

   If the selected region differs from the original location of Azure VM, Veeam Backup & Replication will raise a warning notifying that the locations do not match. Click **Yes** to acknowledge the warning. Otherwise, you will not be able to proceed with the wizard.

> **NOTE**
>
> Data transfer to a new location may require additional costs and may take more time to complete.



## Step 5. Specify VM Name and Resource Group

[This step applies only if you have selected the **Restore to a new location, or with different settings** option at the **Restore Mode** step of the wizard]

At the **Name** step of the wizard, specify a new name and a resource group for the restored Azure VM. To do that, select the necessary VM from the list and perform the following steps:

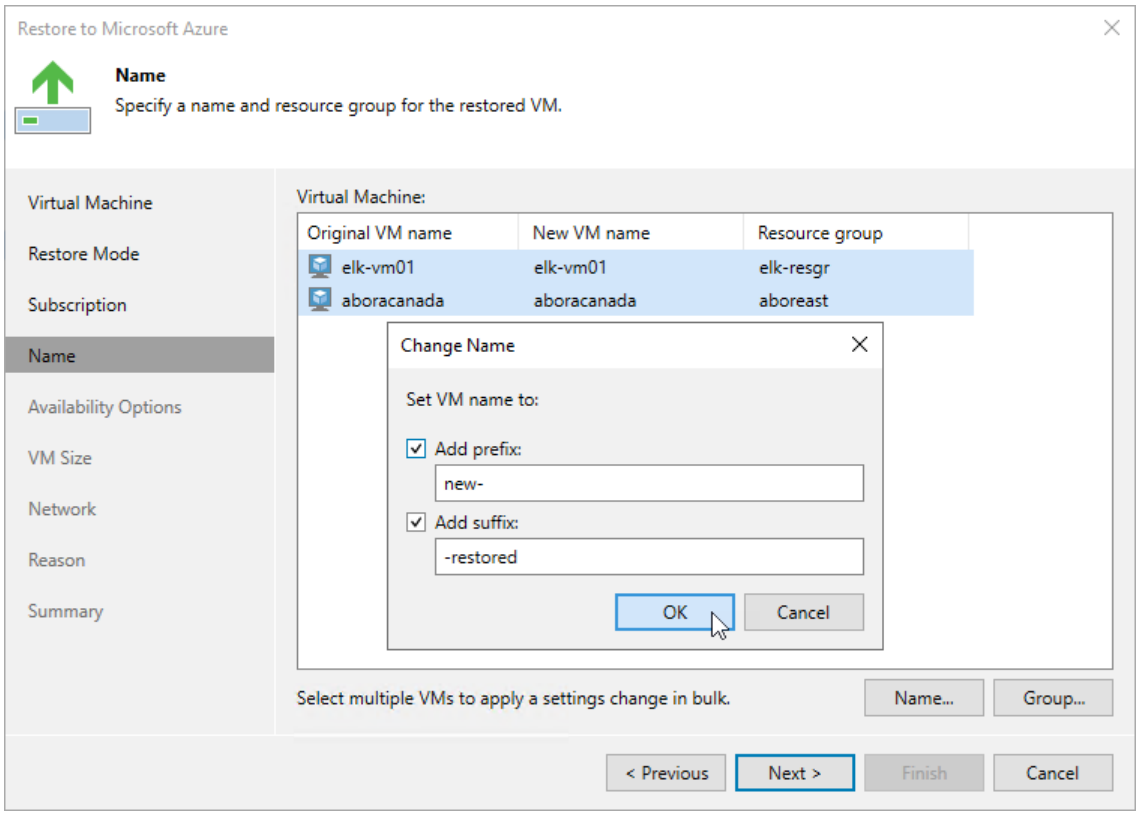
1. Click **Name** and specify a new name for the restored VM in the **Change Name** window. It is recommended that you choose the new name carefully — due to Microsoft Azure limitations, you will not be able to rename the VM after the restore operation completes.

   Note that the name must meet the Microsoft Azure resource name rules.

> **TIP**
>
> You can specify a single prefix or suffix and add it to the names of multiple Azure VMs. To do that, select the necessary instances and click **Name**. In the **Change Name** window, select the **Add prefix** or **Add suffix** check box, and provide the text that you want to add. Then, click **OK**.

2. Click **Group** and select a resource group to which the restored VM will belong in the **Resource group** window.

   For a resource group to be displayed in the list of available groups, it must be created in Microsoft Azure as described in Microsoft Docs.



# Step 6. Specify VM Configuration Settings

[This step applies only if you have selected the **Restore to a new location, or with different settings** option at the **Restore Mode** step of the wizard]

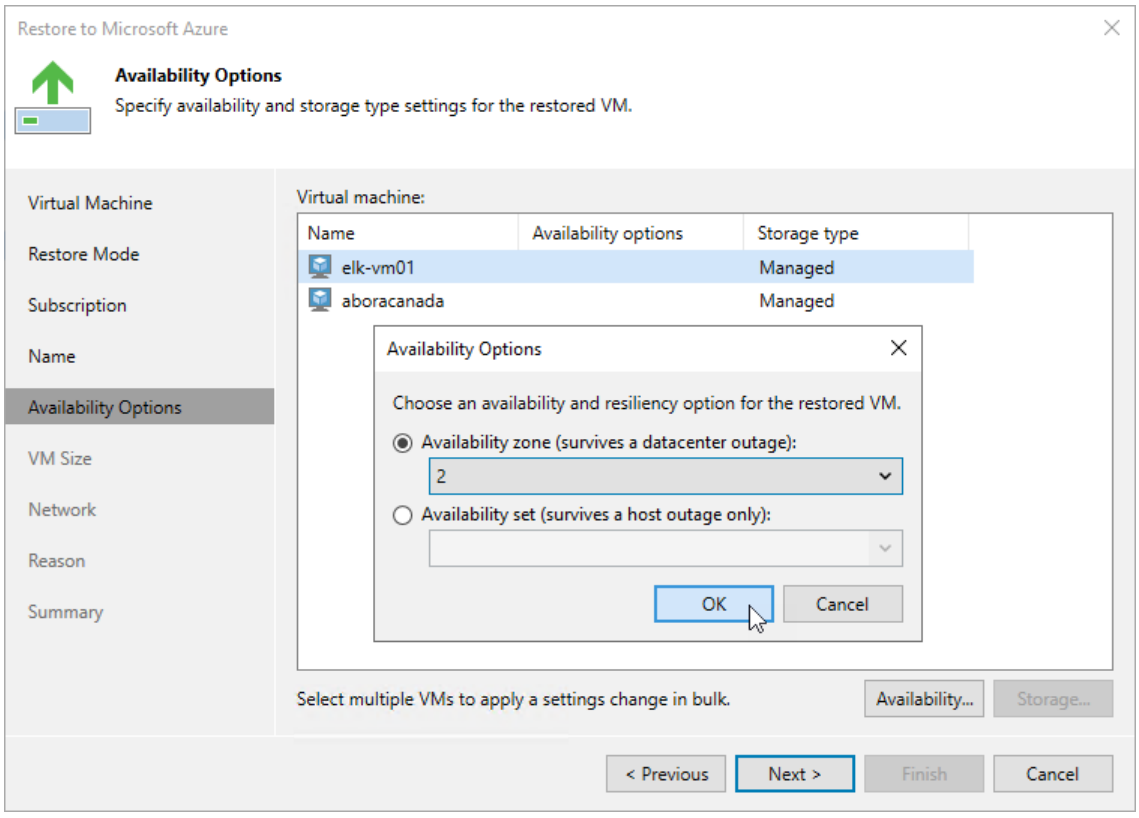
At the **Availability Options** step of the wizard, specify configuration settings for the restored Azure VM. To do that, select the VM and perform the following steps:

1. Click **Availability** and, in the **Availability Options** window, choose whether you want to require any infrastructure redundancy to achieve high availability:
   - Select the **Availability zone** option to restore the VM to a specific availability zone within the selected Azure region, and choose the necessary zone from the drop-down list.
   - Select the **Availability set** option to include the VM in an availability set, and choose the necessary set from the drop-down list. For the availability set to be displayed in the list of available sets, it must be created in Microsoft Azure. For more information on availability sets, see Microsoft Docs.

> **IMPORTANT**
>
> You cannot include Azure VMs with managed disks into unmanaged availability sets, and Azure VMs with unmanaged disks into managed availability sets.

2. [Applies only to Azure VMs with unmanaged disks] Click **Storage** and, in the **Storage type** window, choose whether you want to migrate Azure unmanaged disks to Azure managed disks for the restored VM. For more information on Azure managed disks, see Microsoft Docs.

   If you choose to restore the VM with unmanaged disks, select credentials of a Microsoft Azure storage account in which the restored virtual disks will reside. For credentials to be displayed in the list of available credentials, they must be created in Microsoft Azure as described in Microsoft Docs.



# Step 7. Specify VM Size

[This step applies only if you have selected the **Restore to a new location, or with different settings** option at the **Restore Mode** step of the wizard]

At the **VM size** step of the wizard, you can change the VM size for the restored Azure VM and specify a new name for each restored virtual disk. To do that, select the VM and perform the following steps:

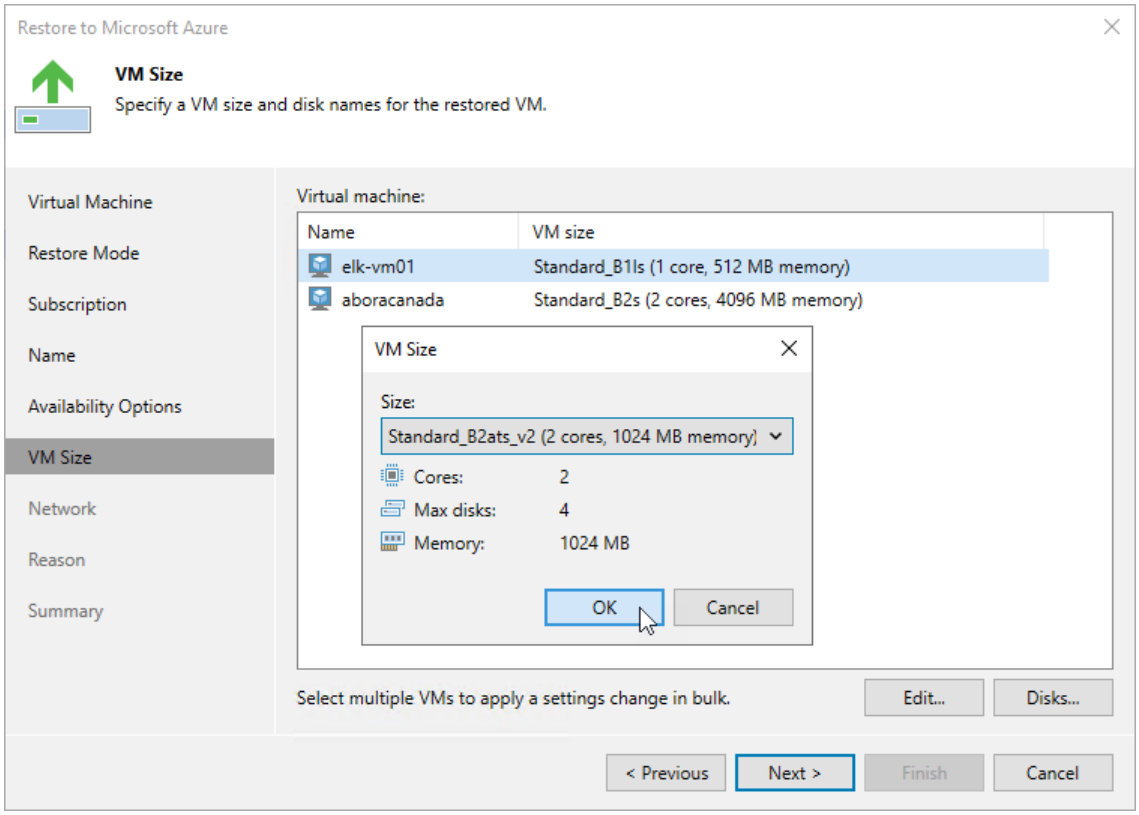
1. Click **Edit**, and select the necessary VM size in the **VM Size** window. For more information on Azure VM sizes, see Microsoft Docs.

> **IMPORTANT**
>
> If the size of the original Azure VM differs from the size of the restored VM, Microsoft Azure may apply additional charges for maintaining the restored Azure VM.

2. Click **Disks**, and select a virtual disk you want to rename in the **VM Disks** window. Then, click **Name**.

   In the **Change Name** window, specify a new name for the selected virtual disk.

> **TIP**
>
> You can specify a single prefix or suffix and add it to the names of multiple restored virtual disks. To do that, select the necessary disks and click **Name**. In the **Change Name** window, select the **Add prefix** or **Add suffix** check box, and provide the text that you want to add. Then, click **OK**.



# Step 8. Configure Network and Security Group Settings

[This step applies only if you have selected the **Restore to a new location, or with different settings** option at the **Restore Mode** step of the wizard]

At the **Network** step of the wizard, you can configure specific network settings for the restored Azure VM. To do that, select the VM and perform the following steps:

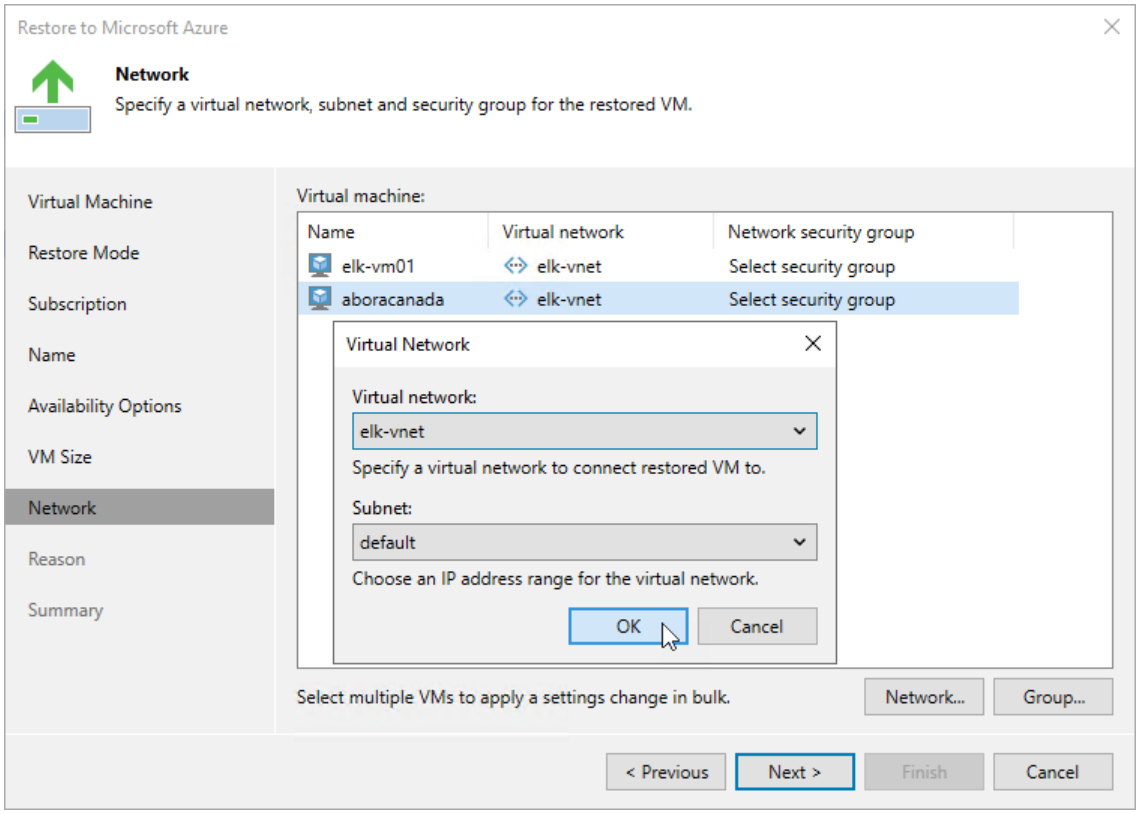
1. Click **Network** and, in the **Virtual Network** window, choose to which virtual network and subnet the restored VM will be connected.

   For a virtual network to be displayed in list of available networks, it must be created for the region specified at step 4 of the wizard in Microsoft Azure, as described in Microsoft Docs.

   For a subnet to be displayed in the list of available networks, it must be created in the specified virtual network as described in Microsoft Docs.

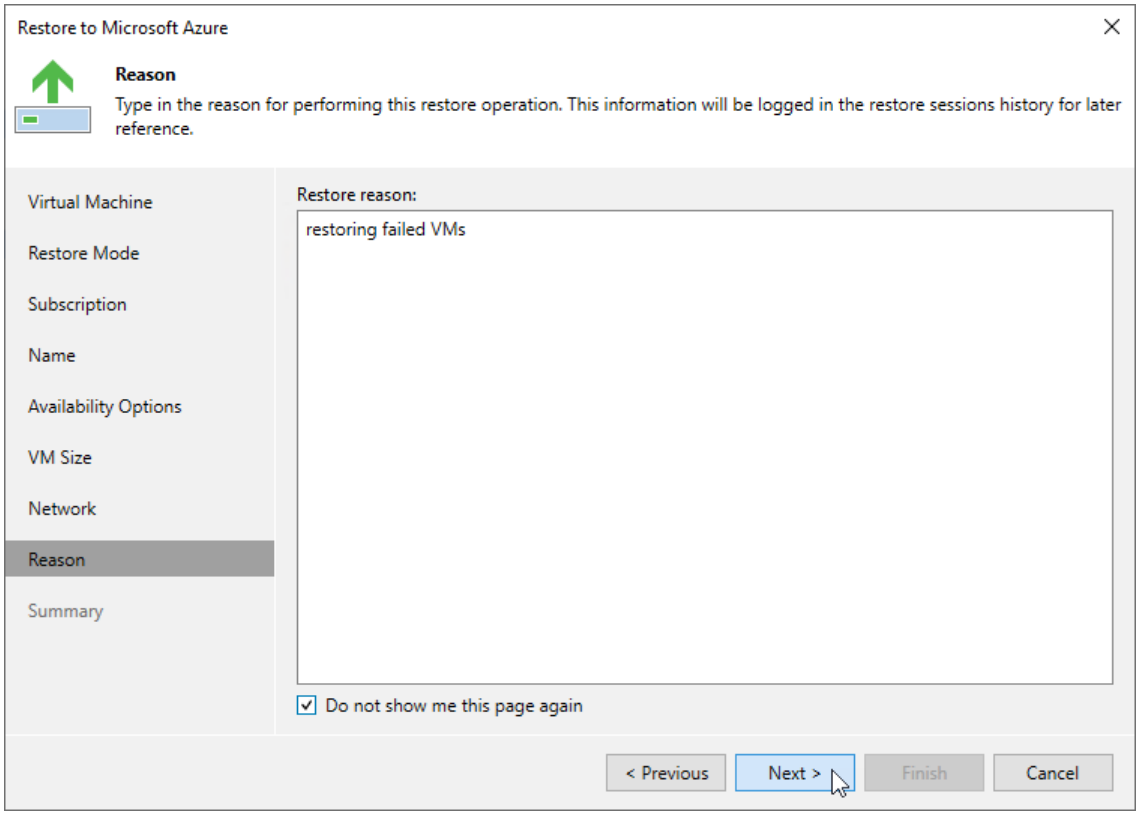
2. Click **Group** and, in the **Network Security Group** window, specify a security group (virtual firewall) that will be associated with the restored VM.

   For a network security group to be displayed in the list of available groups, it must be created in Microsoft Azure and associated with the specified subnet, as described in Microsoft Docs.



# Step 9. Specify Restore Reason

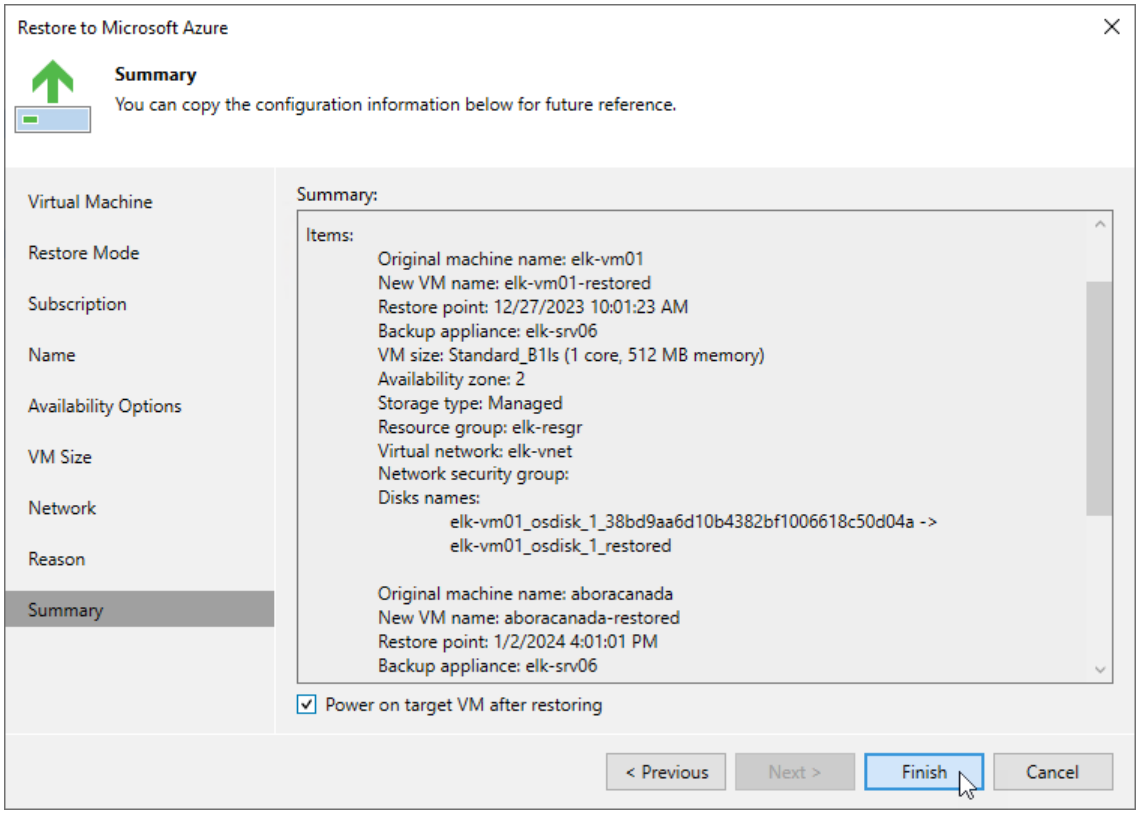
At the **Reason** step of the wizard, specify a reason for restoring the Azure VM. The information you provide will be saved in the session history and you can reference it later.



## Step 10. Finish Working with Wizard

At the **Summary** step of the wizard, review summary information and click **Finish**.

> **TIP**
>
> If you want to start the Azure VM immediately after restore, select the **Power on target VM after restoring** check box.




# Performing Guest OS File Recovery

Veeam Backup & Replication allows you to use image-level backups to restore files and folders of various VM guest OS file systems from the Veeam Backup & Replication console. For more information, see the Veeam Backup & Replication User Guide, section Guest OS File Recovery.

> **IMPORTANT**
>
> Guest OS File Recovery can be performed only using backup files stored in standard repositories for which you have specified credentials of Microsoft Azure storage accounts where the target blob containers reside. To learn how to specify credentials for repositories, see sections Creating New Repositories and Connecting to Existing Appliances.

You can also perform file-level recovery using the Veeam Backup for Microsoft Azure Web UI. For more information, see Performing File-Level Recovery.

# Restoring from Microsoft Windows File Systems (FAT, NTFS or ReFS)

Before you start the restore operation, check the limitations and prerequisites described in the Veeam Backup & Replication User Guide, section Requirements and Limitations.

To restore guest OS files and folders, do the following:

1. In the Veeam Backup & Replication console, open the **Home** view.
2. Navigate to **Backups** > **External Repository**.
3. Expand the backup policy that protects an Azure VM whose files and folders you want to restore, select the necessary VM and click **Guest Files (Windows)** on the ribbon.
4. Complete the **File Level Restore** wizard as described in the Veeam Backup & Replication User Guide, section Restoring VM Guest OS Files (FAT, NTFS or ReFS).

# Restoring Files from Linux, Unix and Other Supported File Systems

> **NOTE**
>
> You can restore files of Linux, Solaris, BSD, Novell Storage Services, Unix and Mac machines. For the list of supported file systems, see the Veeam Backup & Replication User Guide, section Platform Support.

Before you start the restore operation, check the limitations and prerequisites described in the Veeam Backup & Replication User Guide, section Requirements and Limitations.

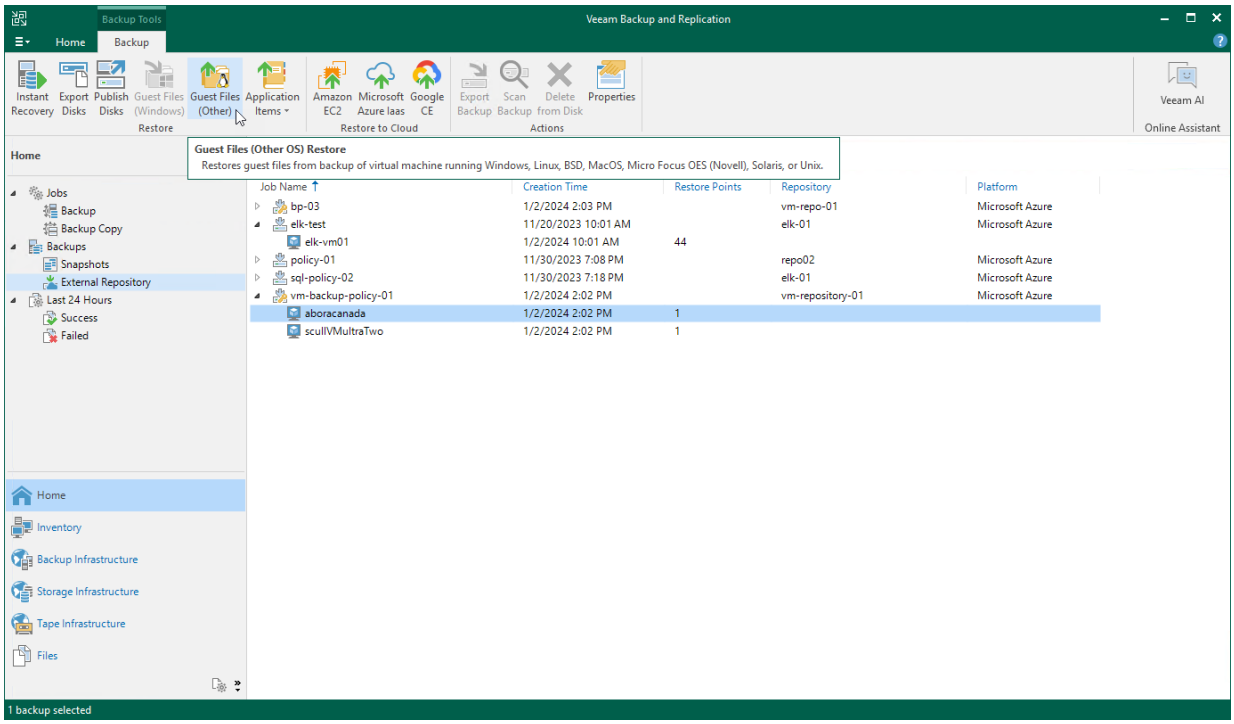
To restore guest OS files and folders, do the following:

1. In the Veeam Backup & Replication console, open the **Home** view.
2. Navigate to **Backups** > **External Repository**.
3. Expand the backup policy that protects an Azure VM whose files and folders your want to restore, select the necessary VM and click **Guest Files (Other)** on the ribbon.
4. Complete the **Guest File Restore** wizard as described in the Veeam Backup & Replication User Guide, section Restoring VM Guest OS Files (Multi-OS).

**TIP**

If the file system whose files and folders you want to restore is not included in the list of supported systems, do either of the following:

- Perform restore to the VMware vSphere environment using the Instant Disk Recovery technology. For more information, see the Veeam Backup & Replication User Guide, section Restore from Other File Systems.
- Perform restore to the Microsoft Hyper-V environment using the Instant Recovery technology. For more information, see the Veeam Backup & Replication User Guide, section Restore from Other File Systems.




# Performing Application Restore

Veeam Backup & Replication provides auxiliary tools — Veeam Explorers — that allow you to restore application items directly from image-level backups of Azure VMs. For more information on Veeam Explorers, see the Veeam Explorers User Guide.

**IMPORTANT**

Application restore can be performed only using backup files stored in standard repositories for which you have specified credentials of Microsoft Azure storage accounts where the target blob containers reside. To learn how to specify credentials for repositories, see sections Creating New Repositories and Connecting to Existing Appliances.

You can restore items of the following applications:

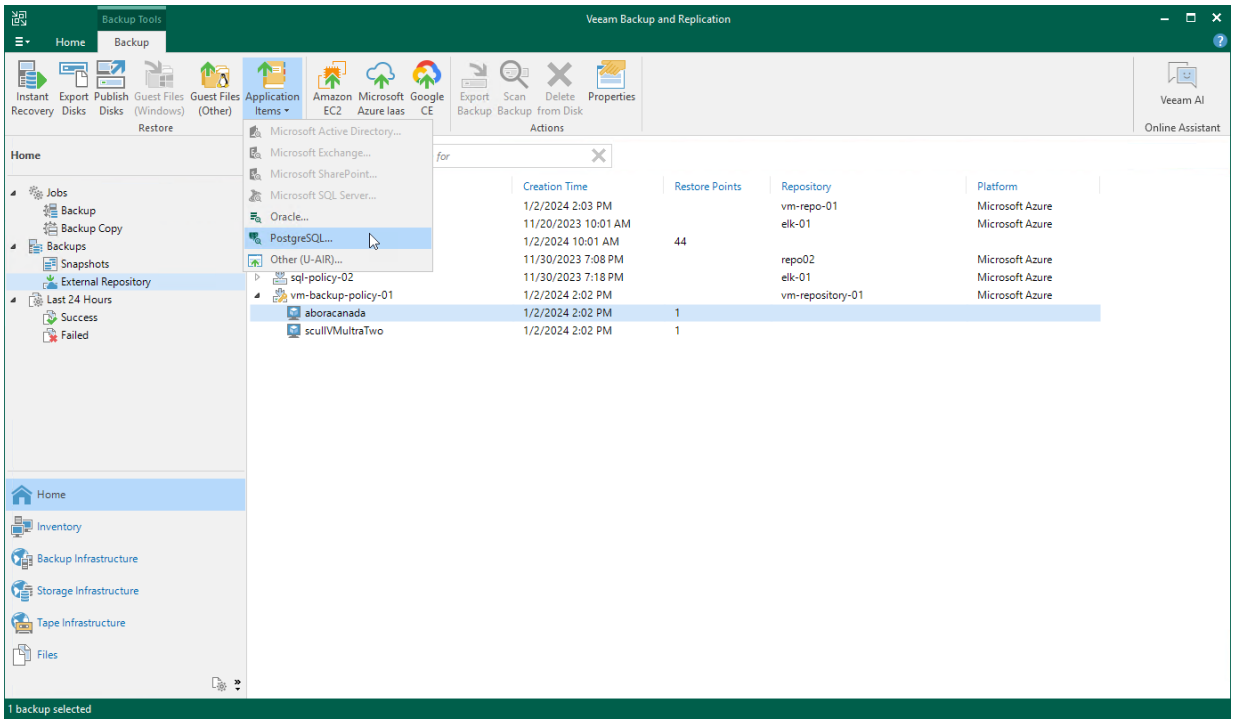
- Microsoft Active Directory
- Microsoft Exchange
- Microsoft SharePoint

- Microsoft SQL Server
- Oracle Database
- PostgreSQL Database

To perform application restore, do the following:

1. In the Veeam Backup & Replication console, open the **Home** view.
2. Navigate to **Backups** > **External Repository**.
3. Expand the backup policy that protects an Azure VM whose application item you want to restore, select the necessary VM and click **Application Items** on the ribbon. Then, select the necessary application.
4. In the restore wizard, select a restore point that will be used to restore the application, specify a restore reason and click **Browse**.
5. In the Veeam Explorer application, perform the steps described in the Veeam Explorers User Guide.

> **IMPORTANT**
>
> The backup from which you want to restore application items must be transactionally consistent. To learn how to create transactionally consistent backups, see section Creating Backup Policies.



# Performing VM Restore Using Web UI

Veeam Backup for Microsoft Azure offers the following restore options:

- VM Restore — restores an entire Azure VM.
- Disk Restore — restores virtual disks attached to an Azure VM.
- File-level Restore — restores individual files and folders of an Azure VM.

You can restore Azure VM data to the most recent state or to any available restore point.

## Performing Entire VM Restore

In case a disaster strikes, you can restore an entire Azure VM from a cloud-native snapshot or image-level backup. Veeam Backup for Microsoft Azure allows you to restore one or more Azure VMs at a time, to the original location or to a new location.

## Before You Begin

To restore an Azure VM from a backup that is stored in an archive repository, you must retrieve the archived data first. You can either retrieve the archived data manually before you begin the restore operation, or launch the data retrieval process right from the restore wizard. To learn how to retrieve data manually, see Retrieving Data From Archive.

## How to Perform VM Restore

To restore an Azure VM, do the following:

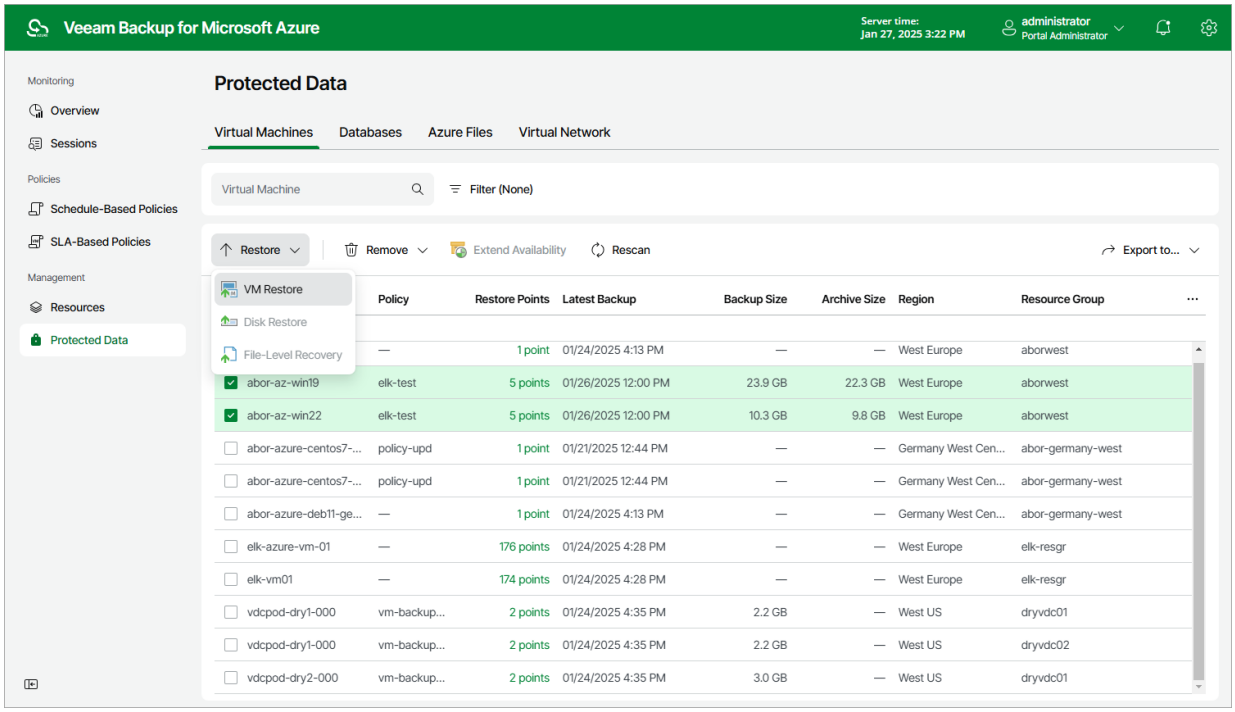
1. Launch the Restore Virtual Machines wizard.
2. Select a restore point.
3. Select a service account.
4. Choose a restore mode.
5. Specify data retrieval settings.
6. Specify Azure VM settings.
7. Specify disk names.
8. Configure network settings.
9. Specify a restore reason.
10. Finish working with the wizard.

# Step 1. Launch Restore Virtual Machines Wizard

To launch the **Restore Virtual Machines** wizard, do the following:

1. Navigate to **Protected Data** > **Virtual Machines**.
2. Select the Azure VM that you want to restore.
3. Click **Restore** > **VM Restore**.

   Alternatively, click the link in the **Restore Points** column. Then, in the **Available Restore Points** window, select the necessary restore point and click **Restore** > **VM Restore**.



# Step 2. Select Restore Point

At the **Virtual Machines** step of the wizard, select a restore point that will be used to restore the selected Azure VM. By default, Veeam Backup for Microsoft Azure uses the most recent valid restore point. However, you can restore the Azure VM data to an earlier state.

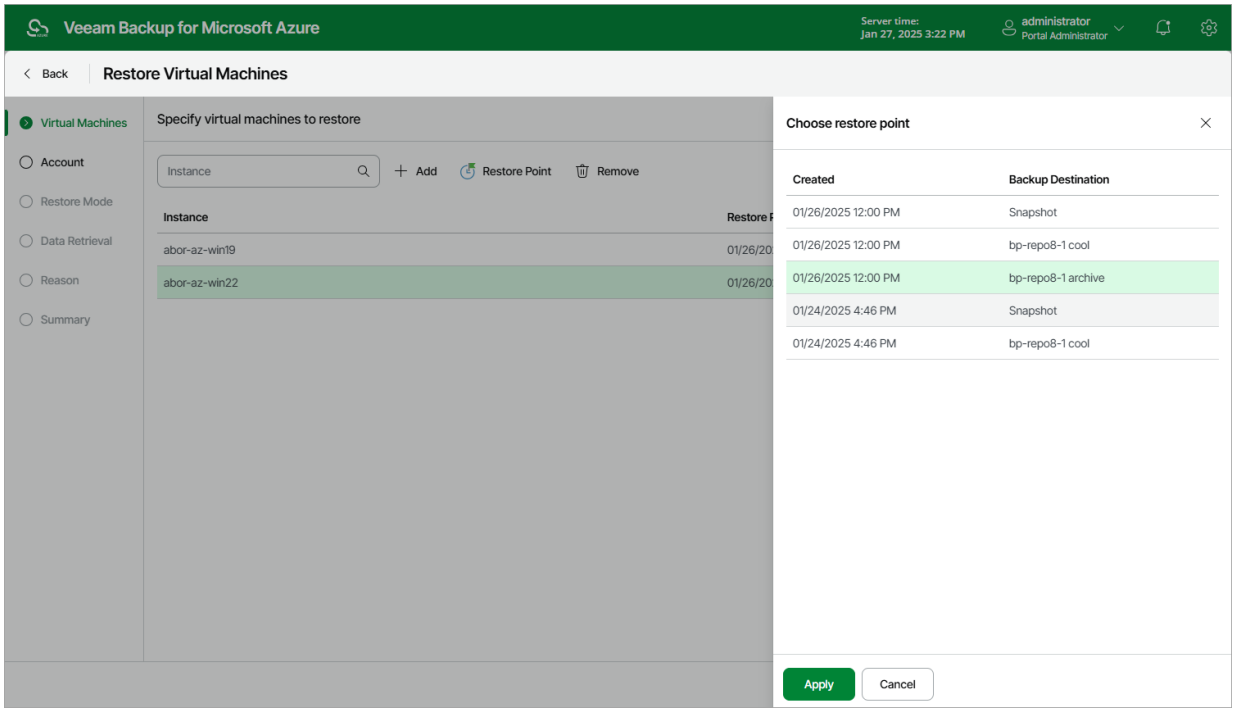
> **IMPORTANT**
>
> If you select a restore point stored in an archive repository and the same restore point is also available in a regular repository, Veeam Backup for Microsoft Azure will display the confirmation window where you must choose whether you want to use the archived or regular restore point to perform the restore operation.

To select a restore point, do the following:

1. Select the Azure VM and click **Restore Point**.
2. In the **Specify restore point** window, select the necessary restore point and click **Apply**.

   To help you choose a restore point, Veeam Backup for Microsoft Azure provides the following information on each available restore point:

   - **Created** — the date when the restore point was created.
   - **Backup Destination** — the type of the restore point:
     - *<Repository Name>* — an image-level backup created by a backup policy.
     - *Snapshot* — a cloud-native snapshot created by a backup policy.
     - *Manual Snapshot* — a cloud-native snapshot created manually.

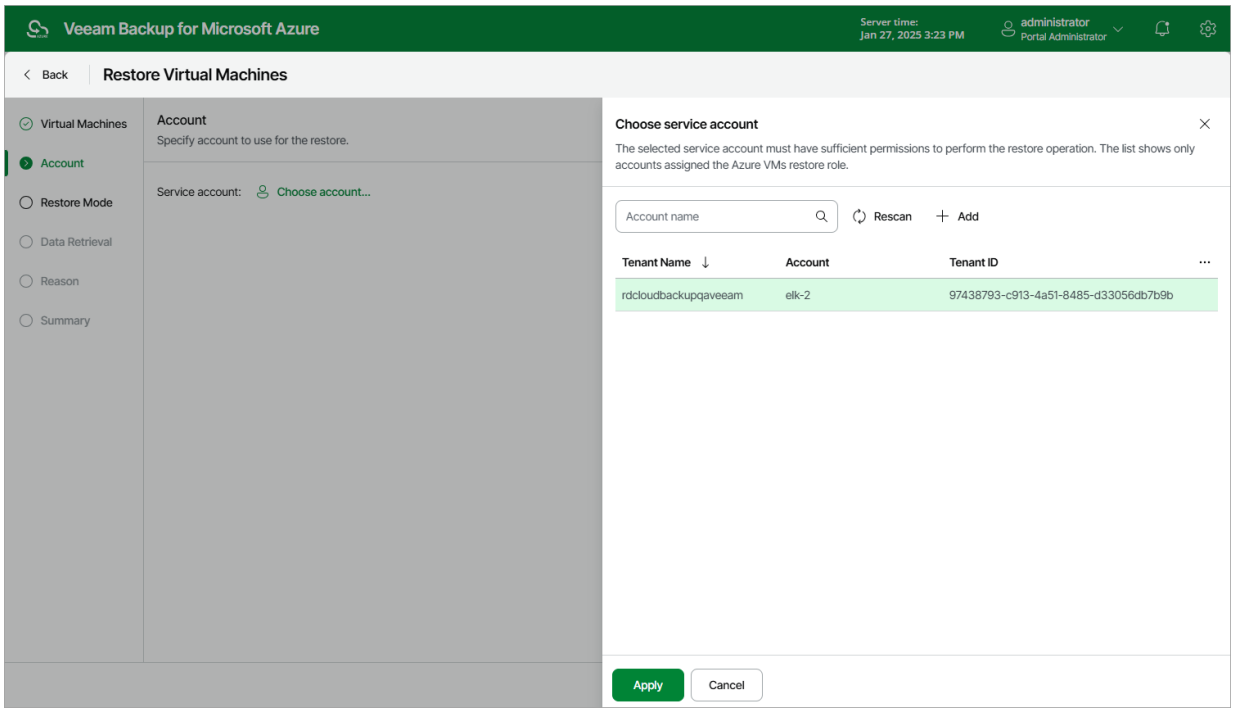


# Step 3. Select Service Account

At the **Account** step of the wizard, select a service account whose permissions Veeam Backup for Microsoft Azure will use to perform the restore operation.

1. Click **Choose account**.
2. In the **Choose service account** window, select the necessary account and click **Apply**. The specified service account must be assigned permissions listed in section Azure VM Permissions.

   For a service account to be displayed in the list of available accounts, it must be added to Veeam Backup for Microsoft Azure and assigned the *Azure VMs Restore* operational role as described in section Adding Service Accounts. If you have not added the necessary service account to Veeam Backup for Microsoft Azure beforehand, you can do it without closing the **Restore Virtual Machines** wizard. To do that, click **Add** and complete the **Add Account** wizard.



# Step 4. Choose Restore Mode

At the **Restore Mode** step of the wizard, choose whether you want to restore the selected Azure VM to the original or to a custom location.

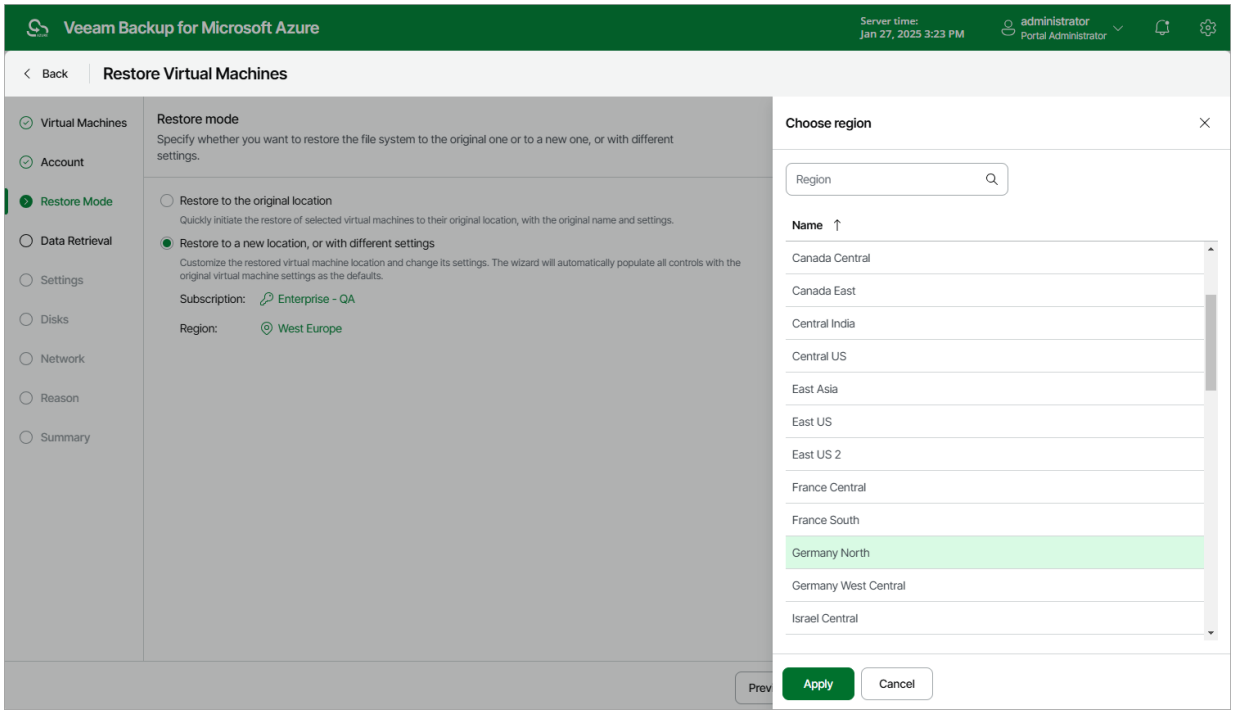
If you select the **Restore to a new location, or with different settings** option, you must also select an Azure subscription and an Azure region in which the restored Azure VM will reside:

1. Click the link in the **Subscription** field. Then, select the necessary subscription in the **Choose subscription** window.

   For a subscription to be displayed in the list of available subscriptions, it must be created in Microsoft Azure and associated with the Microsoft Entra tenant to which the service account specified at step 3 of the wizard belongs.

2. Click the link in the **Region** field. Then, select the necessary Azure region in the **Choose region** window.

> **NOTE**
>
> Data transfer to a new location may require additional costs and may take more time to complete.

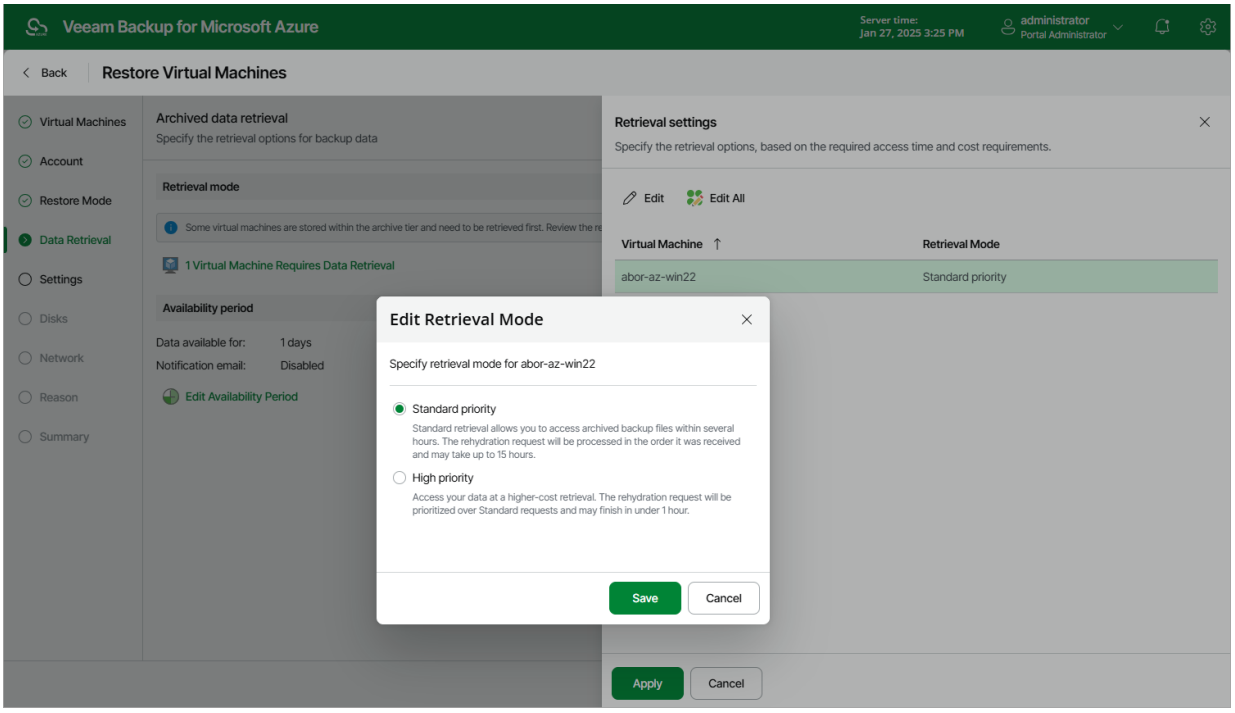


# Step 5. Specify Retrieval Settings

[This step applies only if you have selected a restore point stored in an archive repository at the **Virtual Machines** step of the wizard]

At the **Data retrieval** step of the wizard, choose a retrieval mode and specify a period for which you want to keep the data available.

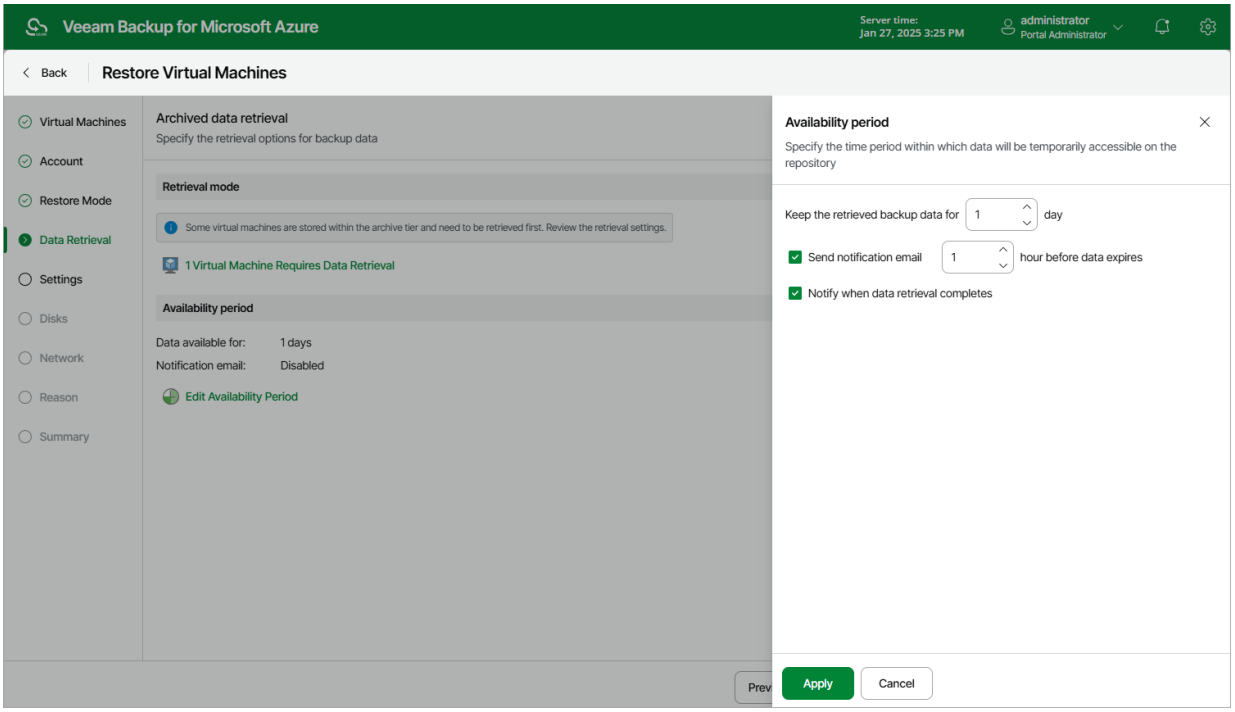
1. Click the link in the **Retrieval mode** section.
   a. In the **Retrieval settings** window, for each processed Azure VM, do the following:
      i. Select an Azure VM and click **Edit**.
      ii. In the **Edit Retrieval Mode** window, select the retrieval mode that Veeam Backup for Microsoft Azure will use to retrieve the archived data, and click **Save**. For more information on data retrieval modes, see Retrieving Data From Archive.
   b. To save changes made to the data retrieval settings, click **Apply**.




