



# Veeam Backup & Replication 12.1 Release Notes

This document provides last-minute information about Veeam Backup & Replication 12.1, including system requirements, installation and upgrade procedures, as well as relevant information on technical support, documentation, online resources, and so on.

The release version of Veeam Backup & Replication 12.1 is available for download at [veeam.com/backup-replication-download.html](https://www.veeam.com/backup-replication-download.html) starting from December 5, 2023.

If you are upgrading to Veeam Backup & Replication 12.1 from previous versions, please **review the [upgrade checklist](#)** closely before performing the upgrade.

## See next:

- [System Requirements](#)
- [Known Issues](#)
- [Installing Veeam Backup & Replication](#)
- [Uninstalling Veeam Backup & Replication](#)
- [Upgrading Veeam Backup & Replication](#)
- [Licensing](#)
- [Updating Veeam Backup & Replication License](#)
- [Technical Documentation References](#)
- [Technical Support](#)
- [Contacting Veeam Software](#)

# System Requirements

We recommend that all 3rd party software and components are kept at the latest patch level since these updates often address issues that can cause slow performance, backup failures, and data corruption.

## VMware Infrastructure

### Platforms

- VMware vSphere
- VMware vCloud Director
- VMware Cloud on AWS
- VMware Cloud on Dell
- Microsoft Azure VMware Solution
- Google Cloud VMware Engine
- IBM Cloud for VMware Solutions
- Oracle Cloud VMware Solution
- VMware Cloud Foundation (VCF)

### Hosts

- ESXi 8.0 (up to 8.0 U2)
- ESXi 7.0 (up to 7.0 U3)
- ESXi 6.x

### Software

- vCenter Server or vCenter Server Appliance 8.0 (up to 8.0 U2)
- vCenter Server or vCenter Server Appliance 7.0 (up to 7.0 U3)
- vCenter Server or vCenter Server Appliance 6.x
- vCloud Director 10.1 to 10.5

Standalone ESXi hosts are fully supported, so vCenter Server and vCloud Director are optional. However, whenever they are present, we highly recommend that you register both with Veeam so that VMs can continue to be tracked as they move across the infrastructure.

### Veeam CDP

The following infrastructure requirements only apply when Veeam CDP replication is used:

- The minimum supported ESXi version is 6.5 U2.
- For Cloud Director Continuous Data Protection, the version of target hosts must be 7.0 or higher. Target hosts of versions 6.5 and 6.7 are not supported.
- Cisco HyperFlex 4.5 (2a) and later can be used as a source or target only with VMware vSphere 7.0 U2 and later. With the previous versions of VMware vSphere, Cisco HyperFlex is not supported.
- Minimum 16GB RAM for source and target ESXi hosts.
- vCenter Server is required (standalone ESXi hosts are not supported).
- Backup server, CDP proxies, vCenter Server, and ESXi hosts must be able to resolve each other's DNS names.
- VMware Cloud on AWS is not supported.

## vSphere Virtual Machines

### Virtual Hardware

- All types and versions of virtual hardware are supported.
- Virtual machines with virtual NVDIMM devices, with virtual disks engaged in SCSI bus sharing or residing on PMem datastores are not supported for host-based backup. Please use the agent-based backup to protect such VMs.
- RDM virtual disks in physical mode, independent disks, and disks connected via in-guest iSCSI initiator are not supported for host-based backup. Such disks are skipped from processing automatically. If backing up these disks is required, please use agent-based backup.

### OS

- All operating systems supported by the VMware vSphere version in use.
- Microsoft VSS integration is supported for Microsoft Windows 2008 and later, except for Nano Server (due to the absence of VSS framework).
- File-level restore is supported for the following file systems, including Microsoft Windows Logical Disk Manager (LDM) dynamic disks and Linux Logical Volume Manager (LVM):

OS	Supported File Systems
Windows	FAT, FAT32 NTFS ReFS
Linux	ext2, ext3, ext4 ReiserFS JFS XFS Btrfs
BSD	UFS, UFS2
Mac	HFS, HFS+
OES	NSS
Solaris	UFS ZFS (except pool versions of Oracle Solaris)

### Software

- VMware Tools (optional, recommended)

## Microsoft Infrastructure

### Platforms

- Microsoft Windows Server Hyper-V
- Microsoft Hyper-V Server (free hypervisor)
- Microsoft Azure Stack HCI

### Hosts

- Hyper-V 2022
- Hyper-V 2019
- Hyper-V 2016
- Hyper-V 2012 R2
- Hyper-V 2012
- Azure Stack HCI

Microsoft Windows 11 Hyper-V (version 21H2, 22H2, 23H2) and Windows 10 Hyper-V (versions 1909 to 22H2) are supported only as a target host for Instant Recovery; host-based backup of its VMs is not supported. You can, however, protect them with agent-based backup.

Microsoft Nano Server with Hyper-V role installed is not supported for any functionality.

### Software

- Microsoft Windows PowerShell 5.1 (optional, enables network-less guest processing)
- Microsoft System Center Virtual Machine Manager 2012 SP1 to 2022

Standalone Hyper-V hosts and clusters are fully supported, so SCVMM is optional. Registering Hyper-V clusters may provide better scalability in large environments.

# Hyper-V Virtual Machines

## Virtual Hardware

- Supported virtual hardware versions are 5.0 to 10.0
- Both Generation 1 and 2 virtual machines are supported.
- Pass-through virtual disks and guest disks connected via in-guest FC or iSCSI initiators are not supported for host-based backup. Such disks are skipped from processing automatically. If backing up these disks is required, please use agent-based backup.

## OS

- All operating systems supported by the Hyper-V version in use.
- Microsoft VSS integration is supported for Microsoft Windows 2008 and later, except for Nano Server (due to the absence of VSS framework). The persistent guest agent requires Windows Server 2008 SP2 or later.
- File-level restore is supported for the following file systems, including Microsoft Windows LDM dynamic disks and Linux LVM:

OS	Supported File Systems
Windows	FAT, FAT32 NTFS ReFS
Linux	ext2, ext3, ext4 ReiserFS JFS XFS Btrfs
BSD	UFS, UFS2
Mac	HFS, HFS+
Solaris	UFS ZFS (except pool versions of Oracle Solaris)

## Software

- Hyper-V integration components (optional, recommended)

# Veeam Backup & Replication Server

## Hardware

*CPU:* x86-64 processor (minimum 4 cores recommended).

*Memory:* 4 GB RAM plus 500 MB RAM for each concurrent job.

*Disk Space:* 5 GB for product installation and 4.5 GB for Microsoft .NET Framework 4.7.2 installation. 10 GB per 100 VM for guest file system catalog folder (persistent data). Additional free disk space for Instant VM Recovery cache folder (non-persistent data, at least 100 GB recommended).

*Network:* 1 Gbps or faster for on-site backup and replication, 1 Mbps or faster for off-site backup and replication. High latency and reasonably unstable WAN links are supported.

## OS

64-bit versions of the following Microsoft Windows operating systems are supported:

- Microsoft Windows Server 2022
- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows 11 (versions 21H2, 22H2, 23H2)
- Microsoft Windows 10 (versions 1909 to 22H2)
- Microsoft Windows 10 LTS (versions LTSB 1607, LTSC 1809, LTSC 2021)

## Configuration Database

- PostgreSQL 14.x, 15.x (version 15.5 is included in the setup)  
Note that Veeam Backup & Replication does not support PostgreSQL installations on cloud database services (for example, Amazon Relational Database Service (RDS)).
- Microsoft SQL Server 2012 to 2022

## Software

- Microsoft .NET Framework 4.7.2 (included in the setup)
- Microsoft Windows Desktop Runtime 6.0.24 (included in the setup)
- Microsoft ASP.NET Core Shared Framework 6.0.24 (included in the setup)
- Microsoft Windows PowerShell 5.1 (included in the setup)
- Microsoft SQL Server System CLR Types (both for SQL Server and PostgreSQL, included in the setup)
- Microsoft Report Viewer Redistributable 2015 (included in the setup)
- Microsoft Universal C Runtime (included in the setup)
- System Center Virtual Machine Manager 2012 SP1 to 2022 Admin UI (optional, to register SCVMM server with Backup & Replication infrastructure)
- Microsoft Edge WebView2 Runtime 119.0.2151.72 (included in the setup)
- Windows Installer 4.5
- Firefox, Google Chrome, or Microsoft Edge (optional, to use Veeam Backup Enterprise Manager web UI)

# Veeam Backup & Replication Console

## Hardware

*CPU:* x86-64 processor.

*Memory:* 2 GB RAM

*Disk Space:* 500 MB for product installation and 4.5 GB for Microsoft .NET Framework 4.7.2 installation.

*Network:* 1 Mbps connection to the backup server. High latency and low bandwidth affect the user interface responsiveness.

## OS

64-bit versions of the following Microsoft Windows operating systems are supported:

- Microsoft Windows Server 2022
- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows 11 (versions 21H2, 22H2, 23H2)
- Microsoft Windows 10 (versions 1909 to 22H2)
- Microsoft Windows 10 LTS (versions LTSC 1607, LTSC 1809, LTSC 2021)

## Software

- Microsoft .NET Framework 4.7.2 (included in the setup)
- Microsoft Windows Desktop Runtime 6.0.24 (included in the setup)
- Microsoft Windows PowerShell 5.1 (included in the setup)
- Microsoft SQL Server System CLR Types (both for SQL Server and PostgreSQL, included in the setup)
- Microsoft Report Viewer Redistributable 2015 (included in the setup)
- Microsoft Universal C Runtime (included in the setup)
- Microsoft Edge WebView2 Runtime 119.0.2151.72 (included in the setup)
- Windows Installer 4.5
- Firefox, Google Chrome, or Microsoft Edge (optional, to use Veeam Backup Enterprise Manager web UI)

## Backup Proxy Server (for VMware, Hyper-V, Agents, Unstructured Data Backup)

### Hardware

*CPU:* x86-64 processor (minimum 2 cores or vCPUs). Using multi-core processors improves data processing performance and allows more tasks to be processed concurrently.

*Memory:* 2 GB RAM plus 500 MB for each concurrent task. In case of file or object storage backup, 4 GB RAM for each concurrent task. The actual size of memory required may be larger and depends on the amount of data to back up, machine configuration, and job settings. Using faster memory improves data processing performance.

*Disk Space:* 750 MB for Microsoft Windows-based proxies; 400 MB for Linux-based proxies.

