Veeam Backup & Replication

What's new in v11?

Veeam® Backup & Replication™ v11 delivers the single platform for comprehensive data management that is powerful and flexible enough to protect each phase of the data lifecycle, while handling all the complexities of a hybrid, multi-cloud environment. The following is a list of the major new features and enhancements added in V11.

Continuous Data Protection (CDP)

Eliminate downtime and minimize data loss for Tier-1 VMware vSphere workloads and perform immediate recoveries to a latest state or desired point in time with the built-in CDP functionality, achieving the most stringent RTO and RPO.

The unique benefits of the **Veeam CDP** implementation include:

- **No VM snapshots —** Veeam CDP captures all write I/O directly in the data path with the *VMware-certified I/O filter driver*, eliminating the need to create VM snapshots as with classic replication jobs. And with I/O level tracking, only the data actually changed is sent over to a DR site, as opposed to larger virtual disk blocks returned by changed block tracking.
- **No workload or hardware dependency —** Protect ANY OS and applications that can run within a vSphere VM. And unlike storage-based replication, Veeam CDP works across non-matching storage arrays, hyperconverged storage solutions and even local vSphere ESXi storage.
- **Asynchronous replication —** Unlike synchronous array-based replication, Veeam CDP can be used across any distance while requiring significantly lower bandwidth, thanks to I/O consolidation when the same block is overwritten multiple times and network traffic compression.
- **Policy-based protection —** Unlike with regular replication jobs, you don't have to worry about scheduling at all. Just define the required RPO (maximum data loss allowed in case of a disaster) and the CDP policy will take care of performing the sync cycles as needed. Also, to reduce monitoring events spam, you can define acceptable RPO violation thresholds so that sporadic connectivity issues do not result in alarms.
- **Flexible retention —** Separately define *short-term retention*, allowing crash-consistent restores to a point in time with RPO period granularity and *long-term retention* policy with optional periodic application-consistent restore points, providing an additional layer of protection.

NEW Veeam® Backup & Replication™ v11 eliminates data loss and ransomware while saving 20X on your long-term archive retention costs. The 4-in-1 solution combining backup, replication, Storage Snapshots and the NEW Continuous Data Protection (CDP) under a single platform delivers faster and more flexible data protection, recovery and retention options. Version 11 unlocks unprecedented resiliency for any size business, offering over 200 new features and enhancements, including the ability to:

- Eliminate data loss with **Veeam CDP**
- Eliminate ransomware with immutable backups on a **Hardened Linux Repository**
- Eliminate downtime with **Instant Recovery for NAS, Microsoft SQL and Oracle**
- Achieve over 20X lower cost, long-term **archive-to-cloud storage on Amazon S3 Glacier & Azure Blob Archive**
- Unify **cloud-native workload protection with AWS and Azure**
- Conquer complexities in your way with **Veeam-powered BaaS & DRaaS**

Compliment **Veeam Backup & Replication v11** with insights, reporting and deep visibility provided by **Veeam ONE™ v11** in one enterprise bundle, **Veeam Availability Suite™ v11**, to meet both your protection and analytics needs.

Add site recovery automation and testing, creating a powerful combination that delivers business continuity with orchestration at any scale with **Veeam Disaster Recovery Orchestrator v4**.

Supported environments

For a detailed list of supported environments, reference the product Release Notes.

- **Flexible deployment models —** Depending on the amount of data under protection, you can opt for virtual CDP proxies or use *dedicated physical CDP proxies* to completely offload all data processing overhead from your vSphere hosts, removing impact to your VM consolidation ratio. In either case, only one proxy per vSphere cluster is required with additional proxies providing redundancy and increased scalability. Note: CDP proxy is the new role that can share a server with other Veeam components.
- **Deployment assistant —** A built-in deployment calculator removes the guesswork by looking at the historical I/O of all VMs selected for protection in the CDP policy to estimate the required bandwidth needed to achieve the specified RPO and evaluates whether your currently available CDP proxy resources are sufficient for the historical change rate.
- **No extra costs —** Veeam CDP is included in your universal license along with existing data protection methods for vSphere VMs: host-based backup or replication, agent-based backup, application-level backup and storage snapshots. And just as before, *using multiple protection methods on the same VM does not consume additional licenses*! No more picking and choosing which VMs to assign an expensive third-party CDP license to — from now on, your creativity with DR strategy planning will only be limited to the available bandwidth!

NOTE: Veeam CDP functionality requires deploying the I/O filter to both the source and target vSphere cluster. This can be done by right-clicking the cluster in the newly added clusters tree view on the Backup Infrastructure tab.

Veeam CDP is included in the **Veeam Universal License**. When using a legacy Socket-based license, **Enterprise *Plus*** edition is required.

Hardened Repository

Keep your backups safe in hardened, malware- and hacker-proof repositories with immutable backups, preventing encryption and deletion by ransomware and malicious actors. This is achieved through the following enhancements for Linux-based backup repositories:

- **Single-use credentials —** Required for the Hardened Repository, the single-use credentials are supplied by the user interactively at the initial deployment time and when installing product updates, but are never stored in the configuration database. This eliminates any possibility for hackers to extract these credentials from a compromised backup server and use them to connect to the repository.
- **No SSH protocol dependency —** All former SSH protocol usage has been encapsulated into the expanded transport protocol. As a result, SSH connectivity is required only at the initial deployment time and when installing product updates. This allows customers to secure SSH with interactive multi-factor authentication (MFA) or even disable the SSH Server completely to protect your repository, even from future zero-day vulnerabilities.
- **Immutable backups —** Wave accidental backup deletions, ransomware and hackers goodbye! You can now make your image-level backups immutable for the specified period of time with GFS backups protected for the entire duration of their retention policy. This functionality uses the native Linux file immutability feature, which restricts modification and deletion of files with the corresponding flag set. The flag can only be removed by a user with root privileges, but the single-use credentials ensure root credentials are not stored on the backup server. So, just ensure they are not saved into any other application and keep the sudoers list empty too!

  For redundancy, the immutability expiration timestamp is stored twice: 1) in the special configuration file and 2) in the extended attribute of each backup file. The first is extended automatically as dependent incremental restore points are added into the backup chain and can also be increased (but never reduced) manually for legal-hold purposes using PowerShell. The second timestamp remains as originally set, due to being a part of the already immutable file. The immutability flag is only removed from the backup file when the local time on the repository server exceeds *both* values.

V11 successfully passed a third-party assessment of compliance with the U.S. financial industry regulations for WORM (Write Once Read Many) storage. A compliant Hardened Repository configuration ensures protection of backup data against manipulation and meets the requirements for non-rewritable, non-erasable storage as specified by SEC 17a-4(f), FINRA 4511(c) and CFTC 1.31(c)-(d) regulations. The compliance assessment was done by Cohasset Associates.

NOTE: Since we're unable to support any backup modes that involve in-place backup file modifications on immutable repositories, this limits your choice to the classic forward incremental backup with periodic full backups. This makes XFS the ideal file system for such repositories, thanks to the spaceless synthetic full technology delivered by our advanced XFS integration (a V10 feature).