2. Click **Edit Availability Period** in the **Availability period** section.
   a. In the **Availability period** window, specify the number of days for which you want to keep the data available for restore operations. You can manually extend the availability period later if required.

> **TIP**
>
> If you want to receive an email notification when data availability period is about to expire, select the **Send notification email** check box and choose when you want to be notified (that is, the number of hours remaining until data expiration).

b. To save changes made to the availability period settings, click **Apply**.



## Step 6. Specify Instance Settings

[This step applies only if you have selected the **Restore to a new location, or different settings** option at the **Restore Mode** step of the wizard]

At the **Settings** step of the wizard, do the following:

1. Select an Azure VM.
2. If you want to specify a name for the restored Azure VM, click **Rename.**

   In the **Virtual machine name** window, specify a new name and click **Apply**.
3. If you want to change the Azure VM settings, click **Edit**.

   In the **Virtual machine settings** window, do the following:

   a. From the **Virtual machine size** drop-down list, select a VM size for the restored Azure VM. For more information on VM sizes, see Microsoft Docs.

> **IMPORTANT**
>
> If the VM size of the original Azure VM differs from the size of the restored VM, Microsoft Azure may apply additional charges for maintaining the restored VM.

   b. From the **Resource group** drop-down list, select a resource group to which the restored Azure VM will belong.

      For a resource group to be displayed in the **Resource group** list, it must be created in the Microsoft Azure portal as described in Microsoft Docs.

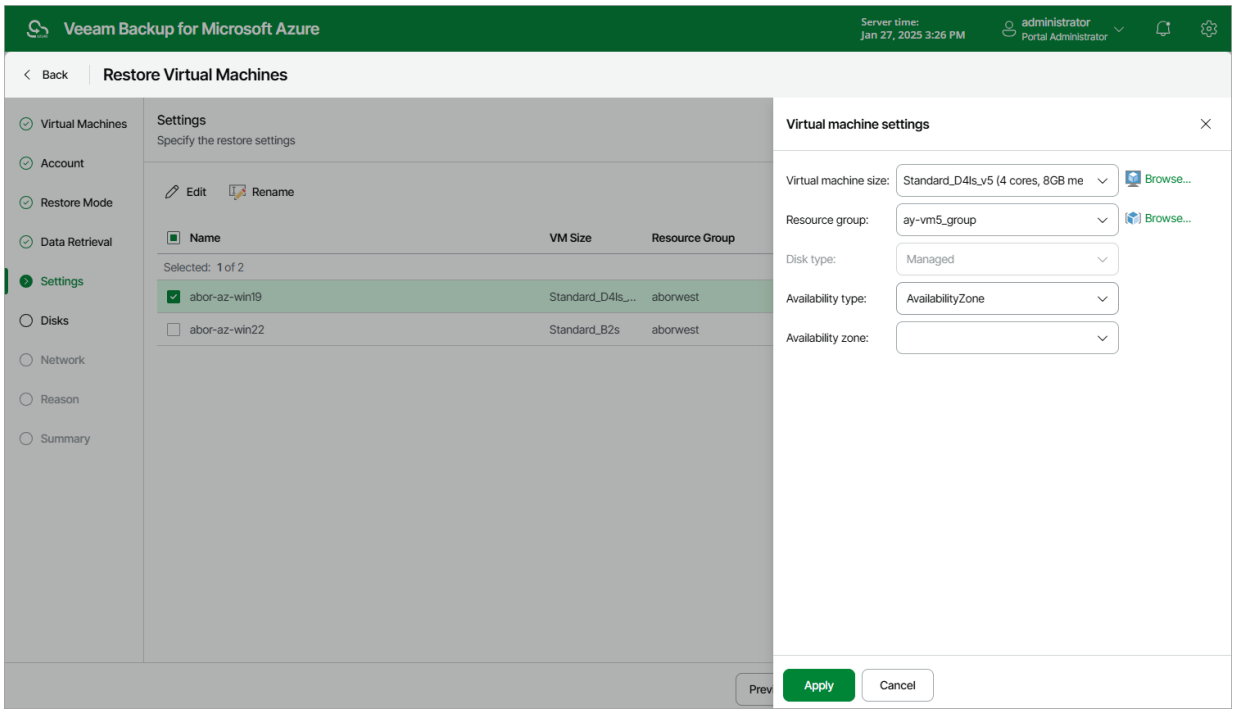
   c. From the **Disk type** drop-down list, select a type of virtual disks that will be attached to the restored Azure VM. For more information on disk types, see Microsoft Docs.

   d. Use the **Availability type** drop-down list to choose whether you want to include the restored Azure VM in an availability set or to place the VM in an availability zone.

      Availability sets allow you to distribute VMs across multiple physical hardware resources. Availability zones allow you to distribute VMs across multiple unique physical locations and to protect your data from datacenter failures. For more information on availability options for virtual machines in Azure, see Microsoft Docs.

   e. To save changes made to the Azure VM settings, click **Apply**.

> **NOTE**
>
> On September 30, 2025, unmanaged disks will be retired in Microsoft Azure. That is why it is recommended that you use managed disks when restoring Azure VMs. For more information, see Microsoft Docs.

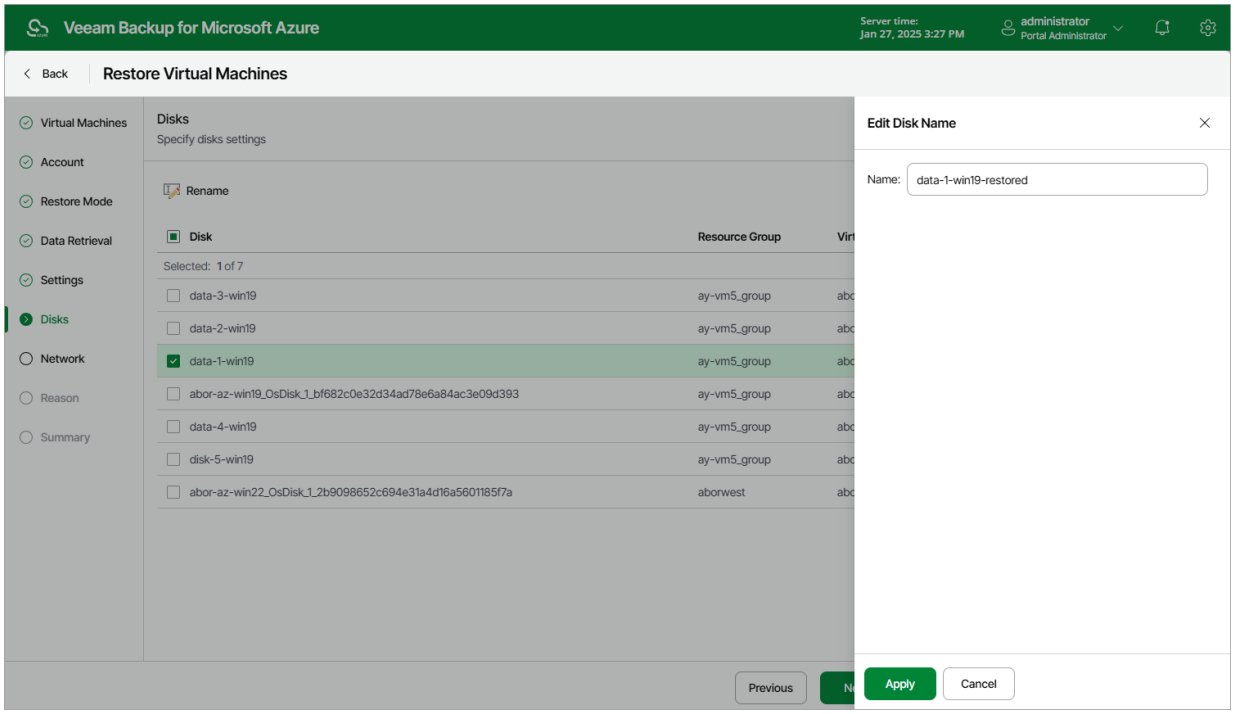

Veeam Backup for Microsoft Azure
Server time:
Jan 27, 2025 3:26 PM
administrator
Portal Administrator
Back
Restore Virtual Machines
Virtual Machines
Account
Restore Mode
Data Retrieval
Settings
Disks
Network
Reason
Summary
Settings
Specify the restore settings
Edit
Rename
Name
VM Size
Resource Group
Selected: 1 of 2
abor-az-win19
Standard_D4ls_...
aborwest
abor-az-win22
Standard_B2s
aborwest
Prev
Virtual machine settings
Virtual machine size:
Standard_D4ls_v5 (4 cores, 8GB me
Browse...
Resource group:
ay-vm5_group
Browse...
Disk type:
Managed
Availability type:
AvailabilityZone
Availability zone:
Apply
Cancel

# Step 7. Specify Disk Names

[This step applies only if you have selected the **Restore to a new location, or different settings** option at the **Restore Mode** step of the wizard]

At the **Disks** step of the wizard, you can specify a new name for each restored virtual disk:

1. Select a virtual disk that you want to rename, and click **Rename**.
2. In the **Edit Disk Name** window, specify a name that you want to use for the selected virtual disk, and click **Apply**.



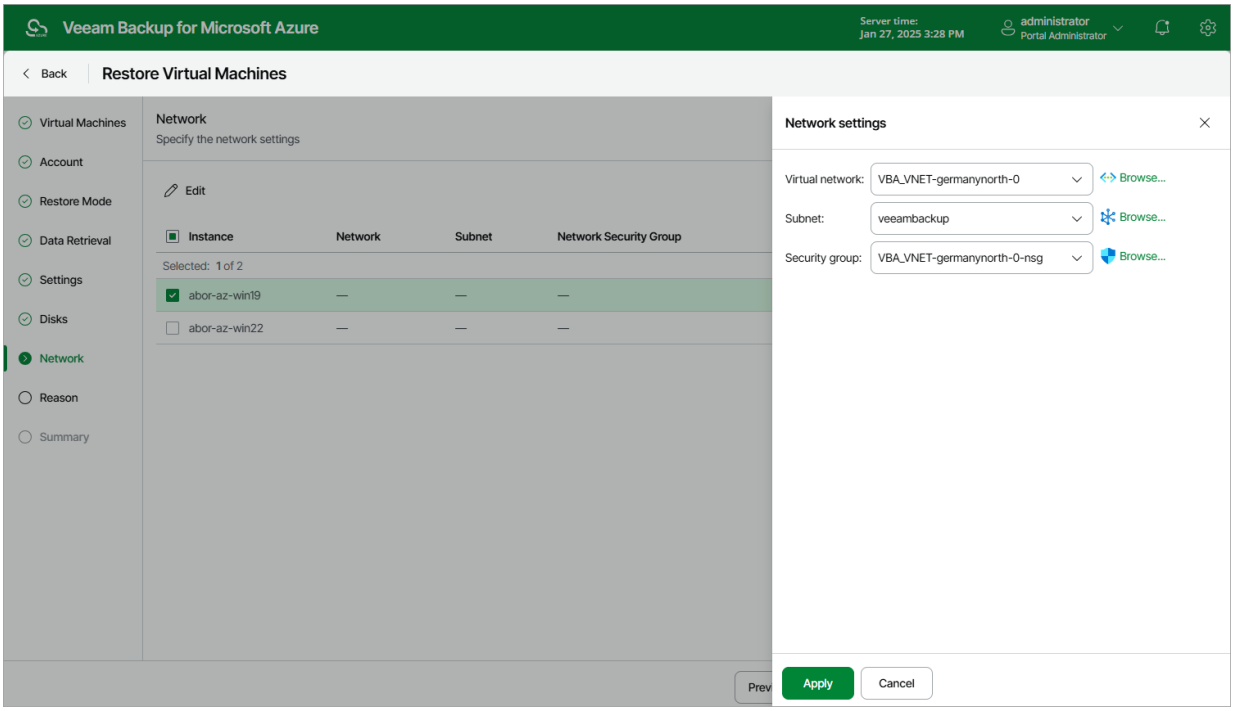
# Step 8. Configure Network Settings

[This step applies only if you have selected the **Restore to a new location, or different settings** option at the **Restore Mode** step of the wizard]

At the **Network** step of the wizard, do the following:

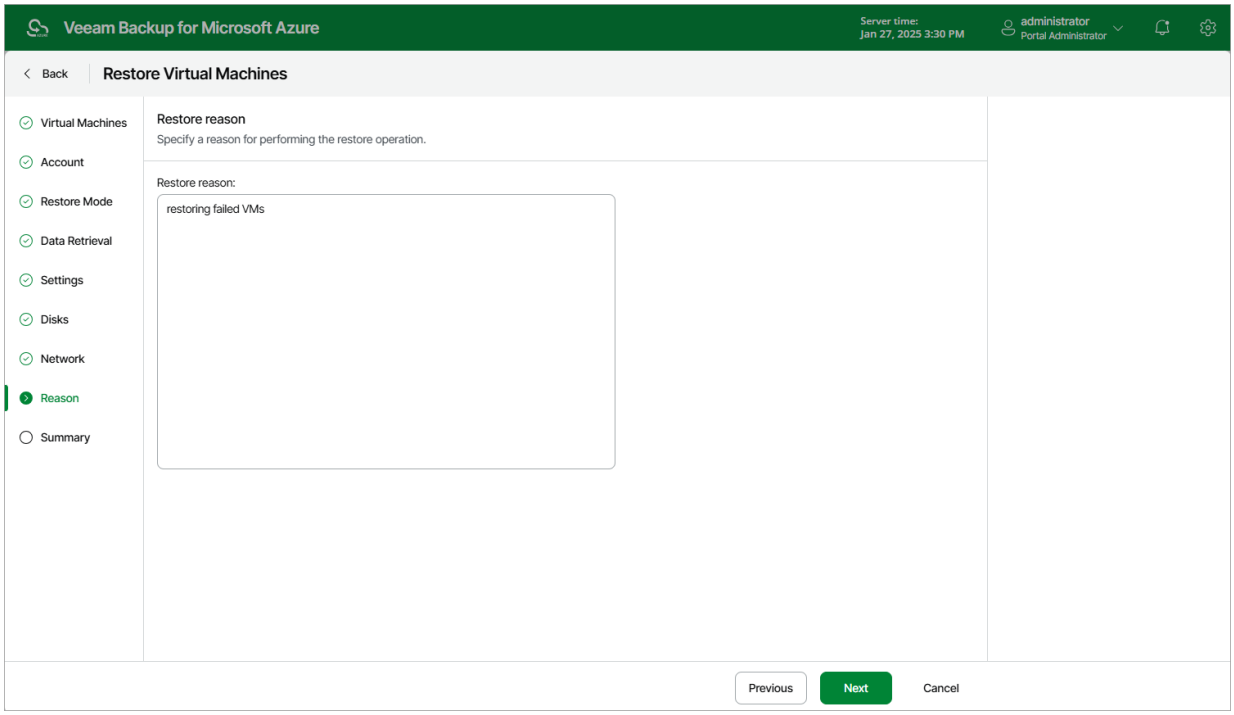
1. Select the Azure VM.
2. Click **Edit**.
3. In the **Network settings** window, select a virtual network and a subnet to which you want to connect the restored Azure VM. For a virtual network to be displayed in the **Virtual network** list, it must be created in the Microsoft Azure portal as described in Microsoft Docs. For a subnet to be displayed in the **Subnet** list, it must be created within the selected virtual network as described in Microsoft Docs.

   You can also specify a security group (virtual firewall) that will be associated with the restored VM. Security groups are used to filter network inbound traffic to and outbound traffic from Azure resources. Each security group contains a set of rules that control the traffic. For a network security group to be displayed in the **Security group** list, it must be created in the Microsoft Azure portal as described in Microsoft Docs.



# Step 9. Specify Restore Reason

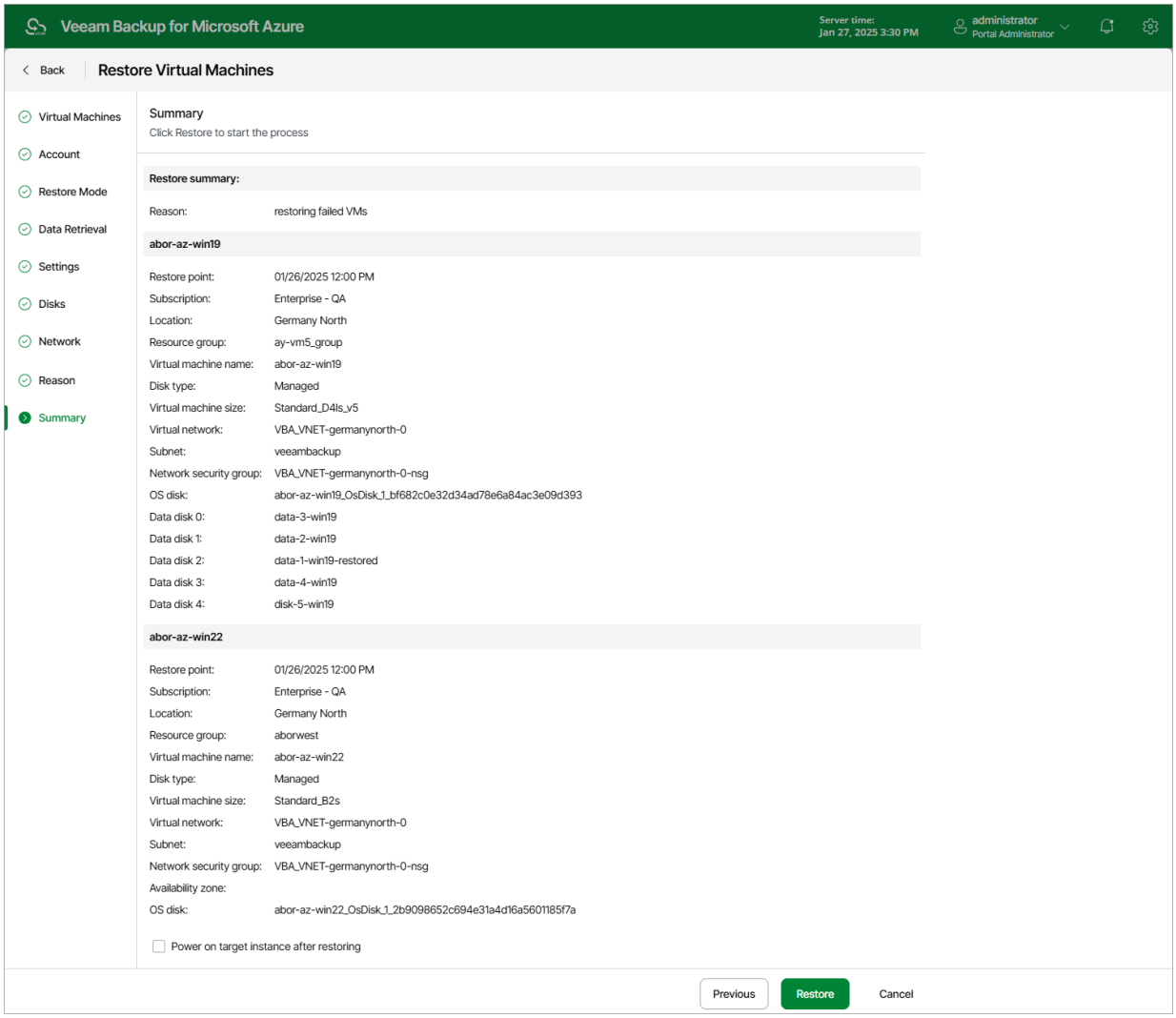
At the **Reason** step of the wizard, specify a reason for restoring the Azure VM. This information will be saved to the session history, and you will be able to reference it later.



## Step 10. Finish Working with Wizard

At the **Summary** step of the wizard, review summary information and click **Restore**.

> **TIP**
>
> If you want to start the restored Azure VM as soon as the restore process completes, select the **Power on target instance after restoring** check box.




# Performing Disk Restore

In case a disaster strikes, you can restore corrupted virtual disks of an Azure VM from a cloud-native snapshot or image-level backup. Veeam Backup for Microsoft Azure allows you to restore virtual disks to the original location or to a new location.

# Before You Begin

To restore a virtual disk from a backup that is stored in an archive repository, you must retrieve the archived data first. You can either retrieve the archived data manually before you begin the restore operation, or launch the data retrieval process right from the restore wizard. To learn how to retrieve data manually, see Retrieving Data From Archive.

# How to Perform Disk Restore

To restore virtual disks attached to a protected Azure VMs, do the following:

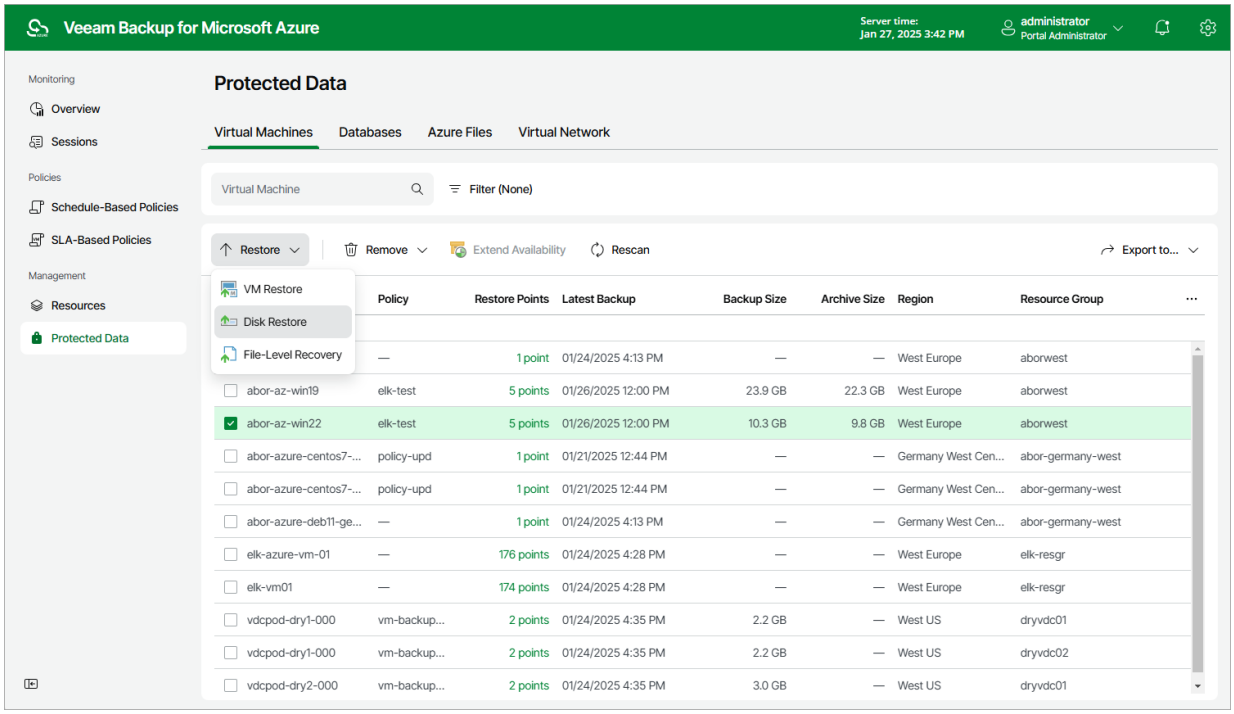
1. Launch the Restore Disks wizard.
2. Select a restore point.
3. Select a service account.
4. Choose a restore mode.
5. Specify data retrieval settings.
6. Specify disk settings.
7. Specify a restore reason.
8. Finish working with the wizard.

# Step 1. Launch Restore Disks Wizard

To launch the **Restore Disks** wizard, do the following:

1. Navigate to **Protected Data** > **Virtual Machines**.
2. Select the Azure VM whose virtual disks you want to restore.
3. Click **Restore** > **Disk Restore**.

   You can also click the link in the **Restore Points** column. Then, in the **Restore Points** window, select the necessary restore point and click **Restore** > **Disk Restore**.



## Step 2. Select Restore Point

At the **Restore Point** step of the wizard, select a restore point that will be used to restore virtual disks of the selected Azure VM. By default, Veeam Backup for Microsoft Azure uses the most recent valid restore point. However, you can restore the disks to an earlier state.

> **IMPORTANT**
>
> If you select a restore point stored in an archive repository and the same restore point is also available in a regular repository, Veeam Backup for Microsoft Azure will display the confirmation window where you must choose whether you want to use the archived or regular restore point to perform the restore operation.

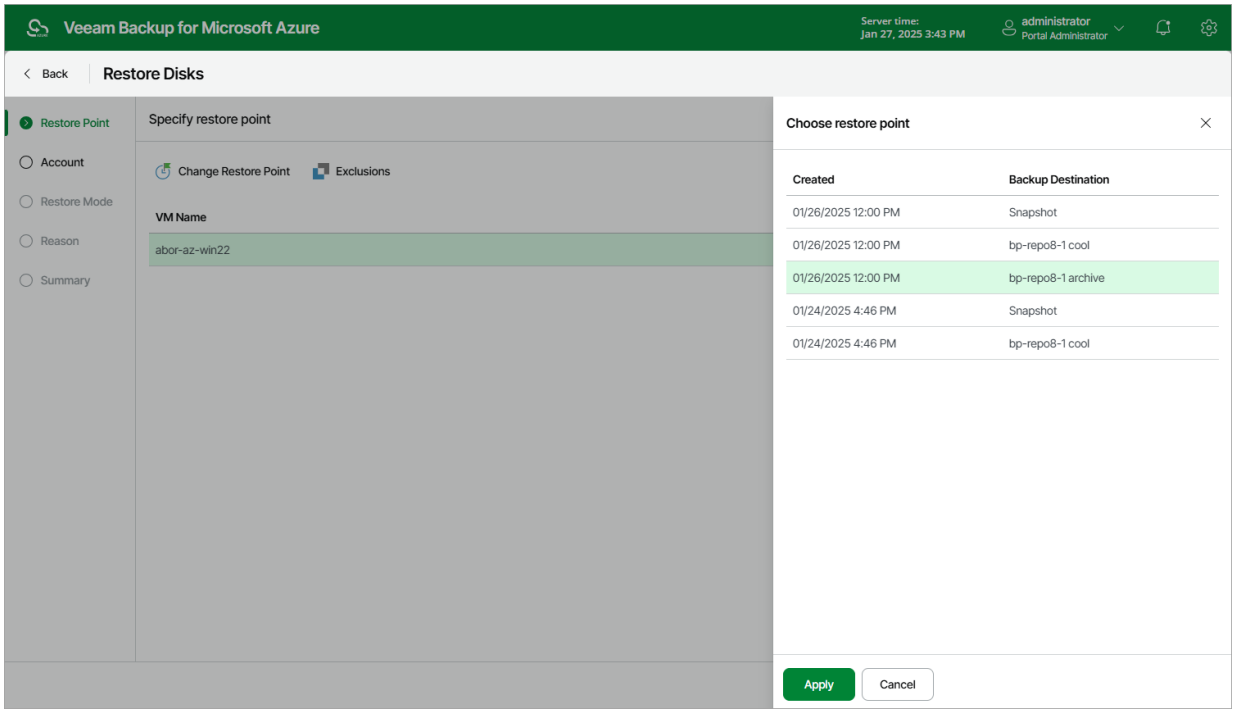
To select a restore point, do the following:

1. Select the Azure VM.
2. Click **Change Restore Point**.
3. In the **Specify restore point** window, select the necessary restore point and click **Apply**.

   To help you choose a restore point, Veeam Backup for Microsoft Azure provides the following information on each available restore point:

   - **Created** — the date when the restore point was created.
   - **Backup Destination** — the type of the restore point:
     - *<Repository Name>* — an image-level backup created by a backup policy.
     - *Snapshot* — a cloud-native snapshot created by a backup policy.
     - *Manual Snapshot* — a cloud-native snapshot created manually.

> **TIP**
>
> If you want to restore only specific virtual disks of the selected Azure VM, you can exclude the unnecessary disks from the restore process. To do that, click **Exclusions** to open the **Select exclusions** window, select check boxes next to the disks that you do not want to restore, and click **Apply**.

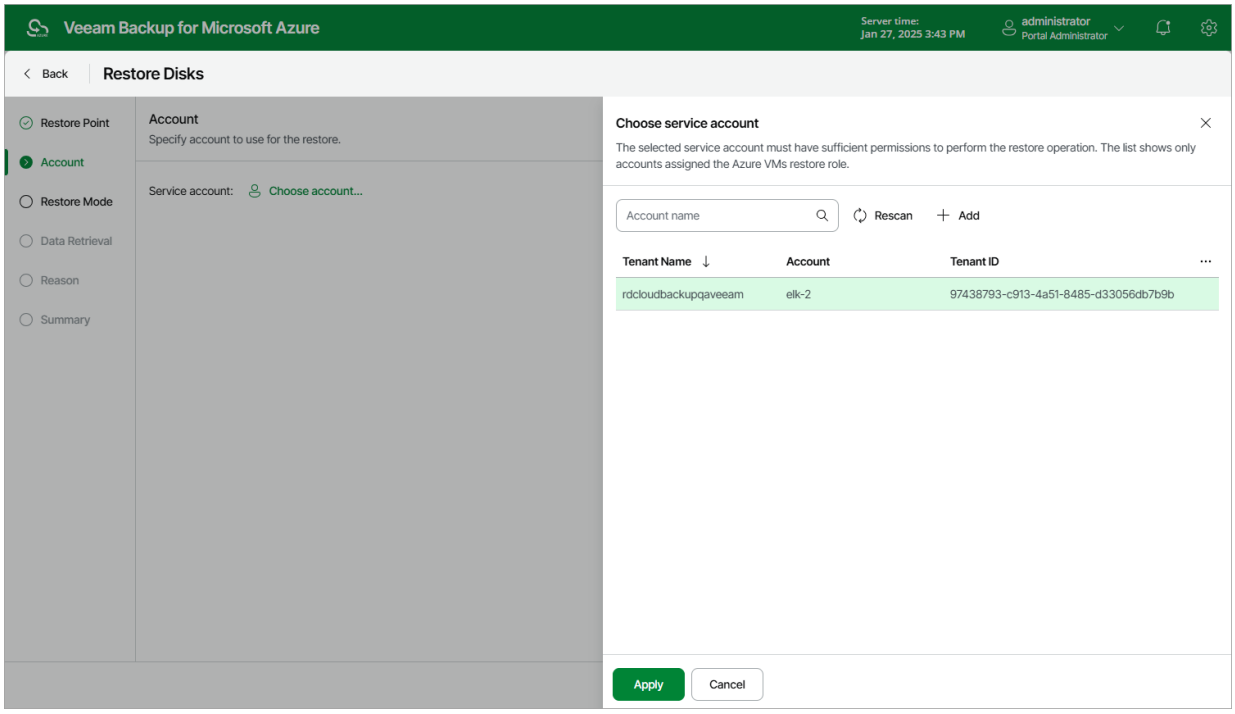


# Step 3. Select Service Account

At the **Account** step of the wizard, select a service account whose permissions Veeam Backup for Microsoft Azure will use to perform the restore operation.

1. Click **Select account**.
2. In the **Choose account** window, select the necessary account and click **Apply**. The specified service account must be assigned permissions listed in section Azure VM Permissions.

   For a service account to be displayed in the list of available accounts, it must be added to Veeam Backup for Microsoft Azure and assigned the Azure VMs Restore operational role as described in section Adding Service Accounts. If you have not added the necessary service account to Veeam Backup for Microsoft Azure beforehand, you can do it without closing the **Restore Disks** wizard. To do that, click **Add** and complete the **Add Account** wizard.



# Step 4. Choose Restore Mode

At the **Restore Mode** step of the wizard, choose whether you want to restore the selected virtual disks to the original or to a custom location.

If you select the **Restore to a new location, or with different settings** option, you must also select an Azure subscription and an Azure region in which the restored virtual disks will reside:

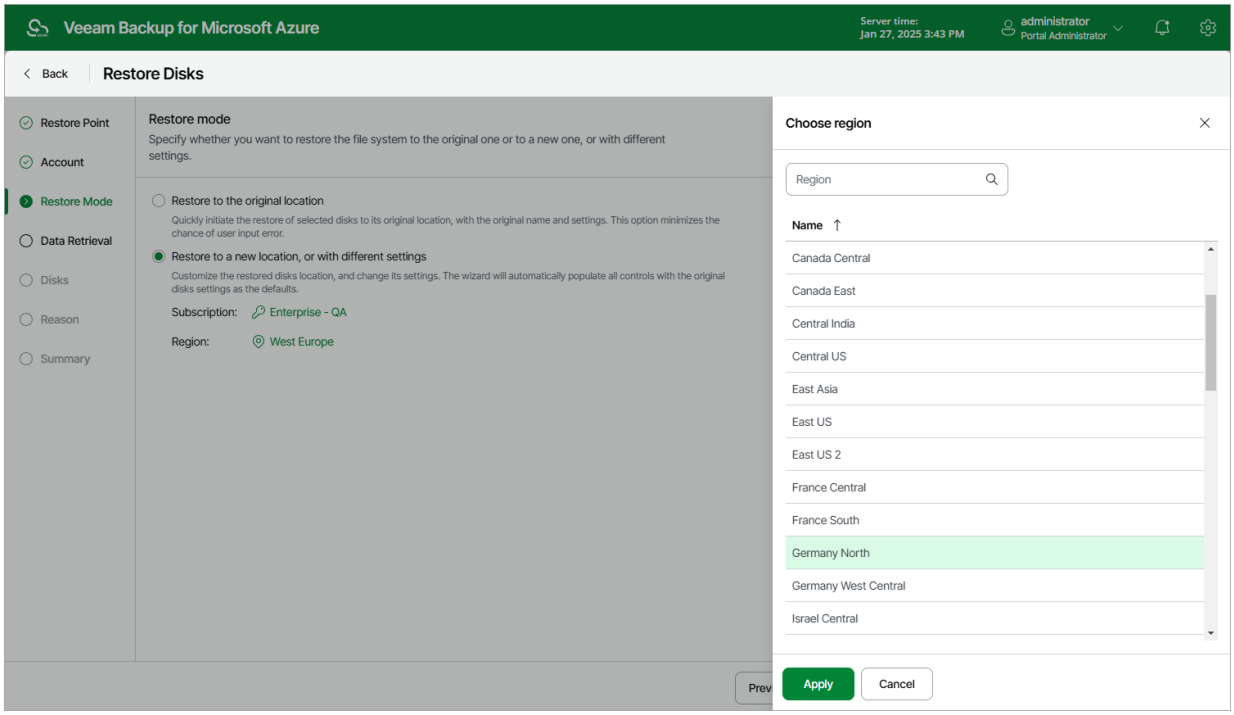
1. Click the link in the **Subscription** field. Then, select the necessary subscription in the **Choose subscription** window.

   For a subscription to be displayed in the list of available subscriptions, it must be created in Microsoft Azure and associated with the Microsoft Entra tenant to which the service account specified at step 3 of the wizard belongs.

2. Click the link in the **Region** field. Then, select the necessary Azure region in the **Choose region** window.

NOTES

- If you choose to restore the disks to the original location, keep in mind that Veeam Backup for Microsoft Azure will restore the disks to the Azure resource group to which the related Azure VM belongs, even if these disks originally belonged to another resource group.
- Data transfer to a new location may require additional costs and may take more time to complete.



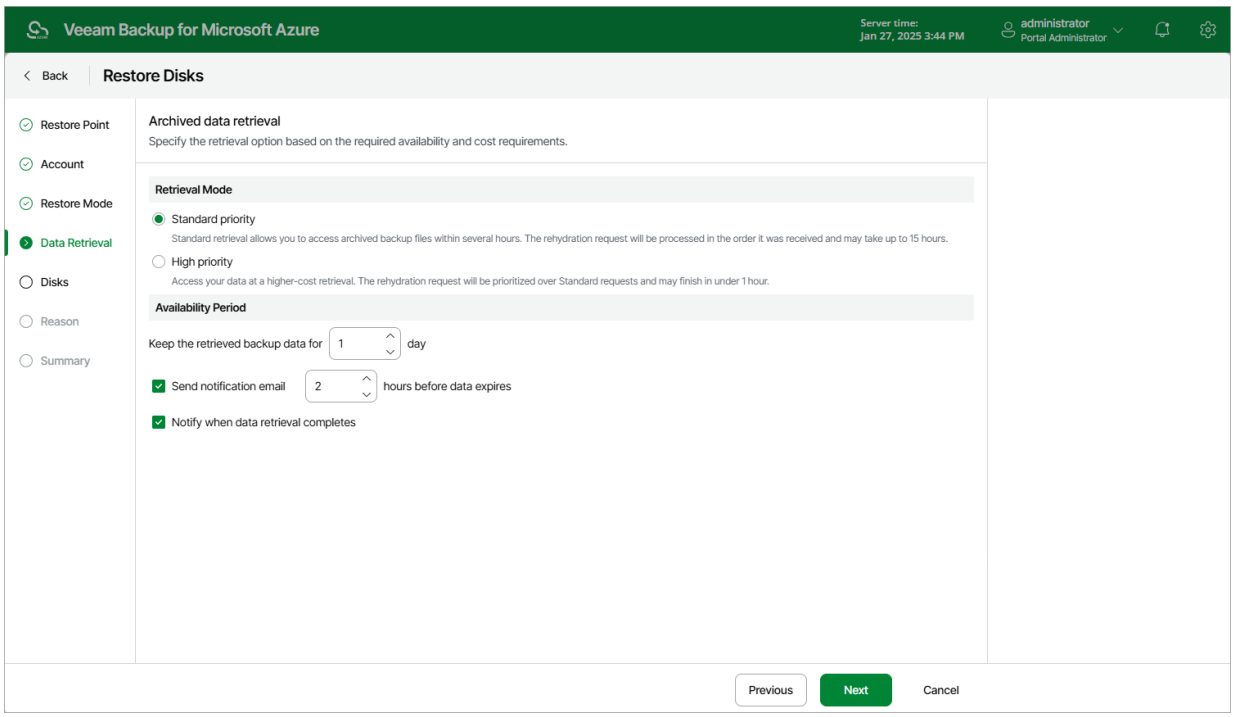
# Step 5. Specify Retrieval Settings

[This step applies only if you have selected a restore point stored in an archive repository at the **Restore Point** step of the wizard]

At the **Data retrieval** step of the wizard, choose a retrieval mode and specify a period for which you want to keep the data available.

1. In the **Retrieval Mode** section, select the retrieval mode that Veeam Backup for Microsoft Azure will use to retrieve the archived data. For more information on data retrieval modes, see Retrieving Data From Archive.
2. In the **Availability Period** section, specify the number of days for which you want to keep the data available for restore operations. You can manually extend the availability period later if required.

> **TIP**
>
> If you want to receive an email notification when data availability period is about to expire, select the **Send notification email** check box and choose when you want to be notified (that is, the number of hours remaining until data expiration).



## Step 6. Specify Disk Settings

[This step applies only if you have selected the **Restore to a new location, or different settings** option at the **Restore Mode** step of the wizard]

At the **Disks** step of the wizard, you can configure disk properties for each restored virtual disk:

1. Select the necessary disk.
2. Click **Edit**.
3. In the **Disk properties** window, do the following:
   a. In the **Disk name** field, specify a new name for the restored virtual disk.
   b. From the **Resource group** drop-down list, select a resource group to which the restored virtual disk will belong.

      For a resource group to be displayed in the list of available resource groups, it must be created in the Microsoft Azure portal as described in Microsoft Docs.

   b. From the **Disk type** drop-down list, select a type for the restored virtual disk. For more information on disk types, see Microsoft Docs.

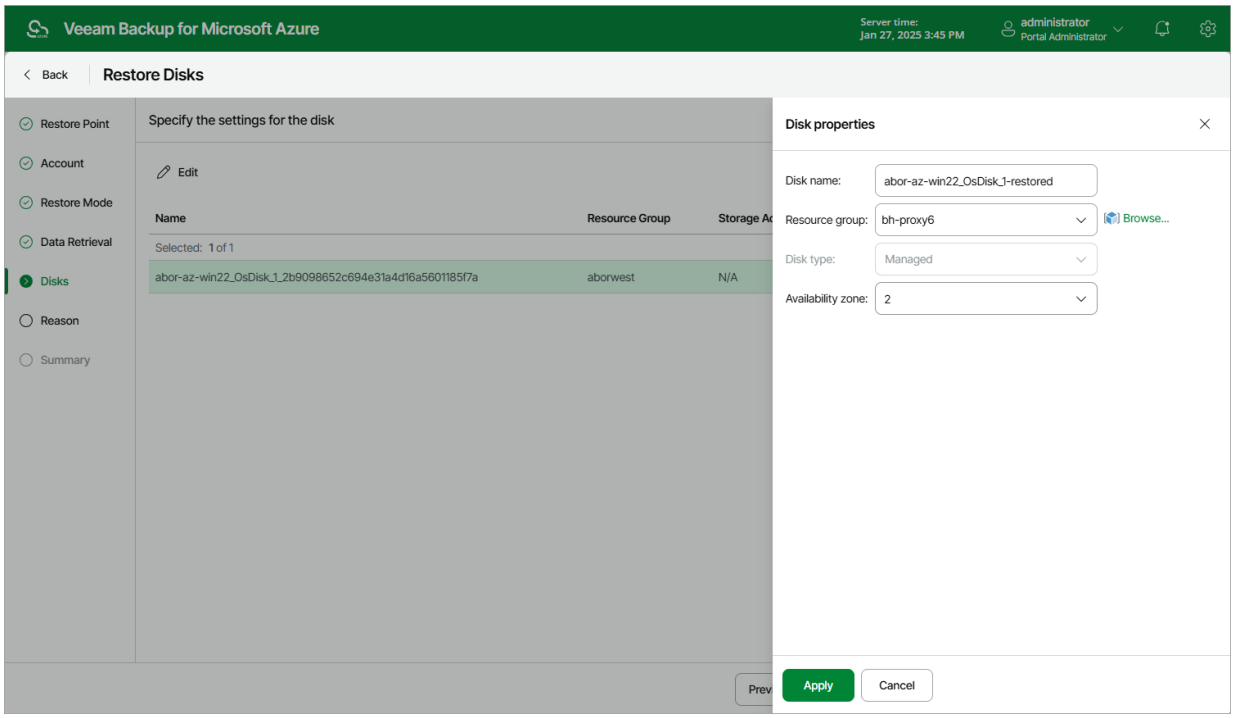
> **NOTE**
>
> You cannot convert managed virtual disks into unmanaged, but you can convert unmanaged virtual disks into managed.

   c. [Applies only to unmanaged disks] From the **Storage account** drop-down list, select an Azure storage account to which you want to restore the selected virtual disk.

      For a storage account to be displayed in the **Storage account** list, it must be created in the Microsoft Azure portal as described in Microsoft Docs.

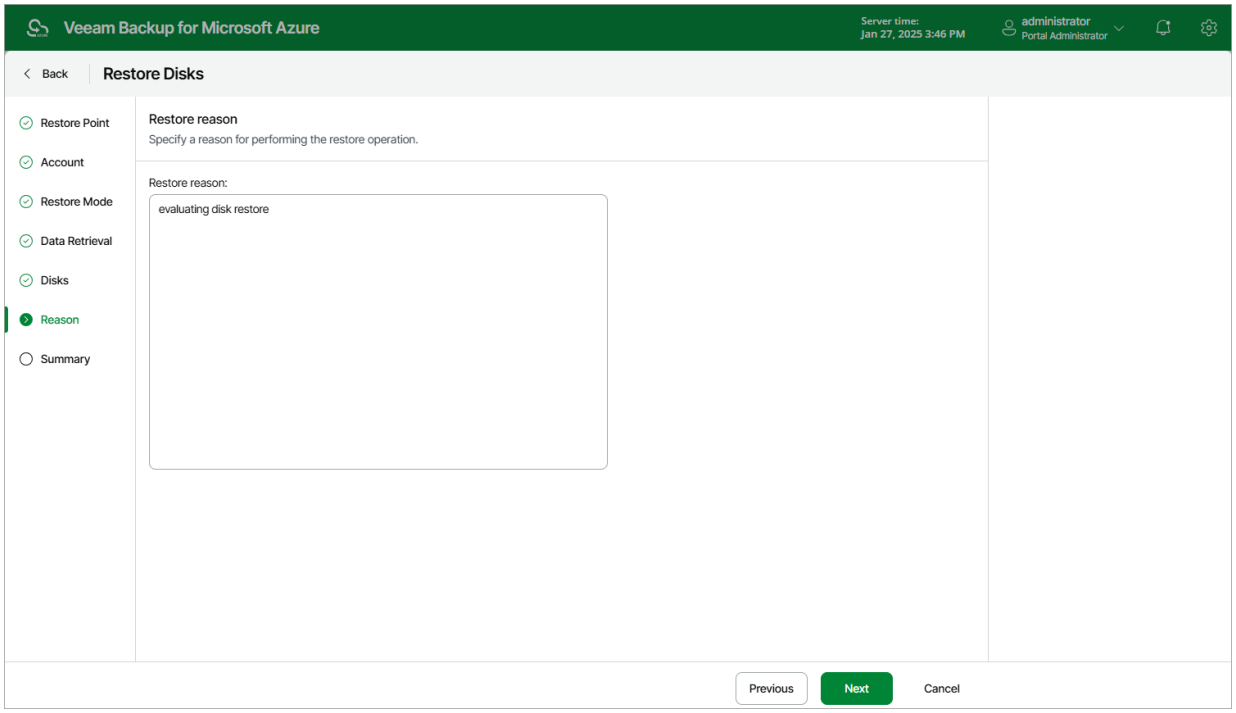
   d. [Applies only to managed disks] From the **Availability zone** drop-down list, select an availability zone to which you want to place the restored virtual disk.

e. To save changes made to the virtual disk settings, click **Apply**.



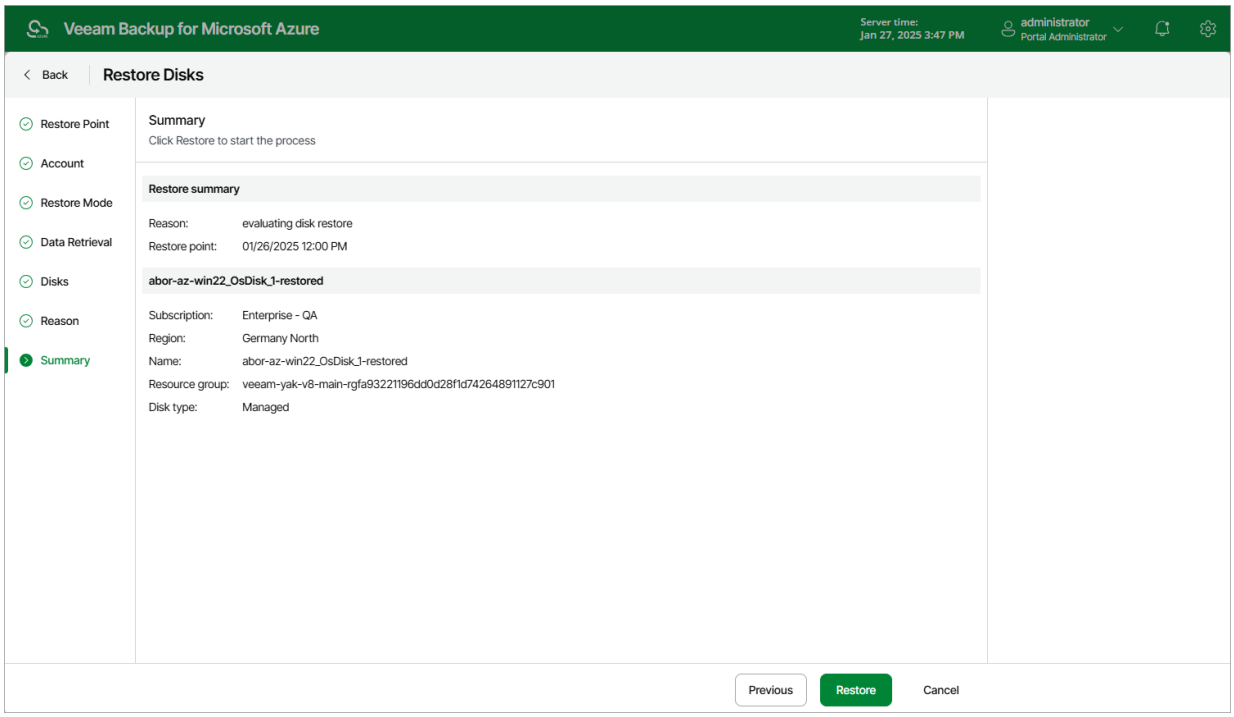
# Step 7. Specify Restore Reason

At the **Reason** step of the wizard, specify a reason for restoring the virtual disks. This information will be saved to the session history, and you will be able to reference it later.



## Step 8. Finish Working with Wizard

At the **Summary** step of the wizard, review summary information and click **Restore**.




# Performing File-Level Recovery

In case a disaster strikes, you can recover corrupted or missing files of an Azure VM from a cloud-native snapshot or image-level backup. Veeam Backup for Microsoft Azure allows you to download the necessary files and folders to a local machine, or restore the files and folders of the source Azure VM to the original location, using the File-level recovery browser.

**IMPORTANT**

- File-level recovery is supported from FAT, FAT32, NTFS, ext2, ext3, ext4, XFS, Btrfs file systems only. For Microsoft Windows systems, file-level recovery is supported for basic volumes only.

  If you want to recover files from file systems that are not supported by Veeam Backup for Microsoft Azure, you can add a backup repository that contains backups of Azure VMs to the backup infrastructure as an external repository, and perform the file-level recovery operation as described in the Veeam Backup & Replication User Guide.
- File-level recovery to the original location is supported only for Windows-based Azure VMs running Windows Server version 2016 (or later) and Windows version 10 (or later), and for Linux-based Azure VMs using the systemd init system.
- File-level recovery of Azure VMs with the Azure Disk Encryption option enabled is not supported in the current Veeam Backup for Microsoft Azure version.
- File-level recovery from virtual disks with Windows-native Data Deduplication enabled is not supported. To work around the issue, you can restore entire virtual disks, and then attach these disks to an Azure VM with the deduplication feature enabled. To learn how to restore entire virtual disks, see Performing Disk Restore.
- File-level recovery of Arm-based Azure VMs to the original location is not supported.

To recover files and folders of a protected Azure VM, do the following:

1. Launch the File-Level Recovery wizard.
2. Select a restore point.
3. Configure restore settings.
4. Specify a restore reason.
5. Finish working with the wizard — start a recovery session.
6. Choose files and folders to recover.
7. Stop the recovery session.

