Contents

CONTACTING VEEAM SOFTWARE ........................................................................................................ 7
ABOUT THIS DOCUMENT ....................................................................................................................... 8
WELCOME TO VEEAM BACKUP FOR MICROSOFT AZURE ................................................................ 9
INTEGRATION WITH VEEAM BACKUP & REPLICATION .................................................................... 10
PLANNING AND PREPARATION ........................................................................................................... 11
  Azure Account Permissions .................................................................................................................. 11
  Azure Service Account Permissions ................................................................................................... 11
  Azure Repository Account Permissions .............................................................................................. 14
Ports ..................................................................................................................................................... 15
Azure Services ...................................................................................................................................... 16
Azure Resource Providers ..................................................................................................................... 17
Considerations and Limitations ............................................................................................................ 18
LICENSING ........................................................................................................................................... 20
  Installing and Removing License ....................................................................................................... 21
  Viewing License Information ............................................................................................................. 23
  Revoking License Units ....................................................................................................................... 24
ARCHITECTURE OVERVIEW .............................................................................................................. 25
DEPLOYMENT ....................................................................................................................................... 29
  Installing Veeam Backup for Microsoft Azure .................................................................................. 29
    Step 1. Launch Create Virtual Machine Wizard .............................................................................. 30
    Step 2. Configure Azure VM Properties ......................................................................................... 32
    Step 3. Select OS Disk Type ............................................................................................................... 34
    Step 4. Configure Network Settings ............................................................................................... 35
    Step 5. Specify Management Options ............................................................................................. 37
    Step 6. Begin Installation ................................................................................................................. 38
  After You Install .................................................................................................................................. 39
  Uninstalling Veeam Backup for Microsoft Azure ............................................................................ 40
    Remove Backed-Up Data .................................................................................................................. 40
    Remove IAM Roles and Azure AD Applications ............................................................................. 41
    Remove Azure Resources ................................................................................................................. 42
ACCESSING VEEAM BACKUP FOR MICROSOFT AZURE .................................................................. 43
CONFIGURING VEEAM BACKUP FOR MICROSOFT AZURE ............................................................... 46
  Managing Accounts ........................................................................................................................... 47
    Managing Service Accounts ............................................................................................................. 47
    Managing Repository Accounts ....................................................................................................... 57
    Managing SMTP and SQL Server Accounts ...................................................................................... 66
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>How Backup Works</td>
<td>135</td>
</tr>
<tr>
<td>VM Backup</td>
<td>135</td>
</tr>
<tr>
<td>SQL Backup</td>
<td>140</td>
</tr>
<tr>
<td>File Share Backup</td>
<td>143</td>
</tr>
<tr>
<td>Retention Policy</td>
<td>144</td>
</tr>
<tr>
<td>Performing VM Backup</td>
<td>148</td>
</tr>
<tr>
<td>Creating Backup Policies</td>
<td>148</td>
</tr>
<tr>
<td>Creating Snapshots Manually</td>
<td>177</td>
</tr>
<tr>
<td>Performing SQL Backup</td>
<td>179</td>
</tr>
<tr>
<td>Creating Backup Policies</td>
<td>179</td>
</tr>
<tr>
<td>Creating Backups Manually</td>
<td>205</td>
</tr>
<tr>
<td>Performing File Share Backup</td>
<td>207</td>
</tr>
<tr>
<td>Creating Backup Policies</td>
<td>207</td>
</tr>
<tr>
<td>Creating Snapshots Manually</td>
<td>225</td>
</tr>
<tr>
<td>Managing Backup Policies</td>
<td>226</td>
</tr>
<tr>
<td>Editing Backup Policy Settings</td>
<td>226</td>
</tr>
<tr>
<td>Setting Backup Policy Priority</td>
<td>227</td>
</tr>
<tr>
<td>Enabling and Disabling Backup Policies</td>
<td>228</td>
</tr>
<tr>
<td>Starting and Stopping Backup Policies</td>
<td>229</td>
</tr>
<tr>
<td>Exporting and Importing Backup Policies</td>
<td>230</td>
</tr>
<tr>
<td>PERFORMING RESTORE</td>
<td>232</td>
</tr>
<tr>
<td>Performing VM Restore</td>
<td>232</td>
</tr>
<tr>
<td>Performing Entire VM Restore</td>
<td>232</td>
</tr>
<tr>
<td>Performing Disk Restore</td>
<td>245</td>
</tr>
<tr>
<td>Performing File-Level Recovery</td>
<td>253</td>
</tr>
<tr>
<td>Performing SQL Restore</td>
<td>261</td>
</tr>
<tr>
<td>Step 1. Launch SQL Database Restore Wizard</td>
<td>262</td>
</tr>
<tr>
<td>Step 2. Select Restore Point</td>
<td>263</td>
</tr>
<tr>
<td>Step 3. Select Azure Account</td>
<td>264</td>
</tr>
<tr>
<td>Step 4. Choose Restore Mode</td>
<td>264</td>
</tr>
<tr>
<td>Step 5. Select Azure SQL Account</td>
<td>265</td>
</tr>
<tr>
<td>Step 6. Specify Retrieval Settings</td>
<td>266</td>
</tr>
<tr>
<td>Step 7. Configure Restore Settings</td>
<td>268</td>
</tr>
<tr>
<td>Step 8. Specify Restore Reason</td>
<td>269</td>
</tr>
<tr>
<td>Step 9. Finish Working with Wizard</td>
<td>270</td>
</tr>
<tr>
<td>Performing File Share Restore</td>
<td>271</td>
</tr>
<tr>
<td>Step 1. Launch Azure Files File-Level Recovery Wizard</td>
<td>272</td>
</tr>
<tr>
<td>Step 2. Select Azure Account</td>
<td>273</td>
</tr>
<tr>
<td>Step 3. Choose Restore Mode</td>
<td>274</td>
</tr>
</tbody>
</table>
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.
Welcome to
Veeam Backup for Microsoft Azure

Veeam Backup for Microsoft Azure is a solution developed for protection and disaster recovery tasks for Microsoft Azure environments. With Veeam Backup for Microsoft Azure, you can perform the following operations:

- Create image-level backups and cloud-native snapshots of Azure VMs.
- Create image-level backups of Azure SQL databases.
- Create cloud-native snapshots of Azure file shares.
- Keep the backed-up data in cost-effective, long-term Microsoft Azure storage accounts.
- Restore individual files of Azure file shares, specific Azure SQL databases, entire Azure VMs, individual virtual disks, and guest OS files and folders.
Integration with Veeam Backup & Replication

Microsoft Azure Plug-in for Veeam Backup & Replication extends the Veeam Backup & Replication functionality and allows you to add Veeam Backup for Microsoft Azure appliances to the Veeam Backup & Replication 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. For more information, see the Integration with Veeam Backup & Replication Guide.
Planning and Preparation

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

- Network ports that must be open to ensure proper communication of Veeam Backup for Microsoft Azure components.
- Permissions that must be assigned to a service or a repository account used to perform Veeam Backup for Microsoft Azure operations.
- Azure services to which Veeam Backup for Microsoft Azure must have outbound internet access.
- 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.

Azure Account Permissions

To allow backup appliance to perform backup and restore operations, Azure accounts added to Veeam Backup for Microsoft Azure must have the following permissions:

- Azure service account permissions
- Azure repository account permissions

Azure 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 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 from image-level backups.
- To restore files of Azure file shares from cloud-native snapshots and image-level backups.
- To create and manage backup repositories.

TIP

To manage backup repositories, you can use service accounts or create specific repository accounts. For more information on permissions required for repository accounts, see Azure Repository Account Permissions.

To get access to Azure resources that you want to protect, Azure service accounts must have the following permissions:
"permissions": [
  "actions": [
    "Microsoft.Authorization/roleAssignments/read",
    "Microsoft.Commerce/RateCard/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/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.Network/loadBalancers/read",
    "Microsoft.Network/networkInterfaces/delete",
    "Microsoft.Network/networkInterfaces/join/action",
    "Microsoft.Network/networkInterfaces/read",
    "Microsoft.Network/networkInterfaces/write",
    "Microsoft.Network/networkSecurityGroups/read",
    "Microsoft.Network/publicIPAddresses/join/action",
    "Microsoft.Network/publicIPAddresses/read",
    "Microsoft.Network/publicIPAddresses/delete",
    "Microsoft.Network/publicIPAddresses/write",
    "Microsoft.Network/virtualNetworks/read",
    "Microsoft.Network/virtualNetworks/subnets/join/action",
    "Microsoft.Network/virtualNetworks/write",
    "Microsoft.Network/virtualNetworks/delete",
    "Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
    "Microsoft.Resources/subscriptions/resourceGroups/moveResources/action",
    "Microsoft.Resources/subscriptions/resourceGroups/delete",
    "Microsoft.Resources/subscriptions/resourceGroups/read",
    "Microsoft.Resources/subscriptions/resourceGroups/write",
    "Microsoft.ServiceBus/namespaces/queues/authorizationRules/ListKeys/action",
    "Microsoft.ServiceBus/namespaces/queues/authorizationRules/read",
    "Microsoft.ServiceBus/namespaces/queues/authorizationRules/write",
    "Microsoft.ServiceBus/namespaces/queues/delete",
    "Microsoft.ServiceBus/namespaces/queues/read",
    "Microsoft.ServiceBus/namespaces/queues/write",
    "Microsoft.ServiceBus/register/action"
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, service accounts must be assigned the following permissions:

```json
"dataActions": [
  "Microsoft.KeyVault/vaults/keys/read",
  "Microsoft.KeyVault/vaults/keys/encrypt/action",
  "Microsoft.KeyVault/vaults/keys/decrypt/action"
]
```
Azure Repository Account Permissions

To manage backup repositories residing in Azure blob containers, Azure repository accounts must have the following permissions:

```
"permissions": [
  {
    "actions": [
      "Microsoft.Authorization/roleAssignments/read",
      "Microsoft.Resources/subscriptions/resourceGroups/read",
      "Microsoft.Storage/storageAccounts/read",
      "Microsoft.Storage/storageAccounts/listKeys/action",
      "Microsoft.Storage/storageAccounts/blobServices/read",
      "Microsoft.Authorization/roleDefinitions/write",
      "Microsoft.KeyVault/vaults/read",
      "Microsoft.KeyVault/vaults/keys/versions/read",
      "Microsoft.KeyVault/vaults/deploy/action"
    ]
  }
]
```

To encrypt data stored in a backup repository using the Azure Key Vault Service, a repository account used to create the backup repository must be assigned the following permissions:

```
"dataActions": [
  "Microsoft.KeyVault/vaults/keys/read",
  "Microsoft.KeyVault/vaults/keys/encrypt/action",
  "Microsoft.KeyVault/vaults/keys/decrypt/action"
]
```
## Ports

The following network ports must be open to ensure proper communication of components in the Veeam Backup for Microsoft Azure infrastructure.

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Protocol</th>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workstation web browser</td>
<td>Backup appliance</td>
<td>TCP</td>
<td>443</td>
<td>Required to access the Web UI component from a user workstation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TCP</td>
<td>443</td>
<td>Required to communicate with the REST API service running on the backup appliance.</td>
</tr>
<tr>
<td>Worker instance</td>
<td>TCP</td>
<td>443</td>
<td>Required to access the Veeam File Level Recovery browser running on a worker instance during the file-level recovery process.</td>
<td></td>
</tr>
<tr>
<td>Backup appliance</td>
<td>Ubuntu Security Update repository (security.ubuntu.com)</td>
<td>HTTP</td>
<td>80</td>
<td>Required to get OS security updates.</td>
</tr>
<tr>
<td></td>
<td>Veeam Update Notification Server (repository.veeam.com)</td>
<td>TCP</td>
<td>443</td>
<td>Required to download information on available product updates.</td>
</tr>
<tr>
<td></td>
<td>SMTP server</td>
<td>TCP</td>
<td>25</td>
<td>Required to send email notifications. <strong>Note:</strong> The TCP 25 port is the port that is most commonly used by SMTP servers.</td>
</tr>
<tr>
<td>Azure VM</td>
<td>Backup appliance</td>
<td>TCP</td>
<td>443</td>
<td>Required to communicate with Windows-based Azure VMs with enabled guest processing option. For more information, see Performing Backup.</td>
</tr>
<tr>
<td>Worker instance</td>
<td>Ubuntu Security Update repository (security.ubuntu.com)</td>
<td>HTTP</td>
<td>80</td>
<td>Required to get OS security updates.</td>
</tr>
<tr>
<td>ServiceBus service</td>
<td>Worker instance</td>
<td>TCP</td>
<td>443</td>
<td>Required to perform image-level backup and restore operations.</td>
</tr>
<tr>
<td>From</td>
<td>To</td>
<td>Protocol</td>
<td>Port</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>------------------------</td>
<td>----------</td>
<td>------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Backup appliance</td>
<td>TCP</td>
<td>443</td>
<td></td>
<td>Required to communicate with Windows-based Azure VMs with enabled guest processing option. For more information, see Performing Backup.</td>
</tr>
</tbody>
</table>

Azure Services

The backup appliance and worker instances must have outbound network access to the following Microsoft Azure services:

- Azure Active Directory
- Azure Resource Manager
- Azure Storage Accounts
- Azure Cost Management
- Azure Instance Metadata Service (AzurePlatformIMDS)
- Microsoft Identity Platform
- Azure Ubuntu Repository
- Azure Service Bus
- Azure Key Vault
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.ServiceBus
- Microsoft.Storage
- Microsoft.Sql
- Microsoft.ManagedServices

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

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

Hardware

<table>
<thead>
<tr>
<th>Component</th>
<th>Recommended Azure VM size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup appliance</td>
<td>• Standard_B2s with 2 CPUs and 4 GB RAM</td>
</tr>
<tr>
<td></td>
<td>• Standard_B2ms with 2 CPUs and 8 GB RAM</td>
</tr>
<tr>
<td>Workers</td>
<td>• Standard_F2s_v2 with 2 CPUs and 4 GB RAM for regular backup</td>
</tr>
<tr>
<td></td>
<td>• Standard_E2_v5 with 2 CPUs and 16 GB RAM for archived backup</td>
</tr>
</tbody>
</table>

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.

