Quest® vRanger® 7.8.7

Installation/Upgrade Guide

© 2026 Quest Software Inc.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept.
20 Enterprise, Suite 100
Aliso Viejo, CA 92656

Refer to our website (https://www.quest.com) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at https://www.quest.com/legal.

Trademarks

Quest, the Quest logo, Foglight, NetVault, vRanger, and Join the Innovation are trademarks and registered trademarks of Quest Software Inc. vCenter, vSphere, vMotion, VMware, and ESXi are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions. Active Directory, Hyper-V, SharePoint, SQL Server, Windows, and Windows Server are registered trademarks of Microsoft Corporation in the United States and/or other countries. Data Domain and DD Boost are trademarks or registered trademarks of EMC Corporation in the United States and other countries. For a complete list of Quest marks, visit https://www.quest.com/legal/trademark-information.aspx. All other trademarks and registered trademarks are property of their respective owners.

Legend

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT NOTE, **NOTE**, **TIP**, **MOBILE**, or **VIDEO:** An information icon indicates supporting information.

vRanger Installation/Upgrade Guide
Updated - February 2026
Software Version - 7.8.7

Contents

Introduction 5
Quest® vRanger®: at a glance 5
Key benefits 5
Major feature list 6
Target audience 7
Recommended additional reading 8

Before you install 9
Before installing vRanger 9
vRanger licensing levels 9
Trial license 10
Single license limitation 10
vRanger installation overview 11
Installing the vRanger server 11
Available backup transports 11
Installing vRanger in a virtual machine (VM) 12
Installing vRanger on a physical server 14
Optimizing your network for backups 15
Installing the vRanger database 16
Database options 16
Installing the databases 17
Installing the vRanger virtual appliance (VA) 17
VA usage 17
Deployment locations 18
Creating a vRanger repository 18
Repository storage devices 18
Bandwidth to repositories 19
Repository size 19
Configuring vCenter permissions 19

System requirements and compatibility 22
Requirements for the vRanger machine 22
Minimum hardware requirements 22
Supported operating systems for installation 23
Supported SQL Server versions 24
Supported platforms 24
Supported vSphere versions 24
Supported Hyper-V versions 25
Supported platforms for physical machine backup 26
Supported virtual appliance (VA) versions 26
Supported disk types and file systems 26
Supported disk types 26
Supported file systems 27
Feature-level requirements 28

Standard backup, restore, and replication . . . 28
Physical backup and restore . . . 28
HotAdd . . . 29
File-level restore (FLR): Windows . . . 29
FLR: Linux . . . 29
Configuration requirements . . . 29
HotAdd disk requirements . . . 29
Password security setting policy . . . 30
Port requirements . . . 30
Compatibility with other applications . . . 31
Microsoft Volume Shadow Copy Service (VSS) . . . 31

Installing vRanger . . . 33
vRanger installation overview . . . 33
Installing vRanger . . . 33
Setting up vRanger . . . 33
Entering vRanger service credentials . . . 34
Installing the vRanger database . . . 34
Entering vRanger database runtime credentials . . . 35
Installing the vRanger Catalog Service . . . 35
Completing the installation . . . 36
Installing the vRanger Catalog Service later . . . 36

Upgrading vRanger . . . 37
Before upgrading vRanger . . . 37
Deprecated repository types . . . 37
vRanger editions . . . 38
Backing up the vRanger database . . . 39
Upgrading a previous vRanger installation . . . 39
Updating the VSS Tools . . . 40
Upgrading the vRanger Database . . . 41
Performing a database upgrade . . . 41
Upgrading the vRanger virtual appliance (VA) . . . 43
Checking the version of your VA . . . 43
Upgrading your VA . . . 43
Upgrading a previous vReplicator installation . . . 45
Technical support resources . . . 46

1

Introduction

- Quest® vRanger®: at a glance
- Key benefits
- Major feature list
- Target audience

Quest® vRanger®: at a glance

vRanger provides a simple, fast, and scalable data- protection solution that deploys seamlessly into virtual environments. vRanger provides high-speed backup and recovery of VMware®, Hyper-V®, and physical Windows Server® environments. It also provides high-speed replication for VMware. It protects entire virtual environments in minutes, detecting and backing up new virtual machines (VMs) automatically, and delivers safe, scalable data protection to even the largest VMware and Hyper-V environments. With vRanger, you can locate and restore individual files in seconds—even if they are buried in virtual and physical backups—from a single, intuitive interface.