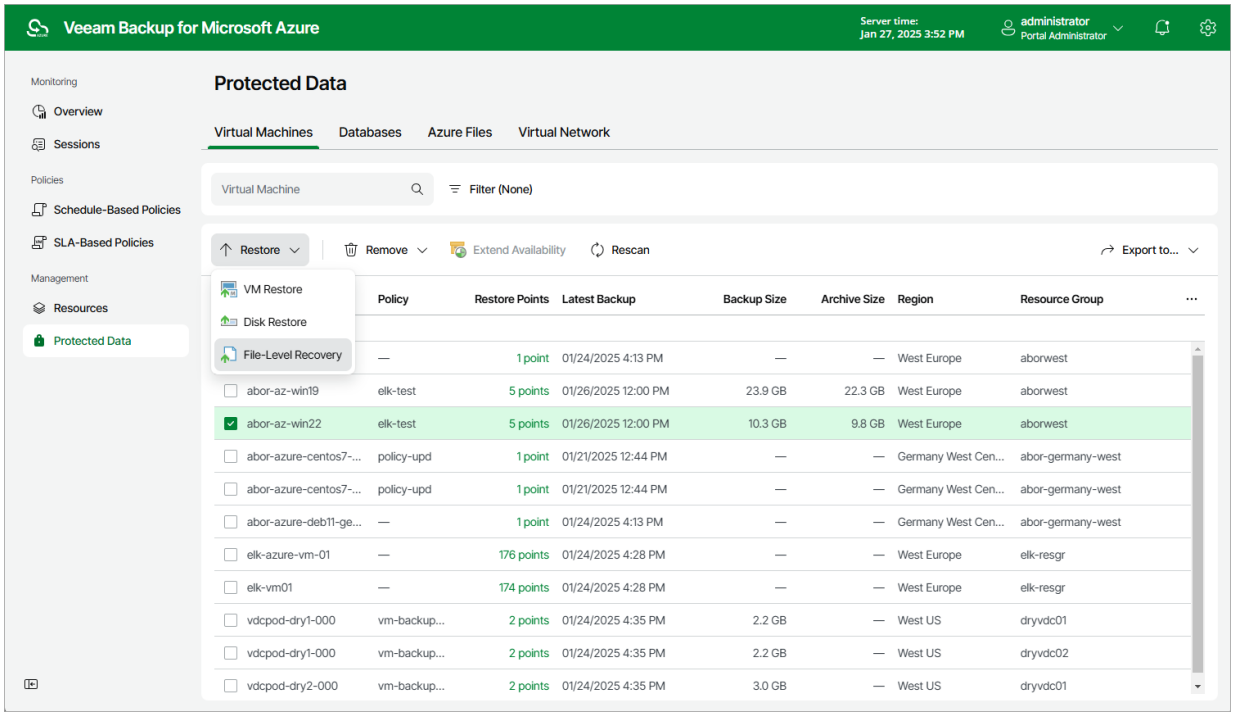
> **IMPORTANT**
>
> To recover files and folders of an Azure VM from a backup that is stored in an archive backup repository, you must retrieve the archived data manually before you begin the file-level recovery operation. To learn how to do that, see Retrieving Data from Archive.

# Step 1. Launch File-Level Recovery Wizard

To launch the **File-level Recovery** wizard, do the following:

1. Navigate to **Protected Data** > **Virtual Machines**.
2. Select the Azure VM whose files and folders you want to recover.
3. Click **Restore** > **File-Level Recovery**.

   Alternatively, click the link in the **Restore Points** column. Then, in the **Available Restore Points** window, select the necessary restore point and click **Restore** > **File-Level Recovery**.



# Step 2. Select Restore Point

At the **Restore Point** step of the wizard, select a restore point that will be used to recover files and folders of the selected Azure VM. By default, Veeam Backup for Microsoft Azure uses the most recent valid restore point. However, you can restore the Azure VM data to an earlier state.

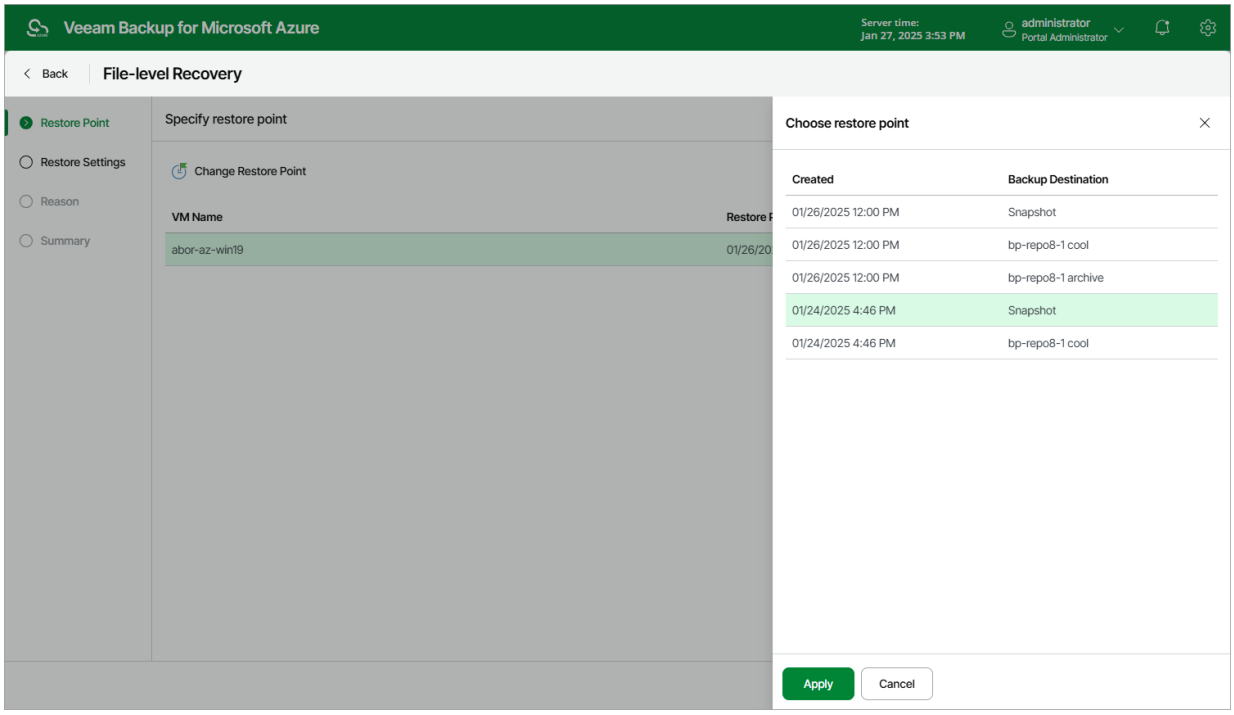
To select a restore point, do the following:

1. Select the Azure VM.
2. Click **Change Restore Point**.
3. In the **Specify restore point** window, select the necessary restore point and click **Apply**.

   To help you choose a restore point, Veeam Backup for Microsoft Azure provides the following information on each available restore point:

   - **Created** — the date when the restore point was created.
   - **Backup Destination** — the type of the restore point:
     - *<Repository Name>* — an image-level backup created by a backup policy.
     - *Snapshot* — a cloud-native snapshot created by a backup policy.
     - *Manual Snapshot* — a cloud-native snapshot created manually.

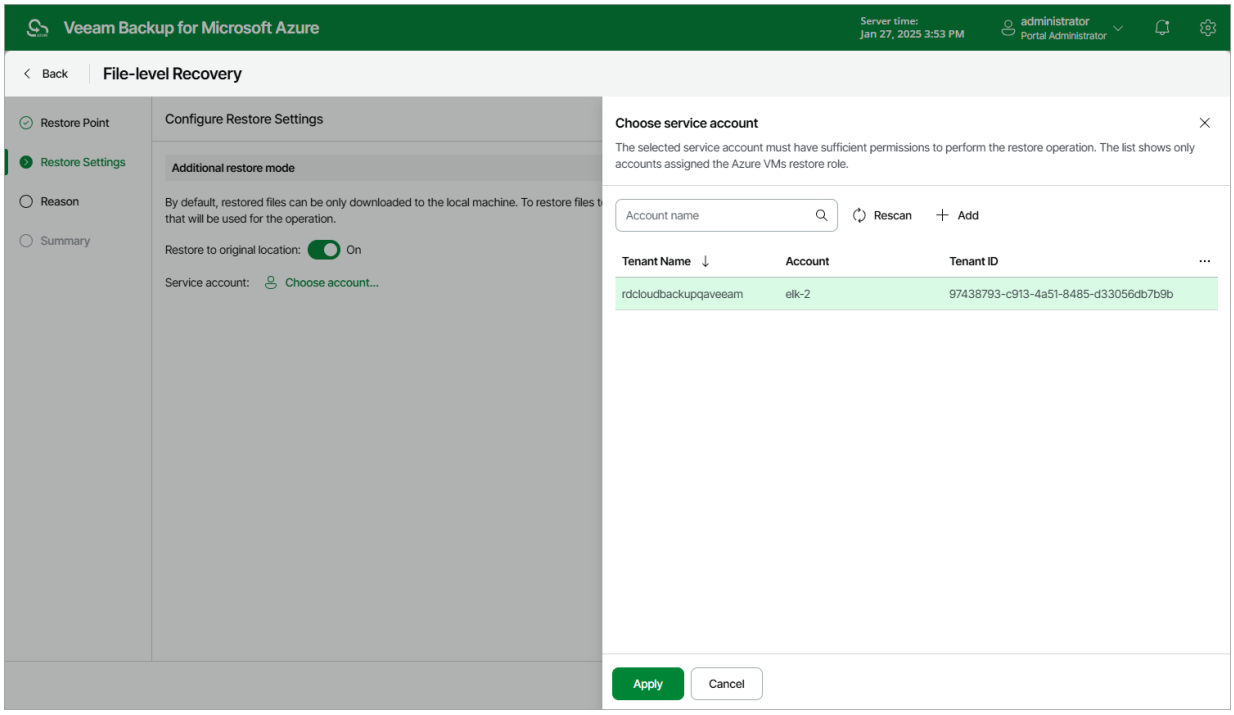
> **IMPORTANT**
>
> If you select a restore point stored in an archive repository, you will be redirected to the Data Retrieval wizard. Complete the **Data Retrieval** wizard, wait until the retrieval operation completes and then launch the **File-level Recovery** wizard again.



# Step 3. Configure Restore Settings

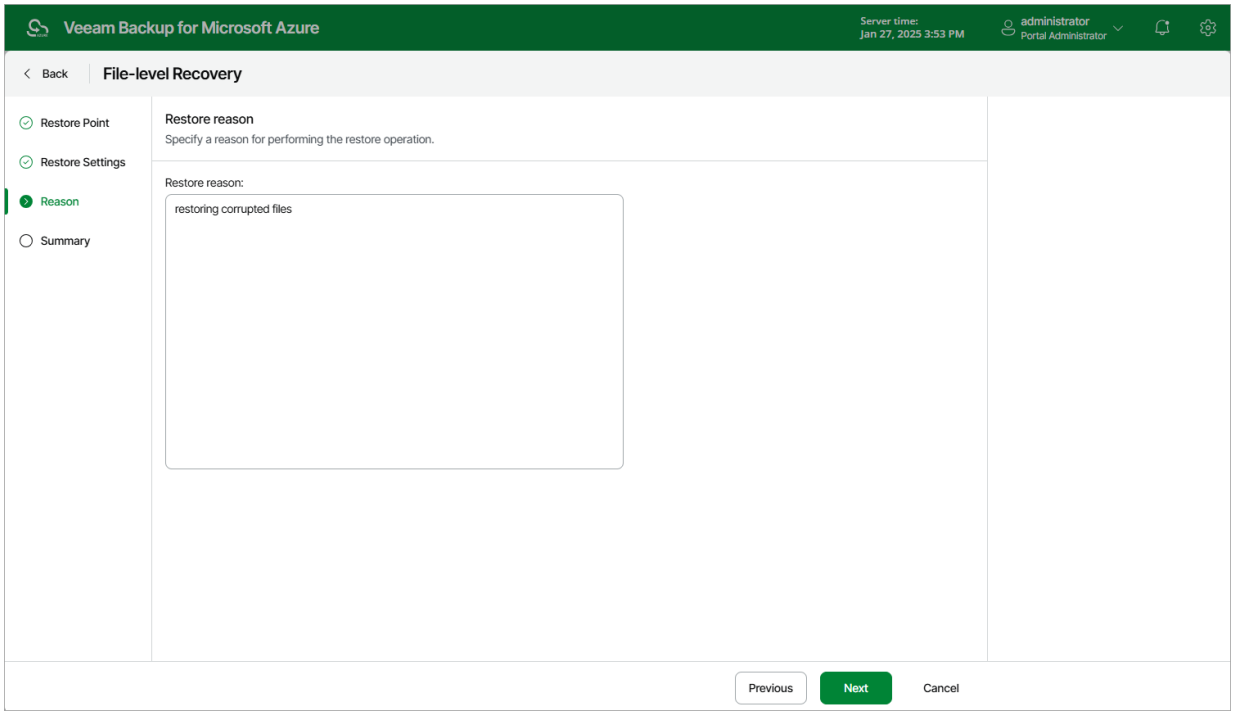
At the **Restore Settings** step of the wizard, choose whether you want to restore files to the original location. To do that, set the **Restore to original location** toggle to *On* and click the link in the **Service account** field. Then, select a service account that will be used for the restore operation. The specified service account must be assigned permissions listed in section Azure VM Permissions.

For a service account to be displayed in the list of available accounts, it must be added to Veeam Backup for Microsoft Azure and assigned the *Azure VMs Restore* operational role as described in section Adding Service Accounts; also, it must belong to the Microsoft Entra tenant and Azure subscription that contain the Azure VM whose files will be restored. If you have not added the necessary account to Veeam Backup for Microsoft Azure beforehand, you can do it without closing the **File-level Recovery** wizard. To do that, click **Add** and complete the **Add Account** wizard.



# Step 4. Specify Recovery Reason

At the **Reason** step of the wizard, specify a reason for recovering files and folders. This information will be saved to the session history, and you will be able to reference it later.



# Step 5. Start Recovery Session

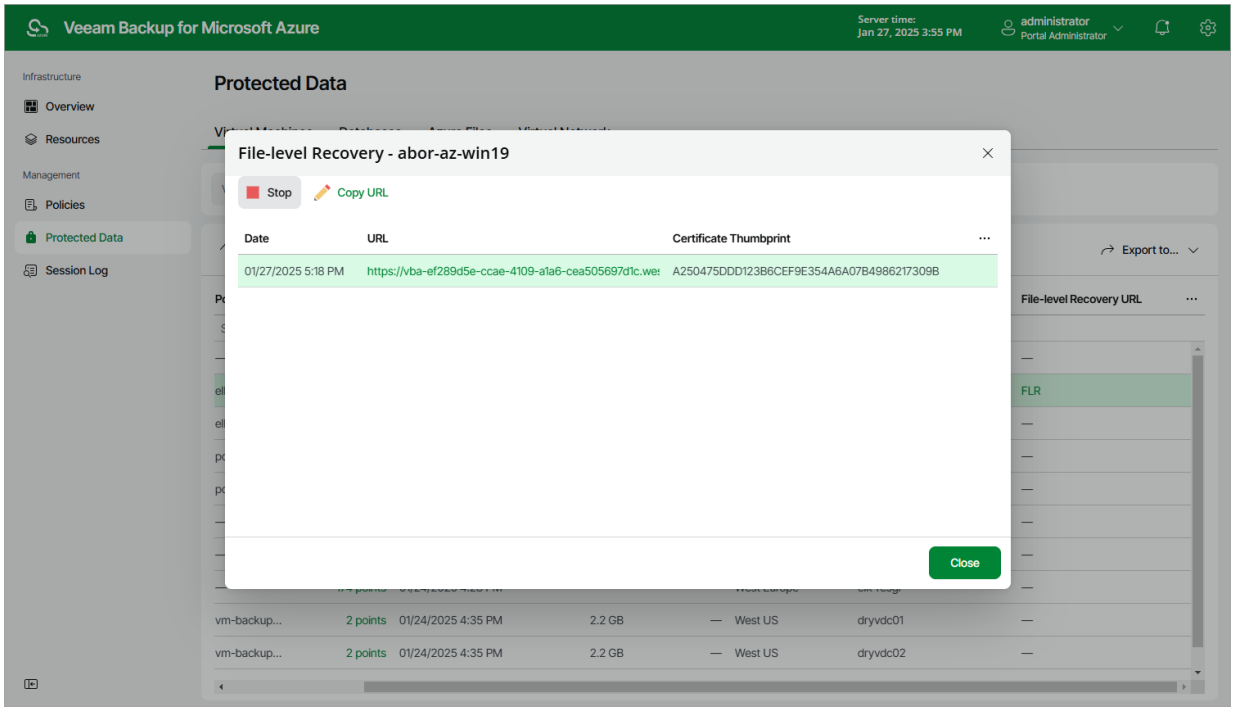
At the **Summary** step of the wizard, review summary information and click **Start**.

As soon as you click **Start**, Veeam Backup for Microsoft Azure will close the **Azure Files File-level Recovery** wizard and start a restore session. You can track the progress of the restore session in the **File-level Recovery** window. To open the **File-level Recovery** window, navigate to **Protected Data** and click the link in the **File-level Recovery URL** column. During the recovery session, Veeam Backup for Microsoft Azure will launch a worker instance and attach virtual disks of the processed Azure VM to it.

In the **URL** column of the window, Veeam Backup for Microsoft Azure will display a link to the file-level recovery browser. You can use the link in either of the following ways:

- Click the link to open the file-level recovery browser on your local machine while the recovery session is running.
- Copy the link, close the **File-level Recovery** window and open the file-level recovery browser on another machine.

> **IMPORTANT**
>
> When you click **Copy URL**, Veeam Backup for Microsoft Azure copies the following information to the clipboard:
>
> - A link to the file-level recovery browser that includes a public DNS name of the worker instance hosting the browser and authentication information used to access the browser.
> - A thumbprint of a TLS certificate installed on the worker instance hosting the file-level recovery browser.
>
> To avoid a man-in-the-middle attack, before you start recovering files and folders, check that the certificate thumbprint displayed in the web browser from which you access the file-level recovery browser matches the provided certificate thumbprint.



## Step 6. Choose Items to Recover

In the file-level recovery browser, you can find and recover items (files and folders) of the selected Azure VM. All recovered items will be saved in a single .ZIP archive to the default download directory on a local machine from which you access the file-level recovery browser, or will be restored to the original Azure VM.

To recover files and folders from a specific folder, perform the following steps:

1. On the **Browse** tab, specify files and folders that you want to recover:
   a. Navigate to the folder that contains the files and folders.
   b. In the working area, select check boxes next to the necessary items and click **Add to Restore List**.

> **NOTE**
>
> When building the file system tree of a Linux-based Azure VM in the file-level recovery browser, Veeam Backup for Microsoft Azure structures files and folders based not on their logical location but on the physical one. That is why the logical system tree of the processed Azure VM may differ from the file system tree displayed in the file-level recovery browser.

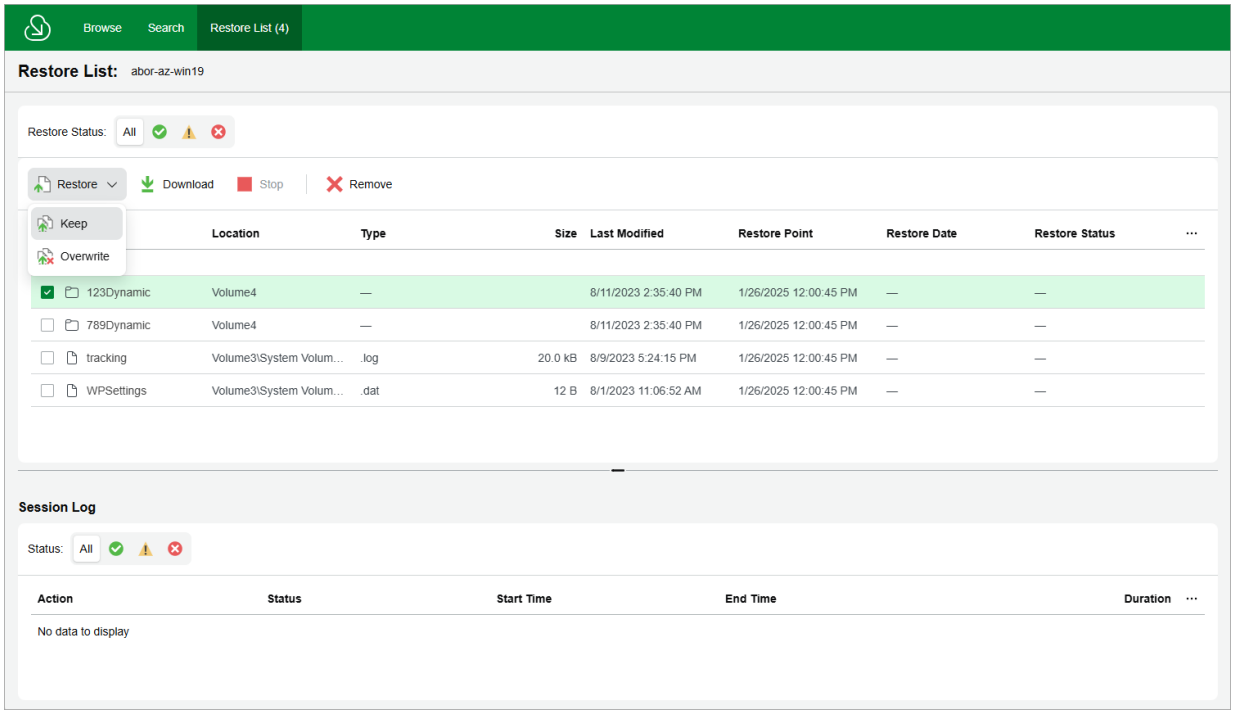
2. Switch to the **Restore List** tab, review the list of files and folders, select check boxes next to the items that you want to recover and do the following:
   - To download the selected files and folders to the local machine, click **Download**.
   - To download the selected files and folders to the original Azure VM, click **Restore** > **Keep**.

     Veeam Backup for Microsoft Azure will save the files with the `_RESTORED_<date>_<time>` suffix to the same directory where the source files are located.
   - To restore the selected files and folders to the original Azure VM, click **Restore** > **Overwrite**.

     Veeam Backup for Microsoft Azure will overwrite the source files.

> **NOTE**
>
> When restoring files that have multiple hard links, Veeam Backup for Microsoft Azure does not modify the state of existing hard links and does not create new ones. Veeam Backup for Microsoft Azure also does not associate any hard links to the files that are restored to a custom location.

As soon as you click **Restore** or **Download**, Veeam Backup for Microsoft Azure will recover the selected files. You can track the progress and view the results of the restore operation in the **Session Log** section of the **Restore List** tab.

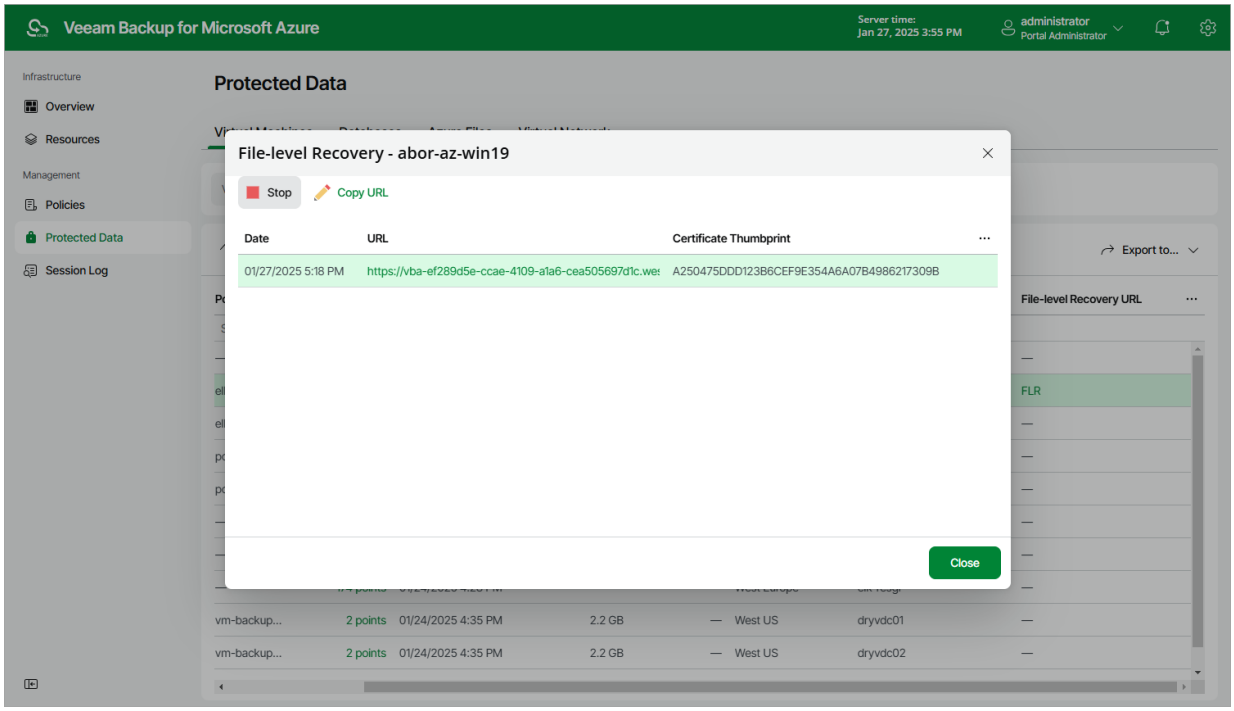


# Step 7. Stop Recovery Session

After you finish working with the file-level recovery browser, it is recommended that you stop the recovery session so that Veeam Backup for Microsoft Azure can unmount and detach virtual disks of the processed Azure VM from the worker instance and deallocate the worker instance.

To stop the recovery session, click **Stop** in the **File-level Recovery** window. If you do not perform any actions in the file-level recovery browser for 30 minutes, and if no files are being restored, Veeam Backup for Microsoft Azure will stop the recovery session automatically.

> **TIP**
>
> If you accidentally close the **File-level Recovery** window, navigate to **Protected Data** and click the link in the **File-level Recovery URL** column to open the window again.



# SQL Restore

The actions that you can perform with restore points of Azure SQL databases depend on whether you access the restore points using the Veeam Backup & Replication console or the Veeam Backup for Microsoft Azure Web UI.

# Performing SQL Restore Using Console

In case a disaster strikes, you can restore an Azure SQL database from an image-level backup. Veeam Backup & Replication allows you to restore one or more databases at a time, to the original location or to a new location. To learn how SQL restore works, see section Performing SQL Restore Using Web UI.

To restore Azure SQL databases, do the following:

1. Launch the Restore to Microsoft Azure SQL Wizard.
2. Select a restore point.
3. Choose a restore mode.
4. Specify target Azure SQL Server settings.
5. Specify a new name for the restored database.
6. Specify a restore reason.
7. Finish working with the wizard.

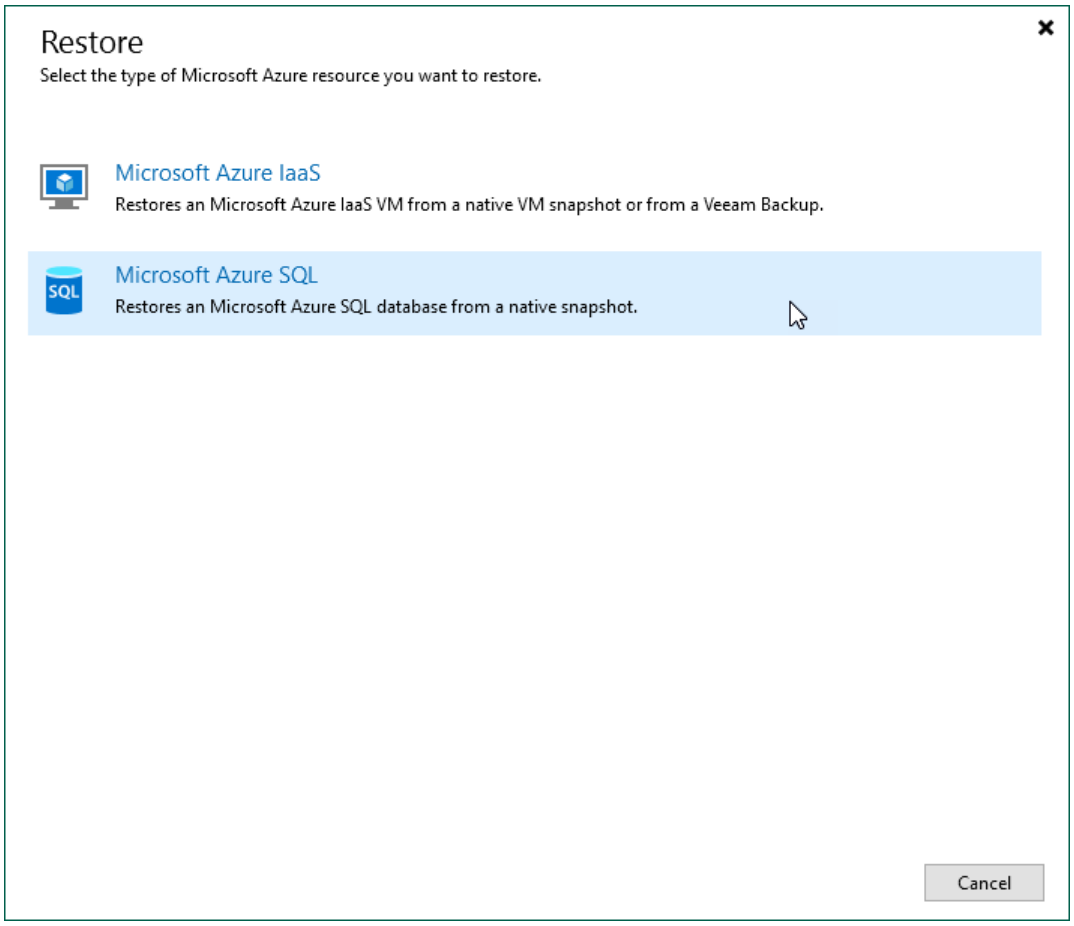
# Step 1. Launch Restore to Microsoft Azure SQL Wizard

To launch the **Restore to Microsoft Azure SQL** wizard, do the following:

1. In the Veeam Backup & Replication console, open the **Home** view.
2. Navigate to **Backups** > **External Repository**.
3. In the working area, expand the backup policy that protects a SQL database you want to restore, select the necessary database and click **Microsoft Azure SQL** on the ribbon.

   Alternatively, you can right-click the database and select **Restore to Microsoft Azure SQL**.

> **TIP**
>
> You can also launch the **Restore to Microsoft Azure SQL** wizard from the **Home** tab. To do that, click **Restore** and select **Microsoft Azure**. Then, select **Microsoft Azure SQL** in the **Restore** window.



# Step 2. Select SQL Database and Restore Point

At the **SQL database** step of the wizard, choose a restore point that will be used to restore the selected Azure SQL database. By default, Veeam Backup & Replication uses the most recent valid restore point. However, you can restore the database data to an earlier state.

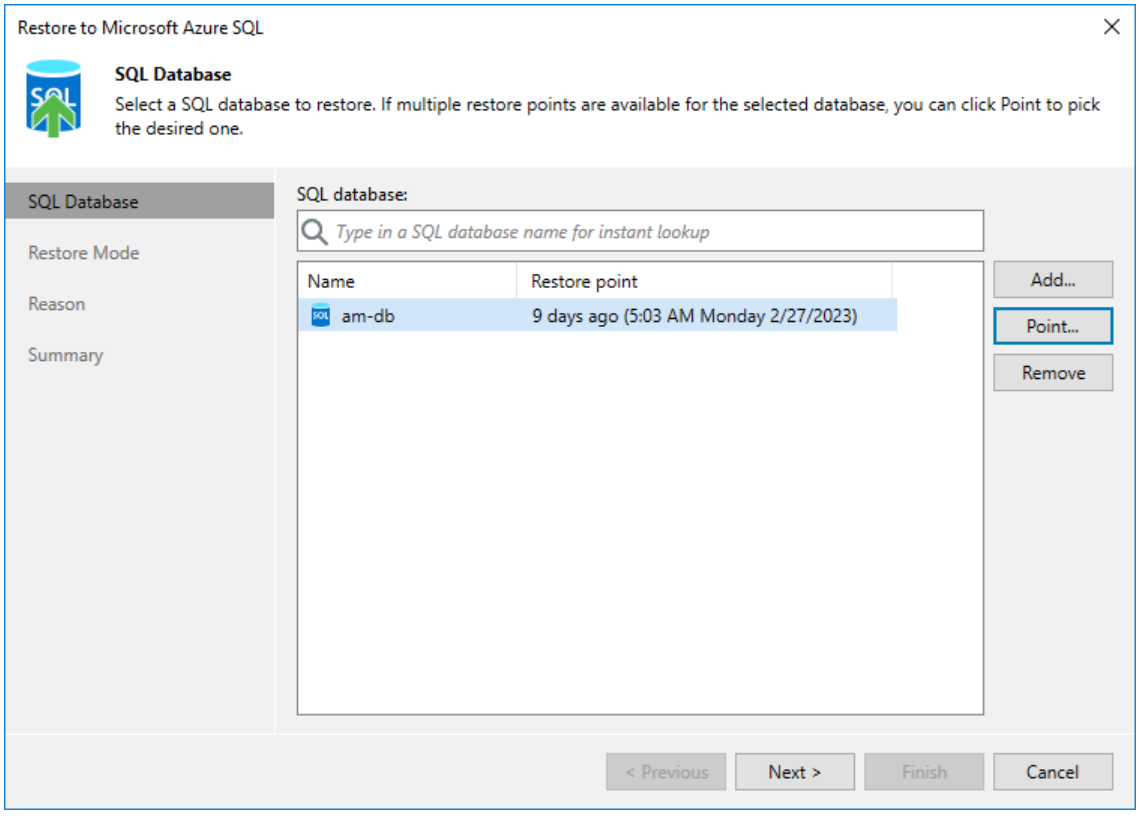
To select a restore point, do the following:

1. In the **SQL database** list, select the SQL database and click **Point**.
2. In the **Restore Points** window, expand the backup policy that protects the SQL database, select the necessary restore point and click **OK**.

   To help you choose a restore point, Veeam Backup & Replication provides the following information on each available restore point:

   - **Job** – the name of the backup policy that created the restore point and the date when the restore point was created.
   - **Type** – the type of the restore point.
   - **Location** – the repository where the restore point is stored.

> **TIP**
>
> You can use the wizard to restore multiple databases at a time. To do that, click **Add**, select more databases to restore and choose a restore point for each of them.



# Step 3. Choose Restore Mode

At the **Restore Mode** step of the wizard, do the following:

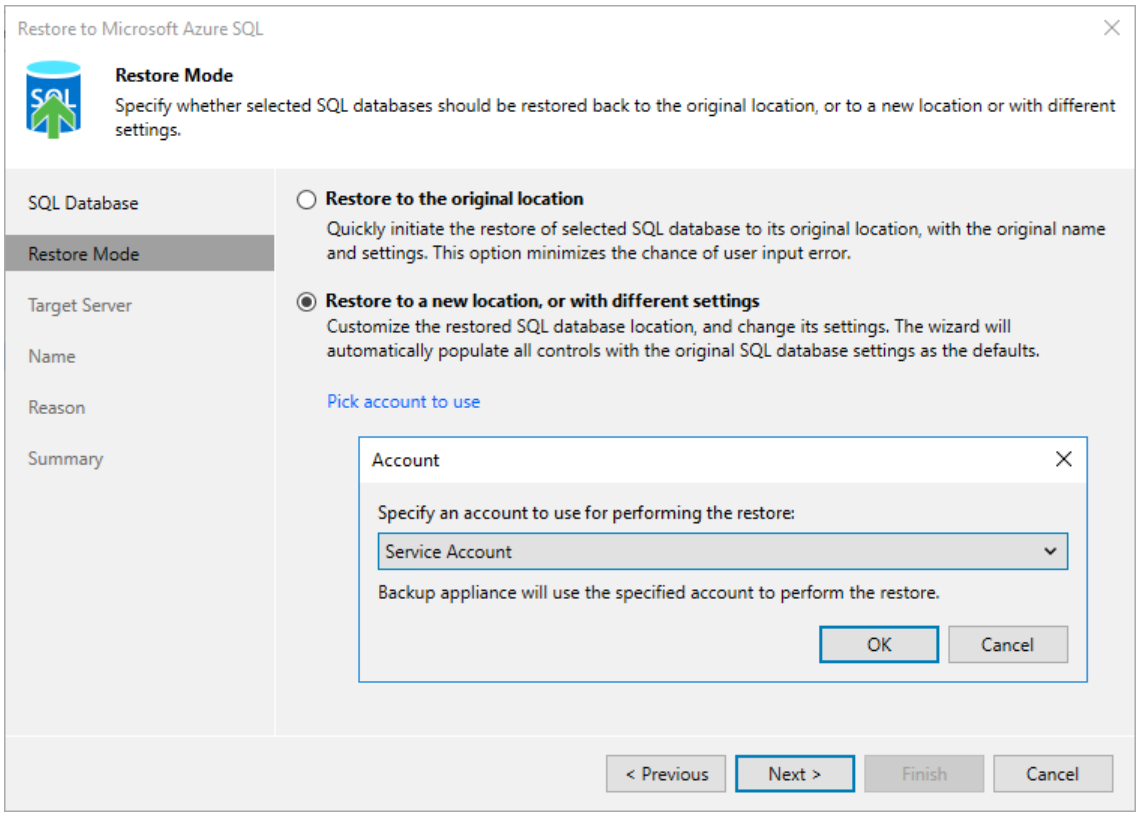
1. Choose whether you want to restore the Azure SQL database to the original or to a new location.

> **IMPORTANT**
>
> If Veeam Backup & Replication cannot automatically detect an Azure SQL account that will be used to access the original SQL Server, the Restore to the original location option will not be available. However, you can restore the database to the original location using the Restore to a new location, or with different settings option. To do that, choose the specified option, select the necessary Azure SQL account at step 4, and proceed with the wizard with the preconfigured settings.

2. Click **Pick account to use** to select a service account whose permissions will be used to perform the restore operation. For more information on the required permissions, see Service Account Permissions.

   For a service account to be displayed in the list of available accounts, it must be added to Veeam Backup for Microsoft Azure and assigned the *Azure SQL Restore* operational role as described in section Adding Service Accounts.

> **NOTE**
>
> To perform restore operations, Veeam Backup & Replication uses permissions of service accounts that belong to the tenants that contained original SQL databases. If none of the service accounts added to Veeam Backup for Microsoft Azure belong to these tenants, the **Restore to the original location** option will not be available.



# Step 4. Specify Target SQL Server Settings

[This step applies only if you have selected the **Restore to a new location, or with different settings** option at the **Restore Mode** step of the wizard]

At the **Target server** step of the wizard, you can specify a target server and its settings for the restored Azure SQL database. To do that, select the database and click **Server**. In the **Target server** window, do the following:

1. From the **SQL server** drop-down list, select a target SQL Server or an Azure SQL Managed Instance that will host the restored database.

   For a SQL Server to be displayed in the list of available servers, it must be created in Microsoft Azure as described in Microsoft Docs.

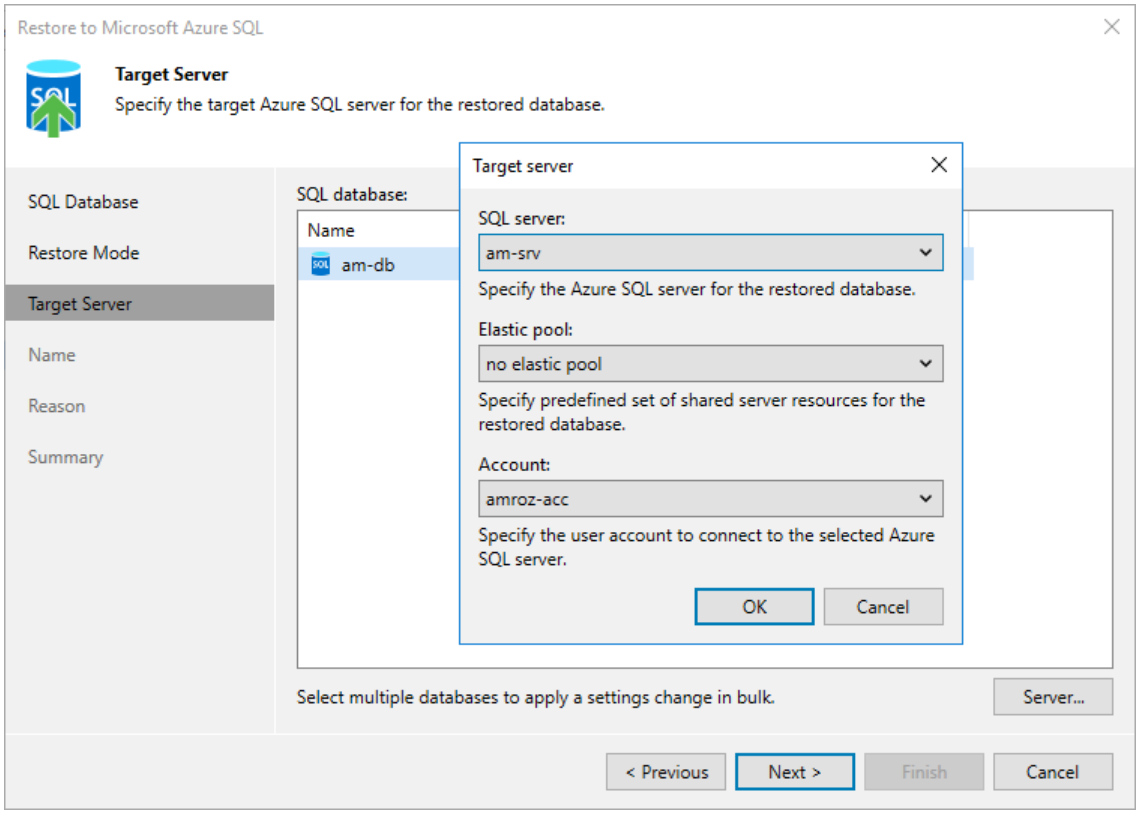
   For an Azure SQL Managed Instance to be displayed in the list of available instances, it must be created in Microsoft Azure as described in Microsoft Docs.

2. [Applies only if you restore databases to a SQL Server] From the **Elastic pool** drop-down list, select an elastic pool to which the restored database will be added.

   For an elastic pool to be displayed in the list of available pools, it must be created in Microsoft Azure as described in Microsoft Docs.

3. From the **Account** drop-down list, select an Azure SQL account that will be used to authenticate against the target SQL Server. Note that the specified account must be created on the target server beforehand and assigned full administrative permissions as described in Microsoft Docs.

   For an Azure SQL account to be displayed in the list of available accounts, it must be added to the Veeam Backup for Microsoft Azure appliance as described in section Adding SMTP and Database Accounts.

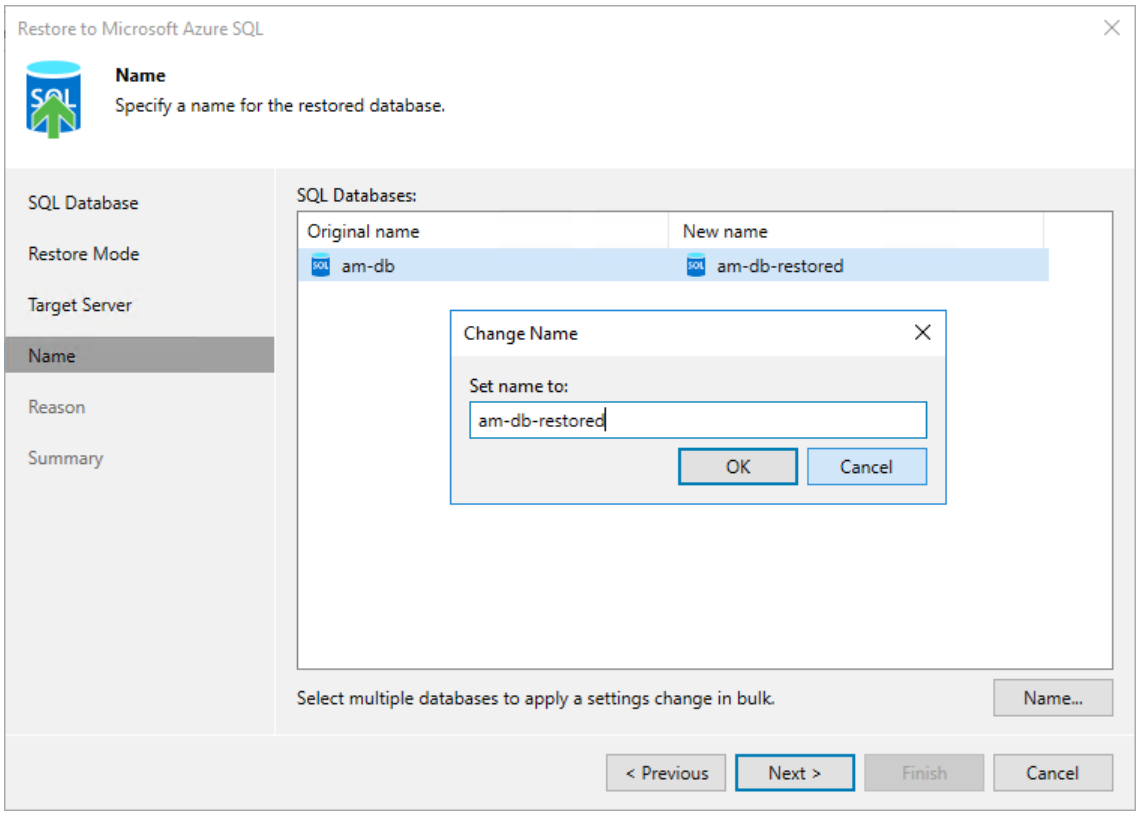


# Step 5. Specify SQL Database Name

[This step applies only if you have selected the **Restore to a new location, or with different settings** option at the **Restore Mode** step of the wizard]

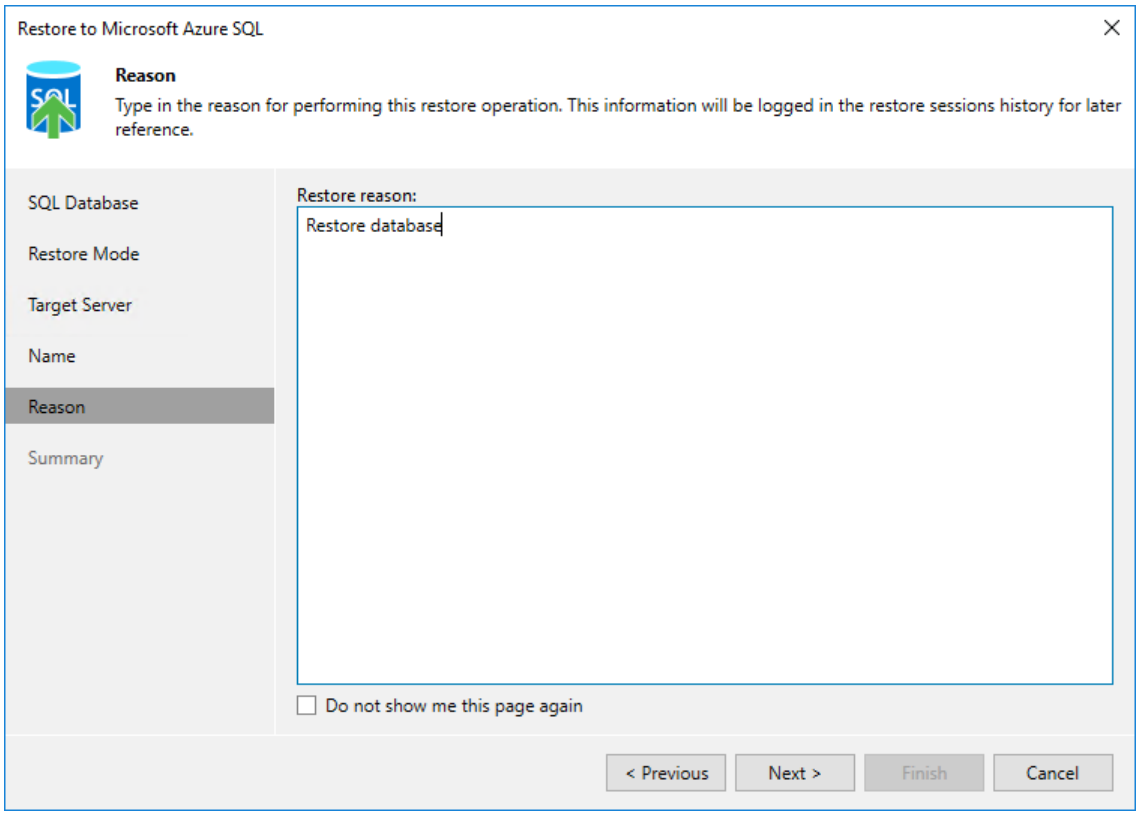
At the **Name** step of the wizard, specify a new name for the restored Azure SQL database. It is recommended that you choose the new name carefully — due to Microsoft Azure limitations, you will not be able to rename the database after the restore operation completes.

> **TIP**
>
> You can specify a single prefix or suffix and add it to the names of multiple SQL databases. To do that, select the necessary SQL databases and click **Name**. In the **Change Name** window, select the **Add prefix** or **Add suffix** check box, and provide the text that you want to add. Then, click **OK**.



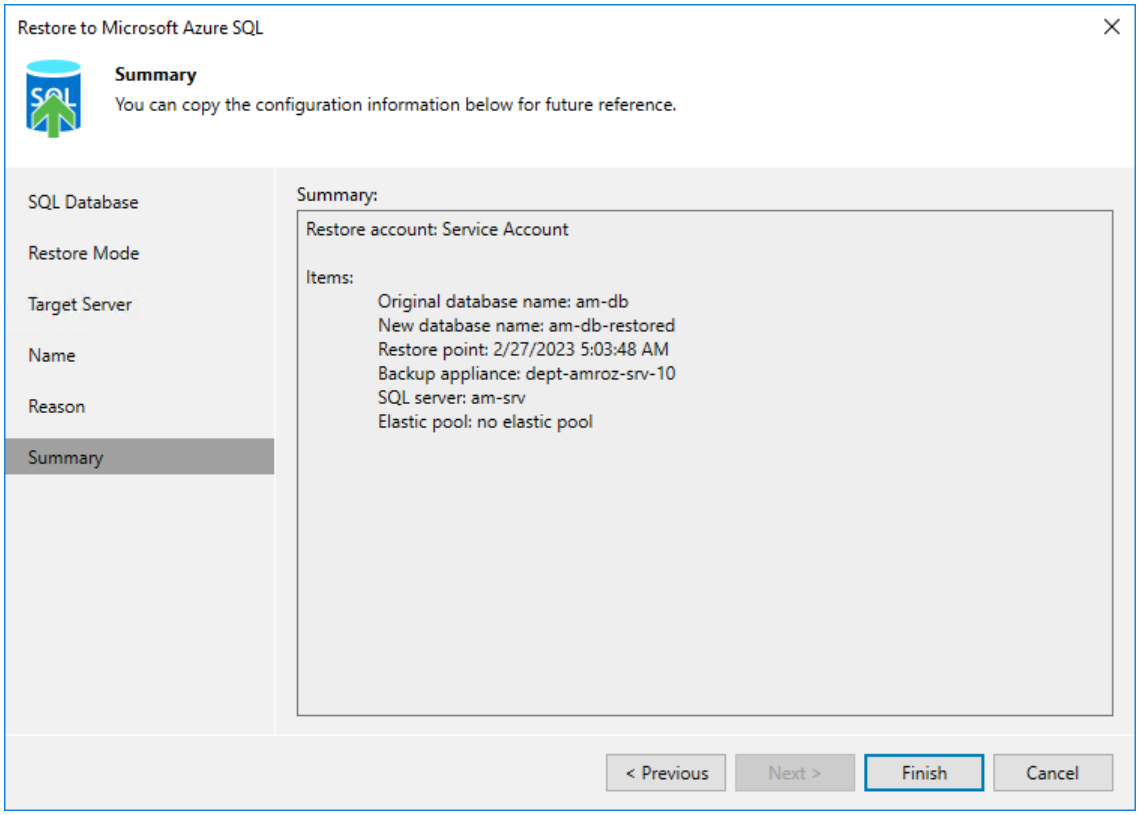
# Step 6. Specify Restore Reason

At the **Reason** step of the wizard, specify a reason for restoring the Azure SQL database. The information you provide will be saved in the session history and you can reference it later.



# Step 7. Finish Working with Wizard

At the **Summary** step of the wizard, review summary information and click **Finish**.



# Performing SQL Restore Using Web UI

In case a disaster strikes, you can restore an entire Azure SQL database from an image-level backup. Veeam Backup for Microsoft Azure allows you to restore one or more databases at a time, to the original location or to a new location.

> **IMPORTANT**
>
> Within one restore session, you can restore only those Azure SQL databases that belong to the same SQL Server.