Network Settings for Worker Instances

Before you start adding worker configurations, consider the following:

- A service endpoint (routing) for the Microsoft.Storage service must be configured for virtual networks to which workers will be connected. To learn how to configure virtual network service endpoints, see Microsoft Docs.

- A subnet to which workers will be connected must have at least one free IP address in the subnet range — Veeam Backup for Microsoft Azure will launch and simultaneously run as many workers as many free IP addresses there are in the subnet range.

- By default, workers use public endpoints to connect to Azure SQL Managed Instances through the 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 the 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 peer in the Microsoft Azure portal. To learn how to peer virtual networks, see Microsoft Docs.

For more information on worker configurations, see Configuring Workers.

Encryption

The current Veeam Backup for Microsoft Azure version supports Azure Disk Encryption with the following limitations:

- Azure Disk Encryption is supported for backup and restore operations only within one Azure region. If you choose to backup or to 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.

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

Backup

Before you start protecting Azure resources, consider the following:

- 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 archive tiering of storage accounts with enabled data redundancy (ZRS, GZRS, RA-GZRS) option.

- When Veeam Backup for Microsoft Azure backs up Azure VMs with IPv6 addresses assigned, it does not save the addresses. That is why if you plan to restore these VMs, keep in mind that you will have to assign IPv6 addresses to the restored VMs manually in the Microsoft Azure portal after the restore process completes.

- 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.

- If an Azure SQL database was migrated to a SQL Server or an Azure SQL Managed Instance, you will have to delete legacy references, orphaned database users and credentials set up with authentication types not supported on Azure SQL, to avoid BACPAC export errors. BACPAC export of databases with external references is not supported.

Security Certificates

Veeam Backup for Microsoft Azure supports certificates only in the .PFX format.
Licensing

Veeam Backup for Microsoft Azure is licensed by the number of protected instances. An instance is defined as a single Azure resource — an Azure VM or Azure SQL Server. An Azure VM is considered to be protected if it has a restore point (snapshot or backup) created by a backup policy during the past 31 days. An Azure SQL Server is considered to be protected if at least one database located on the server has a backup created by a backup policy during the past 31 days.

Each protected instance consumes one license unit from the license scope. However, if an instance has only manually created snapshots or backups, it does not consume any license units.

**NOTE**

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.

Veeam Backup for Microsoft Azure is available in 2 license editions:

- **Free License**
  
  By default, Veeam Backup for Microsoft Azure operates in the *Free* edition that allows you to protect up to 10 instances free of charge. Mind that this license edition does not support indexing of Azure file shares.

- **BYOL (Bring Your Own License)**
  
  The *BYOL* (Bring You Own License) edition is a subscription-based license that expires at the end of the subscription term. The maximum number of instances managed by Veeam Backup for Microsoft Azure depends on the number of units specified in your license. For details on how to obtain the license, contact a Veeam sales representative at Sales Inquiry.

  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.

  For more information on how to install and update the license, see Installing and Removing License.

**NOTE**

Veeam Backup & Replication licensing is applied to Veeam Backup for Microsoft Azure appliances added to the Veeam Backup & Replication infrastructure. For more information, see the Integration with Veeam Backup & Replication Guide.
Installing and Removing License

NOTE
This section applies only to the BYOL edition of Veeam Backup for Microsoft Azure.

Installing License

To install or update a license installed on the backup appliance, do the following:

1. Switch to the Configuration page.
2. Navigate to Licensing > License Info.
3. Click Install License.
4. In the Install License window, click Browse to browse to a license file, and then click Install.

IMPORTANT
If your backup appliance is connected to a standalone Veeam Backup & Replication server, you can manage the license only using the Veeam Backup & Replication console. For more information, see Integration with Veeam Backup & Replication Guide.
Removing License

To remove a license installed on the backup appliance if you no longer need it, do the following:

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

**IMPORTANT**

If your backup appliance is connected to a standalone Veeam Backup & Replication server and has the **BYOL** edition installed, you can remove the license and switch to the **Free** edition only using the Veeam Backup & Replication console.
Viewing License Information

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).
- **Expiration Date** — the date when the license will expire.
- **Licensed to** — the name of an organization to which the license was issued.
- **Support ID** — the unique identification number of the support contract (required for contacting the Veeam Customer Support Team).
- **Type** — the license edition (**Free, Subscription**).

**NOTE**

**Subscription** is the name of the **BYOL** license in Veeam Backup for Microsoft Azure.

- **Instances** — the total number of protected instances that consume license units.

  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.
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.

To revoke a license unit from an instance, 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.
Architecture Overview

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

- **Backup appliance**
- **Backup repositories**
- **Worker instances**

Backup Appliance

The backup appliance is a Linux-based Azure VM where Veeam Backup for Microsoft Azure is installed. The backup appliance performs the following administrative activities:

- Manages infrastructure components.
- Coordinates snapshot creation, backup and recovery tasks.
- Controls backup policy scheduling.

The backup appliance also maintains the configuration database that stores data collected from Veeam Backup for Microsoft Azure for the existing backup policies, protected Azure resources, launched worker instances, connected Microsoft Azure accounts and so on.

Backup Appliance Components

The backup appliance uses the following components:

- **Backup service** — coordinates data protection and disaster recovery operations.
- **Configuration database** — stores data collected for the Veeam Backup for Microsoft Azure infrastructure, backup policies, sessions and so on.
- **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 details, 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 and Azure SQL databases.

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.

**IMPORTANT**

Backups 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 Repositories**

For enhanced data security, Veeam Backup for Microsoft Azure allows you to enable encryption at the repository level. Veeam Backup for Microsoft Azure uses the same encryption standards as Veeam Backup & Replication to encrypt backups stored in backup repositories. To learn what encryption standards Veeam Backup & Replication uses to encrypt its data, see the Encryption Standards section of the Veeam Backup & Replication User Guide.

To learn how to enable encryption at the repository level, configure the repository settings as described in section Adding Backup Repositories, 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.

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

<table>
<thead>
<tr>
<th>Storage Account Type</th>
<th>Supported Performance Tiers</th>
<th>Supported Access Tiers</th>
</tr>
</thead>
<tbody>
<tr>
<td>General-purpose V2</td>
<td>Standard</td>
<td>Hot, Cool, Archive</td>
</tr>
<tr>
<td>BlobStorage</td>
<td>Standard</td>
<td>Hot, Cool, Archive</td>
</tr>
</tbody>
</table>

**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 storage accounts with enabled **data redundancy** (GZRS, RA-GZRS) option.
- Veeam Backup for Microsoft Azure does not support archive tiering of storage accounts with enabled **data redundancy** (ZRS, GZRS, RA-GZRS) option.
Worker Instances

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

Veeam Backup for Microsoft Azure automatically launches worker instances to process Azure VMs and Azure SQL databases 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:

<table>
<thead>
<tr>
<th>Operation</th>
<th>Worker Instance Location</th>
<th>Default Worker Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating image-level backups of Azure VMs</td>
<td>Azure region in which a backup repository storing backed-up data resides</td>
<td>Standard_F2s_v2, 2 CPU, 4 GB RAM</td>
</tr>
<tr>
<td>Creating image-level backups of Azure SQL databases</td>
<td>Azure region in which a SQL Server hosting the processed database resides</td>
<td></td>
</tr>
<tr>
<td>Azure file share indexing</td>
<td>Azure region in which a processed file share resides</td>
<td></td>
</tr>
<tr>
<td>Creating archived image-level backups of Azure VMs</td>
<td>Azure region in which an archive backup repository storing backed-up data resides</td>
<td>Standard_E2_v5, 2 CPU 16 GB RAM</td>
</tr>
<tr>
<td>Creating archived image-level backups of Azure SQL databases</td>
<td>Azure region in which a SQL Server hosting the processed database resides</td>
<td></td>
</tr>
<tr>
<td>Performing health check for created restore points</td>
<td>Azure region in which a target backup repository resides</td>
<td>Standard_F2s_v2, 2 CPU, 4 GB RAM</td>
</tr>
<tr>
<td>Applying retention policy settings to created restore points</td>
<td>Azure region in which a backup repository with backed-up data resides</td>
<td></td>
</tr>
<tr>
<td>Restoring Azure VMs and Azure SQL databases</td>
<td>Azure region in which the restored Azure VM or SQL Server hosting the restored database resides</td>
<td></td>
</tr>
<tr>
<td>Restoring individual virtual disks of Azure VMs</td>
<td>Azure region in which the restored virtual disk resides</td>
<td></td>
</tr>
</tbody>
</table>
Worker instances are launched based on worker configurations and profiles that can be created either automatically by Veeam Backup for Microsoft Azure, or manually by the user as described in Managing Worker Instances.

Worker Instance Components

A worker instance uses the following services:

- **Veeam Data Mover** — the service that performs data processing tasks. During backup, the Veeam Data Mover service retrieves data from snapshots and stores the retrieved data to backup repositories. During restore, the Veeam Data Mover transfers backed-up data from backup repositories to the target location.

- **File-Level Restore Browser** — the web service that allows you to find and save files and folders of a backed-up Azure VM to a local machine. The File-Level Restore 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 Restore browser, see Performing File-Level Recovery.

**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 Update repository (security.ubuntu.com) to get and install security updates on the worker instance. Due to technical limitations, you can neither configure nor disable these updates in the current version of Veeam Backup for Microsoft Azure.

Security Certificates for Worker Instances

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 Restore browser running on a worker instance during the file-level recovery process. A self-signed certificate is generated automatically on the worker instance when the recovery session starts.

Requirements for Worker Instances

For every Azure region where worker instances will be launched, you must specify a virtual network, subnet and a security group to which the worker instances must be connected. Otherwise, Veeam Backup for Microsoft Azure will be able neither to launch worker instances nor to perform the required data protection and disaster recovery operations.

To learn how to configure network settings for worker instances, see Adding Worker Configuration.
Deployment

Veeam Backup for Microsoft Azure comes as an image of a Linux-based VM that you can deploy from Microsoft Azure Marketplace.

Installing Veeam Backup for Microsoft Azure

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

1. Log in to the Microsoft Azure portal.
2. Configure properties of the Azure VM where Veeam Backup for Microsoft Azure will be installed.
3. Select the type of the OS disk that will be attached to the Azure VM.
4. Configure network settings for the Azure VM.
5. Start the installation process.
Step 1. Launch Create Virtual Machine Wizard

To launch the Create a virtual machine wizard, do the following:

1. Sign in to the Microsoft Azure Marketplace portal using credentials of the Microsoft Azure account that you plan to use to install Veeam Backup for Microsoft Azure.

2. In the Search Marketplace field, enter Veeam Backup for Microsoft Azure and click the Search icon.

3. In the list of search results, select the necessary product edition and click Get It Now.
   
   For more information on product editions, see Licensing.

4. In the Create this app in Azure window, do the following:
   
a. Check the contact name, email and phone number of the person responsible for the account used to log in to Microsoft Azure. You can add any missing information if required.

b. Click Continue.
5. Back to the Microsoft Azure portal, click **Create**.
Step 2. Configure Azure VM Properties

At the Basics step of the Create a virtual machine wizard, do the following:

1. From the Subscription drop-down list, select a Microsoft Azure subscription that will be used to manage costs of the backup appliance.
   For a subscription to be displayed in the Subscription list, it must be created and assigned to the tenant as described in Microsoft Docs.

2. From the Resource group drop-down list, select a resource group that will hold resources related to the backup appliance.
   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 Virtual machine name field, enter a name for the backup appliance.

4. From the Region drop-down list, select a Microsoft Azure region where the backup appliance will operate.
   For more information on the Azure regions, see Microsoft Docs.

   **NOTE**
   Regardless of the region you select, you will be able to manage Azure VMs that operate in other Microsoft Azure regions as well.

5. From the Availability options drop-down list, choose whether you want to require any infrastructure redundancy to achieve high availability:
   - Select the Availability set option to include the backup appliance in an availability set. You can either use an existing availability set or create a new one.
     Availability sets allow you to distribute VMs across multiple physical hardware resources.
   - Select the Availability zone option to place the backup appliance in an Availability Zone within the selected Microsoft Azure region.
     Availability Zones allow you to distribute VMs across multiple unique physical locations and to protect your data from datacenter failures. Each Microsoft Azure region contains 3 availability zones. If one or more datacenters in one zone malfunctions, your Azure resources will become instantly available in another zone.
     For more information on availability options for VMs in Azure, see Microsoft Docs.

6. From the Image drop-down list, select Veeam Backup for Microsoft Azure.

7. Make sure the Azure Spot Instance option is disabled.
   The Spot VMs functionality allows Azure to redistribute the currently unused storage capacity between different Azure resources. It is not recommended that you set the Azure Spot Instance to Yes since this may cause a performance malfunction of the backup appliance.
   For more information on using Spot VMs in Azure, Microsoft Docs.

