Veeam Backup & Replication 11a Release Notes

This document provides last-minute information about Veeam Backup & Replication 11a, including system requirements, installation and upgrade procedure, as well as relevant information on technical support, documentation, online resources and so on.

The release version of Veeam Backup & Replication 11a is available for download at veeam.com/backup-replication-download.html starting from March 12, 2022.

If you are upgrading to v11a from previous versions, please **review the upgrade checklist closely** before performing the upgrade.

See next:

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 corruptions.

VMware Infrastructure

Platforms

- VMware vSphere
- VMware vCloud Director
- VMware Cloud on AWS
- VMware Cloud on Dell EMC

Hosts

- ESXi 7.0 (up to 7.0 U3)
- ESXi 6.x
- ESXi 5.5

Software

- vCenter Server or vCenter Server Appliance 7.0 (up to 7.0 U3)
- vCenter Server or vCenter Server Appliance 6.x
- vCenter Server or vCenter Server Appliance 5.x
- vCloud Director 10.x (up to 10.3)
- vCloud Director 9.5 (9.7 or later for replication functionality)

Standalone ESXi hosts are fully supported, so vCenter Server and vCloud Director are optional. However, whenever they are present, we highly recommend that your 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 ESXi version is 6.5 U2.
- 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.

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, because VMware does not support snapshotting such VMs. Please use 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 VMware vSphere version in use.
- Microsoft VSS integration is supported for Microsoft Windows 2008 and later, except 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
- Hyper-V 2008 R2 SP1
- Hyper-V Semi-Annual Channel (versions 1803 to 20H2)

Microsoft Windows 11 Hyper-V (version 21H2) and Windows 10 Hyper-V (versions 1803 to 21H2) 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.

Depending on your Windows Server version, some additional hotfixes not included in the Windows Update distribution must be installed. Please refer to KB1838 for more information.

Software

- Microsoft Windows PowerShell 5.1 (optional, enables network-less guest processing)
- Microsoft System Center Virtual Machine Manager 2012 SP1 to 2019

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

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 2008 R2 SP1
- Microsoft Windows 11 (version 21H2)
- Microsoft Windows 10 (versions 1803 to 21H2)
- Microsoft Windows 8.1
- Microsoft Windows 7 SP1

Software

- Microsoft SQL Server 2008 to 2019 (2016 SP1 Express is included)
- System Center Virtual Machine Manager 2012 SP1 to 2019 Admin UI (optional, to register SCVMM server with Backup & Replication infrastructure)
- Microsoft .NET Framework 4.7.2 (included in the setup)
- Windows Installer 4.5 (included in the setup)
- Microsoft Windows PowerShell 5.1 (included in the setup)
- Firefox, Google Chrome, Microsoft Edge, or Microsoft Internet Explorer 11.0 or later

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 impact user interface responsiveness.

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 2008 R2 SP1
- Microsoft Windows 11 (version 21H2)
- Microsoft Windows 10 (versions 1803 to 21H2)
- Microsoft Windows 8.1
- Microsoft Windows 7 SP1

Software

- Microsoft .NET Framework 4.7.2 (included in the setup)
- Microsoft Windows PowerShell 5.1 (included in the setup)
- Windows Installer 4.5 (included in the setup)
- Firefox, Google Chrome, Microsoft Edge, or Microsoft Internet Explorer 11.0 or later

Backup Proxy Server

Hardware

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

Memory: 2 GB RAM plus 2 GB for each concurrent task. 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, and 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 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 Server 2008 R2 SP1
- Microsoft Windows Server Semi-Annual Channel (versions 1803 to 20H2)
- Microsoft Windows 11 (version 21H2)
- Microsoft Windows 10 (versions 1803 to 21H2)
- Microsoft Windows 8.1
- Microsoft Windows 7 SP1

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

- CentOS 7 to 8.5
- CentOS Stream
- Debian 9.0 to 11.0
- Fedora 30 to 35
- RHEL 6.0 to 8.5
- openSUSE Leap 15.2 and 15.3, Tumbleweed
- Oracle Linux 6 (UEK3) to 8.3 (UEK R6 U2)
- Oracle Linux 6 to 8.5 (RHCK)
- SLES 11 SP4, 12 SP1-SP5, 15 SP0-SP3
- Ubuntu 14.04 LTS, 16.04 LTS, 18.04 LTS, 19.10, 20.04 LTS, 21.04, 21.10

