Contents

CONTACTING VEEAM SOFTWARE ................................................................. 6
ABOUT THIS DOCUMENT ............................................................................. 7
OVERVIEW ...................................................................................................... 8
BACKUP INFRASTRUCTURE COMPONENTS .............................................. 9
PLANNING AND PREPARATION .................................................................. 11
    System Requirements .......................................................................... 12
    Used Ports ......................................................................................... 13
    Required Permissions ......................................................................... 14
    Licensing ............................................................................................ 16
        License Limitations ....................................................................... 17
        Licensing Scenarios ...................................................................... 18
        Managing Licensed Workloads ..................................................... 20
DEPLOYMENT AND CONFIGURATION ...................................................... 23
    Installing Plug-In .............................................................................. 25
    Upgrading Plug-In ............................................................................ 26
    Adding Veeam Backup for Microsoft Azure Appliances .................... 27
        Connecting to Existing Veeam Backup for Microsoft Azure Appliances ...... 28
        Deploying New Veeam Backup for Microsoft Azure Appliances .......... 41
    Managing Veeam Backup for Microsoft Azure Appliances ................. 52
        Viewing Snapshots and Backups ................................................... 53
        Editing Appliance Settings .......................................................... 54
        Opening Appliance Web UI Component ....................................... 55
        Upgrading Appliances ................................................................... 56
        Rescanning Appliances .................................................................. 57
        Removing Appliances ..................................................................... 58
    Adding Blob Storage Backup Repositories ....................................... 60
        Deploying Standard Backup Repositories ..................................... 62
        Deploying Archive Repositories ................................................ 71
    Managing Backup Repositories ......................................................... 80
    Performing Configuration Backup and Restore .................................. 81
        Configuration Backup .................................................................... 82
        Configuration Restore ................................................................... 84
    Uninstalling Plug-In ......................................................................... 94
    Installing and Uninstalling Plug-In in Unattended Mode .................... 95
DATA PROTECTION ..................................................................................... 97
    Creating Backup Policies ................................................................. 98
Managing Backup Policies ........................................................................................................... 99
  Starting and Stopping Policies ................................................................................................. 100
  Editing Policy Settings ............................................................................................................. 102
  Disabling and Removing Policies ............................................................................................. 103
Managing Backed-Up Data ......................................................................................................... 105
Creating Backup Copy Jobs ....................................................................................................... 109
Copying Backups to Tapes ........................................................................................................ 110
Viewing Statistics ...................................................................................................................... 111
DATA RECOVERY ........................................................................................................................ 112
  Restoring to Microsoft Azure .................................................................................................. 113
    Step 1. Launch Restore to Microsoft Azure Wizard ................................................................. 114
    Step 2. Select Azure VMs and Restore Points ....................................................................... 115
    Step 3. Choose Restore Mode ............................................................................................... 116
    Step 4. Specify Azure Subscription and Region ................................................................... 117
    Step 5. Specify VM Names and Resource Groups ................................................................. 118
    Step 6. Configure VM Availability Options .......................................................................... 119
    Step 7. Specify VM Sizes .................................................................................................... 121
    Step 8. Specify Network and Secure Group Settings ............................................................. 122
    Step 9. Specify Restore Reason ............................................................................................ 123
    Step 10. Finish Working with Wizard .................................................................................. 124
  Restoring to Microsoft Azure SQL .......................................................................................... 125
    Step 1. Launch Restore to Microsoft Azure SQL Wizard ....................................................... 126
    Step 2. Select SQL Databases and Restore Points ................................................................. 127
    Step 3. Choose Restore Mode and Service Account ............................................................... 128
    Step 4. Specify Target SQL Server Settings ....................................................................... 129
    Step 5. Specify Name ............................................................................................................ 130
    Step 6. Specify Restore Reason ............................................................................................ 131
    Step 7. Finish Working with Wizard ................................................................................... 132
  Restoring Microsoft Azure File Shares .................................................................................. 133
  Performing Instant Recovery .................................................................................................. 134
  Restoring to Amazon EC2 ....................................................................................................... 136
  Restoring to Nutanix AHV ....................................................................................................... 137
  Restore to Google Compute Engine ....................................................................................... 138
  Exporting Disks ....................................................................................................................... 139
  Restoring Guest OS Files ........................................................................................................ 140
  Restoring Application Items .................................................................................................... 142
  Viewing Statistics ..................................................................................................................... 144
FEATURES AND PLUG-IN VERSIONS ........................................................................................... 146
SUPPORT INFORMATION ............................................................................................................ 147
Contacting Veeam Software

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

Customer Support

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

Company Contacts

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

Online Support

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

- Full documentation set: [veeam.com/documentation-guides-datasheets.html](veeam.com/documentation-guides-datasheets.html)
- Veeam R&D Forums: [forums.veeam.com](forums.veeam.com)
About This Document

This guide provides information on integration of Veeam Backup & Replication and Veeam Backup for Microsoft Azure. The document describes how to install Microsoft Azure Plug-in for Veeam Backup & Replication, how to add Veeam Backup for Microsoft Azure to the Veeam Backup & Replication infrastructure, and gives instructions on how to monitor Veeam Backup for Microsoft Azure sessions and perform restore of Azure VMs, databases and other resources from the Veeam Backup & Replication console.

Intended Audience

This guide is designed for backup administrators who plan to use the Veeam Backup & Replication console to manage backup and restore operations.

Microsoft Azure Plug-in for Veeam Backup & Replication is built on top of Veeam Backup & Replication, and this guide assumes that you have a good understanding of this solution.
Overview

Microsoft Azure Plug-in for Veeam Backup & Replication is a solution that allows you to create and manage data protection and disaster recovery tasks for Microsoft Azure environments and Azure SQL (Azure SQL databases and Azure SQL managed instances). Microsoft Azure Plug-in for Veeam Backup & Replication extends the Veeam Backup & Replication functionality and provides access to Veeam Backup for Microsoft Azure from the Veeam Backup & Replication console. Also, Microsoft Azure Plug-in for Veeam Backup & Replication makes the Veeam Backup & Replication console a single management center for multiple Veeam Backup for Microsoft Azure appliances.

**NOTE**

Microsoft Azure Plug-in for Veeam Backup & Replication is built on top of Veeam Backup & Replication, and this guide assumes that you have a good understanding of this solution.

With Microsoft Azure Plug-in for Veeam Backup & Replication, you can add Veeam Backup for Microsoft Azure appliances into the Veeam Backup & Replication infrastructure and perform the following operations from the Veeam Backup & Replication console:

- Start and stop backup policies.
- Monitor session statistics.
- View created snapshots and image-level backups.
- Restore entire Azure VMs to Microsoft Azure.
- Restore SQL databases to Microsoft Azure SQL.
- Restore Azure file shares to Microsoft Azure Files.
- Restore entire Azure VMs as EC2 instances to Amazon EC2.
- Restore entire Azure VMs as VM instances to Google Cloud Platform.
- Perform Instant Recovery to restore entire Azure VMs as VMs into VMware vSphere or Hyper-V environment.
- Restore entire Azure VMs as VMs into Nutanix AHV clusters.
- Restore guest OS files and folders of Azure VMs.
- Export Azure VM disks in the VMDK, VHD or VHDX formats.
Backup Infrastructure Components

After you integrate Veeam Backup for Microsoft Azure with Veeam Backup & Replication, the backup infrastructure will consist of the following components:

1. **Veeam Backup & Replication**
   An application where you can manage backup infrastructure components, perform restore from image-level backups and snapshots of Microsoft Azure VMs, SQL databases and other resources, copy backups to secondary repositories and tapes, and perform other operations.

2. **Azure Plug-in for Veeam Backup & Replication**
   An installer component that deploys services required for integration with Veeam Backup for Microsoft Azure.

3. **Veeam Backup for Microsoft Azure appliance**
   The main component that performs backup and restore operations in the Microsoft Azure environment.
   
   In the Veeam Backup & Replication console, you can connect to an existing Veeam Backup for Microsoft Azure appliance or launch the deployment of a new one.

4. **Worker instances**
   Temporary Linux-based Microsoft Azure VMs that are created by Veeam Backup for Microsoft Azure to perform backup and restore operations. A worker instance is deployed for each VM included in the running backup policy or restore process. After the backup or restore process completes, the worker instance is immediately removed.

5. **Blob storage backup repositories**
   Microsoft Azure Plug-in for Veeam Backup & Replication supports two types of Blob storage backup repositories:
   
   a. **Standard backup repositories**
      A folder in a blob container where Veeam Backup for Microsoft Azure stores image-level backups of Azure VMs, SQL databases and other resources. For more information on standard backup repositories, see Adding Backup Repositories.

   b. **Archive repositories**
      A folder in a blob container where Veeam Backup for Microsoft Azure stores archive backups of Azure VMs, SQL databases and other resources. For more information on archive, see Adding Backup Repositories.
6. **Additional repositories and tape devices**

Additional repositories are any backup repositories where Veeam Backup & Replication copies the Azure VM backups if you perform backup copy. For more information on backup repositories, see the Backup repositories section in the Veeam Backup & Replication User Guide. You can also use tape devices to store copies of your backup files. For more information on how to back up to tapes, see the Machines Backup to Tape section in the Veeam Backup & Replication User Guide.

---

**What You Do Next**

*Deploy and Configure Infrastructure*
Planning and Preparation

Before you start using Microsoft Azure Plug-in for Veeam Backup & Replication, make sure that the backup infrastructure components meet system requirements, all required ports are open, and user accounts that you plan to use have the required permissions.
System Requirements

Before you start using Microsoft Azure Plug-in for Veeam Backup & Replication, consider the following requirements.

Veeam Backup for Microsoft Azure

Microsoft Azure Plug-in for Veeam Backup & Replication version 11.0.4.x supports integration with Veeam Backup for Microsoft Azure version 4.x.

Veeam Backup & Replication

Microsoft Azure Plug-in for Veeam Backup & Replication version 11.0.4.x supports integration with Veeam Backup & Replication version 11.0.1.1261 (starting from cumulative patch P20211211).

Hardware and Software Requirements

Since Microsoft Azure Plug-in for Veeam Backup & Replication is installed on a Veeam Backup & Replication server, system requirements for the plug-in are similar to the requirements for the Veeam Backup & Replication server. For more information on system requirements for the Veeam Backup & Replication server and other infrastructure components, see the System Requirements section in the Veeam Backup & Replication User Guide.

For the software that must be installed on the machine where Microsoft Azure Plug-in for Veeam Backup & Replication is installed, see the Veeam Cloud Plug-Ins section in the Veeam Backup & Replication User Guide.

Requirements for Azure Services

The Veeam Backup for Microsoft Azure appliance and worker instances must have outbound internet access to a number of Microsoft Azure services. For the list of services, see the Azure Services section in the Veeam Backup for Microsoft Azure User Guide.

Veeam Backup for Nutanix AHV

Microsoft Azure Plug-in for Veeam Backup & Replication supports restore to Veeam Backup for Nutanix AHV version 2.1 and later.
**Used Ports**

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

**NOTE**

During installation, Veeam Backup & Replication and Veeam Backup for Microsoft Azure automatically create firewall rules for the required ports to allow communication for the application components.

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Protocol</th>
<th>Port</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Veeam Backup &amp; Replication server</td>
<td>Veeam Backup for Microsoft Azure appliance, Azure services</td>
<td>TCP</td>
<td>443</td>
<td>Port used for communication with Azure and Veeam Backup for Microsoft Azure.</td>
</tr>
<tr>
<td></td>
<td>Veeam Backup &amp; Replication server</td>
<td>TCP</td>
<td>6172</td>
<td>Port used by Microsoft Azure Plug-in for Veeam Backup &amp; Replication to connect to a component that enables communication with the Veeam Backup &amp; Replication database.</td>
</tr>
<tr>
<td>Veeam Backup &amp; Replication console and Veeam ONE server</td>
<td>Veeam Backup &amp; Replication server</td>
<td>TCP</td>
<td>20443</td>
<td>Port used to connect to Microsoft Azure Plug-in for Veeam Backup &amp; Replication.</td>
</tr>
</tbody>
</table>

For ports required for Veeam Backup for Microsoft Azure, see the Ports section in the Veeam Backup for Microsoft Azure User Guide.
Required Permissions

Make sure user accounts that you plan to use have permissions described in this section.

Veeam Backup & Replication User Account Permissions

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

If you plan to connect to a tenant using Remote Access Console, you must run the console as administrator.

Azure User Account and Service Account Permissions

To deploy or connect to a Veeam Backup for Microsoft Azure appliance, you specify an Azure user account. The Azure user account must be registered in the Global or Government region. Note that the Government region is supported starting from Microsoft Azure Plug-in for Veeam Backup & Replication version 11.0.2.167. This account must have the following permissions:

- If you add an existing account, check the permissions listed in the Veeam Backup for Microsoft Azure User Guide.
- If you create a new account, Veeam Backup & Replication assigns this account the Owner and Key Vault Crypto User roles. These roles are sufficient to perform further operations.

To perform data protection and disaster recovery operations, Microsoft Azure Plug-in for Veeam Backup & Replication uses an Azure service account.

If you deploy a new Veeam Backup for Microsoft Azure appliance from the Veeam Backup & Replication console, the Default service account is created automatically. This service account is granted all the necessary permissions to perform operations within the Azure user account — to back up any VMs, SQL databases or other resources within the account, to store backups in Blob storage containers, and so on.

If you connect to an existing appliance or upgrade an already added appliance, make sure that the service accounts added to the appliance have the following roles and permissions assigned:

- The Contributor role. For more information on built-in roles, see Microsoft Docs.
- The following custom roles: Veeam Service Account and Veeam Repository Account.
- 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, Application Administrator or Global Administrator role. For more information on role permissions, see Microsoft Docs.
- To be able to use Azure Key Vaults and keys, the service account must have the following permissions:

  - Microsoft.KeyVault/vaults/keys/read,
  - Microsoft.KeyVault/vaults/keys/versions/read,
  - Microsoft.KeyVault/vaults/keys/encrypt/action,
  - Microsoft.KeyVault/vaults/keys/decrypt/action

For more information on how to add service accounts and which permissions are required when adding them, see the Adding Azure Service Account section in the Veeam Backup for Microsoft Azure User Guide.
Azure SQL Account

The Azure SQL account that you plan to use when restoring Microsoft Azure databases must have administrative permissions on Azure SQL servers or Azure SQL Managed Instances to which you restore databases.

AWS User Account Permissions

The AWS user account that you plan to use when restoring Azure VMs to Amazon EC2 must have permissions described in the AWS IAM User Permissions section of the Veeam Backup & Replication User Guide.

Google Cloud IAM Service Account Permissions

The IAM service account that you plan to use to connect to Google Cloud Platform must be granted roles described in the Google Cloud Platform IAM User Permissions section in the Veeam Backup & Replication User Guide.

Permissions for Virtualization Servers and Hosts

If you plan to copy backups to on-premises repositories, to perform restore to VMware vSphere or Microsoft Hyper-V, or to perform other tasks related to virtualization servers or hosts, you must check that the user account specified for these servers and host has the required permissions. These permissions are listed in the Using Virtualization Servers and Hosts section in the User Guide for VMware vSphere and in the Using Virtualization Servers and Hosts section in the User Guide for Microsoft Hyper-V.
Licensing

If you want to use capabilities provided by Microsoft Azure Plug-in for Veeam Backup & Replication, you must have a valid license installed on Veeam Backup & Replication. If you install Veeam Backup & Replication without a license, the Microsoft Azure Plug-in for Veeam Backup & Replication capabilities are not available.

In this section, you will see the terminology of Veeam Backup & Replication licensing and Veeam Backup for Microsoft Azure editions. For more information, see the following guides:

- To learn about licensed objects and license types in Veeam Backup & Replication, see the Licensing section in the Veeam Backup & Replication User Guide.

- To learn about editions of Veeam Backup for Microsoft Azure, see the Licensing section in the Veeam Backup for Microsoft Azure User Guide.
License Limitations

Before installing Microsoft Azure Plug-in for Veeam Backup & Replication, mind the following limitations for Veeam Backup & Replication licenses.

