Veeam Backup for Microsoft Azure v6 Release Notes

This document provides last-minute information on Veeam Backup for Microsoft Azure v6, including system requirements, installation, as well as relevant information on technical support, documentation, online resources and so on.

The GA version of Veeam Backup for Microsoft Azure v6 is available starting from December 5th, 2023.

See next:

What's New

Veeam Backup for Microsoft Azure delivers Azure-native, fully automated backup and recovery to easily protect and manage all your Azure data. For the list of new features introduced in version 6, see the Veeam Backup & Replication What's New document.

System Requirements

Hardware

Standard_B2s or Standard_B2ms are the recommended VM sizes for the backup appliance:

- *CPU:* 2 cores (minimum)
- *Memory:* 4 GB (minimum)

Note: if you want to protect a large number of Azure VMs, please choose a bigger Azure VM size.

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

For the latest recommendations on deployment sizing, see the Sizing and Scalability Guidelines section in the Veeam Backup for Microsoft Azure User Guide.

Workers

Standard_F2s_v2 is the recommended and default worker size for standard backup.

Standard_E2_v5 is the recommended and default worker size for archive backup.

Software

Latest versions of Microsoft Edge, Mozilla Firefox or Google Chrome are required to access the Veeam Backup for Microsoft Azure Web UI from your local machine.

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

- Ubuntu 22.04 LTS
- ASP.NET Core Runtime 6.0
- PostgreSQL 15.5
- nginx 1.24
- libpam-google-authenticator 20191231-2
- Veeam Backup for Microsoft Azure installation packages

Installing Veeam Backup for Microsoft Azure

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

For the detailed step-by-step installation procedure, see the Deployment section in the Veeam Backup for Microsoft Azure User Guide.

Upgrading Veeam Backup for Microsoft Azure

To upgrade Veeam Backup for Microsoft Azure to the next version, the backup appliance must be running version 3 or later. The upgrade can be performed only using Microsoft Azure Plug-in for Veeam Backup & Replication.

To install available security and OS updates, download and install them from the appliance Web UI. For more information, see section Updating Veeam Backup for Microsoft Azure in the Veeam Backup for Microsoft Azure User Guide.

Integration with Veeam Backup & Replication

This section provides last-minute information about Microsoft Azure Plug-in for Veeam Backup & Replication 12.6.0.1009, including system requirements and deployment, as well as relevant information on technical support, documentation, online resources and so on.

The Microsoft Azure Plug-in for Veeam Backup & Replication is available for download starting from December 5th, 2023. You can download the plug-in at the Veeam Backup & Replication: Download page: **Additional Downloads** section, **Cloud Plug-ins** tab.

After you install Microsoft Azure Plug-in for Veeam Backup & Replication, you must add a Veeam Backup for Microsoft Azure appliance to the Veeam Backup & Replication infrastructure. For details, see section Adding Appliances in the Veeam Backup for Microsoft Azure User Guide.

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 requirements for the Veeam Backup & Replication server.

Veeam Backup & Replication

Microsoft Azure Plug-in for Veeam Backup & Replication supports integration with Veeam Backup & Replication version 12.1.

Veeam Backup for Microsoft Azure

Microsoft Azure Plug-in for Veeam Backup & Replication supports integration with Veeam Backup for Microsoft Azure version 6.

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 Veeam Backup for Microsoft Azure User Guide.

Licensing

Veeam Backup for Microsoft Azure is licensed using the Veeam Universal License (VUL) installed on the Veeam Backup & Replication server. For more information on Veeam licensing terms and conditions, see Veeam End User License Agreement (EULA).

Standalone version of Veeam Backup for Microsoft Azure is available in 2 editions:

- Veeam Backup for Microsoft Azure Free Edition is available exclusively through the Microsoft Azure Marketplace and allows you to protect up to 10 workloads free of charge.
- Veeam Backup for Microsoft Azure BYOL Edition is available exclusively through the Microsoft Azure Marketplace.

