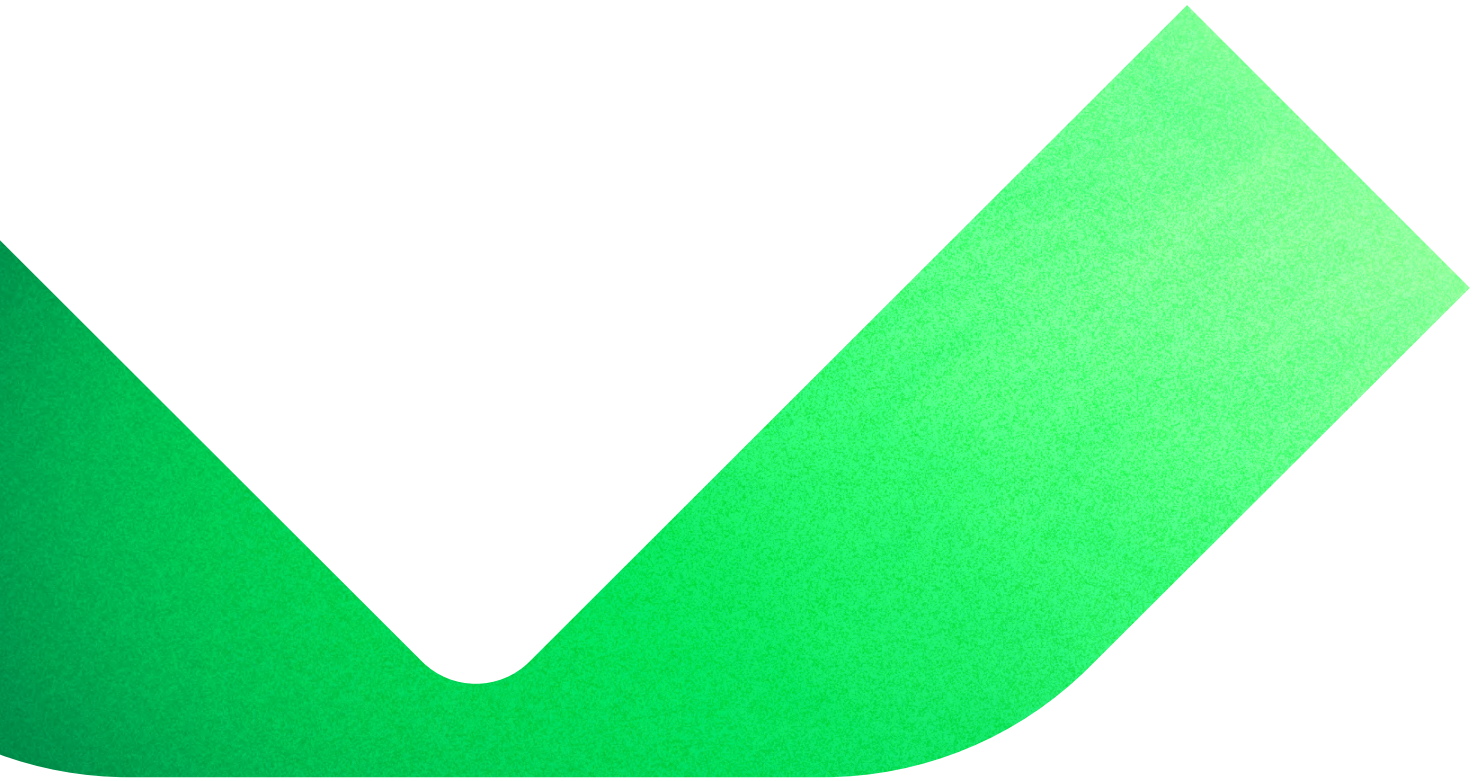
Veeam Backup & Replication v12.2

What's New



Contents

Introduction

Veeam Backup & Replication, the workhorse of Veeam Data Platform, delivers enterprise-grade resiliency capabilities that ensure your protection, response, and recovery in the face of classic disasters and modern cyberattacks across the hybrid cloud. The following is a list of major new features and enhancements added in Veeam Backup & Replication v12.2. All of these capabilities are transacted as Veeam Data Platform, with certain features available only in Advanced or Premium editions.

