## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONTACTING VEEAM SOFTWARE</td>
<td>6</td>
</tr>
<tr>
<td>ABOUT THIS DOCUMENT</td>
<td>7</td>
</tr>
<tr>
<td>WELCOME TO VEEAM BACKUP FOR MICROSOFT AZURE</td>
<td>8</td>
</tr>
<tr>
<td>SYSTEM REQUIREMENTS</td>
<td>9</td>
</tr>
<tr>
<td>LICENSING</td>
<td>11</td>
</tr>
<tr>
<td>Installing and Removing License</td>
<td>12</td>
</tr>
<tr>
<td>Viewing License Information</td>
<td>14</td>
</tr>
<tr>
<td>Revoking License Units</td>
<td>15</td>
</tr>
<tr>
<td>ARCHITECTURE OVERVIEW</td>
<td>16</td>
</tr>
<tr>
<td>DEPLOYMENT</td>
<td>18</td>
</tr>
<tr>
<td>Installing Veeam Backup for Microsoft Azure</td>
<td>18</td>
</tr>
<tr>
<td>Step 1. Launch Create Virtual Machine Wizard</td>
<td>19</td>
</tr>
<tr>
<td>Step 2. Configure Azure VM Properties</td>
<td>21</td>
</tr>
<tr>
<td>Step 3. Select OS Disk Type</td>
<td>23</td>
</tr>
<tr>
<td>Step 4. Configure Network Settings</td>
<td>24</td>
</tr>
<tr>
<td>Step 5. Specify Management Options</td>
<td>26</td>
</tr>
<tr>
<td>Step 6. Begin Installation</td>
<td>27</td>
</tr>
<tr>
<td>After You Install</td>
<td>27</td>
</tr>
<tr>
<td>Uninstalling Veeam Backup for Microsoft Azure</td>
<td>28</td>
</tr>
<tr>
<td>ACCESSING VEEAM BACKUP FOR MICROSOFT AZURE</td>
<td>29</td>
</tr>
<tr>
<td>CONFIGURING VEEAM BACKUP FOR MICROSOFT AZURE</td>
<td>31</td>
</tr>
<tr>
<td>Managing Accounts</td>
<td>32</td>
</tr>
<tr>
<td>Managing Azure Service Accounts</td>
<td>32</td>
</tr>
<tr>
<td>Managing Repository Accounts</td>
<td>42</td>
</tr>
<tr>
<td>Managing Backup Administrator Accounts</td>
<td>51</td>
</tr>
<tr>
<td>Managing Backup Repositories</td>
<td>56</td>
</tr>
<tr>
<td>Adding Backup Repositories</td>
<td>56</td>
</tr>
<tr>
<td>Editing Backup Repository Properties</td>
<td>62</td>
</tr>
<tr>
<td>Removing Backup Repositories</td>
<td>63</td>
</tr>
<tr>
<td>Managing Workers</td>
<td>64</td>
</tr>
<tr>
<td>Adding Worker Configurations</td>
<td>64</td>
</tr>
<tr>
<td>Editing Worker Configurations</td>
<td>69</td>
</tr>
<tr>
<td>Removing Worker Configurations</td>
<td>70</td>
</tr>
<tr>
<td>Removing Worker Instances</td>
<td>71</td>
</tr>
<tr>
<td>Configuring General Settings</td>
<td>72</td>
</tr>
<tr>
<td>Configuring Global Retention Settings</td>
<td>72</td>
</tr>
</tbody>
</table>
Configuring Notification Settings ................................................................................................... 74
Configuring Auto-Backup Settings .................................................................................................79
Working with Certificates .............................................................................................................. 80
Changing Time Zone................................................................................................................................. 81

PERFORMING BACKUP ....................................................................................................................... 82

How Backup Works.................................................................................................................................. 83
Snapshot Chain ......................................................................................................................................... 84
Backup Chain.......................................................................................................................................... 85
Changed Block Tracking ......................................................................................................................... 86
Retention Policy......................................................................................................................................... 87

Creating Backup Policies ....................................................................................................................... 89
Step 1. Launch Add Policy Wizard ...................................................................................................... 90
Step 2. Specify Backup Policy Name .................................................................................................. 90
Step 3. Configure Backup Source Settings ....................................................................................... 91
Step 4. Specify Guest Processing Settings ....................................................................................... 94
Step 5. Configure Backup Target Settings....................................................................................... 97
Step 6. Specify Policy Scheduling Options ..................................................................................... 98
Step 7. Review Cost Estimations ................................................................................................... 106
Step 8. Specify Retry and Email Notification Settings .................................................................. 108
Step 9. Finish Working with Wizard ............................................................................................. 109

Editing Backup Policy Settings ........................................................................................................... 110
Setting Backup Policy Priority .......................................................................................................... 111
Disabling and Enabling Backup Policies.............................................................................................. 112
Starting and Stopping Backup Policies............................................................................................... 113
Creating Snapshots Manually ............................................................................................................... 114
Removing Backups and Snapshots....................................................................................................... 115
Removing Snapshots Created Manually ........................................................................................ 116

PERFORMING RESTORE ..................................................................................................................... 117

Performing VM Restore ....................................................................................................................... 117
Step 1. Launch Restore Virtual Machines Wizard ........................................................................... 118
Step 2. Select Restore Point ......................................................................................................... 119
Step 3. Choose Restore Mode ........................................................................................................ 120
Step 4. Select Subscription ............................................................................................................ 121
Step 5. Specify Instance Settings .................................................................................................. 122
Step 6. Specify Disk Names .......................................................................................................... 124
Step 7. Specify Network Settings .................................................................................................. 125
Step 8. Specify Restore Reason .................................................................................................... 126
Step 9. Finish Working with Wizard .............................................................................................. 127

Performing Disk Restore.................................................................................................................... 128
Step 1. Launch Disk Restore Wizard ................................................................. 129
Step 2. Select Restore Point ............................................................................. 130
Step 3. Choose Restore Mode .......................................................................... 131
Step 4. Select Subscription ............................................................................. 132
Step 5. Specify Disk Settings .......................................................................... 133
Step 6. Specify Restore Reason ....................................................................... 134
Step 7. Finish Working with Wizard ............................................................... 135

Performing File-Level Recovery ..................................................................... 136
Step 1. Launch File-Level Recovery Wizard ................................................... 137
Step 2. Select Restore Point ............................................................................. 138
Step 3. Specify Restore Reason ....................................................................... 139
Step 4. Start Restore Session .......................................................................... 140
Step 5. Download Restored Files and Folders ............................................... 141
Step 6. Stop Recovery Session ...................................................................... 142

VIEWING SESSION STATISTICS ................................................................. 143
COLLECTING OBJECT PROPERTIES ............................................................. 144
UPDATING VEEAM BACKUP FOR MICROSOFT AZURE ................................. 145
  Checking for Updates ............................................................................... 146
  Installing Updates ............................................................................... 147
  Viewing Updates History ..................................................................... 151
GETTING TECHNICAL SUPPORT .................................................................. 152
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 at www.veeam.com/support.html 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 www.veeam.com/contacts.html.

Online Support

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

- Full documentation set: www.veeam.com/documentation-guides-datasheets.html
- Veeam R&D Forums at 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.
- Keep the backed-up data in cost-effective and long-term Microsoft Azure storage accounts.
- Restore 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 into the Veeam Backup & Replication infrastructure. With Microsoft Azure Plug-in for Veeam Backup & Replication, you can manage data protection and recovery operations from the Veeam Backup & Replication console. For more information, see the Integration with Veeam Backup for Microsoft Azure User Guide.
# System Requirements

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

## Network 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>HTTPS</td>
<td>443</td>
<td>Required to access the Web UI component from a user workstation.</td>
</tr>
<tr>
<td></td>
<td>Worker instance</td>
<td>HTTPS</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>
</tr>
<tr>
<td>Backup appliance</td>
<td>Worker instance</td>
<td>SSH</td>
<td>22</td>
<td>Required to deploy the Worker service to worker instances.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RPC</td>
<td>643</td>
<td>Required to communicate with the Worker service running on worker instances.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TCP</td>
<td>9999</td>
<td>Required to perform file-level recovery.</td>
</tr>
<tr>
<td></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>HTTPS</td>
<td>443</td>
<td>Required to download information about available product updates.</td>
</tr>
<tr>
<td></td>
<td>SMTP server</td>
<td>TCP</td>
<td>25</td>
<td>Default port used for sending email notifications. <strong>Note:</strong> The TCP 25 port is the port that is the most commonly used by SMTP servers.</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>
</tbody>
</table>
The backup server 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
- Microsoft Identity Platform
- Azure’s Ubuntu repository
Licensing

Veeam Backup for Microsoft Azure is licensed by the number of protected Azure VMs. 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. Each protected Azure VM consumes 1 license unit. However, if a VM has only manually created snapshots, it does not consume any license units.

**NOTE**

If an Azure VM has not been backed up within the past 31 days, Veeam Backup for Microsoft Azure automatically revokes the license unit from the VM. 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 Azure VMs free of charge.

