

Veeam Backup & Replication

What's New in 9.5 Update 4?

Veeam® Backup & Replication™ 9.5 Update 4, part of Veeam Availability Suite™, delivers Availability for ALL your virtual, physical and cloud-based workloads. Through a single management console, you can manage fast, flexible and reliable backup, recovery and replication of all your applications and data to eliminate legacy backup solutions forever. The following is a list of the major new features and functionalities added in Update 4.

Native Object Storage Support with Veeam Cloud Tier

Veeam Cloud Tier provides scale-out backup repository with unlimited capacity for long-term data retention by using native, cost-effective object storage integrations with Amazon S3, Azure Blob Storage, IBM Cloud Object Storage, as well as numerous S3-compatible service providers and on-premises storage solutions.

Veeam Cloud Tier is implemented as a new storage tier within the scale-out backup repository (SOBR) – the Capacity Tier. It is configured with a policy that automatically tiers backup files to object storage as they age out of the operational restore window, with an option to start tiering the oldest backup files sooner should SOBR's Performance Tier start running out of free disk space.

When using public cloud object storage, your data can be protected with optional source-side encryption (AES 256-bit).

The unique benefits of Veeam's object storage integration include:

- **Transparency:** Backups that have been offloaded to object storage remain transparently accessible to all Veeam functionality – and are readily available for restores directly from object storage, without prior staging.
- **Space efficiency:** In addition to source-side compression, backup files are offloaded to object storage in the forever incremental manner, thus preventing duplication between multiple full backups, which effectively provides source-side deduplication.
- **Bandwidth efficiency:** During restores, egress traffic from object storage is minimized by reading all matching blocks from the closest backup file available on-premises in the Performance Tier – instead of pulling all blocks from object storage, thus reducing the cost of restores.
- **Self-sufficiency:** Offloaded backups are self-sufficient and not dependent on any external catalog or metadata, which allows them to be imported even if the on-premises backup server is completely lost along with its configuration and database.

Veeam product suites designed for every business

Veeam Backup & Replication and Veeam ONE™ are better together. Veeam combines its two marquee solutions to help businesses manage and monitor their entire IT environment, including virtual, physical and cloud-based workloads.

Veeam Availability Suite combines the industry-leading backup, restore and replication capabilities of Veeam Backup & Replication with the advanced monitoring, reporting and capacity planning functionality of Veeam ONE to deliver Availability for all workloads – virtual, physical, and cloud – from a single management console.

Veeam Backup Essentials™ is a powerful, easy-to-use and affordable backup and Availability solution designed for small businesses with less than 250 employees and environments of up to 6 CPU sockets or 30 Instances. Veeam Backup Essentials delivers the exact same functionality as Veeam Availability Suite™ with a savings of up to 60% or more.

- **No vendor lock-in:** Archived backups can be imported from object storage and restored at any point in time in the future by using a free Veeam Backup & Replication Community Edition, without requiring a paid Veeam license. We don't hold your data hostage!
- **No extra costs:** Unlike secondary storage appliance vendors, Veeam does not charge a per-TB subscription for offloading data to object storage. We have no cloud usage tax!

Access to the Cloud Tier functionality of SOBR requires the **Enterprise edition**.

Expanded restore options to AWS and Azure Stack with Veeam Cloud Mobility

Veeam Cloud Mobility provides easy portability and fast recovery of ANY on-premises or cloud-based workloads to Amazon AWS, Microsoft Azure and Azure Stack to maintain business continuity and Availability across hybrid cloud environments, allowing you to:

- Get direct portability of workloads across private, hybrid and public clouds
- Restore and recover workloads directly to the cloud for fast business continuity
- Unlock the test and development use case of the public cloud

In addition to previously released Direct Restore to Microsoft Azure, Update 4 expands Veeam Cloud Mobility with the following new functionality:

Direct Restore to Amazon AWS delivers cloud restore for Veeam backups to optimize resource allocation and minimize cost, enabling you to restore backups of Windows and Linux-based VMs, physical servers and workstations as an AWS EC2 VM, including Amazon Government Cloud and Amazon China. This feature comes with a built-in UEFI to BIOS conversion, making it possible to restore modern Windows workstations directly to AWS EC2 (which does not support UEFI).

Direct Restore to Microsoft Azure Stack builds on top of the proven Direct Restore to Microsoft Azure engine to enable you to restore backups of Windows and Linux-based VMs, physical servers and workstations to Microsoft Azure Stack as an infrastructure as a service (IaaS) VM. Along with Veeam Agents, this functionality provides the complete backup solution for Microsoft Azure Stack IaaS VMs.

Improved Security and Compliance with Veeam DataLabs

Veeam DataLabs is a set of powerful capabilities that empowers IT and developers to test workloads in an isolated environment enabling them to validate updates, test patches, check for security vulnerabilities, ensure compliance, and verify recoverability of Veeam backups. Previously known as Virtual labs, Veeam DataLabs have received new capabilities in Update 4 which enable delivering functionality for better security, compliance and streamlining IT workflows.

Staged Restore enables organizations to make required changes to the database content or application/OS settings before restoring a VM into the production environment. This is achieved by starting up the required restore point in a DataLab directly from backup files, injecting and running

Supported environments

VMware infrastructure*

Platforms

- vSphere 6.x
- vSphere 5.x

Hosts

- ESXi 6.x
- ESXi 5.x

Software

- vCenter Server 6.x (optional)
- vCenter Server 5.x (optional)
- vCloud Director 8.x and 9.x (optional)

Virtual Machines

- All OS's supported by VMware
- Any application
- Any file system

*Only English version of VMware infrastructure is supported

Microsoft infrastructure

Platforms

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2 SP1

Hosts

- Windows Server Hyper-V 2019
- Windows Server Hyper-V 2016
- Windows Server Hyper-V 2012 R2
- Windows Server Hyper-V 2012
- Windows Server Hyper-V 2008 R2 SP1
- Microsoft Hyper-V Server (free hypervisor)

Software

- Microsoft System Center Virtual Machine Manager 2016 or later (optional)
- Microsoft System Center Virtual Machine Manager 2012 R2 (optional)
- Microsoft System Center Virtual Machine Manager 2012 SP1 (optional)
- Microsoft System Center Virtual Machine Manager 2008 R2 SP1 (optional)

Virtual Machines

- All OS's supported by Microsoft Hyper-V
- Any application
- Any file system

Agent Management

Utilization of agent management functionality requires the installation of the redistributable package of Veeam Agent for Microsoft Windows v3 or later and/or Veeam Agent for Linux v3 or later with Veeam Backup & Replication.

a custom script in the guest OS while preserving the changes made, and finally moving the modified state to the production environment to finalize the restore. Use cases for Staged Restore include:

- GDPR compliance around the right to be forgotten, by enabling you to use the same applications or scripts designed to clean up personal data from your production systems, when performing the restore of VMs containing personal data from older backups.
- Streamlining IT workflows by enabling administrators to make the required OS settings changes (such as IP address, DNS or firewall settings), installing or removing applications and performing any other operations required to make the restored VM compliant with the target environment before it is actually placed there.

Access to the Staged Restore functionality requires the **Enterprise edition**.

Secure Restore enables organizations to easily scan guest file system within image-level backups for malware, such as computer viruses or ransomware, prior to performing the restore to the production environment. This is achieved by mounting disks to the mount server associated with the backup repository and triggering an antivirus (AV) scan with one of the supported AV programs installed on the mount server. Use cases for Secure Restore include:

- Detecting “sleeping” ransomware in the selected restore point to improve the time of recovery from a ransomware attack by not bringing ransomware with the restored VM back into the production environment over and over again.
- Verifying backups from locations with less IT control, such as remote and branch offices (ROBO), prior to restoring them into the HQ data center in ROBO disaster recovery (DR) scenarios.
- Scanning the restore point with a different AV program from the one installed on the actual VMs to increase the chance of detecting rare or zero-day malware.

Secure Restore supports Microsoft Windows Defender, Symantec Protection Engine and ESET NOD32 out-of-the-box and is extendable through configuration file to any AV program that provides a basic command line interface.

Enterprise Application Plug-ins

Let your database administrators (DBAs) remain in control of backing up and restoring their databases using native tools they are comfortable with while continuing to centralize all backups into your Veeam backup repository with new enterprise application plug-ins.

- **Veeam Plug-in for SAP HANA** is an SAP certified solution that allows HANA DBAs to use the BACKINT interface to perform backups and restores of HANA databases to and from the Veeam backup repository, including support for HCI SAP HANA deployments.
- **Veeam Plug-in for Oracle RMAN** allows Oracle DBAs to use the RMAN manager to perform backups and restores of Oracle databases into a Veeam backup repository. This RMAN-based integration provides customers with an additional method to achieve Oracle availability and expanded platform without replacing the existing OCI-based integration built into the image-level – which often may be a better fit depending on your scenario.

The additional benefit of leveraging Veeam plug-ins for enterprise applications is support for scale-out backup repository (SOBR), which dramatically increases backup and restore throughput thanks to the scalable multi-node backend that SOBR provides.