Expanded Object Storage Support

Reduce the costs of long-term data archival and retention by up to 20 times, replace manual tape management and achieve end-to-end backup lifecycle management with expanded support for hot object storage in Capacity Tier and support for cold object storage in NEW Archive Tier of Scale-Out Backup Repository™ (SOBR).

For Capacity Tier and NAS file version archiving, in addition to the wide variety of existing choices, you can now use **Google Cloud Storage (GCS)** as the object storage repository. The native integration is built using the proprietary GCS object storage API, but does not support immutable backups at this time, due to the lack of object lock capability in GCS.

For Archive Tier, we're delivering **Amazon S3 Glacier** (including Deep Archive) and **Microsoft Azure Blob Storage Archive Tier** support with the new SOBR Archive Tier. Unlike hot cloud object storage, these coldest tiers have their economics tuned for the "Write Once Read Never" use case and are thus best suited for long-term archival of GFS backups. Their significantly higher API and retrieval costs, as well as retrieval times measured in hours, drove the creation of the dedicated Archive Tier to ensure a cost-effective, yet seamless, backup lifecycle management.

The following are the key features of Archive Tier:

- **Immutable backups —** To help meet compliance requirements, in Amazon S3 Glacier, the archived backups can be optionally made immutable for the entire duration of their retention policy.
- **Policy-based offload —** Just like with Capacity Tier, there are no offload jobs to manage! Just set your archive window high enough to ensure only the restore points you are not likely to access again (outside of special circumstances) are archived — and being smart, software-defined storage, SOBR will take care of data movement across all tiers on its own. Just keep an eye on its daily SOBR status report to make sure it's all green!
- **Cost-optimized archiving —** Due to the high API costs of cold object storage tiers, offloaded data blocks are repackaged into large objects (up to 512MB in size) using helper appliances automatically provisioned in the public cloud for the duration of the archiving session. In addition, to avoid the early deletion penalty, we automatically skip archiving of restore points with the remaining retention time under the minimum required data storage duration of the used storage class.
- **Flexible storage methods —** To lower your costs, by default the Archive Tier offload uses a forever-incremental approach with only a delta from the previous restore point uploaded and stored for each archived restore point. However, for extremely long retention policies, we also provide an option to store each GFS full backup as standalone. This allows you to avoid the single incremental backup chain spanning decades, while still keeping your overall costs reasonable through leveraging storage classes like Amazon S3 Glacier Deep Archive.

- **Self-sufficient archives —** Archived backups are self-sufficient and not dependent on any external metadata, allowing them to be imported even if the on-premises backup server is lost. Furthermore, there's no "vendor lock-in" because archived backups can be imported from object storage and restored at any future point in time using a Veeam Backup & Replication *Community Edition* install, which does not require a valid license. In other words, we don't hold your data hostage!
- **No extra costs —** Unlike secondary storage appliance vendors who obviously hate to see the data leaving their expensive on-premises hardware, Veeam does not charge a per-TB subscription for archiving data to object storage. In other words, we have no cloud usage tax!

SOBR Archive Tier is included in the **Veeam Universal License**. When using a legacy Socket-based license, **Enterprise *Plus*** edition is required.

Expanded Instant Recovery

Make even more of the data center's workloads available instantly with the seamless restore of the following new workloads from the pioneer of Instant VM Recovery®:

- **Instant Recovery of Microsoft SQL Server and Oracle databases —** Database won't start? Developers accidentally dropped a critical table? No problem! Recover any database from backup to the latest state or to an earlier point in time to any production database server or cluster (physical or virtual) in minutes, regardless of its size.

  Selected databases are made available to production applications and database clients instantly and can be modified normally with all changes preserved in cache — while the backup itself is, of course, never changed. In the background, Veeam automatically restores database files to the production storage and then keeps syncing the actual (modified) database state to the production storage.

  To finalize the recovery, you will need to switch the database over to running from the production storage, which can be done with minimal downtime, equivalent to simply restarting the database. This switchover can be done manually or scheduled to happen automatically — either as soon as the synchronization catches up or during your next maintenance window.

  Unlike the interactive Publish functionality, database instant recovery uses a service-based architecture and does not depend on the Veeam Explorer™ user interface running. And should any backup infrastructure component reboot during the instant recovery, the Instant Recovery conveyor will automatically recover itself when all required servers come back online (in case of extended outages longer than one hour, you can resume the instant recovery manually using the Veeam Explorer UI).

  Instant database recovery is included in the **Veeam Universal License**. When using a legacy Socket-based license, **Enterprise** or higher edition is required.

- **Instant Publish of NAS backups —** Lost your NAS or file server? Deleted an entire file share accidentally? No problem! Just publish SMB file shares from backup to the latest state or to an earlier point in time on the selected mount server, enabling your users to instantly access their data in this temporary SMB file share while you're getting the problem fixed or data restored.

  Other use cases discovered by our V11 beta testers involve enabling third-party applications and scripts to instantly access the content of any NAS backup for data mining and other **data reuse** scenarios — to avoid locked files and impact on your production environment, thanks to offloading this activity to backup storage hardware that usually remains idle during production hours. Prototypes were created by community members specializing in the following fields: Machine Learning (ML), searching for Personally Identifiable Information (PII) to aid in compliance processes, and GDPR and Malware detection (automated security analysis of files for sleeping malware with additional antivirus applications).

- **Instant Recovery of ANYTHING to Microsoft Hyper-V —** V11 enables additional data recovery and portability use cases by letting you instantly recover ANY physical server, workstation, virtual machine and cloud instance backups to a Microsoft Hyper-V VM, regardless of what Veeam product was used to create the backup. No learning curve is required, as the recovery just works, thanks to the built-in P2V/V2V conversion logic — enabling restores and migrations with new levels of speed and flexibility and making hybrid-cloud DR a reality.

  And because Veeam backup server runs on Microsoft Windows, the Hyper-V host is effectively built in directly into every backup server and readily available for everyone to use! We even support Windows 10 Hyper-V as the target for this functionality, which, in particular, enables managed service providers (MSP) to build ultra-low-cost Veeam-powered all-in-one DR appliances based on Windows 10 to deploy at their client sites.