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

- Microsoft Windows Server 2008 R2 SP1
- Windows Server Semi-Annual Channel (versions 1803 to 20H2)

For agent-based off-host backup proxy server, 64-bit versions of the following Microsoft Windows operating systems are supported, including 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 Server 2008 R2 SP1
- Windows Server Semi-Annual Channel (versions 1803 to 20H2)

For file share backup proxy server, 64-bit versions of the following Microsoft Windows operating systems are supported, including 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 Server 2008 R2 SP1
- Windows Server Semi-Annual Channel (versions 1803 to 20H2)
- Microsoft Windows 11 (version 21H2)
- Microsoft Windows 10 (version 1803 to 21H2)
- Microsoft Windows 8.1
- Microsoft Windows 7 SP1

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

Software

When proxy server running on Microsoft Windows Server 2008 R2:

- Microsoft Visual C++ 2008 SP1 Redistributable Package (x64). The installation package can be downloaded from https://vee.am/runtime

CDP Proxy Server

Hardware

CPU: x86-64 processor (minimum 8 cores or vCPUs). Using multi-core processors improves data processing performance and allows for more tasks to be processed concurrently.

Memory: 16 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: 1 Gbps or faster.

OS

For VMware vSphere backup proxy, 64-bit versions of the following Microsoft Windows operating systems are supported, including 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 Server 2008 R2 SP1
- Microsoft Windows Server Semi-Annual Channel (versions 1803 to 20H2)
- Microsoft Windows 11 (version 21H2)
- Microsoft Windows 10 (versions 1803 to 21H2)
- Microsoft Windows 8.1
- Microsoft Windows 7 SP1

Backup Repository Server

These requirements also apply to mount servers (if separate from the repository server), gateway servers for file share and deduplicating appliance-based repositories, and cache repository servers (64-bit OS only).

Hardware

CPU: x86 processor (x86-64 recommended).

Memory: 4 GB RAM, plus up to 2 GB RAM (32-bit OS) or up to 4 GB RAM (64-bit OS) for each concurrently processed machine (depending on machine size, number of disks and backup chain length) or file share.

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

OS

Both 32-bit and 64-bit (recommended) versions of the following Microsoft Windows operating systems are supported, including 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 Server 2008 R2 SP1
- Microsoft Windows Server Semi-Annual Channel (versions 1803 to 20H2)
- Microsoft Windows 11 (version 21H2)
- Microsoft Windows 10 (version 1803 to 21H2)
- Microsoft Windows 8.1
- Microsoft Windows 7 SP1

Besides, both 32-bit and 64-bit (recommended) versions of the following Linux distributions are supported:

- CentOS 7 to 8.5
- CentOS Stream
- Debian 9.0 to 11.0
- Fedora 30 to 35
- RHEL 6.0 to 8.5
- openSUSE Leap 15.2 and 15.3, Tumbleweed
- Oracle Linux 6 (UEK3) to 8.3 (UEK R6 U2)
- Oracle Linux 6 to 8.5 (RHCK)
- SLES 11 SP4, 12 SP1-SP5, 15 SP0-SP3
- Ubuntu 14.04 LTS, 16.04 LTS, 18.04 LTS, 19.10, 20.04 LTS, 21.04, 21.10.

Bash shell and SSH connectivity are required to deploy the persistent data mover (SSH Server can then be disabled).

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

- CentOS 8.2, 8.3, 8.4, and 8.5
- Debian 10.x, 11
- RHEL 8.2, 8.3, 8.4, and 8.5

- SLES 15 SP2, SP3
- Ubuntu 18.04 LTS, 20.04 LTS, 21.04, and 21.10

For other distributions, XFS integration support is experimental, with kernel version 5.4 or later recommended.

Tape Server

Hardware

CPU: x86 processor (x86-64 recommended).

Memory: 2 GB RAM plus 200MB for each concurrent backup task. 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

Both 32-bit and 64-bit (recommended) versions of the following 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 Server 2008 R2 SP1
- Microsoft Windows Server Semi-Annual Channel (versions 1803 to 20H2)
- Microsoft Windows 11 (version 21H2)
- Microsoft Windows 10 (version 1803 to 21H2)
- Microsoft Windows 8.1
- Microsoft Windows 7 SP1

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, and 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 by WAN accelerators operating in high-bandwidth mode, so it does not need to be allocated and populated in such cases.