8. In the Size section, choose a size for the backup appliance. The recommended hardware minimum for an Azure VM running Veeam Backup for Microsoft Azure is 2 vCPU and 4 GB RAM.
   By default, the installer selects the optimal size based on the VM performance and cost reduction policy. For more information on sizes for VMs in Azure, see Microsoft Docs.
9. In the **Administrator account** section:
   
a. Set the **Authentication type** option to **Password**.
   
b. In the **Username** and **Password** fields, specify credentials of a user account that you will use for your first login to Veeam Backup for Microsoft Azure.

**IMPORTANT**

Do not use *veeamazure* and *veeamflr* as the user name — otherwise, you will not be able to access the backup appliance after installation. These names are reserved by Veeam Backup for Microsoft Azure.

10. Click **Next : Disks >**.
Step 3. Select OS Disk Type

At the Disks step of the Create a virtual machine wizard, do the following:

1. From the OS disk type drop-down list, select a type of the Azure managed disk that will be attached to the backup appliance.
   
   It is recommended that you use Premium SSD to ensure better performance of the disk. For more information on available Azure managed disk types, see Microsoft Docs.

2. From the Encryption type drop-down list, choose whether you want to use a default platform-managed key or a custom-managed key to encrypt Veeam Backup for Microsoft Azure data.
   
   o Select the Encryption on at-rest with a platform-managed key option to use the default type of encryption.
   
   o Select the Encryption on at-rest with a custom-managed key option to specify your own key. This ensures better control of your keys and data, but has a number of restrictions. For a custom-managed encryption key to be displayed in the Disk encryption set list, it must be created in the Microsoft Azure portal as described in Microsoft Docs.

3. Other options on the Disks page are preconfigured by Veeam Backup for Microsoft Azure and cannot be changed. Click Next: Networking >.
Step 4. Configure Network Settings

At the Networking step of the Create a virtual machine wizard, do the following:

1. From the Virtual network drop-down list, select a virtual network to which you want to connect the backup appliance.
   
   You can either use an existing virtual network or create a new one. For more information on building networks in Microsoft Azure, see Microsoft Docs.

2. From the Subnet drop-down list, select a subnet to which you want to connect the backup appliance.
   
   Subnets allow you to segment virtual networks and distribute the address space among Azure resources. You can either use an existing subnet or add a new one. For more information on managing subnets in Microsoft Azure, see Microsoft Docs.

3. From the Public IP drop-down list, select a public IP address that will be associated with the backup appliance.
   
   Public IP addresses allows Azure VMs to communicate to the Internet and public-facing Azure services. You can either use an existing public IP address or add a new one. For more information on assigning public IP address to Azure resources, see Microsoft Docs.

4. From the Configure network security group drop-down list, select a security group that will be associated with the specified subnet.
   
   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. You can either use an existing security group or create a new one. For more information on configuring security group rules, see Microsoft Docs.

   IMPORTANT

   Consider that security rules configured in the selected network security group must allow direct network traffic to Azure resources, proxy redirect or setting a proxy in Veeam Backup for Microsoft Azure configuration is not supported.

5. Make sure that the Place this virtual machine behind an existing load balancing solution option is disabled.
   
   Load balancers allow you to distribute traffic load among several VMs, but since there is only one VM running Veeam Backup for Microsoft Azure, no load balancing is required. It is not recommended that you set the Place this virtual machine behind an existing load balancing solution option to Yes since this may cause an unpredictable performance malfunction of the VM running Veeam Backup for Microsoft Azure. For more information on using load balancers in Microsoft Azure, see Microsoft Docs.
6. Other options on the **Networking** page are preconfigured by Veeam Backup for Microsoft Azure and cannot be changed. Click **Review + create**.
Step 5. Specify Management Options

At the Management step of the Create a virtual machine wizard, do the following:

1. Use the **Boot diagnostics** option to choose whether you want to capture the console output and screenshots of the backup appliance. This may help you troubleshoot server malfunction issues.
   
   For more information on how to use boot diagnostics in Microsoft Azure, see Microsoft Docs.

2. Use the **OS guest diagnostics** option to choose whether you want to collect capacity-related guest OS metrics. This may also help you troubleshoot server malfunction issues.

3. From the **Diagnostics storage account** drop-down list, select a storage account that will be used to keep the collected diagnostic information. You can either use an existing storage account or create a new one.
   
   To learn how to create Azure storage accounts, see Microsoft Docs.

4. Use the **System assigned managed identity** option to choose whether you want to grant the identity access to the backup appliance. Managed identities ensure protected access to Azure resources.
   
   To learn how to use managed identities, see Microsoft Docs.

5. Make sure the **Enable auto-shutdown** option is set to Off. It is not recommended that you set the Enable auto-shutdown option to On since this may cause an unpredictable performance malfunction of the backup appliance.
6. Click **Review + create**.

Step 6. Begin Installation

At the **Review + create** step of the **Create a virtual machine** wizard, review summary information and click **Create** to begin installation.

**TIP**

If you want to specify advanced configuration settings, deploy additional extensions, pass custom scripts and assign tags to the backup appliance, navigate to the **Advanced** and **Tags** pages. Follow the instructions provided in the wizard to configure the remaining options.
After You Install

To start working with Veeam Backup for Microsoft Azure, you must perform the initial configuration of the backup appliance:

1. In a web browser, navigate to the Veeam Backup for Microsoft Azure web address.
   
   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**

   Internet Explorer is not supported. To access Veeam Backup for Microsoft Azure, use Microsoft Edge (version 40 or later), Mozilla Firefox (version 56 or later) or Google Chrome (version 62 or later).

2. In the **Username** and **Password** fields, specify credentials of the Administrator account that was created during product installation. In future, you can add other users to grant access to Veeam Backup for Microsoft Azure. For more information, see Adding User Accounts.

3. Read and accept both the Veeam license agreement and the 3rd party components license agreement. If you reject the agreements, you will not be able to continue installation.

   To read the terms of the license agreement for the 3rd party components, click 3rd party components license agreement.

   **NOTE**

   To increase the security of the Administrator account, it is recommended that you enable multi-factor authentication (MFA) for the account after you first log in to Veeam Backup for Microsoft Azure. To learn how to enable MFA, see Enabling Multi-Factor Authentication.


5. [Optional] Download and install product updates, as described in Updating Veeam Backup for Microsoft Azure.
Uninstalling Veeam Backup for Microsoft Azure

Veeam Backup for Microsoft Azure creates a number of resources while operating in Microsoft Azure, and these resources are not removed from the Microsoft Azure infrastructure automatically when you uninstall the solution. That is why you need to perform the following steps to uninstall Veeam Backup for Microsoft Azure:

1. Remove backed-up data.
2. Remove IAM roles and Azure AD 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.

Remove 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 Azure account automatically. You can later import the created image-level backups of Azure VMs and backups of Azure SQL databases 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:

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 where the backed-up data is stored.
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 a check box next to the Veeam folder and click Delete.
   - To remove cloud-native snapshots, select check boxes next to the 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.
Remove IAM Roles and Azure AD Applications

**IMPORTANT**
Do not remove IAM roles and Azure AD applications if they are still used by other backup appliances.

To remove IAM roles and Azure AD 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 **Azure Active Directory > App registrations**.
   a. On the **All applications** tab, click **Application (client) ID starts with** and enter an application ID in the search field.
   
   **TIP**
   If you do not know the ID of an AD application created by Veeam Backup for Microsoft Azure, navigate to **Accounts**, switch to the **Azure Accounts** or **Repository 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 the **Veeam Service Account** and **Veeam Repository Account** roles and click **Remove**.
Remove Azure Resources

To remove the backup appliance and all resources created by Veeam Backup for Microsoft Azure, perform the following steps:

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 where the backup appliance resides. The resource group page will open.

3. Remove the Azure VM running Veeam Backup for Microsoft Azure and all resources associated with this Azure VM. To do that:
   a. In the Resources section, enter the name of the backup appliance in the search field.
   b. 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.

4. Remove storage accounts and Service Bus namespaces created by Veeam Backup for Microsoft Azure. To do that:
   a. In the Resources section, enter veeam in the search field.
   b. In the Resources list, select check boxes next to the resources of the Storage account and Service Bus namespace types, and click Delete.
      In the Delete Resources window, type Yes to confirm the action and click Delete.
Accessing Veeam Backup for Microsoft Azure

To access Veeam Backup for Microsoft Azure, in a web browser, navigate to the Veeam Backup for Microsoft Azure web address. 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**

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).

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 Managing Permissions.

**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 Working with 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 during product installation. In future, you can add other user accounts to grant access to Veeam Backup for Microsoft Azure. For more information, see **Managing Permissions**.

   **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 **Keep me logged in** check box to save the specified credentials in a persistent browser cookie so that you do not have to provide credentials every time you access Veeam Backup for Microsoft Azure in a new browser session.

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 Azure accounts to get access to Azure services and resources.**
2. **[Optional] Add user accounts to control access to Veeam Backup for Microsoft Azure.**
3. **Add backup repositories.**
4. **Create worker configurations.**
5. **[Optional] Configure 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 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 Accounts

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

- **Service accounts** — to get access to Azure resources that you want to protect.
- **Repository accounts** — to manage backup repositories assigned to folders in blob containers.
- **SMTP and SQL Server Accounts** — to authenticate against SMTP and Azure SQL Servers.

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 synchronize the Microsoft Azure environment data with the configuration data stored on the backup appliance.
- To access blob containers used as target locations for backed-up data.
- To create and remove snapshots of Azure VM.
- To create and remove snapshots of Azure file shares.

Adding Azure Service Accounts

To add a new service account, do the following:

1. Launch the Add Azure Account wizard.
2. Specify an account name and description.
3. Select a service account type.
4. Select a service provider.
5. Finish working with the wizard.
Step 1. Launch Add Azure Account Wizard

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

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

Step 2. Specify Account Info

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. For more information naming restrictions in Microsoft Azure, see Microsoft Docs.
Step 3. Select Service Account Type

At the **Service Account Type** step of the wizard, choose whether you want to connect to Azure Active Directory using an existing or a newly created service account.

### Add Azure Account

<table>
<thead>
<tr>
<th>Account Info</th>
<th>Select service account type to use</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Service Account Type</strong></td>
<td>Microsoft Azure environment: Global</td>
</tr>
<tr>
<td>Choose your connection type:</td>
<td>Create service account automatically</td>
</tr>
<tr>
<td></td>
<td>Upon authentication, the wizard will do the following:</td>
</tr>
<tr>
<td></td>
<td>• Login to your Microsoft Azure account</td>
</tr>
<tr>
<td></td>
<td>• Create a service principal account</td>
</tr>
<tr>
<td></td>
<td>• Give the service principal account least required privileges to Microsoft Azure</td>
</tr>
<tr>
<td></td>
<td>Specify existing service account</td>
</tr>
</tbody>
</table>

#### Creating Service Account Automatically

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

When you choose to create a service account automatically, Veeam Backup for Microsoft Azure creates a new **Azure AD application** in your Microsoft Azure Active Directory. To create the Azure AD 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**

- The Microsoft Azure account that you use to access the Azure CLI must have the `Microsoft.Authorization/*/Write` permissions assigned in the subscription associated with the backup appliance. For more information on managing role permissions and security in Microsoft Azure, see [Microsoft Docs](#).
- If you have disabled the **Users can register applications option** in the Microsoft Azure portal, make sure that the newly created Azure AD application has the **Application Developer, Application Administrator or Global Administrator** role assigned. For more information on role permissions in Azure Active Directory, see [Microsoft Docs](#).

At the **Logon to Azure** 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**. Note that the code will expire in 15 minutes.
   b. Select an 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 Azure Account** wizard, check whether any errors occurred during the authentication process and click **Next**.
Specifying Existing Service Account

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

When you specify an existing service account, Veeam Backup for Microsoft Azure connects to an existing Azure AD application that grants access to your Azure resources. For Veeam Backup for Microsoft Azure to be able to connect to the Azure AD application, it must be created beforehand as described in Microsoft Docs.

At the Service Account 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 in the application settings of your Azure Active Directory. For more information, see Microsoft Docs.

   The specified Azure AD application must have either a custom role or the Contributor and Key Vault Crypto Officer Azure built-in roles assigned. If the AD application has a custom role assigned, make sure the role is granted the permissions required to perform backup and restore operations. To learn how to create custom roles, see Microsoft Docs.

   **TIP**

   If you have ever created a new service account using the Create service account automatically option, you can also assign to the specified Azure AD application the Veeam Service Account role that has been created in Microsoft Azure environment automatically by Veeam Backup for Microsoft Azure. To learn how to assign Azure roles, see Microsoft Docs.

2. Select an application authentication type:

   o Select the Client (application) secret option to use a client secret. A secret string can be obtained as described in Microsoft Docs.

   o Select the Certificate option to use a certificate to authenticate against the server. Then, click Browse to locate the certificate file.

   For a certificate to be valid, it must be uploaded to the Microsoft Azure portal and assigned to the Azure AD application as described in Microsoft Docs.

   **IMPORTANT**

   Veeam Backup for Microsoft Azure supports certificates only in the .PFX format.
3. In the **Tenant ID** field, enter a tenant ID of the Azure AD application.

You can find the tenant ID in the application settings of your Azure Active Directory. For more information, see [Microsoft Docs](https://docs.microsoft.com).

![Add Azure Account dialog](image.png)
Step 4. Select Active Directory Group

[This step applies only if you have selected the Creating service account automatically option at the Select Service Account Type step of the wizard]

At the Active Directory step of the wizard, add your Azure AD application to an Azure Active Directory group to be able to back up Azure resources as a group:

1. Select the Add specified application to this AD group check box.
2. From the list of available groups, select the necessary group.