Access to the enterprise application plug-ins requires the **Enterprise Plus edition**.

Enhanced Self-Service Capabilities

Improve recovery times and reduce TCO by allowing users to securely manage backups and restores of their own VMs through the self-service backup and restore portal for VMware vSphere with role-based access tied to your already established and maintained vSphere permission system – meaning any infrastructure changes or new hires will not require IT to update delegation rules.

Available delegation modes for brownfield deployments include using the particular vSphere permission or vSphere privilege, which enables users to only see and manage backup and restore of VMs they have the corresponding permission to, or privilege for. And for greenfield deployments, you may choose to leverage the convenience of vSphere tags, with users only having access to VMs with tags specified in their respective self-service configuration.

Self-service portal is based on the existing Enterprise Manager user interface, but is streamlined for this particular use case. Job setup is simplified so users only need to select the VMs back up, as well as select essential parameters such as guest credentials, retention and notifications. Users are blocked from accessing advanced settings, such as repository or backup mode selection, which are managed by the portal administrator through job templates. And as it comes to restores, users are allowed to perform a wide variety of restore options for VMs that Enterprise Manager currently provides including application items, guest files, and full VM.

Access to the self-service backup and restore portal requires the **Enterprise Plus edition**.

Intelligent Diagnostics

Improve your backup reliability and success ratios while reducing total cost of ownership (TCO) through proactive resolution of known issues and configuration problems.

This new feature of Veeam ONE, Intelligent Diagnostics, will monitor Veeam Backup & Replication logs for patterns of known issues and match these with the virtual infrastructure monitoring data. Users will then be notified if it determines that your backup infrastructure may not be optimally configured, your virtual infrastructure is experiencing an issue that may affect backups or your installation is simply missing a critical hot fix – all before these issues have material impact on your backups.

And best of all – unlike alternative solutions – there's no "phone home" involved, as the log mining is performed on-premises using issue signature bundles prepared by Veeam Technical Support and Product Management. In other words, this feature puts the power of Veeam's support logs mining and analysis engine in your hands – so that you hopefully never have to open a support case again.

For more information on Intelligent Diagnostics, please refer to Veeam ONE 9.5 Update 4 release documentation.

Access to the Intelligent Diagnostics functionality requires Veeam Essentials or Veeam Availability Suite.

Platform support

Update 4 delivers full support for all recently shipped platform updates, including:

- **Microsoft Windows Server 2019** support as guest OS of virtual machines protected by Veeam Backup & Replication, for installation of Veeam Backup & Replication and all of its remote components, and for backup with Veeam Agent for Microsoft Windows.
- **Microsoft Windows 10 October 2018 Update** support as guest OS of virtual machines protected by Veeam Backup & Replication, support as guest virtual machines, for installation of Veeam Backup & Replication and all of its remote components, and for backup with Veeam Agent for Microsoft Windows.
- **Microsoft Windows Server Hyper-V 2019** support as a hypervisor host, including support for virtual hardware version 9.0 virtual machines.
- **Microsoft Active Directory 2019, Exchange 2019 and SharePoint 2019** support for application-aware processing, and for item-level recoveries with Veeam Explorer.
- **Oracle Database 18c** support for application-aware processing on Windows-based virtual machines, including transaction log backup and point-in-time restores.
- **VMware vSphere 6.7 U1 ESXi, vCenter Server and vCenter Server Appliance (VCSA)** support.
- **VMware vCloud Director 9.5** support.

In addition to the above-mentioned major features, as a result of on-going R&D efforts and in response to customer feedback, Update 4 also includes hundreds of other enhancements, the most significant of which are listed below.

General

App-aware processing

- Added support for Kerberos-only authentication for vSphere VM application-aware processing. This enables IT to disable NTLM in VM guest networks to prevent pass-the-hash attacks in the virtual environments with less IT control.
- SQL Server transaction logs and Oracle redo logs backup engine will now use the volume with most disk space as a staging location for log backups, instead defaulting to C: drive which often does not have enough free disk space. On Linux, it now chooses the directory with most free spaces between /var/tmp and /tmp.
- Oracle redo logs backup retention policy will now analyze the logs being removed in order to preserve Guaranteed Restore Points (part of Oracle Flashback feature).
- Added support for Oracle Data Guard deployments.

Engine

- Maximum supported individual disk size and backup file size have been increased over 10 times. With the default 1MB block size, the new theoretical VBK format maximums are 120TB for each disk in backup, and 1PB for the total backup file size. Tested maximum is 100TB for both individual disks and backup files.
- Reduced metadata size for backups without encryption by 10MB, benefiting minimum backup file size.
- Optimized backup job initialization and finalization steps, resulting in up to 50% times faster backups of small VMs.
- Image content publishing engine has been reworked for significantly faster file-level and item-level recovery.
- Preferred Networks settings now also affect built-in WAN accelerators.

Linux

- Removed the requirement for adding NOPASSWD:ALL option to the sudoers file for the user account that you want to elevate to root.
- Added support for !requiretty option enabled in the sudoers file, which is the default setting for some Linux distributions (like CentOS).
- When registering a Linux server, you now have an option to failover to using "su" command for distros where "sudo" command is not available.
- SSH fingerprint validation has been extended to all Linux server connections to protect against "man in the middle" (MITM) attacks through managed servers.
- Reliability improvements in the PKI authentication logic.

Microsoft Azure

- Support for Azure CSP subscriptions and Azure Government Cloud.
- Ability to select network security group for the target Azure IaaS VM.
- You can now specify Azure Active Directory users when connecting to your Azure account.

Microsoft Hyper-V

- Hyper-V VM groups can now be used to add VMs to backup and replication jobs.
- Instant recovery of agent backups to a Hyper-V VM now support Windows 10 Hyper-V as the target hypervisor. This is particularly useful for managed service providers by enabling them to create low-cost all-in-one BCDR appliances to deploy at their clients' premises.

Microsoft ReFS

- Added experimental support for block cloning on deduplicated files for Windows Server 2019 ReFS. To enable this functionality, create **ReFS Dedupe Block Clone** (DWORD) = 1 value under HKEY_LOCAL_MACHINE\SOFTWARE\Veeam\Veeam Backup and Replication registry key on the backup server.

VMware vSphere

- vPower NFS write cache performance has been improved by an order of magnitude, dramatically increasing I/O performance of instantly recovered VMs and making a better use of SSD drives often dedicated by customers to write cache.
- vPower NFS scalability has been improved to more efficiently leverage expanded I/O capacity of scale-out backup repository for increased number of VMs that can be running concurrently.
- Added hosts authorization by IP address to vPower NFS server (by default, only the ESXi host that provisioned vPower NFS datastore has access to it). To disable this functionality, create **vPower NFS Disable IP Auth** registry key under HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Veeam\Veeam NFS\ on the mount server.
- SureBackup jobs can now be configured to use vPower NFS cache (in addition to redirecting changes to vSphere datastore), which particularly enables support for using SureBackup against VMs with disks larger than 2TB in environments with only available vSphere storage being VMware VSAN.
- Support for Paravirtual SCSI controllers with more than 16 disks attached.
- vSphere tags are now automatically moved by Quick Migration jobs, and preserved when performing Instant VM Recovery.

RESTful API

- Added JSON support.
- Added RESTful API coverage for viewing and managing agent-based jobs and their backups.

Setup

- Built-in SQL Server version was changed to Microsoft SQL Server 2016 SP1.

Agent Management

General

- Windows Server Core Edition servers and failover clusters support with backup server-managed jobs.
- Wildcards and system environmental variables are now supported for the source data selection on the protected computers.
- Server-managed backup jobs will now use the single backup manager process for all hosts processed by the single backup job, instead of individual manager for each host, significantly reducing backup server resource usage and improving scalability (tested with 1000 agent-based jobs per backup server).

- Server-managed backup jobs now feature Secondary Target step.
- Support for multiple agent-managed jobs for workloads using Server edition of Veeam Agents.
- Agent-managed backup jobs now have backup agents automatically updating its configuration and license when starting the backup, without the need to wait for a periodic or manual protection group rescan.
- Email reporting options can now be customized for agent-managed backup jobs, including setting the time when daily report should be sent.
- Backup server can now optionally clean up retired agent's backups from the repository, similarly to "deleted VM retention" functionality already available in the product.
- Removed the requirement for backup server's DNS name to be resolvable on the agent side.
- Full PowerShell support for all agent management functionality.

Protection groups

- Reboot host option is now shown only when the host reboot is actually required, instead of always.
- Uninstall option now also removes the Veeam Installer service, in addition to the backup agent.
- Test credentials option is now available for protection groups of "individual computers" type.
- Email reporting options can now be customized for protection groups, including setting the time when daily report should be sent.
- Hosts which have been excluded from protection group, based on user-specified settings, are now shown in email reports.
- Protection group rescan session log has been reworked for better clarity.

Application-aware processing

- Transactionally consistent image-level backup and redo log backup for Linux-based Oracle servers is now supported with server-managed jobs.
- Added support for Windows Server Storage Replica, including automatic exclusion of duplicate copies of data at backup time, and automatic disk layout configuration for volume-level restores.
- Microsoft Exchange database availability groups (DAG) nodes are now automatically processed in a sequential manner within a single failover cluster backup job to avoid DAG failover issues.
- Added support for IP-less Microsoft Exchange DAG.