vRanger supports enterprise deduplication and delivers disk-to-disk backup with Quest® QoreStor™, Quest® DR Series System appliances, EMC® Data Domain®, and Quest® NetVault™ SmartDisk to reduce backup storage costs and improve backup time with client-side deduplication.

vRanger scales with your virtual environment by maximizing resources through distributed processing, while simplifying management with central command and control.

vRanger capabilities include:

- Protect entire VMware and Hyper-V environments in minutes.
- Deliver high-speed, storage-thrifty backup and restore for VMware, Hyper-V, and physical Windows servers.
- Quickly locate and restore individual files from virtual and physical backups.
- Replicate key VMs for offsite disaster recovery preparedness.
- Deploy scalable data protection for even the largest virtual infrastructures.

Key benefits

vRanger benefits include:

- Exploits VMware vSphere® performance and scalability enhancements.
- Provides high-speed, resource-efficient backup, replication, and recovery of VMware® and Hyper-V® VM images.
- Delivers maximum storage savings when paired with Quest® QoreStor™, Quest® DR Series System appliances, EMC® Data Domain®, and Quest® NetVault™ SmartDisk

- Supports EMC Data Domain Boost and Quest QoreStor and DR Series RDA for optimized deduplication and replication.
- Operates as an easy-to-deploy, low-resource consumption virtual appliance (VA) for low-impact scalability.
- Improves VM backup and recovery performance with HotAdd support.
- Optimizes use of critical resources in virtual environments, including hypervisor hosts, networks, and storage.
- Includes a catalog for fast file searching and file-level restore.
- Provides protection for the largest VM deployments.
- Offers agent-less, maintenance-free deployment.
- Delivers proven reliability.
- Provides unmatched performance and scalability.
- Comes with world-class service and support.

Major feature list

vRanger backs up and recovers physical environments with blazing speed, a minimum of backup storage, and can restore Windows servers and even individual files and folders. With vRanger, you get comprehensive protection for both your virtual and physical environments that you can manage from one simple interface.

- **VMware® Ready™ Certified for vSphere®**: Exploits the latest in vSphere 6.7 performance and scalability improvements.
- **VMware vSphere / ESXi / vCloud , Virtual Volumes, Storage Profiles, and DRS cluster support** – Provides a wide range of backup and recovery and disaster recovery (DR) capabilities for VMware virtual infrastructures.
- **Microsoft Hyper-V 2022:** Protect the latest Hyper-V versions.
- **Virtual appliance (VA) architecture**: Through centralized and wizard-driven deployment and administration from the vRanger server, delivers scalable and cost-effective distributed data handling and throughput through VAs.
- **Disk-to-disk backup and deduplication**: Supports Quest DR Series system Rapid Data Access (RDA) for optimized client-side deduplication and replication.
- **EMC® Data Domain® (DD Boost™) support**: Supports distributed deduplication with EMC Data Domain appliances using the DD Boost API.
- **Disk-to-disk backup and deduplication:** Offers a Quest NetVault SmartDisk - vRanger Edition add on for enterprise-class deduplication that reduces backup storage footprints by up to 90 percent.
- **VMware HotAdd support**: Performs LAN-free backups with vRanger installed inside a VM and from the vRanger VA. Additionally, HotAdd accelerates network backups of ESXi.
- **Patented Active Block Mapping (ABM)**: Eliminates inactive and white space blocks from protected Windows VMs to speed backup, replication, and recovery jobs as well as reduce network and storage requirements.
- **Change block tracking (CBT):** Eliminates the time required to scan for changed blocks in guest images on vSphere hypervisor systems to improve the speed of backup and replication jobs.
- **Instant file-level restore (FLR) for Windows and Linux®**: Lets you restore a single file from a backup image in the repository through a one-step process.
- **Patented native, full catalog capability**: Provides a native, full catalog of every image in the backup repository, enabling immediate identification of available recovery positions, with one-click restore. Wildcard scanning feature locates backup repository files to be restored.