New Datacenter Workload Support

Proxmox VE

Native support for host-based backups of Proxmox VE virtual machines (VMs) gives users even greater freedom to choose what best fits their changing business needs for virtualization and the cloud. Key highlights of Veeam's integration with Proxmox VE include:

Immutable backups: Keep Proxmox VE VM on-premises and cloud backups safe from encryption by ransomware, accidental deletion, or malicious destruction during cyberattacks with the help of storage-based immutability. Alternatively, leverage native support for tape and rotated drives to achieve true air-gapping at the lowest possible price point.

Uncompromised backup performance: Powered by advanced changed block tracking (CBT) integration and HotAdd backup mode, Proxmox VE users can now leverage fast and efficient VM backups to minimize disruptions from long-running backups and ensure smooth day-to-day operations. Veeam is the first to bring support for CBT backups of even powered-off VMs to the market.

Veeam BitLooker: By automatically excluding unused disk blocks, like those belonging to deleted guest OS files, this intelligent feature significantly enhances backup performance and conserves valuable storage space.

Storage flexibility: Offers support for all Veeam Backup & Replication backup repository types, including hardened repositories and object storage. This empowers businesses to easily create backup repositories from any storage that suits their recovery time objective/recovery point objective (RTO/RPO) requirements and budget.

Freedom with full VM recovery: VMs from leading virtualization platforms (e.g., VMware vSphere, Microsoft Hyper-V, Nutanix AHV, Red Hat Virtualization, and Oracle Linux Virtualization Manager) or the public cloud (e.g., AWS, Microsoft Azure, and Google Cloud) can be promptly restored to Proxmox VE. This can be done the other way around too, which reduces downtime and maximizes productivity. You can also restore your physical server backups to Proxmox VMs, which simplifies disaster recovery (DR) and P2V migrations.

Advanced granular recovery capabilities: Quickly recover all changed and deleted files in case of ransomware attacks or other disasters. This ensures business continuity and peace of mind in the face of unexpected data loss or unplanned disruption.

Nutanix AHV

The new major update for our Nutanix AHV integration represents a fundamental evolution of our support for enterprise AHV environments. This is due to improved centralized management, expanded functional capabilities, and backup architecture simplification.

Prism Central integration: Support your backup operations across Prism Central-managed clusters from a single backup appliance that yields a unified and easy-to-use backup architecture.

Dynamic backup job scope: Leverage Prism Central VM categories (a.k.a., "tags") to facilitate automatic VM inclusion into backup jobs based on Prism Central VM category affiliation.

Backup from secondary VM copies: For Nutanix replication-enabled environments, backup from VM replicas may be enabled with a single checkbox. This allows for backup operations to be offloaded from production clusters, which reduces the impact on production environments. If the replica copy is out of RPO compliance or otherwise unavailable, backup processing will fail back to the production VM instance.

Multiple network adapter support: Both AHV appliances and workers can now leverage multiple network interfaces for improved data processing efficiency.

Advanced job settings: You can now customize job compression level and block size, as well as configure BitLooker options to further reduce backup size and improve performance.

Gmail and Microsoft 365 support email notifications: In addition to basic SMTP servers, V6 now supports Gmail and Microsoft 365 with their OAuth 2.0 protocol-based secure authorization and access token-based authentication.

Resources view: The new VM inventory view of the web interface summarizes your protection posture across managed clusters and lets you add VMs to existing protection policies in a single click. The view is customizable per cluster, protection status, and protection type.

RestAPI enhancements: This includes Prism Central management scope enhancements and multiple network management.

MongoDB

Native backup and recovery support for MongoDB on Linux, the world's most popular NoSQL database, lets you perform backups at the per-replica set level without having to create and manage pre-freeze and post-thaw scripts. We've designed this feature to provide a seamless, simple, and intuitive Veeam user experience while maintaining our connection to the native tool's experience (OpsManager). This means that both database and backup administrators can effortlessly work with our solution without needing extensive knowledge of either Veeam Backup & Replication or MongoDB. Key highlights of Veeam's MongoDB integration include:

Simple discovery: Just add your MongoDB replica sets to our new dedicated protection group and Veeam will automatically identify all replica set members, discover the application topology, and install the necessary backup components on each replica set node.