Not Supported Licenses

The functionality of Microsoft Azure Plug-in for Veeam Backup & Replication is NOT supported:

- If Veeam Backup & Replication uses the Veeam Cloud Connect service provider license
- In the Community Edition of Veeam Backup & Replication

Limitations for Veeam Backup & Replication Licensed by Sockets

If you use Veeam Backup & Replication with a Perpetual per/socket license and you want to connect a Veeam Backup for Microsoft Azure appliance to the Veeam Backup & Replication infrastructure, you must install an additional Perpetual per-instance license or a subscription license. When you install an additional license, the new license merges with the existing Perpetual per/socket license. For details on the merging process, see the Merging Licenses section in the Veeam Backup & Replication User Guide.

If you do not install an additional Perpetual per-instance license or a subscription license, you will be able to use one free license instance per each socket (but maximum 6 free instances for all sockets). After you exceed the limit of free instances, Veeam Backup for Microsoft Azure backup policies for workloads without license instances will start to fail.

To obtain an additional license, contact a Veeam sales representative at Sales Inquiry.
Licensing Scenarios

A workload (Azure VM, SQL database and so on) is considered protected if it has a backup or snapshot created by a backup policy in the last 31 days. The number of license instances that a protected workload consumes depends on the workload type and product edition. For details, see Veeam Licensing Policy.

NOTE

Manual creation of snapshots and SQL backups does not require license instances. For more information on how to create snapshots and backups manually, see the Creating VM Snapshots Manually, Creating Azure SQL Backups Manually and Creating File Share Snapshots Manually sections in the Veeam Backup for Microsoft Azure User Guide.

When you add a Veeam Backup for Microsoft Azure appliance to the Veeam Backup & Replication infrastructure, there are two possible license scenarios:

- **Connecting to an existing Veeam Backup for Microsoft Azure appliance**
  
  If you connect to an existing Veeam Backup for Microsoft Azure appliance, the BYOL license installed on the Veeam Backup for Microsoft Azure appliance becomes invalid. Protected workloads will start consuming license instances from the Veeam Backup & Replication license after the policies run on the connected appliance.

  If you remove the Veeam Backup for Microsoft Azure appliance from Veeam Backup & Replication infrastructure, Veeam Backup & Replication will stop counting backed-up workloads. Veeam Backup for Microsoft Azure continues using the license that was used before you added Veeam Backup for Microsoft Azure to the Veeam Backup & Replication infrastructure.

- **Deploying a new Veeam Backup for Microsoft Azure appliance**
  
  If you deploy a new Veeam Backup for Microsoft Azure appliance in the Veeam Backup & Replication console, protected workloads start consuming instances from the Veeam Backup & Replication license.

  If you remove the Veeam Backup for Microsoft Azure appliance from Veeam Backup & Replication infrastructure, Veeam Backup & Replication stops counting backed-up workloads and Veeam Backup for Microsoft Azure switches to the Free license with 10 available instances. To back up more than 10 instances, you must install a BYOL license on the Veeam Backup for Microsoft Azure appliance. To see how to install a new BYOL license, see the Licensing section in the Veeam Backup for Microsoft Azure User Guide.

Licensing When Connection to Veeam Backup & Replication is Lost

Veeam Backup for Microsoft Azure stores information about workloads licensed by Veeam Backup & Replication. This information allows you to back up workloads even if the connection between the Veeam Backup for Microsoft Azure appliance and Veeam Backup & Replication server is lost. To back up a workload in case of the connection loss, make sure the following conditions are met:

- The workload has already been licensed before the loss of the connection. Note that you are not able to back up new workloads until the connection with Veeam Backup & Replication is restored.

- The workload is still listed as licensed on the Veeam Backup for Microsoft Azure appliance side. For more information on how to open the list of licensed workloads, see the Revoking License Units section (steps 1–2) in the Veeam Backup for Microsoft Azure User Guide.

- The connection was lost less than 31 days ago.
Note that the loss of connection with Veeam Backup & Replication does not affect restore processes and manual creation of snapshots and SQL backups.
Managing Licensed Workloads

After you add a Veeam Backup for Microsoft Azure appliance to the Veeam Backup & Replication infrastructure, you can monitor the number of protected workloads in the Veeam Backup & Replication console. You can also revoke licenses from protected workloads if you do not want to protect these workloads.

Monitoring Licensed Workloads

To monitor protected workloads, do the following:

1. In the Veeam Backup & Replication console, expand the main menu and select License.
2. In the License Information window, switch to the Instances tab.

You will see the following details:

- **Type** — type of protected workloads.
  - Cloud VMs — protected VMs.
  - Cloud File Shares — protect Azure files shares.
  - Cloud Databases — protected SQL servers.

**NOTE**

If you integrate with Veeam Backup for Microsoft Azure 3.0, Veeam Backup & Replication licenses SQL databases, not SQL servers. After you upgrade Veeam Backup for Microsoft Azure to version 3a or later, Veeam Backup & Replication automatically recalculates the consumed license instances.

- **Count** — number of workloads.
- **Multiplier** — number of license instances one workload consumes.
• **Instances** — total number of the consumed license instances.

![License Information](image)

Revoking License Instances

You can revoke licenses from protected workloads and reapply them to other objects that you plan to protect. License revoking can be helpful, for example, if a licensed workload goes out of service or you do not want to protect it anymore.

To revoke a license, do the following:

1. From the main menu, select **License**.
2. In the **License Information** window, open the **Instances** tab and click **Manage**.
3. In the displayed window, select a protected workload and click **Revoke**. Veeam Backup & Replication will revoke the license from the selected object, and the license will be freed for other workloads that you want to protect.
Deployment and Configuration

To configure integration of Veeam Backup & Replication with Veeam Backup for Microsoft Azure, complete the following steps:

1. **Install or upgrade Veeam Backup & Replication.**
   
   Install or upgrade Veeam Backup & Replication up to the required version. Microsoft Azure Plug-in for Veeam Backup & Replication will be automatically installed along with Veeam Backup & Replication.
   
   For more information on how to install or upgrade Veeam Backup & Replication, see the Installing Veeam Backup & Replication and Upgrading Veeam Backup & Replication sections in the Veeam Backup & Replication User Guide.

2. **Install Microsoft Azure Plug-in for Veeam Backup & Replication.**

   Install Microsoft Azure Plug-in for Veeam Backup & Replication on the same machine where Veeam Backup & Replication is installed. For more information on installation, see the Installing Plug-In section.

3. **Add a Veeam Backup for Microsoft Azure appliance.**

   You have two options for adding a Veeam Backup for Microsoft Azure appliance:
   
   - If you have already installed Veeam Backup for Microsoft Azure, you can connect an existing Veeam Backup for Microsoft Azure appliance to the Veeam Backup & Replication infrastructure. For more information, see Connecting to Existing Veeam Backup for Microsoft Azure Appliances.
   
   - If you have not installed Veeam Backup for Microsoft Azure, you can deploy a new Veeam Backup for Microsoft Azure appliance from the Veeam Backup & Replication console. In this case, Veeam Backup & Replication deploys Veeam Backup for Microsoft Azure on an Azure VM automatically. For more information on how to deploy a new appliance, see Deploying New Veeam Backup for Microsoft Azure Appliances.

   After you have added an appliance, we recommend you to set up configuration backup to reduce the risk of data loss. For more information, see Performing Configuration Backup and Restore.

4. **[Optional, for newly added Veeam Backup for Microsoft Azure appliance] Configure worker instances.**

   After you add a new Veeam Backup for Microsoft Azure appliance, open its Web UI component and configure network settings for worker instances. For more information on worker instances and how to configure them, see the Worker Instances section in the Veeam Backup for Microsoft Azure User Guide.

5. **Add standard backup repositories.**

   Adding standard backup repositories may be optional or required:
   
   - If you connect to an existing Veeam Backup for Microsoft Azure appliance, you can omit adding standard repositories since all configured repositories are added to the Veeam Backup & Replication infrastructure automatically. However, you can add standard backup repositories if required.
   
   - If you deploy a new Veeam Backup for Microsoft Azure appliance, you may require to add standard backup repositories — but only in case you want backup policies to produce image-level backups of VMs or backups of SQL databases, or other resources.

   For more information on how to deploy standard backup repositories, see Deploying Standard Backup Repositories.
6. **[Optional] Add archive repositories**

Add archive repositories if you want to store image-level backups of Azure VMs and SQL databases for long periods of time at lower costs. For more information on how to add archive repositories, see *Deploying Archive Backup Repositories*. 
Installing Plug-In

To be able to monitor Veeam Backup for Microsoft Azure appliances and manage their activities in your Veeam Backup & Replication console, you must install Microsoft Azure Plug-in for Veeam Backup & Replication on the Veeam Backup & Replication server.

**NOTE**

Before installing Microsoft Azure Plug-in for Veeam Backup & Replication, you must first stop all policies and disable all jobs, and then you must close the Veeam Backup & Replication console.

To install Microsoft Azure Plug-in for Veeam Backup & Replication version 11.0.4.x, do the following:

1. Go to the [Veeam Backup & Replication: Download](#) page.
2. In the **Additional Downloads** section, switch to the **Cloud Plug-ins** tab.
4. Open the downloaded ZIP file and launch the EXE file.
5. In the setup wizard, accept the license agreement for Veeam and 3rd party components that Veeam incorporates and specify the installation folder. To begin the installation, click **Install**.

**What You Do Next**

After you install Microsoft Azure Plug-in for Veeam Backup & Replication, add Veeam Backup for Microsoft Azure appliances as described in [Add Veeam Backup for Microsoft Azure Appliances](#).
**Upgrading Plug-In**

If you want to upgrade your Microsoft Azure Plug-in for Veeam Backup & Replication to a new version, you do not have to uninstall the previous plug-in version. You only need to install Microsoft Azure Plug-in for Veeam Backup & Replication as described in *Installing Plug-In*.

After you upgrade Microsoft Azure Plug-in for Veeam Backup & Replication, you must also upgrade your appliances in the Veeam Backup & Replication console. For more information on how to upgrade appliances, see *Upgrading Appliances*. 
Adding Veeam Backup for Microsoft Azure Appliances

After you install Microsoft Azure Plug-in for Veeam Backup & Replication, you must add Veeam Backup for Microsoft Azure appliances to the Veeam Backup & Replication infrastructure. You have two options:

- **Connect to existing Veeam Backup for Microsoft Azure appliances.**
  
  If you have already deployed Veeam Backup for Microsoft Azure appliances, you can add these appliances to the Veeam Backup & Replication infrastructure.

- **Deploy new Veeam Backup for Microsoft Azure appliances.**
  
  If you have not deployed Veeam Backup for Microsoft Azure appliances beforehand, you can deploy them from the Veeam Backup & Replication console. In this case, Veeam Backup & Replication will connect to Microsoft Azure and deploy new instances of Veeam Backup for Microsoft Azure. These Veeam Backup for Microsoft Azure appliances will be added to the Veeam Backup & Replication infrastructure automatically.

**NOTE**

You must add a Veeam Backup for Microsoft Azure appliance to the infrastructure of only one Veeam Backup & Replication server. If you add the appliance to another Veeam Backup & Replication server, the synchronization between the appliance and the first Veeam Backup & Replication server will be stopped, and the appliance will be displayed as unavailable. The appliance will start consuming license units from the license of the last Veeam Backup & Replication server to which the appliance was added.
Connecting to Existing Veeam Backup for Microsoft Azure Appliances

To connect to an existing appliance, do the following:

1. Launch the New Veeam Backup for Microsoft Azure Appliance wizard.
2. Specify a deployment mode.
3. Specify a Microsoft Azure account.
4. Specify a Microsoft Azure subscription and appliance location.
5. Select a Microsoft Azure VM.
6. Specify a connection type.
7. Specify credentials.
8. Configure Blob storage backup repositories.
9. Wait for the appliance to be added to the infrastructure.
10. Finish working with the wizard.

NOTE

If you reconnect an appliance from one Veeam Backup & Replication server to another, we recommend you to remove the appliance from the first server and only then add the appliance to another server. If you do not remove the appliance, it will become unavailable on the first server — you will see outdated data and will not be able to perform any operations with the data.
Step 1. Launch New Veeam Backup for Microsoft Azure Appliance Wizard

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

- Open the **Backup Infrastructure** view. Click **Add Server** on the ribbon. In the **Add Server** window, select **Veeam Backup for Microsoft Azure**.
- Open the **Backup Infrastructure** view. In the inventory pane, right-click the **Managed Servers** node and select **Add Server**. In the **Add Server** window, select **Veeam Backup for Microsoft Azure**.
- [If many types of servers are shown] Open the **Backup Infrastructure** view. Click **Add Server** on the ribbon. In the **Add Server** window, click **Veeam cloud-native backup appliance > Veeam Backup for Microsoft Azure**.

### Add Server

Select the type of a server you want to add to your backup infrastructure. All already registered servers can be found under the Managed Servers node on the Backup Infrastructure tab.

- **VMware vSphere**
  Add VMware private cloud infrastructure servers to the inventory.
- **Microsoft Hyper-V**
  Add Microsoft private cloud infrastructure servers to the inventory.
- **Microsoft Windows**
  Add Microsoft Windows server (Windows 2008 R2 SP1 or later, Windows 7 SP1 or later).
- **Linux**
  Add Linux server (must use bash shell, and have SSH and Perl installed).
- **Veeam Backup for AWS**
  Connects to an existing appliance, or deploys a new Veeam Backup for AWS.
- **Veeam Backup for Microsoft Azure**
  Connects to an existing appliance, or deploys a new Veeam Backup for Microsoft Azure appliance.
- **Veeam Backup for GCP**
  Connects to an existing appliance, or deploys a new Veeam Backup for GCP appliance.

[Cancel]
Step 2. Specify Deployment Mode

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

If you want to deploy a new Veeam Backup for Microsoft Azure appliance, see [Deploying New Veeam Backup for Microsoft Azure Appliances](#).

<table>
<thead>
<tr>
<th>Deployment Mode</th>
<th>Connect to an existing appliance</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Registers an existing Veeam Backup for Microsoft Azure appliance.</td>
</tr>
</tbody>
</table>

- **Deploy a new appliance**
  - Deploys a new Veeam Backup for Microsoft Azure appliance from Microsoft Azure Marketplace.
Step 3. Specify Azure Account Settings

At the Account step of the wizard, select credentials of the Microsoft Azure account in which your Veeam Backup for Microsoft Azure appliance is deployed. The user account must have permissions listed in the Required Permissions section.

If you have not added credentials beforehand, click the Manage accounts link or the Add button to add the necessary credentials. Then add the account as described in the Adding Microsoft Azure Compute Accounts section in the Veeam Backup & Replication User Guide. When you add a Microsoft Azure account, Veeam Backup & Replication imports information about subscriptions and resources associated with this account.

**IMPORTANT**

Mind the following:

- Microsoft Azure Stack Hub accounts are not supported.
- Microsoft Azure accounts with multi-factor authentication (MFA) are not supported.
Step 4. Specify Subscription and Region

At the **Subscription** step of the wizard, select the Microsoft Azure subscription that is used to manage resources and costs for your Veeam Backup for Microsoft Azure appliance, and select the region in which the appliance resides.

![Subscription page](image-url)

**Subscription**

Specify a subscription, data center and resource group to connect a backup appliance from. We recommend connecting the backup appliance in the same data center where protected data resides.

- **Subscription**: Enterprise - QA
- **Data center**: West Europe

Select a subscription to connect a backup appliance from.

Select a data center to connect a backup appliance from.
Step 5. Select Azure VM

At the **Virtual Machine** step of the wizard, select the Microsoft Azure VM where Veeam Backup for Microsoft Azure is deployed, that is, the Veeam Backup for Microsoft Azure appliance, and specify a description for future reference.

**IMPORTANT**

The network security group in which Veeam Backup for Microsoft Azure appliance locates must allow the Veeam Backup & Replication server to access the appliance using HTTPS. For more information on how to configure access, see [Microsoft Docs](https://docs.microsoft.com).