Volume-level restore

- You can now perform restores of simple and clustered volumes directly from the backup console. This requires a backup agent installed on the target host and is not supported for the OS volumes.

File-level restore

- You can now allow users without Local Administrator privileges to perform file-level recovery from agent backups using local agent UI. The corresponding option can be found in the Protection Group settings.
- Clustered disks are now accessible on all failover cluster nodes during file-level recovery, so you no longer have to search for the owner node to be able to perform a file-level restore.

Veeam Agent for Windows

- Backup and restore of removable USB drives.
- Added periodic compact and health check option for agent-based backup files.

- Ability to set network traffic throttling, for example when backing up over WAN.
- Ability to restrict backup over VPN connections
- Ability to force backup over Wi-Fi to use the specific Wi-Fi networks (SSIDs) only.

Veeam Agent for Linux

- btrfs file system support (requires Linux kernel version 3.16 or later).
- Snapshot-less file-level backup option that does classic inconsistent Linux file level backup. This option can be useful for when snapshot driver cannot be installed (for example, for security reasons) or when the data source of file-level backup does not support being snapshot (such as an NFS mount).
- Added support to add the entire volume group to the backup job's scope.
- Added periodic Active Full backup option.
- Added support for latest version of all supported Linux distributions. For details, please refer to the What's New in Veeam Agent for Linux 3.0 document.

Restore

General

- Added the ability to export the selected restore point of a particular object in the backup job as a standalone full backup file (VBK) and keep it on a separate retention – or indefinitely. This functionality can be useful for preventing certain restore points from being deleted by the primary backup job's retention for legal hold or archival purposes, or to be able to easily provide the specific restore point to someone on a removable media.
- Extract utility now supports restore from incremental backups, and was made a 64-bit application to enable large backup files support. Remember to update any scripts that include extract utility with archived backup files to use this new version!

File-level recovery

- Performance of file-level recovery through Backup Browser should now be closer to one of the 3rd party file management tools using C:\VeeamFLR mount point.
- Other OS file-level recovery now supports the restoration of SGID and extended attributes (xattr), as long as they are supported by the target file system.
- Overall file restore performance should be noticeably improved with this update.

Veeam Explorer for Microsoft Active Directory

- Added restore summary dialog with details on all restored objects and attributes.
- Improved Active Directory database mounting, search and restore performance.
- Added advanced capabilities for use by Active Directory experts only: ability to restore Microsoft System Objects, CA certificate information and AD Sites subnet items.

Veeam Explorer for Microsoft Exchange

- Added the new view mode that compares the state of mailbox in backup vs. production Exchange server, and only shows differences between them – enabling you to quickly identify and restore changed and deleted items.
- Added support for browsing and restoring items in the Versions subfolder of the Recoverable Items mailbox folder.

- Added restore summary dialog with details on all restored mailbox items.
- Added full PowerShell coverage for all export and restore functionality.

Veeam Explorer for Microsoft SharePoint

- Added home pages restore functionality (Master/Publishing/WebParts pages).
- Added site/list experience setting restore functionality (classic/modern themes).
- Added SharePoint views restore functionality.
- Added support for restoring SharePoint lists and libraries that use Custom Templates.
- Added full PowerShell coverage for all export and restore functionality.

Veeam Explorer for Microsoft SQL Server

- Added the ability to instantly publish a point-in-time state of any backed-up database to the selected SQL Server for dev/test purposes by running the database directly from the backup file. Changed database state can be exported, or discarded with no impact to the actual backup.
- Added the ability to export a point-in-time state of any backed up database to a native SQL Server backup (.BAK file) to simplify the process of providing the database backup to SQL developers, BaaS clients or Microsoft Support.
- Added additional database restore options (NORECOVERY and STANDBY).
- Added the ability to restore databases to any SQL Server failover clusters (not just the original one).
- Major restore performance improvements through multiple optimizations, including parallel restore of multiple database files or file streams and using advanced data fetcher to accelerate single database file restore.
- Added PowerShell coverage for database export, restore and publication functionality.

Veeam Explorer for Oracle

- Added support for Oracle DataGuard databases support (both Physical and Logical).
- Added ability to perform point-in-time database restore from storage snapshots, including those created by external schedulers.
- Added ability to restore databases from Oracle database backups created with Veeam RMAN plug-in (this capability can be blocked on selected Oracle servers if desired, if database administrator wishes to restrict restores to RMAN).
- During the restore, temporary files will now be placed on the volume with most free disk space on the target server, as opposed to disk C:
- Added full PowerShell coverage for all functionality.

Storage Integrations

Storage snapshots integration

- Added full support for multi-homed VMs (VMs with disks on different datastores) in all storage snapshots integrated functionality including Veeam Explorer for Storage Snapshots (for all supported restore types), Backup from Storage Snapshots with snapshot retention, storage snapshot-only jobs (including with secondary destinations), and OnDemand Sandbox from storage snapshots.
- Backup proxy selection logic for Backup from Storage Snapshots has been optimized to prevent "spider web" effect in large environments, with every storage snapshot mounted to multiple backup proxies.

- Jobs using Backup from Storage Snapshots should now complete faster due to optimized snapshot LUN unmount process (done in parallel and with reduced number of LUN rescan operations).
- Backup server will now automatically clean up the Windows registry on backup proxy servers from records of dismantled LUNs (which Windows keeps in hope of reusing) to prevent the registry from ballooning, which eventually leads to OS stability issues.
- Proprietary SCSI initiator has been updated to handle additional SCSI protocol commands, making it one step closer to RFC and enabling support for NetApp Element (HCI/SolidFire) universal storage API plug-in (released with Update 4 as a separate download).
- Added storage certificate validation when registering primary storage with Veeam for additional security (applies to built-in storage integrations only).
- Veeam Backup & Replication update notifications will now include information on updated Universal Storage API plug-ins installed on the backup server.
- Added new and enhanced existing PowerShell cmdlets for storage management.

Primary storage

- DELL EMC Unity integration received some changes to its snapshot export approach to prevent storage from logging warnings and other issues and allow more than one LUN snapshots to be exported to backup proxy.
- Navisphere CLI used in VNX integration was updated to the latest version for security patches.
- IBM Storwize version 8.1.2 support, including support for Data Reduction Pools.
- HPE Nimble support for Nimble OS version 5.1, including group-scoped iSCSI target IQN naming (Nimble GST).
- HPE StoreVirtual firmware version 12.7 support has been added.
- NetApp ONTAP version OS 9.4 support has been added.
- Increased total number of storage snapshots that can be specified in in backup job wizard to 1000. Please check with your storage vendor on the actual limit for the particular storage.

Secondary storage

- DELL EMC Data Domain DDBoost SDK has been updated to version 3.3 for added DD OS 6.1 support and ability to disable read ahead cache during instant recovery for improved I/O performance and significantly reduced I/O load on Data Domain storage.
- You can now delay incremental backup deletion for scenarios involving Data Domain MTree replication. To enable this functionality, set **DDBoostDeleteIncrementStorageAfterHours** (DWORD) value under HKEY_LOCAL_MACHINE\SOFTWARE\Veeam\Veeam Backup and Replication registry key on the backup server to the desired number of hours.
- HPE StoreOnce firmware 4.1 version support (new Gen10 hardware).
- HPE StoreOnce Catalyst SDK updates to version 4.1, adding support for shared read functionality that unlocks many previously unavailable restore scenarios around Instant VM Recovery, Microsoft SQL Server database recovery, as well as all scenarios requiring concurrent access to backup files (such as running multiple restore sessions from the same backup).
- HPE StoreOnce full VM restore logic has been reworked to use sequential read from StoreOnce and random writes to the target datastore, increasing overall restore VM performance up to a few times depending on scenario.
- HPE StoreOnce-based backup repository rescan performance has been improved up to 2 times.
- Quantum DXi deduplicating storage native support has been added. This includes support for OEM partner products leveraging Quantum DXi platform.

Object storage

- Added the ability to register object storage as an external repository, enabling you to see Veeam backups stored there, perform all types of restores directly from object storage, and use Backup Copy jobs to make an on-premises copy of backups stored in object storage. This is the enabling technology behind Veeam Availability for AWS.

Tape

- Backup and restore your NAS volumes to tape with native support for NDMP v4. Just like File to Tape jobs, there are no additional charges per protected data size, however access to this functionality requires the **Enterprise Plus edition**.
- Added support for parallel processing for GFS media pools.
- Added the ability to use daily media set with GFS media pool for incremental backups, and to specify exact start time for GFS tape backup jobs.
- You can now define roles of additional tape libraries in the media pool: active for cross-library parallel processing, passive for failover when target library is offline or lacks available media.
- Support for Write Once Read Many (WORM) tape media.
- Tape lifespan metric is now used to automatically pick the least used media for backup.
- Added the dedicated Tape Operator role to enable delegation of tape media and tape jobs management operations to help desk staff.
- Added automatic ejection tapes from standalone drivers if full during the backup, or when the tape is no longer needed during the restore; as well as an option to automatically eject last tape in the job whether it is full or not.
- Added the ability to order source objects processing for File to Tape and Backup to Tape jobs. For per-VM backup chains, the same processing order will be used as in the primary backup job.
- You can now configure Backup to Tape jobs so that they do not wait for a new backup, and instead immediately start processing the latest available restore point.
- File to Tape jobs now support file extensions and folder name masks for both inclusions and exclusions.
- Restore from incremental file backup set can now only process files that were present in the folder at the time the particular backup set was created, instead of restoring all deleted files that were ever present in the folder.
- File from Tape restore performance has been improved.