Backup flexibility: Your backup policy can be populated with either individual replica sets or entire protection groups. This feature also offers the unique ability to select your preferred node for data retrieval either manually or automatically. This capability ensures that your protected data is retrieved only once, which minimizes the impact from backup activities on your production environment.

Storage flexibility: Support for all Veeam Backup & Replication backup repository types, including hardened repositories and object storage, empower businesses to easily create backup repositories from any storage that suits their RTO/RPO requirements and budget.

Proven backup engine: Behind the scenes, MongoDB protection uses the existing volume-level backup engine from Veeam Agent *for Linux*. This makes many of the features like immutable backups, synthetic full backups, GFS retention policies, encryption, backup copy jobs, and more available upon first release of this new capability.

Veeam Explorer *for MongoDB:* This new addition to the Veeam Explorer family provides users with the flexibility to restore individual collections and databases for day-to-day operational restores, or entire MongoDB instances for DR. Both can be restored to their original or alternative locations.

IBM Db2

Linux on Power support: Looking for a reliable solution to safeguard Db2 workloads that run on Linux on Power? Our updated Veeam Plug-in for IBM Db2 now offers its complete functionality on Power platforms as well! This plug-in operates in standalone mode and supports the same deployment types as our existing plug-in for AIX and Linux x86_64 platforms.

SLES 15 SP5 support: We added full support to allow the plug-in to operate on SLES 15 SP5 distribution. For a complete list of supported OS distributions, refer to the compatibility matrix available in our help center.

SAP HANA

RHEL 9.4 support: Added full support to allow the plug-in to operate on RHEL 9.4 for SAP HANA and RHEL 9.4 for SAP Solutions distributions on both Linux x86 64 and Linux on Power platforms.

Veeam Agent *for Linux*

Latest Linux distribution version support: This new Agent version adds full support for OpenSUSE 15.6, SLES 15 SP6 (for x86_64), and Debian 12.6.

VMware Cloud Director

Full VMware Cloud Director 10.6 support: In addition to the basic compatibility that comes with version 12.1.2 for backup and restore only, this new release delivers full support for this VMware Cloud Director version, including the updated vSphere Web Client plug-in and Veeam Continuous Data Protection (CDP) support.

VMware vSphere

Full vSphere 8.0 Update 3 support: As opposed to the compatibility-level support for vSphere 8.0 U3 provided by version 12.1.2, version 12.2 delivers full support for this vSphere version without requiring you to apply workarounds.

New Cloud Workload Support

Amazon AWS

Amazon Redshift Cluster protection: Manage your Redshift Cluster protection alongside the other AWS workloads you protect with Veeam. Plus, benefit from flexible policy-based scheduling and experience seamless Redshift Cluster recovery in case of disaster.

Amazon FSx protection: Manage your FSx file system protection alongside the other AWS workloads you protect with Veeam. Plus, benefit from flexible policy-based scheduling and experience seamless file system recovery to the original or new location.

Microsoft Azure

Data Lake

Protect production data that resides in Microsoft Azure Data Lake (Gen2) with the powerful backup and recovery functionality that's built on storage-agnostic architecture. Veeam helps you achieve your data recovery objectives without requiring additional hardware investments. The unique benefits of Veeam's backup engine include:

Scalable storage-agnostic architecture: Utilize a proprietary distributed file system that's specifically built to protect of billions of objects — of PBs in size — to a storage target of your choice. You get the complete freedom to direct your backups to object storage or a Scale-out Backup Repository (SOBR) that's built on standard server hardware with internal or directly attached storage.

Efficient forever-incremental backups: This innovative "forever-incremental" engine eliminates the need for periodic active full backups. This efficiency enables users to protect petabyte-sized data buckets with significantly reduced RPOs.

Changed object tracking: A unique approach to monitor modifications delivers industry-leading incremental backup performance. You can now achieve low RPOs without needing native changed object tracking in your object storage.

Naturally, Data Lake backup jobs also come with all the standard Veeam features, such as encrypted backups, backup copies, pre- and post-job scripting for automation, and multiple notification options.