*Network:* 1 Gbps or faster for on-site backup and replication, 1 Mbps or faster for off-site backup and replication. High latency and reasonably unstable WAN links are supported.

### OS

For VMware vSphere backup proxy, 64-bit versions of the following Microsoft Windows operating systems are supported, including the Core edition:

- Microsoft Windows Server 2022
- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows 11 (versions 21H2, 22H2, 23H2)
- Microsoft Windows 10 (versions 1909 to 22H2)
- Microsoft Windows 10 LTS (versions LTSC 1607, LTSC 1809, LTSC 2021)

Besides, 64-bit versions of the following Linux distributions are supported:

- CentOS 7.x
- Debian 10.0 to 12.2
- RHEL 7.0 to 9.3
- Oracle Linux 7 (UEK3) to 9 (UEK R7)
- Oracle Linux 7 to 9 (RHCK)
- SLES 12 SP4 or later, 15 SP1 or later
- Ubuntu 18.04 LTS, 20.04 LTS, and 22.04 LTS

For the Hyper-V off-host backup proxy server, the following operating systems are supported, including the Core Edition (the Hyper-V role must be enabled on the server):

- Microsoft Windows Server 2022
- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012

For agent-based off-host backup proxy server, 64-bit versions of the following Microsoft Windows operating systems are supported, including the Core edition:

- Microsoft Windows Server 2022
- Microsoft Windows Server 2019
- Microsoft Windows Server 2016



- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012

For general-purpose backup proxy server used for file backup and object storage backup, 64-bit versions of the following Microsoft Windows operating systems are supported, including the Core edition:

- Microsoft Windows Server 2022
- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows 11 (versions 21H2, 22H2, 23H2)
- Microsoft Windows 10 (versions 1909 to 22H2)
- Microsoft Windows 10 LTS (versions LTSC 1607, LTSC 1809, LTSC 2021)

SMB 3.0 file share backup from Microsoft VSS snapshots requires Microsoft Windows Server 2012 R2 or later.

For general-purpose backup proxy server used for object storage backup, also 64-bit versions of the following Linux distributions are supported:

- CentOS 7.x
- Debian 10.0 to 12.2
- Oracle Linux 7 (UEK3) to 9 (UEK R7)
- Oracle Linux 7 to 9 (RHCK)
- RHEL 7.0 to 9.3
- SLES 12 SP4 or later, 15 SP1 or later
- Ubuntu: 18.04 LTS, 20.04 LTS, and 22.04 LTS

## CDP Proxy Server

### Hardware

*CPU:* x86-64 processor (minimum 4 cores or vCPUs). Using multi-core processors improves data processing performance and allows for more tasks to be processed concurrently.

*Memory:* 8 GB RAM. Using more memory allows for longer peak write I/O periods before a CDP policy switches to the disk-based write I/O cache. Using faster memory improves data processing performance.

*Disk Space:* 300 MB plus disk-based write I/O cache (non-persistent data, at least 50 GB recommended). A larger cache allows for longer network downtime periods before a CDP policy switches to the CBT mode.

*Network:* 100 Mbps or faster.

### OS

64-bit versions of the following Microsoft Windows operating systems are supported, including the Core edition:

- Microsoft Windows Server 2022
- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012

- Microsoft Windows 11 (versions 21H2, 22H2, 23H2)
- Microsoft Windows 10 (versions 1909 to 22H2)
- Microsoft Windows 10 LTS (versions LTSB 1607, LTSC 1809, LTSC 2021)

64-bit versions of the following Linux distributions are supported. Note that bash shell and SSH are required.

- CentOS 7.x
- Debian 10.0 to 12.2
- Oracle Linux 7 (UEK3) to 8.3 (UEK R6 U2)
- Oracle Linux 7 to 8.5 (RHCK)
- RHEL 7.0 to 9.3
- SLES 12 SP4 or later, 15 SP1 or later
- Ubuntu: 18.04 LTS, 20.04 LTS, and 22.04 LTS

## Backup Repository Server

These requirements also apply to mount servers (if separated from the repository server), gateway servers for file shares, object storage and deduplicating appliance-based repositories, and cache repository servers.

### Hardware

*CPU:* x86-64 processor.

*Memory:* 4 GB RAM, plus not less than 1 GB RAM for each concurrently processed machine disk and not less than 4 GB RAM for each concurrently processed unstructured data source (file share or object storage repository).

*Network:* 1 Gbps or faster for on-site backup and replication, 1 Mbps or faster for off-site backup and replication. High latency and reasonably unstable WAN links are supported.

### OS

64-bit versions of the following Microsoft Windows operating systems are supported, including the Core edition:

- Microsoft Windows Server 2022
- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows 11 (versions 21H2, 22H2, 23H2)
- Microsoft Windows 10 (versions 1909 to 22H2)
- Microsoft Windows 10 LTS (versions LTSC 1607, LTSC 1809, LTSC 2021)

64-bit versions of the following Linux distributions are supported:

- CentOS 7.x
- Debian 10.0 to 12.2
- Oracle Linux 7 (UEK3) to 9 (UEK R7)
- Oracle Linux 7 to 9 (RHCK)
- RHEL 7.0 to 9.3
- SLES 12 SP4 or later, 15 SP1 or later
- Ubuntu: 18.04 LTS, 20.04 LTS, and 22.04 LTS

Bash shell and SSH connectivity are required to deploy the management agent (SSH Server can be disabled afterward and is not required to update Veeam components).

For advanced XFS integration, only the following 64-bit Linux distributions are supported:

- Debian 10.0 to 12.2
- RHEL 8.2 to 9.3
- SLES 15 SP2, SP3, SP4, SP5
- Ubuntu 18.04 LTS, 20.04 LTS, 22.04 LTS

For other distributions, XFS integration support is [experimental](#), with kernel version 5.4 or later recommended.

# Tape Server

## Hardware

*CPU:* x86-64 processor.

*Memory:* 2 GB RAM plus 500MB for each concurrent task. Depending on the source of tape jobs, different entities are considered tasks: for machine backup to tape, a task covers a source job or a source chain if tape paralleling is enabled; for file backup to tape, a task covers an entire server or a file share. Restoring VMs directly from tape requires 400MB of RAM per 1TB of the restored virtual disk size. Tape cloning requires 1GB RAM for each concurrent task.

*Disk Space:* 300 MB, plus 10GB for temporary data storage for backup and restore operations.

*Network:* 1 Gbps or faster.

## OS

64-bit versions of the following Microsoft Windows operating systems are supported, including the Core edition:

- Microsoft Windows Server 2022
- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows 11 (versions 21H2, 22H2, 23H2)
- Microsoft Windows 10 (versions 1909 to 22H2)
- Microsoft Windows 10 LTS (versions LTSC 1607, LTSC 1809, LTSC 2021)

64-bit versions of the following Linux distributions are supported:

- CentOS 7.x
- Debian 10.0 to 12.2
- Oracle Linux 7 (UEK3) to 9 (UEK R7)
- Oracle Linux 7 to 9 (RHCK)
- RHEL 7.0 to 9.3
- SLES 12 SP4 or later, 15 SP1 or later
- Ubuntu: 18.04 LTS, 20.04 LTS, and 22.04 LTS

## WAN Accelerator Server

### Hardware

*CPU:* x86-64 processor. Using multi-core processors improves data processing performance and is highly recommended on WAN links faster than 10 Mbps.

*Memory:* 8 GB RAM. Using faster memory improves data processing performance.

*Disk Space:* Disk space requirements depend on the WAN Accelerator role:

Source WAN Accelerator requires 20 GB per 1 TB of source data to store digests of data blocks of source VM disks. Disk space consumption is dynamic and changes as unique VMs are added to (or removed from) jobs with WAN Acceleration enabled.

Target WAN Accelerator requires global cache size as defined by the user (fixed amount). Disk space is reserved immediately upon selecting the WAN Accelerator as a target one in any job.

*Network:* 1 Gbps or faster for on-site backup and replication, 1 Mbps or faster for off-site backup and replication. High latency and reasonably unstable WAN links are supported.

### TIP

Global cache is not leveraged by source WAN Accelerators or WAN accelerators operating in high-bandwidth mode, so it does not need to be allocated and populated in such cases.

### OS

64-bit versions of the following Microsoft Windows operating systems are supported, including the Core edition:

- Microsoft Windows Server 2022
- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows 11 (versions 21H2, 22H2, 23H2)
- Microsoft Windows 10 (versions 1909 to 22H2)
- Microsoft Windows 10 LTS (versions LTSC 1607, LTSC 1809, LTSC 2021)

## Veeam Backup Enterprise Manager

### Hardware

*Processor:* x86-64 processor.

*Memory:* 4 GB RAM.

*Hard Disk Space:* 2 GB for product installation plus sufficient disk space to store guest file system catalog from connected backup servers (according to data retention policy).

*Network:* 1 Mbps or faster connection to Veeam Backup & Replication servers. Slow or unstable links will impact the performance of Veeam Backup Enterprise Manager data collection operations from Veeam Backup servers.

### OS

Only 64-bit versions of the following operating systems are supported:

- Microsoft Windows Server 2022
- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server Semi-Annual Channel (versions 1803 to 20H2)
- Microsoft Windows 11 (versions 21H2, 22H2, 23H2)
- Microsoft Windows 10 (versions 1909 to 22H2)
- Microsoft Windows 10 LTS (versions LTSC 1607, LTSC 1809, LTSC 2021)

### **Configuration Database**

- PostgreSQL 14, 15 (version 15.5 is included in the setup)  
Note that Veeam Backup Enterprise Manager does not support PostgreSQL installations on cloud database services (for example, Amazon Relational Database Service (RDS)).
- Microsoft SQL Server 2012 to 2022

### **Server Software**

- Microsoft .NET Framework 4.7.2 (included in the setup)
- Microsoft SQL Server System CLR Types (both for SQL Server and PostgreSQL, included in the setup)
- Microsoft Report Viewer Redistributable 2015 (included in the setup)
- Microsoft Universal C Runtime (included in the setup)
- Microsoft Visual C++ 2015-2019 Redistributable (included in the setup)
- Microsoft Internet Information Services 7.5 or later
- Microsoft URL Rewrite 2.0 for IIS 7
- Windows Installer 4.5 (included in the setup)

### **Client Software**

- Firefox, Google Chrome, or Microsoft Edge. The browser must have JavaScript and WebSocket protocol enabled.
- Microsoft Excel to view reports exported to Microsoft Excel format.