OS

Only 64-bit versions of the following operating systems are supported, including 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 Server 2008 R2 SP1
- Microsoft Windows Server Semi-Annual Channel (versions 1803 to 20H2)
- Microsoft Windows 11 (version 21H2)
- Microsoft Windows 10 (version 1803 to 21H2)
- Microsoft Windows 8.1
- Microsoft Windows 7 SP1

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.

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 2008 R2 SP1
- Microsoft Windows Server Semi-Annual Channel (versions 1803 to 20H2)
- Microsoft Windows 11 (version 21H2)
- Microsoft Windows 10 (version 1803 to 21H2)
- Microsoft Windows 8.1
- Microsoft Windows 7 SP1

Server Software

- Microsoft Internet Information Services 7.5 or later
- Microsoft SQL Server 2008 to 2019 (2016 SP1 Express is included)
- Microsoft .NET Framework 4.7.2 (included in the setup)
- Windows Installer 4.5 (included in the setup)

Client Software

- Firefox, Google Chrome, Microsoft Edge, or Microsoft Internet Explorer 11.0 or later. The browser must have JavaScript and WebSocket protocol enabled.
- Microsoft Excel 2007 or later (to view reports exported to Microsoft Excel format).

Backup Target

Backups can be performed 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 version). Using SMB protocol for non-continuously available (CA) file shares is not recommended for reliability reasons.
- Dell EMC DataDomain (DD OS version 6.2 to 7.7) with the DDBoost license. Both Ethernet and Fibre Channel (FC) connectivity are supported.
- ExaGrid (firmware version 5.0.0 or later).
- HPE StoreOnce (firmware version 3.15.1 or later) with Catalyst license. Both Ethernet and Fibre Channel (FC) connectivity are supported.
- Quantum and OEM partners (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. 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)
- Any S3-compatible object storage (on-premises appliance, or cloud storage provider)

Once backups are copied or offloaded to Amazon S3 or Microsoft Azure Blob Storage, 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
- Amazon S3 Glacier Deep Archive
- Microsoft Azure Archive 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 (I/O journal size is limited to 254GB per VM)
- VVOL (I/O journal size is limited to 4GB per VM)

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

LTO3 through LTO9 tape libraries and standalone drives are supported, including Virtual Tape Libraries (VTL). 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 for multiple open handles from a host to a drive to exist at the same time. Usually, such drivers are referred to as "non-exclusive".
- No other backup server or software must be interacting with the tape device.

Storage Snapshot Integrations

Storage snapshot integration is supported for pre-installed plug-ins and additional plug-ins that are available for download at www.veeam.com/backup-replication-download.html.

Cisco HyperFlex/HX-Series

- NFS connectivity only
- HyperFlex 4.0(2x) or later
- Basic authentication is not supported for SSO users in HyperFlex

DataCore SANsymphony

- Fibre Channel (FC) or iSCSI connectivity
- DataCore SANsymphony 10.0 PSP12 or later

Dell EMC Isilon/PowerScale (NAS Backup only)

- NFS or CIFS connectivity
- OneFS versions 8.1.2 to 9.1

Dell EMC PowerMax

- Fibre Channel (FC) or iSCSI connectivity
- Dell EMC PowerMax/VMAX All Flash (PowerMax OS microcode family 5978 or later)
- Unisphere for PowerMax 9.2.1.6 or later

Dell EMC PowerStore

- Fibre Channel (FC) or iSCSI connectivity
- Dell EMC PowerStore T and PowerStore X series (PowerStore OS 2.0 or later)

Dell EMC SC Series/Compellent

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

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

- NFS, Fibre Channel (FC) or iSCSI connectivity
- Dell EMC VNX/VNX2 all OE versions are supported
- DEll EMC Unity XT/Unity, VNXe OE versions 3.x up to 5.1

Fujitsu ETERNUS AF and DX series

- Fibre Channel (FC) or iSCSI connectivity
- 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
- VSP E590, E790, E990 (93-03-01-60/00 or later)
- VSP F350, F370, F700, F900 (88-07-01-x0/00 or later)
- VSP G350, G370, G700, G900 (88-07-01-x0/00 or later)