User interface

Backup console

- Added the ability to schedule Active Full backups on a particular day of the month, as opposed to weekdays.
- Added "Last run" column showing how long ago the particular job was run to all job grids. Remember you can move columns around using drag and drop to put the new column into the desired location.
- Added the ability to hide unwanted columns from all grids via right-click menu.
- Network traffic rules can now have descriptions assigned to help you more easily distinguish between them.
- Added the pre-defined "Internet" network traffic rule for communications to non-private IPv4 addresses, enabling you to easily throttle all Internet traffic. This was previously a hidden rule that automatically enabled a network traffic encryption.
- Backup properties dialog has been updated to correctly group per-VM backup files when selecting a VM, and support downloading and offloading individual backup files from/to scale-out backup repository Capacity Tier.

- Backup console will now automatically update itself when connecting to the updated backup server not just for updates, but also for new product versions.
- Backup and VM deletion progress is now shown to the user; deletion sessions are now available in sessions history.
- Enhanced user interface appearance on 4K monitors.
- Redesigned dashboard wizards for registering infrastructure components and performing restores.

Enterprise Manager

- Protection groups or individual hosts can now be selected as a restore scope for Enterprise Manager restore operator role setting.
- Performing full VM restore with "keep existing" option now adds current date and time as a suffix to the restored VM to enable you to more easily distinguish between multiple restored copies of the same VM.
- SQL Server database restore functionality now supports restore back to the original SQL Server failover cluster, as well as restore of SQL Server AlwaysOn database to a non-original AlwaysOn Group.
- You can now enable high security mode in the Enterprise Manager setup (available for new Enterprise Manager installations only). This mode enforces TLS 1.2 protocol and disable weak ciphers setup option using system-wide settings, and thus may not be compatible with other 3rd party software running on the same server.
- Web UI look and feel has been redesigned to match modern Veeam web UI design guidelines. We hope you will like it better!

Licensing

Veeam Instance Licensing

- Added new Instance-based subscription licensing. This new licensing is non-platform dependent and is portable across all workloads managed by Veeam Backup & Replication including VMs for all supported hypervisors, server agents, workstation agents, enterprise application plug-ins and cloud workloads. Instance licensing dramatically simplifies license management in modern data centers, where the same workload can migrate between physical, virtual and cloud machines over the course of its lifecycle, thus requiring to be protected by different Veeam products.
- Legacy per-VM and per-agent subscription licenses are discontinued by the Veeam Instance licensing. Upon installing Update 4, you have a grace period of 90 days to replace your legacy subscription license with Instance license, which you can download at any time from the Customer Portal.

Socket-based licensing

- There are no changes with perpetual Socket-based licenses availability, which are continued to be sold and supported for vSphere or Hyper-V VMs protection. However, with Update 4 newly issued Socket-based licenses are no longer hypervisor-specific.
- Customer can merge Perpetual (socket-based) and Subscription (instance-based) licenses into the single license file if centralized Veeam management for virtual and other workload protection is required. A single license file with both Sockets and Instances will be set to expire according to the earliest expiring maintenance contract, however customer can always undo merge to get standalone licenses with actual maintenance expiration dates back. Limitations: Instances will not be used for VMware and Hyper-V VM backup (due to the presence of Sockets); perpetual and subscription contracts must be of the same edition.
- Customer can have multiple Perpetual (socket-based) and Subscription (instance-based) licenses of different editions, however each such license must be used in separate backup infrastructures which are not sharing backups, servers or storage between each other, and are protecting different source infrastructures. Limitation: No centralized Veeam management will be available.

- Upon installing Update 4, all perpetual Socket-based licenses will receive 1 Instance for every licensed Socket, up to a maximum of 6 Instances, included at no cost – free for life, with technical support included per your existing maintenance contract. There are no obligations or restrictions, however these added Instances are not cumulative with additional Instances purchased. Included Instances are not reflected in the license file, but can be seen in the License Information dialog. These gifted Instances can be used for any workloads supported by Instance licensing, except vSphere or Hyper-V virtual machines, which, in presence of Socket license, will always use Sockets.

Product edition changes

- Veeam Backup & Replication Enterprise Edition now supports up to 2 scale-out backup repositories with up to 3 active extents each (not counting the Capacity Tier extent), as opposed to only one scale-out backup repository before.
- Veeam Backup Free Edition has been discontinued and replaced by Veeam Backup & Replication Community Edition.
- Added Veeam Backup & Replication Community Edition, which is effectively fully functional Veeam Backup & Replication Standard Edition limited to 10 Instances. For the former Free Edition functionality, Community Edition inherits the same licensing behavior, for example VeeamZIP backups or Quick Migration jobs will not be counted against the 10 Instances limit.

Veeam Cloud & Service Provider Partner Solutions

9.5 Update 4 includes many new features and enhancements for service providers offering Backup as a Service and Veeam Cloud Connect services, most significant of which are listed below. For the full list of enhancements and bug fixes, please see this topic on the private VCSP forum. Not a member of the VCSP forum? [Click here to join](#).

Veeam Cloud Connect

General

- Gateway pools: create and assign pools of cloud gateways to the tenants to enable supporting both Internet and MPLS tenants with the single Cloud Connect server, or to better manage SLAs through dedicated gateway pools.

Backup

- Tape as a Service: service providers can now offer their tape out services to help their tenants achieve compliance and internal policies without maintaining their own tape infrastructure, or to create additional copies of tenant backups for cloud repository disaster recovery purposes, by writing tenant's backups directly to tape with Tenant to Tape jobs. This functionality is only available for backups created by Veeam Backup & Replication 9.5 Update 4 and Veeam Agents 3.0.
- Tenant-driven password change: tenants can now change the password they use to connect to the service provider by editing one on the registered service provider and providing the current password for security purposes.

Replication

- vCloud Director integration: service providers using VMware vCloud Director can now leverage existing networking, infrastructure and self-service management investments for Disaster Recovery as a Service (DRaaS) solutions for lower TCO and higher margins, by using vCloud Director to authenticate tenants and assign them hardware plans based on vCloud vDCs. This includes full RESTful API coverage to enable complete automation.
- Cloud replicas are now automatically removed from configuration on the tenant side after permanent fail over to the service provider data center.
- Added "test" action to RESTful API for Veeam Cloud Connect Replication failover plans.

vCloud Director Self Service Portal

General

- Added "Used quota" column to the self-service configurations grid.
- VM deletion progress is now shown to the tenant.

Veeam Backup & Replication 9.5 Update 3a: What's new?

As the result of an on-going R&D effort, and in response to customer feedback, Veeam Backup & Replication 9.5 Update 3a features a number of enhancements and bug fixes. The most significant updates are listed below.

Platform support

- **VMware vSphere 6.7 support.** Includes the new HTML5 version of vSphere Web Client plug-in for Veeam Backup & Replication, and asynchronous NBD/NBDSSL support for improved read performance of network transport mode with ESXi 6.7.
- **VMware vSphere 6.5 U2 preliminary support.** This update addresses all outstanding U2-specific compatibility issues that can be managed from the Veeam side. However, there is a major regression in ESXi 6.5 U2 code that makes the vSphere API fail randomly during high host CPU load periods, consequently impacting a variety of Veeam Backup & Replication functionality. VMware is currently troubleshooting this bug, and fixing one will most likely require the new ESXi 6.5 U2 build issued.
- **VMware vCloud Director 9.1.** Update 3a provides compatibility for existing vCloud Director support functionality.
- **VMware Cloud on AWS version 1.3** support and preliminary out-of-the-box compatibility with future VMC updates through removal of the API version match requirement.
- **Microsoft Windows Server 1803.** Update 3a provides Windows Server 1803 support as guest virtual machines, for installation of Veeam Backup & Replication remote components, and as a domain controller for Veeam Explorer™ for Microsoft Active Directory.
- **Microsoft Windows Server Hyper-V 1803.** Update 3a provides Hyper-V 1803 support as a hypervisor host, including support for processing VMs with virtual hardware version 8.3.
- **Microsoft System Center Virtual Machine Manager 1801** support.
- **Microsoft Windows 10 April 2018 Update.** Includes support as guest virtual machines and for installation of Veeam Backup & Replication and all of its components.

VMware vSphere

- Includes improved performance of Direct Storage Access (DirectSAN) and Virtual Appliance (Hot Add) transport modes for backup infrastructure configurations through optimizing system memory interaction.