Cosmos DB

Cosmos DB protection: Manage your Microsoft Azure Cosmos DB protection alongside other Azure workloads with Veeam. Enhance your PostgreSQL database protection by adding an extra backup layer on top of Azure's native capabilities and safeguard your data against various types of outages and data loss by utilizing hot, cool, and archive repositories. All of this comes with optional immutability through Azure storage. Plus, benefit from flexible policy-based scheduling and experience seamless database recovery to the original or new location.

Other Features and Enhancements

In addition to the major new features listed above, V12.2 also includes a lot of enhancements that are in response to customer feedback and ongoing R&D findings. The most significant enhancements are listed below:

Direct to Archive

By popular request, SOBRs now support offloading aging backups directly from Performance Tier to Archive Tier. This can now be done without the need for offloaded backups to land on Capacity Tier first, which can be relatively expensive in comparison to archive-class object storage. Previously, Direct to Archive was only supported when Performance Tier was backed by Amazon S3 or Microsoft Azure Blob Storage-based extents. In 12.2, this configuration is supported for all on-premises backup repository types.

This new SOBR capability provides additional flexibility when configuring a SOBR for long-term backup archival in scenarios where the 3-2-1 Rule is achieved with a different process, like by copying backups to another datacenter or exporting them to tape. In these scenarios, you can now save significant cloud object storage costs by archiving backups directly to Archive Tier and skipping Capacity Tier altogether.

That said, Capacity Tier is still the recommended way to implement immediate copying of newly created backups to object storage for DR purposes. If you are currently leveraging Capacity Tier as your offsite backup copy strategy, do not remove it without first replacing your offsite backup copy process with a different one.

CDP I/O Filter Cross Compatibility

V12.2 brings multiple I/O filter protocol version support, which allows I/O filters to continue communicating with an upgraded backup server of later versions. This allows CDP policies to continue functioning in special compatibility mode after the product update, without requiring you to immediately place all ESXi hosts into maintenance mode to perform a I/O filter upgrade.

Placing ESXi hosts into maintenance mode for an I/O filter upgrade is unavoidable and unfortunately cannot be controlled by Veeam since the filter upgrade process is managed entirely by vCenter. That said, you can now postpone this upgrade until the next infrastructure maintenance window, like when a security patch or a periodic update needs to be deployed to your ESXi hosts.

When it comes to Veeam Backup & Replication 12.2 specifically, it can also support I/O filters of version 12.0 and 12.1. This allows organizations who use backup server versions 12 and 12.1 to upgrade to version 12.2 with no disruption, and lets them choose a convenient time to update CDP I/O filters later.

Veeam App for Splunk

With this new Splunk extension, customers can now monitor the health and security status of their Veeam backup infrastructure with Splunk's capabilities. This application enables Splunk customers to analyze Veeam events, monitor Veeam backup environments, and access to alerts, dashboards, and reports while integrating seamlessly with Splunk user roles and location management.

The application also processes events sent by Veeam Backup & Replication and provides Splunk users with built-in dashboards and reports to monitor job statuses and security events. It also provides built-in alerts with severity level management, role-based permissions for locations, application configuration backups, and more. Plus, with multiple Veeam Backup & Replication servers and multiple data source locations supported, this app is ready for the largest Veeam deployments out there!Veeam App for Splunk supports Splunk Enterprise 9.1.0 or Splunk Cloud Platform 9.1.2308 and later, and is available via Splunkbase. Please note that this application requires Veeam Data Platform Advanced or Premium edition licenses.

Security

Malware Detection

Improved Onion link detection: Based on user feedback, the Onion link detection logic has been improved to reduce false positives in some corner cases like browser cache and OS swap files. The inline malware detection engine now intelligently determines the type of file in which Onion links are found and excludes non-text-based files like cache or swap files from consideration, since they are unlikely to represent a usable ransomware note.

Malware detection index improvements: CPU consumption during the guest file system index analysis has been lowered significantly to reduce backup server load. Furthermore, you can now reduce your index retention period if your guest catalog storage is running out of space via the *IndexRetentionDays* (DWORD) registry value under the *HKLM\SOFTWARE\Veeam\Veeam Backup and Replication* key on the backup server and set your preferred retention duration in days.

Role-Based Access Control (RBAC)

Incident API operator role: This new user role is designed exclusively to interact with Veeam Incident API REST endpoints. It's ideal for automated systems or users who only need to create or manage incidents without broader access to the backup server and enhances overall security posture by adhering to the principle of least-privilege.

