Veeam Backup for Microsoft Azure 5a Release Notes

This document provides last-minute information on Veeam Backup for Microsoft Azure 5a, 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 5a is available to deploy from the Microsoft Azure Marketplace starting from May 30th, 2023.

See next:

- System Requirements
- Installing Veeam Backup for Microsoft Azure
- Upgrading to Veeam Backup for Microsoft Azure 5a
- Updating Veeam Backup for Microsoft Azure
- Integration with Veeam Backup & Replication
- Licensing
- Known Issues
- Technical Documentation References
- Technical Support
- Contacting Veeam Software

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 Best Practices 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
- 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. Veeam Backup for Microsoft Azure is available on the Microsoft Azure Marketplace.

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

Configuring Initial Settings

Right after installation, you must perform the initial configuration of Veeam Backup for Microsoft Azure. As part of this configuration, you must read and accept the license agreement, prove that you are the owner of the Azure VM running Veeam Backup for Microsoft Azure, generate a new web certificate and download product updates.

For the detailed step-by-step configuration procedure, see the Veeam Backup for Microsoft Azure User Guide.

Upgrading to Veeam Backup for Microsoft Azure 5a

To perform upgrade of Veeam Backup for Microsoft Azure to version 5a, the backup appliance must be running version 3.0 or later. During upgrade to version 5a, the backup appliance operating system will be updated to Ubuntu 22.04 LTS and version of configuration database will be updated to PostgreSQL 15.

Upgrade to version 5a requires certain actions carried out externally to the backup appliance, including re-deployment of the backup appliance on a new Azure VM and attachment of data disks from the previous backup appliance to this new Azure VM, and can be performed only using Microsoft Azure Plug-in for Veeam Backup & Replication. For more information, see section Upgrading to Veeam Backup for Microsoft Azure 5a in the Veeam Backup for Microsoft Azure User Guide.

Updating Veeam Backup for Microsoft Azure

It is recommended that you timely install available package updates to avoid performance issues while working with the product. Veeam Backup for Microsoft Azure allows you to check for new product versions and available package updates, download and install them from the 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 12.1.5.99, 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 May 30th, 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 the Integration with Veeam Backup & Replication 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.

Veeam Backup for Microsoft Azure

Microsoft Azure Plug-in for Veeam Backup & Replication supports integration with Veeam Backup for Microsoft Azure version 5a.

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 available in 2 editions: Free and BYOL.

Veeam Backup for Microsoft Azure Free Edition

Veeam Backup for Microsoft Azure Free Edition is available exclusively through the Microsoft Azure Marketplace.

Veeam Backup for Microsoft Azure Free Edition is fully featured and allows you to protect up to 10 Azure VMs free of charge.

Veeam Backup for Microsoft Azure BYOL Edition

Veeam Backup for Microsoft Azure BYOL Edition is available exclusively through the Microsoft Azure Marketplace.

Veeam Backup for Microsoft Azure BYOL Edition can be licensed using either the Veeam Universal License (VUL) or a separate license that can be obtained by contacting sales or opening a license case support ticket.

In case of integration with Veeam Backup & Replication, licensing of protected workloads is done on the Veeam Backup & Replication side.

For more information on Veeam licensing terms and conditions, see Veeam End User License Agreement (EULA).

Known Issues

General

- When using multiple accounts pointing to the same subscription, Veeam Backup for Microsoft Azure uses the account added first as the main account.
- 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 Azure Active Directory 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 Veeam 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 Veeam backup appliance, the option remains in the *Enabling* state. To resolve the issue, restart the Veeam backup service.
- GZRS or RA-GZRS storage accounts are not supported for creating archive repositories.
- 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.
- A single backup repository cannot be shared between multiple backup appliances.

Infrastructure

- When copying data from one blob container to another using the Microsoft Azure Portal, the import operation to Veeam Backup for Microsoft Azure as a new repository fails.

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.

UI

- Storage tier UI filters for repositories that infer a storage account access tier cannot be applied on the Repository and Restore Points tabs.

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.
- A Veeam backup appliance cannot detect Azure VM snapshots created by other Veeam 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.
- Due to Microsoft limitations, backup policies protecting Windows-based Azure VMs with enabled guest processing option notify on success even if the PowerShell script fails. To work around the issue, add necessary exceptions to the script.
- Backup health check cannot be performed for encrypted backups with missing metadata files.