- **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 Azure VMs 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 30 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 Azure VMs 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*. 
Installing and Removing License

By default, Veeam Backup for Microsoft Azure 2.0 comes with a Free license. To unlock the full functionality, you must install a Bring Your Own License.

Installing License

To install or update a license on a VM that runs Veeam Backup for Microsoft Azure, 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.
Removing BYOL License

NOTE
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.

To remove a BYOL 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 automatically switches back to the Free edition. In this case, according to the FIFO (first-in first-out) queue, only the first 10 Azure VMs registered in the configuration database remain protected. You can revoke license units from these Azure VMs as described in the Revoking License Units.
Viewing License Information

Each Azure VM that has a restore point created in the past 31 days is considered to be protected and consumes 1 license unit. To view the list of Azure VMs that consume license units, do the following:

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

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

- **Type** — the type of the license unit.
- **Instances** — the number of protected Azure VMs that consume the license units.
- **State** — 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).
- **Last Backup** — the date and time of the last backup session.

![License Usage Tab](image-url)
Revoking License Units

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

To revoke a license unit from an Azure VM, do the following:

1. Switch to the Configuration page.
2. Navigate to Licensing > License Usage.
3. Select the Azure VM that you no longer want to protect.
4. Click Revoke License.
Architecture Overview

The backup infrastructure of Veeam Backup for Microsoft Azure 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 existing backup policies, protected Azure VMs, deployed worker instances, connected Microsoft Azure accounts and so on.

### Backup Repositories

A backup repository is a folder in a blob container where Veeam Backup for Microsoft Azure stores backups of Azure VMs.

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.

### 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 backup files stored in backup repositories. For more information on Veeam Backup & Replication encryption standards, see the **Encryption Standards** section of the Veeam Backup & Replication User Guide.

To learn how to enable encryption at the repository level, see **Adding Backup Repositories**.

### Limitations for Repositories

To use a blob container as a target location for Azure VM 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</td>
</tr>
<tr>
<td>BlobStorage</td>
<td>Standard</td>
<td>Hot, Cool</td>
</tr>
</tbody>
</table>
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 the backup workload and distribute backup traffic when transferring data to backup repositories.

Veeam Backup for Microsoft Azure automatically deploys a worker instance to every processed Azure VM and keeps the instance running for the duration of the backup or restore process. Workers are deployed based on worker configurations that can be created either automatically by Veeam Backup for Microsoft Azure, or manually by the user as described in Adding Worker Configuration.

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 Recovery for Veeam Backup 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 Recovery for Veeam Backup browser is installed automatically on every worker instance that is launched for file-level recovery.

For more information on recovering files of Azure VMs using the File Level Recovery for Veeam Backup browser, see Performing File-Level Recovery.

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 local machine and the File Level Recovery for Veeam Backup 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.

**IMPORTANT**

Veeam Backup for Microsoft Azure can process only those Azure VMs that belong to the Azure subscription associated with the Azure Active Directory where the backup appliance is running. To protect an Azure VM that belongs to the subscription associated with another Azure Active Directory, deploy another instance of Veeam Backup for Microsoft Azure in the subscription with the target directory. For more information about Azure Active Directory and subscriptions, see Microsoft Docs.

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 account 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:
   
   o 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.
   
   o 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 set to No.
   
   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**.

   It is not recommended that you set the **Authentication type** option to **SSH public key** since this may complicate the process of accessing the Veeam Backup for Microsoft Azure UI.

   b. In the **Username** and **Password** fields, specify credentials that will be used to access the Veeam Backup for Microsoft Azure UI.

10. Click **Next > Discs >**.
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 used with 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.
   
   - Select the Encryption on at-rest with a platform-managed key option to use the default type of encryption.
   - 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 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.

5. Make sure that the Place this virtual machine behind an existing load balancing solution option is set to No.
   
   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**.

<table>
<thead>
<tr>
<th>Basics</th>
<th>Disks</th>
<th>Networking</th>
<th>Management</th>
<th>Advanced</th>
<th>Tags</th>
<th>Review + create</th>
</tr>
</thead>
</table>

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. **Learn more**

### Network Interface

When creating a virtual machine, a network interface will be created for you.

- **Virtual network**: twstorageaccounts-rg-vnet
- **Subnet**: default (10.0.0.0/24)
- **Public IP**: (new) VBA-ip
- **NIC network security group**: Advanced

*This VM image has preconfigured NSG rules*

**Configure network security group**: (new) VBA-nsg

**Accelerated networking**: On

*The selected image does not support accelerated networking.*

### Load balancing

You can place this virtual machine in the backend pool of an existing Azure load balancing solution. **Learn more**

**Place this virtual machine behind an existing load balancing solution?**: Yes

[Review + create] [Previous] [Next: Management]
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](https://docs.microsoft.com).

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

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

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 VM running Veeam Backup for Microsoft Azure.

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 perform the initial configuration of Veeam Backup for Microsoft Azure, do the following:

1. In a web browser, navigate to the Veeam Backup for Microsoft Azure.
   
   The URL consists of a public IPv4 address or DNS hostname of the Azure VM where Veeam Backup for Microsoft Azure is installed. Note that the website is available over HTTPS only.
   
   For example:
   
   - IPv4 address — https://135.169.170.192
   - Public DNS hostname — https://abc.ukwest.cloudapp.azure.com/

   **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. 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](#).

3. 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 Backup Administrator Accounts](#).

   **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](#).

4. Generate a new certificate for Veeam Backup for Microsoft Azure, as described in [Replacing Web Certificate](#).

5. 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. To uninstall the solution, you must delete the created resources:

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.
3. Open the resource group where the backup appliance resides.
4. On the Overview page, locate the Azure VM running Veeam Backup for Microsoft Azure and all resources associated with the Azure VM. To do this, in the search field, enter the name of the backup appliance.
5. Select check boxes next to the Virtual machine, Network interface, Public IP address and Disk resource types, and click Delete.
6. In the Delete Resources window, confirm the action and click Delete.

Note that backed-up data will not be removed automatically. You can keep this data in your Microsoft Azure environment and import image-level backups to a new backup appliance as described in section Adding Backup Repositories. If you no longer need the backed-up data, you can remove it manually:

- To remove backups, navigate to a storage account, select the necessary files, and click Delete.
- To remove snapshots, navigate to the resource group, select the necessary snapshots, and click Delete.

**NOTE**

If the resource group contains more than one backup appliance, it is recommended that you remove snapshots from Veeam Backup for Microsoft Azure as described in section Removing Backups and Snapshots before you uninstall the solution.
Accessing Veeam Backup for Microsoft Azure

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

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

   **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).

   The address consists of a public IPv4 address or DNS hostname of the backup appliance. Note that the website is available over HTTPS only.

   **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.

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

   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 users to grant access to Veeam Backup for Microsoft Azure. For more information, see Adding Backup Administrator Accounts. If you forgot the password, you can reset it. To do that, click the **Forgot password** link and follow the steps in the **Password Reset** window.

3. 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.
4. Click **Login**.

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**.

---

**Veeam Backup for Microsoft Azure**

Welcome! Please log in.

**Username:** admin  
**Password:** **********

- Keep me logged in

**Log In**  **Forgot password?**

---

**Logging Out**

To log out of the Veeam Backup for Microsoft Azure, 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. Create accounts to get access to your Azure resources.
2. Add backup repositories.
3. Create worker configurations.

**NOTE**

Even after you add accounts that manage your Azure resources and configure all the necessary settings, Veeam Backup for Microsoft Azure will not populate the list of Azure VMs on the Instances page — unless you create backup policies and specify the regions where the Azure VMs belong, as described in section Creating Backup Policies.
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:

- **Azure service account** — to get access to Azure resources that you want to protect.
- **Repository accounts** — to manage backup repositories assigned to folders in blob containers.
- **Backup administrator accounts** — to allow different users to control access to Veeam Backup for Microsoft Azure.

Managing Azure Service Accounts

When you create an Azure service account to get access to Azure resources (such as subscriptions, resource groups and storage accounts) within your Azure environment, Veeam Backup for Microsoft Azure automatically creates an Azure AD Application.

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

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

**IMPORTANT**

Consider the following:

- You can add only one Azure service account to the Veeam Backup for Microsoft Azure backup infrastructure.
- Due to technical limitations, a service account only grants access to subscriptions added to the tenant where the backup appliance is deployed. Subscriptions that are owned by other tenants will not be available. For more information on tenant and subscription in Microsoft Azure, see Microsoft Docs.

Adding Azure Service Account

To add a new service account, do the following:

1. **Launch the Add Azure Account wizard.**
2. **Specify a connection name.**
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 Account**.
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 may vary depending on the Azure resource type. The following characters are not supported: * : / ? " < > | . For more information naming restrictions in Microsoft Azure, see [Microsoft Docs](https:).

---

![Add Azure Account screenshot](image-url)
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.

<table>
<thead>
<tr>
<th>Add Azure Account</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></td>
</tr>
<tr>
<td></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>
Step 3a. 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 a new Azure AD application, Veeam Backup for Microsoft Azure uses the Microsoft Azure Cross-platform Command Line Interface (Azure CLI). To authenticate Veeam Backup for Microsoft Azure to the Azure CLI, you must provide a single-use verification code.