## Before You Begin

To restore an Azure SQL database from a backup that is stored in an archive repository, you must retrieve the archived data first. You can either retrieve the archived data manually before you begin the restore operation, or launch the data retrieval process right from the restore wizard. To learn how to retrieve data manually, see Retrieving Data From Archive.

## How to Perform SQL Restore

To restore an Azure SQL database, do the following:

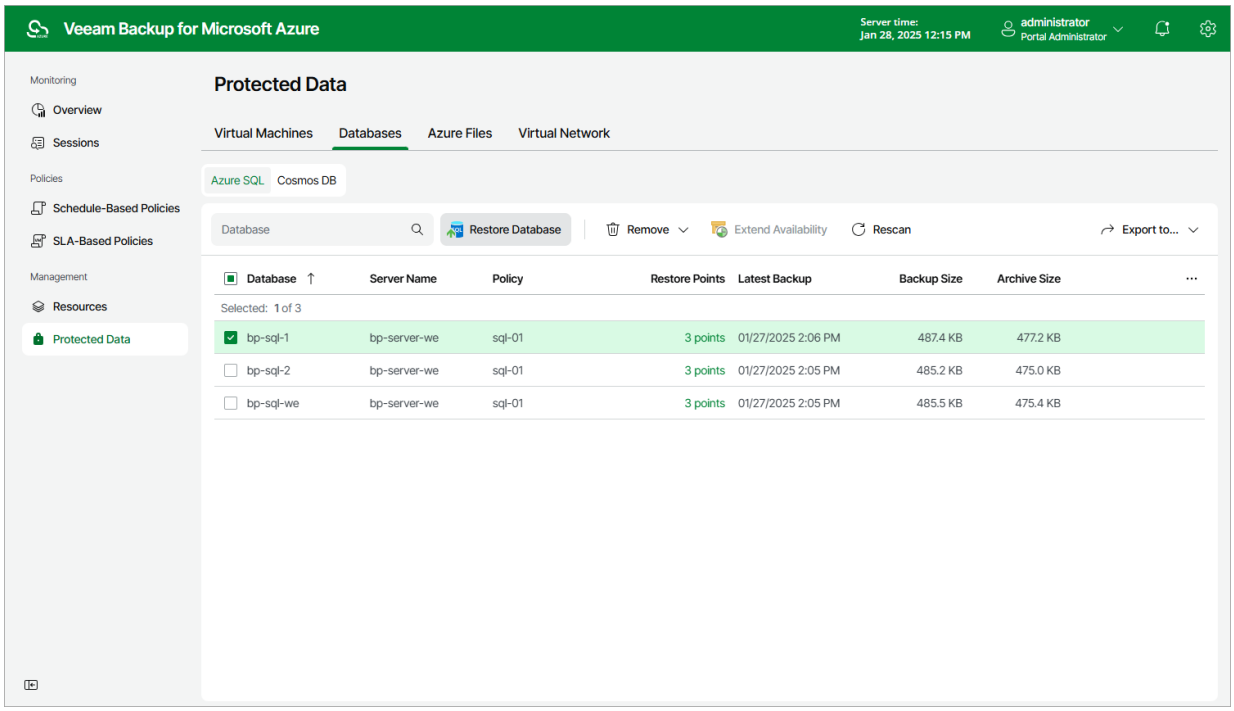
1. Launch the SQL Database restore wizard.
2. Select a restore point.
3. Select a service account.
4. Choose a restore mode.
5. Select an Azure SQL account.
6. Specify data retrieval settings.
7. Configure restore settings.
8. Specify a restore reason.
9. Review summary information.

# Step 1. Launch SQL Database Restore Wizard

To launch the **SQL Database Restore** wizard, do the following:

1. Navigate to **Protected Data** > **Databases** > **Azure SQL**.
2. Select the Azure SQL databases that you want to restore.
3. Click **Restore Database**.

   Alternatively, click the link in the **Restore Points** column. Then, in the **Available Restore Points** window, select the necessary restore point and click **Restore Database**.



# Step 2. Select Restore Point

At the **Databases** step of the wizard, select a restore point that will be used to restore the selected Azure SQL database. By default, Veeam Backup for Microsoft Azure uses the most recent valid restore point. However, you can restore the database data to an earlier state.

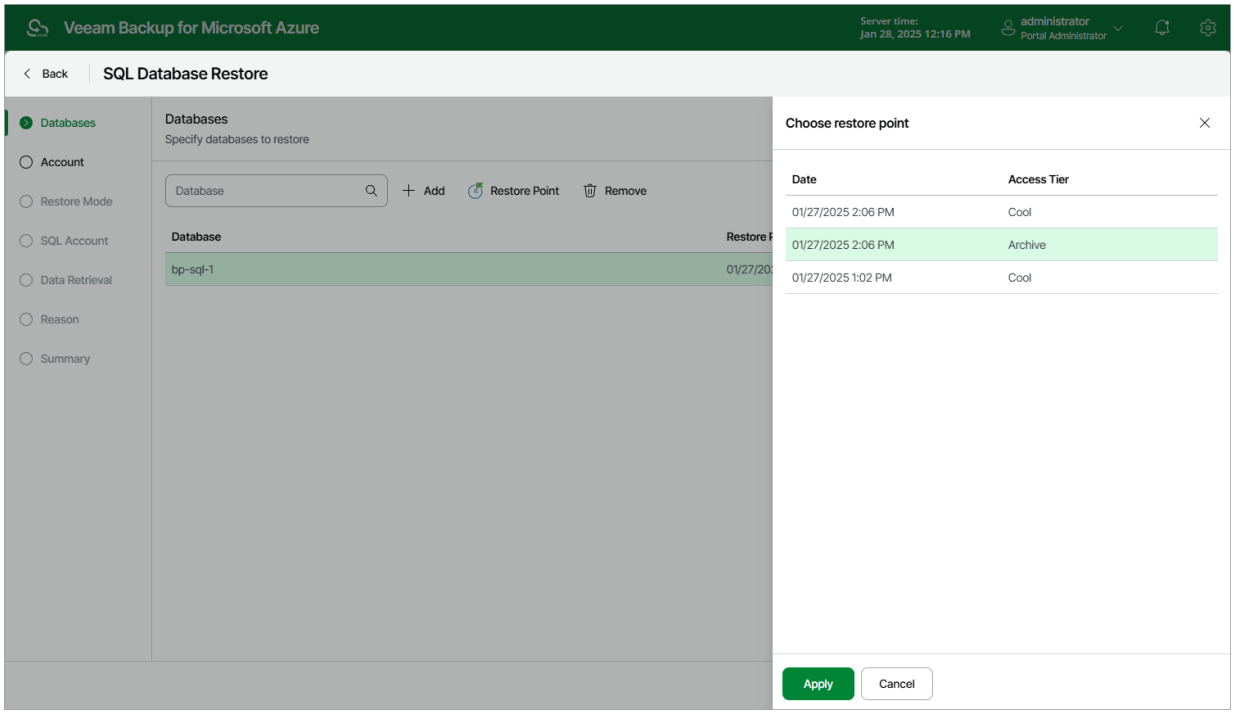
> **IMPORTANT**
>
> If you select a restore point stored in an archive repository and the same restore point is also available in a regular repository, Veeam Backup for Microsoft Azure will display the confirmation window where you must choose whether you want to use the archived or regular restore point to perform the restore operation.

To select a restore point, do the following:

1. Select the Azure SQL database and click **Restore Point**.
2. In the **Specify restore point** window, select the necessary restore point and click **Apply**.

   To help you choose a restore point, Veeam Backup for Microsoft Azure provides the following information on each available restore point:

   - **Date** – the date when the restore point was created.
   - **Access Tier** – the storage tier of a backup repository where the restore point is stored.

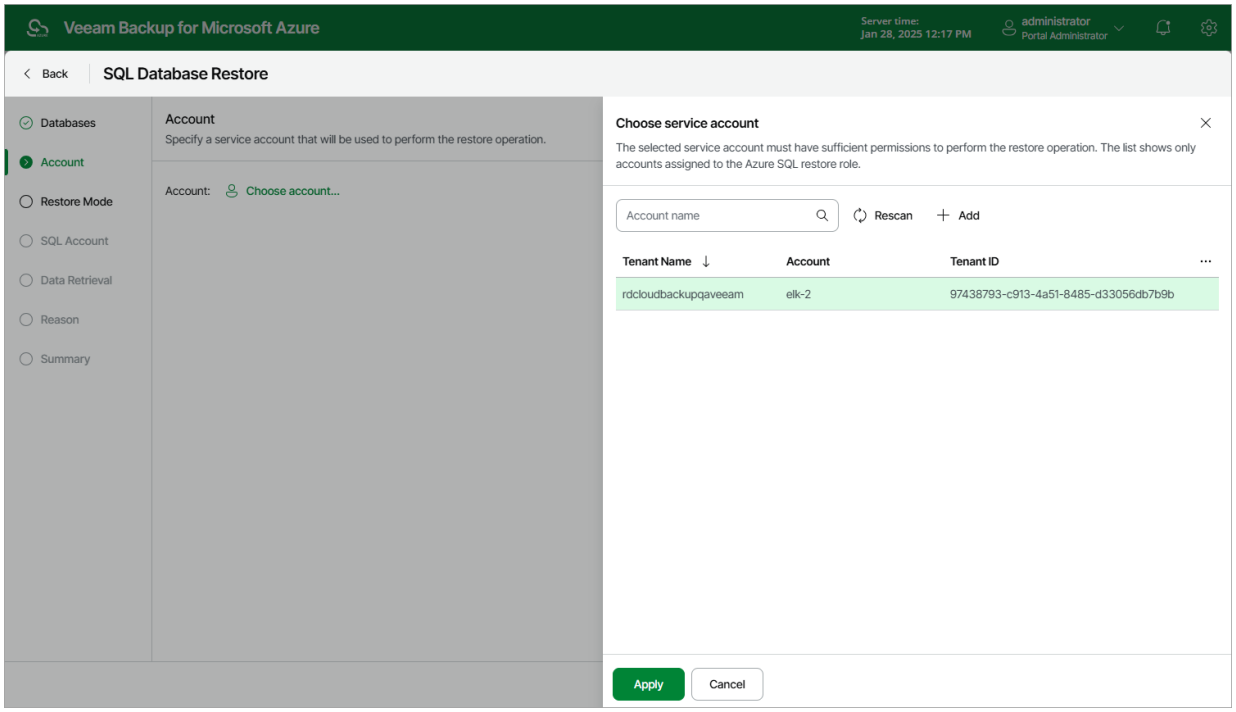


# Step 3. Select Service Account

At the **Account** step of the wizard, select a service account whose permissions Veeam Backup for Microsoft Azure will use to perform the restore operation.

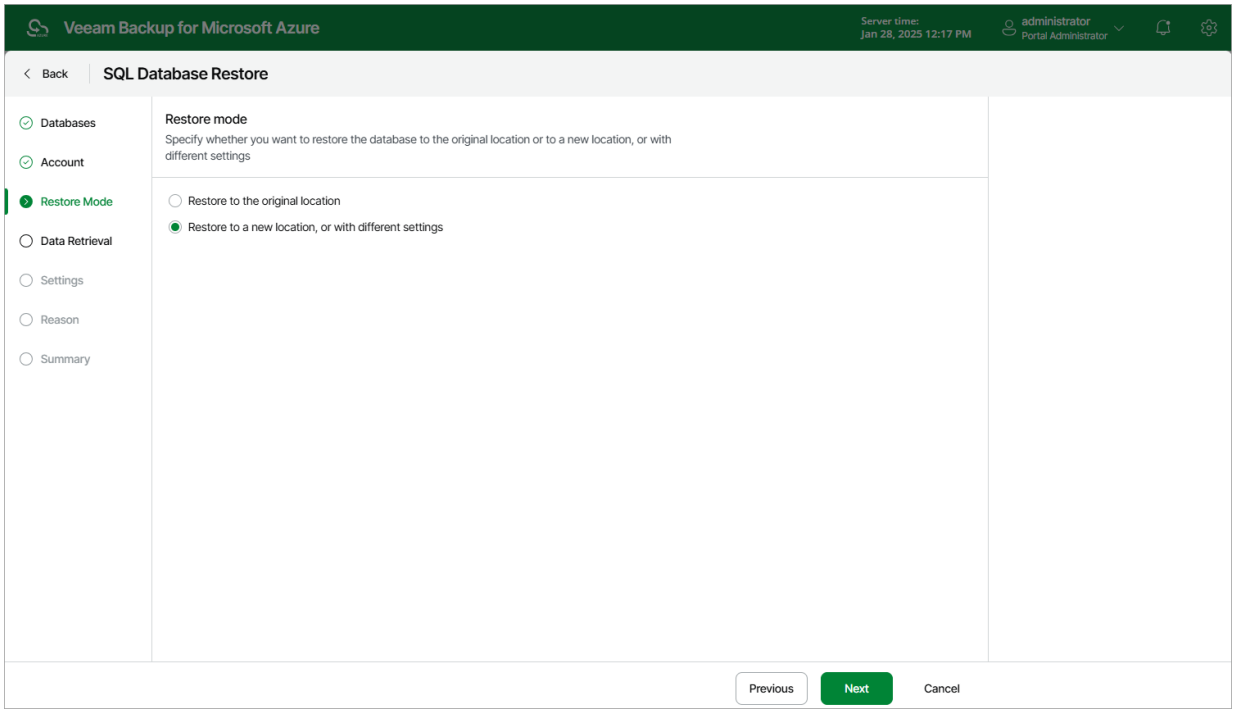
1. Click **Choose account**.
2. In the **Choose service account** window, select the necessary account and click **Apply**. The specified service account must be assigned permissions listed in section Azure SQL Permissions.

   For a service account to be displayed in the list of available accounts, it must be added to Veeam Backup for Microsoft Azure and assigned the *Azure SQL Restore* operational role as described in section Adding Service Accounts. If you have not added the necessary service account to Veeam Backup for Microsoft Azure beforehand, you can do it without closing the **SQL Database Restore** wizard. To do that, click **Add** and complete the **Add Account** wizard.



# Step 4. Choose Restore Mode

At the **Restore Mode** step of the wizard, choose whether you want to restore the Azure SQL database to the original or to a custom location.



# Step 5. Select Azure SQL Account

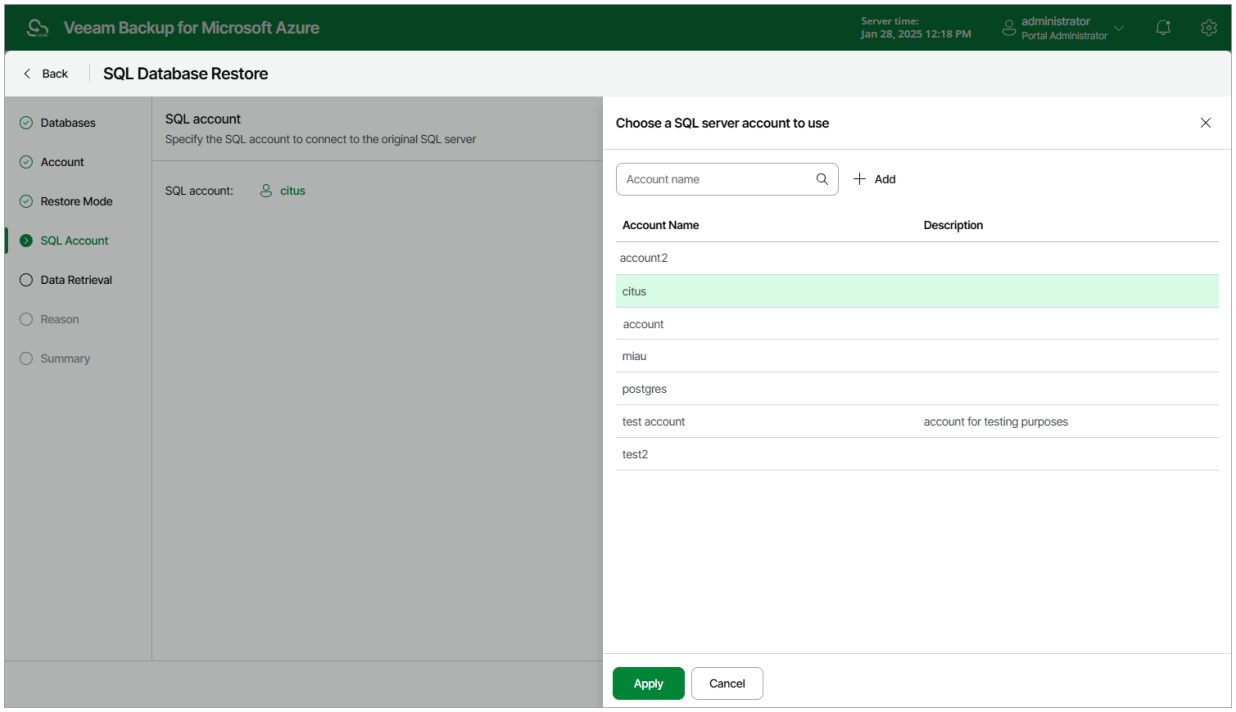
[This step applies only if you have selected the **Restore to the original location** option at the **Restore Mode** step of the wizard]

At the **SQL account** step of the wizard, select an Azure SQL Server account that will be used to authenticate against the SQL Server that will host the restored database.

1. Click **Instance**.
2. In the **Choose a SQL server account to use** window, select the necessary Azure SQL Server account and click **Apply**.

   For an Azure SQL Server account to be displayed in the list of available accounts, it must be added to Veeam Backup for Microsoft Azure as described in section Adding SMTP and Database Accounts.

> **IMPORTANT**
>
> When selecting an Azure SQL Server account, consider the following:
>
> - Portal Operators and Restore Operators can use only those Azure SQL Server accounts that have been specified for the SQL Server in settings of any backup policy created by a Portal Administrator.
> - Microsoft Entra ID authentication is not supported.

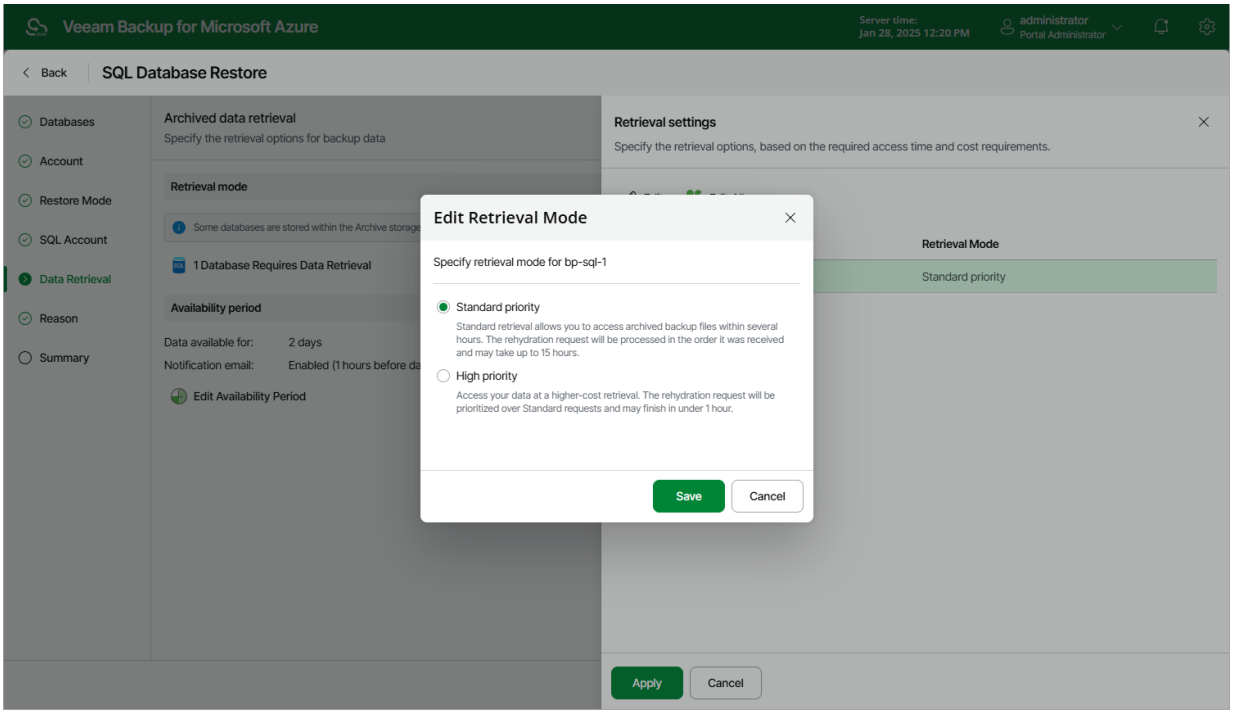


# Step 6. Specify Retrieval Settings

[This step applies only if you have selected a restore point stored in an archive repository at the **Databases** step of the wizard]

At the **Data retrieval** step of the wizard, choose a retrieval mode and specify a period for which you want to keep the data available.

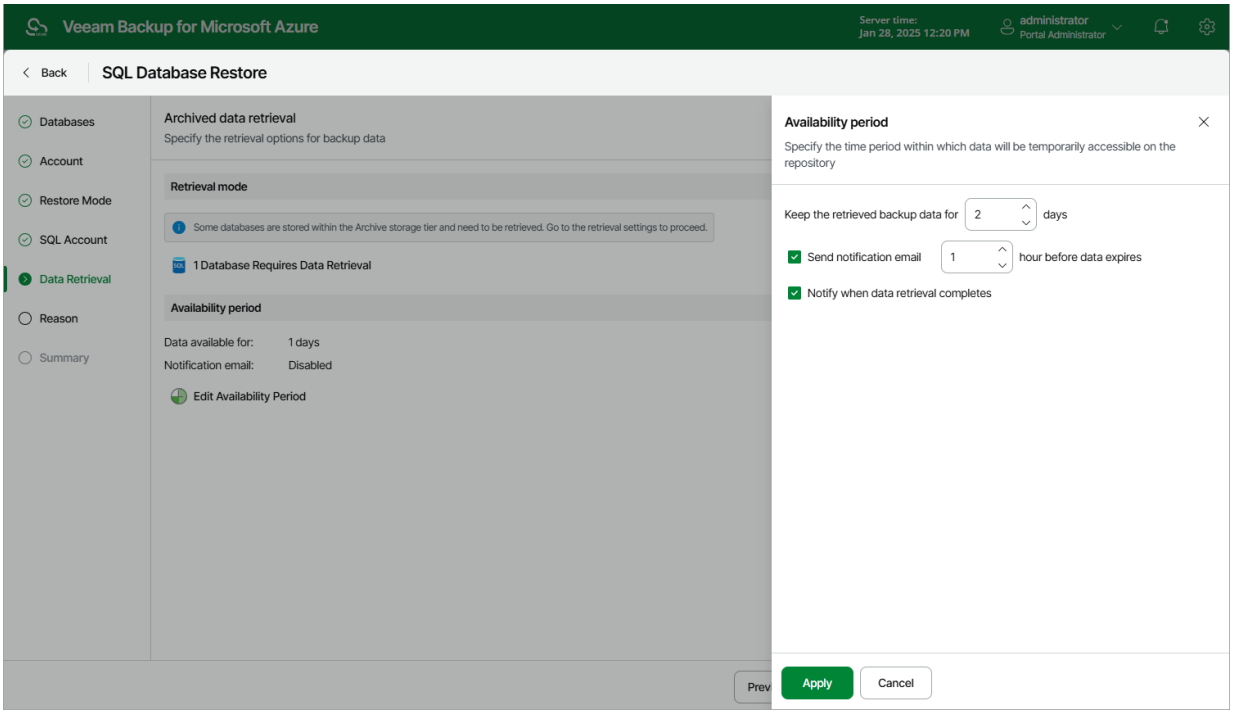
1. Click the link in the **Retrieval mode** section.
   a. In the **Retrieval settings** window, for each processed Azure SQL database, do the following:
      i. Select an Azure SQL database and click **Edit**.
      ii. In the **Edit Retrieval Mode** window, select the retrieval mode that Veeam Backup for Microsoft Azure will use to retrieve the archived data, and click **Save**. For more information on data retrieval modes, see Retrieving Data From Archive.
   b. To save changes made to the data retrieval settings, click **Apply**.




2. Click **Edit Availability Period** in the **Availability period** section.
   a. In the **Availability period** window, specify the number of days for which you want to keep the data available for restore operations. You can manually extend the availability period later if required.

> **TIP**
>
> If you want to receive an email notification when data availability period is about to expire, select the **Send notification email** check box and choose when you want to be notified (that is, the number of hours remaining until data expiration).

b. To save changes made to the availability period settings, click **Apply**.



# Step 7. Configure Restore Settings

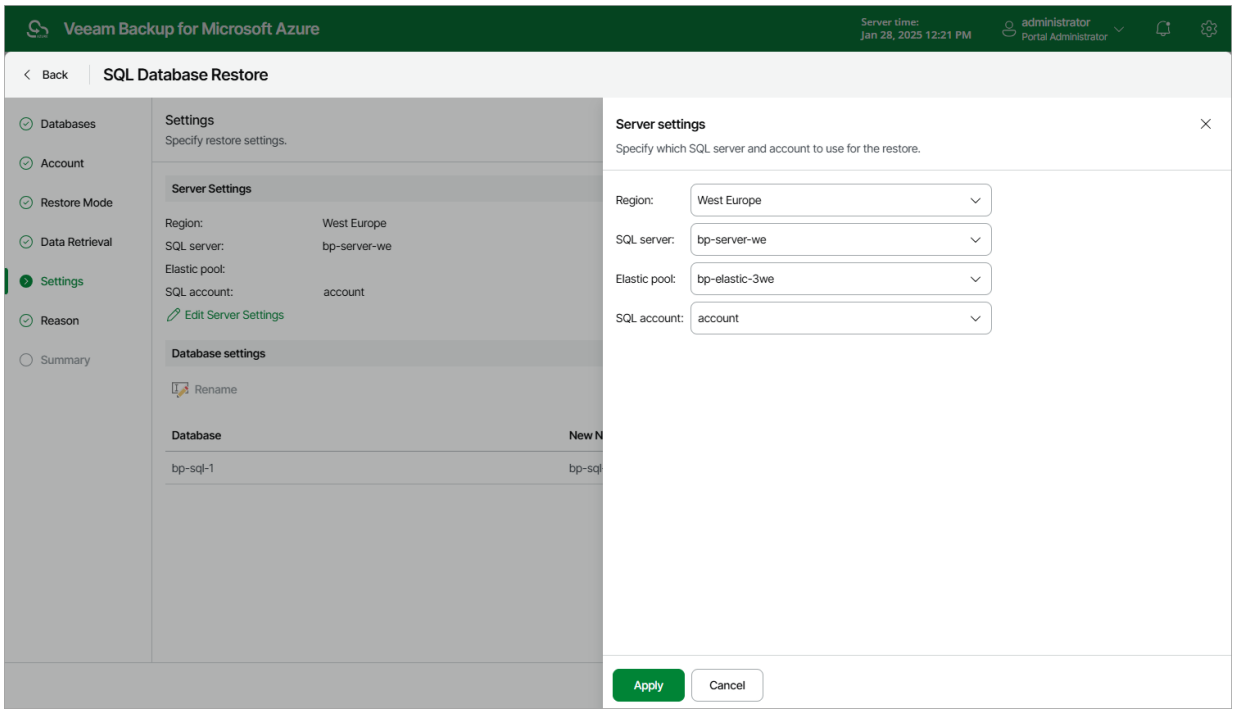
[This step applies only if you have selected the **Restore to a new location, or with different settings** option at the **Restore Mode** step of the wizard]

At the **Settings** step of the wizard, specify a SQL Server that will host the restored databases:

1. Click **Edit Server Settings** in the **Server Settings** section.
2. In the **Server settings** window, do the following:
   a. From the **Region** drop-down list, select an Azure region where the SQL Server that will host the restored database resides.
   b. From the **SQL server** drop-down list, select the target SQL Server.
   c. From the **Elastic pool** drop-down list, select an elastic pool to which the restored database will be added.

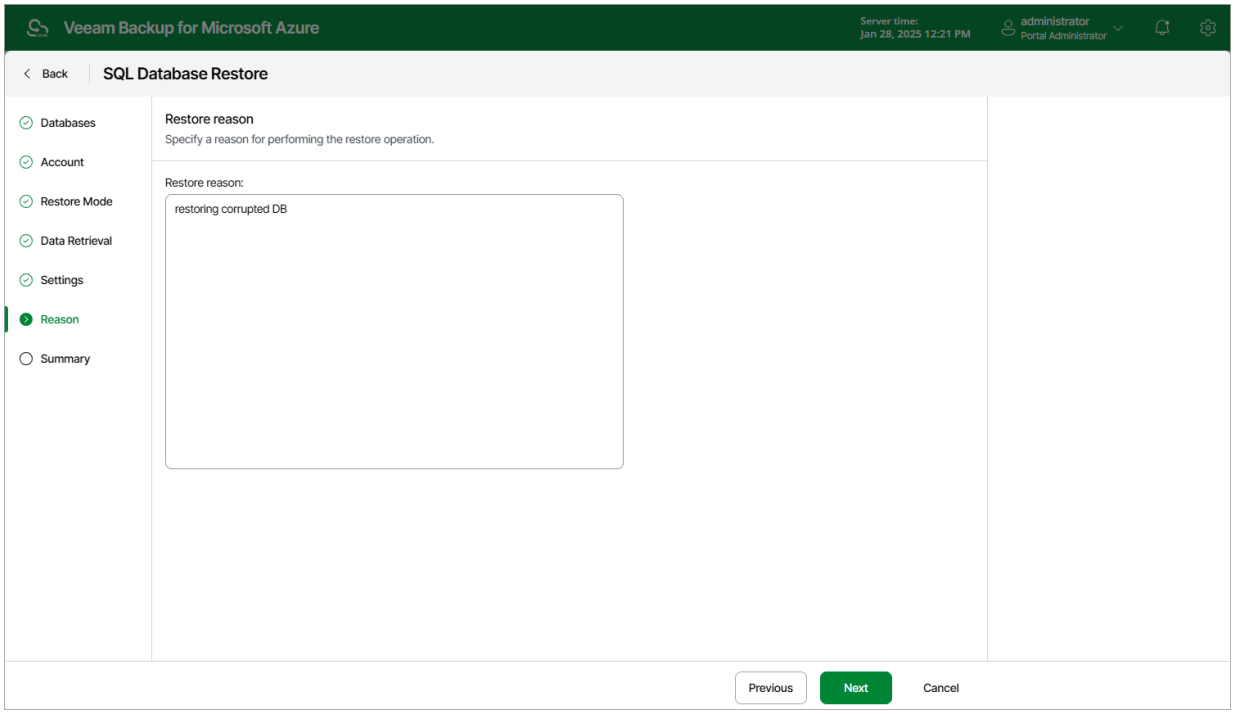
      For an elastic pool to be displayed in the list of available pools, it must be created in the Microsoft Azure portal as described in Microsoft Docs.
   d. From the **SQL account** drop-down list, choose an Azure SQL Server account that will be used to authenticate against the target SQL Server.

      For an Azure SQL Server account to be displayed in the list of available accounts, it must be added to Veeam Backup for Microsoft Azure as described in section Adding SMTP and Database Accounts.
   e. To save changes made to the server settings, click **Apply**.
3. Use the **Database settings** section to specify a new name for the restored database. To do that, select the database and click **Rename**.



# Step 8. Specify Restore Reason

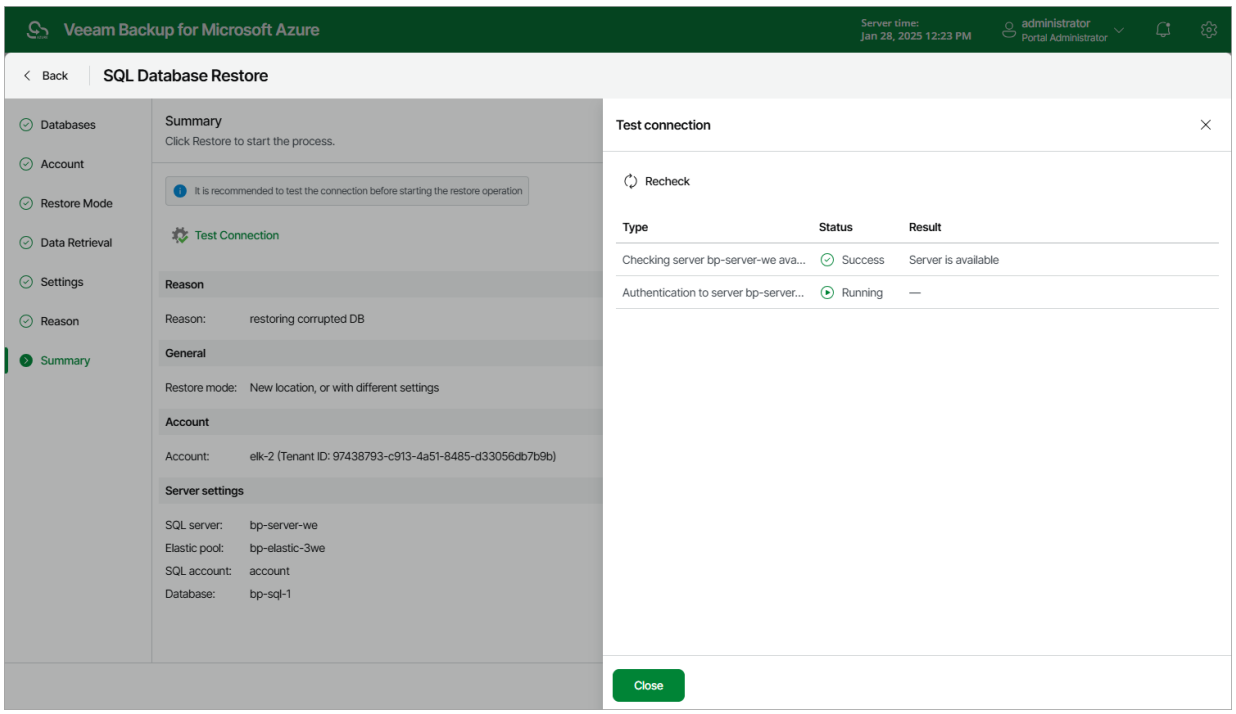
At the **Reason** step of the wizard, specify a reason for restoring the Azure SQL database. This information will be saved to the session history, and you will be able to reference it later.



# Step 9. Finish Working with Wizard

At the **Summary** step of the wizard, review summary information and click **Restore**.

> **TIP**
>
> It is recommended that you check the network connection status of the target SQL Server to verify whether Veeam Backup for Microsoft Azure will be able to connect to the server to perform the restore operation. To run the connection check, click **Test Connection**. Veeam Backup for Microsoft Azure will display the **Test connection** window where you can view the progress and results of the performed check.




# Fixing Network Issues

If the backup policy check reveals that network settings are not configured properly, Veeam Backup for Microsoft Azure will not be able to launch worker instances and thus perform the operation.

To fix network issues:

1. Close the **Test connection** window, and then click **Cancel** to close the **SQL Database Restore** wizard.
2. Depending on the error message received after the backup policy check, do the following:
   - Make sure that network settings are configured for each Azure region selected at step 7. For information on how to configure network settings for Azure regions, see Managing Worker Instances.
   - Make sure that virtual networks specified in network settings for Azure regions have access to the required Azure services. The required Azure services are listed in section Azure Services.
3. After network issues are fixed, you can start the **SQL Database Restore** wizard again.

# Cosmos DB Restore

The actions that you can perform with restore points of Cosmos DB accounts depend on whether you access the restore points using the Veeam Backup & Replication console or the Veeam Backup for Microsoft Azure Web UI.

# Performing Cosmos DB Restore Using Console

Veeam Backup & Replication allows you to restore an entire Cosmos DB account or its specific items from a restorable timestamp, or to restore the database of a Cosmos DB for PostgreSQL or a Cosmos DB for MongoDB account from a backup stored in a repository. To learn how Cosmos DB restore works, see Cosmos DB Restore.

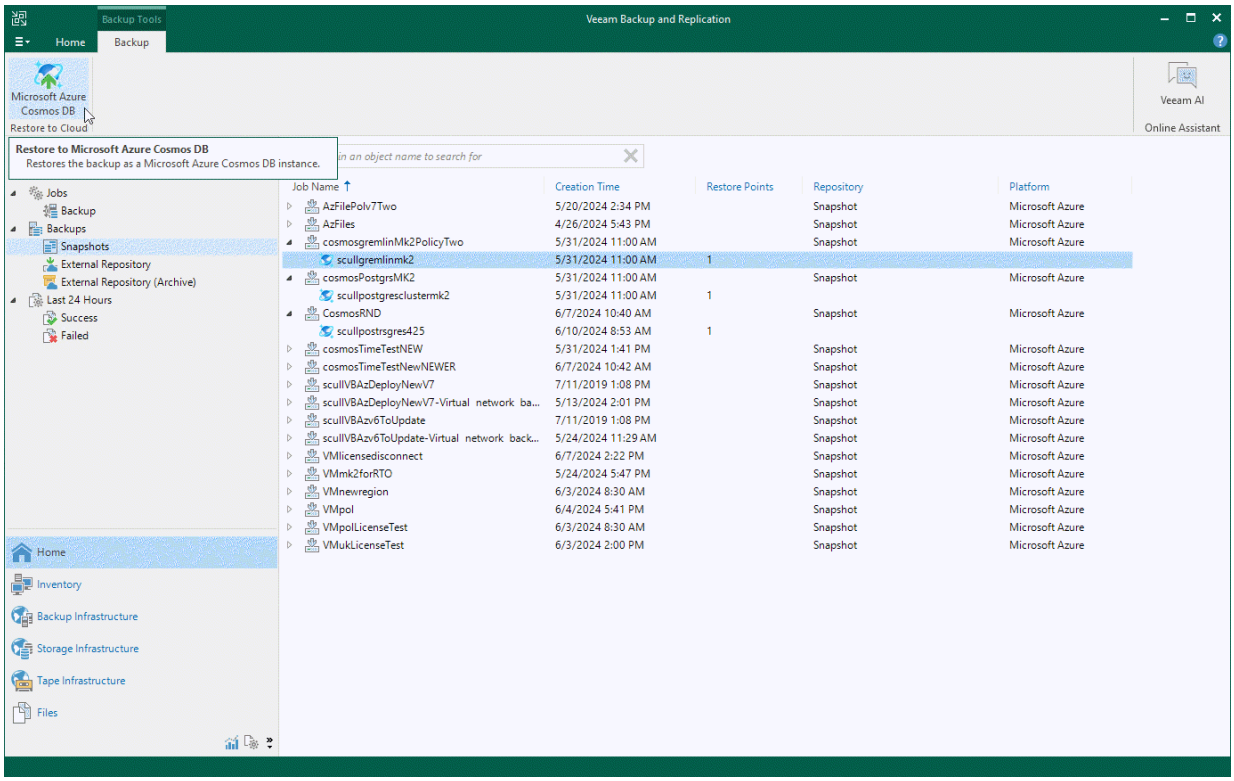
## Point-in-time Restore

To restore a Cosmos DB account from a restorable timestamp, do the following:

1. In the Veeam Backup & Replication console, open the **Home** view.
2. Navigate to **Backups** > **Snapshots**.
3. Expand the backup policy that protects the Cosmos DB account you want to restore, select the account and click **Microsoft Azure Cosmos DB** on the ribbon.

   Alternatively, you can right-click the selected subscription and click **Restore to Microsoft Azure Cosmos DB**.

Veeam Backup & Replication will open the **Cosmos DB Restore** wizard in a web browser. Complete the wizard as described in section Performing Point-in-time Restore.




## Restore From Repository

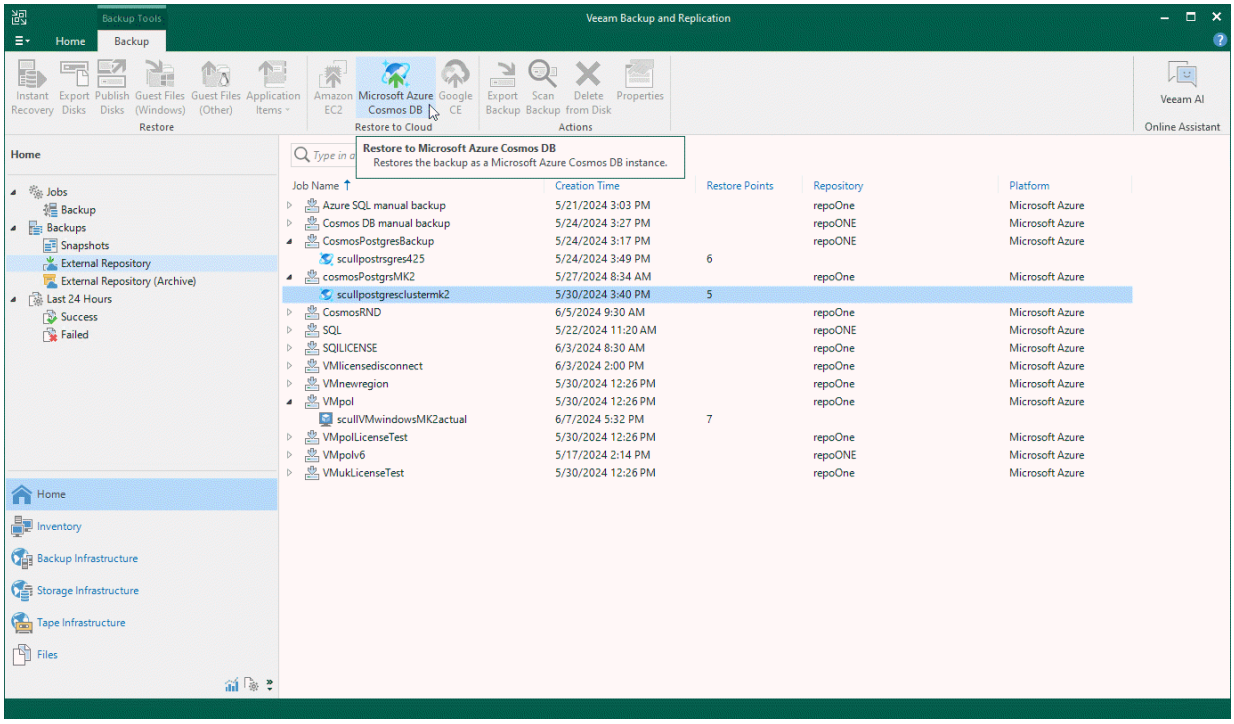
To restore the database of a Cosmos DB for PostgreSQL or a Cosmos DB for MongoDB account from a backup stored in a repository, do the following:

1. In the Veeam Backup & Replication console, open the **Home** view.
2. Navigate to **Backups** > **External Repository** or, to retrieve a backup stored in an archive repository, navigate to **Backups** > **External Repository (Archive)**.

3. Expand the backup policy that protects the database you want to restore, select the Cosmos DB account managing the database and click **Microsoft Azure Cosmos DB** on the ribbon.

   Alternatively, you can right-click the selected subscription and click **Restore to Microsoft Azure Cosmos DB**.

Veeam Backup & Replication will open the **Cosmos DB Restore** wizard in a web browser. Complete the wizard as described in section Performing Restore From Repository.



# Performing Cosmos DB Restore Using Web UI

Veeam Backup for Microsoft Azure offers the following restore options:

- Point-in-time restore — restores a Cosmos DB account from a timestamp to a new location.
- Restore from repository — restores the database of a Cosmos DB for PostgreSQL account or databases and collections of a Cosmos DB for MongoDB account from a backup stored in a repository to the original or to a new location.

> **IMPORTANT**
>
> Consider the following:
>
> - Due to Microsoft Azure limitations, Veeam Backup for Microsoft Azure does not support restore of Cosmos DB accounts encrypted using customer-managed keys. For more information, see Microsoft Docs.
> - Due to Microsoft Azure limitations, when restoring a Cosmos DB for PostgreSQL account that has the geo-redundant backup capability enabled, you can restore this account to its primary region only. Consider that the restored account will have the capability disabled, and you will not be able to change this setting for the account. For more information, see Microsoft Docs.

You can restore Cosmos DB data to the most recent state or to any available restore point.

## Performing Point-in-time Restore

In case a disaster strikes, you can restore an entire Cosmos DB account or its specific items from a timestamp. Veeam Backup for Microsoft Azure allows you to restore one Cosmos DB account at a time to a new location.

> **IMPORTANT**
>
> Consider the following:
>
> - Point-in-time restore is not available for Cosmos DB accounts that have the *Deleting* status.
> - Point-in-time restore is not available for Cosmos DB for PostgreSQL accounts that have either the *Deleted*, *Stopped* or *Dropping* status.
>
>   However, accounts with the *Deleted* status can still be restored if they have backups stored in repositories. To learn how to do that, see Performing Restore From Repository.

## How to Perform Cosmos DB Restore

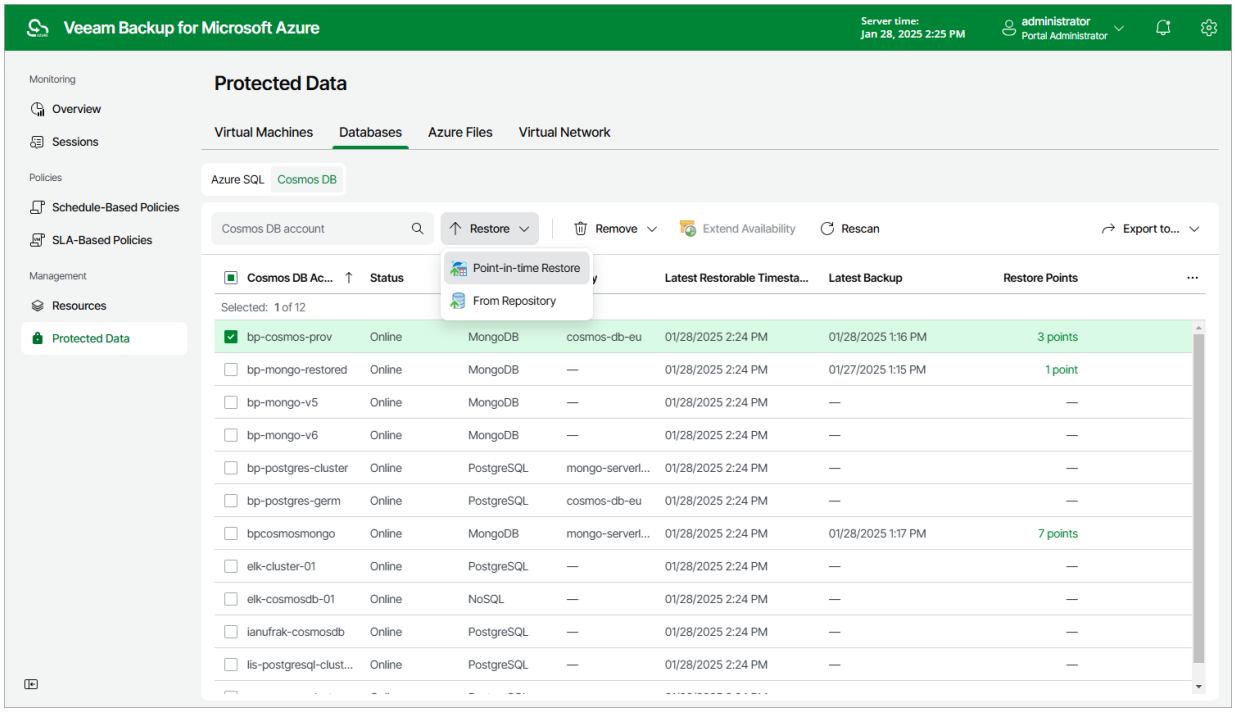
To restore a Cosmos DB account, do the following:

1. Launch the Cosmos DB Restore wizard.
2. Select a restore point.
3. Select a service account.
4. Configure restore settings.
5. Specify a restore reason.
6. Finish working with the wizard.

# Step 1. Launch Cosmos DB Restore Wizard

To launch the **Cosmos DB Restore** wizard, do the following:

1. Navigate to **Protected Data** > **Databases** > **Cosmos DB**.
2. Select the Cosmos DB account that you want to restore.
3. Click **Restore** > **Point-in-time Restore**.



# Step 2. Select Restore Point

At the **Restore Point** step of the wizard, select a timestamp that will be used to restore the selected Cosmos DB account. By default, Veeam Backup for Microsoft Azure uses the most recent valid timestamp. However, you can restore the account data to an earlier state.

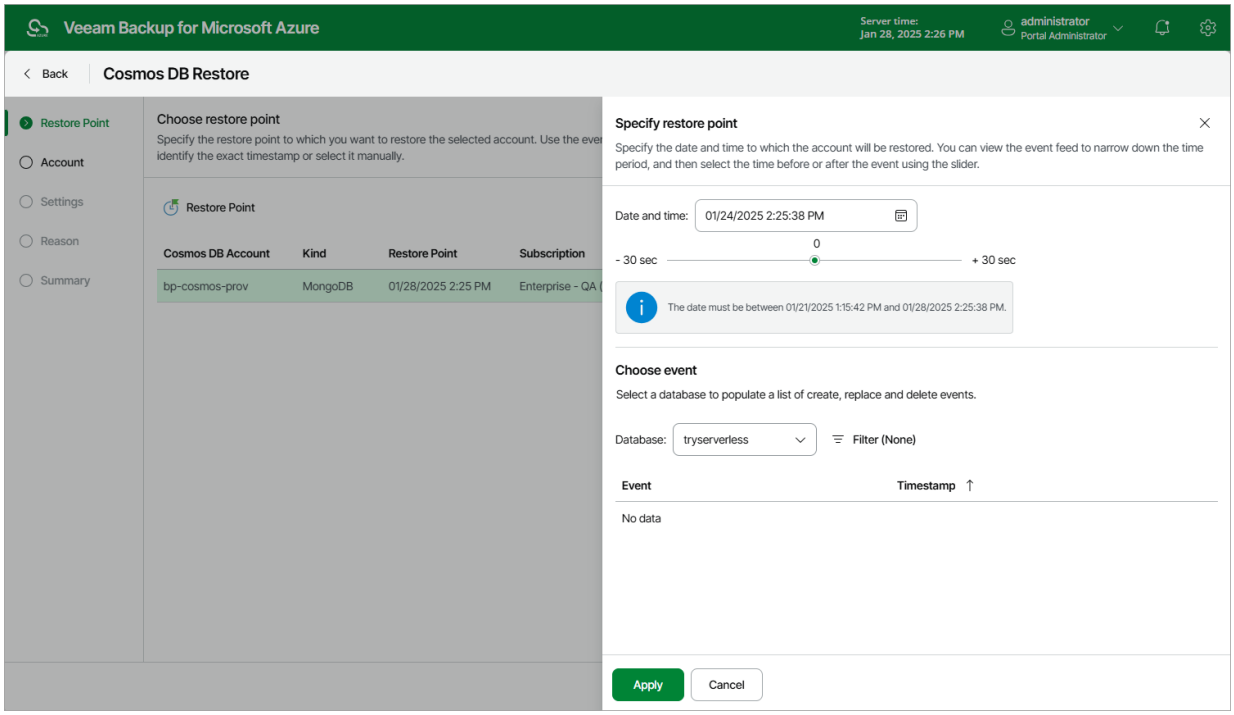
To select a timestamp, do the following:

1. Click **Restore Point**.
2. In the **Specify restore point** window, use either of the following options:
   - Specify the timestamp manually. To do that, click the calendar icon next to the **Date and time** field, choose the timestamp within the available restore window, and click **Apply**.
   - Choose a specific event to identify the necessary timestamp. To do that, select a database whose event you want to use, choose the event from the list of available events, and click **Apply**.

     To adjust the timestamp, you can use the slider below the **Date and time** field.

**NOTES**

- You can only choose an event when restoring Cosmos DB accounts created using the NoSQL, MongoDB RU-based, Apache Gremlin and Table APIs.
- If you want to select a timestamp that is close to the beginning of the restore window, keep in mind that this timestamp may become outdated while you are completing the **Cosmos DB Restore** wizard, which may result in the restore operation failure. That is why it is recommended that you plan the time that you will need to configure the restore settings and choose timestamps accordingly — typically, it takes about 5 minutes to complete the wizard.