Microsoft Azure

- Added support for Direct Restore to *Microsoft Azure* for environments with ExpressRoute or site-to-site VPN connectivity to Azure, in which case proxy and helper appliances may have private IP addresses only. To enable, create *AzurePreferPrivateIpAddresses ForProxyandLinuxAppliance* (DWORD = 1) registry value under **HKLM\SOFTWARE\Veeam\Veeam Backup and Replication** key on the backup server.

Linux File Level Recovery

- Added support for Linux SUID and SGID preservation to "Copy To" operation.
- Added support for Btrfs volumes located on an LVM volume.

Primary Storage Integrations

- Installing Universal Storage API plug-ins on each backup console (in addition to the backup server) is no longer required.
- Storage snapshot-only vCloud Director backup jobs are now supported for all storage integrations which support storage snapshot-only jobs. Previously, it was supported for NetApp only.
- Cisco HyperFlex integration will no longer delete the base sentinel snapshot during each job run to improve processing performance and reduce storage load.

Tape

- Improved performance of enumeration in File to Tape jobs with very large number of files.

Veeam Backup & Replication 9.5 Update 3: What's New?

Built-in management for Veeam Agent for Microsoft Windows and Veeam Agent for Linux

Update 3 delivers reduced data protection management complexity and improved usability by adding agent-based backup capabilities directly into the Veeam Backup & Replication console. This allows users to manage both hypervisor-based and agent-based backup through a single console, thus enabling protection of virtual, physical and cloud workloads. This new functionality includes the following capabilities:

- **Single pane of glass for Availability of virtual, physical and cloud workloads.** Maintain complete control of data protection for ALL your workloads natively through the Veeam Backup & Replication console. Easily manage backups and advanced restore capabilities regardless of where the protected workload is located (virtual, physical or cloud).
- **Centralized backup agent deployment.** Ensure no Windows or Linux computers are left unprotected by centrally deploying Veeam Agent for Microsoft Windows and Veeam Agent for Linux with automated host discovery via dynamic protection groups based on Active Directory containers, or CSV files exported from your existing CMDB system.
- **Windows Server Failover Cluster support.** Protect your mission critical Microsoft Windows Server failover clusters, including SQL Server failover clusters and SQL Server AlwaysOn Availability Groups in a transactionally-consistent fashion – and leverage the full power of Veeam granular recovery technologies for guest file and application item recoveries.

Insider protection for Veeam Cloud Connect

Ensure the ability to recover your data following a cyber-attack by having your Veeam Cloud Connect service provider protect your data against insider attacks.

Service providers using Veeam Cloud Connect can now enable protection of their tenant's backups against accidental or malicious deletion directly from the tenant's console. These deletions are often executed either by hackers who have breached the tenant's network perimeter and obtained powerful credentials with a brute force attack (with the intention of deploying ransomware on the production servers), or by a disgruntled employee with privileges to manage Veeam Backup & Replication.

Data Location Tagging

Ensure data sovereignty compliance required by various regulations, such as the General Data Protection Regulation (GDPR), by tagging production infrastructure and backup infrastructure objects with locations. Location tags are used to prevent accidental errors when configuring backup and replication jobs or performing out-of-place restores, by issuing a warning when an action may result in a data sovereignty violation. Additionally, new Veeam ONE reports use location data to help prove compliance.

IBM Spectrum Virtualize Integration

Reduce the impact on production environments and achieve lower recovery time and point objectives through new storage snapshots integration for IBM Storwize, IBM SAN Volume Controller (SVC) and any other IBM Spectrum Virtualize based storage system, such as Lenovo Storage V series or IBM/Cisco VersaStack. The following functionality is supported with this new integration:

- **Backup from Storage Snapshots:** Lower the impact from backup activities on the VMware environment by retrieving virtual machine (VM) data directly from storage snapshots on primary storage.
- **Veeam Explorer™ for Storage Snapshots:** Recover individual items or entire VMs quickly and efficiently directly from storage snapshots.
- **On-Demand Sandbox™ for Storage Snapshots:** Use storage snapshots to create complete isolated copies of your production environment in just a few clicks, for fast and easy developing, testing and troubleshooting.
- **Snapshot orchestration:** Improve RPOs and radically mitigate potential data loss by using snapshot-only jobs to create additional, more frequent recovery points in the form of application-consistent or crash-consistent primary storage snapshots – or keep storage snapshots created by regular backup jobs on a separate retention schedule, as an additional backup.

Universal Storage Integration API

Extend Availability and improve recovery time and point objectives through out-of-band expansions of primary storage integrations with leading storage providers through plug-ins to a Universal Storage Integration API framework included in Veeam Backup & Replication starting with this update.

This framework enables select storage partners to build integrations of their primary storage systems with advanced Veeam Backup & Replication functionality that leverages storage snapshots (as detailed in the IBM Spectrum Virtualize section above). Update 3 currently provides storage snapshot integrations for VMware through the following [third-party plug-ins](#).

Veeam Backup & Replication 9.5 Update 3 includes hundreds of other enhancements and bug fixes, the most significant of which are listed in the Release Notes document [KB2353](#).

Veeam Backup & Replication 9.5 Update 2: What's New?

Cisco HyperFlex Integration

Reduce backup and recovery times and improve overall operational performance with Backup from Storage Snapshots with the Cisco HyperFlex hyperconverged infrastructure (HCI) platform. Key benefits include:

- **Improved recovery point objectives.** Backups from Storage Snapshots enables running a backup at any time and with any frequency, reducing exposure to data loss.
- **Minimized impact on production environment.** This removes the requirement for creating native VM snapshots, therefore the associated impact of a snapshot removal operation is eliminated. This dramatically reduces the performance impact on production VMs during the backup window.

- **Agentless, application-aware backup** across multiple applications, such as Microsoft Active Directory, Exchange, SharePoint, SQL Server and Oracle.

Veeam Backup Remote Access

Veeam Backup Remote Access further empowers Veeam Cloud & Service Providers (VCSP) partners to deliver managed services by enabling VCSP support staff to remotely connect to a tenant's backup server with the Veeam Backup & Replication console, as well with the Remote Desktop client over the existing Cloud Connect tunnel, without needing to establish VPN connectivity first. This enables remote support, troubleshooting and management of the tenant's backup and replication jobs — and the backup server itself.

Veeam Agents Support

Ensure uninterrupted backup of your physical and cloud workloads into a Veeam repository with full support for the latest releases of Veeam Agent *for Microsoft Windows* 2.0 and Veeam Agent *for Linux* 1.0 Update 1.

Veeam Backup & Replication 9.5 Update 2 includes over 300 other enhancements and bug fixes, the most significant of which are listed in the Release Notes document [KB2283](#).

Veeam Backup & Replication 9.5 Update 1: What's New?

VMware vSphere 6.5 support

Update 1 focuses on delivering full support for VMware vSphere 6.5, including the following new major platform features:

- **Encrypted VMs support.** VMware vSphere 6.5 introduces VMs with encrypted disks. VMs can be backed up in hot add and network (NBD) transport modes only, with hot-add mode requiring that the backup proxy itself is an encrypted VM.
- **VMFS6 and VVOLs 2.0 support.** VMware vSphere 6.5 introduces the new versions of VMFS and VVOL (Virtual Volumes), which are fully supported with this update. This includes support for advanced functionality such as Backup from Storage Snapshots and Veeam Explorer for Storage Snapshots for VMs with virtual disks residing on VMFS 6 datastores.
- **Virtual hardware version 13 support.** VMware vSphere 6.5 introduces a new VM hardware version which increases some configuration maximums and adds the ability to add NVMe controllers to a VM. This update adds the ability to process such VMs.

Veeam Agents *for Linux* Integration

Update 1 enables users to take full advantage of Veeam backup repositories as additional target locations for your Veeam Agent *for Linux* jobs. Using a Veeam backup repository as the target for your backup jobs enables the following additional functionality:

- **Centralized monitoring.** Perform basic monitoring and management for all incoming agent backup jobs, including email notifications on agent backup status.
- **Offsite protection.** Get agent backups off site to disk-based storage, tape or to Veeam Cloud Connect service providers with Backup Copy and Backup to Tape jobs.
- **Backup encryption.** Now, users can choose to optionally encrypt agent backups stored in Veeam backup repositories. All standard Veeam encryption features are supported for endpoint backups, including password loss protection.
- **Disk export.** Export physical disk content from backup into VMDK/VHD/VHDX virtual disk files.

Veeam Backup & Replication 9.5 Update 1 includes over 300 other enhancements and bug fixes, the most significant of which are listed in the Release Notes document [KB2222](#).

Veeam Backup & Replication 9.5: What's New?

Enterprise scalability enhancements

The exponential growth of data and provisioned IT services is forcing businesses and enterprises of all sizes to rethink their Availability strategy. Through a host of new enterprise enhancements, Veeam scales efficiently and effectively, regardless of environment size and number of VMs.