## Backup Target

Backups can be performed directly to the following disk-based storage:

- Local (internal) storage of the backup repository server.
- Direct Attached Storage (DAS) connected to the backup repository server, including external USB/eSATA drives and raw device mapping (RDM) volumes.
- Storage Area Network (SAN). The backup repository server must be connected to the SAN fabric via hardware or virtual HBA, or software iSCSI initiator.
- Network Attached Storage (NAS) able to present its capacity as NFS share (protocol versions 3.0 and 4.1 only) or SMB/CIFS share (all protocol versions). Using consumer-grade NAS storage without an enterprise-grade RAID controller with a battery-backed write cache (BBWC) is not recommended for reliability considerations.
- Amazon S3
- Google Cloud Storage
- IBM Cloud Object Storage
- Microsoft Azure Blob Storage
- Wasabi Hot Cloud Storage
- Any S3-compatible object storage (on-premises appliance or cloud storage provider)
- Dell Data Domain (DD OS version 7.3 to 7.13) with the DDBoost license. Both Ethernet and Fibre Channel (FC) connectivity are supported.
- ExaGrid (firmware version 5.0.0 or later).
- Fujitsu CS800 (CS800 software 3.4.0 or later).
- HPE StoreOnce (firmware version 3.18.18 or later for Gen3 and 4.2.3 or later for Gen4) with Catalyst license. Both Ethernet and Fibre Channel (FC) connectivity are supported.
- Infinidat InfiniGuard (InfiniGuard software 3.6 or later).
- Quantum (DXi software 3.4.0 or later). Supported Quantum DXi systems include DXi4700 (NAS configuration), DXi4700 (multi-protocol configuration), DXi 4800, DXi 6900, DXi 6900-S, DXi 9000, DXi 9100, and DXi V5000. FIPS-compliant operations mode requires DXi software 4.0 or later.

Once backups are created, they can be copied (for redundancy) or offloaded (for long-term retention) to one of the following hot object storage types using the scale-out backup repository Capacity Tier:

- Amazon S3 (including AWS Snowball Edge)
- Google Cloud Storage
- IBM Cloud Object Storage
- Microsoft Azure Blob Storage (including Microsoft Azure Data Box)
- Wasabi Hot Cloud Storage
- Any S3-compatible object storage (on-premises appliance or cloud storage provider)

Once backups are created on Amazon S3, Microsoft Azure Blob Storage, or S3-compatible object storage systems with the archiving extension of Smart Object Storage API, they can be further archived to one of the following respective cold object storage classes using the scale-out backup repository Archive Tier:

- Amazon S3 Glacier Instant Retrieval
- Amazon S3 Glacier Flexible Retrieval
- Amazon S3 Glacier Deep Archive

- Microsoft Azure Archive Tier
- Microsoft Azure Cold Tier

## Veeam CDP

The following source and target datastores are supported:

- NFS on file storage
- VMFS on block storage
- VMFS on internal ESXi storage
- VSAN  
VSAN is supported for all hyper-converged infrastructure (HCI) appliances.
- VVOL  
VVOL is supported for the following vendors: NetApp, HPE Nimble, Pure Storage, and HPE 3PAR. For the list of tested vendor product lines, see [this Veeam KB article](#).

Support for hyper-converged infrastructure (HCI) appliances other than VSAN is pending validation by Veeam. System requirements will be updated based on the testing results.

## Tape

The following types of tape libraries (including VTL) and standalone drives are supported:

- LTO3-LTO9
- IBM 3592 (TS1160 and TS1170)

The tape device must be directly attached to the backup server, to a tape server via SAS, FC, or iSCSI interface.

### Drivers

- Tape devices without device-specific, vendor-supplied OEM drivers for Windows installed will appear in Windows Device Manager as Unknown or Generic and require enabling native SCSI commands mode.
- If multiple drivers are available for your tape device, use the one that allows multiple open handles from a host to a drive to exist simultaneously. Usually, such drivers are referred to as "non-exclusive."
- No other backup server or software must interact with the tape device.



## Storage Snapshot Integrations

Storage snapshot integration is supported for pre-installed and additional plug-ins available for download at [www.veeam.com/backup-replication-download.html](http://www.veeam.com/backup-replication-download.html) (under Additional Downloads).

### Built-in Storage Systems

#### Cisco HyperFlex HX-Series

- VMware integration only
- NFS connectivity only
- HyperFlex 4.0(2x) or later (Backup from Storage Snapshots, Full Integration mode)
- Basic authentication is not supported for SSO users in HyperFlex

#### Dell VNX, VNX2, VNXe, Unity and Unity XT

- NFS, Fibre Channel (FC), or iSCSI connectivity for VMware and Veeam Agent integrations
- Dell VNX/VNX2 all OE versions are supported
- Dell VNXe OE versions 3.x
- Dell Unity XT/Unity OE versions 5.0 up to 5.3

#### Dell PowerScale (formerly Isilon)

- Filer integration for NAS backup functionality
- NFS or SMB (CIFS) connectivity for NAS integration
- OneFS versions 8.1.2 to 9.5

#### Fujitsu ETERNUS HX/AX

- NFS, Fibre Channel (FC), or iSCSI connectivity for VMware and Veeam Agent integrations
- NFS or SMB (CIFS) connectivity for NAS integration
- ONTAP 7-mode versions 8.2 up to 8.2.5
- ONTAP cluster-mode versions 9.1 to 9.13.1
- MetroCluster is supported
- Application-aware data management and SVM-DR ONTAP features are not supported
- Synchronous SnapMirror is not supported

#### HPE 3PAR StoreServ

- Fibre Channel (FC) or iSCSI connectivity for VMware and Veeam Agent integrations
- 3PAR OS versions 3.2.2 to 3.3.2
- WSAPI 1.5 and later
- iSCSI VLAN tags are supported
- Virtual Domains are supported

## HPE Primera

- Fibre Channel (FC) or iSCSI (starting from OS versions 4.3 or later) connectivity for VMware and Veeam Agent integrations
- OS versions 4.x
- Virtual Domains are supported

## HPE Alletra 9000

- Fibre Channel (FC) or iSCSI connectivity for VMware and Veeam Agent integrations
- OS version 9.3 or later
- Virtual Domains are supported

## HPE Alletra MP

- Fibre Channel (FC) connectivity for VMware and Veeam Agent integrations
- OS version 10.2 or later
- Virtual Domains are supported

## HPE Nimble Storage AF-Series, HF-Series and CS-Series

- Fibre Channel (FC) or iSCSI connectivity for VMware and Veeam Agent integrations
- Nimble OS from 5.0 up to 6.1.2

## HPE Alletra 5000/6000

- Fibre Channel (FC) or iSCSI connectivity for VMware and Veeam Agent integrations
- OS version 6.0

## HPE StoreVirtual (formerly LeftHand / P4000 series) and StoreVirtual VSA

- iSCSI connectivity for VMware and Veeam Agent integrations
- LeftHand OS versions 9.5 to 12.8
- HPE SV3200 (LeftHand OS version 13) is not supported

## IBM FlashSystem (formerly Spectrum Virtualize, includes IBM Storwize and IBM SVC)

- Fibre Channel (FC) or iSCSI connectivity for VMware and Veeam Agent integrations
- Spectrum Virtualize from version 8.2 or later
- Policy-based replication is not supported

## IBM N Series

- NFS, Fibre Channel (FC), or iSCSI connectivity for VMware and Veeam Agent integrations

- ONTAP 7-mode versions 8.2 up to 8.2.5
- ONTAP cluster-mode versions 9.1 to 9.13.1
- MetroCluster is supported
- Application-aware data management and SVM-DR ONTAP features are not supported
- Synchronous SnapMirror is not supported

## Lenovo DM Series

- NFS, Fibre Channel (FC), or iSCSI connectivity for VMware and Veeam Agent integrations
- NFS or SMB (CIFS) connectivity for NAS integration
- ONTAP 7-mode versions 8.2 up to 8.2.5
- ONTAP cluster-mode versions 9.1 to 9.13.1
- MetroCluster is supported
- Application-aware data management and SVM-DR ONTAP features are not supported
- Synchronous SnapMirror is not supported

## Lenovo Storage V series

- Fibre Channel (FC) or iSCSI connectivity for VMware and Veeam Agent integrations
- Spectrum Virtualize 8.2 or later
- Policy-based replication is not supported

## NetApp FAS/AFF/ASA, FlexArray (V-Series), ONTAP Edge/Select/Cloud VSA

- NFS, Fibre Channel (FC), or iSCSI connectivity for VMware and Veeam Agent integrations
- NFS or SMB (CIFS) connectivity for NAS integration
- ONTAP 7-mode versions 8.2 up to 8.2.5
- ONTAP cluster-mode versions from 9.1 up to 9.13.1
- MetroCluster is supported
- Application-aware data management and SVM-DR ONTAP features are not supported
- NetApp Synchronous SnapMirror is not supported

## Nutanix Files

- Filer integration for NAS backup functionality
- NFS or SMB (CIFS) connectivity for NAS integration
- Nutanix File Server 3.8.1.3 to 4.2.0

## Universal Storage API Integrated Systems

### DataCore SANsymphony

- Fibre Channel (FC) or iSCSI connectivity for VMware and Veeam Agent integrations
- DataCore SANsymphony 10.0 PSP12 or later

## Dell PowerMax

- Fibre Channel (FC) or iSCSI connectivity for VMware and Veeam Agent integrations
- Dell PowerMax/VMAX All Flash (PowerMax OS microcode family 5978 or later)
- Unisphere for PowerMax 9.2.1.6 or later

## Dell PowerStore

- Fibre Channel (FC) or iSCSI connectivity for VMware and Veeam Agent integrations
- Dell PowerStore T and PowerStore X series (PowerStore OS 3.x or later)

## Dell SC Series (formerly Compellent)

- Fibre Channel (FC) or iSCSI connectivity for VMware and Veeam Agent integrations
- Storage Center OS 7.4.2 or later
- FluidFS and Live Volumes are not supported

## Fujitsu ETERNUS AF and DX series

- Fibre Channel (FC) or iSCSI connectivity for VMware and Veeam Agent integrations
- ETERNUS AF series: AF250 S2, AF650 S2, AF150 S3, AF250 S3, AF650 S3
- ETERNUS DX series: DX60 S4, DX100 S4, DX200 S4, DX500 S4, DX600 S4, DX8900 S4, DX60 S5, DX100 S5, DX200 S5, DX500 S5, DX600 S5, DX900 S5
- Software version:
  - ETERNUS AF S2 and DX S4 series (except DX8900 S4): V10L88-1000 or later
  - ETERNUS AF S3 and DX S5 series, DX8900 S4: V11L30-5000 or later