Security administrator role: This new role is tailored to security teams, which enables businesses to delegate certain sensitive tasks — such as managing saved credentials, backup encryption passwords, and four-eyes authorization requests — without the ability to manage other backup server settings, backups, and restores. By empowering designated personnel to perform these functions, you can ensure internal compliance with security best practices like zero trust.

Security and Compliance Analyzer

Additional security checks: In our ongoing effort to bolster security, we have expanded the analyser's checks to include LSASS and NetBIOS configurations on network backup server interfaces. These enhancements ensure your system adheres to best practices for protecting credentials in memory, securing against unauthorized access, and managing legacy network protocols.

Additional product configuration checks: We added a recommendation against using hardened repositories as backup proxy servers due to expanded attack surfaces with the addition of VMware VDDK and outgoing network connections that are established to protected ESXi hosts.

Auto-apply script: The script referenced in KB4525 has been upgraded to simplify the enforcement of security and compliance measures.

Security Events

Backup server name: We added the originating backup server's fully qualified domain name (FQDN) to both Windows Event Log and Syslog event parameters to facilitate event tracking in infrastructures that have multiple backup servers.

Image-level Backup

Backup Copy

Direct to object from hardened repositories: Backup copy jobs from hardened repositories will now also transfer data directly to object storage as opposed to looping through a gateway server. This helps eliminate potential bottlenecking.

Enhancements for agent-based backups: The backup copy task builder and resource locking manager has been redesigned to enable faster and more robust processing for agent-based backups. This dramatically increases the scalability of these backup copy jobs.

SureBackup

Continuous schedule: We added a new scheduling option to enable continuous operations for SureBackup jobs within specified time windows. In conjunction with the VM randomizer and parallelization limiter, this new capability enables interesting new use cases, such as continuously testing random VMs for recoverability or scanning their disks for threats and unwanted content with YARA rules at hours where the backup infrastructure is idle.

Enhanced NSX-T support: We've improved network mapping logic in a number of corner cases where NSX-T networks are involved.

Unstructured Data Backup

Reduced RAM consumption: File share and object storage backup jobs that process data sources with several billions of objects should now consume significantly less RAM on cache repositories and backup proxies.

Agents

Agent Management

Nosnap agent support: Pre-installed Linux backup agents deployed with the x86 Veeam-nosnap package are now fully supported by all agent management functionalities except application processing. This allows you to control backup settings on Linux systems that cannot use the Veeam snapshot module for whatever reason, and therefore need to rely on LVM snapshots.

Enhanced audit trail retention: Agent-based backup job session histories will now be preserved for backup agents that have been removed from your backup server configuration. These historical sessions will adhere to the global session retention settings specified in your backup server properties.

Veeam Agents *for AIX* and *for Solaris*

Flexible bare metal recovery (BMR): You can now restore your backup to a system with a different combination of disks compared to the original system, or only restore selected volumes.

IPv6 support: The new agent versions now support operations in IPv6-enabled and IPv6-only networks.

List backup content: You can now easily list all the files contained in a selected restore point using CLI without having to mount a backup first.

New compression algorithm: Agents will now use a modern and highly efficient compression algorithms that were first adopted in Veeam Backup & Replication v12 for high and extreme compression levels. This will improve data reduction ratios by up to 20%, lower CPU usage by up to 3x, and increase restore performance by up to 2x compared to the previously used algorithm.

Backup performance improvements: Parallel compression and other under-the-hood tweaks should make your AIX and Solaris backups run significantly faster.

Read-write backup mount: The new ability to publish AIX backup content directly from the backup repository enables several interesting use cases, such as performing database restores with native tools directly from the mounted backup.

ZFS encryption for BMR [Solaris only]: When restoring backups of an encrypted ZFS volume, we will automatically enable ZFS encryption on the restored volume as well.

Veeam Agent *for Mac*

Recovery token support: A simplified way to provide end users with access to a particular backup has made its way to our Mac agents as well. Backup administrators are now able to generate time-limited access keys or recovery tokens that can be shared with users. This allows them to connect to a Veeam repository and perform a restore without needing backup server credentials.

Library selection option: An additional predefined selection option is now available for inclusion or exclusion from backup processes under the "User Profiles Data" section. Library typically contains fonts and other items used by applications that are available to all users of your Mac.