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

1. Click **Copy code to clipboard**.
2. Click [https://microsoft.com/devicelogin](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**.
Step 3b. 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 the existing Azure AD application that grants access to Azure resources. For an Azure AD application to be used, it must be created as described in Microsoft Docs.

**IMPORTANT**

- The selected Azure AD application must have the Microsoft.Authorization/*/Write permission set in the subscription associated with the backup appliance.
- If you have disabled the Users can register applications option on the Microsoft Azure portal, make sure that the service account has the Application Developer role.

For more information on role permissions in Azure Active Directory, see Microsoft Docs.

To specify a service account, do the following:

1. In the Application ID field, enter the application ID.
   
   You can find the application ID in the application settings of your Azure Active Directory. For more information, see Microsoft Docs.

2. Select an application authentication type:
   
   - Select the Client (application) secret option to use a client secret. A secret string can be obtained as described in Microsoft Docs.
   
   - Select the Certificate option to use a certificate to authenticate against the server, 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 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](image-url)
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 resource 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>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary</strong></td>
</tr>
<tr>
<td><strong>General</strong></td>
</tr>
<tr>
<td>Name:</td>
</tr>
<tr>
<td>Description:</td>
</tr>
<tr>
<td>Authentication:</td>
</tr>
<tr>
<td>Tenant ID:</td>
</tr>
<tr>
<td>Active Directory Name:</td>
</tr>
<tr>
<td>AD Group:</td>
</tr>
<tr>
<td><strong>Visual Studio Premium MSDN</strong></td>
</tr>
<tr>
<td>Subscription ID:</td>
</tr>
<tr>
<td><strong>Integration Tests</strong></td>
</tr>
<tr>
<td>Subscription ID:</td>
</tr>
</tbody>
</table>

[39 | Veeam Backup for Microsoft Azure | User Guide]
Editing Azure Service Account

Veeam Backup for Microsoft Azure allows you to modify service account settings specified while adding the service account to the Veeam Backup for Microsoft Azure infrastructure:

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 the 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 uses this account to access any of the existing backup repositories. Remove all the related backup repositories and disable policies, and then try removing the account again.
Managing Repository Accounts

Veeam Backup for Microsoft Azure allows you to configure repository accounts to work with backup repositories. Repository accounts usually have less permissions than your Azure service account and are intended to provide a granular access to backup repositories.

Adding Repository Accounts

To add a new repository account, do the following:

1. Launch the Add Repository Account wizard.
2. Specify the name for the repository.
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 Connection Name

At the Connection Name 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.

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

[Image of the Add Repository Account window with options selected and buttons for Previous, Next, and Cancel]
Step 3a. Create 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 a new Azure AD application, Veeam Backup for Microsoft Azure uses the Microsoft Azure Cross-platform Command Line Interface (Azure CLI). To authenticate Veeam Backup for Microsoft Azure to the Azure CLI, you must provide a single-use verification code.

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

1. Click **Copy code to clipboard**.
2. Click [https://microsoft.com/devicelogin](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 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.
Step 3b. Specify 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 the existing Azure AD application that grants access to Azure resources. For an Azure AD application to be used, it must be created as described in Microsoft Docs.

**IMPORTANT**

The selected Azure AD application must have the Storage Account Contributor role. For more information on role permissions in Azure Active Directory, see Microsoft Docs.

To specify a service account, do the following:

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.

2. Select an application authentication type:

   - Select the Client (application) secret option to use a client secret. A secret string can be obtained as described in Microsoft Docs.
   - Select the Certificate option to use a certificate to authenticate against the server, 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 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 Repository Account](image-url)
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>General</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Name: rep-account-02</td>
</tr>
</tbody>
</table>
|         | Description: Created by Admin
|         | Authentication: Device Logon |
|         | Tenant ID: 97438793-c913-4e51-8485-d33056db7ba5 |
|         | Active Directory Name: Veeam Software Group GmbH |
| Visual Studio Premium with MSDN | Subscription ID: 280921a2-220d-45c9-92dd-62b6df5a3e87f8a2 |

[Previous] [Finish] [Cancel]
Editing Repository Accounts

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

1. Switch to the Configuration page.
2. Navigate to Accounts > Repository Accounts.
3. Select the repository account and click Edit.
   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 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 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 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 Backup Administrator Accounts

To allow different users to access Veeam Backup for Microsoft Azure, you can create the Backup Administrator accounts for these users. Users that log in to Veeam Backup for Microsoft Azure as Backup Administrators are allowed to perform all administrative activities and data protection tasks (for example, to configure settings, to back up Azure VMs, to restore backed-up data and so on).

Adding Backup Administrator Accounts

To add a new account to the Veeam Backup for Microsoft Azure configuration, do the following:

1. Launch the Add User wizard.
2. Specify user information.
3. Specify a password.
4. Finish working with the wizard.
Step 1. Launch Add User Wizard

To launch the Add User wizard, do the following:

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

Step 2. Specify User Information

At the User 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 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.
Step 3. Specify Password

At the Login Info step of the wizard, specify a password that you want to use to access the Veeam Backup for Microsoft Azure UI.

Step 4. Finish Working with Wizard

At the Summary step of the wizard, review configuration information and click Finish.
Changing Backup Administrator Password

You can change the password of the backup administrator whose credentials you used to log in to Veeam Backup for Microsoft Azure.

1. At the top right corner of the Veeam Backup for Microsoft Azure window, click the user name and then click **Change Password**.

2. 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 the user identity by providing a temporary six-digit code generated by an authentication application running on a trusted device.

To enable MFA for a user accessing Veeam Backup for Microsoft Azure as a Backup Administrator, do the following:

1. Switch to the Configuration page.
2. Navigate to Accounts > Backup Admins.
3. Select the account and click Enable MFA.
4. In the MFA Settings window, do the following:
   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. In the Type the received MFA code field, enter a verification code sent by the authentication application.
   d. Click OK.

**NOTE:**
Each user from the Backup Admins page can enable or disable multi-factor authentication for other users.
Managing Backup Repositories

Veeam Backup for Microsoft Azure uses blob containers as target locations to store backups of Azure VMs. To add a blob container to Veeam Backup for Microsoft Azure, configure a backup repository.

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**.

![Add Repository Wizard](image)

Step 2. Specify Repository Name

At the **Repository 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 may vary depending on the Azure resource type. The following characters are not supported: * : / \ " < > | .

![Repository Name](image)
Step 3. Configure Repository Settings

At the **Repository** step of the wizard, specify backup repository settings:

1. **Select an Azure account.**
2. **Select a storage account where the target blob container resides.**

**Step 3a. Select Azure Account**

In the **Select account** section of the **Repository** step of the wizard, 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 an account to be displayed in the **Azure Account** list, it must be added to Veeam Backup for Microsoft Azure as described in sections *Adding Azure Service Account* and *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**.

![Add Repository wizard screenshot](image-url)
Step 3b. Select Storage Account

In the Select storage account section of the Repository step of the wizard, do the following:

1. Click Select.

2. In the Storage Account section, 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.

3. In the Container and Folder section, do the following:
   
   a. From the Container list, select a blob container that will be used as a target location for backups of Azure VMs.
      
      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.
   
   b. Specify a folder where Veeam Backup for Microsoft Azure will store backups of Azure VMs. You can either select an existing folder or create a new one.
      
      ▪ To create a new folder, select the Create new folder option and specify a name for the folder.
      
      ▪ To use an existing folder, select the Use existing folder option and select the necessary folder.
      
      For a folder to be displayed in the Folder list, it must be assigned to any of the repositories ever added (either existing or already removed) to the Veeam Backup for Microsoft Azure infrastructure.

**NOTE**

If the selected folder already contains backups, 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.
Step 4. Specify Repository Options

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

1. If the selected storage account supports tiering In the **Storage tier** section, specify the access tier type to manage costs of storing backed-up data.
   - Select **Hot tier** if you plan to access the backed-up data frequently.
   - Select **Cool tier** if you plan to store backed-up data at least for 30 days and do not need to access it frequently.
   - Select **Inferred tier** if you plan to use the same access tier as specified for the storage account where the selected repository resides.
   - Select **Auto-create all tiers** if you want to instruct Veeam Backup for Microsoft Azure to automatically create two repositories one with hot tier and another with cool tier.

   For more information on access tiers for blob storage accounts, see [Microsoft Docs](https://docs.microsoft.com).

2. If you have selected the **Create new folder** option at the **Select storage account** step of the wizard, choose whether you want to enable encryption.

   If you have selected an existing folder with the enabled encryption, provide a password.
Step 5. Finish Working with Wizard

At the **Summary** step of the wizard, review configuration information, choose whether you want to proceed to the **Sessions Log page**, 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 encryption for the repository, follow the instructions provided in section Adding Backup Repositories (step 7).
   c. At the Summary step of the wizard, review summary information, choose whether you want to proceed to the Sessions Log page, and click Finish.
Removing Backup Repositories

Veeam Backup for Microsoft Azure allows you to permanently remove backup repositories from the backup infrastructure. When you remove a backup repository, Veeam Backup for Microsoft Azure unassigns the repository from the folder in the target blob container, and this 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 backup files previously stored in the repository and keeps these files in the folder in the Microsoft Azure portal. You can assign the folder to a new backup repository, so that Veeam Backup for Microsoft Azure imports the backup 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 backup data, you can remove it as described in section Removing Backups and Snapshots.