## Hitachi VSP

- Fibre Channel (FC) or iSCSI connectivity for VMware and Veeam Agent integrations
- VSP E series (93-03-01-60/00 or later)
- VSP F series (88-07-01-x0/00 or later)
- VSP G series (88-07-01-x0/00 or later)
- VSP 5100 and VSP 5500 (90-05-01-00/00 or later)
- VSP 5200 and VSP 5600 (90-08-01-00/00 or later)

## HPE XP

- Fibre Channel (FC) connectivity for VMware and Veeam Agent integrations
- HPE XP8 (90-05-01-00/00 or later)

## INFINIDAT InfiniBox F-series

- NFS, Fibre Channel (FC), or iSCSI connectivity for VMware and Veeam Agent integrations
- InfiniBox version 5.0 and later

## NEC Storage M Series

- Fibre Channel (FC) or iSCSI connectivity for VMware and Veeam Agent integrations
- M120, M320, M320F, M520, M720, M720F (Storage Control Software revision 1234 or later)

## NEC Storage V Series

- Fibre Channel (FC) or iSCSI connectivity for VMware and Veeam Agent integrations
- V100, V300 (93-04-21-XX or later), V10e (88-08-09-XX or later)

## NetApp SolidFire/HCI

- iSCSI connectivity for VMware and Veeam Agent integrations
- Element OS version 10.0 or later

## Pure Storage FlashArray

- Fibre Channel (FC) or iSCSI connectivity for VMware and Veeam Agent integrations
- Purity version 4.10 or later

## Tintri IntelliFlash (formerly Western Digital IntelliFlash, Tegile)

- NFS, Fibre Channel (FC), or iSCSI connectivity for VMware and Veeam Agent integrations
- Tintri IntelliFlash 3.11 or later

## Veeam Explorer for Microsoft Active Directory

### Microsoft Active Directory Domain Controllers

- Microsoft Windows Server 2022
- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2008

The minimum supported domain and forest functional level is Windows 2008.

## Veeam Explorer for Microsoft Exchange

### Microsoft Exchange

- Microsoft Exchange 2019
- Microsoft Exchange 2016
- Microsoft Exchange 2013

### Software

- Microsoft Outlook for PST exports (optional)

## Veeam Explorer for Microsoft SharePoint

### Microsoft SharePoint Server

- Microsoft SharePoint Server Subscription Edition
- Microsoft SharePoint 2019
- Microsoft SharePoint 2016
- Microsoft SharePoint 2013

The 3rd-party RBS providers are not supported.

## Veeam Explorer for Microsoft SQL Server

### Microsoft SQL Server

- Microsoft SQL Server 2022
- Microsoft SQL Server 2019
- Microsoft SQL Server 2017
- Microsoft SQL Server 2016
- Microsoft SQL Server 2014
- Microsoft SQL Server 2012
- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2008

## Veeam Explorer for Oracle

### OS

Both 32-bit and 64-bit versions of the following operating systems are supported for the database server, according to the Oracle Database version compatibility matrix:

- Microsoft Windows Server 2022
- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2008
- CentOS 5 or later
- RedHat 5 or later
- Oracle Linux 5 or later
- SUSE Linux Enterprise 15
- SUSE Linux Enterprise 12
- SUSE Linux Enterprise 11

### Oracle Database

- Oracle 21
- Oracle 19
- Oracle 18
- Oracle 12
- Oracle 11

### Configuration

- Oracle Automatic Storage Management (optional, requires ASMLib present)

## Veeam Explorer for PostgreSQL

### PostgreSQL

- PostgreSQL 16
- PostgreSQL 15
- PostgreSQL 14
- PostgreSQL 13
- PostgreSQL 12

# Known Issues and Limitations

## Backup infrastructure

- All registered server names must be resolvable into IPv4 or IPv6 addresses.
- Storage infrastructure is rescanned every 10 minutes. Perform the "Rescan Storage" operation manually after storage infrastructure changes. Otherwise, Veeam may not "see" newly added volumes immediately.
- All sensitive information, such as user credentials or encryption keys, is stored in the configuration database encrypted with a machine-specific private key of the backup server. Accordingly, a newly installed backup server cannot decrypt such information if attached to the existing database, so any encrypted information must be supplied manually. To work around this, use the configuration backup and restore functionality for backup server migrations.
- The length of the VM virtual disk file and configuration file names must not exceed 128 symbols.
- A backup proxy cannot transfer a backup to an SMB-based repository when the share is located on the same server as the proxy. To work around this, create a Windows-based backup repository on the proxy server instead.
- Backup jobs containing VMs with non-Latin characters in the name and Quantum DXi, Fujitsu ETERNUS CS800, or Infinidat InfiniGuard as a backup repository fail with an SSH error.

## VMware

- Replication of encrypted VMs with datasets is not supported for vSphere v8
- On ESXi 7.0 and above, the replica failback operation forces digest recalculation for both source and target VMs. The quick rollback option will be ignored.
- Debian and Ubuntu-based Linux backup proxies require that DNS names of vCenter Server and ESXi hosts are resolvable from the proxy server. Otherwise, jobs will fail with the "NFC storage connection is unavailable" error.
- Linux-based backup proxies do not support the processing of VMs with virtual disks without ddb.uuid unique IDs in the hot add mode. Normally, such disks may only be created by specific P2V/V2V conversion tools.
- DirectSAN backup mode: Multipathing (MPIO) for Linux-based backup proxies leverages only path failovers and not load balancing. These are limitations of the VMware VDDK, and the distributions supported for MPIO in DirectSAN are listed in the Virtual Disk Development Kit release notes corresponding to your vSphere version.
- Processing virtual disks with the @ symbol in the disk name is not supported by proxies in VMware VDDK-based transport modes.
- NSX-T networking is not supported for Veeam Cloud Connect Replication.
- NSX networking mapping is not supported during Instant Recovery.
- A virtual backup proxy server cannot be used to back up, replicate, or copy itself in the virtual appliance (hot add) mode. Jobs configured to do this will automatically failover to the Network processing mode. CBT will be disabled for proxy VMs.
- Virtual Windows-based backup proxy must have VMware Tools installed; otherwise, it will be considered as not running and will never be assigned any tasks.
- VMware vStorage API for Data Protection has limitations preventing the hot add process depending on VM configuration. For a complete list of hot add limitations, refer to [KB1054](#). With the default proxy



settings, should the hot add operation fail, the job will switch to the network mode for a specific virtual disk.

- Hard Disk restore may fail with the "*Restore job failed Error: A specified parameter was not correct: unitNumber*" error when restoring the disk to an SCSI controller slot above 15. To work around this, add a paravirtual SCSI controller to the target VM by editing VM virtual hardware settings with vSphere Client.
- Disk mapping functionality is not supported for IDE, SATA, and NVMe disks in the Hard Disk Restore wizard.
- Restoring and replicating VMs between different ESXi versions requires the VMs' virtual hardware version to be compatible with the target host.
- Restoring VM with non-standard virtual disk layout (such as converted from VMware Workstation or VMware Server) as thin may fail. To work around this issue, restore these disks as thick.
- Instant recovery of non-VMware Linux machines to VMware is not supported for backups of machines with mkinitrd missing or with mount points outside of /
- Virtual disk placement and type cannot be customized during full VM restore when restoring backups produced by version earlier than 6.1.
- Replication jobs may fail if the source or target datastore has special symbols in its name.
- Networkless interaction with Microsoft Windows guests having UAC enabled requires that the Local Administrator (MACHINE\Administrator) or Domain Administrator (DOMAIN\Administrator) account is provided on the Guest Processing step.
- Guest customization settings are not backed up and restored for vCloud Director VMs.
- The state of the Standalone VM option of vCloud Director is not preserved with the full VM restore.
- Virtual appliance (hot add) processing mode does not support IDE disks. This is by the design of the VMware hot add functionality, which requires SCSI or SATA adaptors (SATA hot add support requires vSphere 6 or later).
- Direct NFS Access is not supported for VMs with existing snapshots when VMware quiescence is enabled.
- Due to a change in ESXi 6.0 Update 1, replication and quick migration to VVol datastores are not possible with either Veeam or vSphere replication.
- RDM disks in virtual compatibility mode are skipped during Backup from Storage Snapshot.
- Pre-freeze and post-thaw scripts for Linux do not perform elevation to root (sudo) when networkless processing (VIX) is used.
- The entire VM restore to the original location does not preserve disk IOPs limits, erroneously removing the associated records from the VMX file. However, restoring to another location will keep these parameters.
- Encryption storage policy is not supported for the instant recovery to First Class Disk (FCD).

## VMware Cloud on AWS

- Only the hot add transport mode is supported due to API limitations.
- All vPower NFS-based functionality is not supported due to platform limitations.
- Networkless guest interaction is not supported due to API limitations.
- Re-IP addressing and file-level recovery for replicas are not supported.
- Only the cold switch is supported for Quick Migration.

## CDP

- In case of any environmental issues, deploying the I/O filter will fail with the "*Operation is not allowed in the current state*" error returned by the VMware vSphere VIB deployment framework. In most cases, the reason is a DNS issue. Other possible reasons include infrastructure issues such as an expired vCenter EAM certificate.
- CDP policy cannot be created or started with the "*veecdp@REPLICATION was not found*" error in case some storage providers are offline. To fix the issue, refer to VMware [KB76633](#).
- Following the ESXi host update from vSphere 6.x to 7.0, the CDP replica rescan fails with the "*Failed to rescan CDP replicas*" error. To solve the issue, open a support ticket and request updated CDP components (that have been certified by VMware after the Veeam Backup & Replication 12 GA release).
- I/O filter cannot be attached to VMs with snapshots. Remove all snapshots from VMs to be protected before creating a CDP policy.
- Using a vCenter Server as a CDP proxy is not supported and may cause various issues.
- Setup programs of specific primary storage integration plug-ins leave the CDP service stopped after the installation. Please verify the service state following the installation and start it manually if needed.
- Windows Server 2012 is not supported for the Veeam CDP due to incompatibility with the FIPS-certified version of OpenSSL. To use this functionality, disable FIPS-compliant operations in the Security options of the backup server or upgrade your backup server and CDP proxies to Windows Server 2012 R2 or later.