Other enhancements

In addition to the above-mentioned major new features, V11 includes over 200 other enhancements, which are a response to customer feedback and ongoing R&D learnings, the most significant of which are listed below:

General

Backup Engine

V11 more than doubles backup performance for all-in-one Veeam deployments on general-purpose server hardware, enabling customers to exceed 11GB/s backup speed per node — so long as primary arrays and storage fabric can keep up! This huge leap in performance is achieved through the multiple improvements aimed at enterprise-class server and storage hardware:

- **System cache bypass —** With V11, target data movers will bypass OS cache to ensure it does not interfere with controller-side caching and advanced I/O optimizations of enterprise-grade RAID controllers, both reducing the backup repository CPU usage and increasing performance by up to 50%.
- **Aligned writes —** Unaligned writes impact both storage CPU usage and performance, so V11 will avoid them by aligning each backup file data blocks to a 4KB boundary. This feature is enabled by default for newly created repositories and can be mass enabled on the existing repositories with the Set-VBRBackupRepository cmdlet. Active full backup is not required for the new setting to take effect.
- **Improved shared memory transport —** At a data processing speed approaching 100Gbps, even modern RAM speed starts to make a difference to overall data processing performance. V11 optimizes RAM interactions, significantly improving the speed with which data is passed from source to target data movers when they are running on the same server.
- **NUMA awareness —** To avoid internal bus congestion from cross NUMA node traffic, in multi-CPU servers, dependent processes should ideally be placed within the same node. V11 implements full NUMA awareness and ensures source and target data movers never end up in different nodes.
- **Optimal compression improvements —** We updated our default compression algorithm implementation, delivering a slightly better compression ratio and significantly faster decompression performance. For example, the execution of a SQL query returning 30GB of data against Stack Overflow database running in an instantly recovered VM now takes 28% less time compared to V10.
- **Resource scheduler improvements —** We made many optimizations to our backup infrastructure resource scheduler, reducing the time it takes to issue the resource up to 50%, which significantly accelerates job startup time. The improvement should be especially significant in the environments with a large number of backup proxies and SOBR extents.

Restore Engine

After receiving great feedback from applying our advanced data fetcher technology to the virtual tape full export functionality on Windows-based backup repositories in V10, we've expanded this engine to Linux-based repositories. In addition, now we are using it for ALL features and functionality that read backup files content from Veeam repositories. The biggest improvements should be observed on enterprise-grade storage hardware and for functionality that involves bulk data movement, such as full image restores, backup copies, object storage offloads, etc.

PowerShell

- **PowerShell module —** By popular demand, we switched from the PowerShell snap-in to the PowerShell module, which can be used on any machine with the backup console installed. We also no longer require PowerShell 2.0 installed on the backup server, which is something many customers had problems with.
- **New PowerShell cmdlet —** V11 adds 184 new cmdlets for both newly added functionality and expanded coverage of the existing features with a particular focus on restore functionality.

RESTful API

- **RESTful API for backup server —** Our current Veeam Backup Enterprise Manager RESTful API has a concept of exposing functionality available in the EM web-UI only, so we're now also adding RESTful API to the backup server itself, where we will focus on the most typical backup server management needs. V11 provides the new REST API to address the most popular use cases from our customers and partners: backup jobs and backup infrastructure management and bulk import/export for simplified deployment and migrations of backup infrastructure and jobs. To helps us prioritize, please leave feedback on our R&D Forums on what you would like to see covered next!

  RESTful API is included in the **Veeam Universal License**. When using a legacy Socket-based license, **Enterprise *Plus*** edition is required.

Security

- **FIPS compliance —** V11 uses FIPS-compliant encryption modules also in the base product build. By default, FIPS-compliant operations mode is disabled to allow processing of legacy platform versions where FIPS-compliant interaction is not possible (such as VMware vSphere versions prior to 6.5, due to their dependency on non-FIPS compliant VDDK versions), as well as to avoid the performance impact from real-time module integrity checks required by the FIPS certification. You can enable the FIPS-compliant operations mode on the Security tab of the Global Options.

Backup

Application-aware processing

- **Persistent guest agent —** You can now optionally use the persistent guest agent for Windows-based VMs by deploying one through Group Policy or your standard software distribution tool. This approach reduces network ports usage down to just a few static ports (depending on functionality used) and eases the account privileges requirements associated with overcoming UAC to deploy a run-time process into the guest, while also reducing network traffic and guest processing time. Only a tiny installer component needs to be distributed to guests; the rest of the components will be deployed (and kept up to date) automatically.
- **SQL Server integration —** Application-aware processing engine will now use the native MSOLEDBSQL provider if it is available on the SQL Server, enabling the processing of SQL Servers with forced TLS 1.2 without requiring registry edits. In addition, database backup preferences for HA groups will now be honored.

- **Improved visibility on SQL database protection —** The new experimental option for SQL Server allows you to fail the image-level backup session if transaction log backup cannot be initialized or if no SQL databases are found. Use the *AAIPSQLShowExperimentalOptions* (DWORD, 1) registry value on the backup server to make the corresponding checkbox visible in the application-aware processing settings. Please leave feedback on this new option on the R&D Forums!

Backup jobs

- **High priority jobs —** You can now designate some backup jobs as high priority. Such jobs will place their pending tasks into the dedicated resources scheduler queue that is offered for backup infrastructure resources before the queue used by normal priority jobs. Use this setting for backup jobs protecting workloads sensitive to their backup start time or for periodic jobs with strict RPO requirements.
- **Background GFS retention —** GFS full backup retention is now processed independently from the backup job execution as a background system activity on the Veeam repository. This ensures that the expired full backups won't continue to consume repository disk space if the backup job gets disabled for extended time periods.
- **Orphaned GFS backups retention —** The retention policy is now applied to GFS backups that no longer have a job associated with them, based on their last-known retention policy. This removes the need for workarounds, such as keeping the no-longer-necessary jobs protecting a single dummy machine.
- **Deleted VM retention improvements —** Deleted VM retention will no longer be applied if the backup job failed to build the processed machines list to avoid backup deletions caused by temporary infrastructure issues.

Backup Copy jobs

Backup Copy jobs now use the same GFS retention logic as the primary backup jobs. This ensures consistency throughout the product and enables compatibility with new features, such as immutable backups of the Hardened Repository or background GFS backup retention. Specifically, this means the following changes:

- **Time-based GFS retention —** GFS retention for Backup Copy is now time-based, as opposed to the number of restore points in each generation. This guarantees that the GFS restore points will not be kept for less time than necessary, even in the case of accidental manual GFS backup creation.
- **GFS full creation time —** GFS fulls are now created and sealed right on the scheduled day, as opposed to when the corresponding restore point becomes the oldest in the incremental backup chain. This should remove the continuous confusion and concerns of our customers in regards to this process.
- **No quarterly backups —** For consistency with the primary backup jobs GFS, a quarterly backup option is no longer provided. Existing quarterly schedules will be converted to monthly by increasing their retention value accordingly during the upgrade to V11. Existing Backup Copy jobs with GFS retention enabled will be updated automatically during the upgrade.

Other Backup Copy job improvements include:

- **Repository as source —** You can now select the entire repository as a source for the Backup Copy Jobs in immediate copy mode.
- **Daily retention —** Choose between restore point-based and new time-based retention in days for recent backups created by Backup Copy job.

Replication jobs

- **NFS repository support —** You can now specify an NFS-based backup repository in the replication job wizard for hosting replica metadata.

Quick Migration jobs

- **SmartSwitch threshold —** Our internal testing showed that Quick Migration in the SmartSwitch mode takes too much time for VMs with lots of RAM — to the point where it no longer makes sense. The root cause is the time it takes to transfer the memory state over NFC protocol. As a result, starting from V11, we will force cold migration (via power off) for machines with more than 8GB RAM. You can use the *QMSmartSwitchRAMThresholdGB* (DWORD) registry value on the backup server to override the threshold.