To remove a backup repository from the Veeam Backup for Microsoft Azure backup infrastructure, 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. To remove such a repository, you must first delete a reference to this repository in the backup policy settings.

Veeam Backup for Microsoft Azure does not remove backups stored in the backup repository. You can reconnect the folder with backup to a new repository at any time and perform data protection and disaster recovery operations with backups from this repository. To remove backups from repositories, follow the steps described in the Removing Backups and Snapshots section.
Managing Workers

Veeam Backup for Microsoft Azure comes with the default worker configuration that deploys minimum 1 and maximum 5 worker instances depending on the number of processed Azure VMs.

To optimize infrastructure costs and ensure better performance of the backup and restore processes, you can manage the number of worker instances deployed by Veeam Backup for Microsoft Azure by adding custom worker configurations.

Adding Worker Configurations

To add a new worker configuration to the backup infrastructure, do the following:

1. Launch the New Region Specific Worker Configuration wizard.
2. Specify general settings for the worker configuration.
3. Specify network settings for the worker configuration.
4. Finish working with wizard.
Step 1. Launch New Region Specific Worker Configuration Wizard

To launch the **New Region Specific Worker Configuration** wizard, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **Workers > Configuration**.
3. Click **Add**.
Step 2. Specify General Settings

At the **VM Configuration** step of the wizard, do the following:

1. From the **Region** drop-down list, select a region where new worker instances will operate. You must select the same region where the target Azure storage account belongs.

2. Choose the size of VMs that will operate as worker instances:
   a. Click the link next to **VM size** to open the list of the available Azure VM sizes.
   b. In the **Select VM size** window, select the necessary size of an Azure VM and click **OK**.
   For more information on Azure VM sizes, see Microsoft Docs.

3. In the **Min** field, specify the number of workers that Veeam Backup for Microsoft Azure must deploy after you create a new worker configuration. This allows you to reduce the amount of time required to perform the operation.

4. In the **Max** field, specify the maximum number of workers that Veeam Backup for Microsoft Azure can deploy and use simultaneously during a backup or restore operation. This allows you to improve the performance of the operation.

**NOTE**

Veeam Backup for Microsoft Azure keeps each worker instance running for 10 minutes after the backup or restore process completes. When this time expires, the minimum number of worker instances are shut down, and the rest are removed from the backup infrastructure.
Step 3. Specify Network Settings

At the Network Settings 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 New.
   b. In the Create Network window, specify names and ranges of IP addresses for the new virtual network and the new subnet, and click OK.

      To specify IP address ranges, use the CIDR (Classless Inter-Domain Routing) notation. For more information on building networks in Microsoft Azure, see Microsoft Docs.

   IMPORTANT
   - The specified subnet range must have at least one free IP address — Veeam Backup for Microsoft Azure will deploy and simultaneously run as many worker instances as many free IP addresses there are in the subnet range.
   - The selected virtual network must be peered with the network to which the backup appliance is connected. To learn how to manage peering settings, see Microsoft Docs.
   - It is required to configure a service endpoint (routing) to the Microsoft.Storage service. The virtual network settings can be specified on the Microsoft Azure portal. For more information on virtual network service endpoints, see Microsoft Docs.

2. Select a security group that will be associated with the specified subnet. For a security group to be displayed it must be created in advance as described in Microsoft Docs.
Step 4. Finish Working with Wizard

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

After you click **Finish**, Veeam Backup for Microsoft Azure will create the new worker configuration and deploy the specified minimum number of worker instances. To view the list of deployed worker instances, switch to the **Instances** page.

![New Region Specific Worker Configuration](image)

---

**Region and VM size**

- Region: East US
- VM size: Standard_A2_v2
- Price (per hour): 0.091 USD

**Number of workers instances**

- Minimum: 1
- Maximum: 5

**Network settings**

- Virtual Network: IT.Network (10.43.0.0/16)
- Virtual Network Resource Group: res-group-v2
- Subnet: subnet-rg (10.43.0.0/24)
- Network Security Group: azure-proxinetsecuritygroup

---

Click finish to save the region settings and exit the wizard.
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 > Configuration.
3. Select the worker configuration and click Edit.
4. Complete the Edit Region Specific Worker Configuration wizard:
   a. To change the size of Azure VMs that operate as worker instances, and to configure the number of the worker instances deployed during backup and restore operations, follow the instructions provided in section Adding Worker Configuration (step 2).
   b. To modify the virtual network and subnet to which the worker instances are connected, and to change the security group associated with the specified subnet, follow the instructions provided in section Adding Worker Configuration (step 3).
5. 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

To remove a worker configuration from the backup infrastructure, do the following:

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

**NOTE**

When you remove a worker configuration, Veeam Backup for Microsoft Azure permanently removes from the backup infrastructure all worker instances that have been created based on this configuration. If there are any worker instances that are currently involved in a backup or restore process, these instances will be removed only when the process completes.
Removing Worker Instances

To remove from the backup infrastructure a worker instance created based on a worker configuration, 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 will be applied to all performed operations and deployed infrastructure components:

- Define for how long obsolete snapshots and session records must be retained.
- Provide certificates to secure connections between Veeam Backup for Microsoft Azure infrastructure components.
- Configure notification settings for the automated delivery of reports.
- Configure settings for the automatic backup of the backup appliance.

Configuring Global Retention Settings

Veeam Backup for Microsoft Azure allows you to configure global retention settings to specify for how long the following data must be retained in the configuration database:

- Obsolete snapshots
- Session records

Configuring Retention Settings for Obsolete Snapshots

If an Azure VM 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 snapshots become obsolete. Retention policy settings specified in backup policy settings do not apply to obsolete snapshots — these snapshots are removed from Veeam Backup for Microsoft Azure according to their own retention settings.

To configure retention settings for obsolete snapshots, do the following:

1. Switch to the Configuration page.
2. Navigate to Settings > Retention Settings.
3. In the Obsolete snapshots retention section, select one of the following options:
   - Select the Never option if you do not want Veeam Backup for Microsoft Azure to remove obsolete snapshots. This option is selected by default.
   - Select the After option to specify the number of days or months for which obsolete snapshots must be kept in the configuration database. The number of days must be between 3 and 99, the number of months must be between 3 and 1188.
     
     If you select this option, Veeam Backup for Microsoft Azure will first wait for the specified period of time after an Azure VM stops being processed by a backup policy, and then will remove its obsolete snapshots from the configuration database as soon as the period is over.
4. Click Save.
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. These session records are removed from Veeam Backup for Microsoft Azure after 365 days by default. However, you can configure retention settings for the records.

1. In the **Session retention** section of the **Retention Settings** page, select one 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 to specify the number of days or months during which session records must be kept 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**.
Configuring Notification Settings

Veeam Backup for Microsoft Azure allows you to specify email notification settings for automated delivery of reports. The daily report contains cumulative statistics for 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 Settings**.
3. Select the **Enable e-mail notifications** check box.
4. In the **SMTP Server** field, specify a DNS name or an IP address of the SMTP server. All email notifications (including test messages) and daily reports will be sent by this SMTP server.
5. Click **Advanced** to specify user credentials and connection settings.
   In the **Advanced SMTP Options** window:
   a. Specify the port number and connection timeout for the SMTP server. The default SMTP port is **25**.
   b. For an SMTP server with SSL/TLS support, select the **Connect using SSL** check box to enable SSL data encryption.
   c. If your SMTP server requires authentication, select the **This SMTP server requires authentication** check box and select the necessary account from the **Log on as** drop-down list.
      For an SMTP account to be displayed in the **Log on as** list, it must be added to the configuration database as described in section **Adding SMTP Accounts**. If you have not set up credentials beforehand, click **Add** on the right to add credentials.
   d. Click **Apply**.
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, specify the recipient addresses. Use a semicolon to separate multiple addresses.
   For each particular policy, you can specify additional recipients. For more information, see Creating Backup Policies (step 7).

**NOTE**

If you specify the same email recipient in both backup policy notification and global notification settings, Veeam Backup for Microsoft Azure will send each notification twice to this recipient.

8. In the **Subject** field, specify a subject for notification messages. You can use the following runtime in the subject:
   - **%JobName%** — a backup policy name.
   - **%JobResult%** — a backup policy result.
   - **%ObjectCount% instances** — the number of Azure VMs in the backup policy.
   - **%Issues%** — the number of VMs in the backup policy with the **Warning** or **Failed** status.
9. In the **Notify me immediately about** section, select the **Success**, **Warning** or **Failure** check boxes to receive email notifications on policies that completed successfully, failed or completed with warnings.
10. To receive daily reports, select the **Send daily report at** check box and specify at what time reports must be generated and sent.

11. Click **Save**.

**TIP**

Veeam Backup for Microsoft Azure allows you to send a test message to check whether you have configured email settings correctly. To do that, click **Send Test Email**. A test email will be sent to the specified email address.