- **One-step catalog recovery**: Provides advanced search (including wildcards) and right-click recovery selection directly from the management console to speed restore of VMs, savepoints and hosts with native catalog.
- **Advanced Encryption Standard (AES)-256**: Secures protected images block-by-block on the VMware host as they are read so they are also secure over the network and in the backup repository.
- **Full, incremental, and differential backup:** Enables a complete backup cycle for protected images that is optimized for speed and resource efficiency.
- **Full and incremental replication:** Provides the full range of options required to replicate VMware VMs over LANs and WANs efficiently.
- **Replication:** Offers on and off-site options for flexible, reliable disaster recovery.
- **Supports backup and replication of encrypted VMware vSphere VMs**: Provides the full range of options required to backup, restore, replicate, failover, and failback encrypted virtual machines.
- **Physical Windows Server® support**: Supports backup and recovery of Windows physical servers, files, and folders.
- **Synthetic recovery**: Delivers single-pass restore, reading each required block only one time from multiple full, incremental, and differential backup images in the repository for the fastest, most efficient results.
- **VMware vSphere® vMotion® and Storage vMotion® support**: vSphere vMotion support ensures vRanger automatically protects VMware VMs as they move from one host to another, even when backup jobs are running. It also ensures vRanger follows VM storage disks when they are relocated to different data stores; locks VM storage disks when vRanger accesses the disks during a job.
- **Agent-less job execution, patent-pending:** Uses binary injection at run time on VMware ESXi hosts; eliminates burdens of license tracking and maintenance upgrades.
- **Advanced savepoint management**: Lets you manage and use multiple point-in-time copies of backup and replica images for precise image, file, and object restores.
- **Dynamic resource management**: Optimizes real-time use of critical resources; ensures efficiency and that jobs complete faster without exceeding resource capacity.
- **Job multi-streaming:** Lets you run multiple backup, restore, and replication jobs simultaneously for dramatic improvement in performance times.
- **Direct-to-target (D2T) architecture:** Distributes job execution and movement of data with optimal efficiency to improve data protection and ensure seamless scalability.
- **FIPS-compatible:** Address government data security requirements with vRanger Crypto Module, compatible with FIPS 140-2 Level.
- **Inline data validation:** Tests integrity of captured data on the source block-by-block as it is read; ensures image recovery from the backup repository and replica-image usability.
- **Remote management:** Lets you manage data protection jobs through a central console over LAN and WAN connections for control of all systems and sites in an environment.
- **PowerShell® access:** Automate scripts for protection jobs, reducing administrative burdens and human error.

Target audience

This guide is intended for backup administrators and other technical personnel who are responsible for designing and implementing a backup strategy for the organization. A good understanding of the operating system (OS) on which vRanger is running is assumed.

Recommended additional reading

The following documentation is also available:

- *Quest vRanger User's Guide*: This guide describes how to configure and work with vRanger.
- *Quest vRanger Integration Guide for EMC® Data Domain® Boost (DD Boost™)*: This guide describes how to configure vRanger to work with a Data Domain Boost repository to achieve source-side deduplication of backup data.
- *Quest vRanger Integration Guide for Quest NetVault SmartDisk - vRanger Edition*: This guide describes how to configure vRanger to work with a NetVault SmartDisk - vRanger Edition repository to achieve deduplication of backup data.
- *Quest vRanger Integration Guide for Quest DR Series Disk Backup Appliance*: This guide describes how to configure vRanger to work with a DR4x00 appliance to achieve deduplication of backup data.
- *Quest vRanger Integration Guide for Quest QoreStor*: This guide describes how to configure vRanger to work with QoreStor to achieve deduplication of backup data.

2

Before you install

- Before installing vRanger
- vRanger installation overview
- Installing the vRanger server
- Installing the vRanger database
- Installing the vRanger virtual appliance (VA)
- Creating a vRanger repository
- Configuring vCenter permissions

Before installing vRanger

Before installing vRanger, you must decide the best architectural option for your environment. In addition, there are some preliminary configurations that should be made to get the most out of vRanger. The following topics provide some basic information that you must decide where and how to deploy vRanger.