![Virtual Machine Configuration](image-url)
Step 6. Specify Connection Type

At the **Connection Type** step of the wizard, choose whether the Veeam Backup for Microsoft Azure appliance is connected directly to the internet or located in a private network:

- If the Veeam Backup for Microsoft Azure appliance is connected to the internet, and you want the Veeam Backup & Replication server to be connected to the Veeam Backup for Microsoft Azure appliance also through the internet, select **Direct connection**. In this case, the Veeam Backup & Replication server will detect the public or static IP of the Veeam Backup for Microsoft Azure appliance automatically.

- If the Veeam Backup for Microsoft Azure appliance is located in a private network and the Veeam Backup & Replication server is also located in the same private network, or you want the Veeam Backup & Replication server to be connected to the Veeam Backup for Microsoft Azure appliance over Veeam PN, select **Private network**. In the **Specify the IP address or DNS name of the appliance** field, specify the private IP or DNS name of the Veeam Backup for Microsoft Azure appliance.

![New Veeam Backup for Microsoft Azure Appliance](image)

- **Direct connection**
  - The backup server will identify the IP address automatically.

- **Private network**
  - Specify the IP address or DNS name of the appliance:

![Connection Type](image)
Step 7. Specify Credentials

At the **Credentials** step of the wizard, specify credentials of a user account that has administrative privileges on the Veeam Backup for Microsoft Azure appliance. This can be the administrator account created during the installation of Veeam Backup for Microsoft Azure or a user account created during further work with Veeam Backup for Microsoft Azure with **Portal Administrator** role assigned.

If you have not added the credentials beforehand, click the **Manage accounts** link or the **Add** button to add the necessary credentials. For more information on adding credentials, see the **Credentials Manager** section in the Veeam Backup & Replication User Guide.

**IMPORTANT**

Multi-factor authentication (MFA) is not supported. For more information on where to check MFA settings, see the **Configuring MFA Settings** section in the Veeam Backup for Microsoft Azure User Guide.

If you try to add an appliance that runs an outdated version of Veeam Backup for Microsoft Azure, Veeam Backup & Replication will display a warning notifying that the appliance must be upgraded. Click **OK** to upgrade the appliance to the latest version of Veeam Backup for Microsoft Azure that is compatible with the current version of Microsoft Azure Plug-in for Veeam Backup & Replication.

When you add a Veeam Backup for Microsoft Azure appliance, Veeam Backup & Replication saves in the configuration database a thumbprint of the web certificate installed on the appliance. When Veeam Backup & Replication connects to the appliance, it uses the saved thumbprint to verify the appliance identity and to avoid the man-in-the-middle attack. For details on managing web certificates, see the **Working with Certificates** section in the Veeam Backup for Microsoft Azure User Guide.

If the certificate installed on the Veeam Backup for Microsoft Azure appliance is not trusted, Veeam Backup & Replication will display a warning. In the warning window, you can do the following:

- Click **View** for the detailed information about the certificate.
- Click **Continue** to trust the certificate.
- Click **Cancel** if you do not trust the certificate. However, in this case you will not be able to connect to the appliance.
NOTE

When you update a certificate on an appliance, this appliance becomes unavailable in the Veeam Backup & Replication console. To make the appliance available again, acknowledge the new certificate at the **Credentials** step of the **Edit Veeam Backup for Microsoft Azure Appliance** wizard. For more information on how to launch the wizard, see **Editing Appliance Settings**.
Step 8. Configure Repositories

The Repositories step of the wizard displays all repositories added to the Veeam Backup for Microsoft Azure infrastructure. For standard backup repositories, specify credentials to access the repositories and a gateway server to be used. For archive repositories, you do not need to specify credentials and a gateway server because there is no direct connection between Veeam Backup & Replication and archive repositories. They are synchronized from Veeam Backup for Microsoft Azure.

To configure credentials and a gateway server, do the following:

1. In the Repositories list, select a standard backup repository to which you want to configure access and click Edit.
2. In the Repository window, do the following:
   a. From the Credentials drop-down list, select credentials of a Microsoft Azure storage account whose type is supported and that has permissions to access the standard backup repository resources. For more information on permissions, see the Repository Account section of the Veeam Backup for Microsoft Azure User Guide.

   If you have not added credentials beforehand, click the Manage cloud accounts link or the Add button to add the necessary credentials. For more information on adding credentials, see the Microsoft Azure Storage Accounts section in the Veeam Backup & Replication User Guide.

   IMPORTANT

   If you do not specify credentials for a standard backup repository, Microsoft Azure Plug-in for Veeam Backup & Replication will stop periodic rescan of the storage. This can help you reduce data transfer costs since Microsoft Azure Plug-in for Veeam Backup & Replication will send fewer requests to Microsoft Azure.

   However, keep in mind that in this case you will only be able to view, manage backup policies and restore Azure VMs to Microsoft Azure — activities described in the Data Protection and Data Recovery sections will not be available.

   b. From the Use the following gateway server for the Internet access drop-down list, select a gateway server that will be used to access the storage. If you do not specify the credentials, the Veeam Backup & Replication server is used as a gateway server.

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

   By default, the role of a gateway server is assigned to the Veeam Backup & Replication server. If the Veeam Backup & Replication server resides in a location that differs from the location where your Veeam Backup for Microsoft Azure resides, choose a server that is located close to the Veeam Backup for Microsoft Azure appliance. You can choose any Microsoft Windows or Linux server that is added to your Veeam Backup & Replication infrastructure and has internet connection. Note that the server must be added to the Veeam Backup & Replication infrastructure beforehand. For more information on how to add a server, see the Virtualization Servers and Hosts section in the Veeam Backup & Replication User Guide.
a. If data in the standard backup repository is encrypted with a password, select the **Use the following password for encrypted backups** check box. From the drop-down list, select the password that must be used to decrypt the data. In this case, Veeam Backup & Replication will automatically decrypt backup files stored in this repository.

If you have not added the password beforehand, click the **Manage passwords** link or the **Add** button to add the necessary password. For more information on adding passwords, see the **Creating Passwords** section in the Veeam Backup & Replication User Guide.

If you do not specify the decryption password, you can do it later. For more information, see **Decrypting Image-Level Backups**.

If data in the standard backup repository is encrypted with a Key Vault key, Microsoft Azure Plug-in for Veeam Backup & Replication shows the used key but does not allow changing it. You can change the key in the appliance Web UI as described in the **Editing Backup Repository Settings** section in the Veeam Backup for Microsoft Azure User Guide.

After you finish working with the wizard, all Blob storage backup repositories will be displayed on the **Backup Infrastructure** view, under the **External Repositories** node. For more information on where backups are shown, see **Viewing Snapshots and Backups**.

**NOTE**

If a standard backup repository is already added to the infrastructure of another Veeam Backup & Replication server, you will be prompted to claim the ownership of this storage. For more information on taking the ownership, see the **Ownership** section in the Veeam Backup & Replication User Guide.
Step 9. Apply Settings

At the Apply step of the wizard, wait until Veeam Backup & Replication applies the settings. Click Next to complete the procedure of adding the appliance.
Step 10. Finish Working with Wizard

At the **Summary** step of the wizard, review details of the added Veeam Backup for Microsoft Azure appliance and click **Finish**.

If you want to configure worker instances, manage accounts or other settings that are not available in the Veeam Backup & Replication console, click the **backup appliance console** link. For more information on what you can do in the Veeam Backup for Microsoft Azure UI, see the Veeam Backup for Microsoft Azure User Guide.
Deploying New Veeam Backup for Microsoft Azure Appliances

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

1. Launch the New Veeam Backup for Microsoft Azure Appliance wizard.
2. Specify a deployment mode.
4. Specify a Microsoft Azure subscription.
5. Specify an Azure VM.
6. Specify network resources.
7. Specify IP settings.
8. Specify guest OS credentials.
9. Wait for the appliance to be added to the infrastructure.
10. Finish working with the wizard.
Step 1. Launch New Veeam Backup for Microsoft Azure Appliance Wizard

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

- Open the Backup Infrastructure view. Click Add Server on the ribbon. In the Add Server window, select Veeam Backup for Microsoft Azure.
- Open the Backup Infrastructure view. In the inventory pane, right-click the Managed Servers node and select Add Server. In the Add Server window, select Veeam Backup for Microsoft Azure.
- [If many types of servers are shown] Open the Backup Infrastructure view. Click Add Server on the ribbon. In the Add Server window, click Veeam cloud-native backup appliance > Veeam Backup for Microsoft Azure.

Add Server
Select the type of a server you want to add to your backup infrastructure. All already registered servers can be found under the Managed Servers node on the Backup Infrastructure tab.

- VMware vSphere
  Adds VMware private cloud infrastructure servers to the inventory.
- Microsoft Hyper-V
  Adds Microsoft private cloud infrastructure servers to the inventory.
- Microsoft Windows
  Adds Microsoft Windows server (Windows 2008 R2 SP1 or later, Windows 7 SP1 or later).
- Linux
  Adds Linux server (must use bash shell, and have SSH and Perl installed).
- Veeam Backup for AWS
  Connects to an existing appliance, or deploys a new Veeam Backup for AWS.
- Veeam Backup for Microsoft Azure
  Connects to an existing appliance, or deploys a new Veeam Backup for Microsoft Azure appliance.
- Veeam Backup for GCP
  Connects to an existing appliance, or deploys a new Veeam Backup for GCP appliance.
Step 2. Specify Deployment Mode

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

If you want to connect to an existing Veeam Backup for Microsoft Azure appliance, see [Adding Existing Veeam Backup for Microsoft Azure Appliances](#).

---

<table>
<thead>
<tr>
<th>New Veeam Backup for Microsoft Azure Appliance</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Deployment Mode</strong></td>
</tr>
<tr>
<td>Choose whether you want to connect to an existing appliance or deploy a new one.</td>
</tr>
</tbody>
</table>

- **Connect to an existing appliance**
  - Registers an existing Veeam Backup for Microsoft Azure appliance.

- **Deploy a new appliance**
  - Deploys a new Veeam Backup for Microsoft Azure appliance from Microsoft Azure Marketplace.
Step 3. Specify Azure Account Settings

At the **Account** step of the wizard, select credentials of a Microsoft Azure account that will be used to access resources. Microsoft Azure Plug-in for Veeam Backup & Replication will use this Azure account to deploy the Veeam Backup for Microsoft Azure appliance. The user account must have permissions listed in the **Required Permissions** section.

If you have not added credentials beforehand, click the **Manage accounts** link or the **Add** button to add the necessary credentials. Then add the account as described in the **Adding Microsoft Azure Compute Accounts** section in the Veeam Backup & Replication User Guide. When you add a Microsoft Azure account, Veeam Backup & Replication imports information about subscriptions and resources associated with this account.

**IMPORTANT**

Mind the following:

- Microsoft Azure Stack Hub accounts are not supported.
- Microsoft Azure accounts with multi-factor authentication (MFA) are not supported.

![New Veeam Backup for Microsoft Azure Appliance](image)

![Deployment Mode](image)

![Account](image)
Step 4. Specify Subscription

At the Subscription step of the wizard, specify a Microsoft Azure subscription, Microsoft Azure region and resource group settings for an Azure VM where Veeam Backup for Microsoft Azure will be deployed:

1. From the Subscription drop-down list, select a Microsoft Azure subscription. Microsoft Azure Plug-in for Veeam Backup & Replication will use this subscription to manage resources and costs of a VM where the Veeam Backup for Microsoft Azure will be deployed.

   For a subscription to be displayed in the Subscription list, it must be created in advance and associated to the Azure account as described in Microsoft Docs.

2. From the Data center drop-down list, select a Microsoft Azure region in which the Veeam Backup for Microsoft Azure appliance will reside.

3. From the Resource group drop-down list, select a resource group. For a resource group to be displayed in the Resource group drop-down list, it must be created in advance as described in Microsoft Docs.

   To create a new group, select (create new). A veeam-<VMname>-rg<GUID> resource group will be created.
Step 5. Specify Azure VM

At the **Virtual Machine** step of the wizard, specify a name and description for an Azure VM where Veeam Backup for Microsoft Azure will be deployed. Note that the VM name that you specify must follow Azure naming rules. Otherwise, the deployment may fail. For more information on the naming rules, see [Microsoft Docs](https://aka.ms/...).

![Virtual Machine configuration panel](image-url)

**VM name:**
- tw-lab-proxy

**Description:**
- Microsoft Azure appliance
Step 6. Specify Network Resources

At the Networking step of the wizard, specify the network settings of an Azure VM where Veeam Backup for Microsoft Azure will be deployed:

1. From the Virtual network drop-down list, select an Azure virtual network to which the Veeam Backup for Microsoft Azure appliance will be connected. To create a new Azure virtual network, select (create new).

2. From the Subnet drop-down list, select a subnet to which the Veeam Backup for Microsoft Azure appliance will be connected. To create a new subnet, select (create new).

   For a subnet to be displayed in the drop-down list, it must be created in advance as described in Microsoft Docs.

3. From the Network security group drop-down list, select a network security group to which the Veeam Backup for Microsoft Azure appliance will be connected. To create a new security group, select (create new).

   For a security group to be displayed in the drop-down list, it must be created in advance as described in Microsoft Docs.

   **IMPORTANT**

   If you select an existing security group, make sure it has a security rule that allows the Veeam Backup & Replication server to access the Veeam Backup for Microsoft Azure appliance through HTTPS. For more information on how to create security rules, see Microsoft Docs.

4. (If you select to create a new security group) In the Backup server public IP address field, specify a public IP address or a scope of IP addresses in CIDR notation that will be allowed to access the Veeam Backup for Microsoft Azure appliance.

   Veeam Backup for Microsoft Azure will create a security rule for the specified IP addresses. Note that the Veeam Backup & Replication server IP address must fall into the specified IP addresses.

![Networking Configuration](image)
Step 7. Specify IP Settings

At the **IP Assignment** step of the wizard, select a type of the IP address that you want to assign to the Veeam Backup for Microsoft Azure appliance:

- To assign a dynamic IP to the Veeam Backup for Microsoft Azure appliance, select **Dynamic IP address**. You can either select an existing dynamic IP address from the drop-down list, or create a new dynamic IP. To create a new dynamic IP, select **(create new)**.
- To assign a static IP address to the Veeam Backup for Microsoft Azure appliance, select **Static IP address**. You can either select an existing static IP address from the drop-down list, or create a new static IP. To create a new static IP, select **(create new)**.

For an IP to be displayed in the list of available static or dynamic IPs, it must be added as described in [Microsoft Docs](https://docs.microsoft.com).

![IP Assignment](image-url)
Step 8. Specify Credentials

At the Guest OS step of the wizard, specify credentials for the Azure VM where Veeam Backup for Microsoft Azure appliance will be deployed:

1. From the **Create the following administrator credentials** drop-down list, select credentials that will be used to authenticate against the Veeam Backup for Microsoft Azure appliance.

   If you have not added credentials beforehand, click the **Manage accounts** link or the **Add** button to add the necessary credentials. For more information on adding credentials, see the Credentials Manager section in the Veeam Backup & Replication User Guide.

2. In the **Use the following key pair** field, select a key pair that will be used to authenticate against the Veeam Backup for Microsoft Azure appliance. If you have not added a key pair beforehand, you can create it.

   To create a new key pair:
   
   a. Click **Add**.

   b. In the **New Key Pair** window, specify the following settings:

   i. In the **Name** section, specify a name for the key pair.

       The key pair name must be between 1 and 80 characters in length. It must not contain special characters `\"":<>;?,*@&`, whitespace, or begin with `'` or end with `.` or `-`. It must not contain only numbers.

   ii. In the **Path** section, specify the path to the folder where the private key will be located.

       The key pair will be created in the resource group that you have specified at the **Subscription** step of the wizard. If you have selected to create a new resource group, Microsoft Azure Plug-in for Veeam Backup & Replication will create the **VeeamSSHKeys** resource group and will store the key pair there.
Step 9. Apply Settings

At the **Apply** step of the wizard, wait until Veeam Backup & Replication applies the settings and click **Next** to complete the appliance deployment.
Step 10. Finish Working with Wizard

At the **Summary** step of the wizard, review the Veeam Backup for Microsoft Azure appliance configuration settings and click **Finish**.