Backup acceleration technologies double I/O performance and shorten backup windows by up to five times – all while reducing load on primary storage, backup storage and vCenter Servers. Features include:

- **Advanced data fetcher.** Improves backup performance for individual virtual disks up to two times on enterprise-class primary storage while significantly reducing the load on primary storage due to the reduced number of I/O operations required to complete a backup, improving its Availability to production workloads. Advanced data fetcher is available for the VMware platform and the following processing modes: Backup from Storage Snapshots, Virtual Appliance (Hot-Add) and Direct NFS.
- **VMware vSphere infrastructure cache.** Maintains an in-RAM mirror of vSphere infrastructure hierarchy to dramatically accelerate job start up (Building VM list operation) and user interface responsiveness while browsing a virtual infrastructure. This approach removes the load from a vCenter Server, making it more available to perform its core infrastructure management duties, and improves backup success ratio in the environments where jobs would often time out or fail due to an overloaded vCenter Server. The cache is maintained up-to-date with real-time updates via a subscription to vCenter Server infrastructure change events.
- **Highly optimized vSphere infrastructure queries.** Help ensure vSphere API queries complete faster and minimize vCenter Server load when full vSphere infrastructure hierarchy retrieval is required. For example, this is helpful after a backup server is rebooted or Veeam Broker Service (the service hosting the vSphere infrastructure cache) is restarted.

Restore acceleration technologies, including custom-tailored logic for raw disk, deduplicating storage and tape, greatly improve VM restore performance regardless of the restore scenario, including:

- **Instant VM Recovery®** has improved performance up to three times depending on the scenario, with a majority of the improvement observed when recovering multiple VMs at once from per-VM backup file chains.
- **Parallel processing for full VM restore restores** multiple disks in parallel, similar to the way backup is performed. This technique is automatically used for all disk-based backup repositories except Dell EMC Data Domain deduplicating storage.
- **Data Domain accelerated restores** use custom tailored logic during both backup and restore time to ensure maximum full VM restore performance. A portion of this logic introduces changes to the way backups are created on Data Domain storage, so a majority of the performance increase is experienced on newly created backups.
- **Direct restore from tape.** Now, users can perform a full VM restore directly from tape, without the requirement of staging the necessary VM backup files in a repository first. This improves RTO and eliminates the need of locating a repository with sufficient, free disk space to accommodate all of the backup files required to perform the restore. Performing a restore through a staging repository remains an option for when you need to restore a large number of VMs from the same backup file, in which case a restore through a staging repository may improve recovery times.

Engine enhancements. Veeam Backup & Replication 9.5 also includes a wide range of additional enhancements enabling users to scale for very large environments and maintain efficiency when processing jobs containing thousands of VMs or millions of files.

- **Major configuration database optimizations** allow for queries to complete faster while simultaneously reducing back-end SQL Server load, significantly improving user interface responsiveness and job performance. Please note that due to the fact that a portion of these optimizations leverage advanced capabilities available only in SQL Server 2008 or later, SQL Server 2005 is no longer supported as the configuration database.

- **Accelerated metadata processing** improves the performance of jobs containing VMs with a large number of supported applications installed, as well as when applications require large amounts of metadata to be stored as part of the backup (for example, Microsoft SharePoint server with thousands of sites).
- **Purpose-built user interface controls** improve responsiveness and reduce the configuration database load on grids with tens of thousands of objects (e.g., when a user clicks on the Backups node of the management tree).
- **File to Tape performance** has improved by up to 50x when processing large amounts of very small files, making it up to 50% faster than leading legacy tape backup solutions on the same workload. The new engine was tested with 20 million files per job, enabling users to efficiently protect unstructured data to tape or VTL targets.

Advanced Resilient File System (ReFS) integration for Windows Server 2016. The new ReFS 3.1 file system offers greater performance and capacity efficiencies for large-scale datasets, while ensuring backup data resiliency and the protection of business-critical applications through:

- **Fast clone technology** allowing for the creation and transformation of synthetic full backup files to happen up to 20x faster for shorter backup windows and a significantly reduced backup storage load. Backup and restore performance can be further improved with automatic storage tiering provided by a Storage Spaces Direct-based backup repository with an SSD tier.
- **Reduced backup storage consumption** with spaceless full backup technology preventing duplication from occurring, resulting in raw disk space consumption by a Grandfather-Father-Son (GFS) backup archive that rivals deduplicating storage appliances. Further, unlike deduplicating storage, by integrating software dedupe and encryption with advanced ReFS capabilities, these storage savings remain even for encrypted backup files.
- **Ensuring backup archive integrity** and addressing silent data corruption ("bit rot") by monitoring and proactively reporting data corruption with ReFS data integrity streams, including automated and seamless healing of corrupted backup file data blocks inline during restore or during periodic scans of the ReFS data scrubber by leveraging Storage Spaces mirror and parity sets.

Advanced ReFS integration requires a Windows Server 2016-based backup repository backed by a local volume or shared folder. A backup repository must be created after upgrading to 9.5, and backup files must be created on the ReFS volume by the backup job, instead of being copied from another repository.

All of the enterprise scalability enhancements are available in all three product editions, as well as Veeam Backup Free Edition.

FULL integration with Microsoft 2016 data center technologies

Veeam's FULL integration with Microsoft 2016 data center technologies modernizes private cloud platforms and enterprise applications through full support for:

- **Windows Server 2016**, enabling users to install Veeam Backup & Replication components and protect guest VMs running on Windows Server 2016 with application-aware processing and guest file system indexing — all without requiring a direct network connection to the processed Windows 10 or Windows Server 2016 VMs, by leveraging new PowerShell Direct capabilities
- **Microsoft Hyper-V 2016 and Microsoft System Center Virtual Machine Manager 2016 (SCVMM)**, including:
 - **Support for the new Hyper-V 2016 backup framework** that is not reliant on volume snapshots by software or hardware VSS providers coordinated with guest VSS processing. This dramatically improves the Hyper-V backup success ratio in large and busy environments. Please note that both on-host and off-host backup modes remain supported with the new framework.
 - **Support for Hyper-V's Resilient Change Tracking (RCT)** reduces complexity by eliminating the need to run an additional filter driver in the parent partition for changed block tracking functionality for backups, replicas and restores. Unlike Veeam's proprietary changed block tracking, RCT is also supported with third-party SMB3 storage.
 - **Support for Microsoft Hyper-V hosts installed on Nano Server** in on-host backup mode, including support for Storage Spaces Direct, enabling users to immediately deploy Microsoft's recommended Hyper-V 2016 architecture, reducing the size of data center footprints.

- **2016 Microsoft enterprise applications.** Support for 2016 releases of Microsoft enterprise applications is also included, providing application-aware processing for Microsoft Active Directory, Exchange, SharePoint and SQL Server, as well as application item-level recoveries through the corresponding Veeam Explorers™ for each application, ensuring high-speed recovery through fast RTOs of < 15 minutes.

All functionality is available in all product editions, including Veeam Backup Free Edition.

Veeam Restore to Microsoft Azure

Veeam Restore to *Microsoft Azure* delivers cloud restore for backups created by ANY Veeam product, optimizing resource allocation to deliver improved scalability and increased IT efficiency, while minimizing operating costs and limiting capital expenditures. It enables users to take on-premises workloads and restore or migrate them to Azure through an automated P2V or V2V conversion process. Users can:

- Quickly restore Windows and Linux-based VMs, physical servers or endpoints to Azure to minimize business disruption.
- Execute planned workload migrations from on site to the cloud to reduce on-site resource constraints.
- Easily create an Azure-based environment for development and testing. For example, users can test patches and updates to mitigate risks associated with new application version deployment.

In comparison to the technology preview of the Veeam Restore to *Microsoft Azure* appliance released in March 2016, the following new functionality has been added:

- **Restore directly** from a UI without needing to deploy an Azure appliance, copying backup files to it or managing the process in a separate UI. Now, users can simply right-click any backup and restore it directly to Azure.
- **Restore Linux computer backups** created by Veeam Backup & Replication and Veeam Agent for Linux, including automated UEFI to BIOS conversions.
- **Perform parallel disk restore** for faster restore of computers with multiple disks.
- **The Azure proxy** accelerates restores up to 10x by optimizing data transfers to the Azure data center. By leveraging Veeam Cloud Connect technology, data transfers are performed over a single port using encrypted TLS connection, simplifying firewall configurations and removing the need to establish VPN connections to Azure. The Azure proxy VM takes just a few clicks to deploy directly from the Veeam UI, and can be powered off automatically after specific periods of inactivity to reduce Azure consumption costs. Using the Azure proxy is optional.
- **Tighter Azure integration** includes the automated installation of Azure Virtual Machine Agent for Windows VMs, the enabling of Windows firewall rules for Remote Desktop and support for the new Azure Resource Manager deployment model.

Veeam Restore to *Microsoft Azure* is available in all product editions, including Veeam Backup Free Edition.