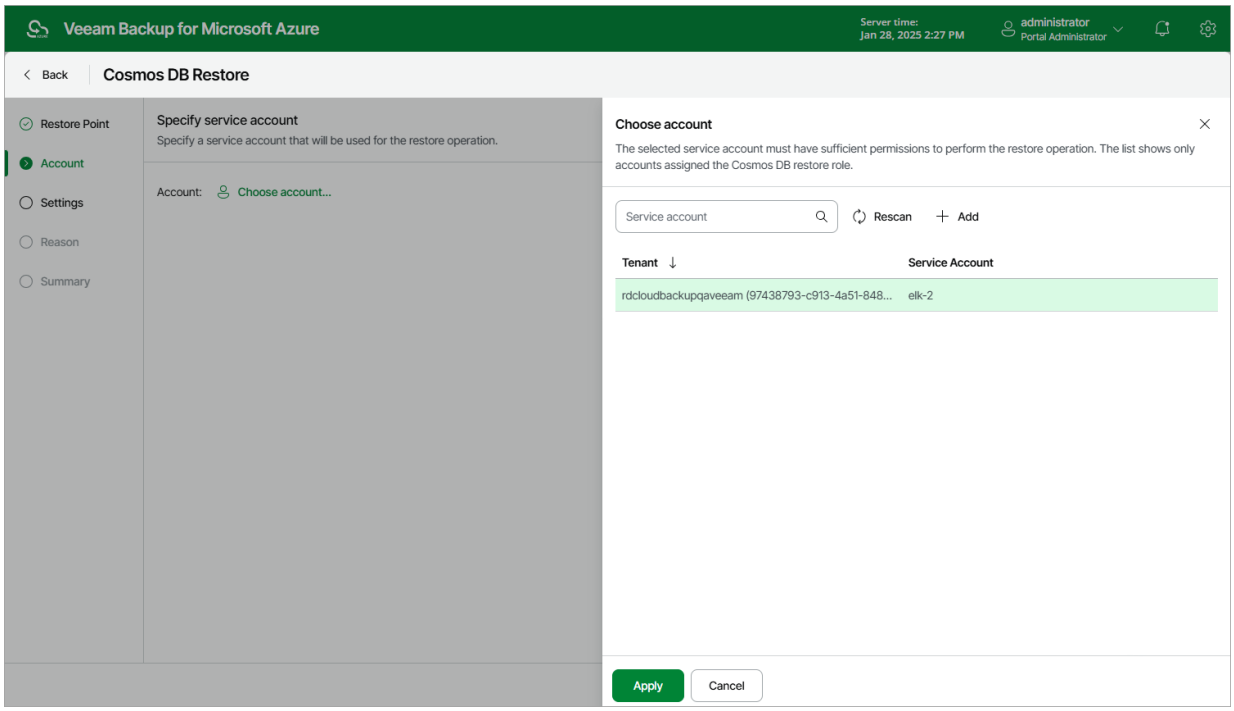


# Step 3. Select Service Account

At the **Account** step of the wizard, select a service account whose permissions Veeam Backup for Microsoft Azure will use to perform the restore operation.

1. Click **Choose account**.
2. In the **Choose account** window, select the necessary account and click **Apply**. The specified service account must be assigned permissions listed in section Cosmos DB Permissions.

   For a service account to be displayed in the list of available accounts, it must be added to Veeam Backup for Microsoft Azure and assigned the *Cosmos DB Restore* operational role as described in section Adding Service Accounts. If you have not added the necessary service account to Veeam Backup for Microsoft Azure beforehand, you can do it without closing the **Cosmos DB Restore** wizard. To do that, click **Add** and complete the **Add Account** wizard.



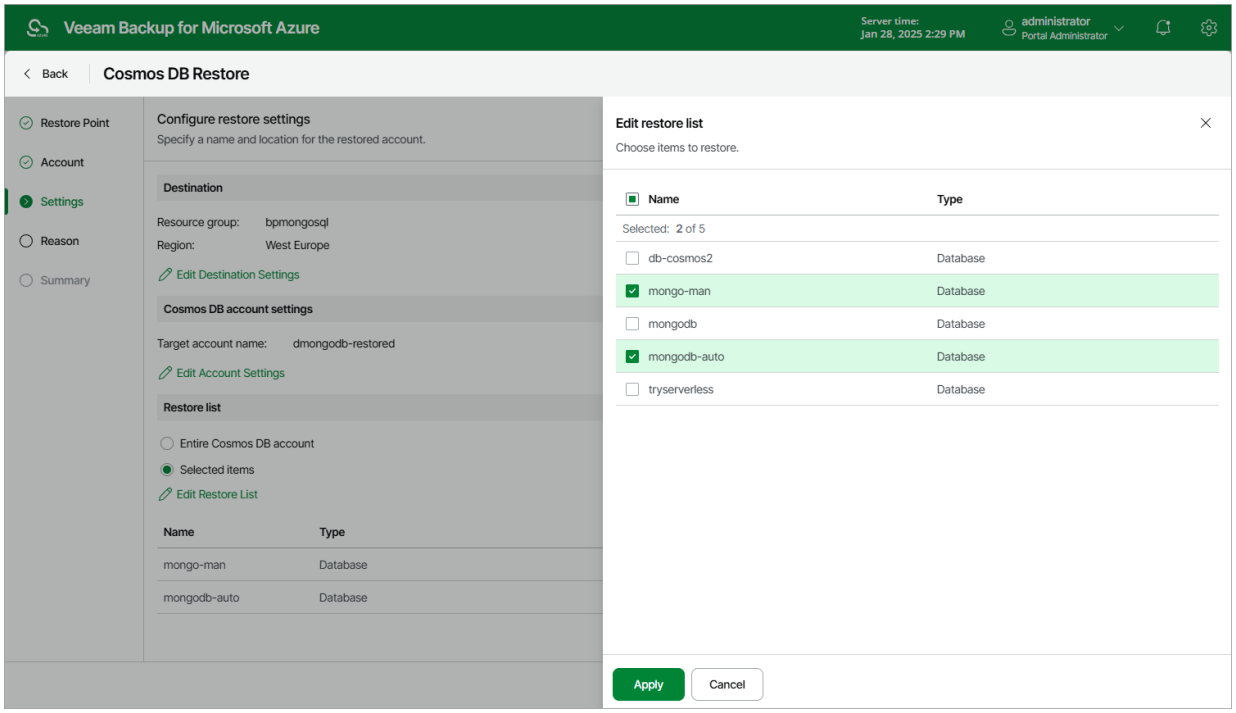
# Step 4. Configure Restore Settings

At the **Settings** step of the wizard, do the followng:

1. In the **Destination** section, click **Edit Destination Settings** to select a resource group and an Azure region to which the account will be restored.
2. In the **Cosmos DB account settings** section, click **Edit Account Settings** to specify a new name for the restored account.
3. [Applies only to Cosmos DB accounts created using the NoSQL, MongoDB RU-based, Apache Gremlin and Table APIs] In the **Restore list** section, choose whether you want to restore the entire Cosmos DB account or its specific items only. If you select the **Selected items** option, you must also specify the items explicitly — to do that, click **Edit Restore List**.

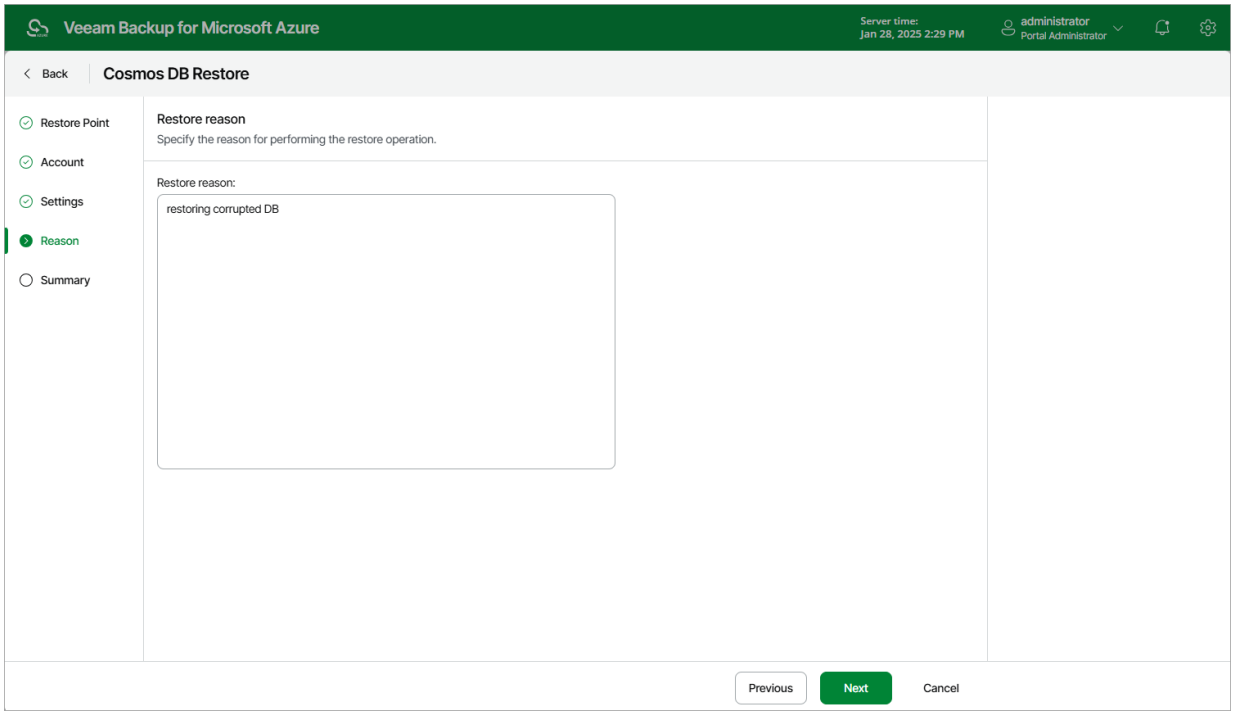
NOTES

- You can choose a resource group only when restoring a Cosmos DB account created using the NoSQL, MongoDB RU-based, Apache Gremlin or Table API. However, you will be able to restore this account only to the region where the source Cosmos DB account or its replica resided.
- When restoring a Cosmos DB for PostgreSQL account, you can choose a region only if the account has the geo-redundant backup capability enabled. However, due to Microsoft Azure limitations, you will be able to restore this account to its primary region only. Consider that the restored account will have the capability disabled, and you will not be able to change this setting for the account. For more information, see Microsoft Docs.



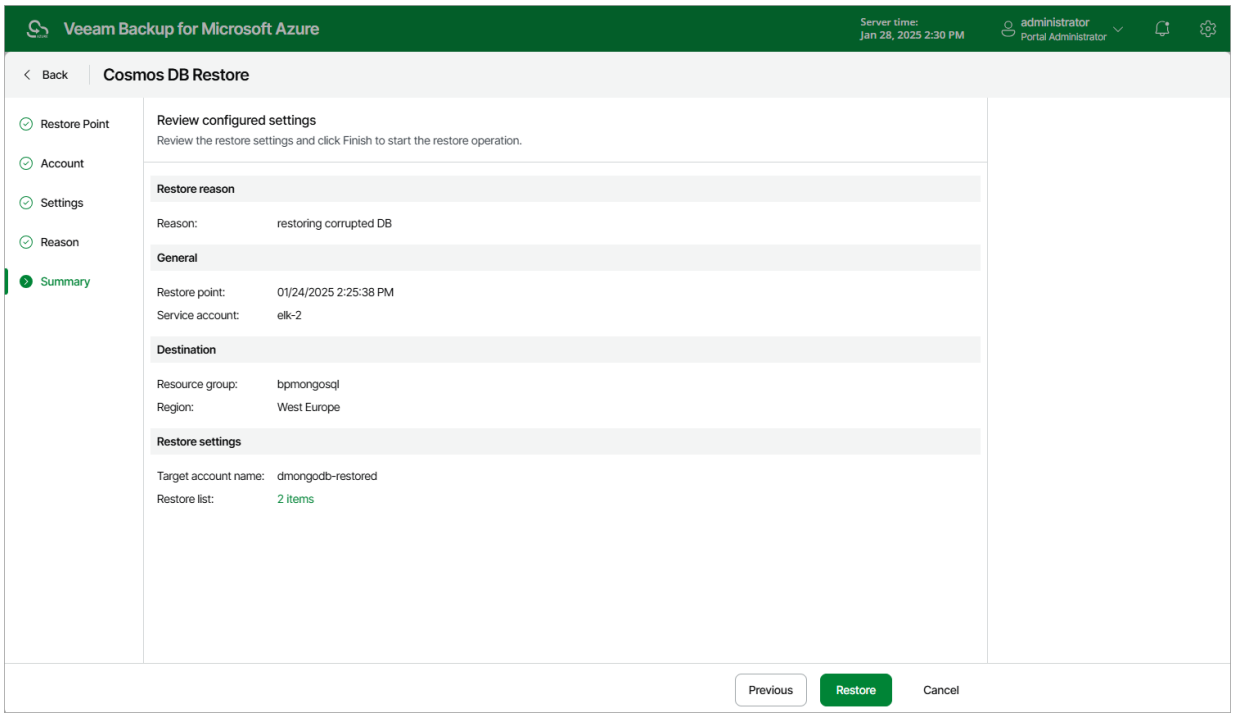
# Step 5. Specify Restore Reason

At the **Reason** step of the wizard, specify a reason for restoring the Cosmos DB account. This information will be saved to the session history, and you will be able to reference it later.



## Step 6. Finish Working with Wizard

At the **Summary** step of the wizard, review summary information and click **Finish**.




# Performing Restore From Repository

In case a disaster strikes, you can restore the database of a Cosmos DB for PostgreSQL account or databases and collections of a Cosmos DB for MongoDB account from a backup stored in a repository. Veeam Backup for Microsoft Azure allows you to restore one database at a time, to the original or to a new location.

# Before You Begin

Consider the following prerequisites:

- To restore a database from a backup that is stored in an archive repository, you must retrieve the archived data first. You can either retrieve the archived data manually before you begin the restore operation, or launch the data retrieval process right from the restore wizard. To learn how to retrieve data manually, see Retrieving Data from Archive.
- If you plan to restore databases and collections of a Cosmos DB for MongoDB account, make sure that the MongoDB version of the target account to which you want to restore the data is not earlier than the MongoDB version of the source account that originally managed these databases and collections.

# How to Perform Cosmos DB Restore

To restore the database of a Cosmos DB for PostgreSQL account or databases and collections of a Cosmos DB for MongoDB account, do the following:

1. Launch the Cosmos DB Restore wizard.
2. Select a restore point.
3. Select a service account.

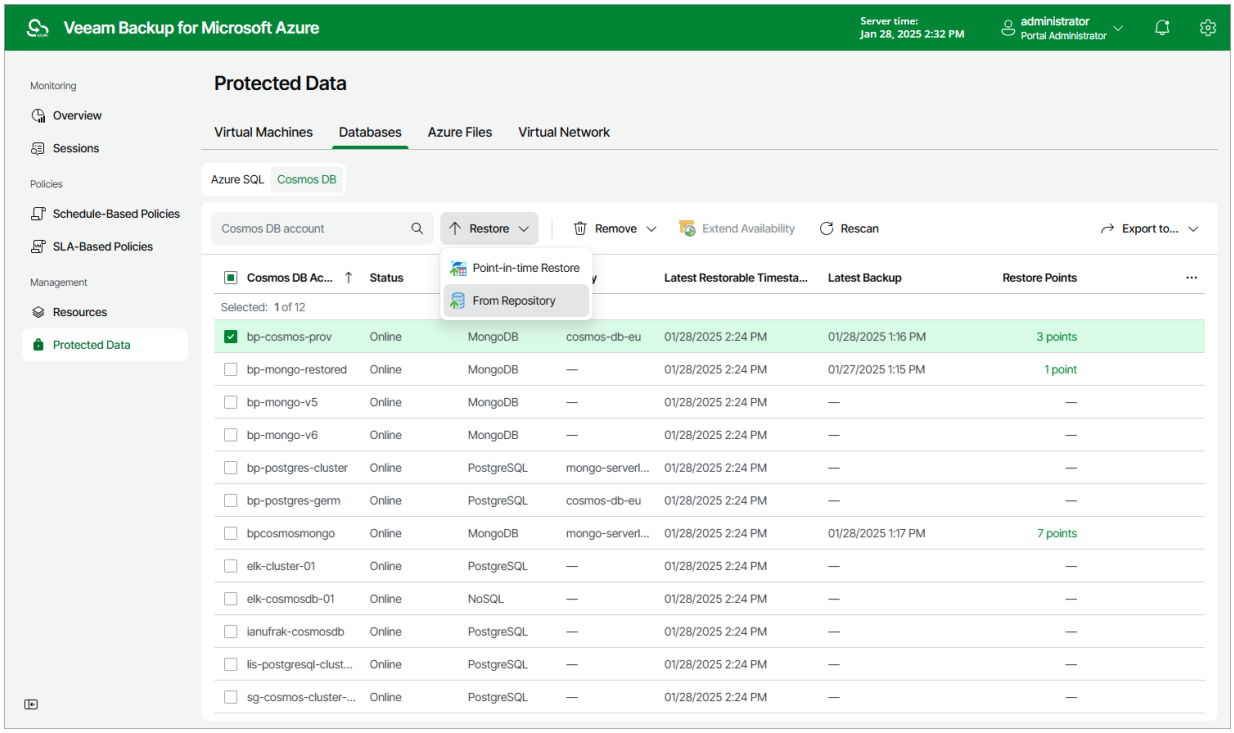
4. Specify data retrieval settings.
5. Configure restore settings.
6. Specify a restore reason.
7. Finish working with the wizard.

# Step 1. Launch Cosmos DB Restore Wizard

To launch the **Cosmos DB Restore** wizard, do the following:

1. Navigate to **Protected Data** > **Databases** > **Cosmos DB**.
2. Select the Cosmos DB account that you want to restore.
3. Click **Restore** > **From Repository**.

   Alternatively, click the link in the **Restore Points** column. Then, in the **Available Restore Points** window, select the necessary restore point and click **Restore**.



# Step 2. Select Restore Point

At the **Restore Point** step of the wizard, select a restore point that will be used to restore the database of the selected Cosmos DB for PostgreSQL account or databases and collections of a Cosmos DB for MongoDB account. By default, Veeam Backup for Microsoft Azure uses the most recent valid restore point. However, you can restore the database data to an earlier state.

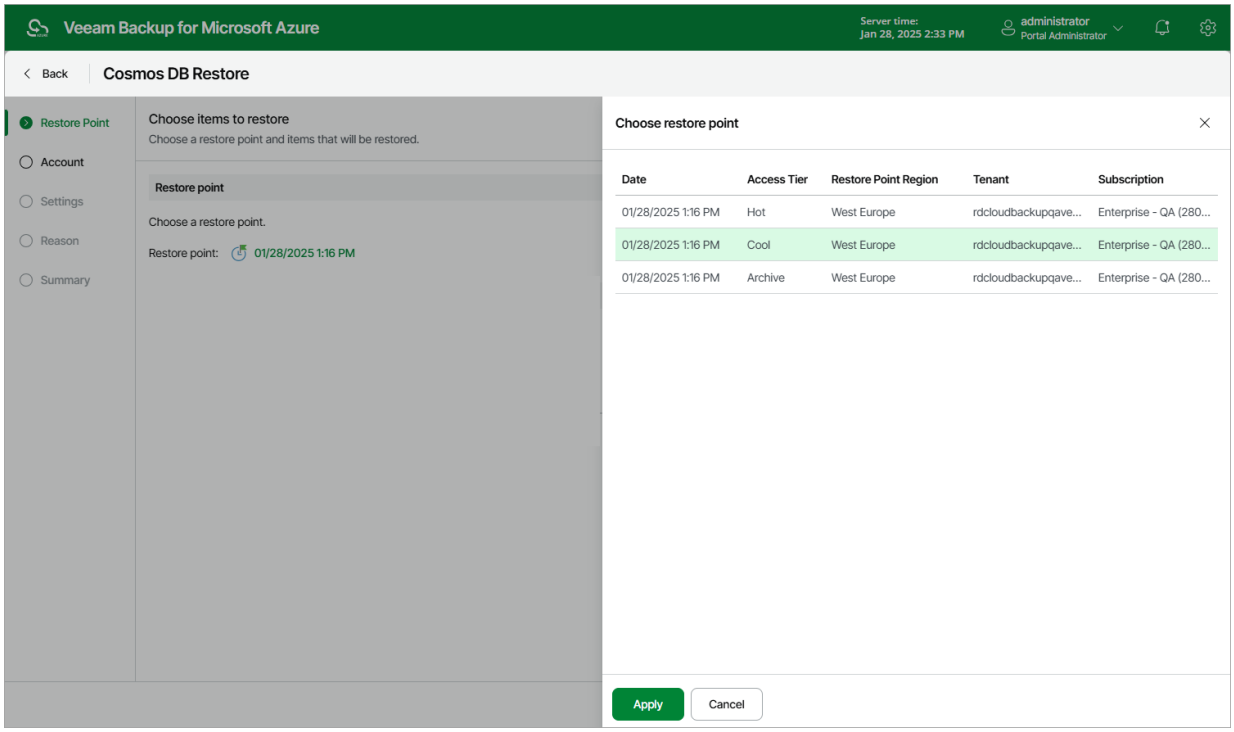
> **IMPORTANT**
>
> If you select a restore point stored in an archive repository and the same restore point is also available in a regular repository, Veeam Backup for Microsoft Azure will display the confirmation window where you must choose whether you want to use the archived or regular restore point to perform the restore operation.

To select a restore point, do the following:

1. Click **Restore Point**.
2. In the **Specify restore point** window, select the necessary restore point and click **Apply**.

   To help you choose a restore point, Veeam Backup for Microsoft Azure provides the following information on each available restore point:

   - **Date** – the date when the restore point was created.
   - **Access Tier** – the storage tier of a backup repository where the restore point is stored.
   - **Restore Point Region** – an Azure region where the restore point resides.
   - **Tenant** – a Microsoft Entra tenant to which the restore point belongs.
   - **Subscription** – an Azure subscription with which the restore point is associated.



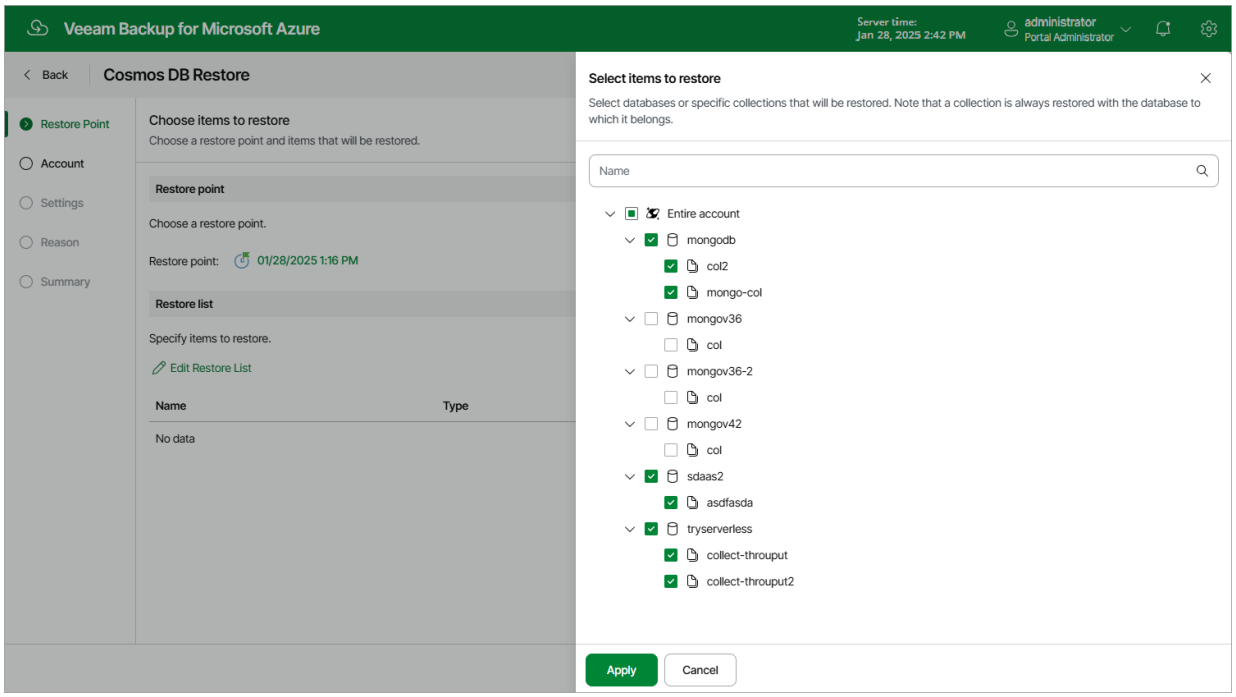
# Selecting Items To Restore

[Applies when performing restore for Cosmos DB for MongoDB accounts only]

To restore granular databases and collections of a Cosmos DB for MongoDB account, do the following:

1. In the **Restore list** section, click **Edit Restore List**.
2. In the **Select items to restore** window, select the necessary databases or collections and click **Apply**.

> **IMPORTANT**
>
> If you select a a collection, Veeam Backup for Microsoft Azure will restore it together with the database to which this collection belongs.

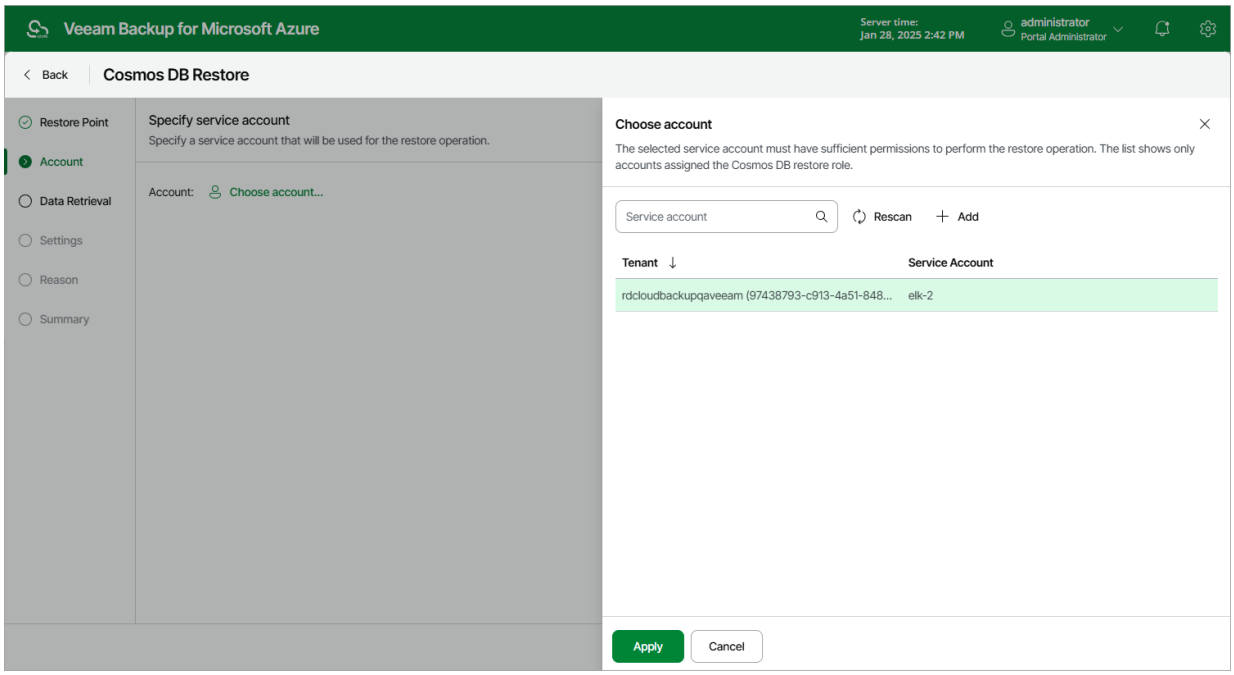


# Step 3. Select Service Account

At the **Account** step of the wizard, select a service account whose permissions Veeam Backup for Microsoft Azure will use to perform the restore operation.

1. Click **Choose account**.
2. In the **Choose service account** window, select the necessary account and click **Apply**. The specified service account must be assigned permissions listed in section Cosmos DB Permissions.

   For a service account to be displayed in the list of available accounts, it must be added to Veeam Backup for Microsoft Azure and assigned the *Cosmos DB Restore* operational role as described in section Adding Service Accounts. If you have not added the necessary service account to Veeam Backup for Microsoft Azure beforehand, you can do it without closing the **Cosmos DB Restore** wizard. To do that, click **Add** and complete the **Add Account** wizard.



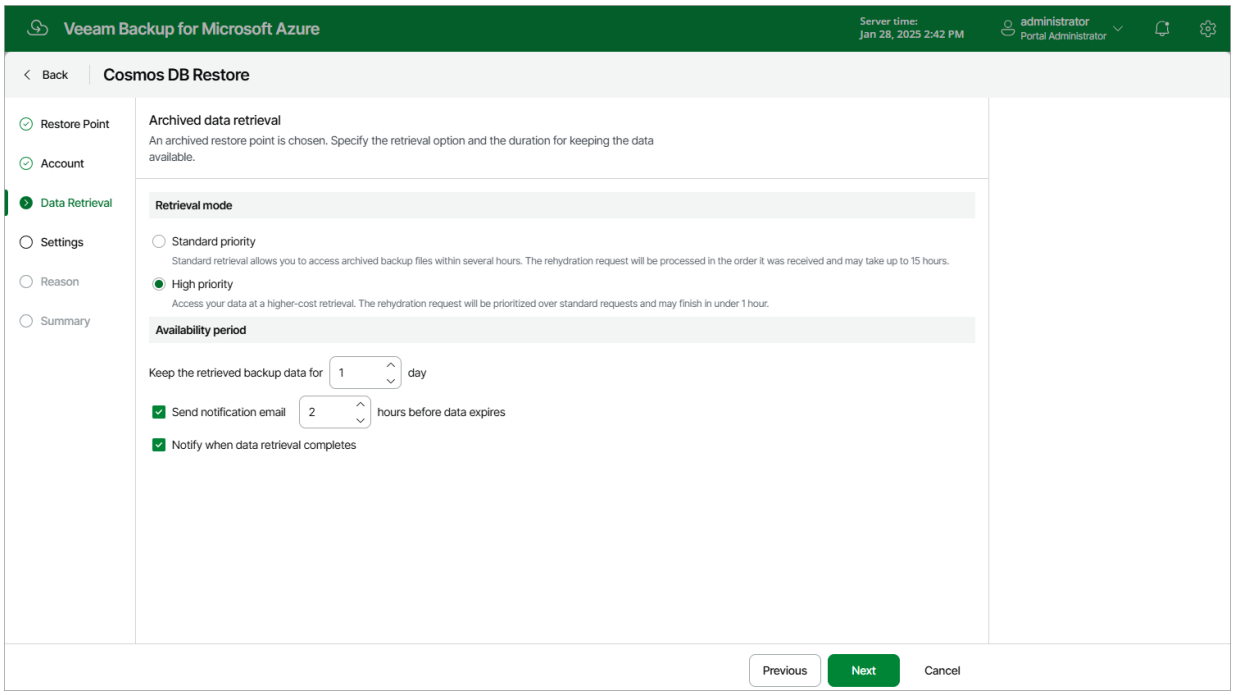
# Step 4. Specify Retrieval Settings

[This step applies only if you have selected a restore point stored in an archive repository at the **Restore Point** step of the wizard]

At the **Data retrieval** step of the wizard, choose a retrieval mode and specify a period for which you want to keep the data available.

1. In the **Retrieval mode** section, select the retrieval mode that Veeam Backup for Microsoft Azure will use to retrieve the archived data, and click **Save**. For more information on data retrieval modes, see Retrieving Data From Archive.
2. In the **Availability period** section, specify the number of days for which you want to keep the data available for restore operations. You can manually extend the availability period later if required.

> **TIP**
>
> If you want to receive an email notification when data availability period is about to expire, select the **Send notification email** check box and choose when you want to be notified (that is, the number of hours remaining until data expiration).



## Step 5. Configure Restore Settings

At the **Settings** step of the wizard, choose whether you want to restore the database to the original or to a custom location, and specify a region and an account to which the selected items will be restored.

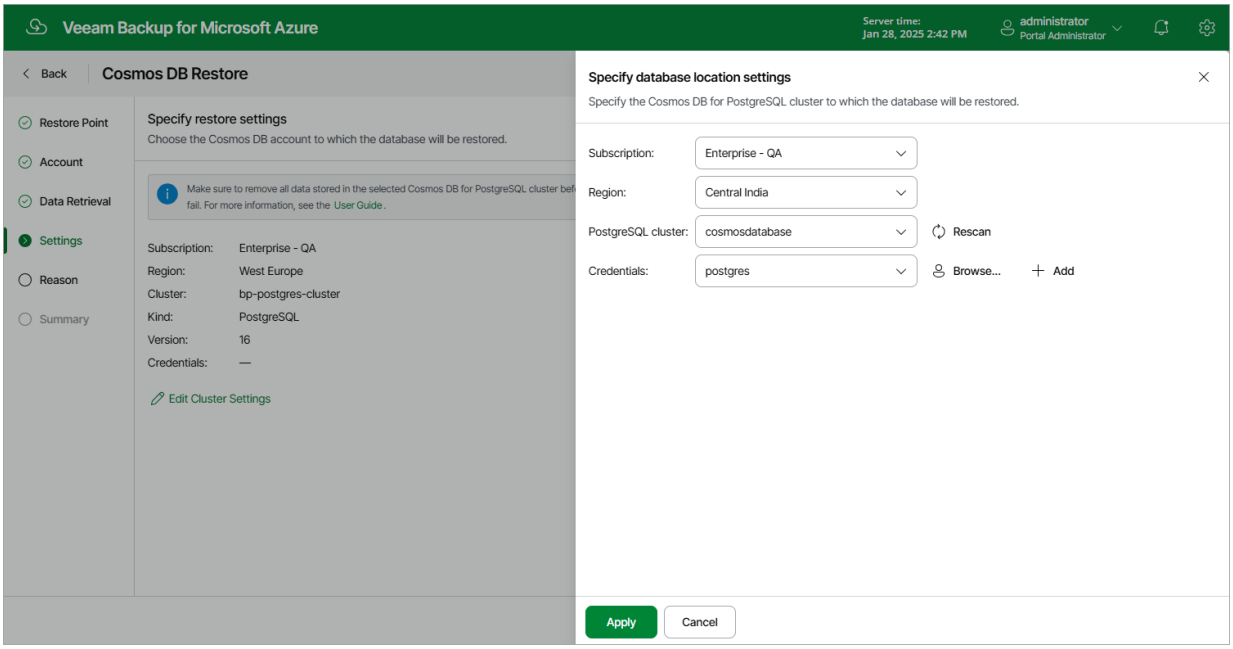
# Configuring Cosmos DB For PostgreSQL Account Restore Settings

To choose the location to which the database of a Cosmos DB for PostgreSQL account will be restored, click **Edit Cluster Settings**, and then select an Azure subscription, an Azure region and a Cosmos DB for PostgreSQL cluster to which the database will be restored.

> **IMPORTANT**
>
> When selecting a Cosmos DB for PostgreSQL cluster, make sure that the selected cluster does not contain any data and has sufficient storage capacity to accommodate the restored database. Otherwise, Veeam Backup for Microsoft Azure will fail to perform the restore operation.

You must also specify a database account that will be used to restore database data to the selected location. It is recommended that you select an account that has the built-in *citus* role.

For a database account to be displayed in the **Credentials** list, it must be added to Veeam Backup for Microsoft Azure as described in section Adding SMTP and Database Accounts. If you have not added the necessary account to Veeam Backup for Microsoft Azure beforehand, you can do it without closing the **Cosmos DB Restore** wizard. To do that, click **Add** and complete the Add Account wizard.



# Configuring Cosmos DB For MongoDB Account Restore Settings

To choose the location to which the selected databases and collections of a Cosmos DB for MongoDB account will be restored, click **Edit Account Settings**, and then select an Azure subscription, an Azure region and a Cosmos DB for MongoDB account to which the databases and collections will be restored. If you want to specify a new name for a restored database or collection, select the necessary item in the **Database settings** section, click **Rename** and provide a new name for the item. Consider that Veeam Backup for Microsoft Azure uses the read-write primary/secondary keys to restore database and collection data to the selected location. For more information, see Microsoft Docs.

> **IMPORTANT**
>
> When selecting a Cosmos DB for MongoDB account, make sure that the MongoDB version of this account is not earlier than the MongoDB version of the Cosmos DB for MongoDB account that originally managed the databases and collections.

You can restore the selected databases and collections to a Cosmos DB for MongoDB account created in either of the following capacity modes: serverless throughput or provisioned throughput. A capacity mode is a native Microsoft Azure capability that allows you to manage costs of all database operations based on throughput (Request Units per second, RU/s). The serverless throughput capacity mode implies that a Cosmos DB for MongoDB account is billed for consumed RU/s only, while the provisioned throughput capacity mode allows you to set a dynamic or specific maximum number of RU/s. For more information on capacity modes, see Microsoft Docs.

When restoring databases and collections to a Cosmos DB for MongoDB account created in the provisioned throughput capacity mode, Veeam Backup for Microsoft Azure automatically re-uses the originally configured throughput settings (if any); however, you can change these settings, if necessary. If the restored databases and collections were originally managed by a Cosmos DB for MongoDB account created in the serverless throughput capacity mode, you must configure throughput settings manually.

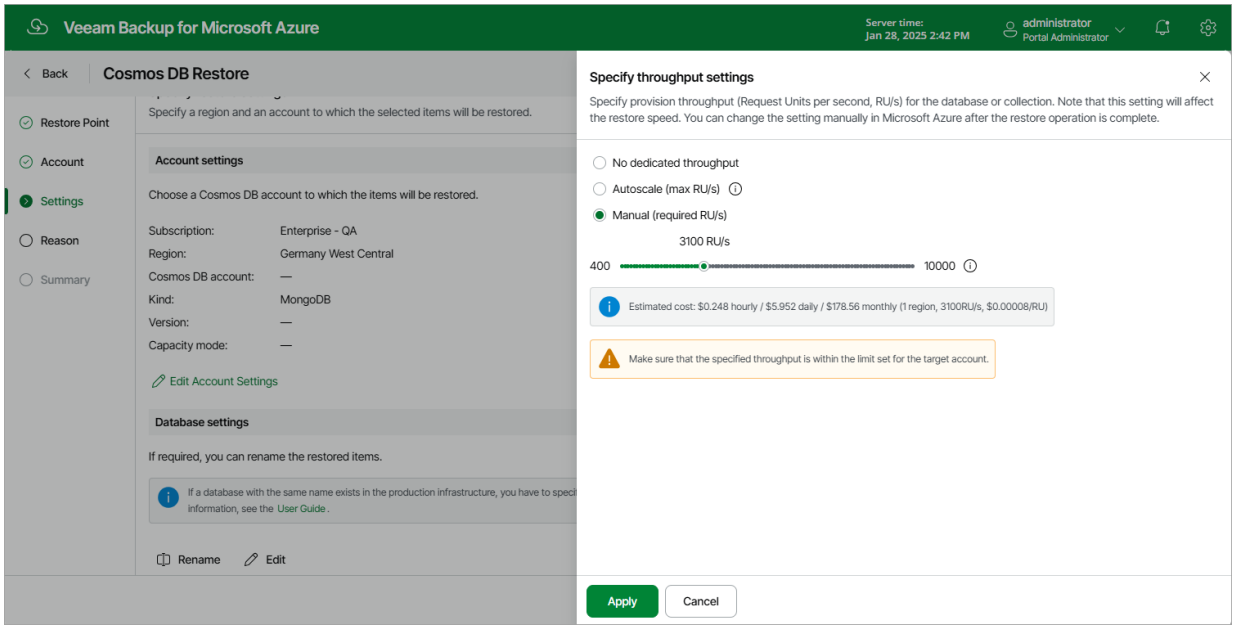
> **IMPORTANT**
>
> When configuring throughput settings, you must specify these settings for at least one granularity level (either for a database or for each of its collections). For more information, see Microsoft Docs.

To specify throughput settings for a database or collection, do the following:

1. In the **Database settings** section, choose an item for which you want to specify the throughput and click **Edit**.
2. In the **Specify throughput settings** window, choose either of the following options:
   - **No dedicated throughput** — if you select this option for a collection, the collection will share the throughput specified for the database to which this collection belongs; if you select this option for a database, you must specify throughput settings individually for each collection that belongs to this database.
   - **Autoscale** — if you select this option, Microsoft Azure will automatically scale the throughput depending on the usage, within the range limited by the maximum number of RU/s you set on the slider.
   - **Manual** — if you select this option, Microsoft Azure will assign the exact throughput based on the number of RU/s that you set on the slider.

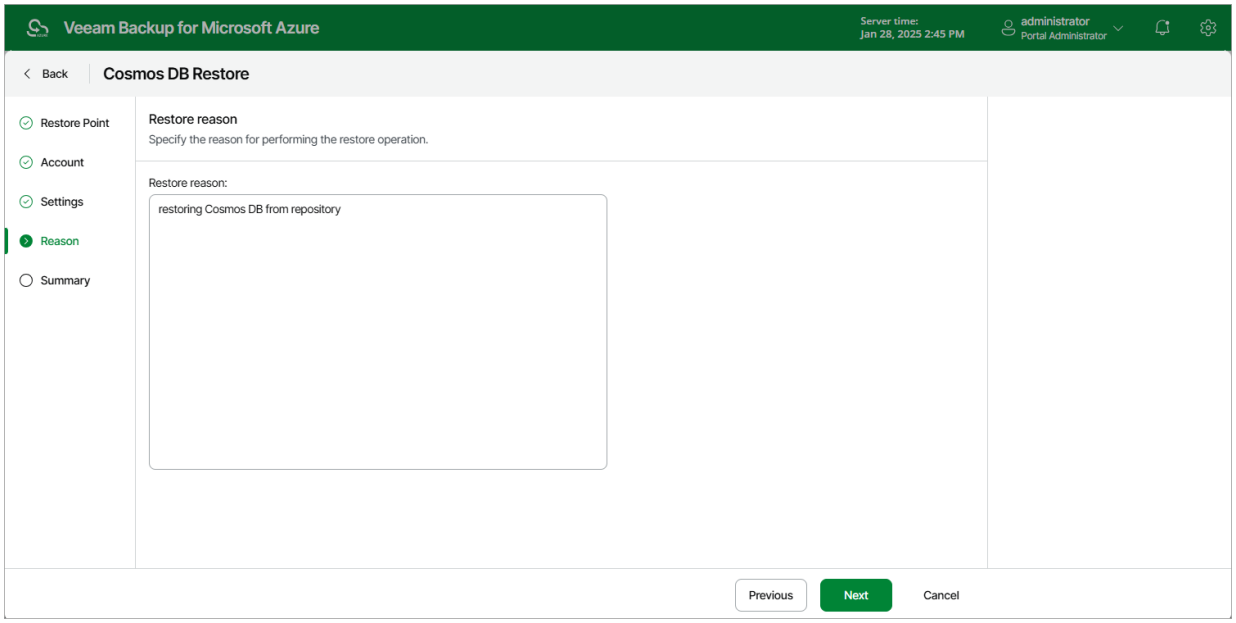
### NOTES

If you select the **Autoscale** or **Manual** option, make sure that the number of RU/s you set on the slider is within the limit set for the target account in Microsoft Azure. The slider is limited by 10000 RU/s — to be able to select a greater number, you can perform the restore operation by sending the HTTP POST request to the `/api/v8/restorePoints/cosmosDb/repository/{restorePointId}/restore` endpoint as described in the Veeam Backup for Microsoft Azure REST API Reference, section Cosmos DB Restore Points.



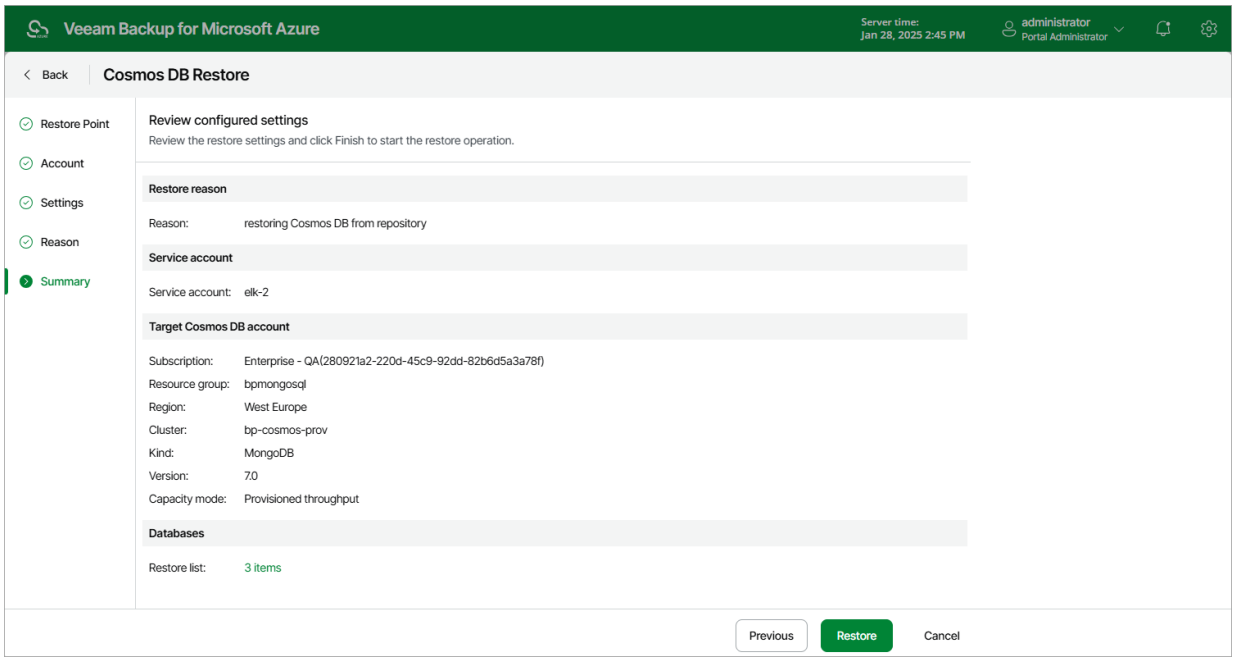
# Step 6. Specify Restore Reason

At the **Reason** step of the wizard, specify a reason for restoring the database. This information will be saved to the session history, and you will be able to reference it later.



# Step 7. Finish Working with Wizard

At the **Summary** step of the wizard, review summary information and click **Finish**.



# File Share Restore

The actions that you can perform with restore points of Azure file shares depend on whether you access the restore points using the Veeam Backup & Replication console or the Veeam Backup for Microsoft Azure Web UI.

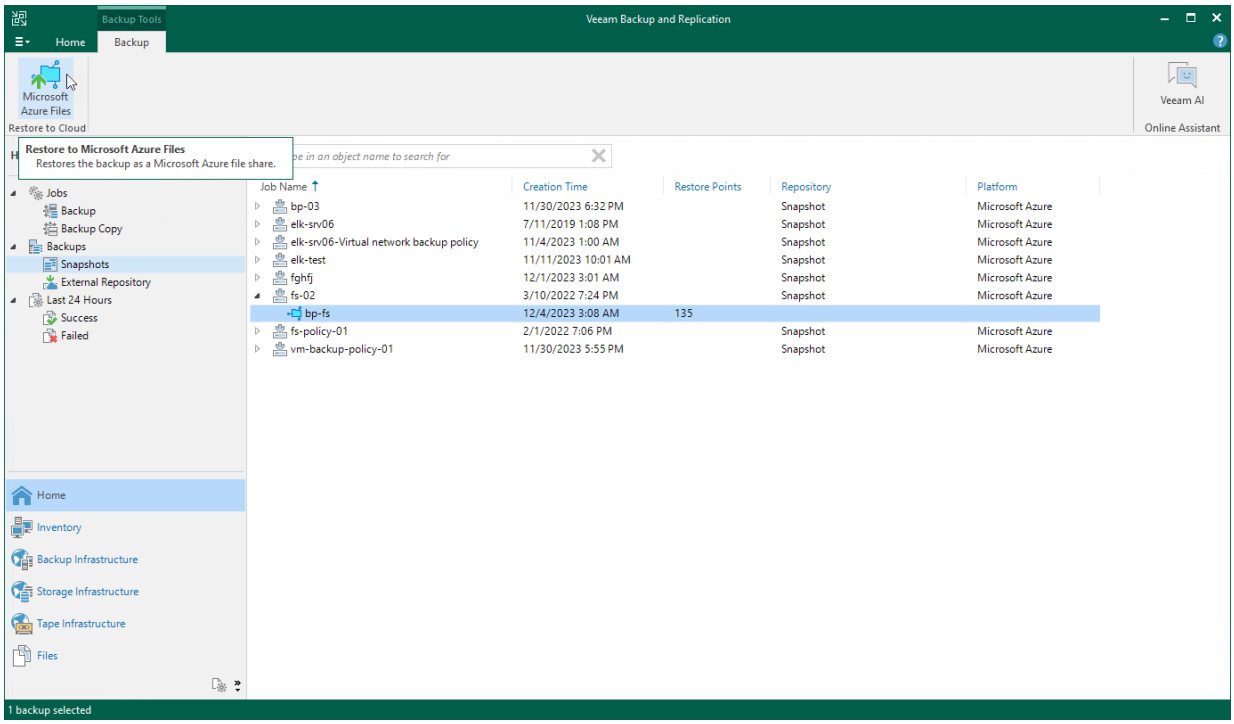
# Performing File Share Restore Using Console

You can recover corrupted or missing files of an Azure file share only using the backup appliance Web UI. However, you can launch the **Azure Files File-level Recovery** wizard directly from the Veeam Backup & Replication console to start the restore operation:

1. In the Veeam Backup & Replication console, open the **Home** view.
2. Navigate to **Backups** > **Snapshots**.
3. Expand the backup policy that protects the Azure file share that hosts files you want to recover, select the necessary file share and click **Microsoft Azure Files** on the ribbon.

   Alternatively, you can right-click the selected file share and click **Restore to Microsoft Azure Files**.

Veeam Backup & Replication will open the **Azure Files File-level Recovery** wizard in a web browser. Complete the wizard as described in section Performing Azure File Share Restore.



# Performing File Share Restore Using Web UI

In case a disaster strikes, you can recover corrupted or missing files of an Azure file share from a cloud-native snapshot. Veeam Backup for Microsoft Azure allows you to restore files and folders to the original file share or to another file share.

> **IMPORTANT**
>
> The **Allow storage account key access** option for Shared Key authorization must be enabled for both the storage accounts where the protected file shares reside and the storage accounts where the file shares to which you plan to restore files and folders reside — otherwise, the restore operation will fail. For more information on the Shared Key authorization, see Microsoft Docs.

## How to Perform File Share Restore

To restore files and folders of a protected Azure file share, do the following:

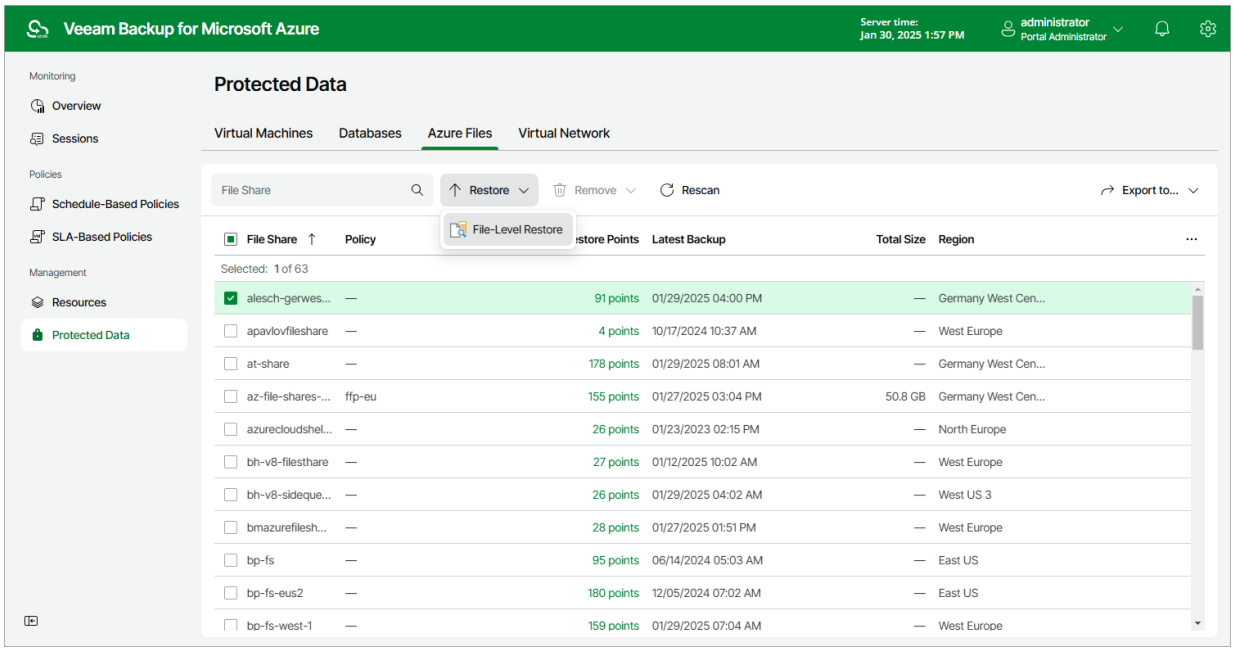
1. Launch Azure Files File-Level Recovery wizard.
2. Select a service account.
3. Choose a restore mode.
4. Specify a restore reason.
5. Finish working with the wizard — start a recovery session.
6. Select a restore point.
7. Choose files and folders to restore.
8. Stop the restore session.