For a group to be displayed in the list, it must be created in the Microsoft Azure portal as described in Microsoft Docs.
Step 5. Finish Working with Wizard

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

<table>
<thead>
<tr>
<th>Add Azure Account</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Info</td>
<td></td>
</tr>
<tr>
<td>Service Account Type</td>
<td>General</td>
</tr>
<tr>
<td>Logon to Microsoft Azure</td>
<td>Name: Azure Service Account</td>
</tr>
<tr>
<td>Active Directory</td>
<td>Description: Created by Admin</td>
</tr>
<tr>
<td></td>
<td>Authentication: Device Logon</td>
</tr>
<tr>
<td></td>
<td>Tenant ID: 3e924ba0-93bc-40d5-8a47-33f07b239a3f</td>
</tr>
<tr>
<td></td>
<td>Active Directory Name: Veeam Software Group GmbH</td>
</tr>
<tr>
<td></td>
<td>AD Group: Veeam.IT.Network</td>
</tr>
<tr>
<td></td>
<td>Visual Studio Premium MSDN</td>
</tr>
<tr>
<td></td>
<td>Subscription ID: 3e924ba0-7bb8-4b83-9c68-15d674fb8b8</td>
</tr>
<tr>
<td></td>
<td>Integration Tests</td>
</tr>
<tr>
<td></td>
<td>Subscription ID: 1142bdc7-879c-42bc-aa23-c31f1c4119a2</td>
</tr>
</tbody>
</table>

[Image of the summary step of the wizard with the Finish button highlighted]
Editing Azure Service Account

For each service account, you can modify settings configured while adding the account:

1. Switch to the Configuration page.
2. Navigate to Accounts > Azure Account.
3. Select the service account and click Edit.
4. Complete the Edit Azure Account wizard.
   a. To provide a new name and description for the account, follow the instructions provided in section Adding Azure Service Account (step 2).
   b. To renew the client secret of the currently used Azure AD application or to connect to another service principal, follow the instructions provided in section Adding Azure Service Account (step 3).
      If you do not plan to change the settings of the Azure AD application, select the Don't change current service account settings option.
   c. [This step applies only if you have selected the Renew application or Specify existing service account option]. To add your Azure AD application to a Microsoft Azure Active Directory resource group, follow the instructions provided in section Adding Azure Service Account (step 4).
   d. At the Summary step of the wizard, review configuration information and click Finish.
Removing Azure Service Account

Veeam Backup for Microsoft Azure allows you to permanently remove a service account from the configuration database if you no longer need it:

1. Switch to the Configuration page.
2. Navigate to Accounts > Azure Account.
3. Select the Azure service account and click Remove.

**NOTE**

You cannot remove a service account that is used by any backup policy, or if Veeam Backup for Microsoft Azure still uses this account to access any of the existing backup repositories. Disable and remove all the related policies, remove all the related backup repositories — and then try removing the account again.
Managing Repository Accounts

Veeam Backup for Microsoft Azure allows you to configure repository accounts that will be used to manage backup repositories. Repository accounts usually have less permissions than your Azure service accounts and are intended to provide a granular access to the repositories.

Adding Repository Accounts

To add a new repository account, do the following:

1. **Launch the Add Repository Account wizard.**
2. **Specify an account name and description.**
3. **Select a repository account type.**
4. **Finish working with the wizard.**

Step 1. Launch Add Repository Account Wizard

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

1. **Switch to the** Configuration **page.**
2. **Navigate to Accounts > Repository Accounts.**
3. **Click Add.**
Step 2. Specify Account Info

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 name is 255 characters.
Step 3. Select Repository Account Type

At the **Repository Account Type** step of the wizard, choose whether you want to connect to Azure Active Directory using an existing or a newly created repository account.

Creating Repository Account Automatically

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

When you choose to create a repository account automatically, Veeam Backup for Microsoft Azure creates a new **Azure AD application** in your Microsoft Azure Active Directory. To create the Azure AD 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**

- The Microsoft azure account which you used to access the Azure CLI must have the `Microsoft.Authorization/*/Write permissions` assigned in the subscription associated with the backup appliance. For more information on managing role permissions and security in Microsoft Azure, see [Microsoft Docs](#).
- If you have disabled the **Users can register applications** option in the Microsoft Azure portal, make sure that the service account has the **Application Developer, Application Administrator or Global Administrator** role. For more information on role permissions in Azure Active Directory, see [Microsoft Docs](#).
At the **Logon to Azure** 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**. Note that the code will expire in 15 minutes.
   b. Select an 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 Azure Account** wizard, check whether any errors occurred during the authentication process.
Specifying Existing Repository Account

[This step applies only if you have selected the Specify existing repository account option at the Select Repository Account Type step of the wizard]

When you specify an existing repository account, Veeam Backup for Microsoft Azure connects to an existing Azure AD application that grants access to your Azure resources. For Veeam Backup for Microsoft Azure to be able to connect to the Azure AD application, it must be created in the Microsoft Azure portal as described in Microsoft Docs.

At the Service Account 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 in the application settings of your Azure Active Directory. For more information, see Microsoft Docs.

   The specified Azure AD application must have either a custom role or the Contributor and Key Vault Crypto Officer Azure built-in roles assigned. If the AD application has a custom role assigned, make sure the role is granted the permissions required to manage backup repositories. To learn how to create custom roles, see Microsoft Docs.

   TIP

   If you have ever created a new service account using the Create repository account automatically option, you can also assign to the specified Azure AD application the Veeam Repository Account role that has been created in Microsoft Azure environment automatically by Veeam Backup for Microsoft Azure. To learn how to assign Azure roles, see Microsoft Docs.

2. Select an application authentication type:

   o Select the Client (application) secret option to use a client secret. A secret string can be obtained as described in Microsoft Docs.

   o Select the Certificate option to use a certificate to authenticate against the server. Then, click Browse to locate the certificate file.

     For a certificate to be valid, it must be uploaded to the Microsoft Azure portal and assigned to the Azure AD application as described in Microsoft Docs.

   IMPORTANT

   Veeam Backup for Microsoft Azure supports certificates only in the .PFX format.
3. In the **Tenant ID** field, enter a tenant ID of the Azure AD application.

   You can find the tenant ID in the application settings of your Azure Active Directory. For more information, see Microsoft Docs.
Step 4. Finish Working with Wizard

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

<table>
<thead>
<tr>
<th>Summary</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
</tr>
<tr>
<td>Name:</td>
<td>rep-account-02</td>
</tr>
<tr>
<td>Description:</td>
<td>Created by Admin\res-group-02</td>
</tr>
<tr>
<td>Authentication:</td>
<td>Device Logon</td>
</tr>
<tr>
<td>Tenant ID:</td>
<td>97438793-c013-4a51-8485-d33056cb7ba5</td>
</tr>
<tr>
<td>Active Directory Name:</td>
<td>Veeam Software Group GmbH</td>
</tr>
<tr>
<td>Visual Studio Premium with MSDN</td>
<td></td>
</tr>
<tr>
<td>Subscription ID:</td>
<td>📅 280921a2-220d-45c9-92dd-82b6d5a3a78fa2</td>
</tr>
</tbody>
</table>

[Image of the Add Repository Account window with the Summary tab highlighted.]
Editing Repository Accounts

For each repository account, you can modify settings configured while adding the account:

1. Switch to the **Configuration** page.
2. Navigate to **Accounts > Repository Accounts**.
3. Select the repository account and click **Edit**.
4. Complete the **Edit Repository Account** wizard.
   
a. To provide a new name and description for the account, follow the instructions provided in section **Adding Repository Accounts** (step 2).

b. To renew the current Azure AD application or to specify another existing repository account, follow the instructions provided in section **Adding Repository Accounts** (step 3).

If you do not plan to update or change the Azure AD application, select the **Don't change current service account settings** option.

c. At the **Summary** step of the wizard, review configuration information and click **Finish** to confirm the changes.
Removing Repository Accounts

Veeam Backup for Microsoft Azure allows you to permanently remove a repository account from the configuration database if you no longer need it:

1. Switch to the **Configuration** page.
2. Navigate to **Accounts > Repository Accounts**.
3. Select the repository account and click **Remove**.

**NOTE**

You cannot remove a repository account if Veeam Backup for Microsoft Azure still uses this account to access any of the existing backup repositories. **Remove all the related backup repositories** and then try removing the account again.
Managing SMTP and SQL Server Accounts

To allow Veeam Backup for Microsoft Azure to authenticate against protected Azure SQL Servers and SMTP servers used for sending email notifications, you must specify credentials that will be used to access the servers.

Adding Accounts

To add an account that will be used to connect to an SMTP server or an Azure SQL Server, do the following:

1. Launch the Add Account wizard.
2. Specify an account name and description.
3. Specify credentials and a type for the account.
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 Info

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 name is 255 characters.

![Account Info screenshot]

Step 3. Specify Credentials

At the **Account** step of the wizard, choose whether the account will be used to connect to an SMTP server or an Azure SQL Server, and specify credentials of a user account that will be used to authenticate against the server.

**IMPORTANT**

If you select the **Azure SQL server account** type, you must specify credentials of a SQL Server Admin account. Azure Active Directory authentication is not supported.

![Account screenshot]
Step 4. Finish Working with Wizard

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

### Editing Accounts

For each SMTP and Azure SQL account, you can modify settings configured while creating 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 provide a new name and description for the account, follow the instructions provided in section **Adding Accounts** (step 2).
   b. To provide a new user name and password for the account, follow the instructions provided in section **Adding Accounts** (step 3).
   c. At the **Summary** step of the wizard, review configuration information and click **Finish**.
Managing Permissions

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 and perform all restore operations.
- **Restore Operator** — can only perform restore operations and view session statistics.

The following table describes the functionality available to users with different roles in the Veeam Backup for Microsoft Azure UI.

<table>
<thead>
<tr>
<th>Tab</th>
<th>Functionality</th>
<th>Portal Administrator</th>
<th>Portal Operator</th>
<th>Restore Operator</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Overview</strong></td>
<td>Dashboard</td>
<td>Full</td>
<td>Full</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Resources</strong></td>
<td>Infrastructure</td>
<td>Full</td>
<td>Full</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Policies</strong></td>
<td>Backup policies</td>
<td>Full</td>
<td>Full</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Protected Data</strong></td>
<td>Restore</td>
<td>Full</td>
<td>Full</td>
<td>Full</td>
</tr>
<tr>
<td></td>
<td>File-level restore</td>
<td>Full</td>
<td>Full</td>
<td>Full</td>
</tr>
<tr>
<td></td>
<td>Remove</td>
<td>Full</td>
<td>Full</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Session Log</strong></td>
<td>Session logs</td>
<td>Full</td>
<td>Full</td>
<td>Full</td>
</tr>
<tr>
<td></td>
<td>Stop session execution</td>
<td>Full</td>
<td>Full</td>
<td>Full</td>
</tr>
<tr>
<td><strong>Configuration</strong></td>
<td>Accounts</td>
<td>Azure service and repository accounts, SQL Server and SMTP accounts, portal users</td>
<td>Full</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Repositories</strong></td>
<td>Backup repositories</td>
<td>Full</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Workers</strong></td>
<td>Worker instances</td>
<td>Full</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Tab</td>
<td>Functionality</td>
<td>Portal Administrator</td>
<td>Portal Operator</td>
<td>Restore Operator</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------</td>
<td>----------------------</td>
<td>-----------------</td>
<td>------------------</td>
</tr>
<tr>
<td><strong>Settings</strong></td>
<td>General settings</td>
<td>Full</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Licensing</strong></td>
<td>Licensing</td>
<td>Full</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Support Information</strong></td>
<td>Updates and logs</td>
<td>Full</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>
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.
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 4a, 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 Permissions.
      If you have selected the Veeam Backup for Microsoft Azure account option at step 4a, 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.
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.
Changing User Passwords

For Veeam Backup for Microsoft Azure user accounts, you can change the password specified while creating the account:

**IMPORTANT**

You cannot change the password for a user account whose user identity was obtained from an identity provider.

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**.
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*. 

![Enabling MFA window](image)
Managing Backup Repositories

Veeam Backup for Microsoft Azure uses blob containers as target locations for image-level backups of Azure VMs and Azure SQL databases. To add a blob container to Veeam Backup for Microsoft Azure, configure a backup repository.

**IMPORTANT**
A backup repository must not be managed by 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.

Adding Backup 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. Specify an access storage tier.
5. Finish working with 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 255 characters. The following characters are not supported: * : / ? " < > | ! @ # $ % ^ &.

![Add Repository]

Step 3. Configure Repository Settings

At the **Settings** step of the wizard, configure settings for the backup repository:

1. In the **Account** section, select an Azure account whose permissions Veeam Backup for Microsoft Azure will use to access Azure storage accounts that will be used as target locations. For more information on permissions required for the Azure account, see **Azure Account Permissions**.

   For an account to be displayed in the **Azure Account** list, it must be added to Veeam Backup for Microsoft Azure as described in section **Adding Azure Service Account** or **Adding Repository Accounts**. If you have not added the necessary repository account to Veeam Backup for Microsoft Azure beforehand, you can do it without closing the **Add Repository** wizard. To add an account, click **Add** and complete the **Add Repository Account wizard**.

2. In the **Location** section, do the following:
   a. Click **Specify storage account**.
      
      In the **Select storage account** window, select a storage account where the target blob container resides. Veeam Backup for Microsoft Azure will use the account to access the backup repository.
      
      For a storage account to be displayed in the **Account** list, it must be created in the Microsoft Azure portal as described in **Microsoft Docs**.