A new Veeam Backup for Microsoft Azure is configured without standard backup repositories. If you want to deploy a standard repository on a new Veeam Backup for Microsoft Azure appliance, select the **Open the Azure Blob backup repository creation wizard when I click Finish** check box. For more information, see the Adding Standard Backup Repositories section.

**NOTE**

After you deploy a new Veeam Backup for Microsoft Azure appliance, you need to configure network settings for worker instances in the appliance Web UI component. For more information on worker instances and how to configure them, see the Worker Instances section in the Veeam Backup for Microsoft Azure User Guide.
Managing Veeam Backup for Microsoft Azure Appliances

To view all added Veeam Backup for Microsoft Azure appliances, open the Backup Infrastructure view and navigate to Managed Servers > Microsoft Azure. The working area displays the full list of configured appliances. Here, you can edit appliance settings, rescan appliance data, remove appliances from the Veeam Backup & Replication infrastructure, or open Web UI component of an appliance right from the Veeam Backup & Replication console.
Viewing Snapshots and Backups

Available backups and snapshots are displayed under subnodes of the **Backups** node in the **Home** view:

- **The Snapshots** subnode shows cloud-native snapshots of all protected workloads.

  In the working area, there is an `<Appliance name>` node. This node displays all snapshots to which your appliance has access, but for which backup policies were removed. Also, this node shows all Azure file shares to which the appliance has access.

  For more information on how Veeam Backup for Microsoft Azure creates cloud-native snapshots, see the Snapshot Chain sections in the Veeam Backup for Microsoft Azure User Guide.

- **The External Repository** subnode shows image-level backups of VMs and backups of SQL databases stored in standard backup repositories. Here, Veeam Backup & Replication marks **decrypted backups** with a special icon (🛠).

  For more information on how Veeam Backup for Microsoft Azure creates backups, see the Backup Chain sections in the Veeam Backup for Microsoft Azure User Guide.

- **The External Repository (Archive)** subnode shows image-level backups stored in archive repositories. These backups are automatically decrypted.

  For more information on how Veeam Backup for Microsoft Azure creates archive backups, see the Archive Backup Chain section in the Veeam Backup for Microsoft Azure User Guide.

- **The External Repository (Encrypted)** subnode shows encrypted image-level backups (backups stored in encrypted Blob storage backup repositories) for which you did not specify the decryption password or the specified password does not match the current password of the repository.

When you expand a node in the working area, the following icons describe which workloads are protected:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Protected Workload</th>
</tr>
</thead>
<tbody>
<tr>
<td>🛠️</td>
<td>Indicates that the protected workload is a VM.</td>
</tr>
<tr>
<td>🛠️</td>
<td>Indicates that the protected workload is a SQL database.</td>
</tr>
<tr>
<td>🛠️</td>
<td>Indicates that the protected workload is an Azure file share.</td>
</tr>
</tbody>
</table>
Editing Appliance Settings

To edit settings of a Veeam Backup for Microsoft Azure appliance, do the following:

1. Open the **Backup Infrastructure** view.

2. In the inventory pane, select **Managed Servers**.

3. In the working area, select the appliance whose settings you want to edit, and click **Edit Appliance** on the ribbon. Alternatively, right-click the appliance and select **Properties**.

4. Complete the wizard as described in the **Connecting to Existing Veeam Backup for Microsoft Azure Appliances** section.
Opening Appliance Web UI Component

If you want to access Veeam Backup for Microsoft Azure and configure options not available from the Veeam Backup & Replication console, you can perform the necessary actions using the Web UI component of an appliance.

To open the Web UI component of a Veeam Backup for Microsoft Azure appliance, do the following:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select **Managed Servers**.
3. In the working area, select the Veeam Backup for Microsoft Azure appliance whose Web UI component you want to open, and click **Open Console** on the ribbon. Alternatively, right-click the appliance and select **Open console**.

Veeam Backup & Replication will open a web browser and navigate you to the Veeam Backup for Microsoft Azure URL. For more information on what you can do in the Web UI component, see the [Veeam Backup for Microsoft Azure User Guide](#).
Upgrading Appliances

To upgrade an appliance to the latest version of Veeam Backup for Microsoft Azure that is compatible with the current version of Microsoft Azure Plug-in for Veeam Backup & Replication, do the following:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select **Managed Servers**.
3. In the working area, select the Veeam Backup for Microsoft Azure appliance that you want to upgrade, and click **Upgrade appliance** on the ribbon. Alternatively, right-click the appliance and select **Upgrade**.

Alternatively, you can edit appliance settings. At the **Credentials** step of the wizard, Veeam Backup & Replication will prompt you to confirm the appliance upgrade. For more information on how to edit the settings, see the **Editing Appliance Settings**.
Rescanning Appliances

If Veeam Backup for Microsoft Azure appliances become unavailable, for example, due to connectivity problems, you can rescan the appliances. Note that the appliance rescan option is disabled for available Veeam Backup for Microsoft Azure appliances.

To rescan a Veeam Backup for Microsoft Azure appliance, do the following:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select **Managed Servers**.
3. In the working area, select the necessary Veeam Backup for Microsoft Azure appliance, and click **Rescan appliance** on the ribbon. Alternatively, you can right-click the appliance and select **Rescan**.
4. In the opened window, click **Yes**.

Veeam Backup & Replication will remove from the configuration database all data collected on the Veeam Backup for Microsoft Azure appliance. Then Veeam Backup & Replication will recollect data including the following: last 24-hour session results, data on all created snapshots, backups and jobs.
Removing Appliances

If you do not plan to manage an appliance using the Veeam Backup & Replication console, you can remove the appliance from the Veeam Backup & Replication infrastructure only. If you do not plan to use the appliance anymore, you can remove it from both the Veeam Backup & Replication and Microsoft Azure infrastructures.

Removing Appliance from Veeam Backup & Replication

After you remove an appliance from the Veeam Backup & Replication infrastructure only, you are not able to perform any data protection and data recovery operations in the Veeam Backup & Replication console. Microsoft Azure Plug-in for Veeam Backup & Replication removes from the Veeam Backup & Replication infrastructure the appliance and backup repositories for which credentials are not specified. However, the appliance and all the connected resources (repositories, subnets and so on) remain in Microsoft Azure.

To remove an appliance from the Veeam Backup & Replication infrastructure:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select **Managed Servers**.
3. In the working area, select the appliance that you want to remove, and click **Remove Appliance** on the ribbon. Alternatively, right-click the appliance and select **Remove**.
4. In the opened window, click **Yes**. If you see the **Delete cloud resources associated with the backup appliance from infrastructure** check box, make sure that it is not selected.

Removing Appliance from Veeam Backup & Replication and Microsoft Azure

Removing Appliances Deployed from Veeam Backup & Replication Console

[The following instructions apply if you have deployed an appliance version 3.x and later from the Veeam Backup & Replication console. If you have deployed an appliance from Microsoft Azure portal, deployed an appliance version 2.x or connected an appliance, see the instructions in Removing Appliances Deployed from Microsoft Azure Portal.]
When you remove appliances from both the Veeam Backup & Replication and Microsoft Azure infrastructures, all the resources created along with the appliances are also removed. The removed resources are VMs on which Veeam Backup for Microsoft Azure is deployed, network interfaces, disks and so on. The resources that remain are resources that already existed at the moment of the appliance creation, repositories and created backups, and resources shared with other VMs.

To remove an appliance from both the Veeam Backup & Replication and Microsoft Azure infrastructures:

1. Open the Backup Infrastructure view.
2. In the inventory pane, select Managed Servers.
3. In the working area, select the appliance that you want to remove, and click Remove Appliance on the ribbon. Alternatively, right-click the appliance and select Remove.
4. In the opened window, select the Delete cloud resources associated with the backup appliance from infrastructure check box and click Yes.

Removing Appliances Deployed from Portal

[The following instructions apply if you have deployed an appliance version 2.x and earlier, or an appliance version 3.x and later from Microsoft Azure portal. If you have deployed an appliance version 3.x or later from the Veeam Backup & Replication console, see the instructions in Removing Appliances Deployed from Veeam Backup & Replication Console.]

To remove an appliance from the Veeam Backup & Replication and Microsoft Azure infrastructures, you must first remove it from Veeam Backup & Replication as described in Removing Appliance from Veeam Backup & Replication. Then remove the resources deployed in Microsoft Azure as described in the Uninstalling Veeam Backup for Microsoft Azure section in the Veeam Backup for Microsoft Azure User Guide.

NOTE

If you deployed an appliance from the Veeam Backup & Replication console and selected to create a new key pair at the Guest OS step of the wizard, you also need to remove the key pair from the resource group that you specified at the Subscription step of the wizard or the VeeamSSHKeys resource group if you selected to create a new resource group.
Adding Blob Storage Backup Repositories

A Blob storage backup repository is a folder in a blob container with a specific tier assigned.

Microsoft Azure Plug-in for Veeam Backup & Replication supports the following types of Blob storage backup repositories:

- **Standard backup repository**
  A standard backup repository is a folder in a blob container with the Hot (inferred) or Cool (inferred) access tier assigned. Microsoft Azure Plug-in for Veeam Backup & Replication uses this repository to store image-level backups of Azure VMs, backups of SQL databases or other resources. We recommend you to store in this repository frequently accessed backups or infrequently accessed backups that must be stored for at least 30 days.

  To store backups in a standard backup repository, first add it to the infrastructure and then enable image-level backups in a backup policy. For more information on how to create a policy, see Performing Backup in the Veeam Backup for Microsoft Azure User Guide.

- **Archive repository**
  An archive repository is a folder in a blob container with the Archive tier assigned. Archive repository allows you to archive image-level backups of Azure VMs, backups of SQL databases, or other resources, that is, to store backups for long periods of time at lower costs. However, restoring from an archived backup is longer and more expensive than restoring from a backup stored in a standard backup repository.

  To restore data from an archive, you first need to retrieve data from it. For more information on how to retrieve data, see Retrieving Data from Archive.

  We recommend you to archive data if it is rarely accessed and stored for at least 180 days or if you want to reduce data-at-rest costs and to save space in the high availability standard backup repository.

  To archive backups, first add an archive repository and then enable backup archiving in backup policies. Note that you can archive only backups created with monthly and yearly retention schemes. For more information on how to create a policy, see Performing Backup in the Veeam Backup for Microsoft Azure User Guide. For more information on how archiving works, see the Enabling Backup Archiving for VMs and Enabling Backup Archiving for Databases section in the Veeam Backup for Microsoft Azure User Guide.

Depending on your configuration, you can connect to existing repositories or deploy new ones.

Connecting to Existing Repository

All Blob storage backup repositories that have been already configured on a Veeam Backup for Microsoft Azure appliance are added automatically to the Veeam Backup & Replication infrastructure when you connect to this appliance.

If a repository that is already added to the Veeam Backup for Microsoft Azure infrastructure is not available in the Veeam Backup & Replication infrastructure, follow the instructions provided in the Editing Veeam Backup for Microsoft Azure Appliance Settings section. For a standard backup repository, at the Repositories step of the Edit Veeam Backup for Microsoft Azure Appliance wizard, specify credentials to be used to access the repository and click Apply, and the repository will be added to the Veeam Backup & Replication infrastructure.
NOTE

[For standard backup repositories] If you do not want or do not have an option to add the Veeam Backup for Microsoft Azure appliance where a standard backup repository is deployed to the Veeam Backup & Replication infrastructure, follow the instructions provided in the Adding External Azure Blob Storage section in the Veeam Backup & Replication User Guide. In this case, restore from backups stored in this Blob storage will work as described in the How Restore to Microsoft Azure Works section in the Veeam Backup & Replication User Guide. This configuration might be necessary, for example, if your product license is not supported.

Deploying New Repositories

When you deploy Blob storage backup repositories in the Veeam Backup & Replication console, they are added to the Veeam Backup for Microsoft Azure infrastructure and are also displayed in the Veeam Backup for Microsoft Azure infrastructure.

For instructions on how to deploy a repository, see the following sections:

- Deploying Standard Backup Repositories
- Deploying Archive Repositories
Deploying Standard Backup Repositories

For more information on a standard backup repository, see Add Blob Storage Backup Repositories.

To deploy a new standard backup repository, do the following:

1. Launch the Add External Repository wizard.
2. Specify a Veeam Backup for Microsoft Azure appliance.
4. Select a blob container.
5. Configure encryption.
6. Wait for the repository to be added to the infrastructure.
7. Finish working with the wizard.
Step 1. Launch Add External Repository Wizard

To launch the Add External Repository wizard, open the Backup Infrastructure view and do one of the following:

- In the inventory pane, select the External Repositories node and click Add Repository on the ribbon. In the opened window, select Veeam Backup for Microsoft Azure > Azure Blob Storage.
- In the inventory pane, right-click the External Repositories node and select Add. In the opened window, select Veeam Backup for Microsoft Azure > Azure Blob Storage.

Veeam Backup for Microsoft Azure
Select the type of Microsoft Azure storage you want to use as a backup repository.

- **Azure Blob Storage**
  Adds Microsoft Azure Blob Storage of hot and cold tiers. Use this option for short-term storage of recent backups.

- **Azure Archive Storage**
  Adds Microsoft Azure Archive Storage. Use this option for cost-efficient archival of long-term backups.
Step 2. Specify Veeam Backup for Microsoft Azure Appliance

At the **Backup Appliance** step of the wizard, specify a name for the standard backup repository and the Veeam Backup for Microsoft Azure appliance to whose infrastructure you want to add the repository:

1. From the **Appliance** drop-down list, select the necessary Veeam Backup for Microsoft Azure appliance. New standard backup repository will be added to the infrastructure managed by the selected Veeam Backup for Microsoft Azure appliance.

   For an appliance to be displayed in the **Appliance** drop-down list, it must be added to the Veeam Backup & Replication infrastructure as described in the Adding Veeam Backup for Microsoft Azure Appliances section.

2. In the **Repository name** field, enter a name for the repository. The maximum length of the name is 125 characters; all special characters except for (_) cannot be used.

   Veeam Backup & Replication will assign this name to the folder that is located in the Veeam/Backup folder in Azure container that you will specify at the Container step of the wizard. Backups saved to this folder will be assigned the same access tier (access tier inferred) as specified for the storage account where the created repository will reside.

3. In the **Description** field, enter a description for future reference.

---

*Image of the wizard interface showing theBackup Appliance tab with fields for Appliance, Repository name, Description.*
Step 3. Specify Storage Account Settings

At the Account step of the wizard, specify settings for an account which will be used to connect to the standard backup repository:

1. From the Credentials drop-down list, select credentials of a Microsoft Azure storage account whose type is supported and where the target blob container resides or will reside. This account will be used to access the backup repository.

   If you have not added credentials beforehand, click the Manage cloud accounts link or the Add button to add the necessary credentials. For more information on adding credentials, see the Microsoft Azure Storage Accounts section in the Veeam Backup & Replication User Guide.

2. From the Gateway server drop-down list, select a gateway server that will be used to access Blob storage.

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

   By default, the role of a gateway server is assigned to the Veeam Backup & Replication server. If the Veeam Backup & Replication server resides in a region that differs from the Azure region where your Veeam Backup for Microsoft Azure resides, choose a server that is located close to the Veeam Backup for Microsoft Azure appliance. You can choose any Microsoft Windows or Linux server that is added to your Veeam Backup & Replication infrastructure and has internet connection. Note that the server must be added to the Veeam Backup & Replication infrastructure beforehand. For more information on how to add a server, see the Virtualization Servers and Hosts section in the Veeam Backup & Replication User Guide.
Step 4. Select Blob Container

At the **Container** step of the wizard, specify Azure Blob storage container where you want to store backups. In the **Container** field specify an Azure Blob storage container where backups will reside. You can create a new container or select an existing one:

- To create a new container, click **Add**. In the **New Container** window, enter a name for the container. Make sure that this name meets the requirements described in [Microsoft Docs](#).
- To specify an existing container, select it from the **Container** drop-down list.

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](#).
Step 5. Configure Encryption

At the Encryption step of the wizard, you can enable data encryption:

1. Select the Enable backup file encryption check box.

2. If you want to use a Key Vault key for encryption, select Perform Azure encryption with the following key and do the following:
   
a. From the Subscription drop-down list, select a Microsoft Azure subscription where the Key Vault is created. The drop-down list shows subscriptions from the tenant in which the selected storage account is located.