VSP 5000 series (90-05-01-00/00 or later)HPE 3PAR StoreServ

- Fibre Channel (FC) or iSCSI connectivity
- 3PAR OS versions 3.2.2 to 3.3.1 MU5
- WSAPI 1.5 and later
- iSCSI VLAN tags are supported
- Virtual Domains are supported

HPE Alletra 6000

- Fibre Channel (FC) or iSCSI connectivity
- OS version 6.0
- Synchronous replication is not supported

HPE Alletra 9000

- Fibre Channel (FC) or iSCSI connectivity
- OS version 9.3
- Virtual Domains are supported

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

- Fibre Channel (FC) or iSCSI connectivity
- Nimble OS 2.3 and later
- HPE Nimble synchronous replication is not supported

HPE StoreVirtual/LeftHand/P4000 series and StoreVirtual VSA

- iSCSI connectivity only
- LeftHand OS versions 9.5 to 12.8
- HPE SV3200 (LeftHand OS version 13) is not supported

HPE Primera

- Fibre Channel (FC) or iSCSI (starting from OS versions 4.3 or later) connectivity
- OS versions 4.x
- Virtual Domains are supported

HPE XP

- Fibre Channel (FC) connectivity

HPE XP8 (90-05-01-00/00 or later)IBM FlashSystem (Storwize), IBM SVC, Lenovo Storage V Series

- Fibre Channel (FC) or iSCSI connectivity
- Spectrum Virtualize 7.6 or later

INFINIDAT Infinibox F-series

- NFS, Fibre Channel (FC) or iSCSI connectivity

InfiniBox version 3.0 and laterNetApp FAS/AFF, FlexArray (V-Series), ONTAP Edge/Select/Cloud VSA and FAS OEM (Fujitsu ETERNUS HX/AX, IBM N series and Lenovo DM series

- NFS, Fibre Channel (FC) or iSCSI connectivity
- ONTAP cluster-mode versions from 8.3 up to 9.9
- ONTAP 7-mode versions 8.2 up to 8.2.5
- MetroCluster is supported
- ONTAP features application-aware data management and SVM-DR are not supported
- NetApp Synchronous SnapMirror is not supported

NetApp SolidFire/HCI

- iSCSI connectivity
- NetApp SolidFire support requires Element OS version 9.0 or later
- NetApp HCI support requires Element OS version 10.0 or later

Pure Storage FlashArray

- Fibre Channel (FC) or iSCSI connectivity
- Purity version 4.10 or later
- Purity ActiveCluster is supported
- Replicated volume snapshots on the target array are supported

Tintri IntelliFlash/Western Digital IntelliFlash/Tegile

- NFS, Fibre Channel (FC) or iSCSI connectivity
- Tintri IntelliFlash 3.9.2, 3.10.1 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 SP1
- Microsoft Exchange 2013
- Microsoft Exchange 2010 SP1, SP2, or SP3

Software

- Microsoft Outlook 2010 or later (64-bit) for PST exports (optional)

Veeam Explorer for Microsoft SharePoint

Microsoft SharePoint Server

- Microsoft SharePoint 2019
- Microsoft SharePoint 2016
- Microsoft SharePoint 2013
- Microsoft SharePoint 2010

The 3rd-party RBS providers are not supported.

Veeam Explorer for Microsoft SQL Server

Microsoft SQL Server

- 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
- Microsoft SQL Server 2005 SP4

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 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 19
- Oracle 18
- Oracle 12
- Oracle 11

Configuration

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

Known Issues and Limitations

Backup infrastructure

- All registered server names must be resolvable into IPv4 address.
- 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 right away.
- 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 will not be able to decrypt such information if attached to the existing database, so any encrypted information will have to be supplied manually. To work around this, use the configuration backup and restore functionality for backup server migrations.
- VM virtual disk file and configuration file names length must not exceed 128 symbols.
- VeeamZIP operations do not respect backup repository I/O throttling settings.
- Backup proxy cannot transfer a backup to an SMB-based repository when the share is located on the same server with the proxy. To work around this, create a Windows-based backup repository on the proxy server instead.