- vRanger licensing levels
- Trial license
- Single license limitation

NOTE: If you are upgrading a previous vRanger version, see Upgrading vRanger.

vRanger licensing levels

There are three levels of vRanger Licensing, each with different available features:

- vRanger Standard Edition (SE)
- vRanger Backup & Replication
- vReplicator

Table 1. Available features

	vRanger Backup & Replication	vRanger Backup & Replication - Physical Backup
VM backup	X	X
Virtual and physical machine restores	X	X
VA-based backup and restore	X	X
Physical machine backup		X
Replication	X	X
Changed Block Tracking (CBT)	X	X
Active Block Mapping (ABM)	X	X

Table 1. Available features

	vRanger Backup & Replication	vRanger Backup & Replication - Physical Backup
LAN-free (SAN)	X	X
LAN-free (HotAdd)	X	X
Catalog	X	X
Windows® file-level restore (FLR)	X	X
Linux® FLR	X	X

For VM backup, a license for vRanger controls the number of source CPUs that you can configure for backup. For licensing purposes, a multi-core processor is counted as a single CPU. For physical backup, each server protected consumes one physical backup license.

NOTE: Virtual and physical machine backup functions are licensed separately.

Trial license

You may evaluate vRanger using the trial license included with the product. The trial provides the following vRanger functionality:

- Virtual machine (VM) backup: 30 CPUs for 30 days
- VM replication: 30 CPUs for 30 days
- Physical machine backup: 10 physical machines for 30 days

To continue using vRanger past the trial period, you must purchase a license and import the new license key provided to you by Quest. If you do not receive your license key, visit https://support.quest.com/licensing-assistance.

Extended trial licenses

Sometimes, it may be necessary to expand the scope of a trial license (add more CPUs for replication for example), extend the duration of a trial, or test a new feature with an already licensed version of vRanger. Starting with vRanger 6.1, you may add an extended trial license to temporarily augment the duration or scope of your existing license.

When using an extended trial license, there are a few key points to remember:

- When applying an extended license over an existing or trial license, the highest license count is used.
- Extended trial licenses make all vRanger features available during the duration of the extended trial. For more information, see the table in vRanger licensing levels.
- When an extended trial license expires, or is removed, the primary license is applied.
- When applying an extended trial license, the list of licensed hosts and physical servers is not maintained. When the extended trial license expires or is removed, you may need to reconfigure host or server licensing to match your original configuration.

Single license limitation

vRanger is available in three versions: vRanger SE, vRanger Backup & Replication, and vReplicator. Outside of an extended trial period—for more information, see Extended trial licenses—only one version of vRanger can be licensed on a machine at any one time. For example, you cannot license vRanger SE and vReplicator on the same machine.

vRanger installation overview

A complete vRanger installation includes four components: the vRanger server, the vRanger database, the vRanger virtual appliances (VAs), and at least one repository. The following topics provide information on the options available for each component.

- Installing the vRanger server
- Installing the vRanger database
- Installing the vRanger virtual appliance (VA)
- Creating a vRanger repository
- Configuring vCenter permissions

Installing the vRanger server

vRanger can be installed either on a physical server or in a VM. As long as the vRanger machine meets the specifications detailed in System requirements and compatibility, application performance should be similar regardless of which option is chosen.

- **Virtual machine (VM)**: When installing vRanger in a VM, you eliminate the need for dedicated hardware while maintaining high performance. Due to the lower cost and increased flexibility, this approach is recommended. For information on installing in a VM, see Installing vRanger in a virtual machine (VM).
- **Physical machine**: The primary benefit of installing vRanger on a physical server is that the resource consumption of backup activity is off-loaded from the virtual environment to the physical proxy. For more information on installing on a physical server, see Installing vRanger on a physical server.

Regardless of which approach you chose, vRanger can leverage the vRanger VAs to perform backup, restore, and replication tasks. This option provides greater scalability while distributing the resource consumption of data protection activities across multiple hosts. For more information, see Installing the vRanger virtual appliance (VA).

Available backup transports

vRanger supports multiple data transport options for backup and restore tasks. The vRanger backup and restore wizards automatically selects the best transport option available based on your configuration. The available transports are:

- **VA-based HotAdd**: Mounts the source VM's disk to the vRanger VA deployed on the source host or cluster. This method allows vRanger to have direct access to the VM data through the VMware® I/O stack rather than the network.