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

   b. From the Key vault drop-down list, select Azure Key Vault where the encryption key is stored.

   **IMPORTANT**

   To get Key Vaults and Key Vault keys, Microsoft Azure Plug-in for Veeam Backup & Replication uses a service account that is added to the appliance and that has access to the tenant in which the selected storage account is located. This service account must have access to Key Vaults and keys. The permissions are listed in Required Permissions.

   c. From the Encryption key drop-down list, select the key you want to use. Veeam Backup for Microsoft Azure will use the current key version.

   **IMPORTANT**

   Do not disable Key Vault keys used for encryption, otherwise the Veeam Backup for Microsoft Azure appliance will not be able to encrypt data, and backup policies that use encrypted repositories for storing backups will fail.

   Do not delete Key Vault keys used for encryption, otherwise the Veeam Backup for Microsoft Azure appliance will not be able to decrypt data stored in these repositories.

3. If you want to use a password for encryption, select Perform Veeam encryption with the following password. From the Use the following encryption password drop-down list, select a password that you want to use.

   If you have not added the password beforehand, click the Manage passwords link or the Add button to add a password. For more information on adding passwords, see the Creating Passwords section in the Veeam Backup & Replication User Guide.
If you further plan to change the encryption method, you will need to go through the edit wizard of the repository or appliance right after you change the encryption method. For more information, see the Editing Settings of External Repository or Editing Appliance Settings sections.
Step 6. Apply Settings

At the **Apply** step of the wizard, wait until Veeam Backup & Replication applies the settings. Click **Next** to complete adding of a new standard backup repository.
Step 7. Finish Working with Wizard

At the **Summary** step of the wizard, review the newly created repository settings and click **Finish**.

Summary:
- Azure blob backup repository has been created successfully
- Appliance: tw-proxy-2306-1346
- Description: Standard backup repository
- Microsoft Azure account: tw03lab
- Data center: Global
- Container: tw-proxy-repo
- Access tier: Inferred
- Gateway server: backupsrv52.tech.local (Backup server)
- Encryption: Disabled
Deploying Archive Repositories

For more information on an archive repository, see Adding Blob Storage Backup Repositories.

To deploy an archive repository, use the following instructions:

1. **Launch the Add External Repository wizard.**
2. **Specify a Veeam Backup for Microsoft Azure appliance and repository name.**
3. **Specify storage account settings.**
4. **Select a blob container.**
5. **Configure encryption.**
6. **Wait for the repository to be added to the infrastructure.**
7. **Finish working with the wizard.**
Step 1. Launch Add External Repository Wizard

To launch the Add External Repository wizard, open the Backup Infrastructure view and do one of the following:

- In the inventory pane, select the External Repositories node and click Add Repository on the ribbon. In the opened window, select Veeam Backup for Microsoft Azure > Azure Archive Storage.
- In the inventory pane, right-click the External Repositories node and select Add. In the opened window, select Veeam Backup for Microsoft Azure > Azure Archive Storage.

Veeam Backup for Microsoft Azure
Select the type of Microsoft Azure storage you want to use as a backup repository.

- Azure Blob Storage
  Adds Microsoft Azure Blob Storage of hot and cold tiers. Use this option for short-term storage of recent backups.

- Azure Archive Storage
  Adds Microsoft Azure Archive Storage. Use this option for cost-efficient archival of long-term backups.
Step 2. Specify Veeam Backup for Microsoft Azure Appliance

At the Backup Appliance step of the wizard, specify an archive repository name and the Veeam Backup for Microsoft Azure appliance to whose infrastructure you want to add the repository:

1. From the Appliance drop-down list, select the necessary Veeam Backup for Microsoft Azure appliance. The archive repository will be deployed in the infrastructure of the selected Veeam Backup for Microsoft Azure appliance.

   For an appliance to be displayed in the Appliance drop-down list, it must be added to the Veeam Backup & Replication infrastructure as described in the Adding Veeam Backup for Microsoft Azure Appliances section.

2. In the Repository name field, enter a name for the archive repository. The maximum length of the name is 125 characters; all special characters except for ( ) _ - . cannot be used.

   Veeam Backup & Replication will assign this name to the folder that is located in the Veeam/Backup folder in Azure container that you will specify at the Container step of the wizard. Backups saved to this folder will be assigned the Archive access tier.

3. In the Description field, enter a description for future reference.

![Add External Repository](image.png)

Backup Appliance
Specify the Veeam Backup for Microsoft Azure appliance to create the backup repository for.

<table>
<thead>
<tr>
<th>Backup Appliance</th>
<th>Account</th>
<th>Container</th>
<th>Encryption</th>
<th>Apply</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance</td>
<td>tw-proxy-1308-1346</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Repository name</td>
<td>lvrepo-archive-encrypt</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>Archive repository</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Step 3. Specify Storage Account Settings

At the **Account** step of the wizard, specify settings for an account which will be used to access the archive repository. From the **Credentials** drop-down list, select credentials of a Microsoft Azure storage account whose **type is supported** and where the target blob container resides or will reside.

If you have not added credentials beforehand, click the **Manage cloud accounts** link or the **Add** button to add the necessary credentials. For more information on adding credentials, see the Microsoft Azure Storage Accounts section in the Veeam Backup & Replication User Guide.
Step 4. Select Blob Container

At the Container step of the wizard, specify Azure Blob storage container where you want to store archive backups. In the Container field specify an Azure Blob storage container where archive backups will reside. You can create a new container or select an existing one:

- To create a new container, click Add. In the New Container window, enter a name for the container. Make sure that this name meets the requirements described in Microsoft Docs.

- To specify an existing container, select it from the Container drop-down list.

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.
Step 5. Configure Encryption

At the Encryption step of the wizard, you can enable data encryption:

1. Select the Enable backup file encryption check box.

2. If you want to use a Key Vault key for encryption, select Perform Azure encryption with the following key and do the following:

   a. From the Subscription drop-down list, select a Microsoft Azure subscription where the Key Vault is created. The drop-down list shows subscriptions from the tenant in which the selected storage account is located. For a subscription to be displayed in the Subscription drop-down list, it must be created in advance and associated to the Azure account as described in Microsoft Docs.

   b. From the Key vault drop-down list, select Azure Key Vault where the encryption key is stored. IMPORTANT To get Key Vaults and Key Vault keys, Microsoft Azure Plug-in for Veeam Backup & Replication uses a service account that is added to the appliance and that has access to the tenant in which the selected storage account is located. This service account must have access to Key Vaults and keys. The permissions are listed in Required Permissions.

   c. From the Encryption key drop-down list, select the key you want to use. Veeam Backup for Microsoft Azure will use the current key version. IMPORTANT Do not disable Key Vault keys used for encryption, otherwise the Veeam Backup for Microsoft Azure appliance will not be able to encrypt data, and backup policies that use encrypted repositories for storing backups will fail. Do not delete Key Vault keys used for encryption, otherwise the Veeam Backup for Microsoft Azure appliance will not be able to decrypt data stored in these repositories.

3. If you want to use a password for encryption, select Perform Veeam encryption with the following password. From the Use the following encryption password drop-down list, select a password that you want to use.

   If you have not added the password beforehand, click the Manage passwords link or the Add button to add a password. For more information on adding passwords, see the Creating Passwords section in the Veeam Backup & Replication User Guide.
NOTE

If you change the encryption method, you will need to go through the edit wizard of the repository or appliance right after you change the encryption method. For more information, see the Editing Settings of External Repository or Editing Appliance Settings sections.
Step 6. Apply Settings

At the **Apply** step of the wizard, wait until Veeam Backup & Replication applies the settings. Click **Next** to complete the procedure of adding the archive repository.
Step 7. Finish Working with Wizard

At the **Summary** step of the wizard, review the newly created archive repository settings and click **Finish**.

**Summary**

You can copy the configuration information below for future reference.

<table>
<thead>
<tr>
<th>Summary:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Azure blob backup repository has been created successfully</td>
</tr>
<tr>
<td>Appliance: tw-proxy-2306-1346</td>
</tr>
<tr>
<td>Description: Archive repository</td>
</tr>
<tr>
<td>Microsoft Azure account: tw05tab</td>
</tr>
<tr>
<td>Data center: Global</td>
</tr>
<tr>
<td>Container: tw-proxy-repo</td>
</tr>
<tr>
<td>Access tier: Archive</td>
</tr>
<tr>
<td>Gateway server: backupsns30.techlocal (Backup server)</td>
</tr>
<tr>
<td>Encryption: Enabled</td>
</tr>
</tbody>
</table>
Managing Backup Repositories

You can perform different operations for standard and archive repositories:

- Archive repositories
  
  You can remove repositories from Veeam Backup & Replication infrastructure as described in Removing Repositories. You can edit archive repositories using the Veeam Backup for Microsoft Azure appliance Web UI. For more information, see the Editing Backup Repository Settings section in Veeam Backup for Microsoft Azure User Guide.

- Standard backup repositories
  
  You can edit, rescan and remove repositories. For more information, see the sections below.

**NOTE**

If you change the encryption method, you need to go through the edit wizard of the repository or appliance right after you change the encryption method. For more information, see the Editing Settings of External Repository or Editing Appliance Settings sections.

Editing Standard Backup Repository Settings

To edit standard backup repository settings, follow the instructions provided in the Editing Settings of External Repository section in the Veeam Backup & Replication User Guide.

Rescanning Standard Backup Repositories

To synchronize backups stored in standard backup repositories across the Veeam Backup & Replication and Veeam Backup for Microsoft Azure infrastructures, follow the instructions provided in the Rescanning External Repository section in the Veeam Backup & Replication User Guide.

Removing Backup Repositories

To remove backup repositories from the Veeam Backup & Replication infrastructure, follow the instructions provided in the Removing External Repositories section in the Veeam Backup & Replication User Guide. Note that the repositories will be removed only from the Veeam Backup & Replication infrastructure; the repository will still exist on the Veeam Backup for Microsoft Azure appliance.

For more information on how to remove the repository from the Veeam Backup for Microsoft Azure appliance, see the Removing Backup Repositories section in Veeam Backup for Microsoft Azure User Guide.
Performing Configuration Backup and Restore

You can back up and restore the configuration database that stores data collected from Veeam Backup for Microsoft Azure appliances. The configuration contains the following information: existing backup policies, protected Azure resources, deployed worker instances, logged session records, local user accounts and so on.

The configuration backup is helpful if an appliance goes down for some reason. In this case, you can reinstall the appliance and quickly restore its configuration from a backup. You can also use a configuration backup to migrate the configuration of one backup appliance to another backup appliance in the Microsoft Azure infrastructure.

We recommend you to regularly perform configuration backup for every appliance present in the Veeam Backup & Replication infrastructure. Periodic configuration backups reduce the risk of data loss and minimize the administrative overhead costs in case any problems with an appliance occur.

NOTE

A Veeam Backup for Microsoft Azure appliance allows you to back up and restore the configuration directly from its Web UI. However, this functionality is disabled if the appliance is added to the Veeam Backup & Replication infrastructure. In this case, you can back up and restore the configuration from the Veeam Backup & Replication UI only.
Configuration Backup

When a Veeam Backup for Microsoft Azure appliance is added to the Veeam Backup & Replication infrastructure, Veeam Backup & Replication manages its configuration backup and restore. When Veeam Backup & Replication performs configuration backup, it backs up the configuration of the backup server and also configurations of all Veeam Backup for Microsoft Azure appliances added to the infrastructure.

By default, Veeam Backup & Replication performs configuration backup daily at 10.00 AM. However, in the default settings, the appliance configuration backup is disabled. To enable the appliance configuration backup, you must enable encryption as described in Performing Configuration Backup.

Backup File Formats and Locations

Backup files are stored in a folder in the backup repository specified in the configuration backup settings. The files have the following formats and are stored in the following folders:

- BCO for the Veeam Backup & Replication configuration. Such configuration backups are stored in the \VeeamConfigBackup\<backup server name> folder.
- BCAZ for the appliance configuration. Such configuration backups are stored in the \VeeamConfigBackup\Azure\<appliance name>_\<VB Instance ID> folders.

If the name of an appliance contains unsupported characters, these characters are replaced with the underscore symbol. This replacement is actual for the folder name and backup file names.

Limitations and Considerations

Mind the following considerations and limitations for configuration backup:

- To back up the configuration of Veeam Backup for Microsoft Azure appliances, you must enable the backup file encryption in the configuration backup settings. Otherwise, Veeam Backup & Replication will back up only the backup server configuration. By default, encryption is disabled.
- We do not recommend you to store configuration backups in the default backup repository or in any other folder on the backup server. In case the backup server fails, you will not be able to recover the failed backup server.
- You cannot store configuration backups in scale-out backup repositories, object storage repositories, Veeam Cloud Connect repositories and external repositories.
- If an appliance is unavailable or is out of a major version (compared to the version that Microsoft Azure Plug-in for Veeam Backup & Replication supports), the appliance configuration is excluded from the backup. For example, if Microsoft Azure Plug-in for Veeam Backup & Replication supports Veeam Backup for Microsoft Azure 5.0 and an appliance version is 4.0, the appliance configuration is skipped.
- During configuration backup, Veeam Backup & Replication processes three appliances at once and starts to process the next appliance as soon as one of those three appliances has already been processed.

Performing Configuration Backup

Before you perform configuration backup, check Limitations and Considerations.
You can perform configuration backup manually or instruct Veeam Backup & Replication to do it automatically on a regular basis:

- To instruct Veeam Backup & Replication to perform configuration backup automatically by schedule, follow the instructions provided in the Scheduling Configuration Backups section in the Veeam Backup & Replication User Guide.

- To create the configuration backup manually, follow the instructions provided in the Running Configuration Backups Manually section in the Veeam Backup & Replication User Guide.
Configuration Restore

Configuration restore can help in the following cases:

- The configuration database got corrupted, and you want to restore data from a configuration backup.
- A Veeam Backup for Microsoft Azure appliance got corrupted, and you want to recover its configuration to a new appliance.
- You want to roll back the configuration to a specific point in time.

Limitations and Considerations

Mind the following limitations and considerations for configuration restore:

- You can restore the configuration only to an appliance that is present in the Veeam Backup & Replication infrastructure.
- You cannot restore the configuration to an unavailable appliance or to an appliance whose major version is outdated.
- You must stop all policies that are currently running on the appliance to which you restore.
- You cannot restore the configuration to a new appliance if the original appliance is present in the Veeam Backup & Replication infrastructure.
- Sessions of policies that were running during backup are not restored.
- Veeam Backup & Replication allows you to restore the configuration to a new appliance if the original appliance is not present in the Veeam Backup & Replication infrastructure. However, we recommend you to stop the original appliance if it is present in the Microsoft Azure infrastructure. This is required because two different appliances must not be connected to the same backup repositories.
- The version of the appliance to which you restore the configuration must be the same or higher than the version of the backed-up appliance.
- The appliance to which you restore the configuration preserves its TLS certificate.
- [If you restore configuration to another appliance] During restore, parameters of the target appliance are overwritten. If you want to save the parameters, you must do it before you start configuration restore.
- [If you restore configuration to another appliance] During restore, Veeam Backup & Replication removes the appliance and its Blob storage backup repositories from the Veeam Backup & Replication infrastructure. If the restore fails, you need to re-add the appliance and its repositories to the Veeam Backup & Replication infrastructure.

Restoring Configuration

To restore the configuration, do the following:

1. Check limitations and considerations.
2. Launch the Configuration Restore wizard.
3. Select a repository and backup.
4. Review the backup file information.
5. Specify a password.
6. Select data to restore.
7. Specify credentials.
8. View restore session details.
9. Finish working with the wizard.
Step 1. Launch Configuration Restore Wizard

To launch the **Configuration restore** wizard, do the following:

1. Open the **Backup Infrastructure** view.
2. Click **Managed Servers > Microsoft Azure**.
3. Select a Veeam Backup for Microsoft Azure appliance to which you want to restore a configuration.
4. Click **Restore Configuration** on the ribbon. Alternatively, you can right-click the selected appliance and select **Restore configuration**.
Step 2. Select Backup

At the **Configuration backup** step of the wizard, from the **Backup repository** drop-down list, select the backup server or a backup repository where the configuration backup is stored. Then click **Browse** and select the necessary configuration backup.