VMware

- After upgrading to v11, replicas that were in the Failback state during the upgrade will be erroneously shown to be in the Failover state. To work around the issue, rescan the affected replicas manually.
- On ESXi 7.0, 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 be failing 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 certain P2V/V2V conversion tools.
- Linux-based backup proxies with configured multipath do not work in DirectSAN and BoSS.
- Processing virtual disks with @ symbol in the disk name is not supported by Linux-based proxies in VMware VDDK-based transport modes.
- NSX-T networking is not supported for Virtual Labs or Veeam Cloud Connect Replication.
- A virtual backup proxy server cannot be used to backup, 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 VM.
- 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.
- For populating replica disks during incremental replication passes and failback, Windows 7 and Windows 8 based backup proxy servers support "network" processing mode only. To work around this, install backup proxy servers on Windows Server OS.
- VMware vStorage API for Data Protection has some 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 failover to the network mode for a specific virtual disk.

- Processing of Fault-Tolerant VMs created on vSphere versions prior to vSphere 6 is not supported.
- Hard Disk restore may fail with the "*Restore job failed Error: A specified parameter was not correct: unitNumber*" error when restoring disk to a 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.
- Restore and replication of VMs between different ESXi versions requires that VM's virtual hardware version is 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 (Vista or later) requires that Local Administrator (MACHINE\Administrator) or Domain Administrator (DOMAIN\Administrator) account is provided on 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, or when Kerberos authentication is enabled on a storage device.
- 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.
- 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 instant recovery to First Class Disk (FCD).

VMware Cloud on AWS

- Only hot add transport mode is supported due to API limitation.
- All vPower NFS-based functionality is not supported due to platform limitation.
- Networkless guest interaction is not supported due to API limitations.
- Re-IP addressing and file-level recovery for replicas are not supported.
- Only 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 online. To fix the issue, refer to VMware KB76633.
- I/O filter cannot be attached to VMs with snapshots. Remove all snapshots from VMs to be protected before creating a CDP policy.
- CDP is not supported for VMs to which VM storage policies with multiple datastore specific rule sets apply. If you need to define datastores to be used for placement of the VMs, you can add a tag rule for vSAN instead of a tag based placement datastore specific rule. For more information on how to create tag rules for vSAN, see VMware Docs.
- Using a vCenter Server as a CDP proxy is not supported and may cause various issues.
- Cisco HyperFlex is not supported as a source or target.
- Certain primary storage integration plug-ins setup programs leave the CDP service stopped after the installation. Please verify the service state following the installation and start it manually if needed.

Hyper-V 2016/2022

- Hyper-V 2022 and SAC version 2004 and 20H2 hosts force 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 Hyper-V 2022 and SAC version 2004 and 20H2 hosts 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 is a known Hyper-V 2016 compatibility issue that 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, make sure 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 cluster functional level is upgraded to Windows Server 2016 or later. Keep in mind that VMs 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, the presence of 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 bug in Microsoft Hyper-V VSS Writer.
- VMs with pass-through virtual disks cannot be processed due to Hyper-V 2016 and later checkpoints limitations.

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.
- When replicating from older to newer Hyper-V host version, failback is only supported to the original location if the original VM still exists.
- Backup of VMs with virtual disks located both on local and shared CSV/SMB storage is not supported due to Hyper-V limitation.
- Deleting Hyper-V replica from disk does not delete the replica VM from SCVMM.
- 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 VM into a subfolder instead.

Linux

To register a Linux server, as well as to update or remove Veeam components, the server must support Password or Certificate-based authentication, have bash shell and SSH Server enabled for the duration of the operation.

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.
- File filter dialog label incorrectly limits the include and exclude functionality to files and file masks only, however, it is also supported to specify full folder paths as exclude filters.
- 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.

Agent Management

- All protected computer names must be resolvable into IPv4 address.
- 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).
- When deleting the backup chain from the disk, GFS restore points are removed even if the option to keep those restore points has been selected.

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 clusters are not currently 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 they are 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 Restore to Hyper-V 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.