# Step 1. Launch Azure Files File-Level Recovery Wizard

To launch the **Azure Files File-Level Recovery** wizard, do the following:

1. Navigate to **Protected Data** > **Azure Files**.
2. Select the Azure file share that you want to restore.
3. Click **Restore** > **File-Level Restore**.

   By default, Veeam Backup for Microsoft Azure uses the most recent valid restore point. However, you can restore files and folders to an earlier state.

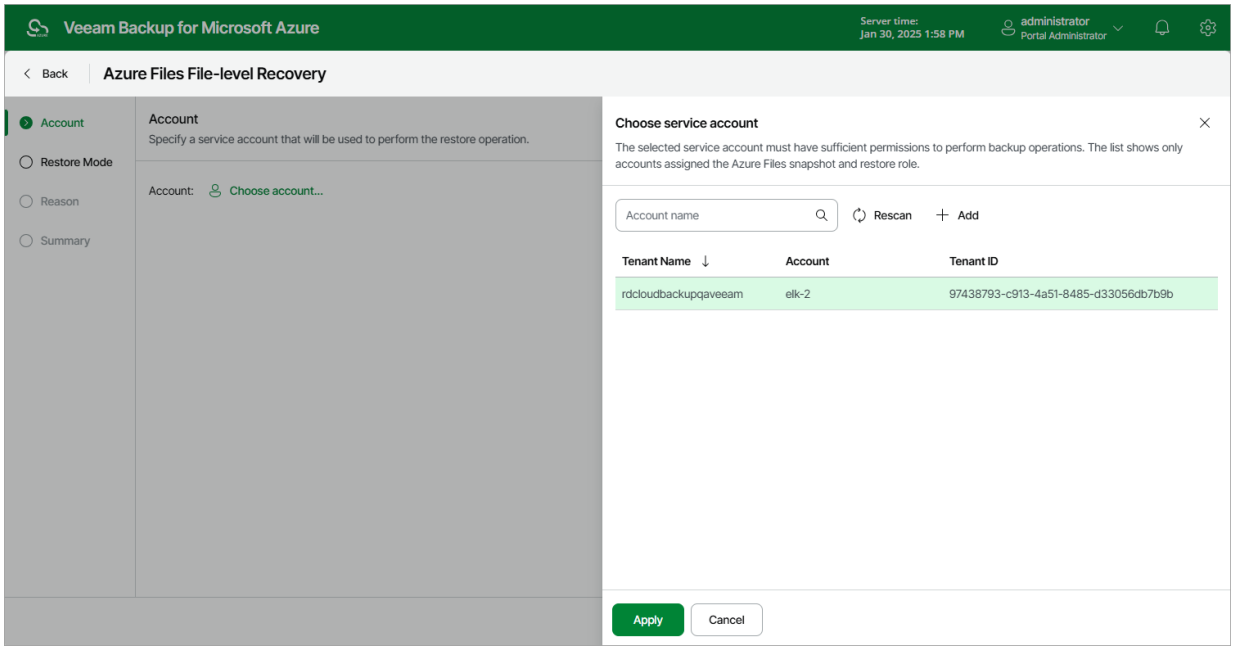


# Step 2. Select Service Account

At the **Account** step of the wizard, select a service account whose permissions Veeam Backup for Microsoft Azure will use to perform the restore operation.

1. Click **Choose account**.
2. In the **Choose service account** window, select the necessary account and click **Apply**. The specified service account must be assigned permissions listed in section Azure Files Permissions.

   For a service account to be displayed in the list of available accounts, it must be added to Veeam Backup for Microsoft Azure and assigned the *Azure Files Snapshot and Restore* operational role as described in section Adding Service Accounts. If you have not added the necessary service account to Veeam Backup for Microsoft Azure beforehand, you can do it without closing the **Azure Files File-Level Recovery** wizard. To do that, click **Add** and complete the **Add Account** wizard.



# Step 3. Choose Restore Mode

At the **Restore Mode** step of the wizard, choose whether you want to restore files of the file share to the original or to a custom location.

If you select the **Restore to a new location, or with different settings** option, you must also specify the file share that will host the restored files, and select an Azure subscription and an Azure region in which the target file share resides:

1. Click the link in the **Subscription** field. Then, select the necessary subscription in the **Choose subscription** window.

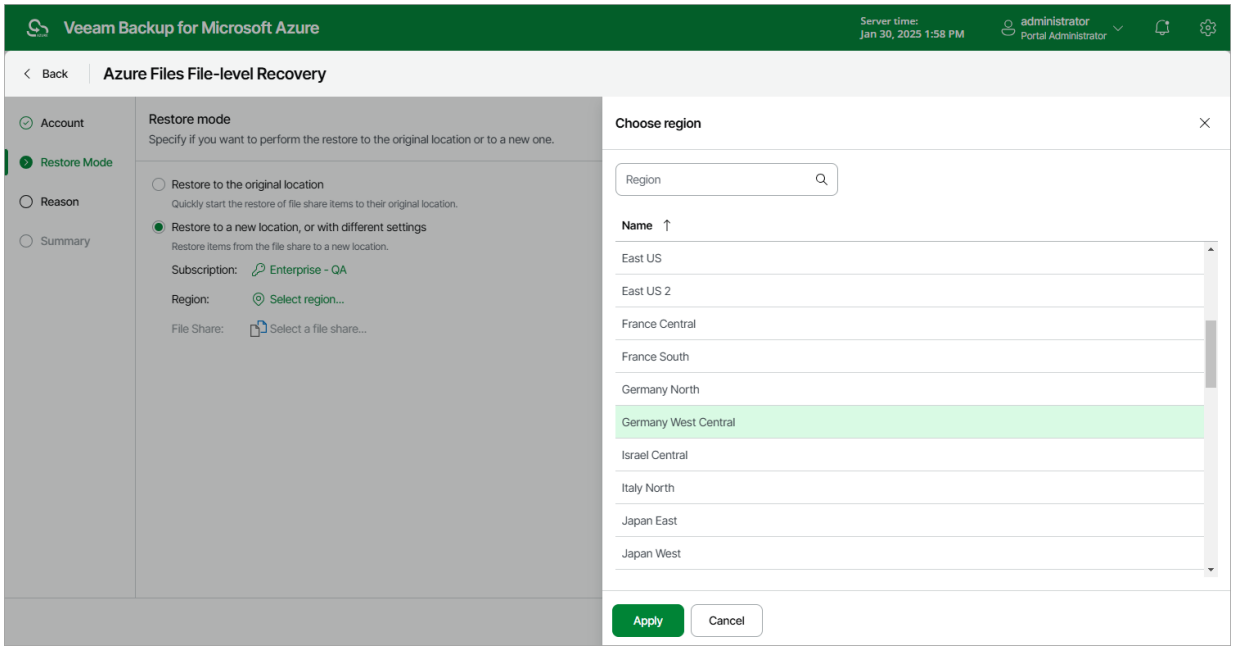
   For a subscription to be displayed in the list of available subscriptions, it must be created in Microsoft Azure and associated with the Microsoft Entra tenant to which the service account specified at step 2 of the wizard belongs.

2. Click the link in the **Region** field. Then, select the necessary Azure region in the **Choose region** window.

3. Click the link in the **File Share** field. Then, select the necessary file share in the **Choose target file share** window.

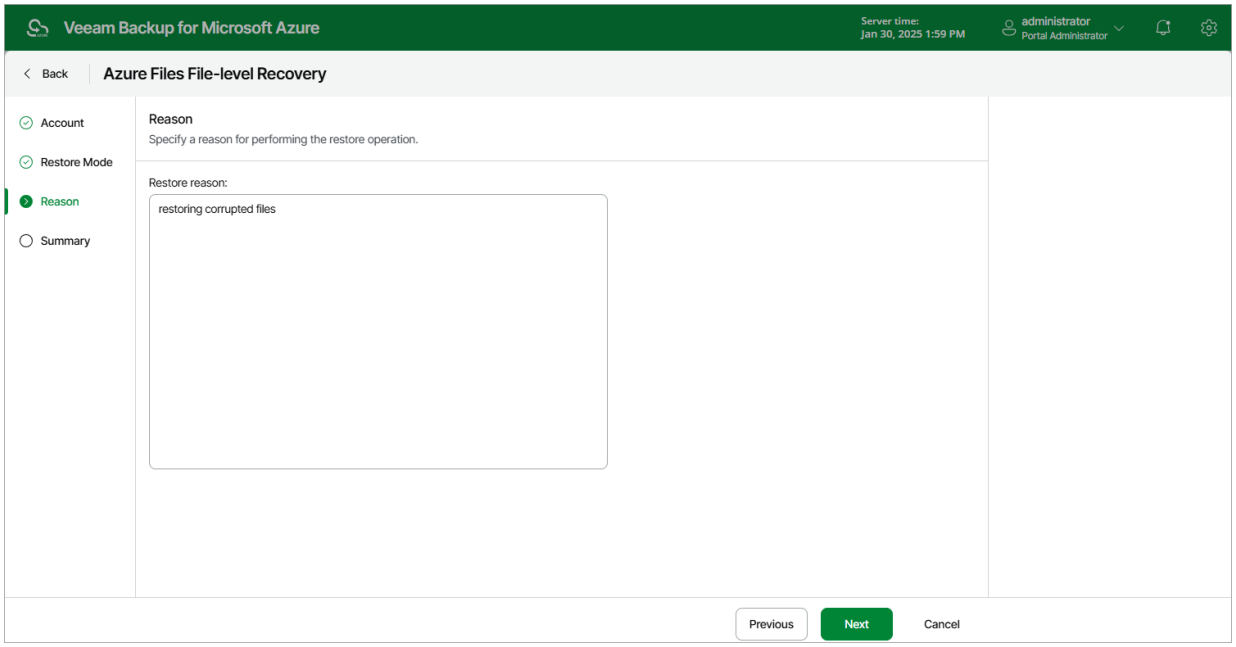
   For a file share to be displayed in the list of available shares, it must be deployed under the selected subscription in the Microsoft Azure portal, as described in Microsoft Docs.

> **NOTE**
>
> Data transfer to a new location may require additional costs and may take more time to complete.



# Step 4. Specify Restore Reason

At the **Reason** step of the wizard, specify a reason for restoring files and folders. This information will be saved to the session history, and you will be able to reference it later.



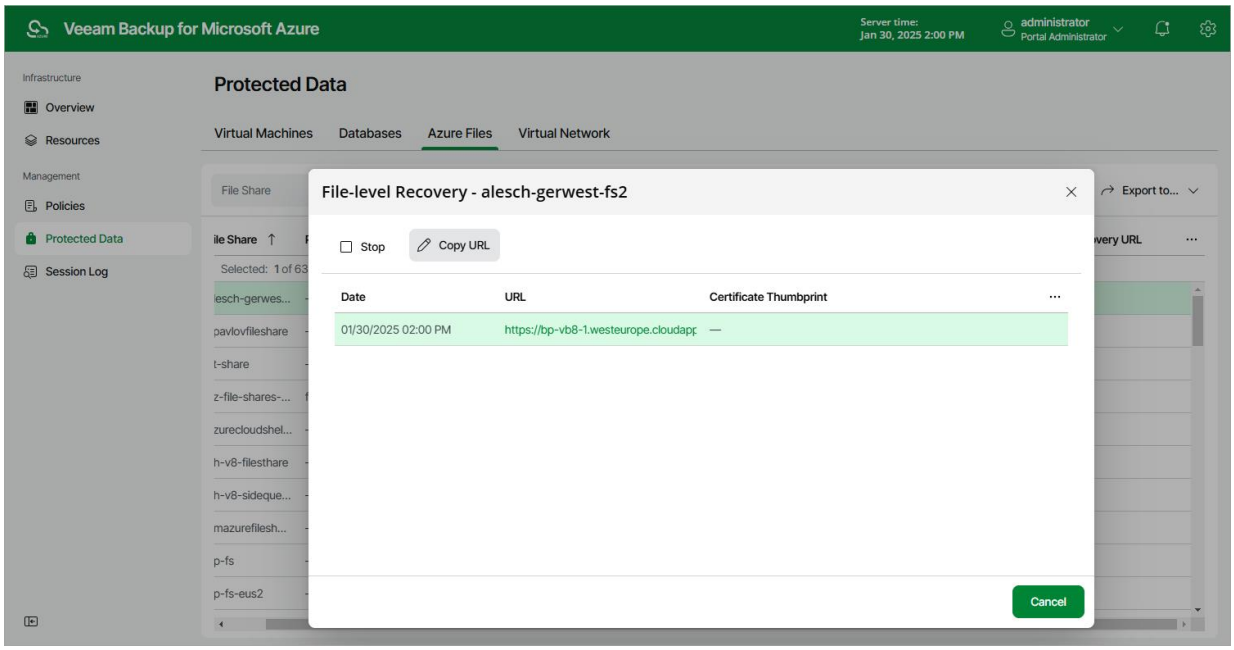
# Step 5. Start Recovery Session

At the **Summary** step of the wizard, review summary information and click **Start**.

As soon as you click **Start**, Veeam Backup for Microsoft Azure will close the **Azure Files File-level Recovery** wizard and start a restore session. You can track the progress of the restore session in the **File-level Recovery** window. To open the **File-level Recovery** window, navigate to **Protected Data** and click the link in the **File-level Recovery URL** column.

In the **URL** column of the window, Veeam Backup for Microsoft Azure will display a link to the file-level recovery browser. You can use the link in either of the following ways:

- Click the link to open the file-level recovery browser on your local machine while the restore session is running.
- Copy the link, close the **File-level Recovery** window and open the file-level recovery browser on another machine.

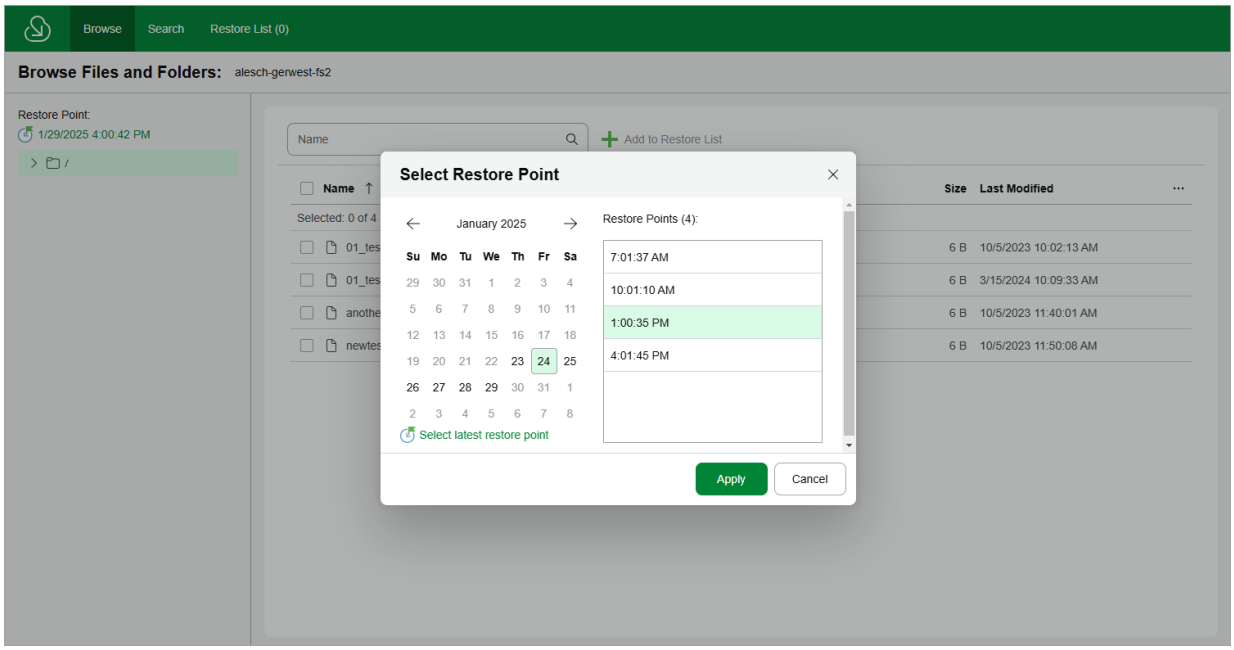


# Step 6. Select Restore Point

By default, Veeam Backup for Microsoft Azure uses the most recent valid restore point. However, you can restore files and folders to an earlier state.

To select a restore point in the file-level recovery browser, do the following:

1. On the **Browse** tab, click the link in the **Restore Point** field.
2. In the Select **Restore Point** window, choose a date when the restore point was created, select the necessary restore point from the **Restore Points** list and click **Apply**.



# Step 7. Choose Items to Recover

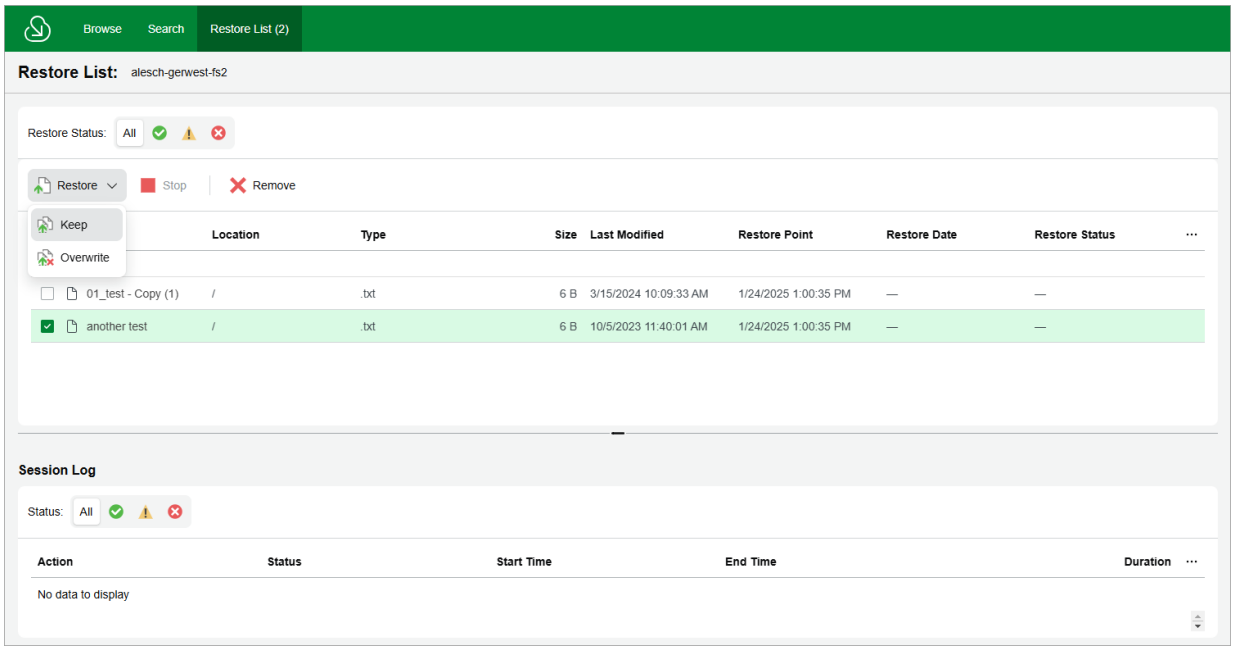
In the file-level recovery browser, you can find and restore items (files and folders) of the selected Azure file share. All restored items will be saved to the specified file share.

1. On the **Browse** tab, navigate to a folder that contains the necessary files.
2. In the working area, select check boxes next to the files and click **Add to Restore List**.
3. Repeat steps 1-2 for all other folders whose files you want to restore.
4. Switch to the **Restore List** tab, review the list of files and folders, select check boxes next to the items that you want to recover and do the following:
   - To restore copies of the selected files and folders to the target file share, click **Restore** > **Keep**.

     If files and folders with the same names exist on the target file share, Veeam Backup for Microsoft Azure will save the selected files to this file share with the following names — `<file_name>-Copy<ordinal_number>`. Otherwise, Veeam Backup for Microsoft Azure will save the selected files to this file share with the original names.
   - To restore the selected files and folders to the target file share, click **Restore** > **Overwrite**.

     If files and folders with the same names exist on the target file share, Veeam Backup for Microsoft Azure will overwrite these files. Otherwise, Veeam Backup for Microsoft Azure will save the selected files to this file share.

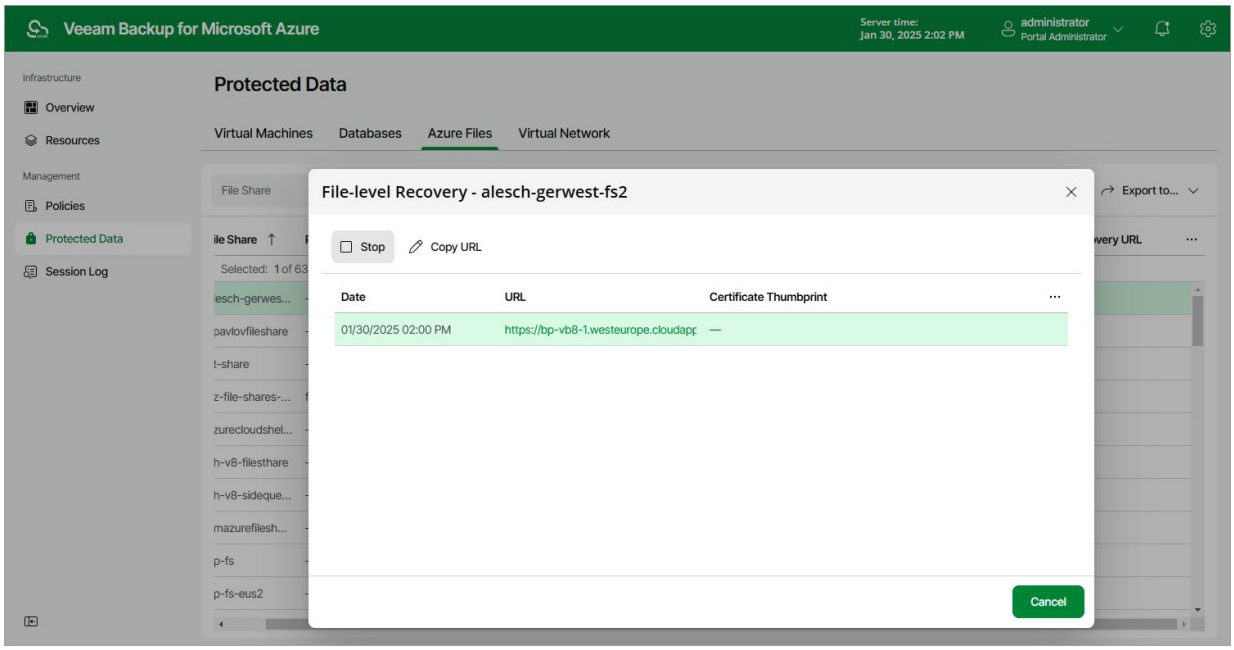
   As soon as you click **Restore**, Veeam Backup for Microsoft Azure will recover the selected files. You can track the progress and view the results of the restore operation in the **Session Log** section of the **Restore List** tab.



# Step 8. Stop Restore Session

After you finish working with the file-level recovery browser, it is recommended that you stop the restore session. To do that, click **Stop** in the **File-level Recovery** window. If you do not perform any actions in the file-level recovery browser for 30 minutes, and if no files are being restored, Veeam Backup for Microsoft Azure will stop the restore session automatically.

> **TIP**
>
> If you accidentally close the **File-level Recovery** window, navigate to **Protected Data** and click the link in the **File-level Recovery URL** column to open the window again.



# Virtual Network Configuration Restore

The actions that you can perform with restore points of the virtual network configuration depend on whether you access the restore points using the Veeam Backup & Replication console or the Veeam Backup for Microsoft Azure Web UI.

# Performing Virtual Network Configuration Restore Using Console

Veeam Backup & Replication allows you to restore the entire Azure virtual network configuration from a virtual network configuration backup to any available restore point. To learn how entire virtual network configuration restore works, see Entire Virtual Network Configuration Restore.

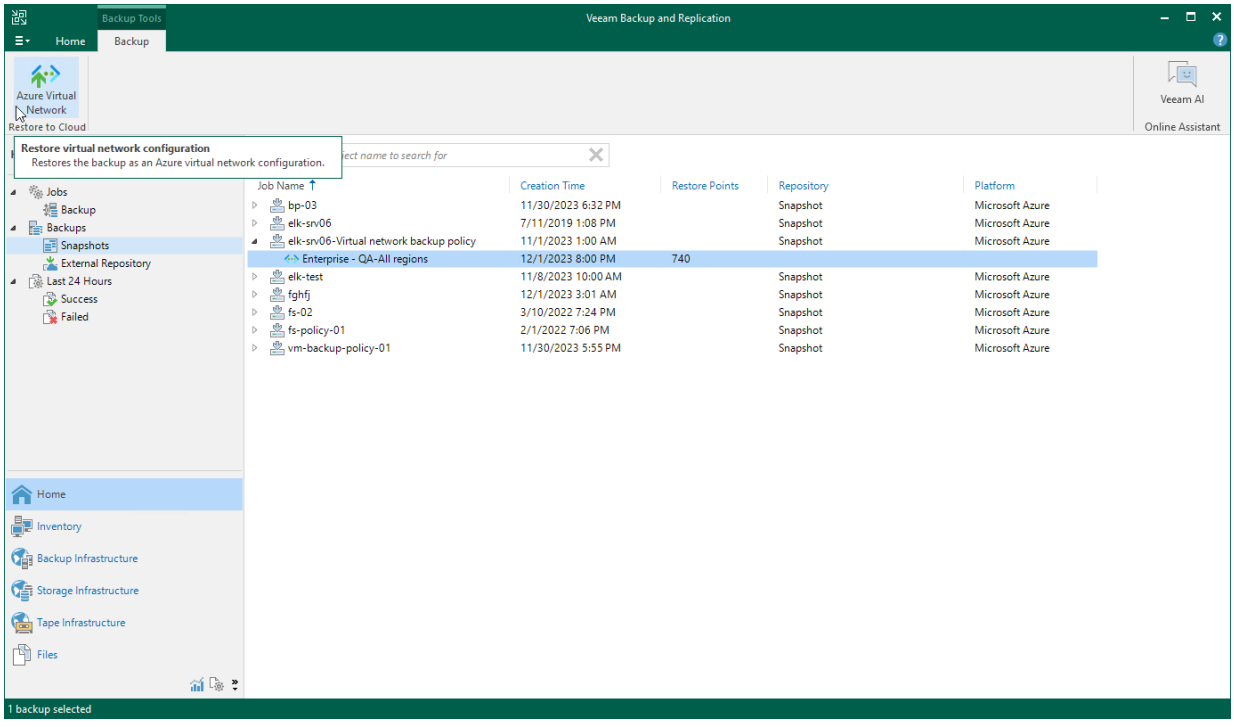
To restore the virtual network configuration, do the following:

1. In the Veeam Backup & Replication console, open the **Home** view.
2. Navigate to **Backups** > **Snapshots**.
3. Expand the backup policy that protects the virtual network configuration, select the Azure subscription whose virtual network configuration you want to restore, and click **Azure Virtual Network** on the ribbon.

   Alternatively, you can right-click the selected subscription and click **Restore to Microsoft Azure virtual network**.

Veeam Backup & Replication will open the **Virtual Network Restore** wizard in a web browser. Complete the wizard as described in section Virtual Network Configuration Restore.

> **IMPORTANT**
>
> Granular restore of the virtual network configuration is not available from the Veeam Backup & Replication console — you can perform it using the Veeam Backup for Microsoft Azure Web UI only.



# Performing Virtual Network Configuration Restore Using Web UI

Veeam Backup for Microsoft Azure offers the following disaster recovery operations:

- Full restore — restores the entire virtual network configuration.
- Granular restore — restores the selected virtual network configuration items.

You can restore the virtual network configuration data to the most recent state or to any available restore point.

## Performing Entire Virtual Network Configuration Restore

In case of unexpected configuration changes, you can restore the entire virtual network configuration from a virtual network configuration backup. Veeam Backup for Microsoft Azure allows you to restore the virtual network configuration to the original location or to a new location.

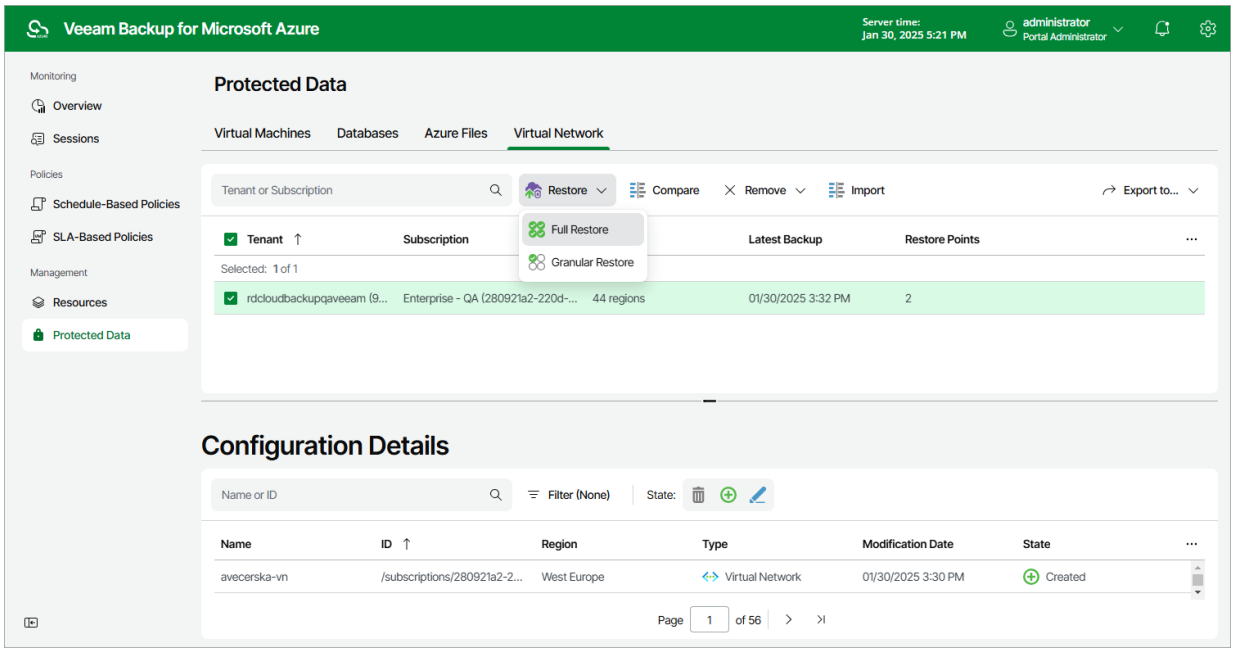
To restore the entire virtual network configuration, perform the following steps:

1. Launch the Virtual Network Restore wizard.
2. Select a region and a restore point.
3. Select a service account.
4. Choose a restore mode.
5. Configure additional restore settings.
6. Specify a restore reason.
7. Finish working with the wizard.

# Step 1. Launch Virtual Network Restore Wizard

To launch the **Virtual Network Restore** wizard, do the following:

1. Navigate to **Protected Data** > **Virtual Network**.
2. Select the configuration record for an Azure subscription whose virtual network configuration you want to restore.
3. Click **Restore** > **Full Restore**.



# Step 2. Select Region and Restore Point

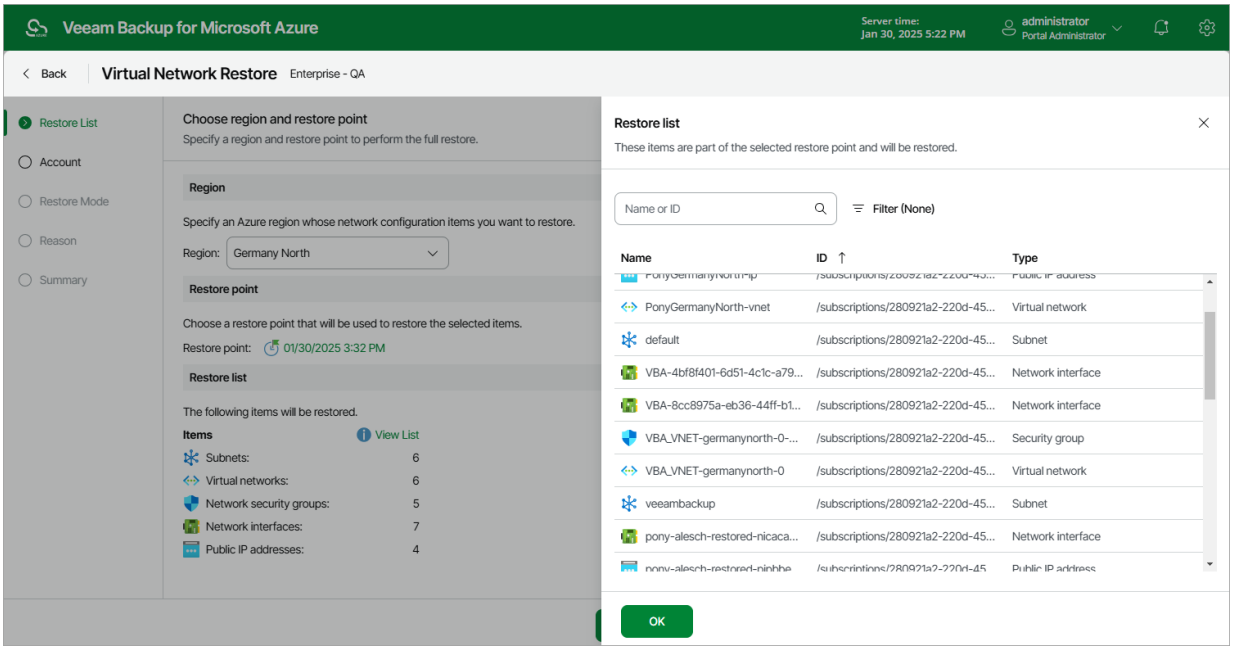
At the **Restore List** step of the wizard, select an Azure region and a restore point that will be used to restore the virtual network configuration items. By default, Veeam Backup for Microsoft Azure uses the most recent valid restore point. However, you can restore the virtual network configuration data to an earlier state.

To select a restore point, do the following:

1. In the **Region** section, select an Azure region whose network configuration items you want to restore.
2. In the **Restore point** section, click the link to the right of **Restore point**.
3. In the **Available restore points** window, select the necessary restore point and click **Apply**.

   For a restore point to be displayed in the list of available restore points, it must be stored in the configuration database. If the restore point that you want to use to recover the virtual network configuration data is stored in a backup repository, you must first import it to the database as described in section Importing Virtual Network Configuration Data.

To view the full list of the virtual network configuration items that will be restored, click **View List** in the **Items** section.

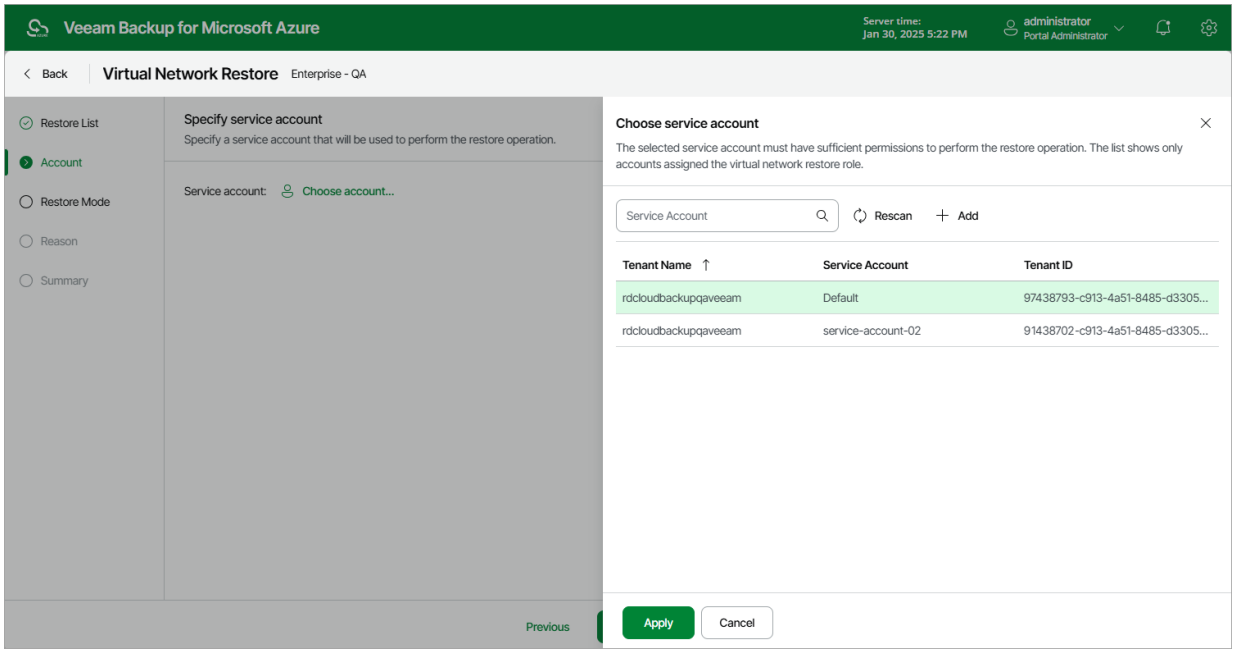


# Step 3. Specify Service Account

At the **Account** step of the wizard, choose a service account whose permissions will be used to perform the restore operation. To do that, click the link to the right of **Service account** and choose the necessary account from the list. The specified service account must be assigned permissions listed in section Virtual Network Configuration Permissions.

For a service account to be displayed in the list of available accounts, it must be added to Veeam Backup for Microsoft Azure and assigned the *Virtual Network Restore* operational role as described in section Adding Service Accounts.

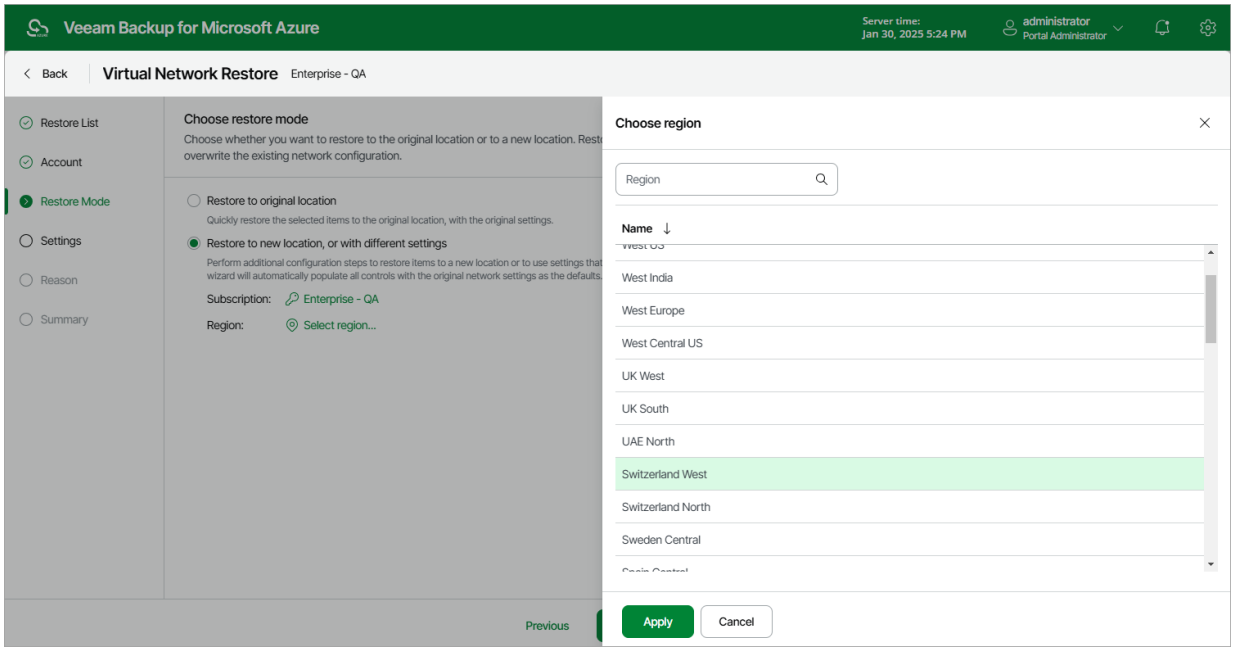
> **IMPORTANT**
>
> Consider the following:
>
> - Make sure that the specified service account belongs to an Microsoft Entra tenant in which you plan to restore the virtual network configuration.
> - It is recommended that you check whether the selected service account has all the permissions required to perform the operation. If the service account permissions are insufficient, the restore operation will fail to complete successfully. To run the service account permission check, follow the instructions provided in section Checking Service Account Permissions.



# Step 4. Choose Restore Mode

At the **Restore Mode** step of the wizard, choose whether you want to restore the selected virtual network configuration to the original or to a custom location. If you select the **Restore to new location, or with different settings** option, specify the target Azure subscription and Azure region where to restore the virtual network configuration.

> **IMPORTANT**
>
> Consider the following:
>
> - A resource group that has the same name as the original resource group must exist in the selected location. Otherwise, Veeam Backup for Microsoft Azure will not be able to perform the restore operation.
> - A virtual network peering can be restored to a new location only in case both peered virtual networks reside in the same region.

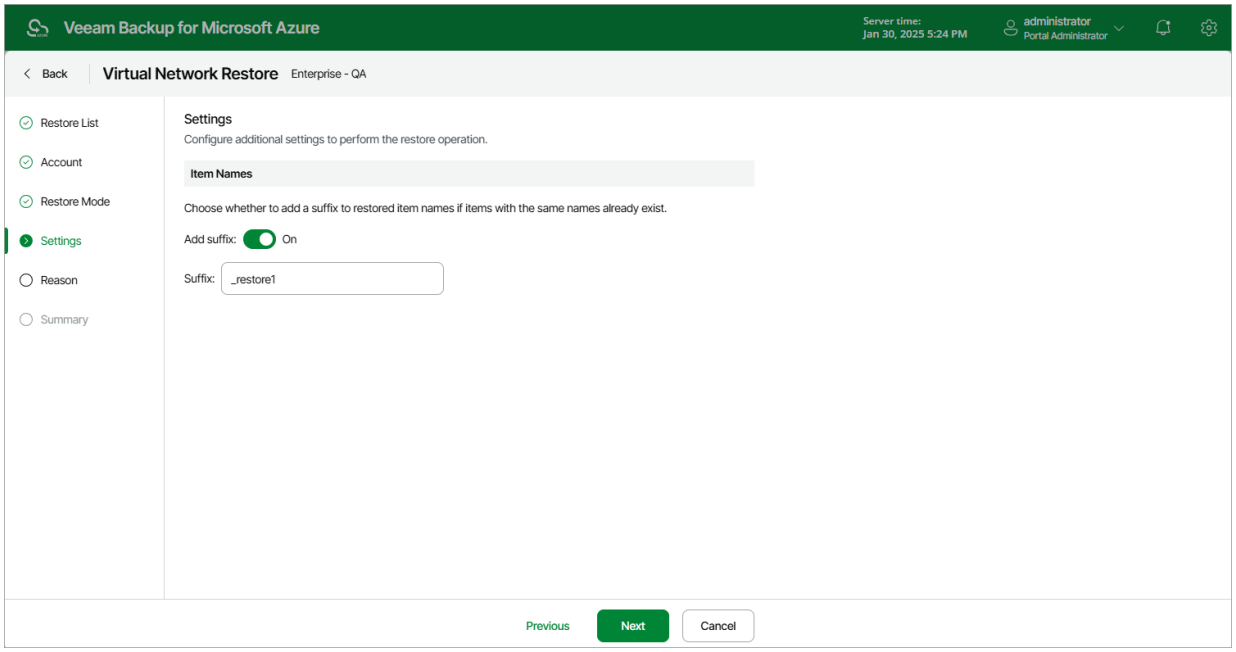


# Step 5. Configure Additional Restore Settings

[This step applies only if you have selected the **Restore to new location, or with different settings** option at the **Restore Mode** step of the wizard]

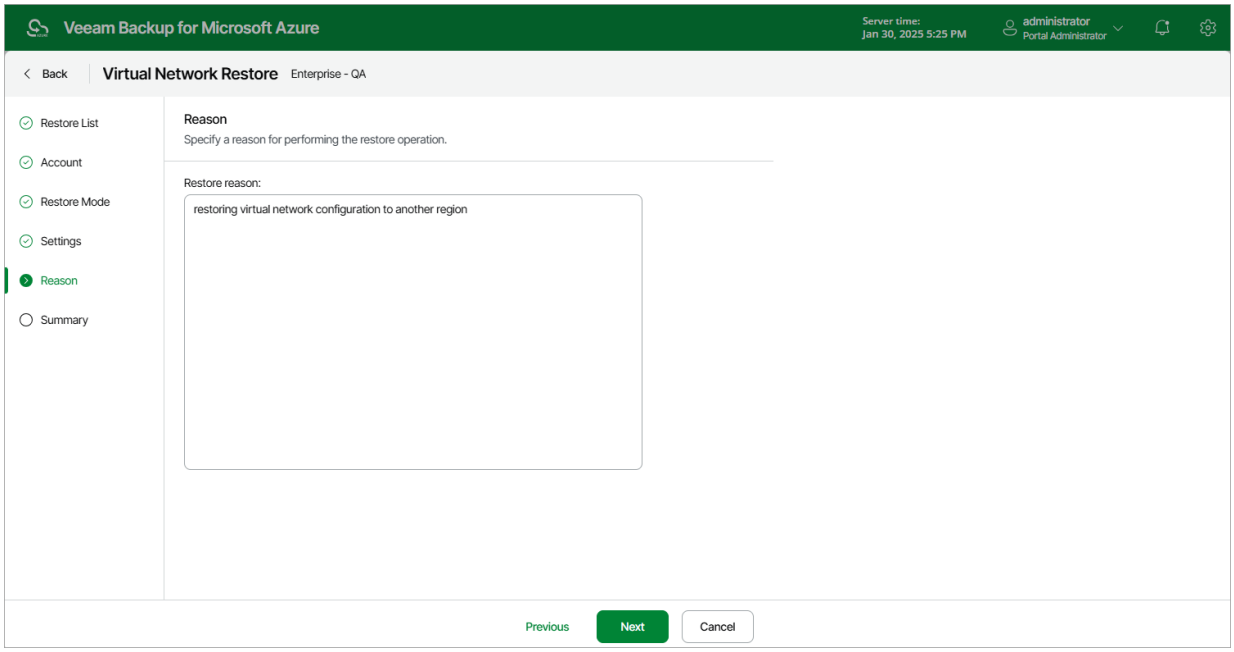
At the **Settings** step of the wizard, you can choose whether to add a suffix to restored item names if items with the same names already exist. To do that, in the **Item Names** section, set the **Add suffix** toggle to *On* and enter the necessary suffix in the **Suffix** field.

> **IMPORTANT**
>
> When restoring the configuration to a new location but the same subscription, make sure the name of each restored item is unique across the entire subscription. Otherwise, Veeam Backup for Microsoft Azure may not be able to perform the restore operation.



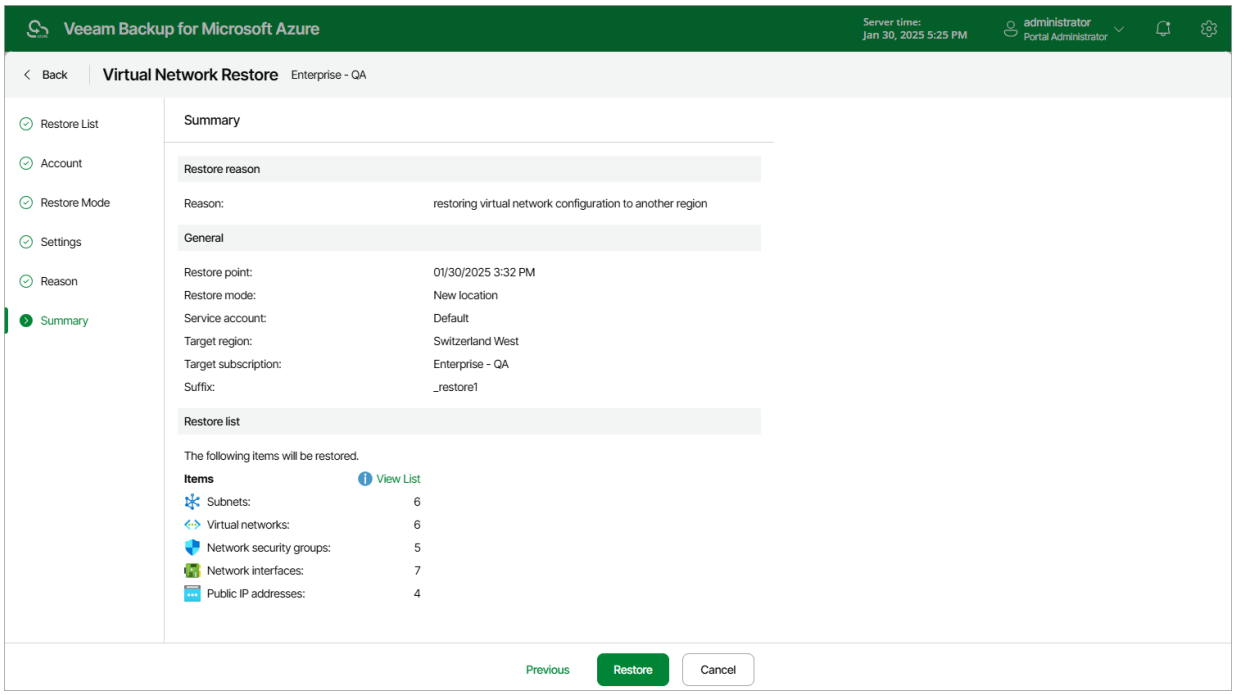
# Step 6. Specify Restore Reason

At the **Reason** step of the wizard, specify a reason for restoring virtual network configuration. The information you provide will be saved in the session history and you can reference it later.



## Step 7. Finish Working with Wizard

At the **Summary** step of the wizard, review summary information and click **Finish**.




# Performing Granular Restore

In case of unexpected configuration changes, you can restore specific items of the virtual network configuration from a virtual network configuration backup. Veeam Backup for Microsoft Azure allows you to restore these items to the original location only.

# How to Perform Granular Restore

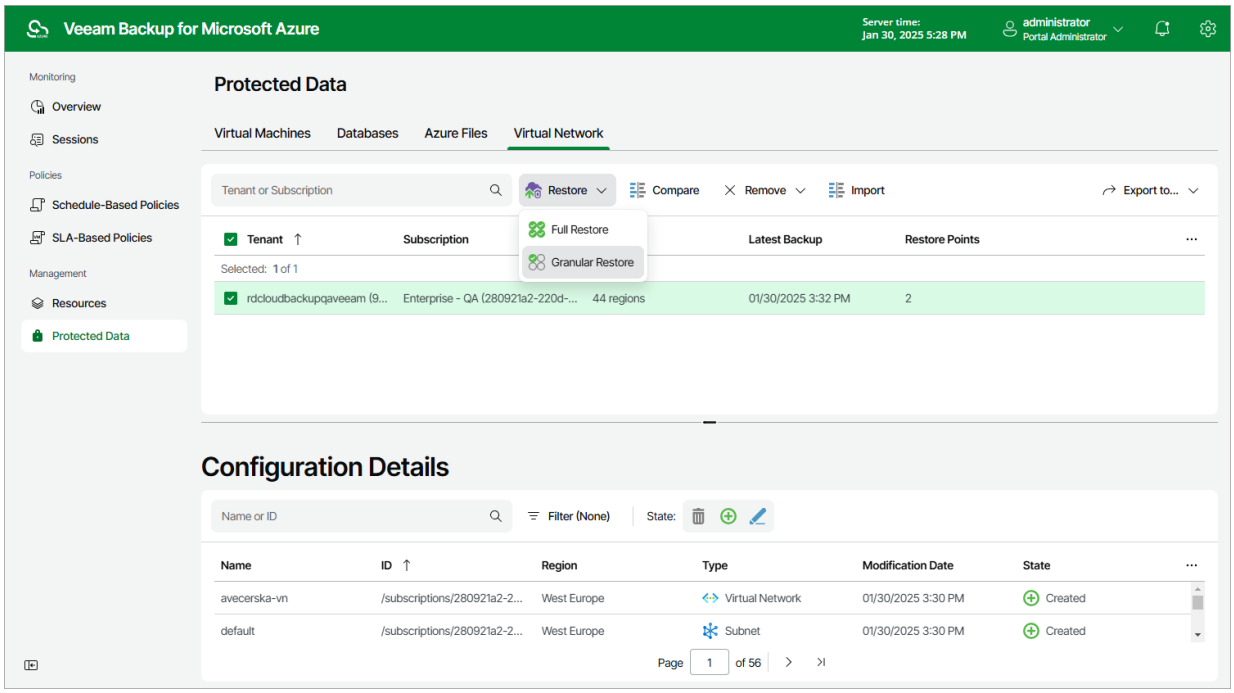
To restore specific items of the virtual network configuration, perform the following steps:

1. Launch the Virtual Network Restore wizard.
2. Select a region, a restore point and items to restore.
3. Select a service account.
4. Specify a restore reason.
5. Finish working with the wizard.