  This method is the preferred transport method, and is available regardless of where vRanger is installed. The vRanger VA must be deployed to the source host or cluster for this transport to be available.

  > **NOTE:** If the host is not properly licensed, or the VA cannot access the storage for the source VM, HotAdd is not available. If a VA is configured and HotAdd is not available, a network backup is performed from the VA.

- **Machine-based HotAdd**: If vRanger is installed in a VM, this method mounts the source VM's disk to the vRanger VM. This method allows vRanger to have direct access to the VM data through the VMware I/O stack rather than the network. With this method, the backup processing activity occurs on the vRanger server.
- **VA-based LAN**: Transfers the source VM's data from the source disk to the vRanger VA over the network. With this method, the backup processing activity occurs on the vRanger VA.

- **Machine-based LAN**: If there is no vRanger VA deployed, vRanger transfers the source VM's data from the source disk to the vRanger machine over the network. With this method, the backup processing activity occurs on the vRanger server.
- **Machine-based SAN**: If there is no VA configured, vRanger determines whether the vRanger server is configured for SAN backups. This method is a high performance configuration that requires vRanger to be connected to your fibre or iSCSI network. In addition, the VMFS volumes containing the VMs to be protected must also be properly zoned and mapped to the vRanger server.

  NOTE: For machine-based transports, the "machine" referenced is the vRanger machine—physical or virtual.

  The transport method describes only how data is read from the source server, not how the data is sent to the repository.

Installing vRanger in a virtual machine (VM)

When vRanger is installed in a VM, you can perform backups and restores either over the network or in a LAN-free mode which uses the SCSI HotAdd functionality on VMware® ESXi™. The following topics provide a summary of each method. Replication and physical backup tasks are always performed over the network.

NOTE: The backup transport method describes only how data is read from the source server, not how the data is sent to the repository.

Available transports

The transports available when vRanger is installed in a VM include the following:

- With vRanger VA:
  - VA-based HotAdd
  - VA-based LAN
  - Machine-based HotAdd
  - Machine-based LAN
- Without the vRanger VA:
  - Machine-based HotAdd
  - Machine-based LAN

HotAdd backups (VMs only)

When vRanger is installed in a VM, LAN-free backups are made possible by the VMware® HotAdd disk transport.

During backups with HotAdd, the source VM's disks are mounted to the vRanger VM, allowing vRanger direct access to the VM's data through the VMware I/O stack. Backup processing occurs on the vRanger VM, with the data then being sent to the configured repository.

Requirements for a HotAdd configuration

To use vRanger with HotAdd, vRanger must meet the following requirements:

- vRanger must be installed in a VM, and that VM must be able to access the target VM's datastores.
- All hosts that the vRanger VM could be vMotioned to must be able to see the storage for all VMs that vRanger is configured to back up.
- You must use a version of VMware vSphere® that supports VMware vSphere Storage APIs - Data Protection (formerly known as vStorage APIs for Data Protection or VADP).

- When using vRanger with machine based HotAdd to backup encrypted VMs, the vRanger VM must also be encrypted.
- When using vRanger with VA-based HotAdd to backup and replicate encrypted VMs, the VA must also be encrypted.

Configuring vRanger for HotAdd

When using HotAdd, make sure to disable automount on the vRanger machine. This step prevents Windows® on the vRanger VM from assigning a drive letter to the target VMDK.

To configure vRanger for HotAdd:

1. Click **Start > Run**, and then enter **diskpart**.
2. To disable automatic drive letter assignment, run the **automount disable** command.
3. If you are using a SAN, verify that the SAN policy is set to Online All by typing **san** and pressing **Enter**.

   If it is not, set it to **online all** by typing **san policy=onlineAll**.
4. To clean any registry entries pertaining to volumes that were previously mounted, run the **automount scrub** command.

LAN backups

vRanger can perform LAN backups one of two ways—either through the vRanger machine, or by using the vRanger VA.

- **VA-based LAN:** This option transfers the source VM's data from the source disk to the vRanger VA over the network using the VMware® VDDK LAN transport. The backup processing activity occurs on the vRanger VA, and then the data is sent to the repository directly.
- **Machine-based LAN:** If there is no vRanger VA deployed, vRanger transfers the source VM's data from the source disk to the vRanger VM over the network. With this method, the backup processing activity occurs on the vRanger server. The backup data flows "direct to target" from the source server to the target repository, which means that the vRanger server does not process the backup traffic.