Restore

Data Integration API

- **Linux target support —** The Data Integration API (DIAPI) has been expanded to support mounting backup content directly to the Linux server.
- **Expanded platform support —** V11 enables image-based backups of all platforms supported by Veeam to be published through the DIAPI. This includes cloud-native backups for AWS, Microsoft Azure and Google Cloud Platform, as well as Nutanix AHV and VMware Cloud Director backups.

File Level Recovery (FLR)

- **Linux FLR without helper appliance —** FLR from Linux file systems can now be performed by mounting backup to ANY Linux machine: dedicated, target or the original one (which is always guaranteed to understand the file system you're trying to restore from). This approach removes the requirement for a vSphere or Hyper-V host to run FLR helper appliance on, while eliminating networking complexities and security concerns around the appliance. It also allows customers to perform FLR directly within cloud-based VMware infrastructure offerings.

  NOTE: Helper appliance still remains available as an option, for example, from archived backups with file systems you're no longer using in the production environment.

- **Linux FLR performance improvements —** Performance of FLR from non-Windows file systems has been increased up to 50% whether you're doing recovery with or without the helper appliance.

Veeam Explorer *for Microsoft Active Directory*

- **DFS configuration restore —** You can now perform restores of the Distributed File System (DFS) configuration in the System Container.

Veeam Explorer *for Microsoft Teams*

- **Microsoft Teams item restore —** Restore Microsoft Teams items directly from the image-level backup of the Veeam Backup for Microsoft Office 365 backup server.

Backup infrastructure

Backup Repository

- **Improved synthetic full performance on ReFS —** Synthetic fulls should now complete up to 2X faster on ReFS, thanks to reduced usage of the relatively long-running Windows API call required for the new synthetic full backup file creation.

- **Disable ReFS integrity streams —** You can now disable ReFS integrity streams for Veeam backup files using the *DisableRefsIntegrityStreams* (DWORD, 1) registry value on the backup server. While we do not recommend disabling integrity streams because data integrity is paramount in data protection, some customers insisted on having the ability to control this setting to improve performance.

Scale-out Backup Repository

- **VeeamZIP™ and exported backups tiering —** Full backups created with VeeamZIP and Export Backup, as well as orphaned backups, are now processed by the Capacity Tier and the Archive Tier policies just like regular backups and can be copied or offloaded to object storage normally. Imported backups will not be tiered just as before.
- **Fast cloning awareness —** SOBR extent scheduler will now take into account that the newly created synthetic full backup file is to be fast cloned and will not require that the home (preferred) extent has enough free disk space to host non-fast-cloned synthetic full backup files. In the previous versions, this may cause SOBR to "explode" when certain extents get close to its capacity because the scheduler starts assigning all synthetic full backups to non-home extents.
- **Offload operations in Windows event log —** The Capacity Tier and Archive Tier copy and offload operations will now create the corresponding events in the system event log for better visibility of these processes for users performing event log-based monitoring.

Object storage repository

- **Task limit —** Added the ability to limit concurrent tasks for better compatibility with on-premises object storage, which can more easily get overwhelmed by large numbers of concurrent API requests. You should not need to use this limit for most public cloud object storage since it is infinitely scalable. However, one use case where this limit may be useful is when you specify a gateway server in the object storage repository settings to proxy access to the internet since depending on the amount of CPU and RAM, this server may run out of compute resources when processing too many concurrent tasks.
- **Restore performance —** Restore performance from on-premises object storage backed by slow hardware has been improved a few times.
- **ListAllMyBuckets permission no longer required —** S3 and Google object storage buckets can now be specified manually in the Object Storage Repository wizard without having to browse for it. This enables service providers to create individual buckets for their clients and delegate permissions with an IAM policy without exposing a list of all of their clients (in the bucket names) to other clients.
- **Decompress blocks before storing —** You can now have backup data blocks decompressed before they are written to object storage. This enables on-premises object storage devices featuring built-in deduplication to process Veeam backup data more efficiently. To enable this behavior, create the *ObjectStorageDisableCompression* (DWORD, 1) registry value on the backup server.

Veeam Cloud Connect

- **Cloud Connect Backup MSP mode —** When the "Allow this Veeam Backup & Replication installation to be managed by the service provider" checkbox is selected in the Service Provider wizard on the tenant-side backup server, backup metadata, like machine names, will not be obscured in the service provider-side backup server, allowing MSPs to deliver managed backup services more efficiently.

- **Microsoft Active Directory-based tenants —** To simplify remote workstations and laptop protection with standalone Veeam Agent *for Microsoft Windows* in an enterprise environment, Veeam Cloud Connect now includes support for tenant quotas based on Active Directory (AD) accounts. This allows end users to leverage their existing AD account to connect a cloud repository with the Cloud Connect infrastructure authenticating the tenant through the AD. Ongoing authentication during backups uses a secondary password to prevent missed backups caused by password changes. However, bare-metal recovery from a cloud repository always requires that the account be successfully authenticated with AD using the current password before allowing access to backups. Also, if the AD account is locked out, neither backup nor restore operations will be possible.
- **Tenant evacuation —** Tenants can now be evacuated from the Scale-out Backup Repository extents using the Start-VBRCloudTenantBackupEvacuation cmdlet.
- **WAN accelerator throttling —** The "Limit incoming traffic from this tenant" setting now applies also to tenants doing data transfers through built-in WAN accelerators. Previously, it was working for the direct data transfer mode only.
- **Cloud Connect server RAM consumption —** We significantly reduced RAM consumption on the Cloud Connect server during the incoming replication job activity.

  Access to Veeam Cloud Connect *for Service Providers* requires a **Rental license**. For access to Veeam Cloud Connect *for the Enterprise*, please contact your Veeam sales representative.

Platforms

Google Cloud Platform (GCP)

- **Veeam Backup *for Google Cloud Platform* integration —** Register Google Cloud Storage (GCS) buckets with backups created by Veeam Backup *for Google Cloud Platform* as external repositories, enabling you to perform all types of restores and copy your GCP VM backups to on-premises backup repositories, or to tape, for disaster recovery purposes and for compliance with the 3-2-1 Rule.

Linux

- **Persistent data mover for Linux —** Transport components are now deployed persistently when you register a Linux server with Veeam. This improves both performance and scalability, as data movers no longer require being pushed to the server each time a task starts. Required rules for built-in Linux firewalls are created automatically for the duration of the backup job (iptables, ufw and firewalld are supported).

  NOTE: For Linux hosts not yet supporting the persistent data mover, such as storage appliances with the Veeam data mover integration, V11 will continue using the run-time data mover.
- **Enhanced data mover security —** When leveraging single-use credentials, the persistent data mover will run as the limited user from the credentials set it was deployed with. As a result, any potential vulnerabilities in the internal data mover API cannot be used by hackers to overtake the operating system.
- **Certificate-based authentication —** As opposed to using the saved Linux credentials, we will now leverage Public Key Infrastructure (PKI) technology for authentication between a backup server and transport components during backup tasks processing with the key pairs automatically generated at the transport deployment time.
- **Elliptic curve cryptography —** To achieve an unprecedented level of security, V11 adds support for elliptic curve (EC)-based SSH key pairs, such as Ed25519 or ECDSA, for establishing SSH connections to Linux servers. If cracking a 228-bit RSA key requires less energy than boiling a teaspoon of water, a 228-bit EC key takes enough energy to boil all water on planet Earth — providing security equivalent to a 2380-bit RSA key!