If you select a backup in a backup repository, Veeam Backup & Replication copies this backup to a temporary folder on the backup server. Veeam Backup & Replication performs restore from this temporary file. After you finish the restore process and close the wizard, Veeam Backup & Replication deletes the temporary configuration file.
Step 3. Review Backup File Information

Veeam Backup & Replication analyzes the content of the selected backup and displays the following groups of settings:

- **Backup file** group shows settings of the configuration backup file.
- [For backup from backup repository] **Downloaded backup file** group shows where the temporary configuration backup is stored.
- **Product** group shows the version of Veeam Backup for Microsoft Azure installed on the Veeam Backup for Microsoft Azure appliance whose configuration you restore.
- **Catalogs** group shows the number of created policies, service accounts, repositories, sessions and so on.

At the **Backup Contents** step of the wizard review the provided information and click **Next** to confirm that you want to use the file for restore.
Step 4. Specify Password

At the **Password** step of the wizard, provide a password to decrypt the configuration backup.

If you forgot or lost the password, click the **I forgot the password** link. Note that this link is available only if password loss protection was enabled when the configuration backup was created and if the conditions described in the *Decrypting Data Without Password* section in the Veeam Backup & Replication Guide are met. There, you can also find instructions on how to decrypt data.
Step 5. Select Data to Restore

By default, Microsoft Azure Plug-in for Veeam Backup & Replication restores configuration data for existing infrastructure components, created backup policies and also the following data:

- **Local users** — data on local user accounts existing on the Veeam Backup for Microsoft Azure appliance. For more information on local users, see the Adding User Accounts section in the Veeam Backup for Microsoft Azure User Guide.

  If you exclude data on local users, Microsoft Azure Plug-in for Veeam Backup & Replication will not overwrite local users and the appliance to which you restore the configuration will have the already existing local users.

- **Session history** — data on policy sessions and restore sessions.

At the **Restore options** step of the wizard, ensure that check boxes are selected near the data you want to restore. If you want to exclude some data from restore, clear the necessary check boxes.

**NOTE**

[If you do not restore local users] After you click **Next**, the restore process will start. You will not be able to stop the process or edit the restore settings.
Step 6. Specify Credentials

[This step is available only if you have selected to restore data on local users.]

At the **Credentials** step of the wizard, select an account with administrative privileges that will be used to connect to the Veeam Backup for Microsoft Azure appliance after the configuration restore finishes. You have the following options:

- Select an existing account with administrative privileges that was created on the appliance whose configuration you restore. In this case, Microsoft Azure Plug-in for Veeam Backup & Replication will validate the specified credentials against the credentials stored in the configuration backup.

- Select a new account, that is, an account that is not present in the configuration backup. In this case, Microsoft Azure Plug-in for Veeam Backup & Replication will create a new local user account and assign administrative privileges to it.

If you have not added the credentials beforehand, click **Manage accounts** or **Add** to add the necessary credentials. For more information on adding credentials, see the **Credentials Manager** section in the Veeam Backup & Replication User Guide.

**NOTE**

After you click **Next**, the restore process will start. You will not be able to stop the process or edit the restore settings.
Step 7. View Restore Session Details

At the **Restore** step of the wizard, Microsoft Azure Plug-in for Veeam Backup & Replication shows the results of every step performed while executing the configuration restore. Wait for the restore process to complete and click **Next**.
Step 8. Finish Working with Wizard

At the **Summary** step of the wizard, check that the restore completed successfully and click **Finish**.

Configuration Restore

**Summary**

Review the configuration restore result, and click Finish to exit the wizard.

Remember to enable all jobs back once configuration data synchronization completes.

**Summary:**

Backup appliance configuration has been successfully restored.
Uninstalling Plug-In

If you uninstall Microsoft Azure Plug-in for Veeam Backup & Replication but do not remove appliances beforehand, the following will take place:

- You will be able to see snapshots. However, you will not be able to do anything with them.
- You will be able to see backups and perform data recovery operations for them (except disk export and application items restore). For more information on recovery operations, see Data Recovery. Note that restore to Microsoft Azure will work as described in the How Restore to Microsoft Azure Works section in the Veeam Backup & Replication User Guide.
- You will not be able to add and manage appliances.
- You will not be able to deploy Azure Blob storage.
- You will not be able to create and manage backup policies. You will be able only to remove backup policies from the Veeam Backup & Replication console.

To uninstall Microsoft Azure Plug-in for Veeam Backup & Replication:

1. From the Start menu of the machine where Microsoft Azure Plug-in for Veeam Backup & Replication is installed, navigate to Control Panel > Programs > Programs and Features.
2. In the list of installed programs, right-click Microsoft Azure Plug-in for Veeam Backup & Replication and select Uninstall.
3. In the opened window, click Remove.

![Uninstall dialog](image)
Installing and Uninstalling Plug-In in Unattended Mode

You can install or uninstall Microsoft Azure Plug-in for Veeam Backup & Replication in the unattended mode using the command line interface. The unattended mode does not require user interaction. You can use it to automate processes in large deployments.

Microsoft Azure Plug-in for Veeam Backup & Replication as Part of Veeam Backup & Replication Installation

If Microsoft Azure Plug-in for Veeam Backup & Replication is a part of Veeam Backup & Replication installation package, follow the instructions provided in the Installing Veeam Backup & Replication in Unattended Mode section in Veeam Backup & Replication User Guide.

Microsoft Azure Plug-in for Veeam Backup & Replication Separate Installation

If Microsoft Azure Plug-in for Veeam Backup & Replication is delivered as a separate .EXE file, use the instructions from this subsection.

Before you start unattended installation, perform the following actions:

1. Download the Microsoft Azure Plug-in for Veeam Backup & Replication .EXE file as described in Installing Plug-In (steps 1-4).
2. Check compatibility of Microsoft Azure Plug-in for Veeam Backup & Replication and Veeam Backup & Replication versions. For more information, see System Requirements.
3. Install Veeam Backup & Replication of the required version if it is not installed.
4. Log on to the target machine under the account that has the local Administrator permissions on the machine.

To install or uninstall Microsoft Azure Plug-in for Veeam Backup & Replication from the .EXE file, use a command with the following syntax:

```
%path% /silent /acceptheula /acceptthirdpartylicenses [/uninstall]
```

The command has the following parameters:

<table>
<thead>
<tr>
<th>Option</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%path%</td>
<td>Yes</td>
<td>Specifies a path to the installation .EXE file on the backup server or in a network shared folder.</td>
</tr>
<tr>
<td>Option</td>
<td>Required</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>/silent</td>
<td>Yes</td>
<td>Sets the user interface level to &quot;no&quot;, which means no user interaction is needed during installation.</td>
</tr>
<tr>
<td>/accepteula</td>
<td>Yes</td>
<td>Specifies that you want to accept the terms of the Veeam license agreement.</td>
</tr>
<tr>
<td>/acceptthirdpartylicenses</td>
<td>Yes</td>
<td>Specifies that you want to accept the terms of the license agreement for the 3rd party components.</td>
</tr>
<tr>
<td>/uninstall</td>
<td>No</td>
<td>Uninstalls the plug-in.</td>
</tr>
</tbody>
</table>

**Examples**

**Installing Microsoft Azure Plug-in for Veeam Backup & Replication**

The following command installs Microsoft Azure Plug-in for Veeam Backup & Replication.

```
AzurePlugin_11.0.4.465.exe /silent /accepteula /acceptthirdpartylicenses
```

**Uninstalling Microsoft Azure Plug-in for Veeam Backup & Replication**

The following command uninstalls Microsoft Azure Plug-in for Veeam Backup & Replication.

```
AzurePlugin_11.0.4.465.exe /silent /accepteula /acceptthirdpartylicenses /uninstall
```
Data Protection

With Microsoft Azure Plug-in for Veeam Backup & Replication, you can protect the following workloads:

- Azure VMs
- SQL databases
- Azure file shares

To protect these workloads, you need to create 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. For more information, see Creating Backup Policies.

After the policies are created, you can manage them as described in Managing Backup Policies.

Additional Data Protection Options for Azure VMs

Using the Veeam Backup & Replication console, you can also add an additional layer of protection for your infrastructure by creating backup copy jobs and backup to tape jobs for Azure VMs.

The backup copy jobs allow you to create and keep multiple instances of the same backed-up data in different locations. For more information, see Creating Backup Copy Jobs for Azure VMs.

The backup to tape jobs allow you to keep backups of VMs on tape devices. For more information, see Copying Azure VM Backups to Tapes.
Creating Backup Policies

When you create a backup policy, Veeam Backup & Replication redirects you to the Veeam Backup for Microsoft Azure Web UI where you can add a backup policy directly to Veeam Backup for Microsoft Azure. For more information on the backup policies, see the following sections in the Veeam Backup for Microsoft Azure User Guide:

- Performing Azure VM Backup
- Performing Azure SQL Backup
- Performing File Share Backup

To create a backup policy:

1. Launch the Add Policy wizard using one of the following instructions:
   - On the Home tab, navigate to Backup Job > Microsoft Azure and click VM, SQL or File share.
   - Open the Home view. In the inventory pane, right-click the Jobs node and select Backup > Microsoft Azure, then click VM, SQL or File share.

   If you have several Veeam Backup for Microsoft Azure appliances added to the Veeam Backup & Replication infrastructure, select the necessary appliance under the Microsoft Azure node.

2. Follow the instructions provided in one of the following sections in the Veeam Backup for Microsoft Azure User Guide:
   - Configuring Azure VM Backup
   - Configuring Azure SQL Backup
   - Configuring Azure File Share Backup
Managing Backup Policies

After you install Microsoft Azure Plug-in for Veeam Backup & Replication, you can use the Veeam Backup & Replication console to manage backup policies created with Veeam Backup for Microsoft Azure. You can start, stop, disable and delete backup policies directly in the Veeam Backup & Replication console.
Starting and Stopping Policies

You can start a backup policy manually. For example, if you want to create an additional restore point in the snapshot or backup chain and do not want to modify the configured backup policy schedule. You can also stop a running backup policy if processing of a workload is about to take too long, and you do not want the policy to produce heavy load on the production environment during business hours.

Starting Backup Policies

To start a backup policy:

1. Open the Home view.
2. In the inventory pane, select Jobs.
3. In the working area, select the necessary backup policies and click Start on the ribbon. Alternatively, right-click one of the selected backup policies and select Start.

Stopping Backup Policies

To stop a backup policy:

1. Open the Home view.
2. In the inventory pane, select Jobs.
3. In the working area, select the necessary backup policies and click **Stop** on the ribbon. Alternatively, right-click one of the selected backup policies and select **Stop**. In the displayed window, click **Yes**.

Veeam Backup for Microsoft Azure will not produce new restore points for workloads, which are added to a backup policy, but have not been processed by the time you stop the policy.
Editing Policy Settings

After you install Microsoft Azure Plug-in for Veeam Backup & Replication, you can edit settings of backup policies created in Veeam Backup for Microsoft Azure. For example, you can add more Azure VMs to a backup policy and change the backup policy description.

To edit a backup policy:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the backup policy that you want to edit, and click **Edit** on the ribbon. Alternatively, right-click the policy and select **Edit**. The **Edit Policy** wizard will open in your browser.
4. Depending on the type of the selected policy, edit the policy as described in one of the following sections in the Veeam Backup for Microsoft Azure User Guide:
   - Creating Azure VM Backup Policies
   - Creating Azure SQL Backup Policies
   - Creating Azure File Share Backup Policies
Disabling and Removing Policies

Microsoft Azure Plug-in for Veeam Backup & Replication allows you to temporarily disable or permanently delete backup policies created by Veeam Backup for Microsoft Azure. When you disable a backup policy, Veeam Backup for Microsoft Azure disables the schedule configured for the backup policy. This means that the backup policy will no longer start automatically. You can enable and start the disabled policy manually any time you need.

Disabling Backup Policies

You can disable a backup policy only if it has a schedule configured beforehand.

To disable a backup policy:

1. Open the Home view.
2. In the inventory pane, select Jobs.
3. In the working area, select the necessary backup policy and click Disable on the ribbon. Alternatively, right-click the necessary backup policy and select Disable.

TIP
To enable a disabled policy, select it and click Disable once again.

Deleting Backup Policies

To delete a backup policy created by Veeam Backup for Microsoft Azure:

1. Open the Home view.
2. In the inventory pane, select Jobs.
3. In the working area, select the necessary backup policy and click **Delete** on the ribbon. Alternatively, right-click the necessary backup policy and select **Delete**.
Managing Backed-Up Data

You can manage backed-up data in the following ways.

Removing Image-Level Backups and Snapshots

You can remove image-level backups and snapshots from Blob storage backup repositories only using the Web UI component of the Veeam Backup for Microsoft Azure appliance. For more information on how to delete snapshots and backups, see the Managing Backed-Up Data section in Veeam Backup for Microsoft Azure User Guide.

Decrypting Image-Level Backups

If you specify decryption passwords for standard backup repositories when adding a Veeam Backup for Microsoft Azure appliance, Veeam Backup & Replication automatically decrypts backup files stored in these repositories. If you do not specify decryption passwords, backup files remain encrypted.

To decrypt backup files:

1. Open the Home view.
2. In the inventory pane, navigate to Backups > External Repository (Encrypted).
3. In the working area, select a backup policy whose image-level backups you want to decrypt or select an individual backup. Then click Specify Password on the ribbon, or right-click one of the selected backups, and select Specify password.
4. In the Password field, enter a password.
   In the Hint field, you can see a hint for the password used to encrypt the backup files. Use this hint to recall the password.
Alternatively, you can specify a decryption password at the Container step of the Edit External Repository wizard. For more information on how to open the wizard, see the Editing Settings of External Repository section in the Veeam Backup & Replication User Guide.

Retrieving Data from Archive

To access data stored in an archive repository, you must first retrieve data. During the data retrieval process, a temporary copy of the archived data is created in a blob container where the archive repository resides. This copy is created in the hot or cool tier and stored for the period of time that you specify when launching the data retrieval process. For more information, see the Copy an archived blob to an online tier section in Microsoft Docs.

To launch the data retrieval process, do the following:

1. Launch the restore wizard as described in Launch Restore to Microsoft Azure Wizard or Launch Restore to Microsoft Azure SQL Wizard.
2. At the Machine or SQL Database step of the restore wizard, select a workload whose backup is stored in an archive repository. Click Next.
3. [If the backup is also stored in a standard repository] In the Confirm restore window, click Archive.
4. Confirm that you want to perform data retrieval by clicking Yes.
5. At the Retrieval Mode step of the Retrieve Backup wizard, select a method for data retrieval:
   - **Standard Priority.** The default priority method. The retrieved data will be available within about 15 hours.
   - **High Priority.** The faster, but more expensive priority method. The retrieved data will be available within about one hour. For example, if the size of a backup file is less than 10 GB.

For more information on priority options, see Microsoft Docs.
6. At the **Availability Period** step of the **Retrieve Backup** wizard, do the following:

   a. In the **Keep retrieved data available for** field, specify the number of days for which you want to keep the data available for restore operations.

   The data will be available during the day when the retrieval finishes plus the specified number of days. Each day starts at 12 AM and ends at 11:59 PM (in your appliance time zone). For example, if the data retrieval finished at 3 PM, June 6, and the number of days is set to 1, the data will be available till 11:59 PM, June 7.

   You will be able to **manually extend data availability** later if required.

   b. If you want to receive an email notification when data availability period is about to expire, select the **Send notification email** check box, and specify the number of hours before the expiration time when the notification must be sent.

   Check that you have configured **global email notification settings** as described in the **Configuring Global Email Notification Settings** section in the Veeam Backup & Replication User Guide.

7. At the **Summary** step of the **Retrieve Backup** wizard, review settings for data retrieval and click **Finish**.

   The retrieved data will be available on the **Home** view, in the **Data Retrieval** node of the inventory pane.