      **IMPORTANT**

      Veeam Backup for Microsoft Azure does not support creation of backup repositories in storage accounts with the enabled **blob soft delete** option.
b. Click **Not specified**.

In the **Select container** window, select a blob container that will be used as a target location for backups of Azure resources.

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**.

c. Choose whether you want to use an existing folder inside the selected blob container or to create a new one to group backups 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 dash (/) 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 backups, mind 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 at the repository level is enabled for the selected folder, 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.

d. [This step applies only if you have selected the **Create new folder** option] In the **Storage class** section, choose whether you want to specify a tier or to instruct Veeam Backup for Microsoft Azure to automatically create 3 separate repositories for the Hot, Cool and Archive access tiers.

If you select the **Choose your tier** option, you must specify the access tier type to manage 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 backed-up data for at least 30 days and do not need to access it frequently.
- Select the **Archive** tier if you plan to store backed-up data for at least 180 days. Consider that to restore data from an archive, you first need to retrieve data from it. For more information on how to retrieve data, see **Retrieving Data from Archive**.
IMPORTANT

For a repository with the **Archive** tier selected, 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)

• 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 storage accounts, see Microsoft Docs.

---

**Step 4. Enable Data Encryption**

At the **Options** step of the wizard, choose whether you want to encrypt backups stored in the selected blob container.

**IMPORTANT**

If you have selected an existing folder at the **Settings** step of the wizard, and 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 cannot change the encryption settings while adding the repository. However, you will be able to **edit the repository settings** later.

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**.
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 beforehand as described in Microsoft Docs. For a cryptographic key to be displayed in the list of available encryption keys, it must be created beforehand as described in Microsoft Docs.

   **IMPORTANT**

   If you want to use an Azure Key Vault cryptographic key for encryption at the repository level, mind the following:

   - Do not disable cryptographic keys used to encrypt repositories. Otherwise, Veeam Backup for Microsoft Azure will not be able to encrypt data, and backup policies that use encrypted repositories for storing backups will fail.

   - Do not delete cryptographic keys used to encrypt repositories. 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. Finish Working with Wizard

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 repository creation, and click Finish.
Editing Backup Repository Properties

For each backup repository, you can modify settings specified while adding the repository to the Veeam Backup for Microsoft Azure infrastructure:

1. Switch to the Configuration page.
2. Navigate to Repositories.
3. Select the repository and click Edit.
   a. To provide a new name and description for the repository, follow the instructions provided in section Adding Backup Repositories (step 2).
   b. To enable or disable encryption for the repository, follow the instructions provided in section Adding Backup Repositories (step 4).
   c. At the Summary step of the wizard, review summary information, choose whether you want to proceed to the Session Log page, and click Finish.
Removing Backup Repositories

Veeam Backup for Microsoft Azure allows you to permanently remove backup repositories from the infrastructure. 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.

**NOTE**

You cannot remove a backup repository that is used by any backup policy. Modify the settings of all the related policies to remove references to the repository, and then try removing the repository again.
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. 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 Architecture Overview.

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 launches worker instances with the same network configurations as those specified for the processed resources. However, to optimize infrastructure costs and to ensure better performance of backup and restore processes, you can add worker configurations to specify network settings for each region in which worker instances will be launched.

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 and a GUID in their names and the Veeam backup appliance ID tag.

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 wizard.

IMPORTANT
By default, all 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, set the Private network deployment toggle to On. 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 Environment.
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. Click Add.

Step 2. Specify General Settings

At the General step of the wizard, select an Azure region where new worker instances will operate.
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](https://docs.microsoft.com).

     **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.
     - It is recommended to configure a service endpoint (routing) to the *Microsoft.Storage* service. The virtual network settings can be specified in the Microsoft Azure portal. For more information on virtual network service endpoints, see [Microsoft Docs](https://docs.microsoft.com).

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](https://docs.microsoft.com).

**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 and Service Bus namespaces created by Veeam Backup for Microsoft Azure. You can tell these resources from other Azure resources by the word *veeam* and the GUID of the backup appliance in their names.

3. Choose whether you want Veeam Backup for Microsoft Azure to assign public IP addresses to workers used for file-level recovery operations.
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 the Veeam Backup for Microsoft Azure infrastructure:

1. Switch to the Configuration page.
2. Navigate to Workers > Network.
3. Select the worker configuration and click Edit.
4. Complete the Edit Worker Network Configuration wizard:
   a. To modify the virtual network and subnet to which the related worker instances are connected, 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 from the infrastructure 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 the Veeam Backup for Microsoft Azure infrastructure, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **Workers > Network**.
3. Select the worker configuration and click **Remove**.

**NOTE**

If there are any worker instances created based on the selected configuration that are currently involved in a backup or restore process, these instances will be removed only when the process completes.
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, health check, indexing or archive operation. Veeam Backup for Microsoft Azure launches one worker instance per each Azure resource added to a backup policy or restore task. The profile of each launched worker instance is selected based on the performed operation and either the total size of virtual disks attached to the processed Azure VM or the total size of the processed Azure SQL database.

There are 4 types of worker profiles in Veeam Backup for Microsoft Azure:

- **Small** — a profile that Veeam Backup for Microsoft Azure uses for creating image-level backups and restoring data if the total disk size of the processed Azure VM or the total size of the processed Azure SQL database is less than 100 GB. This profile is also used to launch worker instances for file-level recovery, file share indexing and health check operations.

- **Medium** — a profile that Veeam Backup for Microsoft Azure uses for creating image-level backups and restoring data if the total disk size of the processed Azure VM or the total size of the processed Azure SQL database is more than 100 GB but less than 1 TB.

- **Large** — a profile that Veeam Backup for Microsoft Azure uses for creating image-level backups and restoring data if the total disk size of the processed Azure VM or the total size of the processed Azure SQL database is more than 1 TB.

- **Archiving** — a profile that Veeam Backup for Microsoft Azure uses for creating archived backups.

Out of the box, Veeam Backup for Microsoft Azure comes with the default set of worker profiles where the small profile is Standard_F2s_v2, the medium profile is Standard_F4s_v2, the large profile is Standard_F8s_v2, and the archiving 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.

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**.

![Add Worker Profiles Wizard](image)

---

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 VM or SQL database at a time. If the number of VMs and databases that must be processed exceeds the maximum number of worker instances specified in the worker configuration, the VMs and databases 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. In the Keep minimum field, specify the number of workers that Veeam Backup for Microsoft Azure will launch in the selected regions after you finish working with the wizard.

   b. In the Keep maximum field, specify the maximum number of workers that Veeam Backup for Microsoft Azure can launch and use simultaneously to process Azure resources in the selected regions during backup and restore operations.

   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. 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 and restore 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.

   d. 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 workers 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. When you remove a profile set, Veeam Backup for Microsoft Azure does not remove currently running worker instances that have been created based on this set — these instances are removed only when the related operations complete.

To remove a profile set from the Veeam Backup for Microsoft Azure infrastructure, do the following:

1. Switch to the Configuration page.
2. Navigate to Workers > Profile.
3. Select the profile set and click Remove.
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 the Veeam Backup for Microsoft Azure infrastructure, 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.
Configuring General Settings

Veeam Backup for Microsoft Azure allows you to configure general settings that are applied to all performed operations and deployed infrastructure components:

- Define for how long obsolete snapshots and session records will be retained.
- Provide certificates to secure connections between Veeam Backup for Microsoft Azure infrastructure 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 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
- 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. 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 **Settings > 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 of days must be between 90 and 36135, the number of months must be between 3 and 1188, and the number of years must be between 3 and 99.

   If you select this option, Veeam Backup for Microsoft Azure will first wait for the specified period of time after an Azure resource stops being processed by a backup policy, and only then will remove its obsolete snapshots from the configuration database.

4. Click **Save**.

**NOTE**

When Veeam Backup for Microsoft Azure removes an obsolete snapshot from the configuration database, it also removes the snapshot from the Microsoft Azure infrastructure.
Configuring Retention Settings for Session Records

Veeam Backup for Microsoft Azure stores records for all sessions of performed data protection and disaster recovery operations in the configuration database on the additional data disk attached to the backup appliance. These session records are removed from the configuration database according to their own 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 20 GB of storage capacity. If you choose not to remove sessions records at all, consider increasing the disk space to avoid runtime problems.
Configuring Global Email 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 SMTP server that will be used for sending email notifications, do the following:

1. Switch to the Configuration page.
2. Navigate to Settings > E-mail.
3. Select the Enable e-mail notifications check box.
4. In the SMTP Server 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.
5. Click Advanced to specify an account that will be used when authenticating against the SMTP server and to configure other connection settings.

   In the Advanced SMTP Options window:
   a. In the Port field, specify a communication port for SMTP traffic. The default SMTP port is 25.
   b. In the Timeout field, specify a connection timeout for responses from the SMTP server.
   c. For an SMTP server with SSL/TLS support, select the Connect using SSL check box to enable SSL data encryption.
   d. If your SMTP server requires authentication, select the This SMTP server requires authentication check box and choose the necessary account from the Log on as drop-down list.

      For an account to be displayed in the Log on as list, it must be added to the configuration database as described in section Adding Accounts. If you have not set up an account beforehand, click Add and follow the steps of the Add Account wizard.
   d. Click Save.
6. In the From field, enter an email address of the notification sender. This email address will be displayed in the From field of notifications.
7. 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 specify additional recipients. For more information, 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.

8. In the Subject field, specify a subject for notification messages. You can use the following variables in the subject:
   a. %JobName% — a backup policy name.
   b. %JobResult% — a backup policy result.
   c. %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.

9. 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.

10. To receive daily reports, select the **Send daily report at** check box and specify the exact time when the reports will be sent.

11. Click **Save**.

**TIP**

Veeam Backup for Microsoft Azure allows you to send a test message to check whether you have configured settings correctly. To do that, click **Send Test E-mail**. A test message will be sent to the specified email address.
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 **Settings > 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. [This step 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.
   c. At the **Summary** step of the wizard, review summary information and click **Finish**.

NOTE

Only .PFX files are supported.
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 begins — clocks are set one hour forward — all policy sessions scheduled to run at the missing hour on this day are skipped. You can run the policies manually as described in Starting and Stopping Backup Policies.
- When DST ends — clocks are set one hour back — all policy sessions scheduled to run 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 Settings > Time Zone.
3. Select the necessary time zone from the Time zone drop-down list.
4. Click Save.

**NOTE**

You cannot 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.

To configure SSO settings for Veeam Backup for Microsoft Azure, complete the following steps:

1. Switch to the Configuration page.
2. Navigate to Settings > Identity Provider.
3. In the Identity provider configuration section, import identity provider settings from a file obtained from your identity provider:
   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.
4. Forward the service provider authentication settings to the identity provider — to obtain the settings, 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.
After you configure SSO settings, you can add user accounts that will be able to log in to Veeam Backup for Microsoft Azure using single sign-on. For more information, see Adding User Accounts.

**IMPORTANT**

To authenticate a user whose identity has been 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 rule on the identity provider side and specify username as the outgoing claim type (if you use Active Directory Federation Service) or the option claim name (if you use Azure Active Directory).
Performing Configuration Backup and Restore

You can back up and restore the configuration database that stores data collected from Veeam Backup for Microsoft Azure for the existing backup policies, protected Azure resources, launched worker instances, 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 backup appliance in the Microsoft Azure infrastructure.

It is recommended that you regularly perform configuration backup for every backup appliance present in the Microsoft Azure infrastructure. Periodic configuration backups reduce the risk of data loss and minimize the administrative overhead costs in case any problems with the backup appliances occur.

You can run configuration backup manually on demand, or instruct Veeam Backup for Microsoft Azure to do it automatically on a regular basis.

**NOTE**

After Veeam Backup for Microsoft Azure creates a configuration backup, it performs a rescan of the whole infrastructure to detect obsolete snapshots. These snapshots are then removed from the configuration database according to the specified [global retention settings](#).

Performing Snapshot-Based Configuration Backup

You can instruct Veeam Backup for Microsoft Azure to automatically create snapshots of the backup appliance. You can then use these snapshots to recover or migrate Veeam Backup for Microsoft Azure data to another Azure VM, as described in [this Veeam KB article](#).

To configure the auto-backup settings, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **Settings > 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 [Retention Policy for Snapshots](#).
   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 must be created every day, on work days (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 specify a time shift to postpone the snapshot creation by a defined amount of time (in minutes) in the specified interval. To do that, use 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 **Settings > 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 **Adding Backup Repositories**. The **Repository** list shows only backup repositories that have encryption enabled.

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 Settings > Configuration Backup.
3. In the Backup schedule section, set the Enable scheduling toggle to On.
4. Click Choose in 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.
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 Retention Policy for Backups.
6. In the Create daily backup at field, choose whether configuration backups will be created every day, on work days (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 **Settings > Configuration Backup**.
3. Use either of the following options:
   - To export the last successful configuration backup:
     1. In the **Overview** section, click **Export Last Backup**.
     2. 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:
     1. In the **Configuration restore** section, click **Available Restore Points**.
     2. In the **Available Restore Points** window, select the necessary backup and click **Export Backup**.
     3. 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.
Restoring Configuration Data

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.

**IMPORTANT**

Before you start the restore process, check the following prerequisites:

- Stop all policies that are currently running.
- Check the version of the backup appliance. In version 4.0, there is no backward compatibility for configuration restore.

To restore the configuration database, 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.
Step 1. Launch Configuration Restore Wizard

To launch the Configuration Restore wizard, do the following:

1. Switch to the Configuration page.
2. Navigate to Settings > 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 store configuration backup files.
  