Direct Restore to Microsoft Azure and Azure Stack

- Certain Linux computer configurations may require Azure VM configuration to be adjusted upon restore to Microsoft Azure. If your VM fails to boot, please contact Veeam Support for assistance.
- VM name, VM group name and VM size are not validated for compatibility with 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

- Under rare unknown circumstances, file-level restore from ReFS 3.1 or later volumes may cause some Windows Server 2019 or later (or Windows 10 1809 or later) mount servers to BSOD, or FLR session to hang. The same applies to replica VM re-IP functionality for VMs with ReFS volumes. To work around this issue, create *ForceVhdMount* (DWORD) = 1 registry value under the *HKLM|SOFTWARE|Veeam|Veeam Backup and Replication* key on the backup server.
- File-level restore may fail if a VM you are restoring from was lacking 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, the mount server and backup console must be installed on Windows Server with the Data Deduplication feature enabled, and the Windows Server version must be the same or greater than one of the VM you are restoring from. Otherwise, deduplication driver incompatibility will cause file-level recovery errors with false data corruption reports.

Multi-OS File-Level Restore with Mount Host

- Mount host kernel must support the source file system from the backup. Otherwise, mount operation may result in kernel panic in some cases.
- LVM snapshots and NSS volumes 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, 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.

Replica Failover

- Starting a replicated VM using means other than the product's user interface (including vSphere Client, Hyper-V Manager, SCVMM, PowerShell) disables 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 backup files.
- Immediately after 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 Enterprise Manager server must be functional for setting up self-service recovery delegation scope.
- The presence of 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

- Automatic virtual lab configuration is not supported for networks with non-private network addresses.
- Automatic virtual lab networking configuration process may fail with the "*Unable to resolve default network settings*" error. To work around the issue, go back to the wizard and try again.

- Automatic virtual lab networking configuration may fail in some cases when DVS are present in the virtual environment. In such cases, use the advanced configuration mode to set up the virtual lab networking manually.
- SureBackup job fails on VM with unsupported or excluded virtual disks which were not explicitly set to be removed from configuration (as a part of disk exclusion settings in the backup job) because test VM cannot find its disks and is unable to start.
- Automatic physical mode RDM disk exclusion in the backup job may lead to the situation where the test VM can connect to the RDM disk, and make irreversible changes on the disk. To avoid this, always exclude the physical RDM disk from the backup job explicitly, 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 and Oracle transaction log backup to a cloud repository are 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 replicas 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 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.
- Failover plans session cannot be viewed once 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.
- Remote Console and Remote Desktop functionality 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" and failover won't work.

Backup Copy

- The backup Copy job in the immediate copy mode 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.

Object Storage

- Not all Amazon and Azure regions may provide cold object storage tiers used by the SOBR Archive Tier

and/or compute resources required to provision proxy appliances for data archival. Pay attention to this when selected the cloud region to use.
- Using the immutability feature with the existing S3 bucket containing backups created by 9.5 Update 4 requires that both Versioning and Object Lock are enabled on the bucket at the same time before the immutability feature is enabled. Any other approach will lead to backup offload failures and the inability to correctly interact with backups in the bucket.
- Data in 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

- Direct restore from tape is supported from backups created by version 9.0 or later.
- File to Tape job fails building a list of files to process if catalog contains files with certain Unicode symbols.
- Backup to Tape job will perform 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 and Oracle transaction log backup to tape is 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.

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 database recovery is not supported when the tnsnames.ora and listener.ora files are stored in a non-default location.
- Instant recovery of the entire Oracle Data Guard is not supported, however, you can restore individual databases.
- Database restore for Oracle Data Guard with tnsnames.ora and listener.ora located in non-default paths is not supported.
- 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, please contact support to enable the workaround.
- Database restore may fail if backed up Oracle server version and 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 ID.
- 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 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 lists values are not restored.

Veeam Explorer for Microsoft SQL Server

- Instant database publishing to 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 that all nodes of the same AlwaysOn availability group are located in the same time zone.
- A point in time restore of the database from an imported backup is not possible.
- Transaction log backup requires that at least one image-level backup of the SQL Server machine is performed. This particularly means that transaction log backup will not function after the full SQL Server machine restore is performed, 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

- VMs with virtual disk files located on different storage volumes are supported only for snapshots created by Veeam Backup & Replication 9.5 Update 4 or later jobs. For other storage snapshots, only disks residing on the same datastore with the VMX file will be available for all restore types.
- Storage snapshots and volumes with a name starting with "VeeamAUX_" are automatically excluded from processing.