- Backup health check cannot be performed for backups with corrupted metadata files.
- Switching or using service accounts from different Microsoft Azure tenants is not supported for a backup policy.

Restore

- When restoring an Azure VM that contains a cloud-init script, the script becomes active during the first boot.
- 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.
- If an Azure VM belongs to a proximity group, Veeam Backup for Microsoft Azure restores the VM without the relation to the group.
- 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.

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 Veeam 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.

Indexing

- To use the Azure Files indexing option, NTLM v2 & SMB 3.0 must be enabled for the selected file shares.

REST APIs

- To review the detailed change log and breaking changes in the REST API v3, see the Veeam Backup for Microsoft Azure REST API Reference.

Licensing

- License keys are not automatically revoked when Azure Files are manually deleted on the **Protected Data** page. To resolve the issue, revoke the license keys manually.

Veeam Backup & Replication Integration

- When you deploy Veeam Backup for Microsoft Azure from the Veeam Backup & Replication console, the service account used by the Veeam backup appliance is created with the *Application Owner* role in Microsoft Azure instead of a role with granular permissions.
- Only the last 24 hours of sessions are synchronized when registering the Veeam backup appliance in Veeam Backup & Replication.
- Job and job session reports are not supported for backup policies created in Veeam Backup for Microsoft Azure.

- If credentials to a Microsoft Azure Blob storage are not specified, encrypted backups will be displayed as non-encrypted ones (there will be no key on the backup icons).
- If credentials to a Microsoft Azure Blob storage are not specified, only full VM restore is available. All other features (backup copy, export disk, and so on) are disabled.
- Only VM restore is available using restore points from archive repositories.
- After you change the way a backup repository is encrypted, all restore points retained in this repository are shown as *Encrypted*. To resolve the issue, update the encryption options for the repository.
- When removing the Veeam 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 the Integration with Veeam Backup & Replication Guide.
- Veeam Backup Enterprise Manager does not support management of policies created in Veeam Backup for Microsoft Azure.
- VM disk restore to the original location is not available from the Veeam Backup & Replication console.
- File-level restore to the original location is not available from the Veeam Backup & Replication console.
- File-level restore from cloud-native snapshots is not available from the Veeam Backup & Replication console.
- Backups and snapshots of Azure VMs, Azure SQL and Azure Files cannot be removed using the Veeam Backup & Replication console.
- If you change the password of a portal user registered in the Microsoft Azure Plug-in, you must also change the user password in the Veeam Backup & Replication console. Otherwise, the connection will not be established.
- When you remove a backup repository from a managed Veeam backup appliance, this repository is not removed from the Veeam Backup & Replication console automatically. To resolve the issue, remove the repository manually.
- To discover new backup repositories created in the Veeam backup appliance, complete the **Edit appliance** wizard in the Veeam Backup & Replication console.
- Running configuration restore sessions are not displayed in the list of system sessions in the Veeam Backup & Replication console.
- The availability time of backups retrieved from an archive storage tier cannot be extended when using Veeam Backup & Replication — use the Veeam backup appliance UI instead.
- Azure compute account must be re-added to the backup console if it was registered as an existing one in Veeam Backup & Replication v12.
- Backup and snapshot size for restore points created by Veeam backup appliances is not displayed in the Veeam Backup & Replication console.
- Restore sessions cannot be stopped by backup and restore operators when using the Veeam Backup & Replication console.
- Azure applications created using the Veeam Backup & Replication console do not have an owner account specified.
- Backup appliance UI-related actions cannot be initiated when connecting to the tenant's backup server using the remote Veeam Backup & Replication console.
- Azure Compute accounts that are using certificates for authentication cannot be used by the Veeam Backup & Replication server.
- After a failed backup appliance upgrade, the rollback procedure will report an error status even though the rollback procedure succeeds. This happens when the backup appliance is configured with Availability zones.
- Export of support logs from backup appliances may fail if the managing backup server is running Microsoft Windows Server 2016 or earlier versions.

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
- Microsoft Azure Plug-In for Veeam Backup & Replication 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** > **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.