  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 a 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.
- **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 infrastructure 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.

![Configuration Restore](image-url)
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.

<table>
<thead>
<tr>
<th>Action</th>
<th>Status</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Starting the restore process...</td>
<td>Success</td>
<td>—</td>
</tr>
<tr>
<td>Validating the configuration restore request...</td>
<td>Success</td>
<td>—</td>
</tr>
<tr>
<td>Downloading the backup restore point...</td>
<td>Success</td>
<td>28 sec</td>
</tr>
<tr>
<td>Preparing data to start the restore...</td>
<td>Success</td>
<td>—</td>
</tr>
<tr>
<td>Validating the configuration backup file...</td>
<td>Success</td>
<td>—</td>
</tr>
<tr>
<td>Starting the restore process...</td>
<td>Success</td>
<td>—</td>
</tr>
<tr>
<td>Stopping the backup appliance service...</td>
<td>Success</td>
<td>1 sec</td>
</tr>
<tr>
<td>Saving the database persistent data...</td>
<td>Success</td>
<td>—</td>
</tr>
<tr>
<td>Enabling the authentication token cache...</td>
<td>Success</td>
<td>—</td>
</tr>
<tr>
<td>Creating a database backup in case of a rollback...</td>
<td>Success</td>
<td>—</td>
</tr>
<tr>
<td>Creating new database for the configuration restore...</td>
<td>Success</td>
<td>—</td>
</tr>
<tr>
<td>Preparing configuration files for restore...</td>
<td>Success</td>
<td>—</td>
</tr>
<tr>
<td>Restoring the backup appliance configuration...</td>
<td>Success</td>
<td>7 sec</td>
</tr>
<tr>
<td>Setting permissions to configuration files...</td>
<td>Success</td>
<td>—</td>
</tr>
<tr>
<td>Restoring the restored database...</td>
<td>Success</td>
<td>—</td>
</tr>
<tr>
<td>Upgrading the database schema version...</td>
<td>Success</td>
<td>—</td>
</tr>
<tr>
<td>Finalizing the database restore process...</td>
<td>Success</td>
<td>—</td>
</tr>
<tr>
<td>Restoring the database persistent data...</td>
<td>Success</td>
<td>—</td>
</tr>
<tr>
<td>Deleting backup files...</td>
<td>Success</td>
<td>—</td>
</tr>
<tr>
<td>Finishing the restore process...</td>
<td>Success</td>
<td>—</td>
</tr>
</tbody>
</table>
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 click **Next**.

**TIP**

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 the issue, click **Recheck** to ensure the backup appliance is now fully functional.

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 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 **Azure SQL** 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).
- **Last Backup** — the date and time of the most recent backup policy (if any).

On the Resources page, you can also perform the following actions:

- Manually create image-level backups of Azure SQL databases and Azure VMs. For more information, see sections Performing SQL Backup and Performing VM Backup.
- Manually create cloud-native snapshots of Azure file shares. For more information, see Performing File Share Backup.

![Resource List Example]

---

117 | Veeam Backup for Microsoft Azure | User Guide
Managing Backed-Up Data

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 is no longer exists in the Microsoft Azure infrastructure, 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 and Removing File Share Snapshots.

Managing 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.
- **Last Backup** — the date and time of the most recent restore point created for the Azure VM.
- **Region** — the region in which the Azure VM resides.
- **VM Size** — the VM size of the Azure VM.
- **Resource Group** — the resource group that stores resources related to the Azure VM.
- **Operating System** — the operating system running on the Azure VM.
- **File-Level Recovery URL** — a link to the File-Level Restore 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 Restore browser and authentication information used to access this worker instance.

- **Tenant ID** — the unique identification number of the Azure tenant where the Azure VM is deployed.
- **Subscription ID** — the unique identification number of the Microsoft Azure subscription that is used to manage costs of 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 **Performing VM Restore**.
Removing 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 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.
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 with 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**.
Removing Azure VM Snapshots Created Manually

If you want to remove specific cloud-native snapshots created for an Azure VM 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**.
Managing 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.
- **Last Backup** – the date and time of the most recent restore point created for the Azure SQL database.
- **Resource Group** – the resource group that stores resources related to the Azure SQL database.
- **Region** – the region in which the Azure SQL database resides.
- **SQL Elastic Pool** – the name of the elastic pool to which the Azure SQL database is added.
- **Tenant ID** – the unique identification number of the Azure tenant where the Azure SQL database belongs.
- **Subscription ID** – the unique identification number of the Microsoft Azure subscription that is used to manage costs of 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 Backups.
- Restore data of backed-up Azure SQL databases. For more information, see Performing SQL Restore.
Removing Backups

Veeam Backup for Microsoft Azure applies the **configured retention policy settings** to automatically remove image-level backups created 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 > Azure SQL**.
2. Select Azure SQL databases whose data you want to remove.
3. Click **Remove** and select either of the following options:
   - **All** — to remove all image-level backups created for the selected Azure SQL databases both by backup policies and manually.
   - **Backups** — to remove all image-level backups created in backup repositories for the selected Azure SQL databases.
   - **Archive** — to remove all image-level backups created in archive repositories for the selected Azure SQL databases.
   - **Manual** — to remove all image-level backups created for the selected Azure SQL databases manually.
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 with 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 > 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 specify the number of hours before the expiration time when the notification must 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 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**.
Removing SQL Backups Created Manually

If you want to remove specific backups created for an Azure VM manually, do the following:

1. Navigate to Protected Data > 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.
Managing File Share 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** — the number of restore points created for the Azure file share.
- **Last Backup** — the date and time of the most recent restore point created for the Azure file share.
- **Resource Group** — the resource group that stores resources related to the Azure file share.
- **Region** — the region in which the Azure file share resides.
- **File-level Recovery URL** — a link to the File-Level Restore 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 Restore browser and authentication information used to access this worker instance.

- **Tenant ID** — the unique identification number of the Azure tenant where the Azure file share belongs.
- **Subscription ID** — the unique identification number of the Microsoft Azure subscription that is used to manage costs of 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 Backups.
- Restore data of backed-up Azure file shares. For more information, see Performing File Share Restore.
Removing 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.

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

If you want to remove specific cloud-native snapshots created for a file share 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.
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 image-level backups of Azure SQL databases**
  An image-level 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 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.

To schedule data protection tasks to run automatically, create backup policies. For Azure VMs and Azure file shares residing in any of the regions added to the backup policies, you can also take cloud-native snapshots manually when needed — for more information, see Creating VM Snapshots Manually and Creating File Share Snapshots Manually. For Azure SQL databases, you can also perform a quick backup manually when needed — for more information, see Creating SQL Backups Manually.
How Backup Works

Veeam Backup for Microsoft Azure does not install agent software inside instances to retrieve data. To back up resource data, Veeam Backup for Microsoft Azure uses native Microsoft Azure capabilities. During every backup session, Veeam Backup for Microsoft Azure creates a cloud-native snapshot (for an Azure VM or an Azure file share) or a BACPAC file (for an Azure SQL database) for each Azure resource added to a backup policy. The cloud-native snapshot is further used to create an image-level backup of the Azure VM, and the BACPAC file is used to create an image-level backup of the Azure SQL database.

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. Keys and 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.

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 target backup repository resides.
      
      By default, Veeam Backup for Microsoft Azure launches worker instances with the same network configurations as those specified for the processed Azure VMs. However, you can add specific worker configurations. For more information, see Managing Worker Instances.
   
   b. Re-creates the virtual disks from the cloud-native snapshot created at step 1 and attaches them to the worker instance.
      
      Note that the cloud-native snapshot used as a source for image-level backup is not a temporary snapshot — when the backup session completes, this snapshot remains in the snapshot chain and is deleted later according to the specified policy scheduling settings.
   
   c. Reads data from the virtual disks on the worker instance, transfers the data to the target backup repository and stores it in the native Veeam format.
      
      To reduce the amount of data read from virtual disks, 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.
   
   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 a backup repository storing backed-up data 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.
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 resource group where the Azure VM belongs.
- Snapshots created for unmanaged virtual disks are saved to the Azure storage account where the Azure VM resides.
- Backups created for managed and unmanaged virtual disks are saved to the target blob container.

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 the Azure region where the processed Azure VM resides. This snapshot becomes a starting point in the snapshot chain.
   
   The creation of the first snapshot may take significant time to complete since Veeam Backup for Microsoft Azure copies the whole image of the Azure VM.

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 creation of subsequent snapshots typically takes less time to complete, compared to the first snapshot in the chain. Note, however, that the completion time still depends on the amount of processed data.

   For more information on how incremental 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.

Cloud-native snapshots

<table>
<thead>
<tr>
<th>Sun</th>
<th>Mon</th>
<th>Tue</th>
<th>Wed</th>
<th>Thu</th>
<th>Fri</th>
<th>Sat</th>
</tr>
</thead>
</table>

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

**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 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 Retention Policy for Backups.
Changed Block Tracking

The changed block tracking (CBT) mechanism allows Veeam Backup for Microsoft Azure to reduce the amount of data read from processed virtual disks, 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. To do that, 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.

IMPORTANT

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 first cloud-native snapshot has not been removed from the chain by the retention policy before an incremental backup session runs. For more information on configuring snapshot retention settings, see Creating Backup Policies.
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](#).
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 also processes all transaction logs of the copied database to create 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 when performing 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 of residing on an Azure SQL Managed Instance — creates a copy of the source database on the staging server using point-in-time restore (PITR) from the point made 10 minutes ago. 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 is located.

   By default, Veeam Backup for Microsoft Azure launches worker instances with the same network configurations as those specified for the processed Azure SQL databases. However, you can add specific worker configurations. For more information, see Managing Worker Instances.

3. 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, be 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 a backup repository and stores it in the native Veeam format.

5. [Applies when performing 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 a backup repository storing backed-up data 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 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 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 Retention Policy for Backups.
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.
File Share Backup

Veeam Backup for Microsoft Azure performs file share 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 the 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 to the configuration database on the backup appliance.
   d. Associates the created index with the share snapshot created at step 1.

      The creation of the index 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.
   e. 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 file share data and saves it in the Azure region where the processed file share resides. This snapshot becomes a starting point in the snapshot chain.

      The creation of the first snapshot may take significant time to complete since Veeam Backup for Microsoft Azure copies the whole image of the Azure file share.

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 creation of subsequent snapshots typically takes less time to complete, compared to the first snapshot in the chain. Note, however, that the completion time still depends on the amount of processed data.

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

Each cloud-native snapshot in the snapshot chain contains metadata. Metadata includes information about the processed Azure 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 a source Azure file shares during recovery operations, and so on.

Cloud-native snapshots act as independent restore points for backed-up Azure 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 Retention Policy for Snapshots.

## Retention Policy

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 policy can be specified:

- **In restore points** — for cloud-native snapshots.
  
  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 Retention Policy for Snapshots.

- **In days/months/years** — for image-level backups and archives.
  
  Restore points in the backup chain can be stored only for the allowed period of time. If a restore point is older than the specified limit, Veeam Backup for Microsoft Azure removes it from the backup chain. For more information, see sections Retention Policy for Backups and Retention Policy for Archived Backups.

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

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

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

Mind 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 File Share Data.

Retention Policy for Backups

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

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.
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 in it 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.

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.
      
      ![Diagram](image)
      
      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.

   ![Diagram](image)

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.

   ![Diagram](image)
Performing VM Backup

To produce cloud-native snapshots and image-level backups of Azure VMs, 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.

One backup policy can be used to process multiple Azure VMs within different regions, but you can back up each Azure VM with one backup policy at a time. If an Azure VM 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 Azure VM from processing. For information on how to set a priority for a backup policy, see Setting Backup Policy Priority.

To schedule data protection tasks to run automatically, create backup policies. For each protected Azure VM, you can also take a cloud-native snapshot manually when needed.

Creating Backup Policies

To create a 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 Policies > Virtual Machines.
2. 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: * : / ? " < > | @ # $ % ^ & ,.

---

149 | Veeam Backup for Microsoft Azure | User Guide
Step 3. Configure Backup Source Settings

At the Sources step of the wizard, specify backup source settings:

1. Select the Azure Active Directory where Azure VMs that you plan to back up reside.
2. Choose regions where Azure VMs that you want to back up reside.
3. Select resources to back up.

Step 3a. Select Azure Active Directory

In the Source section of the Sources step of the wizard, choose an Azure Active Directory where Azure VMs that you plan to back up reside.

1. Click Select Azure Active Directory.
2. In the Choose an Azure account from the available list window, select the necessary directory from the Azure Active Directory list.
   For an Azure Active Directory to be displayed in the list of available directories, it must be created in the Microsoft Azure portal as described in Microsoft Docs.
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, select resources that you want to back up or to exclude from the policy:

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 the 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. From the Resource type drop-down list, select either of the following options:

      - Subscription — to back up Azure VMs that belong to 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.

   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 where the resources belong, return to step 3a and click Rescan in the Choose an Azure account from the available list 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 the subscriptions, resource groups, tags or Azure VMs that you do not want to back up — the procedure is the same as described for including resources in the backup scope.

Mind 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 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 about 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 Service Bus 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 inbound and outbound access using the **443** port, you must allow HTTPS traffic over **443** port for `<FQDN>.servicebus.windows.net`, where `<FQDN>` is the name of the Service Bus namespace used by the Veeam backup service.

To find the Service Bus namespace name, do the following:

1. Log in to the Microsoft Azure portal.
2. Select the Azure service where the backup appliance belongs.
3. Choose the resource group associated with the backup appliance.