Known Issues

General

- During backup policy creation, the **Cost Estimation** step of the wizard may display an incomplete list of protected Azure VMs. To resolve the issue, click **Rescan** at the **Sources** step of the backup policy wizard.
- Cost estimation calculation can be slow when a large number of snapshots is defined.
- To retrieve a tenant name, the Azure AD application must have the *Organization.Read.All* Graph permission assigned.
- Due to the lack of the required Azure SDK API calls, the backup appliance can only create an Azure Service Bus Service with minimum TLS 1.0. However, for communication purposes, TLS 1.2 is used.
- Under certain conditions, large bundled support logs may fail to be downloaded. To resolve the issue, collect only specific logs requested by the Veeam Customer Support Team.
- When you enable the **Private network deployment** option with no Azure service accounts added to the backup appliance, the operation fails with an error persisting even after adding the required service account. To resolve the issue, switch between the messaging services or deployment modes.
- The cost calculator may return zero values for backup policies when using containers as a source for backups. This happens when the initial discovery process has not been completed yet. To resolve this issue, wait for 5-10 minutes and re-launch the policy wizard to review the cost estimation data.
- When editing a service account using the **Renew application** option, the **Export** button on the **Permission Check** step does not allow exporting the required permissions. As a workaround, run the permissions check for the selected account from the **Account** page and export the permissions from the opened dialog.
- For appliances deployed in the Poland Central region, switching to the Service Bus messaging service might fail due to the inability to create a Service Bus namespace. To address this, manually create the namespace in Microsoft Azure, assign the 'Veeam backup appliance ID' tag to the namespace, and then proceed with the switch of the service.
-

Infrastructure

- By default, Veeam Backup for Microsoft Azure does not download and check the CRL file of the storage account when creating a repository. To enable the check, contact the Veeam Customer Support Team.
- If you enable boot diagnostics with managed storage account on worker instances, Microsoft Azure creates a dedicated storage account. This account will not be automatically removed by the backup appliance after the worker is deallocated.

Upgrade

- The **Backup Size** column on the **Protected Data** tab will not display any values until a backup policy protecting the corresponding resource runs successfully at least once.
- After upgrading from v4 or earlier, backup policies with enabled archives may temporarily display a question mark in the **Transaction** column on the **Cost Estimation** step. This issue gets resolved after the first successful policy run.
- After upgrading from v5 or earlier, the security and package updates are not installed on the backup appliance automatically. To resolve this issue, update the appliance manually as described in section Installing Updates in the Veeam Backup for Microsoft Azure User Guide.

Backup

- The default worker profile (Standard_F2s_v2) may run out of memory after creating 100 or more restore points. To resolve the issue, use a different worker profile.
- If you change the selected service account in the backup policy settings, it is required to restart the backup service to apply the changes.
- When operating in the private deployment mode, to perform Azure VM backup within the subscription in which the backup appliance is deployed, the service account used to deploy workers must be assigned Azure VMs: snapshot, backup and Azure VMs: restore roles in addition to the worker management role.
- A backup appliance cannot detect Azure VM snapshots created by other backup appliances. This limitation does not apply when restoring a configuration backup to a new appliance.
- It may take up to 10 minutes for Veeam Backup for Microsoft Azure to connect to a staging server when processing Azure SQL Managed instances.
- When backing up Azure SQL Managed instances using a staging server, both the Azure SQL backup and Azure SQL restore roles must be assigned to the service account selected in the policy settings.
- Due to Microsoft limitations, backup policies protecting Windows-based Azure VMs with the enabled guest processing option notify on success even if the PowerShell script fails. To work around the issue, add necessary exceptions to the script.
- Storage accounts with the Premium file shares type cannot be selected in the Add Azure Files Policy wizard. To work around the issue, explicitly include file shares deployed in these accounts to the policy scope.

Restore

- When restoring an Azure VM that contains a cloud-init script, the script becomes active during the first boot.
- When restoring an Azure VM with Ultra disk capability enabled, even without Ultra disks attached, restore may fail unless VM is restored to a region and availability zone that supports Ultra disks.
- When restoring an Azure VM with multiple network interfaces to a different location, only 2 network interfaces are restored.
- When restoring an Azure VM, all restored network interfaces will be in the same subnet and network security group that are assigned to the primary network interface.
- If an Azure VM belongs to a proximity group, Veeam Backup for Microsoft Azure restores the VM without the relation to the group.
- When restoring a VM to the original location, the disks are always restored to the resource group of the source VM, even if the source disks originally belonged to a different resource group.
- Veeam Backup for Microsoft Azure cannot perform in-guest file recovery for Azure VMs that are encrypted by using Azure Disk Encryption.
- Veeam Backup for Microsoft Azure cannot recover files of Windows-based Azure VMs with the ReFS file system.
- File-level recovery to the original location is not supported for Azure VMs with the ARM architecture.
- When restoring files to the original location, the notification bell incorrectly displays a Success status even if the operation fails. However, the **Session Log** page accurately reflects the operation status.
- Veeam Backup for Microsoft Azure ignores Microsoft Azure locks on existing databases when restoring databases to the original location.
- When restoring databases to the original location, replication and failover group settings for databases are not preserved.
- If a service account used by a backup policy for creating VM snapshots is removed, the entire VM and disk restore from these snapshots might fail. To resolve the issue, either manually rescan the region

where the snapshots are located or wait for the automatic infrastructure rescan performed every 24 hours.