# Step 1. Launch Virtual Network Restore Wizard

To launch the **Virtual Network Restore** wizard, do the following:

1. Navigate to **Protected Data** > **Virtual Network**.
2. Select the configuration record for an Azure subscription whose virtual network configuration you want to restore.
3. Click **Restore** > **Granular Restore**.

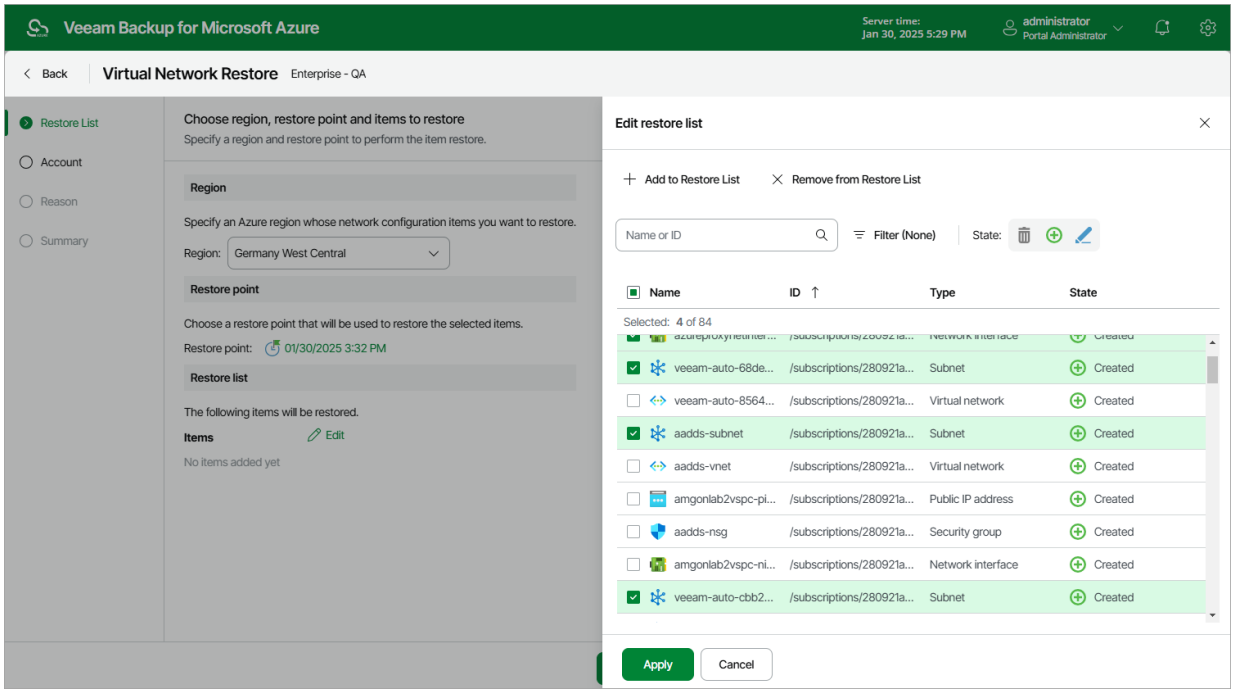


# Step 2. Select Region, Restore Point and Items to Restore

At the **Restore List** step of the wizard, select virtual network configuration items you want to restore, and choose an Azure region and a restore point that will be used to restore the selected items. By default, Veeam Backup for Microsoft Azure uses the most recent valid restore point. However, you can restore the virtual network configuration data to an earlier state.

1. To select the region and the restore point:
   a. In the **Region** section, select an Azure region whose network configuration items you want to restore.
   b. In the **Restore point** section, click the link to the right of **Restore point**.
   c. In the **Available restore points** window, select the necessary restore point and click **Apply**.
2. To select the virtual network configuration items:
   a. In the **Items** section, click **Edit**.
   b. In the **Edit restore list** window, click **Add to Restore List**.
   c. In the **Items List** window, select check boxes next to the items that you want to restore, and click **Add**.
   d. In the **Edit restore list** window, review the restore list and click **Apply**.

> **IMPORTANT**
>
> A resource group that has the same name as the original resource group must exist in the original location. Otherwise, Veeam Backup for Microsoft Azure will not be able to perform the restore operation.

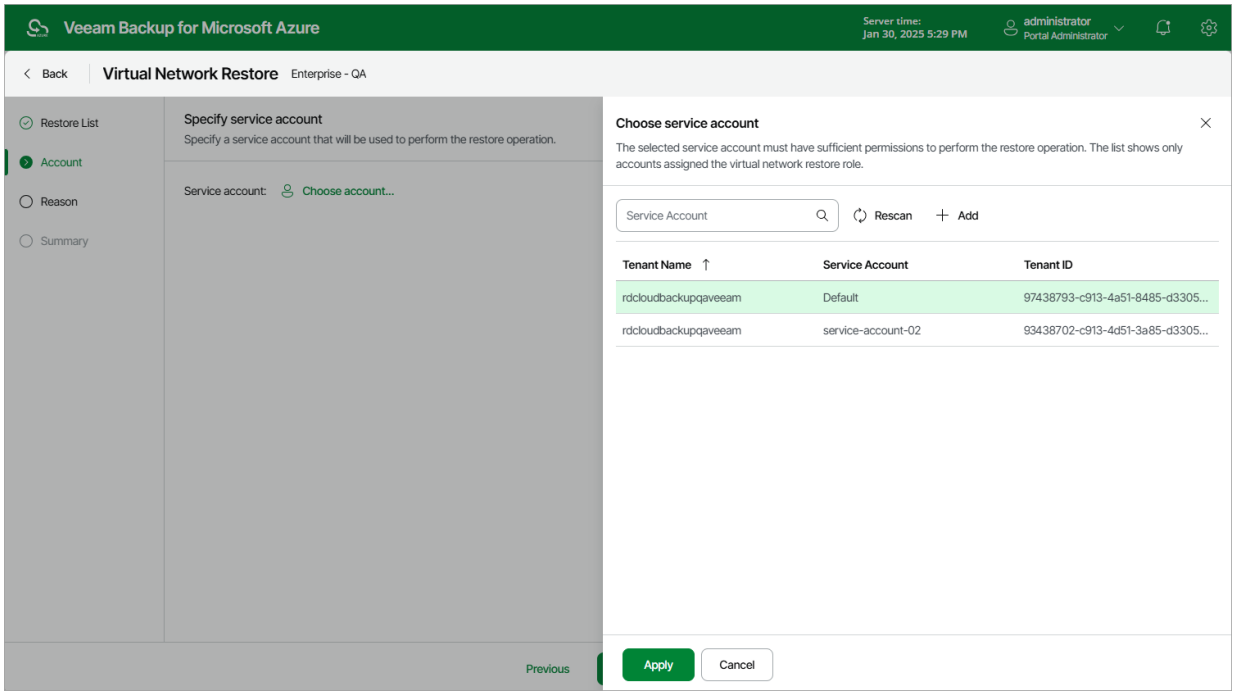


# Step 3. Specify Service Account

At the **Account** step of the wizard, choose a service account whose permissions will be used to perform the restore operation. To do that, click the link to the right of **Service account** and choose the necessary account from the list. The specified service account must be assigned permissions listed in section Virtual Network Configuration Permissions.

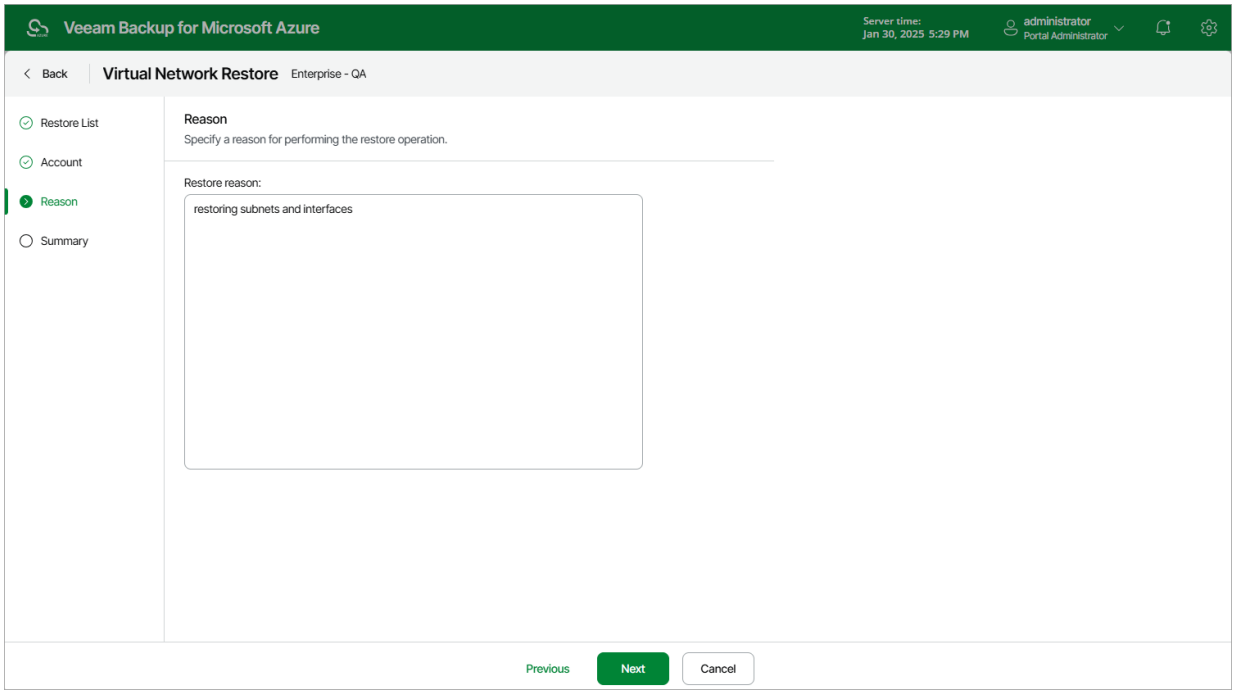
For a service account to be displayed in the list of available accounts, it must be added to Veeam Backup for Microsoft Azure and assigned the *Virtual Network Restore* operational role as described in section Adding Service Accounts.

> **IMPORTANT**
>
> It is recommended that you check whether the selected service account has all the permissions required to perform the operation. If the service account permissions are insufficient, the restore operation will fail to complete successfully. To run the service account permission check, follow the instructions provided in section Checking Service Account Permissions.



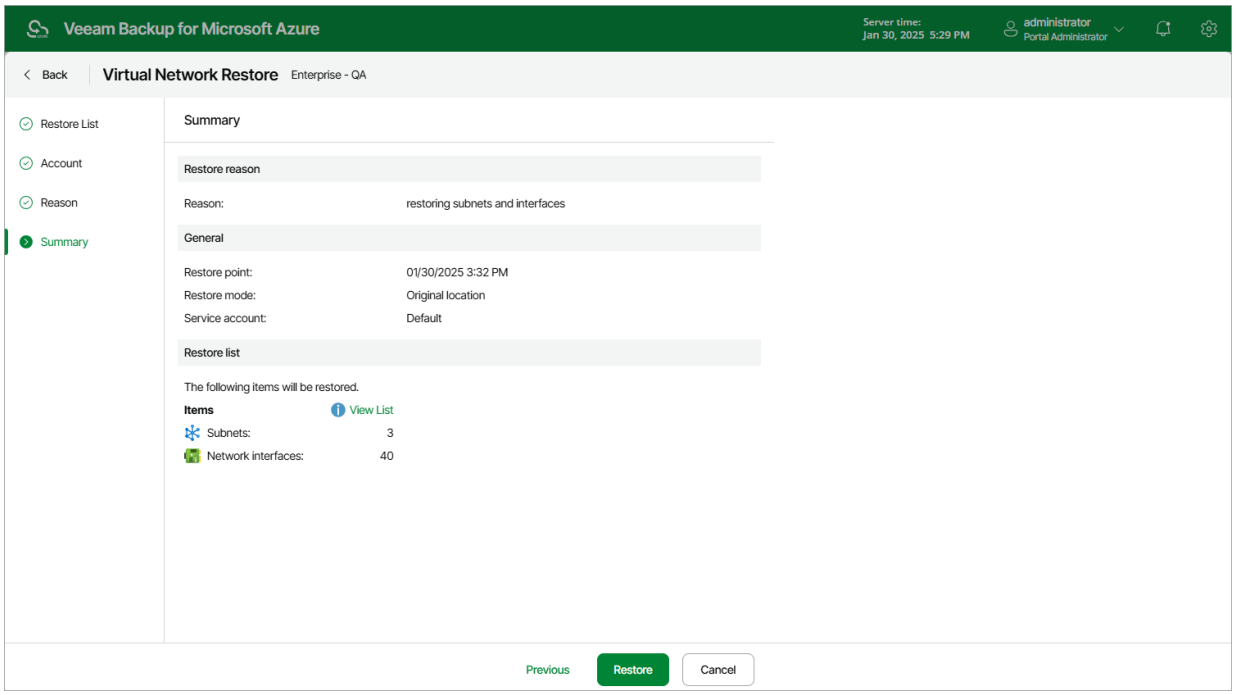
# Step 4. Specify Restore Reason

At the **Reason** step of the wizard, specify a reason for the restore of virtual network configuration items. The information you provide will be saved in the session history and you can reference it later.



# Step 5. Finish Working with Wizard

At the **Summary** step of the wizard, review summary information and click **Finish**.



# Performing Instant Recovery

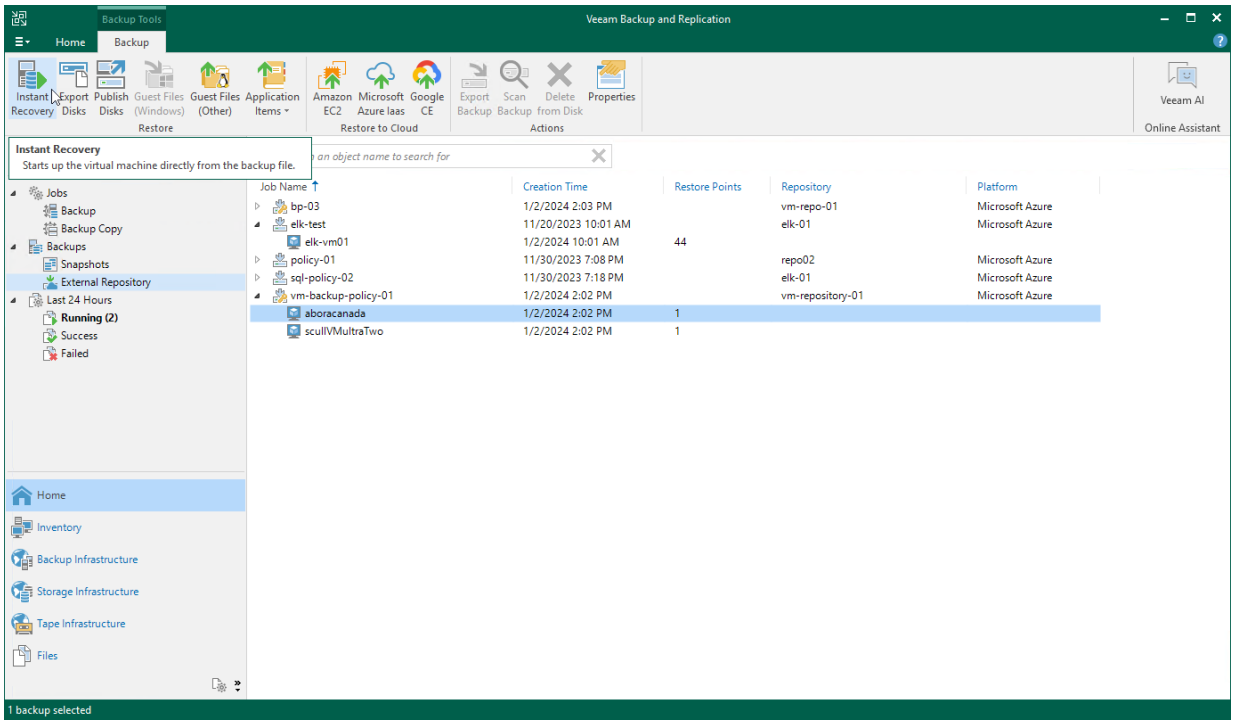
Veeam Backup & Replication allows you to use the Instant Recovery feature to restore Azure VMs from image-level backups to VMware vSphere and Microsoft Hyper-V environments, or to Nutanix AHV clusters. For more information, see the Veeam Backup & Replication User Guide for VMware vSphere, Veeam Backup & Replication User Guide for Microsoft Hyper-V and Veeam Backup for Nutanix AHV User Guide, section *Instant Recovery*.

> **IMPORTANT**
>
> Instant Recovery can be performed only using backup files stored in standard repositories for which you have specified credentials of Microsoft Azure storage accounts where the target blob containers reside. To learn how to specify credentials for repositories, see sections Creating New Repositories and Connecting to Existing Appliances.

Before you start the restore operation, make sure to add to the backup infrastructure a vCenter Server, a Microsoft Hyper-V server, or a Nutanix AHV cluster that will manage restored VMs. To learn how to add servers or clusters to Veeam Backup & Replication, see the Veeam Backup & Replication User Guide, section Adding VMware vSphere Servers, Adding Microsoft Hyper-V Servers, or Adding Nutanix AHV Cluster.

To perform Instant Recovery, do the following:

1. In the Veeam Backup & Replication console, open the **Home** view.
2. Navigate to **Backups** > **External Repository**.
3. Expand the backup policy that protects an Azure VM that you want to recover, select the necessary VM and click **Instant Recovery** on the ribbon.
4. Select **VMware vSphere**, **Microsoft Hyper-V** or **Nutanix AHV**.
5. Depending on the selected **Instant Recovery** option, complete the **Instant Recovery** wizard as described in the Veeam Backup & Replication User Guide, section Performing Instant Recovery of Workloads to VMware vSphere VMs, Performing Instant Recovery of Workloads to Hyper-V VMs or Performing Instant Recovery of Workloads to Nutanix AHV.



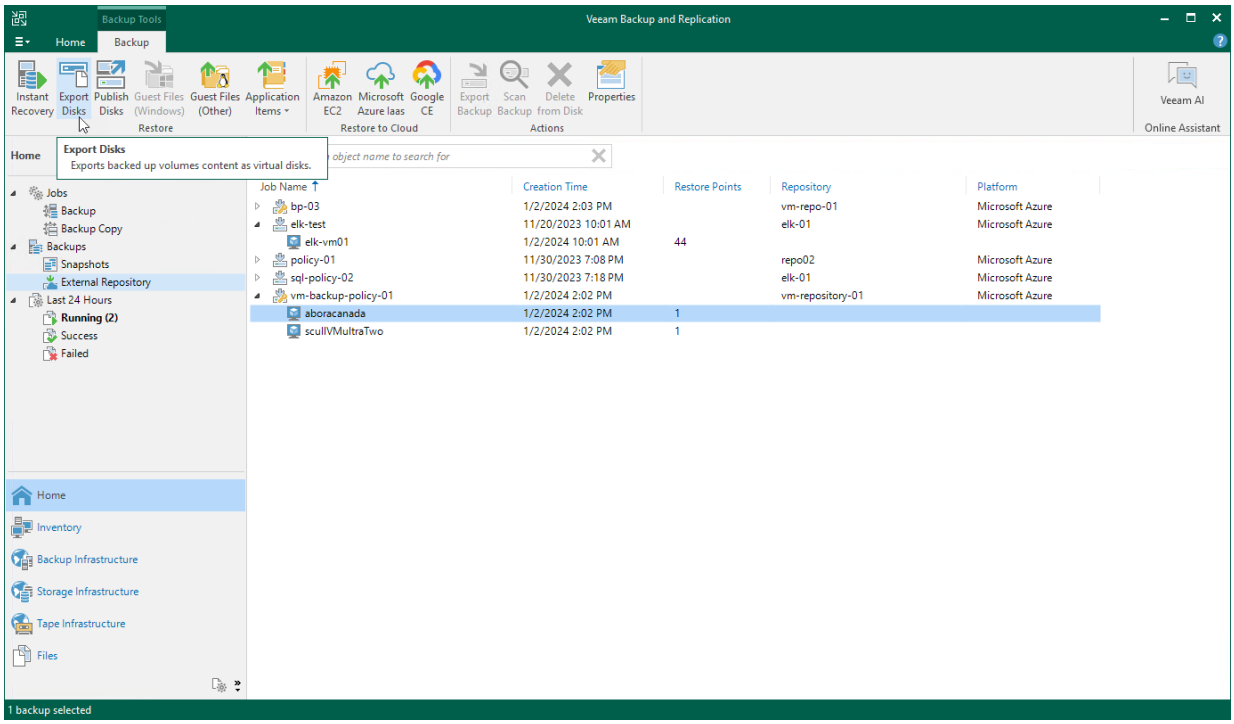
# Exporting Disks

Veeam Backup & Replication allows you to export disks, that is, to restore virtual disks of Azure VMs from image-level backups created by Veeam Backup for Microsoft Azure and to convert them to the VMDK, VHD and VHDX formats. You can save the converted disks to any server added to the backup infrastructure or place the disks on a datastore connected to an ESXi host (for the VMDK disk format only). For more information, see the Veeam Backup & Replication User Guide, section Disk Export.

> **IMPORTANT**
>
> Exporting Disks can be performed only using backup files stored in standard repositories for which you have specified credentials of Microsoft Azure storage accounts where the target blob containers reside. To learn how to specify credentials for repositories, see sections Creating New Repositories and Connecting to Existing Appliances.

To restore disks of an Azure VM to the VMDK, VHD or VHDX format, do the following:

1. In the Veeam Backup & Replication console, open the **Home** view.
2. Navigate to **Backups** > **External Repository**.
3. Expand the backup policy that protects an Azure VM whose disks you want to restore, select the necessary VM and click **Export Disk** on the ribbon.
4. Complete the **Export Disk** wizard as described in the Veeam Backup & Replication User Guide, section Exporting Disks.



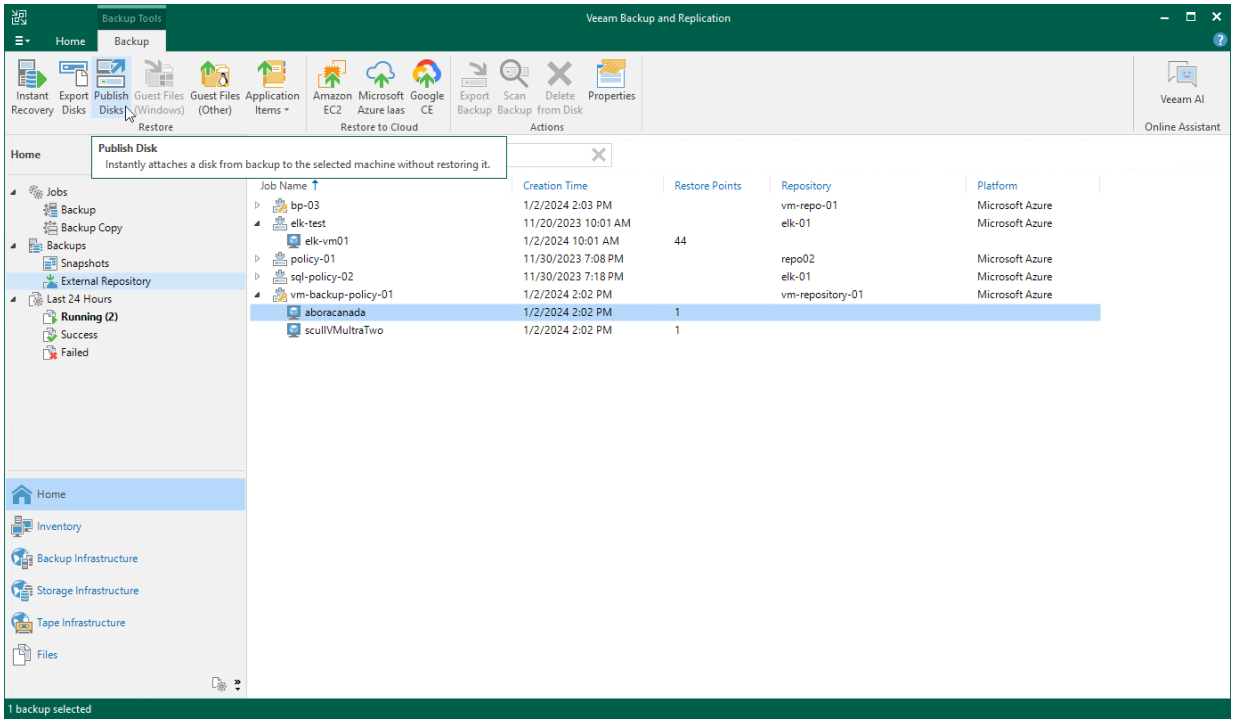
# Publishing Disks

Veeam Backup & Replication allows you to publish point-in-time disks, that is, to attach specific virtual disks of backed-up Azure VMs to any server to instantly access data in the read-only mode. You can copy the necessary files and folders to the target server, and perform an antivirus scan of the backed-up data. For more information, see the Veeam Backup & Replication User Guide, section Disk Publishing (Data Integration API).

> **IMPORTANT**
>
> Publishing Disks can be performed only using backup files stored in standard repositories for which you have specified credentials of Microsoft Azure storage accounts where the target blob containers reside. To learn how to specify credentials for repositories, see sections Creating New Repositories and Adding Appliances.

To publish virtual disks of an Azure VM, do the following:

1. In the Veeam Backup & Replication console, open the **Home** view.
2. Navigate to **Backups** > **External Repository**.
3. Expand the necessary backup policy, select the Azure VM whose disks you want to publish and click **Publish Disks** on the ribbon.
4. Complete the **Publish Disks** wizard as described in the Veeam Backup & Replication User Guide, section Publishing Disks.



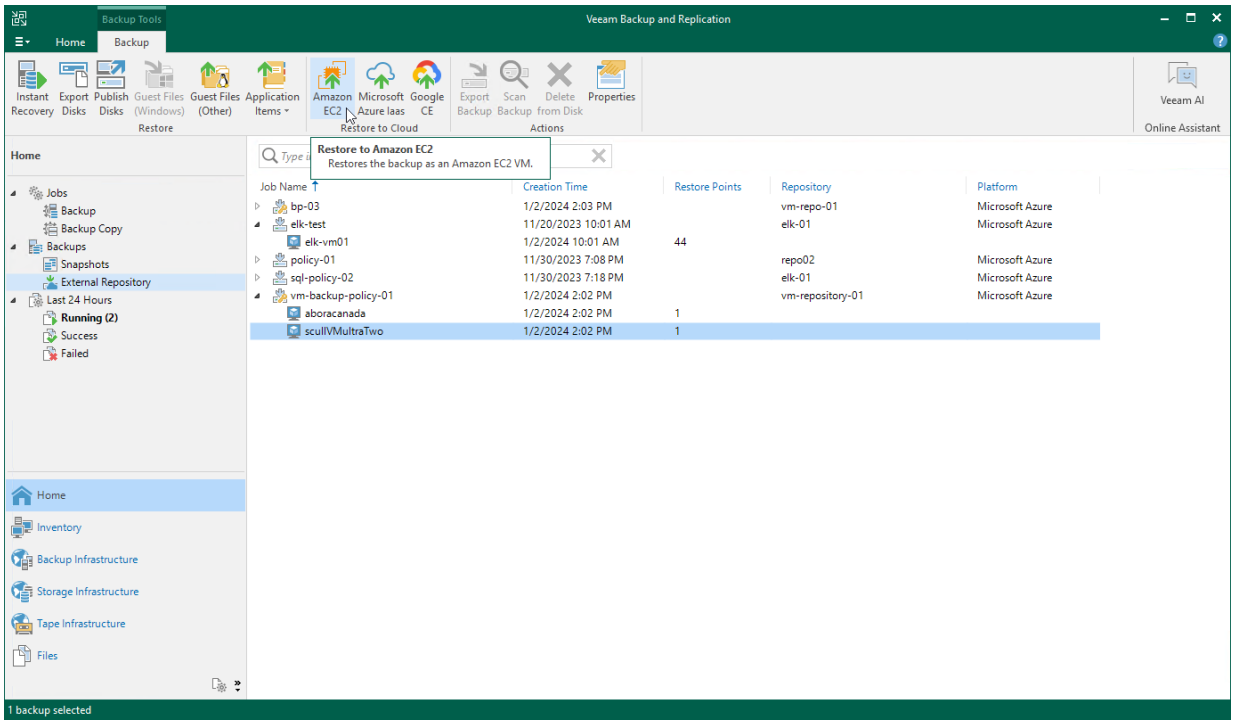
# Restoring to AWS

Veeam Backup & Replication allows you to restore Azure VMs from image-level backups created with Veeam Backup for Microsoft Azure to AWS as EC2 instances. You can restore Azure VMs to any available restore point. For more information, see the Veeam Backup & Replication User Guide, section Restore to Amazon EC2.

> **IMPORTANT**
>
> Consider the following:
>
> - Restore to AWS can be performed only using backup files stored in standard repositories for which you have specified credentials of Microsoft Azure storage accounts where the target blob containers reside. To learn how to specify credentials for repositories, see sections Creating New Repositories and Connecting to Existing Appliances.
> - Before you start the restore operation, check the limitations and prerequisites described in the Veeam Backup & Replication User Guide, section Before You Begin.

To restore an Azure VM to AWS, do the following:

1. In the Veeam Backup & Replication console, open the **Home** view.
2. Navigate to **Backups** > **External Repository**.
3. Expand the backup policy that protects an Azure VM that you want to restore, select the necessary VM and click **Amazon EC2** on the ribbon.
4. Complete the **Restore to Amazon EC2** wizard as described in the Veeam Backup & Replication User Guide, section Restoring to Amazon EC2.



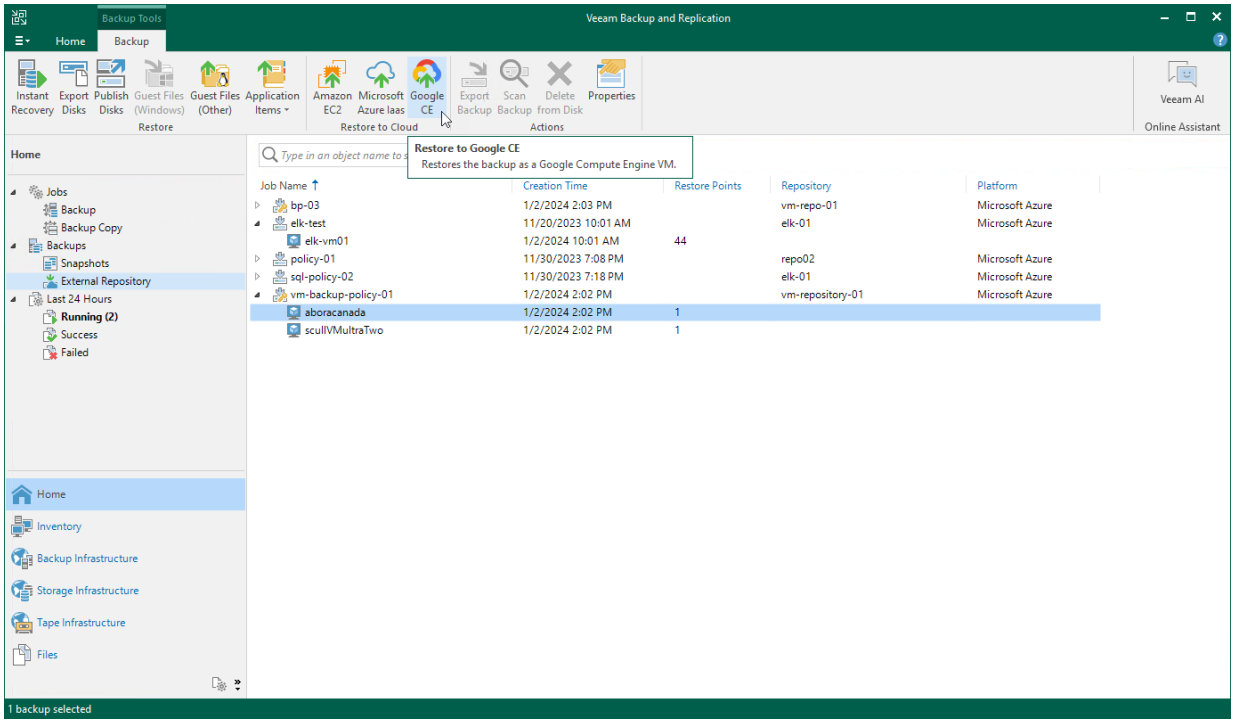
# Restoring to Google Cloud

Veeam Backup & Replication allows you to restore Azure VMs from image-level backups created with Veeam Backup for Microsoft Azure to Google Cloud as VM instances. You can restore VMs to any available restore point. For more information, see the Veeam Backup & Replication User Guide, section Restore to Google Compute Engine.

> **IMPORTANT**
>
> Consider the following:
>
> - Restore to Google Cloud can be performed only using backup files stored in standard repositories for which you have specified credentials of Microsoft Azure storage accounts where the target blob containers reside. To learn how to specify credentials for repositories, see sections Creating New Repositories and Connecting to Existing Appliances.
> - Before you start the restore operation, check the limitations and prerequisites described in the Veeam Backup & Replication User Guide, section Before You Begin.

To restore an Azure VM to Google Cloud, do the following:

1. In the Veeam Backup & Replication console, open the **Home** view.
2. Navigate to **Backups** > **External Repository**.
3. Expand the backup policy that protects an Azure VM that you want to restore, select the necessary VM and click **Google CE** on the ribbon.
4. Complete the **Restore to Google Compute Engine** wizard as described in the Veeam Backup & Replication User Guide, section Restoring to Google Compute Engine.



# Restoring to Nutanix AHV

Veeam Backup & Replication allows you to restore Azure VMs from image-level backups created with Veeam Backup for Microsoft Azure to Nutanix AHV as Nutanix AHV VMs. You can restore VMs to any available restore point. For more information, see the Veeam Backup for Nutanix AHV User Guide, section Performing Restore.

> **IMPORTANT**
>
> Restore to Nutanix AHV can be performed only using backup files stored in standard repositories for which you have specified credentials of Microsoft Azure storage accounts where the target blob containers reside. To learn how to specify credentials for repositories, see sections Creating New Repositories and Connecting to Existing Appliances.

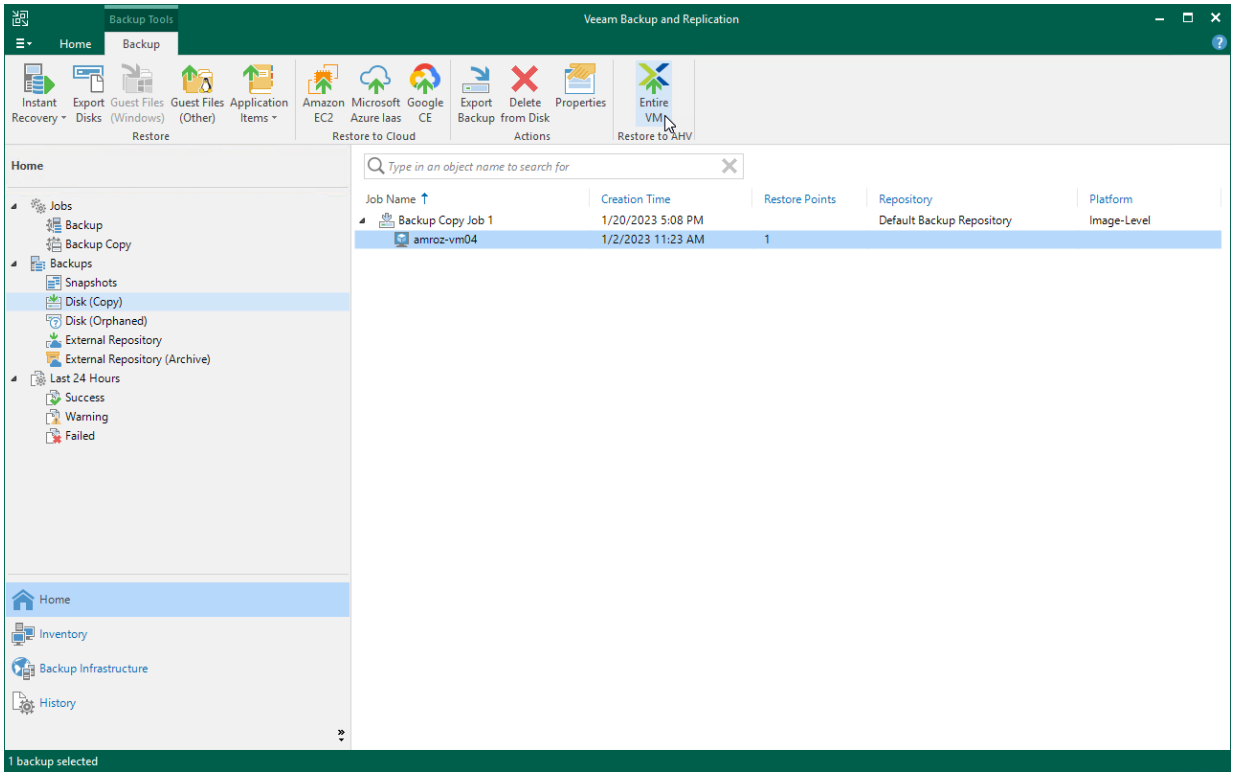
Before you start the restore operation:

- Configure the backup infrastructure as described in the Veeam Backup for Nutanix AHV User Guide, section Deployment.
- If you restore Azure VMs from standard backups, make sure that these backups have been copied to an on-premises backup repository as described in the Veeam Backup & Replication User Guide, section Creating Backup Copy Jobs for VMs and Physical Machines.
- If you restore Azure VMs from backups copied to the Archive access tier of a scale-out backup repository, make sure to retrieve these backups from archive as described in the Veeam Backup & Replication User Guide, section Retrieving Backup Files.

To restore an Azure VM to a Nutanix AHV cluster, do the following:

1. In the Veeam Backup & Replication console, open the **Home** view.
2. Navigate to **Backups** > **Disk (Copy)**.
3. Expand the backup policy that protects an Azure VM you want to restore, select the necessary VM and click **Entire VM** on the ribbon.

4. Complete the **Restore to Nutanix AHV** wizard as described in the Veeam Backup for Nutanix AHV User Guide, section Restoring VMs Using Veeam Backup & Replication Console.



# Reviewing Dashboard

Veeam Backup for Microsoft Azure comes with an **Overview** dashboard that provides at-a-glance real-time overview of the protected Azure resources and allows you to estimate the overall backup performance. The dashboard includes the following widgets:

- **Sessions for Last 24 Hours** – displays the number of all sessions started for data protection and disaster recovery operations (including system sessions) that completed successfully during the past 24 hours, the number of sessions that completed with warnings, the number of sessions that completed with errors, and the number of sessions that are currently running.

  To get more information on the sessions, click either **View Session Logs** or any of the widget rows. In the latter case, the **Session Log** tab will show only those sessions that have the same status as that clicked in the widget.

  For more information on the **Session Log** tab, see Viewing Session Statistics.

- **Successful Task Ratio** – displays the number of snapshots, backups and archived backups successfully created by backup policies during a specific time period (the past 24 hours by default), and the number of attempts that were made to create these restore points.

  To specify the time period, click the link next to the **Schedule** icon. To get more information on the created snapshots, backups or archived backups, click any of the widget rows. In the latter case, the **Session Log** tab will show only those sessions during which Veeam Backup for Microsoft Azure created the same items as that clicked in the widget.

  For more information on the **Session Log** tab, see Viewing Session Statistics.

- **Top Policies** – shows top 8 backup policies for fluctuations in execution time (including retries). For each policy, the widget calculates the growth rate to detect whether it took less or more time for the policy to complete in comparison with the previous policy run.

- **Protected Workloads** – displays the number of available Azure resources that got protected by Veeam Backup for Microsoft Azure during a specific time period (the past 24 hours by default).

  To specify the time period, click the link next to the **Schedule** icon. To get more information on the protected resources, click any of the widget rows.

  For more information on the available resources, their properties and the actions you can perform for the resources, see Viewing Available Resources.

- **Storage Usage** – displays the amount of storage space that is currently consumed by backups and archived backups created by Veeam Backup for Microsoft Azure in blob containers, and the number of snapshots created for the protected resources. The widget also calculates the ratio of the total amount of storage space used in the Standard Storage class to the total amount of storage space used in the Cool, Hot and Archive access tiers.

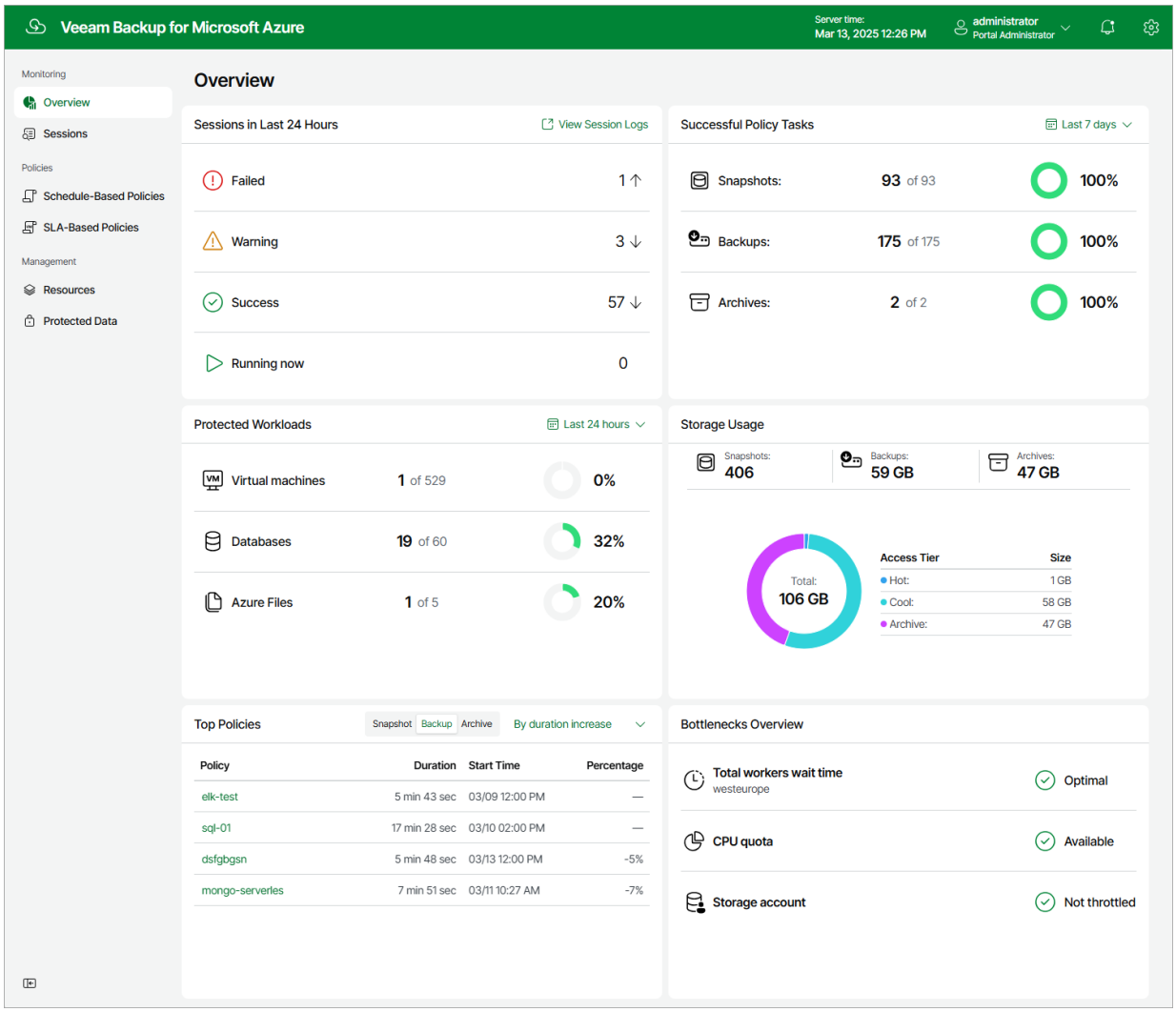
- **Bottlenecks Overview** – is designed to help you avoid possible backup bottlenecks.

  The widget analyzes the total amount of time waited to launch worker instances during data protection operations in different Azure regions, and displays the most problematic region (if any).

  The widget also analyzes the amount of CPU quota across all regions to detect whether the quota has already been reached in any of the regions, and whether Veeam Backup for Microsoft Azure failed to launch a worker instance in that region during a backup or restore process. For more information on VM sizes of Azure VMs that operate as worker instances, see Managing Worker Instances.

  The widget also analyzes the number of management operations performed in Azure storage accounts where Veeam Backup for Microsoft Azure writes data to backup repositories, and displays a warning if the storage throttling limit for any of these accounts has been breached.

To learn how to resolve a bottleneck, click the **How to resolve?** link in the widget row.



# Viewing Session Statistics

For each performed data protection or disaster recovery operation, Veeam Backup for Microsoft Azure starts a new session and stores its records in the configuration database.

## Viewing Session Statistics Using Veeam Backup & Replication Console

You can track real-time statistics of all running and completed operations on the **Jobs**, **Last 24 hours** and **Running** nodes. For more information, see Veeam Backup & Replication User Guide, sections Viewing Real-Time Statistics and Viewing Job Session Results.

Veeam Backup & Replication also allows you track statistics of data recovery operations initiated from Veeam Backup for Microsoft Azure. To do that, do either of the following:

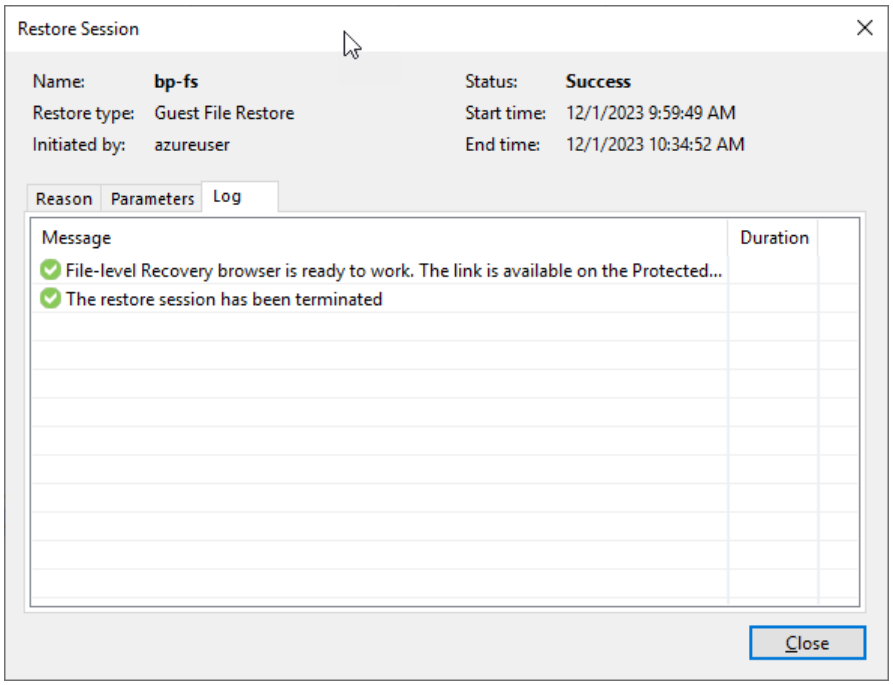
- In the Veeam Backup & Replication console, open the **Home** view and navigate to **Last 24 hours**. In the working area, double-click the necessary restore session.

  Alternatively, select the session and click **Statistics** on the ribbon.

- In the Veeam Backup & Replication console, open the **History** view and navigate to **Restore**. In the working area, double-click the necessary restore session.

  Alternatively, select the session and click **Statistics** on the ribbon.

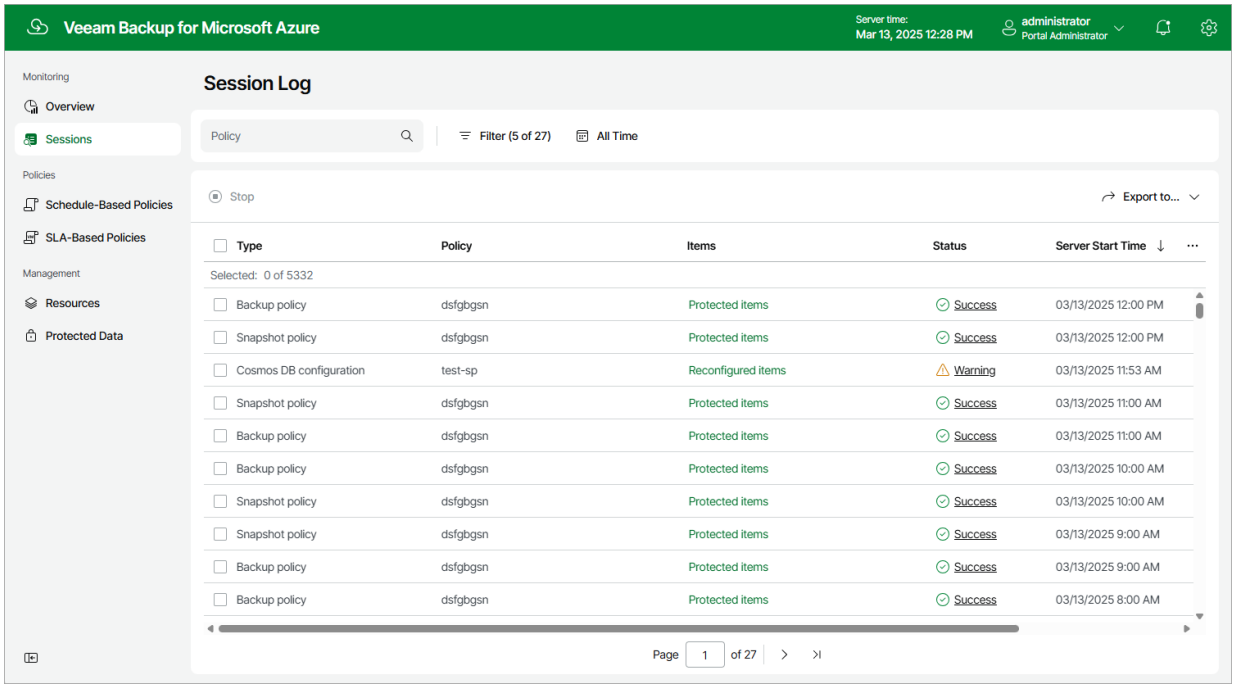
The **Restore Session** window will display restore session details such as the name of the VM instance whose data is being restored, the account under which the session has started, the session status and duration, information on the restore point selected for the restore operation, and the list of tasks performed during the session.