---

**Adding SMTP Accounts**

To add credentials that will be used to access an SMTP server, do the following:

1. Launch the **Add Account wizard**.
2. Specify an account display name.
3. Specify user name and password.
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 > SMTP.
3. Click Add.

Step 2. Specify Account Display Name

At the Account Name step of the wizard, use the Name and Description fields to enter a name for the new SMTP account and to provide a description for future reference. The maximum length of the name is 255 characters.
Step 3. Specify Credentials

At the Account step of the wizard, specify credentials of a user account to be used to authenticate against the SMTP server, and click Finish.

[Image of Add Account dialog box with fields for Account Info and Account, and buttons for Previous, Finish, and Cancel]
Editing SMTP Accounts

For each credentials record, you can modify the settings configured while creating the record:

1. Switch to the **Configuration** page.
2. Navigate to **Accounts > SMTP**.
3. Select the SMTP 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 SMTP Accounts** (step 2).
   b. To provide a new user name and password for the account, follow the instructions provided in section **Adding SMTP Accounts** (step 3).
Configuring Auto-Backup Settings

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 > System**.
3. Set the **Enable Auto-Backup** toggle to **On**.
4. Click **Customize settings**.
5. In the **Self-Backup Settings** window, do the following:
   a. In the **Number of restore points** field, specify the number of snapshots that Veeam Backup for Microsoft Azure must keep.
   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 weekdays (Monday through Friday) or on specific days.
      - Select the **Monthly at this time** option if you want Veeam Backup for Microsoft Azure to create snapshots once a month on a defined day.
      - Select the **Periodically every** option if you want Veeam Backup for Microsoft Azure to create snapshots repeatedly throughout a day with a specific time interval. You can choose whether snapshots must be created every several hours or minutes. You can also instruct Veeam Backup for Microsoft Azure to create snapshots continuously, one after another.

   **TIP**

   If you choose to create snapshots once every several hours, you can also 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**.
Working with 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 Certificate.
4. Complete the Replace Certificate 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 generate a new self-signed certificate and manually trust it in your browser.
      - 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 a new 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.
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.

Since the backup appliance is deployed on an Azure VM in Microsoft Azure environment, 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 and click **Save**.
Performing Backup

With Veeam Backup for Microsoft Azure, you can protect Azure VM 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 a blob to an Azure storage account in the native Veeam format.

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.
How Backup Works

During every backup session, Veeam Backup for Microsoft Azure creates a cloud-native snapshot for each Azure VM added to a backup policy. The cloud-native snapshot is further used to create an image-level backup of the Azure VM. Veeam Backup for Microsoft Azure performs backup in the following way:

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

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 where the target location resides.
   b. Re-creates 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 until the next image-level backup session.
   c. Reads data from the virtual disks on the worker instance, transfers the data to a backup repository and stores it in the native Veeam format.

Veeam Backup for Microsoft Azure encrypts and compresses data that you back up to backup repositories.

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 the types of the virtual disks, see Microsoft Docs.
Snapshot Chain

During every backup session, Veeam Backup for Microsoft Azure creates a cloud-native snapshot for each Azure VM added to the backup policy. The cloud-native snapshot itself is a collection of point-in-time snapshots 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 VM data and saves it in the Azure region where the processed Azure VM resides. This snapshot becomes a starting point of 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.

Cloud-native snapshots act as independent restore points for a backed-up Azure VM. 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.

Each cloud-native snapshot in a snapshot chain contains metadata. Metadata includes information about the processed Azure VM, 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 and apply retention policy, load the configuration of a source Azure VM during recovery operations and so on.

**NOTE**

You can define the number of cloud-native snapshots that must be retained in a snapshot chain in section [Creating Backup Policies](#) (step 6).
Backup Chain

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

The backup chain includes backup files of the following types:

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

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 file in a backup repository. The full backup file becomes a starting point of 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 an incremental backup file in a backup repository. The content of each incremental backup file depends on the content of the full backup file and the preceding incremental backup files in the backup chain.

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

If some file 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 backup files from the backup repository manually. Instead, you must specify retention policy settings that will let you maintain the necessary number of backup files in the backup repository. For more information, see Creating Backup Policies (step 6).
Changed Block Tracking

The changed block tracking (CBT) mechanism allows Veeam Backup for Microsoft Azure to perform quick and cost-efficient image-level backup to backup repositories.

Veeam Backup for Microsoft Azure uses the CBT mechanism to reduce the amount of data read from processed virtual disks:

- During a full backup session, Veeam Backup for Microsoft Azure reads only written data blocks, 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.

![Full backup and incremental backup diagram]

When the first backup session (full backup session) is performed, Veeam Backup for Microsoft Azure creates a cloud-native snapshot of an Azure VM. Veeam Backup for Microsoft Azure sends API requests to access the content of the snapshot and detects unallocated data blocks.

When the next incremental backup session is performed, a new cloud-native snapshot is created. Veeam Backup for Microsoft Azure sends API requests to access and compare the content of two cloud-native snapshots (a snapshot created during the previous backup session and a snapshot created during the current backup session). Snapshot comparison 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.
Retention Policy

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

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.
  
  Restore points in the backup chain can be stored in the configuration database only for the allowed period of time. If a restore point is older than the specified time limit, Veeam Backup for Microsoft Azure removes it from the backup chain. For more information, see Retention Policy for 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.

![Retention Policy for Snapshots Diagram]

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 section Removing Snapshots Created Manually.
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 transforms the backup chain in the following way:
   a. Veeam Backup for Microsoft Azure rebuilds the full backup file to include there data of the incremental backup file that follows the full backup file. To do that, Veeam Backup for Microsoft Azure injects into the full backup file data blocks from the earliest incremental backup file 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 file from the chain as redundant — this data has already been injected into the full backup file.

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 file, 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.
Creating Backup Policies

To produce 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 backups must be stored, when the backup process must start 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 create a backup policy, do the following:

1. Launch the Add 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 settings 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 Policy Wizard

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

1. Navigate to **Policies**.
2. Click **Add**.

---

Step 2. Specify Backup Policy Name

At the **Name** 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 may vary depending on the Azure resource type. The following characters are not supported: * : / \ ? " < > | .

---

![Add Policy Wizard](image-url)
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 **Azure Account** section of the **Sources** step of the wizard, choose an Azure Active Directory that manages resources that you want to protect.

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).

![Veeam Backup for Microsoft Azure](image-url)
Step 3b. Select Regions

In the **Specify Regions** 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**.

![Choose Regions Window](image-url)
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.
3. **If you selected Protect the following resources**:
   a. **From the Resource type drop-window**, select the necessary type of resources:
      - **Subscriptions** — to back up Azure VMs that belong to specific subscriptions.
      - **Resource Groups** — to back up Azure VMs that belong to specific resource groups.
      - **Tags** — to back up Azure VMs that have specific tags assigned.
      - **Virtual Machines** — to back up only specific Azure VMs.
   b. **From the Name or ID drop-down window**, select the necessary item and click **Protect**.
      Alternatively, you can click **Browse to select specific source from the global list**, select check boxes next to the necessary VM instances or labels in the list of available resources, and then click **Protect**.

3. **To save changes made to the backup policy settings**, click **Apply**.
Step 4. Specify Guest Processing Settings

If you back up Azure VMs that are currently running, at the Guest Processing step of the wizard, you can configure guest processing settings. These settings allow you to specify what actions Veeam Backup for Microsoft Azure will perform when communicating with the instance guest OS to create transactionally consistent backups.

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.** For an Azure VM running applications that do not support Microsoft VSS, you can instruct Veeam Backup for Microsoft Azure to run custom scripts on the instance before and after the backup operation. For example, Veeam Backup for Microsoft Azure can execute a pre-snapshot script on the instance 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 instance volumes. After the snapshot is created, a post-snapshot script can start the applications again.

  - **Pre-snapshot script** quiesces the file system and application data on the Azure VM guest OS. It brings the VM to a consistent state before Veeam Backup for Microsoft Azure triggers an Azure VM snapshot.
  
  - **Post-snapshot script** brings an Azure VM and applications to their initial state after the snapshot is created.

Guest scripting option doesn’t require the enabled Microsoft VSS. It can be applied both to the Windows-based and Linux-based Azure VMs.
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.

Enabling Guest Scripting

To specify pre-snapshot and post-snapshot scripts that must be executed for Azure VMs:

- 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 Windows instances toggle to On. The Specify scripting settings for Microsoft Windows instances window will open.

IMPORTANT

Supported script formats:

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

At the **Targets** step of the wizard, you can enable the following additional data protection scenarios:

- In the **Snapshot** section, you can assign labels 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 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. Click **Apply**.

- 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 must 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 archive restore points for longer periods of time. 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 must create cloud-native snapshots and image-level backups.

   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 must 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. Use the **Run at** drop-down list to choose whether you want the backup policy to run everyday, on working days (Monday through Friday) or on selected days.
4. 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 must be stored.

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 week days when the backup policy must create cloud-native snapshots and image-level backups.
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.

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, 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 must be stored.

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 must create cloud-native snapshots and image-level backups.

**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. 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, 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 must be stored.