Microsoft Azure

- **Fully integrated Azure-native backup —** Cloud-native Azure data protection is now built directly into the Veeam Backup & Replication console. This requires Veeam Backup *for Microsoft Azure* v2.
- **Azure Stack HCI support —** Added support for the new hyperconverged infrastructure (HCI) operating system from Microsoft, which is, in essence, an on-premises Hyper-V infrastructure delivered as an Azure service.
- **Restore to generation 2 VM —** Added experimental support for Direct Restore *to Microsoft Azure* to provision a generation 2 VM as the target. To enable this functionality, create the *AzureEnableGeneration2VMRestore* (DWORD, 1) registry value on the backup server.

Nutanix AHV

- **Veeam Backup *for Nutanix AHV* 2.1 —** New functionality includes disk exclusion in backup jobs, better integration with Nutanix Volume Groups for restore, UI enhancements and more. For the complete list of new features, please refer to the corresponding Release Notes document.

VMware vSphere

- **Instant first class disk recovery —** When performing instant disk recovery, users can now choose to restore a disk from backups as a standard VMDK attached to the specified vSphere VM or as a first-class disk (FCD), which can be managed independently of vSphere VMs and consumed directly by next-gen container-based applications.
- **AND for vSphere tags —** In addition to specifying multiple individual vSphere tags as a job scope, you can now use a combination of vSphere tags — in which case, only VMs with every selected tag assigned will be processed (classic AND operator behavior). When using this approach, take greater care monitoring unprotected VMs, for example, with Veeam ONE™ — as such setup makes it much easier to unintentionally lose VMs from the protection scope and end up with no recent backups for them.
- **Two-step failback —** To make the failback time more predictable for large VMs and reduce downtime, we've made the failback process more controlled. In the first stage of the process, which takes most of the time, the replica VM is still running while digests are calculated and the failback target machine is being restored to the pre-failback snapshot state. Once this process completes, the replica VM is placed into the Ready to Switch status and can be failed back with minimal downtime required for the final delta transfer. The switchover operation can be performed manually or automatically — either as soon as the replica is ready for switchover or at the scheduled time during the next maintenance window.
- **Linux proxy transport modes —** Supported transport modes now include Direct Storage Access (for block and NFS storage), Network (NBD/NBDSSL) and Backup from Storage Snapshots (for block storage only). In addition, the existing hot-add transport mode performance has been improved significantly with the advanced data fetcher technology, previously leveraged by Windows-based proxies only.
- **Linux proxy CBT restore —** Added support for Quick Rollback functionality to Linux-based backup proxies for full VM restore and failback to the original location.
- **NBD multi-threading —** The backup engine is now capable of establishing multiple NBD connections per VMDK for better performance of network transport mode. At the same time, due to the low limit of max NBD connections per ESXi host, there are reliability concerns associated with increasing the number of such connections. While our resource scheduler tracks NBD tasks per host to ensure they remain within the limit, we decided that a marginal performance benefit is not worth the risk of enabling this new behavior for our entire customer base right away, as there might be external NBD connections too. However, you can use the fully supported *VMwareNBDConnectionsPerDisk* (DWORD) registry value on the backup server to give this functionality a try. Our internal testing showed that the best performance is achieved with two NBD connections per disk. Please share your results in the Veeam R&D Forums to help us decide whether to enable this functionality by default in future updates!

- **VMware Remote Console support —** The user interface functionality that enables opening a VM console now leverages the more secure VMware Remote Console. You will be offered the opportunity to download and install the console upon the first attempt to use any related functionality.
- **VDDK version update —** VDDK 6.7 has been updated to version 6.7.3, which, among other issues, should fix issues with asynchronous NBD I/O usage.

VMware Cloud Director

- **Cloud Director replication —** New dedicated replication job type enables service providers to perform vApp replication within and across Cloud Director (VCD) instances. The replication job processes vApp VMs and metadata (such as networking or VM start order) to create a ready-to-use replica vApp in the target Cloud Director that can be leveraged instantly in case of a disaster.
- **Native Cloud Director plug-in —** This new capability allows service providers to extend the Cloud Director tenant UI to include Veeam Backup & Replication functionality, enabling tenants to manage their own backups and restores without leaving the convenience of the Cloud Director web console. This integration is based on Veeam's existing Cloud Director self-service backup portal.
- **Multiple Cloud Director servers support —** Cloud Director self-service backup portal now supports environments with multiple VCD servers registered with Veeam Backup & Replication, and you can pick the desired VCD server when creating your organization configuration.
- **Multiple configuration support —** Cloud Director self-service backup portal now supports the creation of multiple self-service configurations for the same VCD organization.
- **Enhanced Cloud Director portal access flexibility —** You can now specify custom VCD roles in the *vCloudPortalBackupAdminRole* (STRING) and *vCloudPortalRestoreOperatorRole* (STRING) registry values on the backup server to allow all VCD users with the corresponding VCD role to access the self-service backup portal for their respective organization with either the Backup Administrator or Restore Operator role on the portal. Without these registry values populated, behavior remains as it was in the previous versions: only the VCD users with administrative permissions on the VCD organization are allowed to access the self-service backup portal for the corresponding organization with the Backup Administrator portal role.
- **Cloud Director 10.2 support —** Full support for both on-premises installations and cloud-based deployments with VMware Cloud Director service.

Primary storage integrations

General

- **Instant disk recovery from storage snapshots —** Reduce your instant recovery footprint by restoring only the required disks of large vSphere VMs (for example, only OS disk or only data disks) directly from storage-based snapshots. Instantly mount disks from a snapshot to the selected VM for other use cases, for example, comparing the disk content or performing mass file-level recoveries using third-party tools.
- **Restore point-based retention for storage snapshots —** Retention of restore points in storage snapshots is now processed on a per-VM basis. Previously, storage snapshots themselves were considered to be restore points, which resulted in a number of issues in corner cases, like failed retries, VM migration to another volume, etc.

Dell EMC VNX/VNXe/Unity/Unity XT

- **Integration tool version —** Updated the Dell EMC Navisphere and Unisphere CLI tools to the latest version for TLS 1.2 support.

HPE 3PAR/Primera

- **3PAR Remote Copy support —** Asynchronous periodic 3PAR/Primera replication is now supported in all storage snapshot integration functionality. This includes managing storage snapshot replication, separate retention for snapshot replicas and backup from snapshot replicas on the secondary array to avoid impact from backup activities on the primary array.
- **Nimble multi-protocol support —** Storage snapshot integration functionality now supports Nimble storage having both FC and iSCSI protocols enabled on the same array.
- **Versions support —** Added support for 3PAR OS 3.3.1 MU5 and dropped support for 3PAR OS versions below 3.2.2 and WSAPI prior to version 1.5.