Veeam Agent *for Microsoft Windows*

File restore target selection: Users can now leverage the new "Restore To" option during file-level recoveries to specify a different Windows machine than the restore target. This dramatically simplifies restore operations when the original machine is no longer available and can facilitate complex migration scenarios by providing the flexibility needed to easily extract all data from a backup to the desired destination.

ReFS support in cloud machines: File-level recovery is now supported from cloud-native agent backups of AWS EC2 instances and Microsoft Azure VMs with ReFS disks.

UI branding: In response to popular demand, we introduced the ability to customize your control panel logo image and tray icon. This feature allows you to align the user interface with your corporate aesthetics and reinforce your brand's identity. To perform customizations, create the *LogoIcon* (DWORD, 1) registry value under the *HKLM\SOFTWARE\Veeam\Veeam Endpoint Backup* key on each endpoint and place your custom *logo.png* and *logo.ico* files into the *%ProgramFiles%\Veeam Endpoint Backup\Resources* folder.

Application Plug-ins

General

Plug-in throttling: You can now reduce application plug-in CPU usage by instructing the agent to start with a lower process priority. This grants your production application preferential access to your compute resources, which reduces the impact on your production environment due to backup activities occurring during periods of high system load. Because the impact on backup performance may be noticeable, we recommend throttling only in highly loaded environments.

Oracle

Database authentication: The Oracle RMAN plug-in now supports database authentication in both standalone and managed modes. This capability is particularly beneficial in Oracle environments where OS authentication is disabled. In addition to enhanced authentication capabilities, this feature also improves Oracle RAC processing because the previous need to add the grid user to the *oradba* group is no longer necessary.

Application policy enhancements: You can now select your desired application policy authentication type, which lets you leverage the authentication method that best fits your environment by connecting to the Oracle instance with your specified database user. This further enhances security and control.

Improved configuration experience: The new flexible configuration wizard allows you to easily specify database user credentials at the per-database level, either by using the same set of common credentials for multiple databases or specifying unique credentials for each database.

RAC processing visibility: In response to user feedback, we expanded the application policy action log to display the specific node that's being used as a source during Oracle RAC processing, thus providing a better visibility into the backup process.

Backup Appliances

General

Imageless deployment: You can now deploy cloud backup appliances directly from the Veeam Backup & Replication server to reduce complexity and enhance infrastructure management efficiency. This method ensures a consistent environment, which significantly reduces the likelihood of configuration errors and improves deployment reliability.

AWS

Immutability architecture improvements: We have made some optimizations that will allow users to save up to 30% on immutability extension costs compared to the previous version. To further reduce costs, we will now use a default generation period of up to 25 days for immutability, instead of 10 days.

Microsoft Azure

Backup copy for virtual network configuration: Enhance your virtual network configuration protection by adding an extra layer of protection with backup copies to hot or cool repositories, with support for immutability to prevent data loss or corruption. Easily import backup copies to any Veeam Backup *for Microsoft Azure* appliance for hassle-free restores.

Worker placement flexibility: Simplify your resource management by selecting the tenant, subscription, and resource group for your worker deployments. For example, you can deploy workers in dedicated subscriptions for added isolation or within the same subscription as your protected resources for improved efficiency. This can help streamline resources and cost management for your backup and restore operations while ensuring adherence to internal security standards and regulations.

oVirt KVM

This section applies to Red Hat Virtualization (RHV) and Oracle Linux Virtualization Manager (OLVM) platforms.

Restore to the original location: When performing file-level recoveries, users now have the option to restore files directly to their original location, thus avoiding many extra clicks to specify your destination. When using this option, you can also choose whether to keep or replace existing files if they're still present at the original location.

Improved backup performance: Multiple under-the-hood worker enhancements have been made to improve backup performance and reduce compute resource consumption.

BitLooker enhancement: BitLooker performance has been improved by skipping the processing of small disk image chunks altogether to avoid backup slowdowns on highly fragmented disks.

Storage Integrations

Object Storage

V12.2 is a recommended upgrade to all object storage users due to the multiple under-the-hood improvements and optimizations. The new version should put significantly less stress on object storage by reducing the frequency of certain API calls by up to 10 times, which also reduces costs for cloud object storage providers that do charge for API calls. We've also reduced gateway server memory consumption and enhanced our code's reliability in several corner cases observed in customer support.