Cisco HyperFlex

- Scenarios, where several Cisco HyperFlex systems are registered under different VMware vCenter Servers, are not currently supported. It is recommended to back up VMs of each VMware vCenter Server instance using a separate Veeam backup server.

Dell EMC VNX(e)

- Legacy SnapView snapshot technology is not supported in favor of VNX Snapshot.
- Concurrent operations from the same LUN (such as backup and restore) are not supported due to EMC VNXe limitation.

NetApp ONTAP

- Infinite volumes are not supported.
- vFiler DR units are not supported and are automatically hidden by the UI.
- Configurations with VM stored on a non-default vFiler based on qtree (instead of volume) are not supported.

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 DPI setting to 100% or 125% using the Display settings of the Windows Control Panel.

User Interface

- If a NETBIOS domain name differs from a fully qualified domain name, 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.

PowerShell

- Restores from imported backups residing on a CIFS share are not supported through PowerShell.

Upgrade

- For Windows Server Hyper-V versions 2008 R2 to 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 v11, jobs will automatically perform a full scan-based incremental run for machines with virtual disks formatted with NTFS with cluster size equal or larger than 64KB.

Installing Veeam Backup & Replication

Veeam Backup & Replication Server

To install Veeam Backup & Replication 11a 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 the Veeam Backup & Replication tile.
3. Accept the terms of Veeam Backup & Replication and 3rd party components license agreements to install the product. You can find a copy at veeam.com/eula.html
4. Provide setup program with your license file.
5. Review the default installation settings. To change the defaults, select the **Let me specify different settings** and go through additional wizard steps.
6. Click **Install** to start the installation and follow the setup wizard steps.
7. 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 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 the Veeam Backup Enterprise Manager tile.
2. Accept the terms of the License Agreement to install the product.
3. Provide setup program with your license file.
4. Review the default installation settings. To change the defaults, select the **Let me specify different settings** and go through additional wizard steps.
5. Click **Install** to start the installation and follow the setup wizard steps.
6. 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 11a supports automated in-place upgrade from any version 11 build, from any version 10 build and from version 9.5 Update 4b (build 9.5.4.2866) which preserves all products settings and configuration. To upgrade from earlier versions, please contact our Customer Support.

Upgrade checklist:

1. Veeam Backup & Replication v11a uses the same license file format introduced with v10, so you can use your existing v10 license file to install v11a and future versions. Do check the support expiration date in the license file though, as your support contract must be active as of the date when the version you're installing was built.
2. Are you using Veeam Backup Starter? This edition has been discontinued, so v11a will not accept such license files. Please download a replacement license file from the Customer Portal before upgrading.
3. Are you using Server 2019 based ReFS backup repositories? If yes, avoid upgrading them to Server 2022 and/or mounting ReFS volumes from Server 2019 to new Server 2022 installs until you read this thread on Veeam R&D forums. Microsoft has addressed the known regression in the ReFS format upgrade code, the fix is now publicly available.
4. Are you using Veeam Availability Orchestrator 3.0 or earlier? Veeam Backup & Replication 11a is not compatible with these versions. Please upgrade to Veeam Availability Orchestrator 4.0 before upgrading to Veeam Backup & Replication 11a.
5. Are you using Veeam Backup Enterprise Manager? If yes, start the upgrade procedure from this component. Note that Enterprise Manager 11 supports backup servers version 9.5 Update 4 or later, so you can potentially run both old and new versions of the backup server side by side if required.
6. Are you using Veeam ONE to monitor your backup infrastructure? If yes, upgrade it first. Veeam ONE 11 supports monitoring of backup servers version 9.5 Update 4 or later.
7. Are you using Veeam Backup Enterprise Manager server added to Veeam ONE? If yes, first upgrade Veeam ONE, second upgrade Veeam Backup Enterprise Manager, third upgrade Veeam Backup & Replication.
8. 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, then upgrade Veeam Backup & Replication to version 11a build 11.01.1261 or later.
9. Are you using Veeam Plug-in for Oracle RMAN or Veeam Plug-in for SAP HANA? If yes, you must upgrade Veeam Backup & Replication first, then you can upgrade Veeam Plug-ins. Veeam Backup & Replication 11 supports Veeam Plug-ins version 11 and 10a (10.0.1.4854).
10. Check if the backup server to be upgraded is installed on the supported operating system version according to the System Requirements section above. If not, please create a configuration backup, install v11a on the supported OS first, then restore the configuration backup created earlier.
11. Ensure there are no active processes, such as any running jobs and restore sessions. Disable any periodic jobs and data management activities, so that they do not start during the upgrade.
12. Do you have backup copy jobs with synthetic GFS full backups? Before the upgrade, make sure that all GFS candidates (incremental restore points created on days when GFS was scheduled and that are 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.