## Hyper-V 2016/2022

- The Hyper-V 2022 host forces the VM configuration version to be updated from 5.0 to 8.0.
- Restoring VMs, which were backed up from Hyper-V 2012R2 (or later) hosts in the crash-consistent state, to the Hyper-V 2022 host fails with the "*Writer 'Microsoft Hyper-V VSS Writer' is failed at 'VSS\_WS\_FAILED\_AT\_POST\_RESTORE'*" error due to a bug in Hyper-V.
- Application-aware processing of VMs with Windows guest OS other than Windows Server 2016 and Windows 10 fails with the "*Failed to take in-guest VSS snapshot COM error: Code: 0x80042308*" error. This known Hyper-V 2016 compatibility issue is fixed by updating Hyper-V integration components on the affected guests with [KB3063109](#).
- Application-aware processing of Active Directory domain controllers running on a guest OS other than Windows Server 2016 fails with the "*Failed to create VM recovery checkpoint*" error (32770). To resolve this issue, ensure the latest Windows Updates are installed for the guest OS on the affected VMs.
- Backing up VMs from the Hyper-V cluster in the rolling upgrade is supported. However, RCT will not be leveraged until the upgrade is completed for all nodes and the cluster functional level is upgraded to Windows Server 2016 or later. Note that the VM virtual hardware version must be upgraded to version 8.0 before RCT can be leveraged on the VM.
- Virtual machines with VMPmemController virtual hardware are skipped from processing due to a Hyper-V limitation around checkpointing of such VMs. Additionally, such machines may cause restore operations to the same Hyper-V host to hang on Hyper-V 2016 versions earlier than the 1803 SAC release due to a Microsoft Hyper-V VSS Writer bug.
- VMs with pass-through virtual disks cannot be processed due to limitations in Hyper-V 2016 and later checkpoints.

## Hyper-V

- Virtual disks consisting of multiple files (such as from virtual machines originally created on Virtual Server 2005) are not supported for processing.
- CPU Type SCVMM parameter is not backed up and restored on Hyper-V VMs.
- Backup of VMs with virtual disks located both on local and shared CSV/SMB storage is not supported due to Hyper-V limitation.
- Off-host backup from deduplicated volume fails if the Data Deduplication feature is disabled on the backup proxy server.
- Shared VHDX virtual disks can be backed up in crash-consistent mode only.
- Transaction log backup for Microsoft SQL Cluster running on shared VHDX is not supported due to a Microsoft limitation (no VSS support for Shared VHDX).
- Restoring a VM into the root folder of SMB share fails. To work around the issue, restore the VM into a subfolder instead.
- Off-host backup of a VM with Shared Virtual Hard Disks is not supported.

## Scale-Out Backup Repository

- Rebalancing the Scale-Out Backup Repository with the Performance Tier comprising immutable or object storage repositories is not supported. The first run of SOBR rebalancing may skip Microsoft SQL log backups and the related image-level backups. These backups will be relocated on the next run.

## NAS Backup

- When files are backed up directly from the Windows server, NTFS sparse files are handled as regular files, and thus are inflated during the restore.
- When files are backed up directly from Linux servers, the maximum full file path length is limited to 4096.
- Symlinks within Linux-based SMB shares are not supported and prevent the backup jobs from executing correctly.
- Force removal of SOBR extent (without backup evacuation) requires running the health check on impacted backups twice: after removing the extent and after running the backup job for the first time.
- Backing up NFS 4.1 root server with multiple file shares located on different file systems may lead to the NAS backup job failing or the ACL being lost or corrupted.

## Object Storage Backup

- Restoring object storage backups to an object storage system other than the one they were taken from is only supported when the target system correctly implements all API calls from the S3 standard, as leveraging required S3 API calls that are incorrectly or incompletely implemented may lead to unexpected results including the data loss.
- It is not possible to restore bucket or container content to its original location whenever the original bucket has been completely removed from the account. Use the restore to a new bucket option as a workaround.

## Agent Management

- Universal and Domain local groups are not supported as containers for Microsoft Active Directory-based protection groups. Use Global groups instead.
- The processing rate for agent backup jobs may show incorrect values (much higher than actual).

- Password loss protection is not supported for agents backing up data to an object storage repository.

## Microsoft Windows Server Failover Cluster

- Workgroup clusters, multi-domain clusters, and mixed OS version clusters are not supported for agent-based backup.
- Only failover clusters with shared disks are supported. CSV (Cluster Shared Volume) based disks are not supported for agent-based backup.
- SQL Server AlwaysON Clusterless Availability Groups and Availability Groups based on multiple SQL Server Failover Clusters are not supported for agent-based backup.
- NetBIOS and DNS names for all failover cluster nodes must be resolvable from the backup server.
- Failover clusters with the same NetBIOS names are not supported even when joined in different domains.
- Adding a new node into the failover cluster will result in a full backup performed for all shared disks.
- Bare Metal Recovery restore is not supported for shared disks. Such disks will be filtered out and not displayed in the corresponding wizard. To restore the content of such disks, use volume-level recovery or disk export functionality.
- Instant Recovery automatically skips clustered volumes during recovery.

## Direct Restore to Amazon EC2

- Direct restore of disks larger than 5TB requires using a proxy appliance; otherwise, restore will fail with the "*Object is too large*" error.
- Restore of AWS-native VMs (originating from AWS) with boot type UEFI can have the wrong boot type and may not boot properly. To restore a machine, use the AmazonDefaultWindowsImage registry key with specifying AMI, which will support the EFI boot type.

## Direct Restore to Microsoft Azure and Azure Stack Hub

- Specific Linux computer configurations may require Azure VM configuration to be adjusted upon the restore to Microsoft Azure. If your VM fails to boot, contact Veeam Support for assistance.
- The VM name, VM group name, and VM size are not validated for compatibility with the Microsoft Azure naming policy and storage account type and may cause the restore to fail.
- Microsoft Azure Stack subscription limits are not validated before the restore.

## Secure Restore

- Microsoft Windows Defender does not support the Secure Restore option to stop antivirus scanning after the first virus has been found, so the entire volume will always be scanned.

## Windows File Level Restore

- File-level restore may fail if a VM you are restoring from lacks free disk space at the time of backup.
- Storage Spaces volumes are not supported for file-level recovery. Consider using Instant VM Recovery to recover guest files from such VMs. Note that Microsoft does not support Storage Spaces within a VM.
- To restore files from deduplicated volumes, ensure the mount server and backup console are installed on Windows Server with the Data Deduplication feature enabled and the Windows Server version is the same or greater than the version of the VM you are restoring from. Otherwise, the deduplication driver incompatibility will cause file-level recovery errors with false data corruption reports.
- Compare with production always shows C:\Windows\System32\config and its content as deleted.

- CopyTo operation cannot be canceled in the remote mount server case.

## Multi-OS File-Level Restore with Mount Host

- The mount host kernel must support the source file system from the backup. Otherwise, the mount operation may result in kernel panic in some cases.
- LVM snapshots are not supported.
- For restores from the ZFS pool, the mount server kernel must support ZFS and have the zpool tool installed.
- Restore from BTRFS volumes is only possible with the mount host that is not the original host because there cannot be multiple BTRFS volumes with the same UUID attached to the same host.

## Multi-OS File-Level Restore with Helper Appliance

- Legacy Logical Volume Manager version 1 (LVM1) volumes are not supported.
- Encrypted LVM volumes are not supported.
- Spanned, striped, mirrored, and RAID-5 Windows dynamic disks are not supported. To work around the issue, use Windows File Level Restore instead.
- Non-standard file system configuration support is limited (for example, configurations where the file system journal is located on another volume, separately from the actual file system, are only supported for the ext3 file system, but not for other file systems).
- Restoring files to the original location for Windows VMs is not supported. To work around this, use Windows FLR instead.

## Guest File System Indexing

- File ownership data is not collected for files on non-NTFS volumes.
- File ownership data is not collected for guest files of Hyper-V VMs.
- Indexes cannot be published if there are locales or Unicode characters in the file system path.

## Replica Failover

- Starting a replicated VM using means other than the product user interface (including vSphere Client, Hyper-V Manager, SCVMM, and PowerShell) disables the advanced replication functionality such as Re-IP and failback.

## Configuration Backup and Restore

- Under certain circumstances, some encrypted backups may get disconnected from the corresponding job and appear as Imported. To work around the issue, use the backup mapping functionality to reconnect the job to the backup files.
- Immediately after the configuration restore, Enterprise Manager may show duplicate jobs, and some jobs may be missing. The issue will go away by itself after some time.

## Enterprise Manager

- NETBIOS names of backup servers must be resolvable on the Enterprise Manager server.
- Reverse DNS lookup on the Enterprise Manager server must be functional for setting up the self-service recovery delegation scope.
- The .NET 3.5.1 WCF HTTP Activation Windows component prevents Enterprise Manager from functioning. To work around the issue, uninstall this component.

- The self-service configuration dialog does not display correctly in Microsoft Internet Explorer 11. To work around the issue, use another supported browser.

## SureBackup

- The automatic virtual lab configuration is not supported for networks with non-private network addresses.
- The automatic virtual lab networking configuration process may fail with the "*Unable to resolve default network settings*" error. To work around the issue, return to the wizard and try again.
- The automatic virtual lab networking configuration may sometimes fail when DVS are present in the virtual environment. In such cases, use the advanced configuration mode to manually set up the virtual lab networking.
- SureBackup job fails on VM with unsupported or excluded virtual disks that were not explicitly set to be removed from configuration (as a part of disk exclusion settings in the backup job) because the test VM cannot find its disks and cannot start.
- Automatic physical mode RDM disk exclusion in the backup job may lead to a situation where the test VM can connect to the RDM disk and make irreversible changes on the disk. To avoid this, always explicitly exclude the physical RDM disk from the backup job, selecting the option to remove the excluded disks from the configuration.
- Some antivirus applications are known to cause BSOD on the backup repository server when the SureBackup job is started. To prevent this, exclude backup folders from monitoring.

## Cloud Connect Backup

- Microsoft SQL Server, Oracle, and PostgreSQL transaction log backup to a cloud repository is not supported. However, Backup Copy jobs in the immediate copy mode are supported for copying transaction logs backups to a cloud repository.