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 must 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 must be stored.
5. To save changes made to the backup policy settings, click Apply.
Enabling Backup Archiving

You can archive restore points created according to the daily, weekly or monthly schedule for longer periods of time:

- Cloud-native snapshots can be archived for weeks and months.
- Image-level backups can be archived for weeks, months and years.

To archive restore points, you must create at least 2 different schedules: one schedule will control the regular creation of restore points, while another schedule will control the backup archiving process. In terms of backup archiving, Veeam Backup for Microsoft Azure treats schedules of different types as tiers with the ascending priority: daily, weekly, monthly, yearly. When you configure multiple schedules, Veeam Backup for Microsoft Azure first creates restore points according to the lower-tire schedule, and then archives one of the created restore points according to higher-tier schedules.

In the backup archiving scenario, 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 archived backups. Once a flag of a higher-tier schedule is assigned to a restore point, this restore point can no longer be removed — it remains archived 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 lower-tier 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 to archive one of the created snapshots for 2 weeks. In this case, you must create 2 schedules when configuring the backup policy settings — daily and weekly:

1. In the daily scheduling settings, you must select hours and days when snapshots must be created (for example, 7:00 AM, 9:00 AM, and 11:00 AM; Work Days), and specify a number of daily restore points to retain (for example, 3).

Veeam Backup for Microsoft Azure will propagate these settings to the schedule of a higher tier (which is the weekly schedule in our example).
2. In the weekly scheduling settings, you must specify which one of the snapshots created by the daily schedule must be archived, and choose for how long you want to archive the selected snapshot.

For example, if you want to archive the daily restore point created at 7:00 AM on Monday for 2 weeks, you must 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 treat this restore point as archived and will add the (W) flag to it.

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.

By 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 higher-tier schedule. Instead, Veeam Backup for Microsoft Azure will unassign the (D) flag from the restore point. This restore point will be archived 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 higher-tier 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 archived restore points will exceed the retention limit. Veeam Backup for Microsoft Azure will unassign the (W) flag from the earliest archived restore point. Since no other flags are assigned to this restore point, Veeam Backup for Microsoft Azure will remove this restore point from the snapshot chain.
Step 7. Review Cost Estimations

[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 resources that will be consumed to protect the Azure VMs added to the backup policy. The total estimated cost includes the following:

- **Snapshot** — 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 machine type, the number of virtual disks attached, the number of restore points to be kept in the snapshot chain, and the configured scheduling settings.

- **Backup** — 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 machine type, the number of virtual disks attached, the number of restore points to be kept in the backup chain, and the configured scheduling settings.

- **Traffic** — the cost of transferring Azure VM data between Azure regions during data protection operations (for example, if protected Azure VM and 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.

- **Transaction** — 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, configure the scheduling settings to run the backup policy less frequently.
## Cost Estimation

Cost calculated based on assumptions and can be used only as an approximation.

Virtual machine mmmml is backed up to a different region. If it was done intentionally, no changes are required. This and another issue may significantly affect cost. More details...

<table>
<thead>
<tr>
<th>Service</th>
<th>Cost (USD)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Snapshots</td>
<td>$3.48</td>
</tr>
<tr>
<td>Backups</td>
<td>$2.58</td>
</tr>
<tr>
<td>Traffics</td>
<td>$1.07</td>
</tr>
<tr>
<td>Transactions</td>
<td>$0.15</td>
</tr>
</tbody>
</table>

**Estimated monthly cost:** $7.38

<table>
<thead>
<tr>
<th>Virtual Machine</th>
<th>Snapshot</th>
<th>Backup</th>
<th>Traffic</th>
<th>Transaction</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>mmmml</td>
<td>$2.48</td>
<td>$2.68</td>
<td>$1.07</td>
<td>$0.15</td>
<td>$7.38</td>
</tr>
</tbody>
</table>
Step 8. Specify Retry and Email Notification Settings

At the Settings step of the wizard, you can specify automatic retry and 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. Specify the maximum number of attempts to run the backup policy. The time interval between retries is 60 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.

Notification Settings

You can define whether Veeam Backup for Microsoft Azure must send email notifications on backup policy results.

1. In the Notifications section, set the Enabled toggle On.

IMPORTANT

To enable the email notifications, you must configure email notification settings beforehand as described in section Configuring Notification Settings.

2. In the Email address field, specify a recipient email address. Use a semicolon to separate multiple addresses.

NOTE

If you specify the same email recipient in both backup policy notification and global notification settings, Veeam Backup for Microsoft Azure will send each notification twice to this recipient.
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 9. Finish Working with Wizard**

At the **Summary** step of the wizard, review summary information and click **Finish**.
Editing Backup Policy Settings

For each backup policy, you can modify settings specified while creating the policy:

1. Navigate to Policies.

2. Select the check box next to the necessary backup policy and click Edit.

3. Complete the Edit Policy wizard:

   a. To provide a new name and description for the policy, follow the instructions provided in section Creating Backup Policies (step 2).

   b. To choose another Azure Active Directory, to modify the list of regions where Azure VMs that you plan to back up reside, or to add Azure resources to the backup policy, follow the instructions provided in section Creating Backup Policies (step 3a, step 3b or step 3c).

   c. To modify guest processing options, follow the instructions provided in section Creating Backup Policies (step 4a or step 4b).

   d. To assign labels to cloud-native snapshots, or to instruct Veeam Backup for Microsoft Azure to create image-level backups, follow the instructions provided in section Creating Backup Policies (step 5).

   e. To modify the schedule configured for the policy, follow the instructions provided in section Creating Backup Policies (step 6).

   f. To configure automatic retry and notification settings, follow the instructions provided in section Creating Backup Policies (step 7).

   d. At the Summary step of the wizard, review configuration information and click Finish.
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. Click **Policy Priority**.
3. In the **Priority Order** window:
   a. Select a backup policy in the list of existing policies.
   b. To move the policy up or down the list, use the **Up** and **Down** arrows.
   c. To save changes made to the priority order, click **Apply**.

**NOTE**

If an Azure VM is included into multiple backup policies, it will be processed only by the backup policy that has the highest priority.
Disabling and Enabling Backup Policies

By default, Veeam Backup for Microsoft Azure runs all created backup policies according to the specified schedule. 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. Select the check box next to the necessary backup policy, and click **Enable** or **Disable**.
Starting and Stopping Backup Policies

You can start a backup policy manually, for example, if you want to create an additional restore point in the snapshot or backup chain and do not want to change the backup policy schedule. You can also stop a backup policy if processing of an Azure VM 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. Select the check box next to the necessary backup policy, and click Start or Stop.
Creating Snapshots Manually

Veeam Backup for Microsoft Azure allows you to manually create snapshots of Azure VMs that are added to your backup policies. Each snapshot is saved to the same Azure region where the protected Azure VM reside.

**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 Removing Snapshots Created Manually.

To manually create a cloud-native snapshot of an Azure VM, do the following:

1. Navigate to **Instances**.
2. Select the check box next to the necessary Azure VM.
   
   For an Azure VM to be displayed in the list, it must reside in any region included in a backup policy as described in section Creating Backup Policies (step 3c).
3. Click **Take Snapshot Now** and complete the 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 sections Adding Azure Service Account and Adding Repository Accounts.
   
   b. Click **Tags from source volumes will not be copied and custom tags will not be applied** to assign labels 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. Click **Apply**.
   
   d. At the **Summary** step of the wizard, select check box next to the **Go to sessions log after finish** option to track the progress of snapshot creation.
   
   e. Review the configuration information and click **Finish**.

---

![Image of Take Manual Snapshot wizard](image-url)
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 separate backup files from Microsoft Azure storage accounts manually. If some files in the backup chain are missing, you will not be able to roll back to the necessary state.

To remove snapshots and backups created by a backup policy, do the following:

1. Navigate to Protected Data.
2. Select check boxes next to the necessary Azure VMs.
3. Click Remove and choose whether you want to remove snapshots, backups or both.
Removing 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**.
Performing Restore

Veeam Backup for Microsoft Azure allows you to perform the following restore operations:

- **VM Restore** — restores an entire Azure VM from a cloud-native snapshot or image-level backup.
- **Disk Restore** — restores virtual disks attached to an Azure VM.
- **File-Level Recovery** — recovers 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 VM Restore

In case a disaster strikes, Veeam Backup for Microsoft Azure allows you to restore an entire Azure VM from a cloud-native snapshot or image-level backup. You can restore one or more Azure VMs at once, 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 Microsoft Azure capabilities. To restore an Azure VM from an image-level backup, Veeam Backup for Microsoft Azure performs the following steps:

1. Launches a worker instance in the Azure region where the restored Azure VM will reside.
2. 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.
3. Restores backed-up data to the empty virtual disks on the worker instance.
4. Detaches the virtual disks with the restored data from the worker instance.
5. Removes the worker instance from the Microsoft Azure environment.
6. Creates an Azure VM in the specified location.
7. Attaches the virtual disks with the restored data to the Azure VM.
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. Choose a restore mode.
4. Select a subscription.
5. Specify Azure VM settings.
7. Select a virtual network.
8. Specify a restore reason.