13. Are you using backup copy jobs targeted at a backup repository with rotated drives? If yes, mind that after the upgrade, the retention will start taking into account restore points on missing rotated drives. To store the necessary number of restore points on all rotated drives, increase the retention value before the upgrade.
14. Are you using integration with Veeam Backup for Microsoft Azure? If yes, after upgrade to 11a, select the existing Microsoft Azure compute account in the Manage Cloud Credentials, click **Edit**, and go through the Microsoft Azure Compute Account to update account permissions. Otherwise, you can face problems when adding an external repository with backups created by Veeam Backup for Microsoft Azure 3.0.

Additional considerations when upgrading from version 9.5 Update 4b:

1. Are you using an Instance license to protect some of your vSphere or Hyper-V VMs with agent-based backup jobs in presence of a Socket license? As enforcement of the Veeam Licensing Policy, starting from v10 hosts where such VMs are running will consume Socket licenses. This may result in your agent-based backup jobs failing after the upgrade due to insufficient Socket licenses. Before upgrading to v11a, please review the Licensing section of the What's New in v10 document for the detailed description of all changes that happened with the v10 release.
2. The v11a setup wizard will offer to download your v11a license automatically. This requires uploading your currently installed license to Veeam servers. If your backup server has no Internet connection, or if you prefer not to have your license uploaded, or in case of license upgrade issues – please download your license from the Customer Portal manually. Note that you must have an active maintenance agreement at the time when you access the portal.

Upgrading Veeam Backup Enterprise Manager

To perform an upgrade of Veeam Backup Enterprise Manager to version 11a, you must be running version 9.5 Update 4b or later on the supported operating system (refer to the System Requirements section of this document). To upgrade from previous versions, please contact our Customer 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.
4. Click the Veeam Backup Enterprise Manager tile.
5. Follow the setup wizard steps as outlined in the installation procedure above. Be sure to select the same SQL database and instance that was used by the previous Veeam Backup Enterprise Manager version.
6. If you have 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 perform an upgrade of the Veeam Backup & Replication server to version 11a, you must be running version 9.5 Update 4b (build 9.5.4.2866) 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 built-in configuration backup functionality.
4. Mount the product ISO and use autorun, or run the *Setup.exe* file.
5. Click the Veeam Backup & Replication tile.
6. Follow the upgrade wizard steps as outlined in the installation procedure above. Be sure to select the same SQL database and instance that was used by the previous product version.
7. If you are using remote backup consoles, upgrade them manually using the product ISO file. Unfortunately, the automatic upgrade is not supported this time 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 upgrade, you can run the Upgrade wizard at any time later from the main product menu. Note that out-of-date product components cannot be used by jobs until they are 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. [For Veeam Backup & Replication 11GA (build 11.0.0.837) with installed cumulative patch P20210319 or later] If you are using 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 Set-VBRLinux PowerShell cmdlet to mass-deploy. Until you do this, those Linux servers will continue using the legacy run-time 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 underlying hypervisor host (for vSphere or Hyper-V VMs protection only). For more information, see Veeam Licensing Policy at 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

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, please contact Veeam Renewals at veeam.com/renewal.html

Updating Veeam Backup & Replication License

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 **Configuration > Licensing** tab in Enterprise Manager UI, and click **Install License.**
2. Browse to the license file (**.lic**) that was 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**) that was 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
- User guides: www.veeam.com/documentation-guides-datasheets.html
- Community forums: 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.

> **TIP**
>
> Before contacting technical support, consider searching for a solution on Veeam Community Forums at 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 to build our products with your suggestions in mind. We encourage all customers to join Veeam Community Forums at veeam.com/forums and share their feedback directly with the R&D team.

Should you have a technical or licensing issue or question, please feel free to contact our Customer Support organization directly. We have qualified technical and customer support staff available 24 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. 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.