## Cloud Connect Replication

- Cloud replica status is not refreshed in real-time, but rather periodically. You can press F5 to retrieve the most current state.
- vApp-level networks are not supported for the network mapping functionality (only org-level networks).
- For non-Windows VMs, guest network settings cannot be detected automatically. Because of that, network mapping in the replication job wizard must be performed manually. Additionally, if you are replicating non-Windows VMs only, you need to manually specify the default gateways for each production network by using the Manage Default Gateways dialog on the Service providers node of the Backup infrastructure tab of the management tree.
- Network extension functionality requires static IP addresses assigned to the processed VMs. Dynamic IP addressing via DHCP is not supported, and DHCP must be disabled.
- The failover plan session cannot be viewed once the failover has been performed.
- Enabling VM auto-import in vCloud Director settings may impact replication functionality.
- Using the move functionality of vCloud Director to move cloud replicas may cause virtual disk loss.
- The Remote Console and Remote Desktop features are not supported for vCloud Director-based tenants.
- If a cloud provider renames the Virtual Switch in Hyper-V and updates the Hardware plan, network mapping will stop working for this Hardware plan. The replicas will be in the "Not connected" status, and failover will not work.

- Tenants' CDP failover plans are not visible in the Cloud Connect Self-Service portal.

## Backup Copy

- Backup copy jobs no longer support selecting workloads from backup copies or "from infrastructure."
- In the immediate copy mode, the backup copy job processes only the latest backup files chain. To make such jobs copy all existing backups, create BackupCopyMirrorAll (REG\_MULTI\_SZ) registry value under the *HKLM\SOFTWARE\Veeam\Veeam Backup and Replication* key on the backup server. This value should be populated with Backup Copy job names.
- The backup copy job with the vCloud Director workload may fail to start the backup over the WAN accelerator to a backup repository with a gateway server.
- Legacy backup copy job pointed to a Scale-out repository may fail to start the scheduled health check activity.
- A synthetic full backup is not created according to the backup copy job schedule for vCloud Director workloads if the primary backup job did not create any restore points for the same date.

## Object Storage

- For Backup from Object Storage, backup and restore to different object storage systems and software versions are only supported when all API calls from the AWS S3 standard are supported. Not following this requirement can lead to unexpected situations, including data loss.
- Not all Amazon and Azure regions may provide cold object storage tiers used by the SOBR Archive Tier and compute resources required to provision proxy appliances for data archival. Pay attention to this when selecting the cloud region to use.
- Using the immutability feature with the existing S3 bucket containing backups created with Veeam Backup & Replication 9.5 Update 4 requires that both Versioning and Object Lock are enabled on the bucket simultaneously before the immutability feature is enabled. Any other approach will lead to backup offload failures and the inability to interact correctly with backups in the bucket.
- Data in an object storage bucket/container must be managed solely by Veeam, including retention and data management. Enabling lifecycle rules is not supported and may result in backup and restore failures.

## Tape

- Source backup chain upgrade for VM backups will cause Backup to Tape to process the upgraded chain from scratch to ensure the data and metadata consistency on the tape media.
- File to Tape job fails to build a list of files to process if the catalog contains files with certain Unicode symbols.
- Backup to Tape job will perform a full backup during each run if the source forever forward incremental backup job or backup copy job in the immediate copy mode has a retention of less than 3 restore points or if the source backup copy job in the periodic copy mode has a retention of less than 4 restore points.
- SQL, PostgreSQL, and Oracle transaction log backup to tape are not supported.
- If you manage several tape libraries with the same Veeam backup server and use barcodes to identify tapes in these libraries, all barcodes must be unique across all tape libraries.
- Incorrect restore options might be displayed for NDMP backups on tape and NAS backups on tape when right-clicking the backup under the Home > Backups > Tape node. Use the File node as a workaround.
- Total values in the GFS tape job email report summary are incorrect. Use the details from the email report body to get the correct Read, Transferred, and Size values.

- Backing up NFS 4.1 root server with multiple file shares located on different file systems may lead to the file to tape job failing or the ACL being lost or corrupted.

## Application Plug-ins

- After migrating the Veeam configuration (using .bco file) and upgrading to version 12.1, restore from application plug-in backups that reside on the Capacity Tier or download of these backups fails. Contact Veeam Technical Support to get a workaround.

## K10 Integration

- Manually exported K10 backups fail to import to Veeam Backup & Replication with the "*Object reference not set to an instance of an object*" error.

## Veeam Explorer for Microsoft Exchange

- Restoring public folder items from the system "In-Place Hold Items" folder to the original location restores them to the newly created folder with the same name instead of the actual system folder.

## Veeam Explorer for Oracle

- Instant recovery of the entire Oracle Data Guard is not supported. However, you can restore individual databases.
- The database restore for Oracle Data Guard with tnsnames.ora and listener.ora located in non-default paths is not supported.
- The database export functionality may fail for databases larger than 1TB in size due to the SSH command limit. If you have such databases in your environment, contact Veeam Support to enable the workaround.
- The database restore may fail if the backed-up Oracle server version and the target server version have different patch levels.
- Oracle Real Application Clusters (RAC) and Oracle Data Guard deployments with snapshot standby option enabled are not supported with OCI-based integration. To work around this issue, use Veeam Plug-in for Oracle RMAN.
- Oracle XE on Linux is not supported.
- 32-bit Oracle application running on 64-bit operating systems is not supported.
- Configuration with multiple Oracle versions on the same machine is not supported.
- ASM-based Oracle deployments running in virtual machines with Open-VM-Tools installed are not supported.

## Veeam Explorer for Microsoft SharePoint

- Modified By field of restored documents is updated with the account performing the restore.
- Restored Issue list items are assigned new Issue IDs.
- Restore of Time Card list is not supported.
- Versioning settings of SharePoint lists are not preserved on restore.
- Restoring Generic List and Pages Library may fail with the "*No content type 'XXX' found in web YYY*" error.
- Importing Picture Library export may result in IDs being changed for some items.
- Importing Project Tasks list export does not preserve column order.
- Importing SharePoint list export does not preserve Validation Settings.



- Some Rating Settings of Discussion list values are not restored.

## Veeam Explorer for Microsoft SQL Server

- Instant database publishing to the SQL Server cluster requires a free drive letter on all cluster nodes according to the number of clustered disks in the backup. Instant database recovery requires twice the number of free drive letters.
- A point-in-time restore with fine-tuning requires all nodes of the same AlwaysOn availability group to be in the same time zone.
- Transaction log backup requires that at least one image-level backup of the SQL Server machine is performed. That means that transaction log backup will not function after the full SQL Server machine restore or for newly appearing databases until the next image-level backup is performed.
- Transaction log backups are not supported for Windows Server 2008 or earlier VMs on Hyper-V 2012 R2.
- SQL Server 2017 and later Graph Tables are not currently supported.

## Veeam Explorer for Storage Snapshots

- Multi-home restore is supported for snapshots created by jobs only, not the ones created during a rescan operation. For other storage snapshots, only disks residing on the same datastore with the VMX file will be available for all restore types.
- Data about VM NIC adapters is not collected during snapshot-only and backup from storage snapshot jobs with snapshot retention. This may result in SureBackup failure for VMs from those snapshots. Regular restores from such snapshots or restores from backups created by such jobs are not affected.

## NetApp ONTAP

- Infinite volumes are not supported.
- Target units of SVM DR/vFiler DR relationships are not supported and are automatically hidden by the UI.

## IBM FlashSystem

- Using IBM FlashSystem storage integration with the new volume snapshot technology may result in clone deletion warnings in the job session and empty volume groups left on the storage due to a very short timeout value. We recommend contacting Veeam Support for assistance with increasing the clone deletion timeout and cleaning up the volume groups.

## Globalization

- Non-ASCII characters are not supported in the product installation path. Some user interface (UI) controls may appear misplaced when a non-standard display DPI setting is set. To work around the issue, change the DPI setting to 100% or 125% using the Display settings of the Windows Control Panel.

## AI Assistant

- Windows Server 2012 is not supported for the Veeam AI Assistant. To use this functionality, your backup server and backup console must run on Windows Server 2012 R2 or later.

## User Interface

- If a NETBIOS domain name differs from a fully qualified domain name, the AD browser dialog will resolve the NETBIOS domain name incorrectly when new credentials are added. To work around the issue, fix credentials manually.

- Job filter functionality includes unmanaged Linux agent jobs under both Server and Workstation workload types.

## Enterprise Manager

- Instant Recovery to another location will fail with the "*Failed to prepare change storage*" error if the Redirect cache option is used.
- Restoring Oracle application items to another server from a Windows-based machine backup fails if the default logging level is enabled in Enterprise Manager. Contact Veeam Support to get the registry key for changing the logging level.

## PowerShell

- Restores from imported backups residing on an SMB (CIFS) share are not supported through PowerShell.

## Setup and Upgrade

- Windows Smart Screen may block the Veeam Backup & Replication ISO file, preventing it from mounting. To work around the issue, go to the ISO file properties, open the General tab, and unblock the file in the Security section.
- For Windows Server Hyper-V 2012 and Windows Server Hyper-V 2012 R2, the first job run after the upgrade will not use the changed block tracking information and thus may take longer than expected.
- After upgrading to Veeam Backup & Replication 12.1, jobs will automatically perform a full scan-based incremental run for machines with virtual disks formatted with NTFS with cluster sizes equal to or larger than 64KB.

# Installing Veeam Backup & Replication

## Veeam Backup & Replication Server

To install the Veeam Backup & Replication 12.1 server and management console:

1. Download the [latest ISO version](#) since it will have the latest available cumulative patch built in.
2. Mount the ISO and use autorun or the *Setup.exe* file. Click **Install** in the **Veeam Backup & Replication 12.1** splash screen.
3. Select the **Install Veeam Backup & Replication** option.
4. Accept the terms of Veeam Backup & Replication and 3<sup>rd</sup> party components license agreements to install the product. You can find a copy at [veeam.com/eula.html](http://veeam.com/eula.html)
5. Provide the setup program with your license file.
6. Review the default installation settings. To change the defaults, click **Customize Settings** and go through additional wizard steps.
7. Click **Install** to start the installation and follow the setup wizard steps.
8. Launch the backup console by clicking the **Veeam Backup & Replication** product icon on your desktop and specify localhost to connect to the local backup server.

## Veeam Backup Enterprise Manager

If you want to manage one or more Veeam Backup servers with a centralized management web UI, install Veeam Backup Enterprise Manager. You only need one Enterprise Manager installation per environment.