   The Service Bus namespace name will be displayed in the Name column of the resource table.
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, at the **Guest Processing** step of the wizard, do the following:

- 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**

Supported script formats:

- For Windows-based Azure VMs Veeam Backup for Microsoft Azure supports the EXE, BAT, CMD, WSF, JS, VBS and PS1 file formats.
- For Linux-based Azure VMs Veeam Backup for Microsoft Azure supports the SH file format.

In the opened window, specify pre-snapshot and post-snapshot scripts that must 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 must 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 work days (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**

   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, see How Backup Works.

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 Retention Policy for Snapshots.
   - 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 Retention Policy for Backups.
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 the Veeam Backup for Microsoft Azure infrastructure as described in section **Adding Backup Repositories**.

6. To save changes made to the backup policy settings, click **Apply**.

To allow the **CBT mechanism** to be used when processing Azure VM data by the backup policy, the number of snapshots to keep in a snapshot chain must be enough to ensure that the first cloud-native snapshot has not been removed from the chain by the retention policy before an incremental backup session runs. Consider the following example. You want a 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 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 a full 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 will be still present in the snapshot chain and can be further used to create an incremental backup.
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, see How Backup Works.

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 Retention Policy for Snapshots.
   - 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 Retention Policy for Backups.

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 the Veeam Backup for Microsoft Azure infrastructure 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, see **How Backup Works**.

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 **Retention Policy for Snapshots**.
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 Retention Policy for Backups.

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 the Veeam Backup for Microsoft Azure infrastructure 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 Retention Policy for Backups.
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 the Veeam Backup for Microsoft Azure infrastructure 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, Working Days), 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

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 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 with 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 with the Archive access tier that will store archive backups.

**IMPORTANT**

- 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.
- If you enable backup archiving, it is recommended that you set the Snapshots to keep value to 0, to reduce unexpected snapshot charges.
- If you enable backup archiving, 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 the Microsoft Azure infrastructure 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 Retention Policy for Backups.

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.
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 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.

**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 monthly 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 first 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 first 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 send notifications according to 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. Do not use spaces after semicolons between the specified email 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.
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.

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.
Step 9. Finish Working with Wizard

At the Summary step of the wizard, review summary information and click Finish.
Creating 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 Backup Policies (step 3c).
3. Complete the Take Manual Snapshot wizard:
   a. At the Account step of the wizard, select an Azure account whose permissions Veeam Backup for Microsoft Azure will use to create a snapshot.
      
      For an account to be displayed in the Azure Account list, it must be added to Veeam Backup for Microsoft Azure as described in section Adding Azure Service Account or Adding Repository 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

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.

One backup policy can be used to process multiple Azure SQL databases within different regions, but you can back up each Azure SQL database with one backup policy at a time. If an Azure SQL database 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 Azure SQL database from processing. For information on how to set a priority for a backup policy, see Setting Backup Policy Priority.

To schedule data protection tasks to run automatically, create backup policies. For each protected Azure SQL database, you can also create an image-level backup manually when needed.

IMPORTANT

Veeam Backup for Microsoft Azure does not support back up of databases hosted by Azure Arc-enabled SQL Managed Instances and SQL Servers on Azure Arc-enabled servers.

Creating 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 a 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 Policies > Azure SQL.
2. 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 backup source settings:

1. Select an Azure Active Directory where SQL Servers and databases that you plan to back up reside.
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 Azure Active Directory

In the Source section of the Sources step of the wizard, choose an Azure Active Directory where SQL Servers and databases that you plan to back up reside.

1. Click Select Azure Active Directory.
2. In the Choose an Azure account from the available list window, select the necessary directory from the Azure Active Directory list.
   For an Azure Active Directory to be displayed in the list of available directories, it must be created in the Microsoft Azure portal as described in Microsoft Docs.
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, select resources that you want to 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 the 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. From the Resource type drop-down list, 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.

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 where the resources belong, return to the step 3a and click Rescan in the Choose an Azure account from the available list 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 or SQL Servers that you do not want to back up — the procedure is the same as described for including resources in the backup scope.

Mind 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 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 Veeam Backup for Microsoft Azure uses staging servers to protect Azure SQL databases, see How Backup Works.

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 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 Policy wizard. To add an account, 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](https://docs.microsoft.com).

   **IMPORTANT**

   If you use custom Transparent Data Encryption (TDE) to protect SQL Server data, mind 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 Accounts](https://docs.microsoft.com). 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 Policy** wizard. To add an account, click **Add** and complete the **Add Account wizard**.

   **NOTE**

   To perform backup with a staging server, Veeam Backup for Microsoft Azure uses the default Azure service account 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.

   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.
3. Use the Run at drop-down list to choose whether you want the backup policy to run every day, on work days (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 Retention Policy for Backups.
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 the Veeam Backup for Microsoft Azure infrastructure 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 Retention Policy for Backups.
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 the Veeam Backup for Microsoft Azure infrastructure 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 Retention Policy for Backups.
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 the Veeam Backup for Microsoft Azure infrastructure 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 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 Retention Policy for Backups.

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 the Veeam Backup for Microsoft Azure infrastructure as described in section Adding Backup Repositories.

5. To save changes made to the backup policy settings, click **Apply**.

![Backup Settings](image.png)
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, Working Days), 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 Retention Policy for Backups.
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 with 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 with the Archive access tier that will store archived data.
**IMPORTANT**

- 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.
- If you enable backup archiving, 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 the Microsoft Azure infrastructure 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 Retention Policy for Backups.
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.

<table>
<thead>
<tr>
<th>March</th>
<th>May</th>
<th>July</th>
<th>September</th>
<th>November</th>
<th>January</th>
<th>February</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mon, Week 1</td>
<td>Mon, Week 1</td>
<td>Mon, Week 1</td>
<td>Mon, Week 1</td>
<td>Mon, Week 1</td>
<td>Mon, Week 1</td>
<td>Mon, Week 1</td>
</tr>
</tbody>
</table>

![Graph showing backup and archive sessions]

- **Injecting data blocks**
- **Incremental archive backups**
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.

**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 monthly 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 first 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 first 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 **On**.
   
   If you set the toggle to **Off**, Veeam Backup for Microsoft Azure will send notifications according to 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. Do not use spaces after semicolons between the specified email 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.
Step 7. 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 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.

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 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 Disabling and Enabling 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 the 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 System Requirements.
4. After the network issues are fixed, you can enable the backup policy as described in section Disabling and Enabling Backup Policies.
Creating 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 > 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 an Azure Active Directory whose permissions Veeam Backup for Microsoft Azure will use to create a backup.
      
      For an Azure Active Directory to be displayed in the list of available directories, it must be created in the Microsoft Azure portal as described in Microsoft Docs.
   
   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 the Veeam Backup for Microsoft Azure infrastructure as described in section Adding Backup Repositories.
   
   **NOTE**

   You can select only a backup repository with the Hot or Cool access tier.

   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 File Share Backup

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.

One backup policy can be used to process multiple Azure file shares within different regions, but you can back up each Azure file share with one backup policy at a time. If an Azure file share 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 Azure file share from processing. For information on how to set a priority for a backup policy, see Setting Backup Policy Priority.

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 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 Policies > Azure Files.
2. 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 backup source settings:

1. **Select an Azure Active Directory where Azure file shares that you plan to protect reside.**
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 Azure Active Directory

In the **Account** section of the **Sources** step of the wizard, choose an Azure Active Directory where Azure file shares that you plan to protect reside.

1. **Click Configure account.**
2. **In the Choose an Azure account from the available list window, select the necessary directory from the Azure Active Directory list.**
   For an Azure Active Directory to be displayed in the list of available directories, it must be created in the Microsoft Azure portal as described in Microsoft Docs.
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, select resources that you want to protect.

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 the 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. From the Resource type drop-down list, 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 specific source from the global list and wait for Veeam Backup for Microsoft Azure to populate the resource list.

      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 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 where the resources belong, return to step 3a and click Rescan in the Choose an Azure account from the available list 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 resource groups, Azure file shares or storage accounts that you do not want to protect — the procedure is the same as described for including resources in the backup scope.

Mind 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 within a file share snapshot.

**IMPORTANT**

When performing indexing operations, Veeam Backup for Microsoft Azure uses the Server Message Block (SMB) 3 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.
3. Use the **Run at** drop-down list to choose whether you want the backup policy to run everyday, on work days (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 Retention Policy for Snapshots.
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 **Retention Policy for Snapshots**.
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 Retention Policy for Snapshots.

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, Working Days), 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).

![Diagram 1](image1.png)

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.

![Diagram 2](image2.png)

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.

![Diagram 3](image3.png)
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 **On**.
   - If you set the toggle to **Off**, Veeam Backup for Microsoft Azure will send notifications according to 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. Do not use spaces after semicolons between the specified email 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.
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.

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 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 Managing File Share 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 an Azure account whose permissions Veeam Backup for Microsoft Azure will use to create a snapshot.
      
      For an account to be displayed in the **Azure Account** list, it must be added to Veeam Backup for Microsoft Azure as described in section Adding Azure Service Account or Adding Repository 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**.
Managing Backup Policies

After you create backup policies, you can edit, enable and run them, and also 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, export settings of the existing policies and import new ones.

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 or Performing File Share Backup.

![Edit VM Policy Interface](image-url)
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 **Policy Priority**.
3. In the **Priority Order** window, use the **Up** and **Down** arrows to set the priority order for backup policies, and click **Apply** to save the settings.

   The first backup policy in the list will have the highest priority.

**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.

![Veeam Backup for Microsoft Azure interface showing policies and sessions]

```
At the end of the policy tab, you will see a list of all instances and their corresponding status. To view details about a specific backup session, click on the status icon next to the instance. This will open a pop-up window displaying the backup session details, including the type of backup (backup policy or snapshot policy), the start and end times, and the status (success, error, or warning).

![Backup session details]

```

---

228 | Veeam Backup for Microsoft Azure | User Guide
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 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.

To start or stop a 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 backup policy as a template for creating other backup policies. You can export a 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.

Exporting Backup Policies

To export a 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 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**.
Performing Restore

In various disaster recovery scenarios, Veeam Backup for Microsoft Azure allows you to perform the following restore operations using backed-up data:

- **Restore of Azure VMs** — restores Azure VMs from cloud-native snapshot or image-level backups to the original location or to a new location.
- **Restore of Azure SQL databases** — restores Azure SQL databases from image-level backups to the original or to a new location.
- **Restore of Azure file shares** — restore files of Azure file shares from cloud-native snapshots to the original location or to a new location.

Performing VM Restore

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.

How VM Restore Works

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 to archived backups] Retrieves data from the archived restore point.
2. Launches a worker instance in the Azure region where the restored Azure VM will reside.
3. Creates empty virtual disks and attaches them to the worker instance.
   - The number of empty virtual disks equals the number of virtual disks attached to the backed-up Azure VM.
4. Restores backed-up data to the empty virtual disks on the worker instance.
5. Detaches the virtual disks with the restored data from the worker instance.
6. Deallocates the worker instance.
7. Creates an Azure VM in the specified location.
8. Attaches the created virtual disks with the restored data to the Azure VM.

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 an Azure account.
4. Choose a restore mode.
5. Specify data retrieval 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 check box next to the necessary Azure VM.
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.
2. Click **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.
Step 3. Select Azure Account

At the **Account** step of the wizard, select an Azure account whose permissions Veeam Backup for Microsoft Azure will use to perform the restore operation.

1. Click **Select account**.

2. In the **Choose an Azure account** window, select the necessary account and click **Apply**.

For an Azure Active Directory to be displayed in the list of available directories, it must be created in the Microsoft Azure portal as described in [Microsoft Docs](https://docs.microsoft.com/en-us/azure/active-directory).
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 a Microsoft 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 added and associated with the Azure account selected at step 3, as described in Microsoft Docs.

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 specify the number of hours before data expiration when the notification will be sent.
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 the 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 where 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.
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 in the Microsoft Azure portal 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 and associated to the necessary subnet 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.

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 to archived backups] Retrieves data from the archived restore point.
2. Launches a worker instance in the Azure region where the restored virtual disks will reside.
3. Creates empty virtual disks and attaches them to the worker instance.
   - The number of empty virtual disks equals the number of disks you want to restore.
4. Restores backed-up data to the empty virtual disks on the worker instance.
5. Detaches the virtual disks with the restored data from the worker instance.
6. Deallocates the worker instance.

**NOTE**

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.

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 an Azure account.
4. Choose a restore mode.
5. Specify data retrieval 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 check box next to 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 Exclude disks from restore window, select check boxes next to the disks that you do not want to restore, and click Apply.
Step 3. Select Azure Account

At the Account step of the wizard, select an Azure account whose permissions Veeam Backup for Microsoft Azure will use to perform the restore operation.

1. Click Select account.

2. In the Choose an Azure account window, select the necessary account and click Apply.

For an Azure Active Directory to be displayed in the list of available directories, it must be created in the Microsoft Azure portal as described in Microsoft Docs.
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 a Microsoft 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 added and associated with the Azure account selected at step 3, as described in Microsoft Docs.

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 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 specify the number of hours before data expiration when the notification will be sent.
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 where 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.
   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.

NOTE
You cannot convert managed virtual disks into unmanaged, but you can convert unmanaged virtual disks into managed.

![Disk properties window](image-url)
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.

![Screenshot of Veeam Backup for Microsoft Azure wizard with the Reason step highlighted]

**Step 8. Finish Working with Wizard**

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

![Screenshot of Veeam Backup for Microsoft Azure wizard with the Summary step highlighted]
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 using the File-Level Restore browser.