Lenovo

- **Lenovo DM support —** Added built-in Lenovo ThinkSystem DM Series storage snapshot integration.

NetApp

- **ONTAP 9.8 support —** Added NetApp ONTAP 9.8 support for storage snapshot integration except for processing of VMs residing on FlexGroup volumes. Note: You can still use regular host-based or agent-based backup for protecting such VMs.

Secondary storage integrations

ExaGrid

- **AD authentication support —** Added support for Microsoft Active Directory-based authentication for registering ExaGrid with Veeam.
- **SOBR placement logic —** Per ExaGrid request, in light of the global deduplication they provide, we disabled the special SOBR extent scheduling logic designed for deduplicating storage and making SOBR prefer placing new full backup on the same extent with the previous full backup. You can revert to the previous placement logic by creating *ExaGridEnableNewFullToSameExtent* (DWORD, 1) registry value under the HKLM\SOFTWARE\Veeam\Veeam Backup and Replication key on the backup server.
- **UI defaults —** We now recommend setting compression level to Optimal in the backup job wizard when ExaGrid is specified as the target repository and we enabled the "Decompress backup data blocks before storing" option in the backup repository wizard by default when registering an ExaGrid-based repository. This new default will allow ExaGrid to perform deduplication effectively, regardless of the protected workload.

Dell EMC Data Domain

- **Data Domain OS support —** Added support for DD OS versions 7.1, 7.2 and 7.3, while dropping support for all DD OS versions lower than 6.1. Please upgrade your DD OS version prior to upgrading to V11.
- **Data Domain Boost SDK version —** DD Boost SDK has been updated to version 7.0.

HPE StoreOnce

- **Backup Copy jobs as source —** Backup Copy jobs can now also be used as the source for Catalyst Copy jobs. Previously, only primary backup jobs were supported as the source.
- **Tape out for Catalyst Copy backups —** Backup to Tape jobs now support Catalyst Copy jobs as the source.
- **Health check performance —** Backup health check performance in Catalyst Copy jobs has been increased a few times through parallel processing.
- **Delayed backup copy deletion UI —** Catalyst Copy jobs enable delayed deletion of backup copies from the secondary storage, resulting in longer retention on the Catalyst Copy targets. The deletion delay can now be controlled directly in the user interface, as opposed to the registry setting. This functionality is compatible with both HPE StoreOnce and HPE Cloud Volume Backup storage.
- **Cloud Volumes Backup support —** V11 adds official support for Catalyst Copy jobs to HPE Cloud Volumes Backup.
- **Catalyst SDK version —** HPE StoreOnce Catalyst SDK has been updated to version 4.2.4 with V11 protocol version.
- **Catalyst API sessions tagging —** Veeam file share backup jobs now tag Catalyst API calls with the special VeeamNAS tag. HPE support intends to use this information to differentiate Veeam workloads in their support cases for faster resolution.

Quantum DXi

- **Quantum FastClone support —** V11 officially supports enabling fast cloning on backup repositories backed by Quantum DXi models that support this functionality. Please contact Quantum support to confirm the status of the storage model you're using.
- **Improved full VM restore performance —** We added optimized restore logic for full VM restore, which is already used in other deduplicating storage integrations. Veeam backup proxy will now do sequential reads from Quantum and random writes to the target disks, as opposed to restoring blocks in the order they are stored in the target disk.

Deduplicating storage integrations are included in the **Veeam Universal License**. When using a legacy Socket-based license, **Enterprise** or higher edition is required.

Tape

- **Tape copy —** Easily clone selected tapes for the purposes of creating additional off-site copies, refreshing stored data to combat magnetic media decay over time or migrating your archives to modern LTO generation with migrations to both earlier and later generations supported. The backup server will update the backup catalog with references to the cloned (target) tapes, while also preserving references to the original (source) tapes.
- **Tape verification —** Verify your archived tapes periodically to ensure the stored data is still readable and consistent. Tape verification may be required for compliance reasons, and it helps you to sleep better at night too!
- **Restore all tape content —** Easily salvage all data from a media set that includes a failing tape by dumping all files that are still readable to the specified location.
- **Maintenance mode —** Put entire tape libraries or specific drives into maintenance mode to tell all your tape jobs not to use them temporarily.

- **Per-job drive limit —** You can now limit tape drive usage at the individual job level for Backup to Tape jobs.
- **Force tape erase —** The tape erase process will now ignore all non-critical errors, such as block size or header issues, since they are irrelevant for a tape about to be wiped clean.
- **Cluster-aware backup for NetApp ONTAP-based storages —** Cluster Aware Backup is an NDMP v4 protocol extension that enables the NDMP server to establish a data connection on a node that owns a volume, optimizing the data flow and improving NDMP backup performance.
- **Backup to Tape job sources —** Backup to Tape jobs can now process backup copies of Nutanix AHV and Mac backups, as well as of cloud-native backups for AWS, Azure and Google — enabling you to archive your cloud machine backups to tape for compliance purposes.
- **File to Tape job performance improvements —** Thanks to enhanced File to Tape job pre-processing logic, backup and restore operations now complete up to 10 times faster for datasets with a large number of files and folders in the protection scope.
- **File to Tape job protection scope —** You can now specify the entire data source (Windows Server or SMB/NFS file server) as the source in File to Tape jobs, which will protect all of its shares and exports, including those newly added. This new capability required changing the File from Tape restore wizard in order to support restore from such backups, which as a side effect now also allows you to configure mass restores of multiple file shares in a single pass of the wizard.
- **Enhanced reporting —** Backup, restore and tape verification jobs will now create a CSV file with all files that it could not process in the job's log folder.
- **Restore from Tape UX improvements —** Required tapes are now automatically displayed for every restore point selected in the wizard. You no longer need to view each of the selected restore points — just click Next and wait for the Insert these tapes prompt to appear.
- **Tape management UI improvements —** Added cleaning tape media lifespan to the tape properties dialog and tape library and drive serial numbers to the device properties dialog. The tape rescan session now indicates when it is completed. The location tag can now be set on NDMP servers. Context menus on the Tape Infrastructure tab have been updated for better clarity. Width of all columns was adjusted to fit the expected content out of the box.
- **LTO-9 support —** All native tape support functionality in V11 has been successfully validated against engineering samples of LTO-9 tape hardware kindly provided to us by IBM. If tape is the future, then V11 is ready for it!

Backup agents

Agent management

- **Backup from Storage Snapshots —** Microsoft Windows Servers with volumes hosted on supported storage arrays can now be backed up using "managed by server" agent-based backup jobs from native storage snapshots. This approach moves the backup data processing load from the protected server to the dedicated backup proxy. Furthermore, the usage of native storage snapshots eliminates the I/O overhead from the system running off of Software VSS snapshots for the duration of the backup. By addressing these two classic agent-based backup challenges, V11 brings LAN-free, zero-impact backups, *identical to off-host VMware and Hyper-V VM backup*, to physical servers and clusters, allowing users to protect even their busiest 24/7 workload without breaching SLAs. All built-in and Universal Storage API-based storage integrations with iSCSI or FibreChannel connectivity are supported, and no vendor-specific Hardware VSS Provider is required.