Configuration Restore

- Under certain circumstances, the worker configuration check performed during the configuration restore may fail when using service and repository accounts from the same tenant with a different set of permissions. No user action is required.
- Connection to the backup appliance using SSH fails if the original user is no longer present in the OS list of users after the configuration restore.
- Under certain circumstances, the repository check performed after the configuration restore may fail when some Azure SQL resources were deleted but are still registered in the configuration backup. To resolve the issue, click **Recheck** at the **Configuration Check** step of the restore wizard.
- After the configuration restore, the backup appliance does not re-create Service Bus premium namespaces automatically. To resolve this, disable the private deployment mode and then enable it again.
- When restoring a configuration backup containing numerous virtual network restore points, there might not be enough space on the data disk to start the restore. To resolve this, increase the data disk size in Microsoft Azure and expand the ext4 partition on the data disk.

REST APIs

- To review the detailed change log and breaking changes in the REST API v6, see the Veeam Backup for Microsoft Azure REST API Reference.

Veeam Backup & Replication Integration

- When you deploy Veeam Backup for Microsoft Azure from the Veeam Backup & Replication console, the default service account is automatically created on the backup appliance. It is connected to the same AD application as the Azure compute account used for deployment, and shares the same permissions. For more information, see the Veeam Backup for Microsoft Azure User Guide.
- When deploying a backup appliance from the Veeam Backup & Replication console, available updates are also installed on the created Azure VM. If the update fails, the backup appliance might not be added to the backup infrastructure automatically. To resolve the issue, add it manually as described in section Connecting to Existing Appliances in the Veeam Backup for Microsoft Azure User Guide.
- Job and job session reports are not supported for backup policies created in Veeam Backup for Microsoft Azure.
- When removing the backup appliance from the Veeam Backup & Replication infrastructure, you also remove all Blob Storage backup repositories for which credentials are not set. To remove the connected resources from Microsoft Azure, see section Removing Appliances in the Veeam Backup for Microsoft Azure User Guide.
- Backups and snapshots of Azure VMs, Azure SQL, Azure Files and Azure virtual network configurations cannot be removed using the Veeam Backup & Replication console.
- Running configuration restore sessions are not displayed in the list of system sessions in the Veeam Backup & Replication console.
- Azure compute account must be re-added to the backup console if it was registered as an existing one in Veeam Backup & Replication v11 and earlier.
- Backup and snapshot size for restore points created by backup appliances is not displayed in the Veeam Backup & Replication console.
- If a user in Veeam Backup & Replication is assigned several roles, the user will be able to perform Veeam Backup for Microsoft Azure operations available to the role with the highest priority. Thus, if the user

has both the Veeam Backup Operator and Veeam Restore Operator roles, this user will act as the restore operator.

- When removing the backup appliance with the **Delete cloud resources associated with the backup appliance?** check box selected, Veeam Backup & Replication will also remove the network security group that might be shared with other user resources.

Technical Documentation References

If you have any questions about Veeam Backup for Microsoft Azure, use the following resources:

- Product web page
- Veeam Backup for Microsoft Azure documentation
- Veeam R&D forums

Technical Support

Veeam offers email and phone technical support for customers on maintenance and during the official evaluation period. For better experience, please provide the following information when contacting Veeam Customer Support:

- Version information for the product and all infrastructure components
- Error message and/or accurate description of the problem you are having
- Log files

> **TIP**
> To export the log files, select **Support Information** > **Download Logs** from the configuration menu, click **Download Logs**, and specify a time interval for which the logs must be collected.

To submit your support ticket or obtain additional information, please visit the Veeam Customer Support Portal. Before contacting Veeam Customer Support, consider searching for a resolution on Veeam R&D Forums.

Contacting Veeam Software

At Veeam Software, we pay close attention to comments from our customers — we make it our mission to listen to your input, and to build our products with your suggestions in mind. We encourage all customers to join Veeam R&D Forums and share their feedback directly with the R&D team.

Should you have a technical or licensing issue or question, please feel free to contact our Customer Support organization directly. We have qualified technical and customer support staff available 24/7 who will help you with any inquiry that you may have.

Customer Support

For the most up-to-date information about our support practices, business hours and contact details, please visit the Veeam Customer Support Portal.

Company Contacts

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