**IMPORTANT**

If Azure Disk Encryption is enabled for virtual disks attached to the selected Azure VM, Veeam Backup for Microsoft Azure will not be able to perform the file-level recovery operation. File-level recovery for Azure VMs with the Azure Disk Encryption option enabled is not supported in the current Veeam Backup for Microsoft Azure version. For more information on Azure Disk Encryption, see Microsoft Docs.

You can recover files and folders from the following file systems only:

- Microsoft Windows systems — FAT, FAT32, NTFS.
- Linux systems — ext2, ext3, ext4, XFS, Btrfs.

Veeam Backup for Microsoft Azure supports file-level recovery only for Microsoft Windows basic volumes.

**TIP**

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 Veeam Backup & Replication infrastructure as an external repository, and perform the file-level recovery operation as described in the Veeam Backup & Replication User Guide.

How File-Level Recovery Works

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. Launches the File-Level Restore browser.
   - The File-Level Restore browser displays the file system tree of the backed-up Azure VM. In the browser, you select the necessary files and folders to recover.

4. Saves the selected files and folders to the local machine.

5. Detaches the virtual disks from the worker instance.

6. Deallocates the worker instance.
Before You Begin

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.

How to Perform File-Level Recovery

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. Specify a restore reason.
4. Finish working with the wizard — start a recovery session.
5. Choose files and folders to recover.
6. Stop the recovery session.
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 check box next to the necessary Azure VM.
3. Click Restore > File-Level Recovery.

You can also 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 **Virtual Machine** 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. 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 4. 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 **File-level Recovery** wizard, start a recovery session and display the **File-Level Recovery** window. 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.

**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.

In the **File-Level Recovery** window, you can track the progress of the recovery session. In the **URL** column of the window, Veeam Backup for Microsoft Azure will display a link to the File-Level Restore browser. You can use the link in either of the following ways:

- Click the link to open the File-Level Restore 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 Restore 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 Restore browser the 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 Restore 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 Restore browser matches the provided certificate thumbprint.
Step 5. Download Recovered Files and Folders

In the File-Level Restore 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 machine from which you access the File-Level Restore browser.

1. In the File-Level Restore browser, 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 recover.
4. Switch to the Restore List tab.
5. On the Restore List tab, review the list of items to recover, select check boxes next to the items, and click Download.
Step 6. Stop Recovery Session

After you finish working with the File-Level Restore 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 Restore browser for 30 minutes, 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.
Performing SQL Restore

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.

How SQL Restore Works

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

1. [Applies to archived backups] 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. [This step 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.

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 Azure SQL database, do the following:

1. **Launch the SQL Database restore wizard.**
2. **Select a restore point.**
3. **Select an Azure 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 > Azure SQL.**
2. Select the check box next to the necessary Azure SQL Database.
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.

To select a restore point, do the following:

1. Select the Azure SQL database.
2. Click **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:

- **Date** — the date when the restore point was created.
- **Size** — the size of the restore point:
- **Access Tier** — the storage tier of a backup repository where the restore point is stored.
Step 3. Select Azure Account

At the **Account** step of the wizard, select an Azure account whose permissions Veeam Backup for Microsoft Azure will use to perform the restore operation.

1. Click **Select account**.
2. In the **Choose an Azure account** window, select the necessary account and click **Apply**.

For an Azure Active Directory to be displayed in the list of available directories, it must be created in the Microsoft Azure portal as described in Microsoft Docs.

---

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 Accounts.

   IMPORTANT

   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.
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 specify the number of hours before data expiration when the notification will be sent.
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]

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 Account](#).
   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 the 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 the System Requirements section.
3. After network issues are fixed, you can start the SQL Database Restore wizard again.
Performing File Share Restore

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.

How File Share Restore Works

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 Restore browser.
   The File-Level Restore 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.

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 an Azure 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 check box next to the necessary Azure file share.
3. Click **Restore > File-Level Restore**.

Alternatively, click the link in the **Restore Points** column. Then, in the **Available Restore Points** window, select the necessary restore point and click **File-Level Restore**.
Step 2. Select Azure Account

At the **Account** step of the wizard, select an Azure account whose permissions Veeam Backup for Microsoft Azure will use to perform the restore operation.

1. Click **Select account**.

2. In the **Choose an Azure account** window, select the necessary account and click **Apply**.

   For an Azure Active Directory to be displayed in the list of available directories, it must be created in the Microsoft Azure portal as described in [Microsoft Docs](https://docs.microsoft.com).

![Choose an Azure account window](image-url)
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 a Microsoft 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 added and associated with the Azure account selected at step 3, as described in Microsoft Docs.

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 Restore 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, start a restore session and display the File-Level Recovery window.

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.

In the File-Level Recovery window, you can track the progress of the restore session. In the URL column of the window, Veeam Backup for Microsoft Azure will display a link to the File-Level Restore browser. You can use the link in either of the following ways:

- Click the link to open the File-Level Restore 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 Restore 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 Restore browser the includes a public DNS name of the backup appliance hosting the browser and authentication information used to access the browser.
- A thumbprint of a TLS certificate installed on the backup appliance hosting the File-Level Restore browser.

To avoid a man-in-the-middle attack, before you start restoring files and folders, check that the certificate thumbprint displayed in the web browser from which you access the File-Level Restore browser matches the provided certificate thumbprint.
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 Restore browser, you can find and restore items (files and folders) of the selected Azure file share. All restored items will be saved in a single .ZIP archive to the default download directory on a machine from which you access the File-Level Restore browser.

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.
5. On the **Restore List** tab, review the list of files and folders, select check boxes next to the items that you want to restore, and click **Restore**.
Step 8. Stop Restore Session

After you finish working with the File-Level Restore 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 Restore browser for 30 minutes, 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.
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** page will show only those sessions that have the same status as that clicked in the widget.

  For more information on the **Session Log** page, see **Viewing Session Statistics**.

- **Successful Policy Tasks** — 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** page 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** page, 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. You can track real-time statistics of all running and completed operations on the Session Log page.

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 .CSV or .XML file. To do that, navigate to the necessary tab and click Export. Veeam Backup for Microsoft Azure will save the file with the exported data to the default download directory on the local machine.

**NOTE**

Even if you try to export properties of a specific object, Veeam Backup for Microsoft Azure will still export all properties of all objects present on the currently opened tab.
Updating Veeam Backup for Microsoft Azure

Veeam Backup for Microsoft Azure allows you to check for new product versions and available package updates, download and install them right from the Web UI.

It is recommended that you timely install available 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.

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 the 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 use either of the following options:

- Install updates immediately
- Schedule update installation

You can also set a reminder to send update notifications.

**IMPORTANT**

You can update the backup appliance using the Veeam updater service only. Updating of the backup appliance manually is not supported.

---

## Installing Updates

**IMPORTANT**

Before you install a product update, make sure all backup policies are disabled and restore tasks are finished. Otherwise, the update process will interrupt 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 will 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 on 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 Updater](image.png)

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 next Monday.

2. **Click** Remind me later.

![Veeam Updater page](image-url)
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.
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 infrastructure components
- The error message or an accurate description of the problem you are facing
- Log files

Viewing Product Details

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 Azure Tenant ID — the unique identification number of the Azure tenant where the backup appliance is deployed.
- 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 Logs

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.
Appendix. Working in Private Environments

For Veeam Backup for Microsoft Azure to be able 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 workers 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 a storage account.
- Configure network settings for a SQL Server.
- Configure network settings for a SQL Managed Instance.

Configuring Network Settings for Storage Accounts

To allow Veeam Backup for Microsoft Azure to create and manage backup repositories, and to back up unmanaged Azure VMs and file shares, in a storage account where your 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.

**IMPORTANT**

Firewall rules are applied only for VNets that are created in the same region or in paired regions. That is why if the backup appliance and the storage account are residing in different regions that are not paired, you must create private endpoints to securely connect to resources that you want to protect. For more information on paired Azure regions, see Microsoft Docs.
Configuring Firewall Settings

To configure firewall rules for a storage account, 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 where a storage account in which you want to create a private endpoint belongs. The resource group page will open.
4. In the Resource list, locate and click the storage account in which resources that you want to protect reside. The Storage account page will open.
6. On the Firewalls and virtual networks tab, choose the Selected networks option and click Add existing virtual network.
7. In the Add networks window:
   a. From the Subscription drop-down list, select a Microsoft Azure subscription where 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 workers 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 workers are connected.

   NOTE
   To allow access from virtual networks to storage accounts, Microsoft Azure uses service endpoints. If any of the selected networks do not have service endpoints enabled for Microsoft.Storage, Microsoft Azure will raise a warning. In this case, click Enable and wait for the process to complete. For more information on 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. Private endpoints are network interfaces that use private IP addresses from your virtual network. For more information on private endpoints, see Microsoft Docs.

You must create a separate private endpoint for every VNet to which the backup appliance or workers are connected. To create a private endpoint, complete the following steps:

1. Launch the Create a private endpoint wizard.
2. Configure private endpoint settings.
4. Specify virtual network settings.
5. Specify DNS settings.
6. Assign tags.
7. Finish working with the wizard.

Step 1. Launch Create a Private Endpoint Wizard

To launch the Create a private endpoint wizard, 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 where a storage account in which you want to create a private endpoint belongs. The resource group page will open.
4. In the Resources list, select the storage account. The Storage account page will open.
6. Switch to the Private endpoint connections tab and click Private endpoint to launch the wizard Create a private endpoint wizard.
Step 2. 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 a Microsoft Azure subscription where your virtual network belongs.

2. From the Resource group drop-down list, select a resource group where your newly created private endpoint will reside. 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 workers 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: Configuration >**.

![Creating a private endpoint in Microsoft Azure](image-url)
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 workers are connected.

2. From the Subnet drop-down list, select a subnet to which the backup appliance or workers are connected. For a subnet to be displayed, it must be created within a specified 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 where the DNS zone will belong.
   c. From the Resource group drop-down list, select the resource group where the DNS zone will reside.

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.

![Image of Microsoft Azure portal with Create a private endpoint wizard and tags configuration](image)

**Step 7. Finish Working with Wizard**

At the **Review + create** step of the **Create a private endpoint** wizard, review configured settings and click **Create**.
Configuring Network Settings for SQL Server

To allow Veeam Backup for Microsoft Azure to back up SQL Servers operating in private environment, 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.

**IMPORTANT**

Firewall rules are applied only for VNets that are created in the same region or in paired regions. That is why if the backup appliance and the SQL Server are residing in different regions that are not paired, you must create private endpoints to securely connect to resources that you want to protect. For more information on paired Azure regions, see Microsoft Docs.

Configuring Firewall Settings

To configure firewall rules for a SQL Server, 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 where a storage account in which you want to create a private endpoint 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.

**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.

6. On the Firewalls and virtual networks tab, click Add existing virtual network.
7. In the Create/Update virtual network rule window, create a new firewall rule:
   a. In the Name field specify a name for the rule.
   b. From the Subscription drop-down list, select a Microsoft Azure subscription where Azure VM hosting Veeam Backup for Microsoft Azure belongs.
   c. From the Virtual networks drop-down list, select check boxes next to virtual networks to which workers are connected.
   d. From the Subnets drop-down list, select check boxes next to subnets to which workers are connected.

**NOTE**

To allow access from virtual networks to SQL Servers, Microsoft Azure uses service endpoints. If any of the selected networks do not have have service endpoints enabled for Microsoft.Sql, Microsoft Azure will raise a warning. In this case, click Enable and wait for the process to complete. For more information on service endpoints, see Microsoft Docs.
Creating Private Endpoints

If the backup appliance resides in another region than the SQL Server that you want to protect, or you do not want to add firewall rules, you can create private endpoints for your SQL Server to allow Veeam Backup for Microsoft Azure access to the databases. Private endpoints are network interfaces that use private IP addresses from your virtual network. For more information on private endpoints, see Microsoft Docs.

You must create a separate private endpoint for every VNet to which workers are connected. To create a private endpoint, complete the following steps:

1. Launch the Create a private endpoint wizard.
2. Configure private endpoint settings.
4. Specify configuration settings.
5. Assign tags.
6. Finish working with the wizard.

Step 1. Launch Create a Private Endpoint Wizard

To launch the Create a private endpoint wizard, 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 where a storage account in which you want to create a private endpoint 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.
6. Switch to the Private access tab and click Create a private endpoint to launch the wizard Create a private endpoint wizard.
Step 2. 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 a Microsoft Azure subscription where Azure VM hosting Veeam Backup for Microsoft Azure belongs.

2. From the **Resource group** drop-down list, select a resource group where your newly created private endpoint will reside. 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](https://docs.microsoft.com).

3. In the **Name** field, enter a name for the private endpoint.

4. From the **Region** drop-down list, select a Azure region of the virtual network to which workers are connected.

   For more information on the Azure regions, see [Microsoft Docs](https://docs.microsoft.com).

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 Subscription drop-down list, select a Microsoft Azure subscription where 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: Configuration >.
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 workers are connected.
2. From the Subnet drop-down list, select a subnet to which workers are connected. For a subnet to be displayed, it must be created within a specified 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.
   a. From the Subscription drop-down list, select a subscription where the DNS zone will belong.
   b. From the Resource group drop-down list, select the resource group where the DNS zone will reside.
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**.
Configuring Network Settings for SQL Managed Instance

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 workers 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 workers are connected. Leave the default settings for the other options in this section.
   c. From the Subscription drop-down list, select a Microsoft Azure subscription where workers reside.
   d. From the Virtual networks drop-down list, select the virtual network to which workers are connected.
   e. Click Add.