Instant Recovery from ANY backup

Veeam invented Instant VM Recovery. Now, we are introducing Instant Recovery for physical computers! Veeam Backup & Replication 9.5 enables users to perform instant recovery of endpoints and physical servers into a Hyper-V VM. This provides the ability to:

- Immediately spin up a failed physical server from a backup, providing time to perform troubleshooting and/or acquiring replacement parts
- Run lost laptops directly from their last backup until a replacement is acquired, providing users access via an RDP connection from any thin client that supports RDP (e.g., a smartphone, a tablet)
- In conjunction with Veeam Cloud Connect, enterprises and service providers can manage complete disaster recovery (DR) of remote offices and tenant locations by spinning up backups delivered to the main data center by Veeam Cloud Connect, as Hyper-V VMs

Instant Recovery is supported from backups created by Veeam Endpoint Backup™ FREE 1.5, but will work best with Veeam Agent for *Microsoft Windows* 2.0 or later due to additional information collected about the computer during backup.

Instant Recovery is available in all product editions, including Veeam Backup Free Edition. Please note that this functionality requires Microsoft Hyper-V. If you do not have a Hyper-V infrastructure, you can simply enable the Hyper-V role on the backup server itself.

Nimble storage snapshot integration

Expanding on existing integrations with Hewlett Packard Enterprise (HPE), NetApp and Dell EMC, Veeam extends its direct storage snapshot support to Nimble Storage users to help reduce the impact on production environments and achieve lower recovery time and point objectives (RTPO™) with:

- **Backup from Storage Snapshots.** Lower the additional impact from backup activities on production storage by retrieving VM data from storage snapshots on primary storage and replicated copies on secondary storage.
- **Veeam Explorer for Storage Snapshots.** Recover individual application items, guest files or entire VMs quickly and efficiently from storage snapshots on primary storage and their replicated copies on secondary storage systems – whether they were created by a Veeam job or a native snapshot scheduler.
- **On-Demand Sandbox™ for Storage Snapshots.** Use storage snapshots on primary and secondary storage systems to create complete isolated copies of production environments in just a few clicks for dev/test and troubleshooting purposes.

Nimble storage snapshot integration requires Enterprise *Plus* edition, with the exception of Veeam Explorer for Storage Snapshots which is available in all product editions, including Veeam Backup Free Edition.

Enhanced VMware vCloud Director support for service providers.

Maintaining IT efficiency and agility requires a new approach to keeping Infrastructure as a Service (IaaS) models Always-On. Simplify management, increase efficiency and improve confidentiality by empowering vCloud Director tenants with a self-service backup and restore portal based on Veeam Backup Enterprise Manager, including:

- **Native vCloud authentication and integrated access scoping** allows tenants to continue to use their existing vCloud Director credentials for the self-service portal and restricts them from being able to backup and restore only the VMs belonging to their respective organizations. This enhances the tenant experience and reduces costs for the service provider, as any tenant change (e.g., disabling a tenant, changing passwords or adding new vApps or VMs) is immediately reflected in the portal.
- **Self-service backup** allows tenants to maintain better control over their backups by controlling existing jobs and creating new ones. Job setup is simplified so tenants only need to select VMs to perform backups of, as well as select essential parameters such as guest credentials, retention and notifications. Tenants are blocked from accessing advanced settings, such as repository or backup mode selection, which are managed by service providers through job templates.
- **Self-service restore** allows tenants to perform a wide variety of restore options for VMs that Veeam Backup Enterprise Manager currently provides including application items, guest files, full VM and full vApp restores. These restores can now be easily performed in just a few clicks by tenants themselves, improving RTOs and reducing costs for service providers.

Access to the self-service backup and restore portal requires the Enterprise *Plus* edition.

Additional enhancements

As a result of ongoing research and development efforts and in response to customer feedback, Veeam Backup & Replication 9.5 also includes an extensive range of additional features and enhancements, including the most significant listed below. All enhancements are available in all product editions featuring the corresponding functionality, unless stated otherwise.

Engine

- **Parallel processing of per-VM backups.** Health check and compact operations will now process each backup file chain in parallel when per-VM backup file chains are used.
- **Proxy affinity.** This new backup repository setting allows users to specify backup proxies which are allowed to perform backups to and restores from the chosen repository. This capability is useful in a variety of scenarios, including keeping backup traffic local to multiple all-in-one Veeam backup appliances. This functionality is available in Enterprise and Enterprise *Plus* editions only.
- **Retention check after backup job failure.** Jobs will now apply a retention policy even if the backup itself fails. This will allow customers with an overfilled backup repository to lower the retention in the job settings, and apply the new setting so new backups can be created. However, please note that jobs in forever forward incremental backup are unable to simply delete the oldest backups due to a full backup file merge requirement.
- **GFS retention enhancement.** To reduce the requirements for archive repository disk space, the oldest GFS full backup will now be removed before a new GFS full backup file is sealed and a new synthetic full is created.
- **Backup Copy job performance enhancements.** Backup Copy jobs should now initialize much faster and no longer cause load on virtual infrastructures due to obtaining the required information about processed VMs from the configuration database instead of the infrastructure.
- **Preferred networks for Linux.** Preferred network settings now also apply to managed servers running Linux.
- **Network throttling for Quick Migration.** Quick Migration operations will now adhere to network consumption throttling rules.
- **Restore audit data retention.** Restore operations audit events will now adhere to global event retention rules to avoid overfilling the configuration database.
- **Third-party components updated.** A number of third party engine components have been updated for enhanced stability and security, particularly OpenSSL to address its latest vulnerabilities.

vSphere

- **Direct NFS priority over Hot-Add.** To prevent undesired VM stun issues from hot adding virtual disks located on an NFS share, Intelligent Load Balancing will not leverage Virtual Appliance (hot add) proxies as long as at least one Direct NFS capable proxy is available.
- **Direct NFS proxy location awareness.** Intelligent Load Balancing now automatically selects the best Direct NFS proxies based on the number of hops to the datastore, providing optimal proxy selection in distributed environments.
- **Thick disk type selection.** Users can now choose thick disk type (lazy zeroed or eager zeroed) when performing a full VM restore or setting up a replication job. Choosing to preserve the source disk type will also distinguish between and preserve the correct thick disk type.
- **Replica VM count balancing.** When replicating to a cluster, each replica VM is now created on the host with least VMs registered at the time of replica VM creation.
- **NBD connections limit increase.** The legacy limit for the maximum amount of virtual disks processed by NBD transport has been increased from 7 to 28 for ESXi 5.0 or later hosts, based on their architectural differences around NFC connections handling.

Hyper-V

- **Performance enhancements.** Jobs processing legacy Hyper-V host versions (2012 R2 and earlier) should now initialize up to 2x faster due to the accelerating Building VMs list, CSV enumeration and VM ownership retrieval operations.
- **VLAN remapping.** Added the ability to map VLANs in virtual networks mapping the rules of the replication job wizard.

Primary storage integrations

- **Protocol selection.** For primary storage supporting multiple protocols (FC/iSCSI/NFS), users can now select the protocols used by Veeam to prevent backup jobs from attempting to connect to storage over undesired interfaces.
- **Proxy selection.** Users can now select the specific backup proxies to be used for storage rescan and backup from storage snapshot operations.

Dell EMC Data Domain

- **DD OS 5.7 support.** Updated DDBoost SDK to version 3.1 for added support of DD OS 5.7.

HPE 3PAR StoreServ

- **Virtual Domains.** Added support for 3PAR Virtual Domains feature.
- **VLAN tagging.** Added support for 3PAR iSCSI VLAN tagging feature.

HPE StoreOnce

- **Increased limits.** The maximum number of supported increments in a backup chain now depends on the StoreOnce model used for the backup repository, instead of being limited to seven for all StoreOnce models.
- **Traffic control.** The ability to control Catalyst traffic check summing and compression settings in the StoreOnce wizard has been added to enable these settings to be optimized for the network used for backup and copy.
- **Bandwidth mode control.** The Catalyst bandwidth mode is primarily based on the Catalyst store setting, instead of being forced to high bandwidth mode.
- **Catalyst over FC enhancements.** The reliability of establishing Catalyst over FC connection to StoreOnce in cases when all available FC connections are occupied has been increased.
- **Catalyst update.** The StoreOnce Catalyst software integrated with 9.5 has been updated to the latest version 3.14 and features various performance optimizations.

NetApp

- **Data ONTAP 9.0 support.** Added support for NetApp Data ONTAP version 9.0.
- **Data LIF support.** Backup from Storage Snapshots will now fetch virtual disk data LIF (logical interface) belonging to the NetApp cluster node hosting the processed virtual disks, as opposed to picking the fastest LIF. This will remove the unnecessary load on the node with the fastest LIF, as well as the cluster network.
- **SVM Root Volume Protection support.** Added support for the Clustered Data ONTAP 8.3 SVM Root Volume Protection feature.

Scale-out Backup Repository™

- **Temporary expansion.** Enterprise edition users are now allowed to add a fourth extent, even though no more than three extents can be online at the same time, with the fourth remaining in maintenance mode. This will help with upgrading Scale-out Backup Repository capacity by attaching a larger storage unit, followed by evacuation of backups from the smallest one.

Application-aware processing

- **Oracle on SUSE support.** Added support for application-aware processing and redo log backup for Oracle servers installed on SUSE Linux Enterprise Server (SLES) versions 11 and 12.