Step 1. Launch Restore Virtual Machines Wizard

To launch the Restore Virtual Machines wizard, do the following:

1. Navigate to Protected Data.
2. Select the check box next to the necessary Azure VMs.

   For an Azure VM to be displayed in the list, it must be added to the backup policy as described in section Creating Backup Policies (step 3c).

3. Click Restore > VM Restore.

   You can also click the link associated with the Azure VM that you want to restore in the Restore Points column. Then, in the Available Restore Points window, select a restore point to which to restore data and click Restore > VM Restore.
Step 2. Select Restore Point

At the **Instances** step of the wizard, you can add multiple Azure VMs and select a restore point for each Azure VM that you want to restore. By default, Veeam Backup for Microsoft Azure uses the latest valid restore point.

To select a restore point for an Azure VM, do the following:

1. Select an Azure VM from the list and click **Restore Point**.
2. In the **Select Restore Point** window, select the necessary restore point and click **Select**.

   In the **Backup Destination** column, you can see the restore point type:
   - **Backup Repository** — perform a restore from an image-level backup. If you select this option, Veeam Backup for Microsoft Azure will launch a worker instance.
   - **Snapshot** — perform a restore from a snapshot that resides in the associated Azure resource group.

For more information on how Veeam Backup for Microsoft Azure creates backups and snapshots, see How Backup Works and Backup Chain.

<table>
<thead>
<tr>
<th>Instance</th>
<th>Size</th>
<th>Restore Point</th>
</tr>
</thead>
<tbody>
<tr>
<td>alesch-rg1-vm</td>
<td>65.0 GB</td>
<td>02/03/2021 8:07 PM</td>
</tr>
<tr>
<td>veeam-proxy-appliance-azure-1yis</td>
<td>150.0 MB</td>
<td>02/09/2021 11:00 AM</td>
</tr>
<tr>
<td>alesch-win10-unmngd</td>
<td>127.0 GB</td>
<td>02/03/2021 8:05 PM</td>
</tr>
</tbody>
</table>
Step 3. Choose Restore Mode

At the **Restore Mode** step of the wizard, choose whether you want to restore the selected Azure VMs to the original or to a custom location.

- **Restore to the original location**
  
  Quickly initiate the restore of selected virtual machines to their original location, with the original name and settings.

- **Restore to a new location, or with different settings**

  Customize the restored virtual machine location and change its settings. The wizard will automatically populate all controls with the original virtual machine settings as the defaults.
Step 4. Select Subscription

[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 Subscription step of the wizard, select a Microsoft Azure subscription and location to which you want to restore Azure VMs.

1. From the Subscription drop-down list, select the necessary subscription.
   For a subscription to be displayed in the Subscription list, it must be created and associated to the account as described in Microsoft Docs.

2. From the Location drop-down list, select the necessary region.
   Data transfer to a new location may require additional costs and may take more time to complete.

### Specify subscription and location

- **Subscription:** Visual Studio Premium with MSDN
- **Location:** West Europe

Choose the Microsoft Azure data center region where the disks should be restored.
Step 5. 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 Instance step of the wizard, configure properties of each Azure VM that you want to restore.

1. Select the check box next to the necessary Azure VM and click Properties.

2. In the Virtual Machine Properties window, do the following:
   a. From the Virtual machine size drop-down list, choose a size for the restored Azure VM. For more information on VM sizes, see Microsoft Docs.
   b. From the Resource group drop-down list, select a resource group in which the restored Azure VM must belong.
      For a resource group to be displayed in the Resource group list, it must be created as described in Microsoft Docs.
   c. From the Disk type drop-down list, select the type of virtual disks that will be attached to the restored Azure VM. For more information on disk types, see Microsoft Docs.
   d. In the Availability type section, 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.
   f. Click Apply.

IMPORTANT

If the size of the original VM differs from the size of the restored VM, Microsoft Azure may apply additional charges for maintaining the restored VM.
Step 6. 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 **Rename Disk** window, enter a name that you want to use for the selected virtual disk and click **Apply**.

![Screenshot of the Rename Disk window in the Veeam Backup for Microsoft Azure user guide.](image-url)
Step 7. Specify 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, you can change network settings of the selected Azure VMs.

1. Select the check boxes next to the necessary Azure VMs and click Properties.
2. In the Network Properties window, do the following:
   a. From the Select virtual network drop-down list, select a virtual network to which you want to connect the restored Azure VMs.
      For a virtual network to be displayed in the Select virtual network list, it must be created as described in Microsoft Docs.
   b. From the Select subnet drop-down list, select a subnet within the specified virtual network to which you want to connect the restored Azure VMs.
      For a subnet to be displayed in the Select subnet list, it must be created as described in Microsoft Docs.
   c. From the Select 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.
      For a network security group to be displayed in the Select network security group list, it must be created and associated to the necessary subnet as described in Microsoft Docs.
   d. Click Apply.
Step 8. Specify Restore Reason

At the **Reason** step of the wizard, specify a reason for restoring the Azure VMs. This information will be saved to the session history and you will be able to reference it later.

![Reason step of the wizard](image)

Type in the reason for performing this restore operation

- **Reason:**
  - Disaster recovery reason

[Next] [Previous] [Cancel]
Step 9. Finish Working with Wizard

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

![Restore Virtual Machines](image)

Click finish to restore

**Restore summary:**

- **Reason:** Disaster recovery reason

**alesch-rg1-vm**

- **Restore point:** 02/03/2021 8:07 PM
- **Subscription:** Visual Studio Premium with MSDN
- **Location:** West Europe
- **Resource group:** alesch-westeu
- **Virtual machine name:** alesch-rg1-vm
- **Disk type:** Managed
- **Virtual machine size:** Standard_F4s
- **Virtual network:** alesch-westeu
- **Subnet:** default
- **OS disk:** alesch-rg1-vm_disk1_2f63e8b80a2a43e89661e8f062929
- **Data disk 0:** alesch-rg1-vm-d2
- **Data disk 1:** alesch-rg1-vm-d0
- **Data disk 2:** alesch-rg1-vm-d11
- **Data disk 3:** alesch-rg1-vm-d3
- **Data disk 4:** alesch-rg1-vm-d8
- **Data disk 5:** alesch-rg1-vm-d15
Performing Disk Restore

In case a disaster strikes, Veeam Backup for Microsoft Azure allows you to restore corrupted virtual disks of Azure VMs from a cloud-native snapshots or image-level backups. You can 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 Microsoft Azure capabilities. To restore virtual disks from an image-level backup, Veeam Backup for Microsoft Azure performs the following steps:

1. Launches a worker instance in the Azure region where the restored virtual disks will reside.
2. 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.
3. Restores backed-up data to the empty virtual disks on the worker instance.
4. Detaches the virtual disks with the restored data from the worker instance.
5. Removes the worker instance from the Microsoft Azure environment.

**NOTE**

Veeam Backup for Microsoft Azure does not attach the restored persistent disks to any Azure VM instance – the disks are placed to the specified location as standalone virtual disks.

How to Perform Disk Restore

To restore virtual disks of Azure VMs, do the following:

1. **Launch the Disk Restore wizard.**
2. **Select a restore point.**
3. **Choose a restore mode.**
4. **Select a subscription.**
5. **Specify disk settings.**
6. **Specify a restore reason.**
7. **Review summary information.**
Step 1. Launch Disk Restore Wizard

To launch the **Restore Disks** wizard, do the following:

1. **Navigate to Protected Data.**
2. **Select the check box next to the necessary Azure VM.**
   
   For an Azure VM to be displayed in the list, it must be added to the backup policy as described in section **Creating Backup Policies** (step 3c).

3. **Click **Restore > Disk Restore.**

   You can also click the link associated with the Azure VM that you want to restore in the **Restore Points** column. Then, in the **Available 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, you can select a restore point for the Azure VM that you want to restore and specify virtual disks that you want to exclude from the restore operation. By default, Veeam Backup for Microsoft Azure uses the latest valid restore point.

To select a restore point for the Azure VM, do the following:

1. Select the necessary Azure VM from the list and click **Change Restore Point**.
2. In the **Select Restore Point** window, select the necessary restore point and click **Select**.

In the **Backup Destination** column, you can see the restore point type:

- **Backup Repository** — perform a restore from an image-level backup. If you select this option, Veeam Backup for Microsoft Azure will launch a worker instance.
- **Snapshot** — perform a restore from a snapshot that resides in the associated Azure resource group.

For more information on how Veeam Backup for Microsoft Azure creates backups and snapshots, see **How Backup Works** and **Backup Chain**.
Step 3. Choose Restore Mode

At the **Restore Mode** step of the wizard, choose whether you want to restore virtual disks of the selected Azure VM to the original or to a custom location.

<table>
<thead>
<tr>
<th>Restore Disks</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Restore Point</strong></td>
</tr>
<tr>
<td><strong>Restore Mode</strong></td>
</tr>
</tbody>
</table>

### Restore mode

- **Restore to the original location**
  
  Quickly initiate the restore of selected disks to its original location, with the original name and settings. This option minimizes the chance of user input error.

- **Restore to a new location, or with different settings**
  
  Customize the restored disks location, and change its settings. The wizard will automatically populate all controls with the original disks settings as the defaults.