---

### Extending Data Availability

To extend time for which you want to keep retrieved data available for restore operations:

1. Open the **Home** view.

2. In the inventory pane, click the **Data Retrieval** node.

3. In the working area, select a workload for which you want to extend availability of the retrieved data.

4. On the ribbon, click **Extend Availability**. Alternatively, right-click the selected workload and click **Extend availability**.
4. In the opened window, specify the number of days for which you want to keep the data available for restore operations. Click **OK**.
Creating Backup Copy Jobs

Having just one backup does not provide the necessary level of safety. The primary backup of Azure VM may get lost together with production data, and you will have no backups from which you can restore data. Veeam Backup & Replication offers the backup copy functionality that allows you to create and keep multiple VMs of the same backup data in different locations.

Backup copy is a job-driven process. Veeam Backup & Replication fully automates the backup copy process and lets you specify retention settings to maintain the desired number of restore points, as well as full backups for archival purposes. For more information on the backup copy functionality, see the Backup Copy section in the Veeam Backup & Replication User Guide.

To create a backup copy job, do the following:

1. On the Home tab, click Backup Copy and select Azure IaaS backup.
2. Complete the New Backup Copy Job wizard as described in the Creating Backup Copy Jobs section in the Veeam Backup & Replication User Guide.
Copying Backups to Tapes

Storing data on tape devices helps you improve the level of safety and implement the 3-2-1 rule (3 copies, 2 types of media, 1 offsite location).

To administer all operations on tapes from your Veeam Backup & Replication console, Veeam Backup & Replication allows you to automate copying of image-level backups to tape devices and lets you specify scheduling, archiving and media automation options. For more information on the supported tapes and operations which you can perform with tapes, see the Tape Devices Support section in the Veeam Backup & Replication User Guide.

To copy Azure VM backups to tapes, do the following:

1. Check that you have copied Azure VM backups to on-premises repositories.
   
   If you have not copied the backups, follow the instructions provided in Creating Backup Copy Jobs.

2. Configure the tape infrastructure:

   a. Connect tape devices as described in the Tape Devices Deployment section in the Veeam Backup & Replication User Guide.

   b. Perform the initial configuration as described in steps 1–3 of the Getting Started with Tapes section in the Veeam Backup & Replication User Guide.

3. Create and complete a backup to tape job as described in the Creating Backup to Tape Jobs section in the Veeam Backup & Replication User Guide.
Viewing Statistics

After you install Microsoft Azure Plug-in for Veeam Backup & Replication, you can use the Veeam Backup & Replication console to view real-time statistics for any backup policy. Note that sessions for snapshots created manually in the Web UI component of an Veeam Backup for Microsoft Azure appliance are not displayed in the Veeam Backup & Replication console. For more information on how to review statistics, see the Viewing Real-Time Statistics section in the Veeam Backup & Replication User Guide.

**NOTE**

Veeam Backup & Replication does not show indexing session statistics. For more information on indexing, see the Configure Indexing Option section in Veeam Backup for Microsoft Azure User Guide.
Data Recovery

Veeam Backup for Microsoft Azure offers the following recovery options that you can run to restore Azure resources in various disaster recovery scenarios:

- **Restore to Microsoft Azure**
  Restore entire Azure VMs from cloud-native snapshots or image-level backups.

- **Restore to Microsoft Azure SQL**
  Restore entire Azure SQL databases from image-level backups.

- **Instant Recovery**
  Immediately restore Azure VMs to VMware vSphere or Hyper-V environment.

- **Restore to Amazon EC2**
  Restore Azure VMs from backups to Amazon EC2.

- **Restore to Nutanix AHV**
  Restore Azure VMs from backups to Nutanix AHV clusters.

- **Restore to Google Compute Engine**
  Restore Azure VMs from backups to Google Compute Engine.

- **VM Disk Export**
  Restore disks of Azure VMs from backups created by Veeam Backup for Microsoft Azure and convert them to disks in the VMDK, VHD or VHDX format.

- **VM Guest OS Files Restore**
  Recover individual guest OS files from Windows or Linux file systems.

- **Application Items Restore**
  Restore application items (Microsoft Active Directory, Microsoft Exchange, Microsoft SharePoint, and Microsoft SQL Server).
Restoring to Microsoft Azure

In case a disaster strikes, you can restore entire Azure VMs from cloud-native snapshots or image-level backups.

To restore VMs from cloud-native snapshots, Veeam Backup & Replication invokes native Azure capabilities. To restore VMs from image-level backups, Veeam Backup & Replication uses different algorithms depending on whether a Veeam Backup for Microsoft Azure appliance is present in the Veeam Backup & Replication infrastructure:

- If a Veeam Backup for Microsoft Azure appliance and Azure Blob storage connected to it are present in the Veeam Backup & Replication infrastructure, Veeam Backup & Replication uses the restore algorithm described in the How VM Restore Works section in the Veeam Backup for Microsoft Azure User Guide.

- If a Veeam Backup for Microsoft Azure appliance is not present in the Veeam Backup & Replication infrastructure and only Azure Blob storage connected to this appliance is present there, Veeam Backup & Replication uses the restore algorithm described in the How Restore to Microsoft Azure Works section in the Veeam Backup & Replication User Guide.

To restore VMs, do the following:

1. Launch the Restore to Azure wizard.
2. Select Azure VMs and restore points.
3. Specify a restore mode.
4. Specify an Azure subscription and region.
5. Specify VM names and resource groups.
6. Configure VM availability options.
7. Specify VM sizes.
8. Specify network and secure group settings.
9. Specify a restore reason.
10. Finish working with the wizard.
Step 1. Launch Restore to Microsoft Azure Wizard

To restore data from image-level backups or cloud-native snapshots, launch the **Restore to Microsoft Azure** wizard. However, we recommend that you restore Azure VMs from cloud-native snapshots. In this case, Veeam Backup & Replication will be able to invoke native Azure capabilities to make the restore process complete faster.

To launch the **Restore to Microsoft Azure** wizard, do one of the following:

- On the **Home** tab, click **Restore** and select **Microsoft Azure**. In the **Restore** window, select **Microsoft Azure IaaS > Restore from Microsoft Azure VM snapshot** if you want to restore from cloud-native snapshots, or **Microsoft Azure IaaS > Restore from Veeam backup** if you want to restore from image-level backups.

- Open the **Home** view. In the inventory pane, navigate to **Backups > External Repository** if you want to restore from image-level backups, or to **Backups > Snapshots** if you want to restore from cloud-native snapshots. In the working area, expand the necessary backup policy, select VMs that you want to restore and click **Microsoft Azure IaaS** on the ribbon. As an alternative, right-click one of the selected VMs and select **Restore to Microsoft Azure IaaS**.

![Restore](image)
Step 2. Select Azure VMs and Restore Points

At the Virtual Machine step of the wizard, select Azure VMs that you plan to restore and select a restore point for each VM:

1. On the right of the wizard window, click Add VM.

2. In the Backup Browser window, expand the necessary backup policy, select VMs that you want to restore and click Add.

3. By default, Microsoft Azure Plug-in for Veeam Backup & Replication recovers VMs to the latest state. However, if you want to restore VMs to an earlier state, do the following:
   a. In the Virtual machines to restore list, select the necessary VM and click Point.
   b. In the Restore Points window, select the restore point from which you want to restore the VM and click OK.

   [If you restore from image-level backups] Each restore point is marked with a flag of the related retention scheme type: the (R) flag is used to mark restore points created with daily retention, (W) — weekly, (M) — monthly, and (Y) — yearly.
Step 3. Choose Restore Mode

At the Restore Mode step of the wizard, choose whether you want to restore Azure VMs to the original or a new location, and select a service account that will be used for restore:

1. Choose where to restore VMs:
   - To restore VMs with initial settings to their original location, select Restore to the original location. If you select this option, you will proceed to the Reason step of the wizard.
   - To restore VMs to a different location or with different settings (such as subscription, network settings and so on), select Restore to a new location, or with different settings. If you select this option, the Restore to Microsoft Azure wizard will include additional steps for specifying the target Azure region and VM settings.

2. To select a service account, click Pick account to use and, in the Account window, select the account that will be used for restore. This account must have permissions listed in Required Permissions.

For a service account to be displayed in the drop-down list, it must be added as described in the Adding Azure Service Account section in the Veeam Backup for Microsoft Azure User Guide.
**Step 4. Specify Azure Subscription and Region**

[This step is available if you have selected the **Restore to a new location, or with different settings** option at the **Restore Mode** step of the wizard.]

At the **Subscription** step of the wizard, select a Microsoft Azure subscription and location to which you want to restore Azure VMs:

1. From the **Subscription** drop-down list, select a Microsoft Azure subscription that will be used to manage resources and costs for the restored VMs.
   
   For a subscription to be displayed in the **Subscription** list, it must be created and associated to your Azure account as described in Microsoft Docs.

2. From the **Region** drop-down list, select a region to which you want to restore VMs.

   If the selected region differs from the original VM location, you will see a warning message notifying that the locations do not match. Click **OK** to acknowledge the warning. Otherwise, you will not be able to proceed to the next step of the wizard.

   **NOTE**
   
   Data transfer to a new location may require additional costs and may take more time to complete.
Step 5. Specify VM Names and Resource Groups

[This step is available if you have selected the Restore to a new location, or with different settings option at the Restore Mode step of the wizard.]

At the Name step of the wizard, you can change resource groups and specify new names for restored VMs:

1. To change resource groups, do the following:
   a. In the Resource group list, select VMs whose resource groups you want to change and click Group.
   b. In the Resource group window, select the necessary resource group.
      For a resource group to be displayed in the Resource group list, it must be created as described in Microsoft Docs.

2. To rename VMs, do the following:
   a. In the Resource Group list, select VMs that you want to rename and click Name.
   b. In the Change Name window, specify a new VM name if you have selected one VM, or specify a suffix or prefix that will be added to VM names if you have selected multiple VMs. Click OK.

***IMPORTANT***
The VM name that you specify must follow Azure naming rules. Otherwise, the restore operation may fail. For more information on the naming rules, see Microsoft Docs.
Step 6. Configure VM Availability Options

[This step is available if you have selected the **Restore to a new location, or with different settings** option at the **Restore Mode** step of the wizard.]

At the **Availability Options** step of the wizard, you can specify in which availability zone or availability set to place restored Azure VMs, and which disk type to use:

1. [For unmanaged disks] To select a disk type that will be used with the restored VMs, do the following:
   a. In the **Virtual machines** list, select the necessary VM and click **Storage**.
   b. In the **Storage type** window, select the necessary **disk type**. For unmanaged disks, also select from the **Storage account** list an Azure storage account to which you want to restore disks of the selected VM.
   
   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.

2. To specify an availability set or zone, do the following:
   a. In the **Virtual machines** list, select the necessary VMs and click **Availability**.
   b. In the **Availability Options** window, do the following:
      - To place the VMs in an availability zone, select **Availability zone**. Then select the necessary zone.
        For zones available in the region that you have selected at the **Subscription** step of the wizard, see Microsoft Docs.
      - To include the VMs in an availability set, select **Availability set**.
        For an availability set to be displayed in the drop-down list, it must be created in the Azure portal. Also, the availability set must be in the same region and resource group as the restored VMs. Otherwise, the availability set may not be displayed.

**IMPORTANT**

You cannot include managed VMs into unmanaged availability sets, and unmanaged VMs into managed availability sets.
For more information on availability sets and zones, see [Microsoft Docs](https://docs.microsoft.com).

### Availability Options

Specify availability and storage type settings for the restored VM.

<table>
<thead>
<tr>
<th>Virtual machine:</th>
<th>Availability options</th>
<th>Storage type</th>
</tr>
</thead>
<tbody>
<tr>
<td>bp-lin-vm3</td>
<td>Managed</td>
<td>Managed</td>
</tr>
<tr>
<td>bp-image-1</td>
<td>Managed</td>
<td>Managed</td>
</tr>
</tbody>
</table>

Choose an availability and resiliency option for the restored VM.

- **Availability zone (survives a datacenter outage):**
  - Choose the number of availability zones.

- **Availability set (survives a host outage only):**
  - Choose the availability set.
Step 7. Specify VM Sizes

[This step is available if you have selected the Restore to a new location, or with different settings option at the Restore Mode step of the wizard.]

At the VM size step of the wizard, you can choose sizes and disk names for VMs that will be restored:

1. To change VM sizes, do the following:
   a. In the Virtual machine list, select the necessary VMs and click Edit.
   b. In the VM size window, select sizes for the restored VMs from the Size drop-down list. Click OK.

   For more information on VM sizes, see Microsoft Docs.

   **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.

2. To rename virtual disks, do the following:
   a. In the Virtual machine list, select the necessary VMs and click Disks.
   b. In the VM Disks window, select virtual disks that you want to restore and click Name.
   c. In the Change Name window, specify a new disk name if you have selected one disk, or specify a suffix or prefix that will be added to restored disk names if you have selected multiple disks. Click OK.
   d. In the VM Disks window, click OK.
Step 8. Specify Network and Secure Group Settings

[This step is available if you have selected the **Restore to a new location, or with different settings** option at the **Restore Mode** step of the wizard.]

At the **Network** step of the wizard, you can change network properties for restored VMs:

1. To change virtual networks and subnets, in the **Virtual machine** list, select the necessary VMs and click **Network**.

   In the **Virtual Network** window, do the following:

   a. From the **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 **Virtual network** list, it must be created as described in Microsoft Docs.

   b. From the **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 **Subnet** list, it must be created as described in Microsoft Docs.

   c. Click **OK**.

2. To change **network security groups**, in the **Virtual machine** list, select the necessary VMs and click **Group**.

   From the **Network security group** drop-down list, select a security group that will be associated with the specified subnet. Click **OK**.

   For a network security group to be displayed in the **Network security group** list, it must be created as described in Microsoft Docs.
Step 9. Specify Restore Reason

At the **Reason** step of the wizard, specify a reason for restoring Azure VMs. The information you provide will be saved in the session history and you can reference it later.
Step 10. Finish Working with Wizard

At the Summary step of the wizard, review the configured restore settings and click Finish.

If you want to start Azure VMs right after restore, select the Power on target VM after restoring check box.
Restoring to Microsoft Azure SQL

In case a disaster strikes, Microsoft Azure Plug-in for Veeam Backup & Replication allows you to restore Azure SQL databases from backups. For more information on how restore works, see the Performing Azure SQL Restore section in the Veeam Backup for Microsoft Azure User Guide.

To restore Azure SQL databases, do the following:

1. Launch the Restore to Microsoft Azure SQL Wizard.
2. Select Azure SQL databases and restore points.
3. Specify a restore mode.
5. Specify an Azure SQL database name.
6. Specify a restore reason.
7. Finish working with the wizard.
Step 1. Launch Restore to Microsoft Azure SQL Wizard

To launch the Restore to Microsoft Azure SQL wizard, do one of the following:

- On the Home tab, click Restore and select Microsoft Azure. In the Restore window, select Microsoft Azure SQL.

- Open the Home view. In the inventory pane, navigate to Backups > External Repository. In the working area, expand the necessary Azure SQL backup policy, select the databases that you want to restore and click Microsoft Azure SQL on the ribbon. Alternatively, you can right-click one of the selected databases and select Restore to Microsoft Azure SQL.
Step 2. Select SQL Databases and Restore Points

At the SQL database step of the wizard, select Azure SQL databases that you plan to restore and select a restore point for each SQL database:

1. On the right of the wizard window, click Add.
2. In the Backup Browser window, expand the necessary Azure SQL backup policy, select SQL databases that you want to restore and click Add.
3. By default, Microsoft Azure Plug-in for Veeam Backup & Replication recovers SQL databases to the latest state. However, if you want to restore Azure SQL databases to an earlier state, do the following:
   a. In the SQL database list, select the necessary SQL database and click Point.
   b. In the Restore Points window, expand the necessary Azure SQL backup policy, select the restore point from which you want to restore the Azure SQL database and click OK.