- **Oracle Data Guard support.** Added support for application-aware processing and redo log backup for Oracle servers using Data Guard.
- **Veeam Backup for Microsoft Office 365 support.** Added support for application-aware processing of Veeam Backup for Microsoft Office 365 servers.

File-level recovery

- **OES 2015 support.** Added support for file-level recovery from 64-bit NSS volumes and AD-enabled NSS volumes on Open Enterprise Server 2015.
- **Copy to credentials.** A file-recovery attempt to a shared folder requiring credentials will now prompt users for credentials with Multi-OS File Level Recovery.
- **File-level recovery performance.** Increased Windows file-level recovery performance up to 3x depending on the scenario.

SureBackup

- **Domain Controller roles.** Added the dedicated Active Directory domain controller roles which instruct SureBackup® jobs to perform authoritative or non-authoritative domain controller restore respectively.
- **Veeam Backup for Office 365.** Added the dedicated role for Veeam Backup for Microsoft Office 365 servers.

Veeam Explorers

- **Lazy database load.** All Veeam Explorers will now mount database files to restore from as needed, as opposed to automatically mounting all known databases at start up.
- **Traffic flow optimization.** Restore traffic no longer flows through the console, but goes directly from repository mount server to the target server.
- **Improved user interface.** All Veeam Explorers now feature context-sensitive toolbar ribbons.

Veeam Explorer for Microsoft Active Directory

- **Windows Server 2016 Directory Services support.** Added support for Active Directory object-level recovery from forests running in 2016 functional level (including user and computer account password restore).
- **Expiring links.** Uniquely, support for expiring links restore, a new feature of Windows Server 2016 Directory Services, includes export to LDF file, functionality that is not available in the native LDIFDE utility.

Veeam Explorer for Microsoft Exchange

- **Restore from Purges folder.** Added support for restoring items from the Purges folder used by Exchange when Litigation Hold or single-item recovery features are enabled. Veeam Explorer will present these items under the Litigation Hold Items and In-Place Hold Items mailbox folders, respectively, in the mailbox folder tree.
- **Veeam Backup for Microsoft Office 365 support.** Added support for restoring from archive databases (.ADB files) created by Veeam Backup for Microsoft Office 365 – both from local files or by connecting directly to an archive server.

Veeam Explorer for Microsoft SharePoint

- **SharePoint 2016 support.** Added support for item-level recovery from Microsoft SharePoint 2016 content databases.
- **Site restore report.** Added detailed site restore report detailing restore status for each site object.

Veeam Explorer for Microsoft SQL Server

- **SQL Server 2016 support.** Added support for database-level, table-level and SQL object-level recovery from Microsoft SQL Server 2016.
- **Additional table types support.** Added support for restoring SQL objects from the following table types: System-versioned temporal table, memory-optimized table (in-memory OLTP) and file table.

- **Restore performance enhancements.** Improved database restore performance up to 3x in all SQL Server deployment scenarios, including blob stores.

Veeam Explorer for Oracle

- **Dynamic parameters restore.** Added support for restoring dynamic database parameters.
- **Restore performance enhancements.** Slightly improved database restore times by accelerating specific database management operations.

Veeam Backup Enterprise Manager

- **Scalability enhancements.** The Enterprise Manager engine was heavily optimized for very large environments and tested against databases containing one million restore points. Additionally, reporting performance, web UI responsiveness and new backup server registration times were significantly improved for large environments.
- **Oracle database restore.** The self-service, application-item level recovery functionality was expanded with self-service Oracle database restores by delegated database administrators.
- **Exchange mailbox item restore improvements.** Added CAS server auto discovery and enhanced certificates handling logic.
- **Improved self-service capabilities.** In light of adding a self-service backup and restore portal for vCloud Director, the Enterprise Manager web UI was enhanced with new capabilities to perform Quick Backup operations on the VMs tab, as well as delete backup jobs, backup files and erase individual VMs content from multi-VM backup files.
- **1-Click FLR for agent backups.** Guest file system catalog search and 1-Click File Level Recovery is now supported for backups created by Veeam Agent for *Microsoft Windows 2.0* and Veeam Agent for *Linux 1.0*.
- **Concurrent catalog search.** Multiple web UI users are now able to perform guest file system catalog searches concurrently without commonly experiencing timeouts.

Veeam Cloud Connect (Tenant)

- **Parallel processing.** Tenants can now back up or replicate multiple VMs and disks in parallel, based on the concurrent task limit set by the service provider, thus improving job performance on fast links. Please note that parallel processing applies to direct transport mode only, as built-in WAN accelerators will still process disks sequentially regardless of this setting.
- **Replication from backup in a cloud repository.** Tenants can now perform replication from a backup residing in a cloud repository, enabling a new DR option without generating additional network traffic or impacting production VMs.
- **Security enhancements.** Veeam Cloud Connect service will now attempt to use more secure TLS 1.2 and TLS 1.1 authentication algorithms when establishing a connection to the service provider. In addition, failover to SSL 3.0 has been explicitly disabled for all Veeam Cloud Connect components.
- **Configuration backup to cloud repository.** Added support for performing configuration backups to a cloud repository, except for those backed by a scale-out repository.

Veeam Cloud Connect (Service Provider)

- **Per-VM backup file chains support.** Cloud repositories can now be backed by backup repositories with the per-VM backup file chains setting enabled to improve scalability and better support for deduplicating storage appliances.
- **Scale-out Backup Repository support.** Cloud repositories can now be backed by scale-out backup repositories to simplify backup storage management and save costs for service providers. The supported process for migrating existing tenant backups from simple repositories to scale-out backup repositories will be provided by Veeam. For more information, please refer to Veeam Cloud & Service Provider Forum.

- **Advanced ReFS integration support.** Cloud repositories backed by backup repositories meeting the requirements for Advanced ReFS Integration fully support the corresponding functionality.
- **Improved diagnostic logging.** Multiple improvements were made to specific areas of tenant job logging where it was possible to do so without exposing a tenant's confidential information.

Tape

- **Automatic tape driver cleaning.** Yes, finally! The backup server will now monitor tape drive status events and automatically perform a cleaning as required, as long as the cleaning cartridge is available in the tape library.
- **Tape job priority.** We have heard you loud and clear, and added an option to delay primary jobs start up while tape jobs are still processing some of the required backup files, instead of killing the tape jobs immediately.
- **Waiting for tape notification improvements.** The email report and job Action log message now contain information about the tape device and media pool that lacks free media.
- **Adjustable GFS media set retention.** Similar to simple media pools, it is now possible to change the retention for previously written tape media within any GFS media set.
- **Additional media set variable.** Added "month numeric" variable to media set naming variables.
- **Tape job wizard enhancements.** Now, you can select multiple files to add to a File to Tape job at once, see additional information about the selected media pool in the tape job wizard, and specify linked backup job wait time in hours (in addition to minutes).
- **Backup operator permissions.** Veeam Backup Operators user role is now allowed to perform essential tape infrastructure management operations such as inventory, eject, rescan etc.
- **Other optimizations.** Additional optimizations include multiple, under-the-hood enhancements improving stability and performance of GFS archival, parallel processing, tape encryption, file-level recovery and catalog operations.

User interface

- **New VeeamZIP™ retention options.** Additional VeeamZIP backup retention options of three months, six months and one year have been added to existing options for customers using VeeamZIP as a VM archival tool.
- **Free space threshold for production datastores.** You can now set the percent of free disk space on the production datastore, indicating when jobs should issue a warning or fail completely instead of creating a VM snapshot to prevent the datastore from overflowing with snapshot data. This is an addition to the existing BlockSnapshotThreshold registry value (default is 2GB), which continues to serve as the last line of defense when the above functionality is disabled, as is the case for upgrading users. The new settings can be found under Options > Notifications.
- **Proxy selection.** You can now specify the proxy and disk type to use when exporting backed up volume as a virtual disk.
- **Restricted hours warning.** We will now display a warning if a user attempts to start a job during restricted hours. This is defined in the job's backup window setting.
- **Color themes.** For those of you who find Veeam Green to be too acidic, we now provide three additional color themes featuring neutral colors. The color theme is a per-user setting attaching to a specific backup server, allowing users to color-code backup servers to more easily distinguish between them during Alt-TAB.

PowerShell

- **More lenient execution policy support.** The Veeam PowerShell extension execution policy requirement has been lowered from RemoteSigned to Bypass.
- **Ongoing enhancements** with new cmdlets added to cover all new 9.5 functionality, as well as multiple enhancements to existing cmdlets based on user feedback.

Enhancements for service providers

- **Configuration backup and restore enhancements.** By popular demand, the configuration backup email report now includes backup server name. Additionally, Veeam Cloud Connect server configuration database migration is now fully supported by a configuration restore in Migration mode.
- **RESTful API enhancements.** Added support for managing Backup Copy jobs and backup files, expanded existing APIs for file-level recovery and job scheduling according to feedback, and implemented many smaller enhancements.
- **Trial VMs.** With per-VM rental licenses, the product will now track newly added VMs separately for the purpose of built-in usage reporting. Such VMs will not be included in the usage reports until the following month.



Learn more
www.veeam.com



Download free trial
vee.am/backup