To install Veeam Backup Enterprise Manager:

1. Mount the ISO and use autorun or the *Setup.exe* file. Click **Install** in the **Veeam Backup & Replication 12.1** splash screen.
2. Select the **Install Veeam Backup Enterprise Manager** option.
3. Accept the terms of the License Agreement to install the product.
4. Provide the setup program with your license file.
5. Review the default installation settings. To change the defaults, click **Customize Settings** and go through additional wizard steps.
6. Click **Install** to start the installation and follow the setup wizard steps.
7. Once the installation is complete, access the Veeam Backup Enterprise Manager web UI by clicking the **Veeam Backup Enterprise Manager** product icon on your desktop.

## Uninstalling Veeam Backup & Replication

1. From the Start menu, select **Control Panel > Add or Remove Programs**.
2. In the programs list, select **Veeam Backup & Replication** and click the **Remove** button.
3. In the programs list, select and remove any additional remaining Veeam components.

# Upgrading Veeam Backup & Replication

Veeam Backup & Replication 12.1 supports an automated in-place upgrade from any version 11 build and from version 10a (build 10.0.1.4854), which preserves all product settings and configuration. To upgrade from earlier versions, contact our [Veeam Technical Support](#).

Use the following checklist to ensure your infrastructure is ready for the Veeam Backup & Replication upgrade. The built-in configuration check mechanism of the Veeam Backup & Replication Upgrade wizard performs some of the checks. Still, you can control them manually before starting the upgrade procedure.

## Licensing

1. Veeam Backup & Replication 12.1 uses the same license file format introduced with version 10, so you can use your existing version 10/11 license file to install version 12.1
2. Your support contract must be active as of the date when the product build you are installing was built. This is determined by the Support Expiration date in the installed license. If required, you can install a new license during the upgrade procedure.
3. Are you using Veeam Backup Starter? This edition has been discontinued, so Veeam Backup & Replication 12.1 will not accept such a license file. Please download a replacement license file from the [Customer Portal](#) before upgrading.

## System Requirements

1. Check if the backup server to be upgraded is installed on the supported operating system version according to [System Requirements](#). If it is not, create a configuration backup, install Veeam Backup & Replication 12.1 on the supported OS first, and then restore the configuration backup created earlier. To learn how to perform the migration, see the [Migrating Veeam Backup & Replication to Another Backup Server](#) section in the Veeam Backup & Replication User Guide.
2. Make sure that backup infrastructure components meet the system requirements listed in the [System Requirements](#) section of this document. In particular, ensure all backup infrastructure servers are based on 64-bit operating systems.
3. Ensure that the environment you will protect with Veeam Backup & Replication meets the requirements listed in the [System Requirements](#) section of this document.
4. Make sure that all necessary ports are open.
5. Make sure that all necessary permissions are granted.
6. Are you using a hardened repository? If yes, ensure that any Linux server associated with the hardened repository is configured to use a non-root account. For more information, see [this Veeam KB article](#).
7. Do you have any jobs using the **Transform previous backup chains into rollbacks** option? This option has been removed from the product, and such jobs are no longer supported. For more information, see [this Veeam KB article](#).
8. Are you using File to Tape jobs? Consider the following:
  - They have been re-engineered for scalability and are no longer free with Veeam Backup & Replication 12.1. You will have a grace period of 3 months following the upgrade to Veeam Backup & Replication 12.1, during which your existing jobs will not consume a license. For more information, see [Instance Consumption for Object Storage Backup, File Backup, and File to Tape Jobs](#).
  - File to tape jobs can now process Distributed File Systems (DFS) data.
9. Are you using installations of Veeam Backup & Replication and Veeam Backup for Microsoft 365 on the same machine? First upgrade Veeam Backup for Microsoft 365, second upgrade Veeam Backup &

Replication.

10. Are you using integration with Veeam Backup for Microsoft Azure? If yes, after upgrading to Veeam Backup & Replication 12.1, select the existing Microsoft Azure compute account in the Manage Cloud Credentials, click **Edit**, and go through the Microsoft Azure Compute Account wizard to update account permissions. Otherwise, you can face problems when adding an external repository with backups created by Veeam Backup for Microsoft Azure 6.0.
11. Are you using Server 2019-based ReFS backup repositories? If yes, avoid upgrading them to Server 2022 or mounting ReFS volumes from Server 2019 to new Server 2022 installations until you read [this thread](#) on Veeam R&D forums. Microsoft has addressed the known regression in the ReFS format upgrade code, and the fix is now publicly available.
12. Are you using Scale-Out Backup Repositories with immutable performance tier extents? Make sure that all extents have the same immutability settings.

### Integration with Veeam Management and Monitoring Products

1. Are you using **Veeam ONE** to monitor your backup infrastructure? If yes, upgrade it first. Veeam ONE supports monitoring of backup servers version 10a or later.
2. Are you using **Veeam Backup Enterprise Manager**? If yes, consider the following:
  - **Important!** Starting with Veeam Backup Enterprise Manager 12, a new port ([port 9405](#)) is used for certificate communication between Enterprise Manager and Veeam Backup & Replication. Ensure that your firewalls are configured to take into account this new port to avoid communication issues between Enterprise Manager and Veeam Backup & Replication.
  - Start the upgrade procedure with this component. Veeam Backup & Replication should be upgraded after that. If you have a backup server installed on the same machine, upgrade it immediately after completing the upgrade of the Veeam Backup Enterprise Manager server. Otherwise, the Veeam Configuration Database Connection Utility (DBConfig) utility will not work correctly for Veeam Backup & Replication.
  - From Veeam Backup Enterprise Manager, you cannot edit jobs managed by backup servers of earlier versions, as well as Veeam Agent backup jobs, file share backup jobs, and backup copy jobs. To edit the settings of such jobs, use the Veeam Backup & Replication console.
3. Are you using the **Veeam Backup Enterprise Manager** server added to **Veeam ONE**? If yes, first upgrade Veeam ONE, second upgrade Veeam Backup Enterprise Manager, and third upgrade Veeam Backup & Replication.
4. Are you using **Cloud Connect**? If yes, check with your Cloud Connect service provider if they have already upgraded their systems to at least the version you are upgrading to.
5. [For upgrade from Veeam Backup & Replication earlier than version 11a build 11.01.1261] Are you using Veeam Backup & Replication within the infrastructure of **Nutanix Mine** version 2.0.1 or earlier? If yes, upgrade Nutanix Mine to version 3.0 first, then upgrade Veeam Backup & Replication to version 12.1.
6. Are you using **Veeam Disaster Recovery Orchestrator**? If yes, note that Veeam Disaster Recovery Orchestrator 5.0 is compatible with Veeam Backup & Replication 11 and 11a, Veeam Disaster Recovery Orchestrator 6.0 – with Veeam Backup & Replication 11a and 12, Veeam Disaster Recovery Orchestrator 7.0 – with Veeam Backup & Replication 12 and 12.1. If necessary, upgrade Veeam Disaster Recovery Orchestrator before upgrading to Veeam Backup & Replication 12.1.

### Integration with Veeam Backup for Public Clouds

Are you using Veeam Backup & Replication integrated with Veeam Backup for Public Cloud solutions? The plugins of these products must be aligned with the version of the products. Do not upgrade to Veeam Backup &

Replication 12.1 until you install the matching plug-in versions for Veeam Backup for AWS (version 7), Microsoft Azure (version 6), and Google Cloud (version 5).

### Integration with Veeam Backup for Hypervisors

Are you using Veeam Backup & Replication integrated with Veeam Backup for Hypervisors?

- **Veeam Backup for Nutanix AHV:** the plug-in for version 5.1 of this product is included with the Veeam Backup & Replication 12 redistributable. During the upgrade to version 12.1, the plug-in will be automatically upgraded.
- **Veeam Backup for Red Hat Virtualization:** the plug-in for version 4 of this product is included with the Veeam Backup & Replication 12 redistributable. During the upgrade to version 12.1, the plug-in will be automatically upgraded to the required version.

### Integration with Veeam Backup Agents and Enterprise Plug-Ins

1. Are you using **Veeam Agents** managed via Veeam Backup & Replication?
  - If you use versions **Veeam Agent for Microsoft Windows** or **Veeam Agent for Linux 4.0**, they will stop working after upgrading to Veeam Backup & Replication 12.1. In this case, we recommend immediately upgrading **Veeam Agent for Microsoft Windows** or **Veeam Agent for Linux** to 6.1. If you use **Veeam Agent for Microsoft Windows** or **Veeam Agent for Linux 5.0** or later, they will continue working after upgrading to Veeam Backup & Replication 12.1, but new features implemented in Veeam Backup & Replication 12.1 will not be supported. In this case, you can upgrade **Veeam Agent for Microsoft Windows** or **Veeam Agent for Linux** to 6.1 later if the support of new features is not critical for you.  
**Note:** If you use a nosnap version of **Veeam Agent for Linux**, starting from Veeam Backup & Replication 12.1, you can manage such Veeam Agents through a protection group for pre-installed agents only.
  - If you use **Veeam Agent for Mac 1.0**, it will stop working after upgrading to Veeam Backup & Replication 12.1. In this case, we recommend immediately upgrading **Veeam Agent for Mac** to 2.1. If you use version 1.0.1 of the agent, it will continue working with Veeam Backup & Replication 12.1, but new features of Veeam Backup & Replication 12.1 will not be supported. We recommend upgrading the agent to version 2.1 at your earliest convenience.
  - If you use versions **Veeam Agent for IBM AIX** or **Veeam Agent for Oracle Solaris 3.0** or later, they will continue working after upgrading to Veeam Backup & Replication 12.1, but new features of Veeam Backup & Replication 12.1 will not be supported. In this case, you can upgrade **Veeam Agent for IBM AIX** or **Veeam Agent for Oracle Solaris** to 4.1 later if the support of new features is not critical for you.
2. Are you using **Veeam Plug-In for Oracle RMAN**, **Veeam Plug-In for SAP HANA**, **Veeam Plug-In for SAP on Oracle**, or **Veeam Plug-In for Microsoft SQL Server**? If yes, you upgrade Veeam Backup & Replication first, then you can upgrade Veeam Plug-ins.

### Integration with Storage Systems

1. Make sure your storage systems work on a supported operating system:
  - **Huawei:** storage arrays of this vendor are not supported for Veeam storage snapshot integration. Remove the storage arrays from the backup server configuration and use other backup transport modes instead.
  - **Cisco HyperFlex:** the minimum supported operating system version is v4.0(2x). Upgrade to it or remove the storage arrays from the backup server configuration.
  - **HPE 3PAR WSAPI:** the minimum supported WSAPI version is 1.5. Upgrade to it or remove the storage arrays from the backup server configuration.