Each restore point is marked with a flag of the related retention scheme type: the (R) flag is used to mark restore points created with daily retention, (W) — weekly, (M) — monthly, and (Y) — yearly.
Step 3. Choose Restore Mode and Service Account

At the Restore Mode step of the wizard, choose whether you want to restore Azure SQL databases to the original or a new location and specify the service account settings:

1. Choose where to restore databases:
   - To restore databases with initial settings to their original location, select Restore to the original location.
     If you select this option, you will proceed to the Reason step of the wizard.
   - To restore databases to a different location or with different settings (such as subscription, network settings and so on), select Restore to a new location, or with different settings.
     If you select this option, the Restore to Microsoft Azure SQL wizard will include additional steps.

   NOTE
   If the backup from which you restore contains databases of multiple SQL servers and this backup was protected using a staging server, you can restore to the original location only databases of the SQL server that was used as a staging server. Other databases can be restored only to a new location or with different settings.

2. To select a service account, click Pick account to use and, in the Account window, select the account that will be used to access Azure resources. This account must have permissions listed in Required Permissions.

   For a service account to be displayed in the drop-down list, it must be added as described in the Adding Azure Service Account section in the Veeam Backup for Microsoft Azure User Guide.

![Restore to Microsoft Azure SQL](image)
Step 4. Specify Target SQL Server Settings

[This step is available if you have selected the *Restore to a new location, or with different settings* option at the *Restore Mode* step of the wizard.]

At the *Target server* step of the wizard, specify the target Azure SQL server and its settings:

1. In the *SQL database* list, select an Azure SQL database for which you want to configure the target SQL server and click *Server*.

2. In the *Target server* window, do the following:

   a. From the *SQL server* drop-down list, select the Azure SQL server or an Azure SQL Managed Instance to which Microsoft Azure Plug-in for Veeam Backup & Replication will restore the database.

   b. From the *Elastic pool* drop-down list, select a set of performance resources that you want to allocate to the restored Azure SQL database.

   **NOTE**
   Mind the following:
   - If you have not configured an elastic pool beforehand, you do not need to specify this setting.
   - This option applies only if you restore databases to Azure SQL server.

   c. From the *Account* drop-down list, select the Azure SQL account that will be used to access the server or managed instance. This account must have permissions listed in *Required Permissions*.

For an Azure SQL account to be displayed in the drop-down list, it must be created as described in the *Adding Accounts* section in the Veeam Backup for Microsoft Azure User Guide.
Step 5. Specify Name

[This step is available if you have selected the Restore to a new location, or with different settings option at the Restore Mode step of the wizard.]

By default, Microsoft Azure Plug-in for Veeam Backup & Replication restores an Azure SQL database with its original name. However, you can define a new name for the restored database if necessary.

To define a new name for the database:

1. In the Virtual machines list, select the necessary databases and click Name.

2. In the Change Name window, do the following:
   a. If you have selected one database, specify a name under which the database will be restored.
   b. If you have selected multiple databases, specify a prefix or suffix that will be added to the original names. For this, select the necessary check box and type the text to be added.

![Change Name window]

Select multiple databases to apply settings change in bulk.
Step 6. Specify Restore Reason

At the **Reason** step of the wizard, specify a reason for restoring Azure SQL databases. The information you provide will be saved in the session history and you can reference it later.

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

At the **Summary** step of the wizard, review the configured Azure SQL database restore settings and click **Finish**.
Restoring Microsoft Azure File Shares

Microsoft Azure Plug-in for Veeam Backup & Replication allows you to launch restore of Azure file shares. Restore is performed from cloud-native snapshots as described in the Performing Azure File Share Restore section in the Veeam Backup for Microsoft Azure User Guide.

To restore an Azure file share, do the following:

1. Open the Home view and navigate to the Backups > Snapshots node in the inventory pane.
2. In the working area, select an Azure file share and click Microsoft Azure Files on the ribbon. Alternatively, you can right-click the selected file share and click Restore to Microsoft Azure Files.

   Microsoft Azure Plug-in for Veeam Backup & Replication will redirect you to the appliance Web UI console, the Protected Data > Azure File page.
3. In the appliance Web UI console, select the check box next to the necessary Azure File Share.
4. Click Restore > File-Level Restore.
5. Complete the wizard as described in the Performing Azure File Share Restore section in the Veeam Backup for Microsoft Azure User Guide.
Performing Instant Recovery

Instant Recovery helps you immediately restore an Azure VM from an image-level backup to VMware vSphere or Hyper-V environment.

For more information on Instant Recovery to VMware vSphere, see the Instant Recovery section in the Veeam Backup & Replication User Guide for VMware vSphere. For more information on Instant Recovery to Hyper-V, see the Instant Recovery section in the Veeam Backup & Replication User Guide for Microsoft Hyper-V.

Instant Recovery to VMware vSphere

To perform Instant Recovery to VMware vSphere environment, do the following:

1. Check that you have added to the backup infrastructure a vCenter Server that will manage restored Azure VMs.
   
   If you have not added the server, follow the instructions provided in the Adding VMware vSphere Servers section in the Veeam Backup & Replication User Guide.

2. Launch and complete the Instant Recovery to VMware wizard.
   
   To do that, in the inventory pane, navigate to the Backups > External Repository node. In the working area, expand the necessary job, and select backups of Azure VMs that you want to recover. On the ribbon, click Instant Recovery > VMware vSphere. Then follow the instructions provided in the Performing Instant Recovery of Workloads to VMware vSphere VMs section in the Veeam Backup & Replication User Guide.

   **NOTE**
   
   When you perform Instant Recovery to VMware vSphere environment for Azure VMs, you will not be able to choose a restore mode and configure a helper appliance.
Instant Recovery to Hyper-V

To perform Instant Recovery to Hyper-V environment, do the following:

1. Check that you have added to the backup infrastructure a Microsoft Hyper-V server to which you plan to restore Azure VMs.

   If you have not added a Microsoft Hyper-V server follow the instructions provided in the Adding Microsoft Hyper-V Servers section in the Veeam Backup & Replication User Guide.

2. Launch and complete the Instant Recovery to Hyper-V wizard as described in Performing Instant Recovery of Workloads to Hyper-V VMs section in the Veeam Backup & Replication User Guide.

   **NOTE**
   
   When you perform Instant Recovery to Microsoft Hyper-V environment for Azure VMs, you will not be able to choose a recovery mode.
Restoring to Amazon EC2

Veeam Backup & Replication allows you to restore Azure VMs from image-level backups created with Veeam Backup for Microsoft Azure as Amazon EC2 instances. You can restore Azure VMs to any available restore point. For more information on restoring VMs to Amazon EC2, see the Restore to Amazon EC2 section in the Veeam Backup & Replication User Guide.

To restore Azure VMs as Amazon EC2 instances, do the following:

1. Check limitations and prerequisites listed in the Veeam Backup & Replication User Guide.
2. Launch and complete the Restore to Amazon EC2 wizard.

To do that, open the Home view and navigate to the Backups > External Repository node in the inventory pane. In the working area, select VMs that you want to restore. On the ribbon, click Amazon EC2. Then follow the instructions provided in the Restoring Machines section in the Veeam Backup & Replication User Guide.
Restoring to Nutanix AHV

Veeam Backup & Replication allows you to restore Azure VMs from image-level backups created with Veeam Backup for Microsoft Azure to Nutanix AHV clusters. You can restore VMs to any available restore point.

To perform restore to Nutanix AHV clusters, do the following:

1. Check that you have configured the backup infrastructure required for Veeam Backup for Nutanix AHV as described in the Deployment section in the Veeam Backup for Nutanix AHV User Guide.

2. Make sure that backups of the necessary Azure VMs are in an on-premises repository. If you have not copied the backup beforehand, follow the instructions from the Creating Backup Copy Jobs for VMs and Physical Machines section in the Veeam Backup & Replication User Guide.

To restore Azure VMs from backups stored in the archive tier of a scale-out backup repository, you do not need to copy backups to on-premises repositories. However, you must retrieve data as described in the Retrieving Backup Files section in the Veeam Backup & Replication User Guide.

3. Launch and complete the Restore to Nutanix AHV wizard.

   To do that, open the Home view after Veeam Backup & Replication finishes copying backups. In the inventory pane, navigate to the Backups > Disk (Copy) node. In the working area, expand the necessary job, and select backups of VMs that you want to recover. On the ribbon, in the Restore to AHV section, click Entire VM. Then follow the instructions provided in the Restoring VMs Using Veeam Backup & Replication Console section in the Veeam Backup for Nutanix AHV User Guide.
Restore to Google Compute Engine

Veeam Backup & Replication allows you to restore Azure VMs from image-level backups created with Veeam Backup for Microsoft Azure to Google Compute Engine (GCE). You can restore VMs to any available restore point. For more information on restoring VMs to GCE, see the Restore to Google Compute Engine section in the Veeam Backup & Replication User Guide.

To restore VMs to GCE, do the following:

1. Check limitations and prerequisites listed in the Veeam Backup & Replication User Guide.

2. Launch and complete the Restore to Google wizard.
   
   To do that, open the Home view and navigate to the Backups > External Repository node in the inventory pane. In the working area, select VMs that you want to restore. On the ribbon, click Google CE. Then follow the instructions provided in the Restoring Machines section in the Veeam Backup & Replication User Guide.
Exporting Disks

Veeam Backup & Replication allows you to restore disks of Azure VMs from image-level backups created with Veeam Backup for Microsoft Azure. You can restore disks in the VMDK, VHD or VHDX format. For more information on VM disks export, see the Azure VM Disk Export section in the Veeam Backup & Replication User Guide.

To restore disks of VMs and convert them to the VMDK, VHD or VHDX format:

1. Launch the Export Disk wizard. To do this, open the Home view. In the inventory pane, navigate to Backups > External Repository. In the working area, select VMs whose disk you want to export. On the ribbon, click Export Disks.

2. Complete the wizard as described in the Exporting Disks section in the Veeam Backup & Replication User Guide.
Restoring Guest OS Files

You can restore individual guest OS files and folders from image-level backups of an Azure VM. When restoring guest OS files, you do not need to extract image-level backups of VMs to a staging location, or start VMs prior to a restore. You can restore files and folders directly from image-level backups. For more information on guest OS file recovery, see the Guest OS File Recovery section in the Veeam Backup & Replication User Guide.

You can restore files from different guest OS file systems using the following methods.

Restoring from FAT, NTFS or ReFS

To restore guest OS files from FAT, NTFS or ReFS, do the following:

1. Check limitations and prerequisites listed in the Veeam Backup & Replication User Guide.
2. Launch and complete the File Level Restore wizard.
   To do that, open the Home view and navigate to Backups > External Repository. In the working area, select a VM whose files you want to restore. On the ribbon, click Guest Files (Windows). Then follow the instructions provided in the Restoring VM Guest OS Files (FAT, NTFS or ReFS) section in the Veeam Backup & Replication User Guide.

Restoring from Linux, Unix and Other File Systems

To restore guest OS files from Linux, Unix and other file systems, do the following:

1. Check limitations and prerequisites listed in the Veeam Backup & Replication User Guide.
2. Launch and complete the Guest File Restore wizard.
   To do that, open the Home view and navigate to Backups > External Repository. In the working area, select a VM whose files you want to restore. On the ribbon, click Guest Files (Other). Then follow the instructions provided in the Restoring VM Guest OS Files (Multi-OS) section in the Veeam Backup & Replication User Guide.
Restoring from Other File Systems

You can restore files from systems other than those listed in the File-Level Restore section in the Veeam Backup & Replication User Guide. For this purpose, use the Instant Recovery technology. To learn how to use this technology to restore files, follow the instructions provided in the Restore from Other File Systems section in the User Guide for Microsoft Hyper-V.
Restoring Application Items

Veeam Backup & Replication provides auxiliary tools called Veeam Explorers that allow you to restore application items directly from image-level backups of Azure VMs.

You can restore items of the following applications:

- Microsoft Active Directory
- Microsoft Exchange
- Microsoft SharePoint
- Microsoft SQL Server
- Oracle Database

To restore application items from backups of Azure VMs:

1. Launch the restore wizard. To do that, open the Home view. In the inventory pane, navigate to Backups > External Repository. In the working area, select the necessary VM backup, click Application Items on the ribbon and select the necessary application.

2. Complete the restore wizard. To extract the application databases from the backup and open it in the Veeam Explorer, perform the following steps:
   a. At the Restore Point step of the wizard, select a restore point from which you want to restore application items.
   b. At the Reason step of the wizard, enter the information on the restore reason for future reference.
   c. At the Summary step of the wizard, review the information on the Azure VM whose application items you want to restore.

Veeam Backup & Replication will open the Veeam Explorer console to select the application that will allow you to restore application items from the selected backup or snapshot.
IMPORTANT

Mind the following:

- To be able to restore application items in the Veeam Explorer console, you must manually attach the database that you want to restore. For details on working with Veeam Explorers, see Veeam Explorers User Guide.
- The backup from which you want to restore must be application-consistent. For details on enabling the application-consistent backups, see the Enable Application-Aware Processing section in the Veeam Backup for Microsoft Azure User Guide.
Viewing Statistics

Microsoft Azure Plug-in for Veeam Backup & Replication allows you to view statistics on data recovery operations that Veeam Backup & Replication perform to recover, restore and export Azure resources. You can view the information on the restore reason, the parameters of the restored Azure resources, the logs of the restore session and so on.

Veeam Backup & Replication provides information on the following recovery operations that are initiated from Veeam Backup for Microsoft Azure:

- Entire Azure VM restore
- SQL database restore
- Disk restore
- File-level restore

To view the restore session statistics, do one of the following:

- Open the Home view, in the inventory pane select Last 24 hours. In the working area, double-click the necessary restore session.
  Select the session and click Statistics on the ribbon or right-click the session and select Statistics.

- Open the History view, in the inventory pane select Restore. In the working area, double-click the necessary restore session.
  Select the session and click Statistics on the ribbon or right-click the session and select Statistics.

The restore session window will display the following information on restore sessions:

- The top of the window will show general session statistics: a name of the machine whose data is restored, the account under which the session was started, the session status and duration details.

- The Reason tab will show the restore reason that was specified when running the restore.

- The Parameters tab shows information about the restore point selected to restore the files.
- The **Log** tab shows a list of operations performed during the session.

```
<table>
<thead>
<tr>
<th>Message</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Starting File-level Recovery for bp-lin-vm3</td>
<td>0:01:07</td>
</tr>
<tr>
<td>Using worker VBA-ac725a61-009d-4338-9f6-d6ee4f8e771f for restore</td>
<td></td>
</tr>
<tr>
<td>Mounting restore point completed successfully</td>
<td>0:03:06</td>
</tr>
<tr>
<td>File-level Recovery browser is ready to work. The link is available on</td>
<td></td>
</tr>
<tr>
<td>the Protected...</td>
<td></td>
</tr>
</tbody>
</table>
```
# Features and Plug-In Versions

The following table shows major features that were added in each version of Microsoft Azure Plug-in for Veeam Backup & Replication:

<table>
<thead>
<tr>
<th>Microsoft Azure Plug-in for Veeam Backup &amp; Replication version</th>
<th>Features</th>
</tr>
</thead>
</table>
| 11.0.2.x                                                        | - Connecting and deploying an appliance  
|                                                                 | - Deploying standard backup repositories  
|                                                                 | - Azure VM protection  
|                                                                 | - Restore of Azure VMs  
|                                                                 | - Azure user account in the Government region (11.0.2.167)  |
| 11.0.3.x                                                        | - SQL database protection  
|                                                                 | - Restore of SQL databases  
|                                                                 | - Deploying archive repositories  |
| 11.0.4.x                                                        | - Backup and restore of the appliance configuration  
|                                                                 | - Restore of Azure file shares  |
Support Information

If you have any questions or issues with Microsoft Azure Plug-in for Veeam Backup & Replication, Veeam Backup & Replication or 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, we recommend you provide information on the installed products to the Veeam Customer Support Team. Product logs contain this information.

To export logs, do the following:

1. From the main menu of the Veeam Backup & Replication console, select Help > Support Information.
2. At the Scope step of the Export Logs wizard, select Export all logs for selected components.
3. In the Managed servers list, select the Veeam Backup & Replication server, Veeam Backup for Microsoft Azure appliances and other components for which you want to export logs.
4. Complete the wizard as described in the Export Logs section in the Veeam Backup & Replication User Guide.