NOTE: Generally, this configuration yields the slowest performance, and should be avoided if possible. A better option is to deploy a VA to any VMware® ESXi™ servers, and use that VA for backup and restore tasks.

Considerations for installing vRanger in a VM

Read the following notes regarding limitations and considerations about installing vRanger in a VM:

- When installing vRanger in a VM, it is not supported to perform a machine-based backup of the vRanger VM. In other words, the vRanger VM cannot back itself up. You may, however, perform a VA-based backup of the vRanger VM.
- When using vRanger with machine based HotAdd to backup encrypted VMs, the vRanger VM must also be encrypted.

  When using vRanger with VA-based HotAdd to backup and replicate encrypted VMs, the VA must also be encrypted.
- When creating the VM for vRanger, Quest recommends that you create a fresh VM rather than cloning an existing VM or template.

  In recent versions of Windows®, volumes are recognized by a serial number assigned by Windows. When VMs are cloned, the serial number for each VM volume is cloned as well. During normal operations, this cloning is not an issue; however, when vRanger is cloned from the same source or template as a VM being backed up, the vRanger volume has the same serial number as the source volume.

For backup operations using HotAdd, source disk volumes are mounted to the vRanger VM. If the source VM volumes have the same disk serial number as the vRanger volume, which is the case with cloned VMs, the source VM's serial number is changed by Windows when mounted to the vRanger VM. When restoring from these backups, the boot manger does not have the expected serial number, causing the restored VM not to boot until the boot information is corrected.

Installing vRanger on a physical server

Installing vRanger on a physical server provides a method to off-load backup resource consumption from the VMware® ESXi™ host and network. While you can perform Machine-based LAN in this configuration, LAN-free backups are the primary driver for using vRanger in a physical server. For more information, see LAN-free backups (VM backups only) and LAN backups.

NOTE: With vRanger installed on a physical server, you can still take advantage of the vRanger VAs for backup, restore, and replication activity. For more information, see Installing the vRanger virtual appliance (VA).

Available transports

The transports available when vRanger is installed in a physical machine include the following:

- With vRanger VA:
  - VA-based HotAdd
  - VA-based LAN
  - Machine-based SAN
  - Machine-based LAN
- Without the vRanger VA:
  - Machine-based SAN
  - Machine-based LAN

LAN-free backups (VM backups only)

With vRanger installed on a physical machine, you may perform LAN-free backups with either the VA-Based HotAdd or Machine-based SAN transports.

- **VA-based HotAdd:** This transport mounts the source VM's disk to the vRanger VA deployed on the source host or cluster. This method allows vRanger—through the VA—to have direct access to the VM data through the VMware® I/O stack rather than the network. In this configuration, data is sent directly from the VA to the repository.

  This method is the recommended transport option due to the simplicity and flexibility of the configuration. To use this option, you must have a vRanger VA deployed on every host or cluster for which you want to configure backups. For more information on HotAdd, see Requirements for a HotAdd configuration.
- **Machine-based SAN:** This transport option uses your fibre-channel infrastructure or iSCSI network to transport backup data to the vRanger machine.

  To perform machine-based SAN backups, vRanger must be installed on a physical system attached to your SAN environment. This setup is a high performance configuration that requires vRanger to be connected to your fibre or iSCSI network. In addition, the VMFS volumes containing the VMs to be protected must also be properly zoned and mapped to the vRanger server.

Configuring vRanger for machine-based SAN backups

With vRanger installed on a physical server, the following configurations must be made:

- Disable automount on the vRanger machine:

  Click **Start > All Programs**, and enter **diskpart**.

  Run the **automount disable** command to disable automatic drive letter assignment.
- Run the **automount scrub** command to clean any registry entries pertaining to previously mounted volumes.
- On your storage device, zone your LUNs so that the vRanger HBA or iSCSI initiator can see and read them.
- Only one vRanger server should see a set of VMFS LUNs at one time. For backups only, The vRanger server should have only **read-only** access to the LUNs. To perform LAN-free restores, ensure that the vRanger server has **Read + Write** access to any zoned VMFS LUNs to which you want to restore.