- **Protection group for pre-installed agents —** This protection group (PG) type provides a convenient way to install agents using third-party software distribution solutions, when deploying them from the backup server is not possible due to security and network connectivity restrictions. The PG wizard creates a custom agent installation package that enables an agent to connect to the backup server automatically using the PKI-based authentication with a PG certificate. The backup server then places an incoming agent into the protection group that created their installation package and issues the new personal authentication certificate. At which point, you can use the agent in "managed by agent" backup policies normally. There's no requirement for the backup server to be able to connect to agents over the network, as the agents themselves will query the backup server for changed policy settings several times per day.
- **Export as virtual disk improvements —** Disks from agent-based backups can now be exported as fixed VHD/VHDX disks to allow for mounting them in Microsoft Azure services (previously, disks could only be exported as dynamic).
- **Unprotected hosts email notification —** Added an optional email notification for hosts that were not backed up at least once within the specified number of days with the "managed by agent" backup policy.
- **Remove from configuration —** You can now remove machines from Protection Groups via the context menu on the host.
- **Recovery media from backup copies —** Recovery media can now also be created from backups created by Backup Copy jobs.
- **Veeam Agent *for Microsoft Windows* —** The agent-based backup job wizard now provides the ability to configure the "Backup all volumes except excluded" setting for the volume-level backup mode, exclude OneDrive folder from processing and use the new user profile backup mode.

Veeam Agents

- **Veeam Agent *for Microsoft Windows* v5:** New functionality includes support for Microsoft Windows 10 version 20H2, wider Microsoft .NET Framework versions compatibility to avoid the reboot requirement following the .NET installation, daily and GFS retention options for servers, user profiles backup in the file-level mode, improved VPN connection detection, FIPS compliance and more. For the complete list of new features, please refer to the corresponding What's New document.
- **Veeam Agent *for Linux* v5:** New functionality includes new OS versions support, extended attributes backup in the file-level mode, multiple recovery media enhancements, FIPS compliance and more. For the complete list of new features, please refer to the corresponding What's New document.
- **Veeam Agent *for Mac*:** The new agent delivers managed end-user data backup for any macOS device from Veeam Backup & Replication, allowing you to seamlessly integrate Mac laptop and workstation protection into your overall data protection strategy. And unlike the built-in Apple Time Machine software, Veeam Agent *for Mac* allows you to meet the 3-2-1 Rule through creating additional on-site and off-site backups using the familiar Veeam features and functionality.

  Built on the proven Veeam Agent *for Linux* agent engine, the Mac agent includes the following features:

  - Backup of user data and external USB drives content
  - Integration with configuration profiles of MDM solutions
  - Simple self-service file-level restore by end users via a local UI

Enterprise applications plug-ins

General

- **SOBR Capacity Tier support —** Backups and backup copies of all enterprise application plug-ins can now be copied or moved to object storage with the SOBR Capacity Tier functionality. Just as with image-level backups, restore from backups offloaded to object storage is fully transparent.
- **Performance enhancements —** We've made major performance improvements on all fronts, particularly thanks to the new approach to the metadata handling with per-backup metadata files, dramatically improving overall scalability. Please check the upgrade documentation on how to migrate your existing backups to the new metadata format.
- **Self-healing metadata —** Periodic backup health check scans all restore points every six hours and recreates missing metadata files, which may be caused when backup is interrupted by an external event. You can change this period by creating the *DbPluginMissingMetaRegenerationAttemptIntervalMinutes* (DWORD) value on the backup server.
- **FIPS compliance —** All enterprise application plug-ins now use FIPS-compliant encryption modules.

Veeam Plug-in *for Oracle RMAN*

- **Oracle Data Guard support —** Full support for backup of Oracle Data Guard deployments.
- **Improved RAC compatibility —** Oracle RAC installations with empty /etc/oratab file are now supported.

Veeam Plug-in *for Oracle RMAN on AIX*

This new plug-in provides the same functionality, installation and configuration experience as its Solaris counterpart. Supported versions include IBM AIX 6.1, 7.1, 7.2 and Oracle 11, 12, 18, 19 (ppc64 version).

Veeam Plug-in for SAP HANA

- **SAP HANA 1.0 support —** In addition to the existing SAP HANA 2.0 support, this release now supports SAP HANA Database 1.0 SPS 12 or newer (please refer to KB2997 for the installation instructions). The plug-in officially certified by SAP for HANA versions 1.0 and 2.0.

Veeam Plug-in for SAP on Oracle

This new SAP certified plug-in provides integration with SAP BR*Tools to enable Oracle database backups directly to Veeam repositories with both util_file and util_file_online backup modes supported. Note that Veeam Plug-ins for Oracle RMAN and for SAP on Oracle can be used together for running backups in rman_util mode. Supported versions include 64-bit versions of:

- OS: SLES 11,12 and 15; RHEL 6 and 7; Oracle Linux 6 and 7
- Oracle: 11.2 up to 19.1
- BR*tools: 7.20 Patch 42 or later

Enterprise application plug-ins are included in the **Veeam Universal License**. When using a legacy Socket-based license, **Enterprise *Plus* edition** is required.

NAS Backup

General

- **Root protection scope —** You can now specify the entire data source (SMB/NFS file server) as the source in file share backup jobs, which will protect all of its shares and exports, including newly added. This new capability required changing the file share restore wizard in order to support restores from such backup, which, as a side effect, now also allows you to configure mass restores of multiple file shares in a single pass of the wizard. In addition, storage snapshot folders will be excluded from processing automatically whenever detected, so you no longer have to explicitly add them to the backup job exclusions list.

  NOTE: You can convert existing backups into the format accepted for mapping in a newly created backup job with the root-based scope using the Convert-VBRNASBackupRootFormat cmdlet.

- **Improved performance —** File share backup and Backup Copy job performance are now up to 2X faster, thanks to the usage of multiple upload streams between source and target data movers with transfers over high-latency networks benefiting from this change the most.

- **Intelligent load balancer —** In the presence of multiple backup proxies, file share backup jobs will now automatically detect and use the least occupied backup proxy (just like VM backup jobs already do), allowing for more even load and full compute capacity utilization.

- **Locked file alerts —** You can now control whether you want to log file and file attributes processing issues as a warning in the overall file share backup job result. In addition, the path to the audit file listing all locked files is now displayed in the job log.

- **Version-based retention —** To better control backup repository storage consumption, you can now choose between applying the version-based retention to file versions in the archive repository only (a V10 behavior) or have the cross-cutting retention across both the backup and archive repositories.

- **Automatic backup mapping for backup copies —** Backup copy processes will now attempt to automatically detect the presence of the seeded backup upon the first run and will continue the existing backup with an increment if a seed is present.