- **HPE Nimble:** the minimum supported operating system version is 5.0. Upgrade to it or remove the storage arrays from the backup server configuration.
  - **Dell Data Domain:** the supported operating system version is 7.3 to 7.12. Upgrade to it, or the backup jobs pointed to this repository will fail to start.
  - **HPE StoreOnce:** the minimum supported operating system version is 3.18.18 for Gen3 and 4.2.3 for Gen4. Upgrade to it, or the backup jobs pointed to this repository will fail to start.
2. Select the secondary destination for IBM HyperSwap configurations explicitly in the backup job.

### Other Changes

1. Note that the last known time-based retention policy is now applied to backups belonging to disabled backup jobs and to orphaned backups. You can use the new Copy Backup functionality of Veeam Backup & Replication 12.1 to create a fully independent copy of the required backups, which will not be subject to the retention policy.
2. Veeam Backup & Replication 12 supports protecting NAS backups with Backup to Tape jobs. If you have entire repositories added as sources for backup to tape jobs, make sure these repositories contain only backups that you want to protect with backup to tape jobs.

### Upgrade Process

1. Make sure the latest run for all existing jobs has been completed successfully. Rerun any failed jobs.
2. Ensure there are no running jobs, restore sessions, Instant Recovery sessions, or SureBackup jobs. We recommend that you do not stop running jobs and let them complete successfully.
3. Disable any periodic and backup copy jobs temporarily to prevent them from starting during the upgrade.
4. Disable CDP policies. Otherwise, the CDP filter driver will not be upgraded.
5. Ensure there are no active tasks from standalone (unmanaged) agents.
6. Ensure there are no active Veeam Disaster Recovery Orchestrator tasks.
7. Perform the configuration backup, as described in [Running Configuration Backups Manually](#). Ensure you have configuration backup encryption enabled. Otherwise, stored credentials will not be included in it. For more information, see [Creating Encrypted Configuration Backups](#).

### Additional Considerations for Upgrade from Veeam Backup & Replication 10

Do you have backup copy jobs with synthetic GFS full backups? Before the upgrade, ensure that all GFS candidates (incremental restore points created on days when GFS was scheduled and expected to be transformed into full GFS restore points) are already transformed into GFS restore points. To force the backup copy job to transform all GFS candidates, you can temporarily decrease the short-term retention to a value less than the number of restore points between the latest restore point and the most recent GFS candidate and then wait till all the candidates are transformed.

Before Veeam Backup & Replication version 11, Veeam Backup & Replication created GFS candidates on days when GFS was scheduled and only then transformed them into full GFS restore points according to the short-term retention. For more information on how restore points were transformed, see [Synthetic Weekly Full Backups](#). Starting from Veeam Backup & Replication version 11, Veeam Backup & Replication creates GFS restore points according to a new schedule and creates them right on the scheduled days. For more information, see [Changes in GFS Retention](#). After the upgrade, Veeam Backup & Replication no longer transforms previous GFS candidates into full GFS restore points. This means that all GFS candidates lose their GFS status. They become regular incremental restore points and are deleted according to the short-term retention policy.

## Upgrading Veeam Backup Enterprise Manager

To upgrade Veeam Backup Enterprise Manager to version 12.1, you must run version 10a (build 10.0.1.4854) or later on the supported operating system (refer to the [System Requirements](#) section of this document). To upgrade from previous versions, contact [Veeam Technical Support](#).

1. Download the [latest ISO version](#) since it will have the latest available cumulative patch built in.
2. Perform a backup of the corresponding SQL Server configuration databases used by the Enterprise Manager server so that you can go back to the previous version in case of issues with the upgrade.
3. Mount the product ISO and use autorun or run the *Setup.exe* file. Click **Upgrade** in the **Veeam Backup & Replication 12.1** splash screen.
4. Select the **Upgrade Veeam Backup Enterprise Manager** option.
5. Follow the setup wizard steps as outlined in the installation procedure above. Be sure to select the same SQL database and instance used by the previous Veeam Backup Enterprise Manager version.
6. If you have the Veeam Backup & Replication server installed on the server, upgrade it immediately after completing the upgrade of the Veeam Backup Enterprise Manager server. Otherwise, this local backup server will not be able to run jobs.

Please note that immediately after the upgrade, Enterprise Manager performance may be impacted due to the configuration database being optimized by the maintenance job. This can take up to an hour, depending on the database size.



## Upgrading Veeam Backup & Replication Server

To upgrade the Veeam Backup & Replication server to version 12.1, you must run version 10a (build 10.0.1.4854) or later. To upgrade from previous versions, contact [Veeam Technical Support](#).

1. Download the [latest ISO version](#) since it will have the latest available cumulative patch built in.
2. Ensure there are no active processes, such as any running jobs and restore sessions. We recommend that you do not stop running jobs and let them complete successfully instead. Disable any periodic and Backup Copy jobs so that they do not start during the upgrade.
3. Perform a backup of the corresponding SQL Server configuration databases used by the backup server so that you can easily go back to the previous version in case of issues with the upgrade. You can also use the built-in configuration backup functionality.
4. Mount the product ISO and use autorun or run the *Setup.exe* file. Click **Upgrade** in the **Veeam Backup & Replication 12.1** splash screen.
5. Select the **Upgrade Veeam Backup & Replication** option.
6. Follow the upgrade wizard steps as outlined in the installation procedure above. Be sure to select the same SQL database and instance used by the previous product version.
7. If you use remote backup consoles, upgrade them manually using the product ISO file. Unfortunately, if you upgrade from versions earlier than 12 (build 12.1.0.2131), the automatic upgrade is not supported due to the major version number change.
8. Open the Veeam Backup & Replication user interface. If necessary, the automated upgrade wizard will automatically appear, prompting you to upgrade product components running on remote servers. Follow the wizard to complete the upgrade process.
9. If some remote servers are unavailable at the time of the upgrade, you can run the Upgrade wizard at any time later from the main product menu. Note that jobs cannot use out-of-date product components until updated to the backup server version.
10. If you are using the Virtual Labs functionality, please open the settings of each virtual lab and click through the wizard to redeploy each virtual lab with the new proxy appliance version.
11. If you use Linux servers for your backup infrastructure components, the upgrade process will automatically deploy the new persistent data mover only to Linux servers with the VMware Backup Proxy role. To deploy it on other Linux servers, click through the Linux server properties or use the Set-VBRLinux PowerShell cmdlet to mass-deploy. Until you do this, those Linux servers will continue using the legacy runtime data mover to avoid issues with the backup repository not meeting the persistent data mover requirements.
12. Enable any scheduled jobs that you have disabled before the upgrade.

Please note that immediately after the upgrade, backup server performance may be impacted due to the configuration database being optimized by the maintenance job. This can take up to an hour, depending on the database size.

# Licensing

Veeam Backup & Replication can be licensed per protected workload with Veeam Universal License (VUL) or per CPU Socket of the underlying hypervisor host (for vSphere or Hyper-V VMs protection only). For more information, see Veeam Licensing Policy at [veeam.com/licensing-policy.html](https://www.veeam.com/licensing-policy.html)

The trial license key is sent to you automatically after downloading the product. The trial license is valid for 30 days from that moment and includes Basic technical support.

To obtain a full license key, please refer to [veeam.com/buy-veeam-products-pricing.html](https://www.veeam.com/buy-veeam-products-pricing.html)

Subscription VUL and Perpetual VUL licenses include a maintenance plan with Premium support. Perpetual Socket license includes a one-year maintenance plan with Basic support. To renew or upgrade your maintenance plan, contact Veeam Renewals at [veeam.com/renewal.html](https://www.veeam.com/renewal.html)

## Updating Veeam Backup & Replication License

The Veeam Backup & Replication server license is managed centrally by the Enterprise Manager server. If you are using Enterprise Manager, do not update the license on individual backup servers directly, as Enterprise Manager will force its license to all connected backup servers.

To install the new license file to a backup server connected to the Enterprise Manager server:

1. Open the **Configuration > Licensing** tab in Enterprise Manager UI, and click **Install License**.
2. Browse to the license file (.lic) sent to you after registration to install the license. To learn more, see the Licensing section.
3. The provided license file will be automatically propagated and applied to all Veeam Backup servers connected to this Enterprise Manager server.

To install the new license file to a standalone backup server that is not managed by the Enterprise Manager server:

1. Select License from the main menu.
2. Click the Install license button to browse to the license file (.lic) sent to you after registration to install the license. To learn more, see the Licensing section.

# Technical Documentation References

If you have any questions about Veeam Backup & Replication, you may use the following resources:

- Product web page: [www.veeam.com/vm-backup-recovery-replication-software.html](http://www.veeam.com/vm-backup-recovery-replication-software.html)
- User guides: [www.veeam.com/documentation-guides-datasheets.html](http://www.veeam.com/documentation-guides-datasheets.html)
- Community forums: [www.veeam.com/forums](http://www.veeam.com/forums)

To view the product help, press the **F1** key or select **Help > Online Help** from the main menu.

## Technical Support

We offer email and phone technical support for customers with active maintenance agreements and during the official evaluation period. For a better experience, please provide the following when contacting our technical support:

- Version information for the product and all infrastructure components.
- Error message and/or accurate description of the problem you are having.
- Log files. To export the log files, select **Help > Support Information** from the main menu and follow the wizard to export the relevant set of log files.

To submit your support ticket or obtain additional information, please visit [veeam.com/support.html](http://veeam.com/support.html).

### TIP

Before contacting technical support, consider searching for a solution on Veeam R&D Forums at [veeam.com/forums](http://veeam.com/forums)

# Contacting Veeam Software

At Veeam Software, we pay close attention to comments from our customers – and make it our mission to listen to your input and build our products with your suggestions in mind. We encourage all customers to join Veeam R&D Forums at [veeam.com/forums](https://www.veeam.com/forums) and share their feedback directly with the R&D team.

Should you have a technical or licensing issue or question, contact our Customer Support organization directly. We have qualified technical and customer support staff available 24 hours a day, 7 days a week, who will help you with any inquiry that you may have.

## Customer Support

For the most up-to-date information about our support practices, business hours, and contact details, please visit [veeam.com/support.html](https://www.veeam.com/support.html). You can also use this page to submit a support ticket and download the support policy guide.

## Company Contacts

For the most up-to-date information about company contacts and office locations, please visit [veeam.com/contacts](https://www.veeam.com/contacts).