Background checkpoint removal: Checkpoint removal operations have been decoupled from the backup job and will now run as a system session after backup jobs and offload processes finish and there are no conflicting tasks. Checkpoint removal has the lowest priority for the task scheduler. In addition, this process is triggered daily at 3 a.m. to perform the same activity for backup no longer associated with any jobs. This change will remove additional load from object storage when it is already extremely busy accepting incoming backups and prevent backup jobs from appearing to "hang" at the end while processing checkpoint removal.

Intelligent extent selection: Unstructured data backups pointed to SOBRs will now consider running task count and the available free space during extent selection. This more intelligent allocation will improve load distribution across SOBR extents compared to just selecting them solely based on available free space.

Primary Storage

Immutable snapshots integration for HPE Storage Arrays: HPE 3PAR, Primera, Alletra, and Alletra MP storage users now have one additional immutability option in their toolbox. V12.2 brings an option to use HPE's native Virtual Lock functionality to make created storage snapshots immutable. This offers an extra layer of security against data tampering and ransomware attacks by creating read-only storage snapshots.

USAPI Plug-in for IBM FlashSystem: The built-in storage snapshot integration for IBM FlashSystem has been re-implemented into the dedicated USAPI plug-in, enabling IBM to continue managing it on their own and provide more timely updates that are not dependent on Veeam Backup & Replication release vehicles. The full set of features that our users rely on has been preserved in this transformation, as is the continuity of job and snapshot history.

Tape

Hardware compression: To ensure optimal usage by all backup job types, hardware compression is now enabled by default for all new tape jobs. This change should enhance data transfer efficiency and maximize storage capacity without offload performance degradation.

Source restore point monitoring: By popular demand, the "no new restore points" warning will now only be logged when the source job actually fails to create a new restore point. This change should eliminate unnecessary warnings when the source backup job simply did not run yet or has been intentionally disabled.

File backup to tape enhancements: In addition to significantly improving the performance of file backup to tape jobs, we've also refined the job retry logic and conflict handling in several corner case scenarios that were reported by our customers.

Backup Console

Elevated AI capabilities: The Veeam AI Assistant has been migrated to the new GPT-4o model. This upgrade should improve response times and quality, especially as it comes to REST code creation and analysis. With GPT-4o, navigating Veeam's features, troubleshooting issues with your custom Veeam PowerShell scripts, and exploring best practices becomes more enjoyable and intuitive than ever. Now all your questions are answered with significantly improved precision.

Redesigned dashboards: Managed servers, protection groups, and object storage dashboards have been redesigned to add the necessary groupings to accommodate the ever-increasing number of available options. This is due to the continuous expansion of supported platforms and storage devices.

Improved UI performance: We have reduced configuration database load and improved load time and responsiveness for the following UI views and dialogs: The Home > Backup view, the Home > Jobs view, the Backup Properties dialog, the Tape Media Details dialog, and the Entire Machine Recovery wizard.

Configuration backup and restore improvements: We enhanced our code's reliability in several corner cases that were observed in customer support, particularly surrounding large-scale deployments of file-to-tape backup jobs. These enhancements should facilitate seamless large-scale configuration database migrations from Microsoft SQL Server to PostgreSQL.

Enterprise Manager

One-click restore enhancements: Enterprise Manager web UI and its self-service backup and restore portals now support file-level recovery for backups that do not include system disks.

Upgrade performance: Enterprise Manager database upgrade performance has been improved by order of magnitude.

This document includes only features and enhancements that were first introduced in version 12.2. If you are looking for information on previous V12 releases, refer to the following documents:

What's New in 12.1 (released Dec. 5, 2023)

What's New in 12.0 (released Feb. 14, 2023)

About Veeam Software

Veeam, the #1 global market leader in data resilience, believes businesses should control all their data whenever and wherever they need it. Veeam provides data resilience through data backup, data recovery, data freedom, data security, and data intelligence. Based in Seattle, Veeam protects over 550,000 customers worldwide who trust Veeam to keep their businesses running. Learn more at www.veeam.com or follow Veeam on LinkedIn @veeam-software and X @veeam.