### Table: Restore Disks

<table>
<thead>
<tr>
<th>Restore Point</th>
<th>Restore Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

[Previous] [Next] [Cancel]
Step 4. Select Subscription

[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 Subscription step of the wizard, select a Microsoft Azure subscription and location to which you want to restore virtual disks of the selected Azure VM.

1. From the Subscription drop-down list, select a subscription to which you want to perform a restore.
   For a subscription to be displayed in the Subscription list, it must be created and associated to the account as described in Microsoft Docs.

2. From the Location drop-down list, select a region to which you want to restore data.
   Data transfer to a new location may require additional costs and may take more time to complete.
Step 5. Specify Disk Settings

[This step applies only if you chose to perform a restore to a new location or with different settings at the Restore Mode step of the wizard.]

At the Disks step of the wizard, change disk properties of the selected Azure VM.

1. Select the necessary virtual disk from the list and click Edit.
2. In the Disk Properties window, do the following:
   a. In the Disk name field, enter a name that you want to use for restored virtual disks.
   b. From the Resource group drop-down list, select a resource group where the restored virtual disks must belong.
      For a resource group to be displayed in the Resource group list, it must be created as described in Microsoft Docs.
   c. From the Disk type drop-down list, select a type of virtual disks that you plan to restore. For more information on disk types, see Microsoft Docs.
      You cannot convert managed virtual disks into unmanaged, but you can convert unmanaged virtual disks into managed.
   d. [Applies only for the managed disk type] From the Availability Zone drop-down list, select an Availability Zone to which you want to place the disk.
   e. [Applies only for the unmanaged disk type] 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.
   f. Click Apply.
Step 6. 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.

<table>
<thead>
<tr>
<th>Reason</th>
<th>Type in the reason for performing this restore operation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Restore reason:</td>
</tr>
<tr>
<td></td>
<td>Disaster recovery reason</td>
</tr>
</tbody>
</table>

![Image of the Reason step of the wizard](image)
### Step 7. Finish Working with Wizard

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

<table>
<thead>
<tr>
<th>Restore Disks</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Reason</strong></td>
<td>Disaster recovery reason</td>
</tr>
<tr>
<td><strong>Restore point</strong></td>
<td>02/03/2021 10:07 AM</td>
</tr>
<tr>
<td><strong>Summary</strong></td>
<td></td>
</tr>
<tr>
<td><strong>alesh-rg1-vm-d2</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Subscription</strong></td>
<td>Visual Studio Premium with MSDN</td>
</tr>
<tr>
<td><strong>Region</strong></td>
<td>West Europe</td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>alesch-rg1-vm-d2</td>
</tr>
<tr>
<td><strong>Resource group</strong></td>
<td>alesch-westeu</td>
</tr>
<tr>
<td><strong>Disk type</strong></td>
<td>Managed</td>
</tr>
<tr>
<td><strong>alesh-rg1-vm-d0</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Subscription</strong></td>
<td>Visual Studio Premium with MSDN</td>
</tr>
<tr>
<td><strong>Region</strong></td>
<td>West Europe</td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>alesch-rg1-vm-d0</td>
</tr>
<tr>
<td><strong>Resource group</strong></td>
<td>alesch-westeu</td>
</tr>
</tbody>
</table>

Click **finish to restore**.
Performing File-Level Recovery

In case a disaster strikes, you can recover corrupted or missing files of an Azure VM from a cloud-native snapshot or image-level backup.

IMPORTANT
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 restore only for Microsoft Windows basic volumes and dynamic simple volumes with disabled data deduplication.

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 restore files and folders from a cloud-native snapshot, the worker instance is launched in the region where the source Azure VM resides.
   - To restore files and folders from an image-level backup, the worker instance is launched in the region where the target storage bucket 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 Recovery for Veeam Backup browser.
   - The File Level Recovery for Veeam Backup browser displays the file system tree of the backed-up Azure VM. In the browser, you select the necessary files and folders to restore.
4. Saves the selected files and folders to the local machine.
5. Detaches the virtual disks from the worker instance.
6. Removes the worker instance from the Microsoft Azure environment.

How to Perform File-Level Recovery

To perform a file-level recovery, do the following:

1. Launch the File-Level Recovery wizard.
2. Select a restore point.
3. Specify a restore reason.
4. Start a restore session.
5. Download the restored files and folders.
Step 1. Launch File-Level Recovery Wizard

To launch the File-Level Recovery wizard, do the following:

1. Navigate to Protected Data.
2. Select the check box next to the necessary Azure VM.
   
   For an Azure VM to be displayed in the list, it must be added to the backup policy as described in section Creating Backup Policies (step 3c).

3. Click File-level recovery.

   You can also click the link associated with the Azure VM that you want to restore in the Restore Points column. Then, in the Available Restore Points window, select the necessary restore point and click File-Level recovery.
Step 2. Select Restore Point

At the Virtual Machine step of the wizard, you can 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 latest valid restore point.

To select a restore point, do the following:

1. Select the necessary Azure VM from the list and click Change Restore Point.

2. In the Select Restore Point window, select the necessary restore point and click Select.

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:
  - **Backup Repository** — perform a restore from an image-level backup. If you select this option, Veeam Backup for Microsoft Azure will launch a worker instance.
  - **Snapshot** — perform a restore from a snapshot that resides in the associated Azure resource group.

For more information on how Veeam Backup for Microsoft Azure creates backups and snapshots, see How Backup Works and Backup Chain.
Step 3. Specify Restore 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.

![Reason step of the wizard](image)
Step 4. 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 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 FLR link in the File-level recovery column.

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 Recovery for Veeam Backup browser. You can use the link in either of the following ways:

- Click the link to open the File Level Recovery for Veeam Backup browser on your local machine while the recovery session is running.
- Copy the link, close the File-Level Recovery window and open the File Level Recovery for Veeam Backup browser on another machine.

**IMPORTANT**

When you click **Copy URL**, Veeam Backup for Microsoft Azure copies the following information to the clipboard:

- A link to the File Level Recovery for Veeam Backup 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 Recovery for Veeam Backup browser.

To avoid a man-in-the-middle attack, before you start recovering files and folders, check that the certificate thumbprint displayed in the web browser from which you access the File Level Recovery for Veeam Backup browser matches the provided certificate thumbprint.
Step 5. Download Restored Files and Folders

In the File Level Recovery for Veeam Backup browser, you can find and restore files and folders of the backed-up Azure VMs. Restored items are saved in a .zip archive to the default download directory on a machine from where the File Level Recovery for Veeam Backup browser is launched.

1. Navigate to the folder that contains the necessary files.
2. In the working area, select check boxes next to the items and click Download.

If you want to download items from multiple folders and restore these items all at once, do the following:

1. Navigate to the folder that contains the necessary files.
2. In the working area, select check boxes next to the items and click Add to Recovery List link.
3. Click Pending Recovery link.
4. In the Recovery List window, review the list of items and click Download.
Step 6. Stop Recovery Session

After you finish working with the File Level Recovery for Veeam Backup 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 Azure VM from the worker instance and remove the worker instance.

To stop the recovery session, click Stop in the File-level Recovery window. If you do not perform any actions in the File Level Recovery for Veeam Backup 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.

### File-level Recovery - elesch-BasicA1

<table>
<thead>
<tr>
<th>Date</th>
<th>URL</th>
<th>Certificate Thumbprint</th>
</tr>
</thead>
<tbody>
<tr>
<td>02/11/2021 10:15...</td>
<td><a href="https://iba-060daefd-a7d7-4811-4d0f">https://iba-060daefd-a7d7-4811-4d0f</a></td>
<td>3B55B290C087A0586957112BC424349D259CEA</td>
</tr>
</tbody>
</table>
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 Sessions 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 VMs 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 must 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 page 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 page.
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 available updates manually if required:

1. Switch to the **Configuration** page.
2. Navigate to **Support Information** > **Updates**.
3. 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 Backup for Microsoft Azure 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 now
- Schedule update installation

You can also set a reminder to send update notifications.

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 Backup for Microsoft Azure Updater page:
   a. Switch to the Configuration page.
   b. Navigate to Support Information.
   c. On the Updates tab, click Check and view updates.

2. On the Veeam Backup for Microsoft Azure 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.
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 Backup for Microsoft Azure 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 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 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 Backup for Microsoft Azure 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.
Viewing Updates 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 > Updates.
3. Click Check and view updates.
4. On the Veeam Backup for Microsoft Azure page, switch to the History tab.

For each date when an update was installed, the Veeam Backup for Microsoft Azure 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. At the top right corner of the Veeam Backup for Microsoft Azure window, click Configuration.
2. Navigate to Support Information.

The About section of the Updates page will display the following information:

- Server Version — the currently installed version of Veeam Backup for Microsoft Azure.
- Worker Version — version of the worker instance.
- 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.
Downloading Logs

To download the product logs, do the following:

1. Switch to Configuration.
2. Navigate to Support Information.
3. Switch to the Download Logs page and click Download Logs.
4. In the Download Logs window, specify a time interval for which the logs must 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 OK, the logs will be saved locally in the default download folder as a single LOG.ZIP archive.