# Viewing Session Statistics Using Veeam Backup for Microsoft Azure Web UI

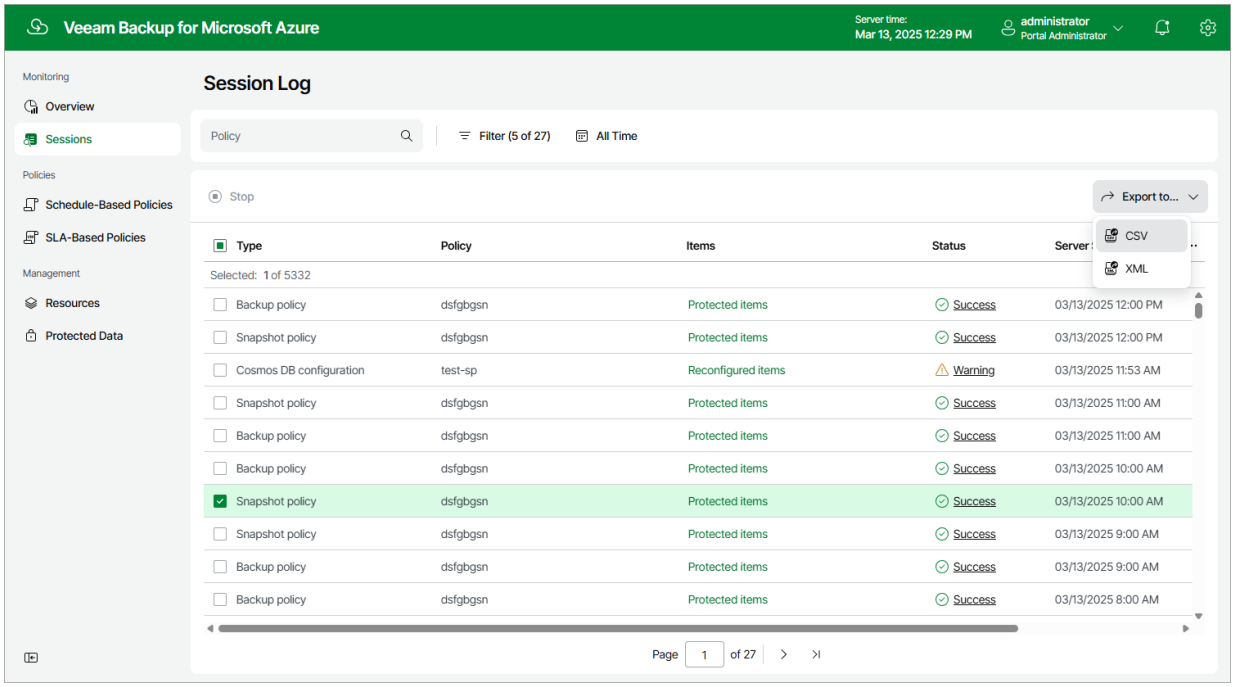
You can track real-time statistics of all running and completed operations on the **Sessions** tab. To view the full list of tasks executed during an operation, click the link in the **Status** column. To view the full list of Azure resources processed during an operation, click the link in the **Items** column.

> **TIP**
>
> If you want to specify the time period during which Veeam Backup for Microsoft Azure will keep session records in the configuration database, follow the instructions provided in section Configuring Global Retention Settings.



# Collecting Object Properties

You can export properties of objects managed by Veeam Backup for Microsoft Azure as a single file in the CSV or XML format. To do that, navigate to the necessary tab, select the objects whose properties you want to export and click **Export to**. Veeam Backup for Microsoft Azure will save the file with the exported data to the default download directory on the local machine.



# Updating Veeam Backup for Microsoft Azure

Veeam Backup for Microsoft Azure allows you to check for new product versions and available package updates. It is recommended that you timely install available package updates to avoid performance issues while working with the product. For example, timely installed security updates may help you prevent potential security issues and reduce the risk of compromising sensitive data.

# Updating Appliances Using Console

Starting from Veeam Backup for Microsoft Azure version 5a, you can upgrade backup appliances from the Veeam Backup & Replication console only. Direct upgrade to Veeam Backup for Microsoft Azure version 8 is supported from Veeam Backup for Microsoft Azure version 6.0 or later. To upgrade from an earlier version, you must first perform upgrade to Veeam Backup for Microsoft Azure version 6.0 or 7.0.

**IMPORTANT**

Consider the following:

- Before you upgrade a backup appliance, check whether the Veeam Backup for Microsoft Azure version is compatible with the current version of Microsoft Azure Plug-in for Veeam Backup & Replication. For more information, see System Requirements.
- If your backup appliance used the Azure Service Bus messaging service in versions prior to version 8, you must switch to the Azure Queue Storage service in the appliance Web UI immediately after you upgrade to version 8. Otherwise, Veeam Backup for Microsoft Azure will no longer be able to perform backup and restore operations. For more information, see Configuring Deployment Mode.

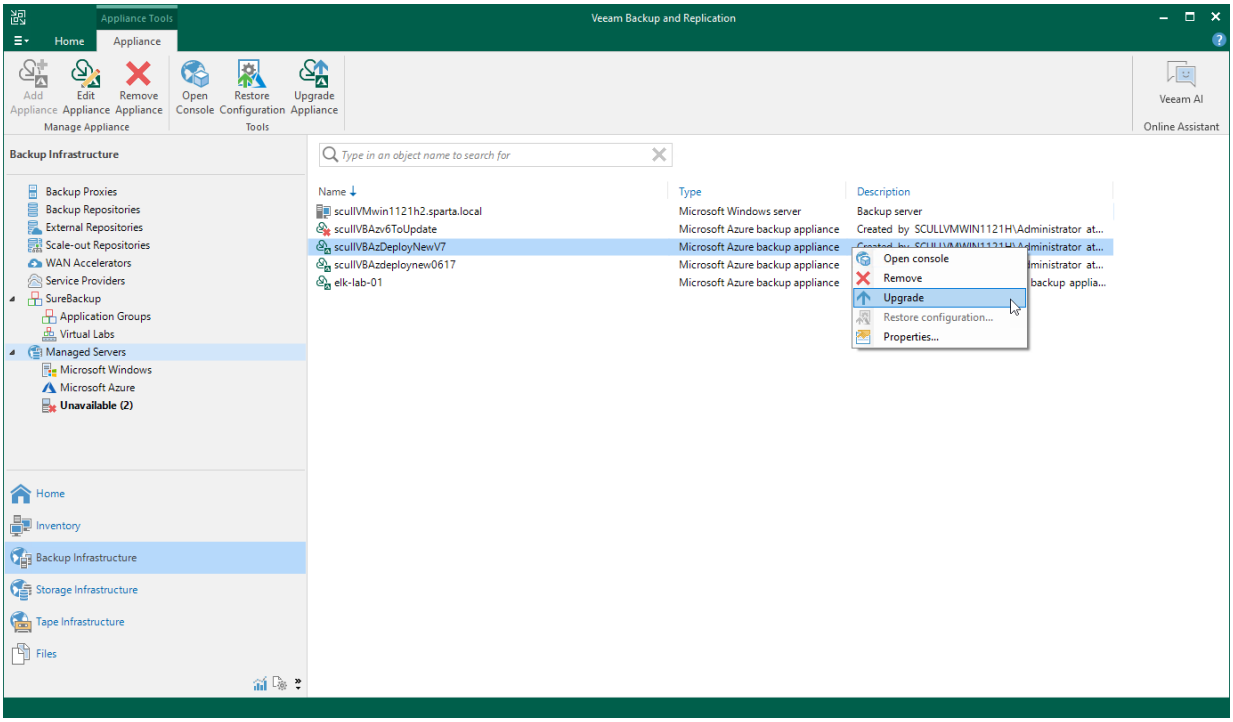
Microsoft Azure Plug-in for Veeam Backup & Replication allows you to download and install new available Veeam Backup for Microsoft Azure versions and package updates:

1. In the Veeam Backup & Replication console, open the **Backup Infrastructure** view.
2. Navigate to **Managed Servers**.
3. Select the necessary backup appliance and click **Upgrade Appliance** on the ribbon.

   Alternatively, right-click the appliance and select **Upgrade**.

**NOTE**

As soon as you click **Upgrade Appliance**, Veeam Backup & Replication will verify connection to the specified backup appliance. If the appliance is assigned a dynamic IP address, you will receive a warning regarding the retirement of these IP addresses. To learn how to eliminate this warning, see Eliminating Warnings.


Appliance Tools
Veeam Backup and Replication
Home
Appliance
Add Appliance
Edit Appliance
Remove Appliance
Manage Appliance
Open Console
Restore Configuration
Upgrade Appliance
Tools
Veeam AI
Online Assistant
Backup Infrastructure
Type in an object name to search for
Backup Proxies
Backup Repositories
External Repositories
Scale-out Repositories
WAN Accelerators
Service Providers
SureBackup
Application Groups
Virtual Labs
Managed Servers
Microsoft Windows
Microsoft Azure
Unavailable (2)
Name
Type
Description
scullVMwin1121h2.sparta.local
Microsoft Windows server
Backup server
scullVBAzv6ToUpdate
Microsoft Azure backup appliance
Created by SCULLVMWIN1121H\Administrator at...
scullVBAzDeployNewV7
Microsoft Azure backup appliance
scullVBAzdeploynew0617
Microsoft Azure backup appliance
elk-lab-01
Microsoft Azure backup appliance
backup applia...
Open console
Remove
Upgrade
Restore configuration...
Properties...
Home
Inventory
Backup Infrastructure
Storage Infrastructure
Tape Infrastructure
Files

# Upgrading to Version 6.0 or 7.0 from Version 5.0 or Earlier

To upgrade Veeam Backup for Microsoft Azure to version 6.0 or 7.0, a backup appliance must be running version 3.0 or later. To upgrade the appliance, check the prerequisites and follow the instructions provided in section Updating Appliances Using Console.

When you perform upgrade to Veeam Backup for Microsoft Azure version 6.0 or 7.0 from Veeam Backup for Microsoft Azure version 5.0 or earlier, the backup appliance operating system is upgraded from Ubuntu 18.04 LTS to Ubuntu 22.04 LTS, and the configuration database is upgraded to PostgreSQL 15.5. Consider that the upgrade procedure includes re-deployment of the backup appliance on a new Azure VM and attachment of data disks from the previous appliance to this new Azure VM.

## How Upgrade to Version 6.0 or 7.0 Works

When upgrading backup appliances to version 6.0 or 7.0 from Veeam Backup for Microsoft Azure version 5.0 or earlier, Veeam Backup & Replication performs the following steps:

1. Instructs Veeam Backup for Microsoft Azure to create a cloud-native snapshot of the original appliance. If the upgrade process fails, the appliance will be reverted to the created snapshot.

   Consider that this snapshot will not be automatically removed by Veeam Backup & Replication from Microsoft Azure after the upgrade operation completes successfully. You can remove this snapshot manually if you no longer need it, or keep it in case you will need to roll back the appliance to the previous state.

2. Upgrades version of the appliance configuration database to PostgreSQL 15.5: creates a new PostgreSQL database on the virtual data disk of the original appliance, copies all configuration data to this database and removes the old database.

3. Saves the following configuration files and settings to the virtual data disk of the original appliance: the appliance configuration file (`/etc/veeam/azurebackup/Config.ini`), users, MFA and time zone settings, and Linux environment (`/etc/ssh/`, `/root/`, `/home/`).

4. Detaches the virtual data disk from the original Azure VM and removes the VM from Microsoft Azure.

5. Launches a new Azure VM with the same name and network configuration from the Veeam Backup for Microsoft Azure version 6.0 or 7.0 image. By default, the launched VM will have 2 disks attached: one OS disk containing Ubuntu 22.04 LTS as an operating system and one empty virtual data disk.

6. Attaches the virtual data disk of the original appliance to the newly created appliance.

7. Restores the configuration files and settings saved at step 3 to the new OS disk.

8. Detaches the default virtual data disk from the newly created appliance and removes the disk from Microsoft Azure.

9. Removes the OS disk of the original Azure VM from Microsoft Azure.

## Limitations and Prerequisites

Before you start the upgrade process, consider the following requirements and limitations:

- The Microsoft Azure compute account (service account) specified when deploying a backup appliance or connecting to the appliance must be assigned permissions required to perform upgrade. For the list of required permissions, see Plug-In Permissions.

- Outbound internet access must be allowed from the backup appliance to the PostgreSQL APT repository (*apt.postgresql.org*, *apt-archive.postgresql.org*) through port **80** over the HTTP protocol.
- Outbound internet access must be allowed from the backup appliance to the PostgreSQL website (*postgresql.org*) through port **443** over the HTTPS protocol to download the repository key https://www.postgresql.org/media/keys/ACCC4CF8.asc.
- Outbound internet access must be allowed from the backup appliance to the Veeam Update Notification Server through port **443** over the HTTPS protocol.
- Outbound internet access must be allowed from the backup appliance to the Ubuntu Security Repository through port **80** over the HTTP protocol.
- During upgrade, the data disk of the backup appliance will temporarily contain files of 2 databases. That is why the size of the data disk must be twice the total amount of storage space used by the configuration database.
- During upgrade, Veeam Backup & Replication will create the new root virtual disk with the default settings. That is why if you have modified root disk settings, for example have increased disk size, these settings will not be transferred, and custom 3rd-party software installed on the backup appliance will not be migrated.

# Updating Appliances Using Web UI

Veeam Backup for Microsoft Azure automatically notifies you about newly released product versions and package updates available for the operating system running on the backup appliance. However, starting from Veeam Backup for Microsoft Azure version 5a, you can use the Veeam Backup for Microsoft Azure Web UI to install package updates only. To upgrade Veeam Backup for Microsoft Azure to new versions, follow the instructions provided in section Updating Appliances Using Console.

# Upgrading Appliances

Starting from Veeam Backup for Microsoft Azure version 5a, you can upgrade backup appliances from the Veeam Backup & Replication console only. Direct upgrade to Veeam Backup for Microsoft Azure version 8 is supported from Veeam Backup for Microsoft Azure version 6.0 or later. To upgrade from an earlier version, you must first perform upgrade to Veeam Backup for Microsoft Azure version 6.0 or 7.0 as described in section Upgrading to Version 6.0 or 7.0 from Version 5.0 or Earlier.

**IMPORTANT**

- Before you upgrade a backup appliance, make sure that all backup policies are both disabled and stopped, and no restore tasks are currently executing. Otherwise, the update process will interrupt the running activities, which may result in data loss.
- If your backup appliance used the Azure Service Bus messaging service in versions prior to version 8, you must switch to the Azure Queue Storage service immediately after you upgrade to version 8. Otherwise, Veeam Backup for Microsoft Azure will no longer be able to perform backup and restore operations. For more information, see Configuring Deployment Mode.

To upgrade a backup appliance, do the following:

1. Install Microsoft Azure Plug-in for Veeam Backup & Replication as described in section Deployment.

   If you do not have a valid Veeam Backup & Replication license, you can download a 30-day trial version of the product.

2. Add the backup appliance to the Veeam Backup & Replication infrastructure as described in section Connecting to Existing Appliances.

   When connecting to the backup appliance, Veeam Backup & Replication will display a warning notifying you that the appliance must be upgraded. Acknowledge the warning to allow Veeam Backup & Replication to automatically upgrade the appliance to the necessary version.

**NOTE**

When you add a backup appliance to the Veeam Backup & Replication infrastructure, the license installed on the appliance becomes invalid. Protected instances start consuming license units from the license installed on the Veeam Backup & Replication server. However, as soon as you remove the backup appliance from the Veeam Backup & Replication infrastructure, Veeam Backup for Microsoft Azure will continue using the license that had been used before you added the backup appliance to the Veeam Backup & Replication infrastructure.

For more information on licensing scenarios, see Licensing.

3. [Applies only if the backup appliance has not been upgraded at step 2] Upgrade the appliance as described in section Updating Appliances Using Console.

4. After the upgrade process completes, you can remove the backup appliance from the Veeam Backup & Replication infrastructure, as described in section Removing Appliances, if you do not plan to further manage this appliance from the Veeam Backup & Replication console.

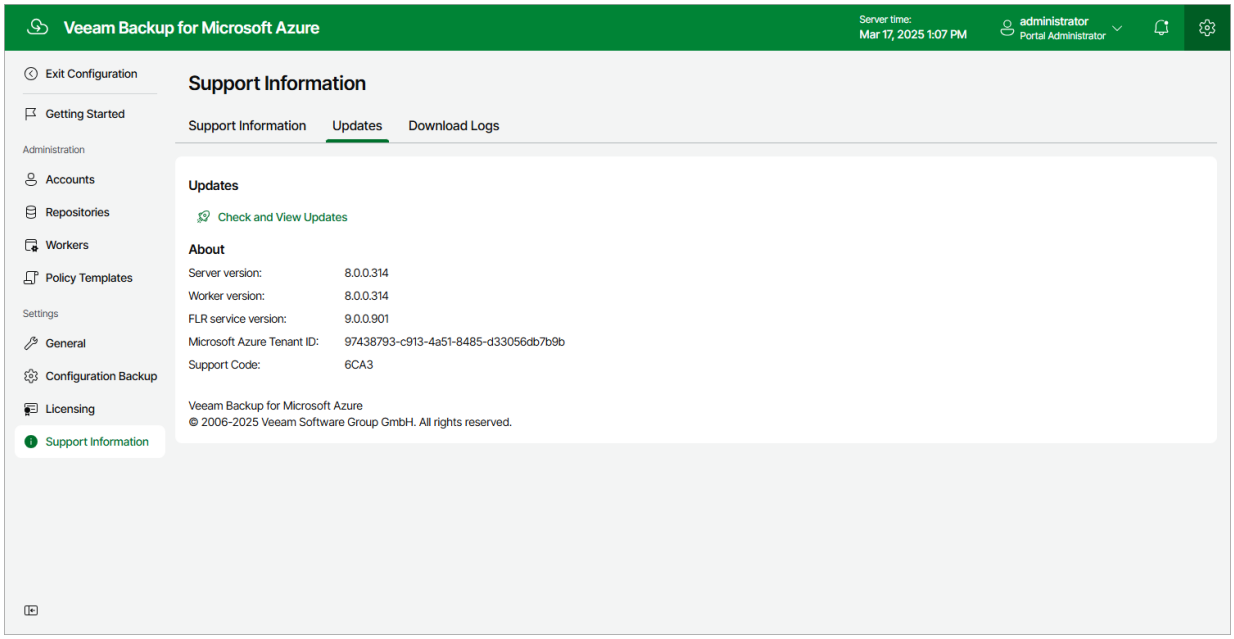
   Make sure to remove the appliance from the Veeam Backup & Replication infrastructure before you uninstall Veeam Backup & Replication. Otherwise, Veeam Backup for Microsoft Azure will not be able to perform backup and restore operations due to the licensing issues.

   If you remove the backup appliance from the backup infrastructure, you will no longer be able to create backups of virtual network configurations and Cosmos DB accounts. For more information, see Integration with Veeam Backup & Replication.

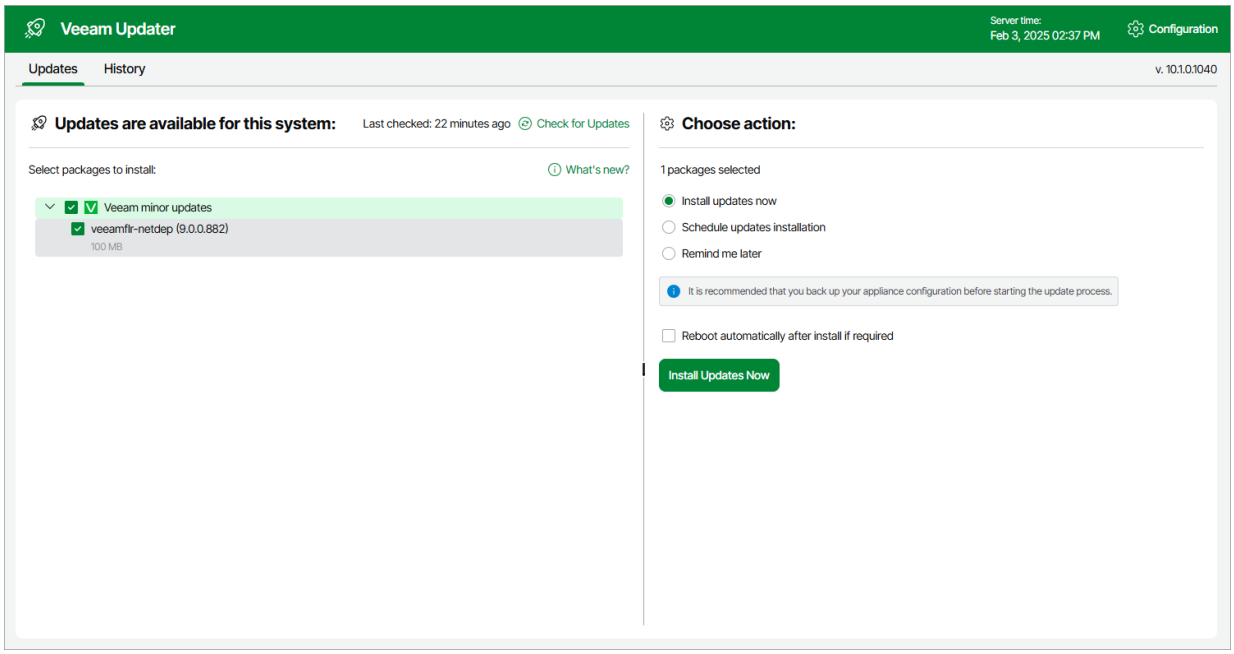
# Checking for Updates

Veeam Backup for Microsoft Azure automatically notifies you about newly released product versions and package updates available for the operating system running on your backup appliance. However, you can check for the available updates manually if required:

1. Switch to the **Configuration** page.
2. Navigate to **Support Information**.
3. Switch to the **Updates** tab.
4. Click **Check and View Updates**.




If new updates are available, Veeam Backup for Microsoft Azure will display them on the **Updates** tab of the **Veeam Updater** page. To view detailed information on an update, select the check box next to the update and click **What's new?**



# Installing Updates

To download and install new product versions and available package updates, you can do either of the following:

- Install updates immediately
- Schedule update installation

You can also set a reminder to send update notifications.

> **IMPORTANT**
>
> - Updating standalone backup appliances manually is not supported. You can update these appliances using the Veeam Updater service only.
> - Updating backup appliances managed by Veeam Backup & Replication servers backup appliances using the Veeam Updater service is not supported. You can update these appliances using the Veeam Backup & Replication as described in section Updating Appliances Using Console.

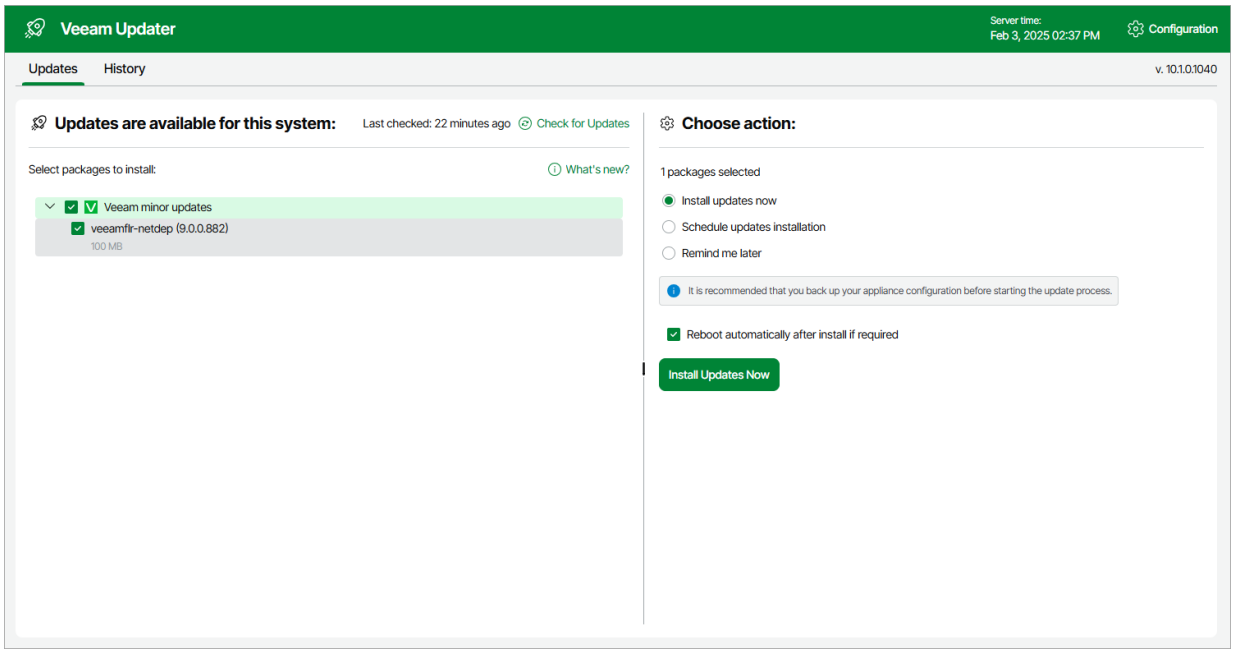
# Installing Updates

> **IMPORTANT**
>
> Before you install a product update, make sure that all backup policies are both disabled and stopped, and no restore tasks are currently executing. Otherwise, the update process will interrupt the running activities, which may result in data loss.

To download and install available product and package updates:

1. Open the **Veeam Updater** page:
   a. Switch to the **Configuration** page.
   b. Navigate to **Support Information**.
   c. Switch to the **Updates** tab.
   d. Click **Check and View Updates**.
2. On the **Veeam Updater** page, do the following:
   a. In the **Updates are available for this system** section, select check boxes next to the necessary updates.
   b. In the **Choose action** section, select the **Install updates now** option, select the **Reboot automatically after install if required** check box to allow Veeam Backup for Microsoft Azure to reboot the backup appliance if needed, and then click **Install Updates Now**.

> **NOTE**
>
> The updater may require you to read and accept the Veeam license agreement and the 3rd party components license agreement. If you reject the agreements, you will not be able to continue installation.




Veeam Backup for Microsoft Azure will download and install the updates; the results of the installation process will be displayed on the History tab. Keep in mind that it may take several minutes for the installation process to complete.

> **NOTE**
>
> When installing product updates, Veeam Backup for Microsoft Azure restarts all services running on the backup appliance, including the Web UI service. That is why Veeam Backup for Microsoft Azure may log you out when the update process completes.

# Scheduling Update Installation

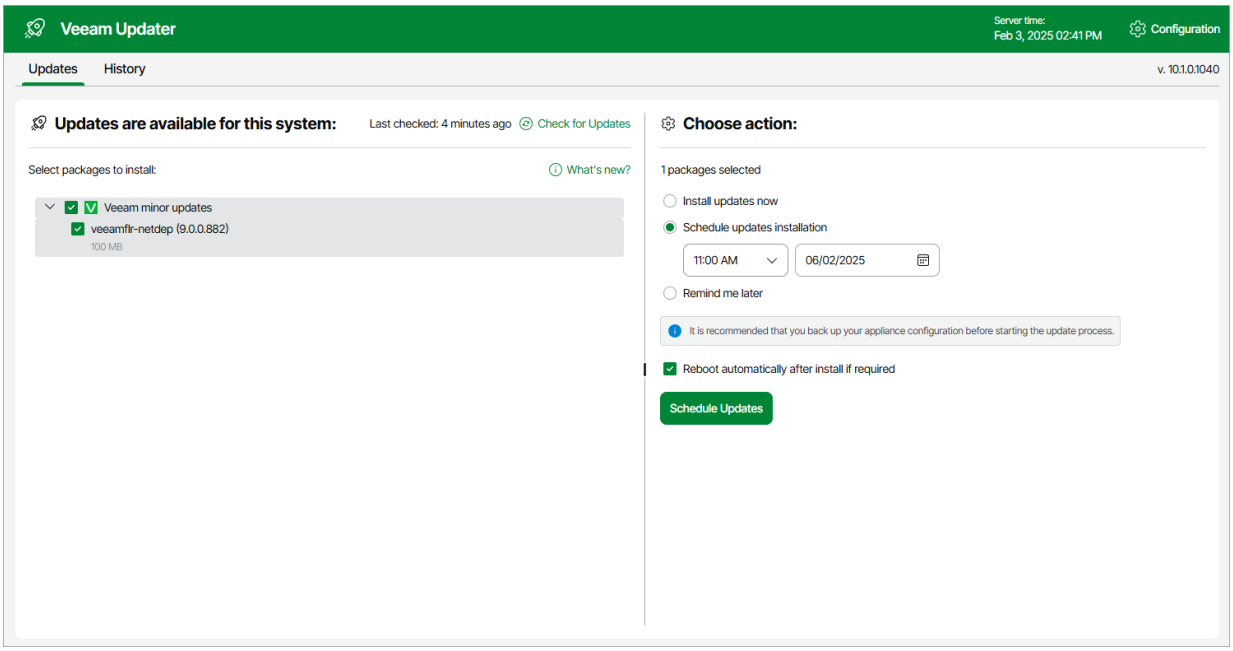
You can instruct Veeam Backup for Microsoft Azure to automatically download and install available product versions and package updates on a specific date at a specific time:

1. On the **Veeam Updater** page, in the **Updates are available for this system** section, select check boxes next to the necessary updates.
2. In the **Choose action** section, do the following:
   a. Select the **Schedule updates installation** option and configure the necessary schedule.

> **IMPORTANT**
>
> When selecting a date and time when updates must be installed, make sure no backup policies are scheduled to run at the selected time. Otherwise, the update process will interrupt the running activities, which may result in data loss.

   b. Select the **Reboot automatically after install if required** check box to allow Veeam Backup for Microsoft Azure to reboot the backup appliance if needed.

c. Click **Schedule Updates**.




Veeam Backup for Microsoft Azure will automatically download and install the updates on the selected date at the selected time; the results of the installation process will be displayed on the History tab.

# Setting Update Reminder

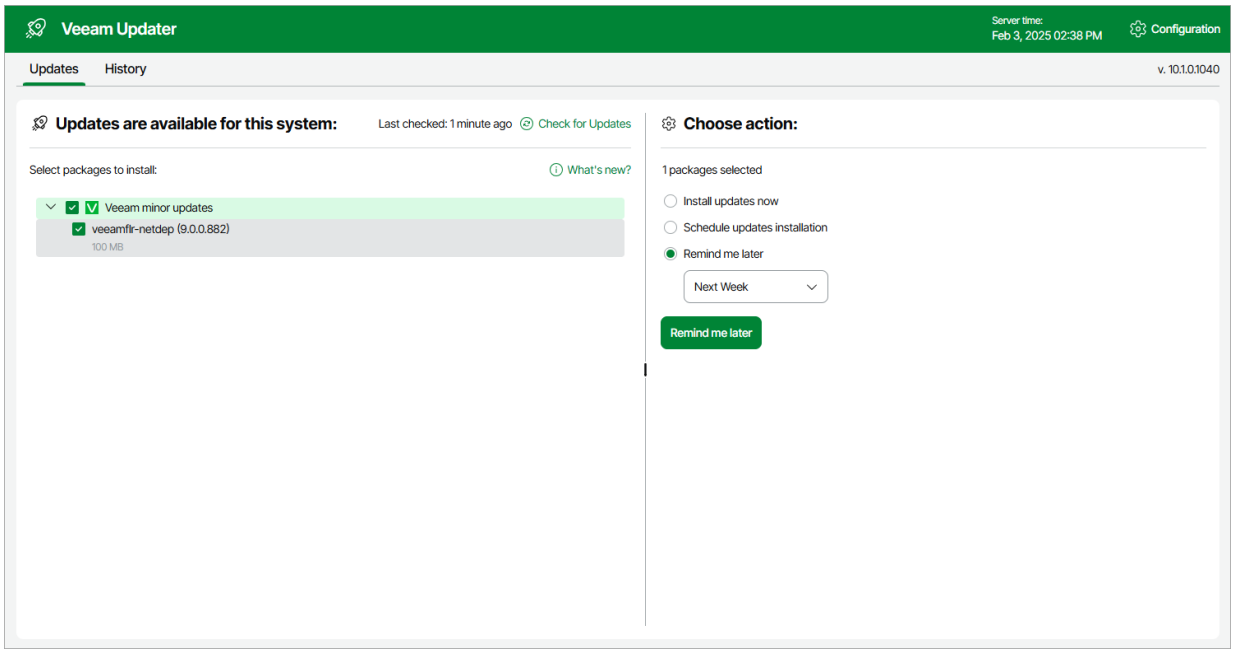
If you have not decided when to install available product versions and package updates, you can set an update reminder — instruct Veeam Backup for Microsoft Azure to send an update notification later.

To do that, on the **Veeam Updater** page, in the **Choose action** section, do the following:

1. Select the **Remind me later** option and choose when you want to receive the reminder.

   If you select the **Next Week** option, Veeam Backup for Microsoft Azure will send the reminder on the following Monday.

2. Click **Remind me later**.



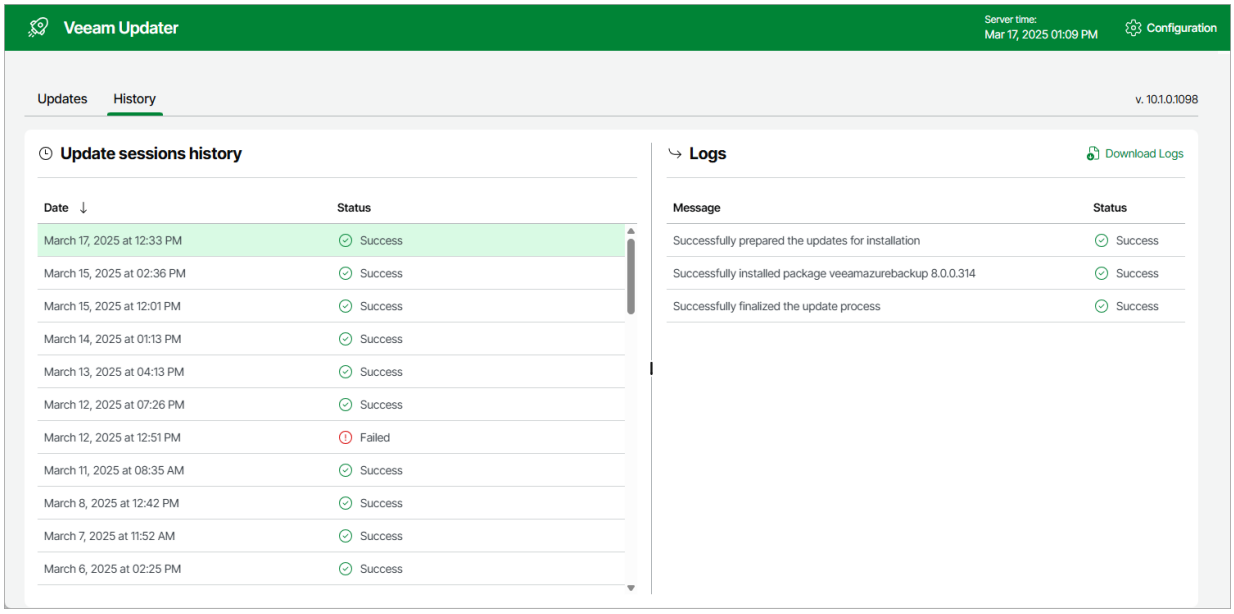
# Viewing Update History

To see the results of the update installation performed on the backup appliance, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **Support Information**.
3. Switch to the **Updates** tab.
4. Click **Check and View Updates**.
5. On the **Veeam Updater** page, switch to the **History** tab.

For each date when an update was installed, the **Veeam Updater** page will display the name of the update and its status (whether the installation process completed successfully, completed with warnings or failed to complete).

To download logs for the installed updates, select the necessary date in the **Date** section, and click **View Full Log**. Veeam Backup for Microsoft Azure will save the logs as a single file to the default download directory on the local machine.



# Configuring Web Proxy

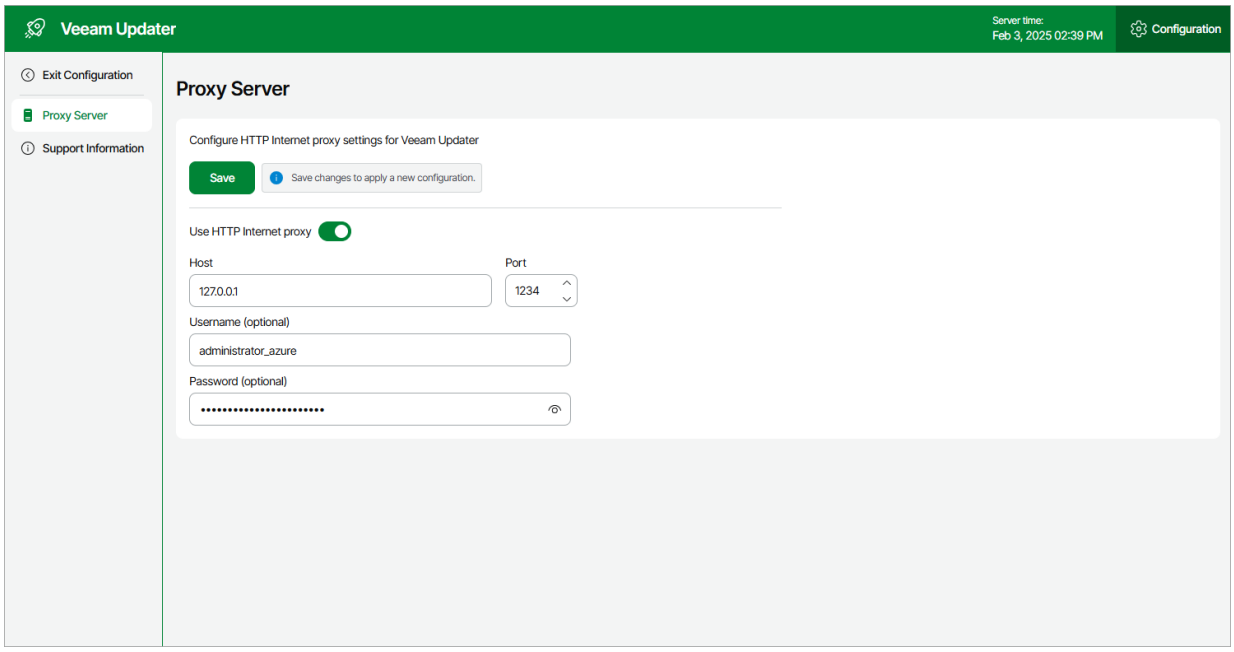
To check for available package updates for Veeam Backup for Microsoft Azure, the Veeam Updater service running on the backup appliance connects to Veeam repositories over the internet. If the backup appliance is not connected to the internet, you can instruct Veeam Backup for Microsoft Azure to use a web proxy that will provide access to the required resources.

> **IMPORTANT**
>
> Veeam Backup for Microsoft Azure does not support access to resources through HTTPS proxy.

To configure connection to the internet through a web proxy, do the following:

1. Open the **Veeam Updater** page:
   a. Switch to the **Configuration** page.
   b. Navigate to **Support Information**.
   c. On the **Updates** tab, click **Check and View Updates**.
2. On the **Veeam Updater** page:
   a. Switch to the **Configuration** page.
   b. Navigate to **Proxy Server**.
   c. Set the **Use Internet proxy** toggle to *On*.
   d. In the **Host** field, enter the IP address or FQDN of the web proxy.
   e. In the **Port** field, enter the port used on the web proxy for HTTP or HTTPS connections.
   f. [Applies only if the web proxy requires authentication] In the **Username** and **Password** fields, enter credentials of the user account configured on the web proxy to access the internet.
   g. Click **Apply**.

> **IMPORTANT**
>
> You cannot modify the web proxy settings during checking for updates.


Veeam Updater
Server time:
Feb 3, 2025 02:39 PM
Configuration
Exit Configuration
Proxy Server
Support Information
Proxy Server
Configure HTTP Internet proxy settings for Veeam Updater
Save
Save changes to apply a new configuration.
Use HTTP Internet proxy
Host
127.0.0.1
Port
1234
Username (optional)
administrator_azure
Password (optional)

# Getting Technical Support

If you have any questions or issues with Veeam Backup for Microsoft Azure, you can search for a resolution on Veeam R&D Forums or submit a support case in the Veeam Customer Support Portal.

When you submit a support case, it is recommended that you provide the Veeam Customer Support Team with the following information:

- Version information for the product and its components
- The error message or an accurate description of the problem you are facing
- Log files

## Viewing Product Details Using Veeam Backup for Microsoft Azure Web UI

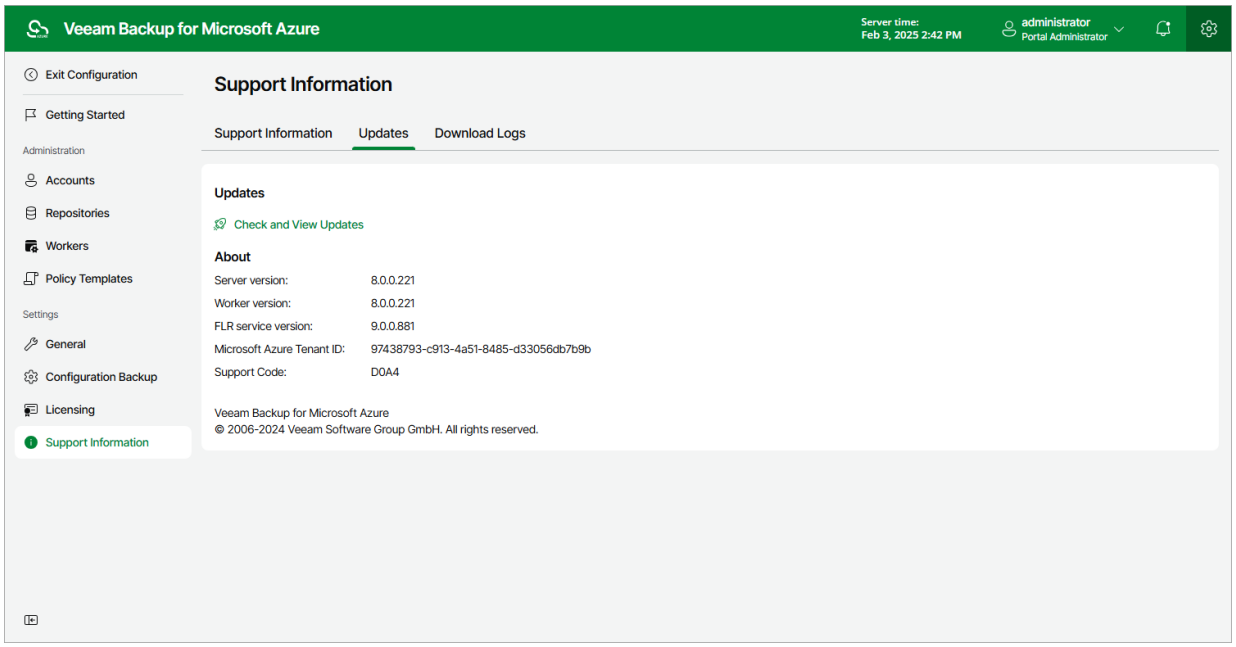
To view the product details, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **Support Information** > **Updates**.

The **About** section of the **Updates** page displays the following information:

- **Server version** — the currently installed version of Veeam Backup for Microsoft Azure.
- **Worker version** — the version of worker instances launched by Veeam Backup for Microsoft Azure.
- **FLR service version** — the version of the File-level recovery service currently running on the backup appliance.
- **Microsoft Entra tenant ID** — the unique identification number of the Microsoft Entra tenant to which the backup appliance belongs.
- **Support Code** — the unique identification number of the Veeam support contract.

> **TIP**
>
> You can click the link in the **Updates** section to check for, download and install new product versions and available package updates. For more information, see Updating Veeam Backup for Microsoft Azure.



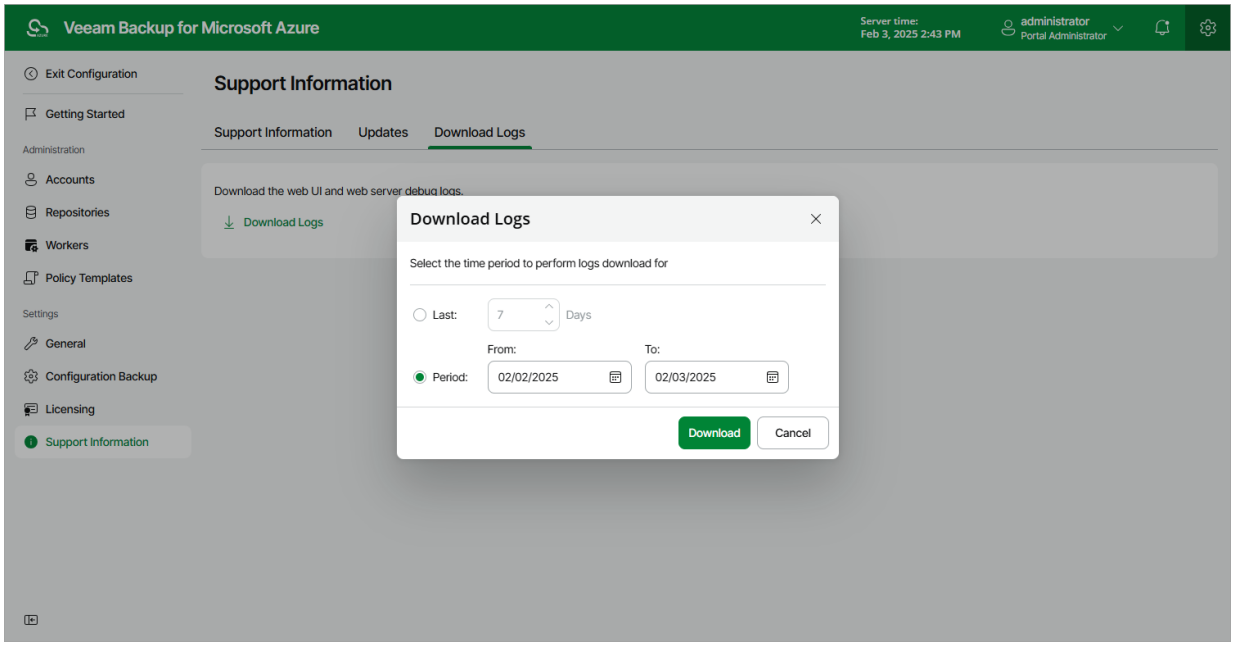

# Downloading Product Logs Using Veeam Backup for Microsoft Azure Web UI

To download the product logs, do the following:

1. Switch to the **Download Logs** tab.
2. Click **Download Logs**.
3. In the **Download Logs** window, specify a time interval for which the logs will be collected:
   - Select the **Last** option if you want to collect data for a specific number of days in the past.

- Select the **Period** option if you want to collect data for a specific period of time in the past.

After you click **Download**, the logs will be saved locally in the default download folder as a single .ZIP archive.

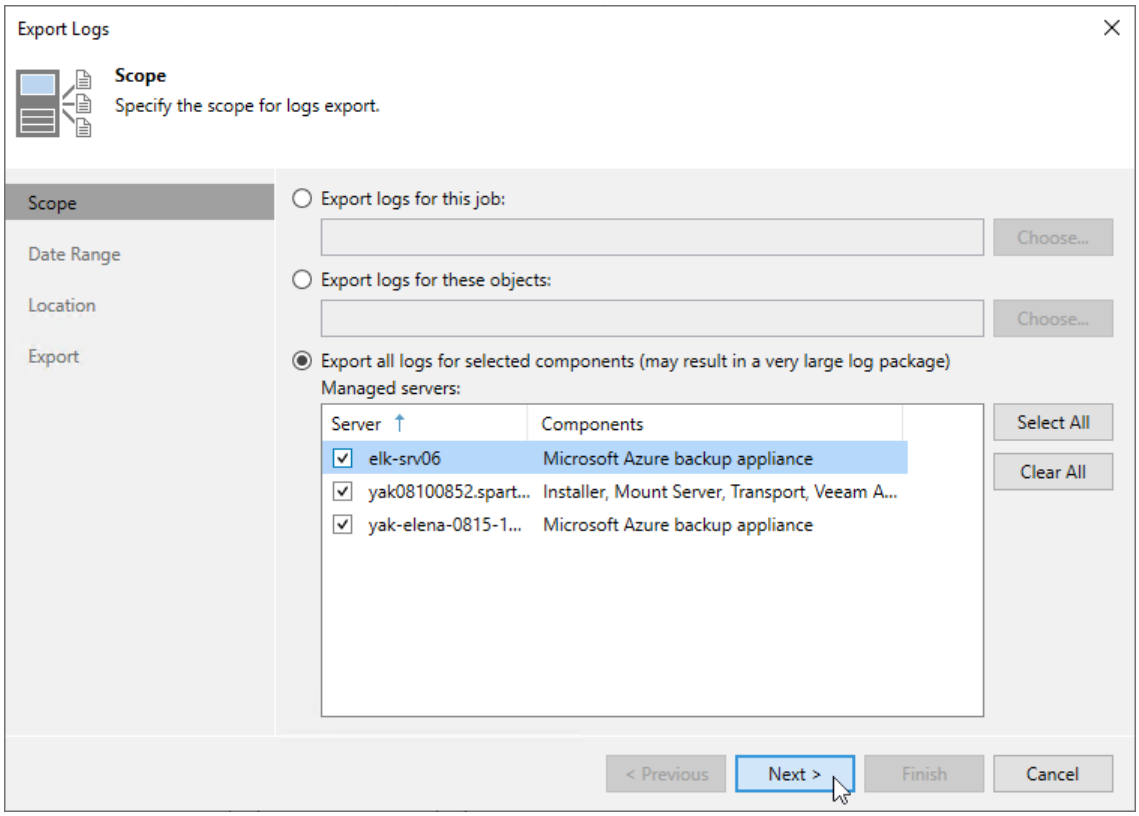



# Downloading Product Logs Using Veeam Backup & Replication Console

To export the product logs, do the following:

1. In the Veeam Backup & Replication console, open the main menu and navigate to **Help** > **Support Information**.
2. In the **Export Logs** wizard, do the following:
   a. At the **Scope** step, select the **Export all logs for selected components** option. Then, in the **Managed servers** list, select the backup server, backup appliances and other components for which you want to export logs.

b. Complete the wizard as described in the Veeam Backup & Replication User Guide, section Export Logs.



# Configuring HTTP Proxy for Backup Appliances

To manage the inbound and outbound traffic of your backup appliance, you can configure an HTTP proxy. Using an HTTP proxy provides access to the required services and resources, enhancing the security, efficiency and privacy of your backup environment.

> **NOTE**
>
> The provided instruction does not apply to worker instances that are deployed to perform backup and restore operations, as well as to the Veeam Updater service. To learn how to configure an HTTP proxy for the Veeam Updater service, see Configuring Web Proxy.

To configure connection to the internet through an HTTP proxy, do the following:

1. On the Azure VM on which Veeam Backup for Microsoft Azure is installed, open the configuration file used to set global environment variables by running the following command in a terminal window:

   ```
   sudo nano /etc/environment
   ```

3. In the configuration file, do the following:

   a. Add a connection to an HTTP proxy server by setting the `http_proxy="http://host:port"` variable.

   b. Add a connection to an HTTPS proxy server by setting the `https_proxy="http://host:port"` variable.

      The `https_proxy` variable must have the same HTTP proxy address specified in its value as the `http_proxy` variable.

> **IMPORTANT**
>
> Veeam Backup for Microsoft Azure does not support access to resources through HTTPS proxy. The `https_proxy` variable is used only to ensure that the HTTPS traffic is sent to the HTTP proxy.

   c. [Applies only if the proxy server requires authentication] To authenticate against the proxy server, set the `http_proxy="http://username:password@host:port"` or the `https_proxy="http://username:password@host:port"` variable.

   d. Specify the IP addresses that are not required to use the proxy to connect to your backup appliance by setting the `NO_PROXY="<addresses>"` variable, where `<addresses>` is a comma-separated list of necessary IP addresses or DNS names.

      The list must include the following addresses: `169.254.169.254` — the IP address of the Azure Instance Metadata Service (IMDS), `localhost` and `127.0.0.1` — the DNS name and the IP address of your local machine.

   e. Save the changes and close the configuration file.

4. To apply changes, reboot the Azure VM on which Veeam Backup for Microsoft Azure is installed.

5. Use either Azure network security groups or firewall rules to allow inbound and outbound access to the Azure VM on which Veeam Backup for Microsoft Azure is installed for all necessary IP addresses including those of your backup server, the HTTP proxy itself, IMDS, and so on.

   Note that Veeam Backup for Microsoft Azure version 8 does not support connection to email server specified in the notification settings through an HTTP proxy. If you plan to configure these settings, you must allow inbound and outbound access to the Azure VM on which Veeam Backup for Microsoft Azure is installed for the necessary email server.

**IMPORTANT**

- For Veeam Backup for Microsoft Azure to be able to create and manage backup repositories when using the configured HTTP proxy, open a support case.
- The provided instruction applies to backup appliances that operate public virtual networks. If you want to configure an HTTP proxy for a backup appliance deployed in a private environment, open a support case.