Primary storage integrations

- **Enterprise NAS filer integration —** Native Dell EMC Isilon, Lenovo DM and NetApp FAS integrations allow you to register the entire filer as a data source and perform file share backups without having to obtain access permissions to each protected file share. In addition, backup from such data sources will be performed from native storage snapshots out of the box to avoid locked files without requiring complex setup and scripts to manage snapshots.

  NOTE: You can convert existing backups into the format accepted for mapping in a newly created backup job with the NAS filer-based scope using the Convert-VBRNASBackupStorageFormat cmdlet.

- **Native changed file tracking integration —** V11 file share backup jobs can integrate with Dell EMC Isilon Changelist API to reduce storage load and improve the performance of incremental backups in scenarios where backed up file shares have a large number of subfolders with low change rates.

Secondary storage integrations

- **Large blobs —** File share backup and Backup Copy jobs will now automatically switch to using 1GB blobs when deduplication storage appliances are used as the target. This increases scalability up to 20 times for storage devices that support a limited amount of files per appliance (e.g., HPE StoreOnce) and improves backup and restore performance up to a few times for all deduplication storage.

NOTE: You can use Convert-VBRNASBackupStorageFormat cmdlet to upgrade your existing jobs to use large blobs.

- **Metadata extents —** When using Scale-out Backup Repositories consisting exclusively of slow storage, like deduplicating appliances, you can improve backup and restore performance by a few times by introducing a small metadata-only extent with fast storage which will only be used to store backup metadata. Being an advanced feature, it can be configured with PowerShell only using the Set-VBRRepositoryExtent cmdlet.

User interface

Backup console

- **No local admin requirement —** The backup console no longer requires operators to use an account with the Local Administrator group membership on the system that runs the console. This helps to improve security by not having to assign administrative privileges to all console operators. When console update installation is required and for restore scenarios that actually do require Local Administrator privileges, you will be offered the opportunity to restart the console under an administrative account.
- **Orphaned backups —** Backups without an associated job are much easier to track now, thanks to the new Orphaned node under Backups. Previously, such backups ended up in the Imported backups node and were impossible to distinguish.
- **Filter-based job nodes —** You can now add custom job views (a V10 feature) as persistent nodes to the management tree for faster access to the favorite views you are using most often.
- **Backup immutability info —** We added a column showing the Hardened Repository backup immutability expiration time to the backup properties dialog.
- **Action log timestamps —** By popular demand, in addition to the operation duration column, you can now display the timestamp column with the time when each operation started. To do this, right-click the action log header.
- **Windows notification center integration —** We will now use the Windows notification center to display interactive notifications such as a SQL Server configuration database approaching its size limit (new in V11), tape job waiting for a tape to be inserted and other important messages that were previously displayed in a system tray balloon message.
- **No more Finish button confusion —** The Finish button on the last step of file-level and item-level recovery wizards has been renamed to Browse to better convey the fact that the process will continue with the items selection. Previously, some users were too scared to click this button due to wrongly assuming the restore will start before they actually selected what to restore.
- **Swagger console —** You can now open the new backup server RESTful API interactive documentation (powered by Swagger) directly from the main menu.
- **Deprecated features —** The "Transform previous backup chains into rollbacks" functionality has been deprecated, so the corresponding checkbox is no longer present in the user interface for newly created jobs. If you need help with transitioning away from this backup mode, please share your use case on the Veeam R&D Forums. We plan to remove this capability completely in our next major release in 2022.

Enterprise Manager

- **Web UI localization —** We added the industry-standard GetText localization framework to Enterprise Manager —and thanks to our local pre-sales engineering team, Veeam Backup Enterprise Manager v11 ships with the following translations already built in: French, German, Italian, Japanese, Spanish and Simplified Chinese.

- **SSO logon experience —** We have changed the logon UI to no longer require entering a username for SSO logons. Instead, we immediately redirect users to the configured identity provider for authentication. This enables users from an organization using credential-less authentication (for example, smartcard-only environments) to log on to the Enterprise Manager and its portals.
- **SAML support for vSphere Self-Service Backup Portal —** The portal has been getting much interest from outside of its original target audience, particularly from service providers. To support this trend, we added SAML integration, enabling service providers to give their tenants access to the portal by assigning quotas to external users and groups. In the case of SAML accounts, the only supported delegation mode is vSphere Tags-based.
- **UI enhancements —** For Microsoft Exchange items recovery, we will now display the mailbox name next to the username to avoid confusion for people with similar names. We also added object search functionality when defining the scope of the Restore Operator role.

Licensing

General

- **Best change is no changes, finally! —** V11 uses the same license file format introduced back with V10. Such license files are no longer tied to a particular software version, allowing you to use your existing V10 license file for V11, so long as your maintenance contract is still active.
- **License auto update in the setup —** When performing an in-place upgrade from V9, the setup wizard will offer you the chance to download the V11 license file automatically. This requires uploading your currently installed license to Veeam servers. If your backup server has no internet connection or if you prefer not to have your current license uploaded — you can download your license file from the Customer Portal instead.
- **License auto update in the product —** When installing a license file, you will now be offered the opportunity to have license extensions downloaded automatically when you renew or expand your contract. This optional functionality requires the backup server to send the license ID, the installation ID and workload usage counters to Veeam servers periodically. If you'd rather not share this information with Veeam, do not enable this functionality and instead download your updated license files from the Customer Portal and install them manually.
- **Simplified license renewal —** You can now initiate the license renewal process directly from the License Information dialog. The Renew button redirects users to the Veeam website and the license renewal request form with some of the required information already pre-populated based on the currently installed license.

Veeam Universal License (VUL)

- **Doubled NAS protection —** After reviewing the average discounts our sales have been providing in VUL-based NAS protection opportunities, we decided to double the amount of NAS data covered by one license from 250GB to 500GB. This change also means that you can now protect the first 500GB of data from any file source at no cost (up from 250GB with V10a). To take advantage of the new NAS backup capacity entitlement, you must upgrade to V11.
- **Starter edition removal —** This edition was discontinued in the fall of 2020, so V11 will not accept such license files. Please download a replacement license file for Veeam Backup Essentials™ from the Customer Portal — it's a free upgrade for the remainder of your contract.

Socket-based licenses

- **Product editions removal —** Just like VUL, Socket-based licenses are now offered to net new customers in a single, fully featured edition, formerly known as Enterprise *Plus*. Existing customers who already own a Socket-based license can continue to use, renew and expand whatever license edition they have. If you're interested in any functionality not available in your product edition, contact your Veeam sales representative for special offers on upgrading your Socket license edition or migrating to VUL.

Community Edition

- **Now with even more features —** The updated V11 *Community Edition* includes all new V11 features and enhancements except those few tagged with the special licensing requirements. It also benefits from the NAS backup capacity entitlement change, now allowing protection of over 5TB of NAS data with the free license — with the first 500GB of data per file share not consuming the license at all.

  Support *Community Edition* by upgrading to Veeam Backup Essentials if possible! The subscription costs less than a dinner in a fancy restaurant, while giving you access to ALL features and 24/7 customer support! Such conversions help us continue offering enterprise-class data protection for free to those who truly can't afford it.