LAN backups

vRanger can perform LAN backups one of two ways—either through the vRanger machine, or by using the vRanger VA.

- **VA-based LAN:** This option transfers the source VM's data from the source disk to the vRanger VA over the network using the VMware® VDDK LAN transport. The backup processing activity occurs on the vRanger VA, and then the data is sent to the repository directly.
- **Machine-based LAN:** If there is no vRanger VA deployed, vRanger transfers the source VM's data from the source disk to the vRanger machine over the network. With this method, the backup processing activity occurs on the vRanger server. The backup data flows "direct to target" from the source server to the target repository, which means that the vRanger server does not process the backup traffic.

NOTE: Generally, this configuration yields the slowest performance, and should be avoided if possible. A better option is to deploy a VA to any VMware® ESXi™ servers, and use that VA for backup and restore tasks.

Installing with other applications

Customers often want to install vRanger on the same server as another application. Due to the wide variety of factors that may affect performance, it is impossible to make blanket recommendations. Some key concerns to keep in mind:

- Many customers, to maximize their hardware investment, want to install vRanger on the same server as VMware® vCenter™. This practice is not recommended.
- During testing, many customers install vRanger with other Quest products. In this case, Quest does not recommend installing vRanger on the same machine as Quest Foglight.
- Only one version of vRanger may be installed on a machine at one time. For example, you may not install vRanger SE and vReplicator on the same machine.

Optimizing your network for backups

vRanger pushes much data through the network quickly. While this performance is good for minimizing your backup window, if not configured properly it can degrade your production network.

An important best practice is to separate the backup traffic from the production network by configuring a dedicated backup network.

NOTE: This approach requires that each VMware® ESXi™ host and the vRanger machine have two NICs installed.

1. Using the first (primary) network interface card (NIC), connect the vRanger server, the vRanger VAs, the VMware® vCenter™ Server, and Management Network of each ESXi server host to the production network.
2. Create a virtual switch, connecting it to a dedicated physical NIC on each ESXi host.

   This setup becomes the dedicated backup network.
3. On the vRanger server, each VA, and each repository, configure a second virtual NIC.
4. Connect this second NIC to the dedicated backup network.

Using NIC teaming

NIC teaming is a feature of VMware® Infrastructure that allows you to connect a single virtual switch to multiple physical Ethernet adapters. To utilize NIC teaming, two or more network adapters must be up-linked to a virtual switch. The main advantage of NIC teaming is increased network capacity for the virtual switch hosting the team.

When bonding NICs into a team, it is important to use NICs from the same vendor as different NIC vendors achieve bonding differently. When using teamed NICs with vRanger, it is critical that the NICs are teamed for performance rather than load balancing. vRanger backups are streamed as a continuous file—changing NICs during a data stream causes backup errors.

NOTE: For more information on NIC teaming, see VMware KB article 1004088.

Installing the vRanger database

vRanger utilizes a SQL Server® database to store application and task configuration data. The database can be either the embedded SQL Server Express instance—the default—or a SQL Server database running on your own SQL Server or SQL Server Express instance.

Database options

The database deployment occurs during the initial installation of vRanger. The default installs a SQL Server® Express database on the vRanger server. You can also install vRanger using a separate SQL Server instance. If you intend to use your own SQL Server instance and want to use the vRanger cataloging feature, the SQL Server instance must be installed on the vRanger server. For more information, see Installing the databases.

- **Default:** By default, the Installation Wizard uses the selection to install vRanger with the embedded SQL Server® 2014 SP3 Express database. The SQL Server Express database can only be installed on the vRanger server.

  NOTE: While the embedded SQL Server Express database is free and simple to install, there is a size limit of 10 GB per database.
- **External SQL Server Instance:** The Installation Wizard guides you through configuring vRanger with an external SQL Server® database. There is also an option in the Install Wizard to configure the database connection manually, but the guided approach is recommended.

  IMPORTANT: For a list of supported SQL Server database versions, see System requirements and compatibility.

Installing the databases

When installing vRanger, consider the database selection carefully as migrating from a SQL Server® Express installation to an external SQL Server database carries a risk of corrupting application data.

If you do ***not*** intend to use cataloging, to provide the most flexibility, Quest recommends that you install vRanger using an external SQL Server database server. This step allows you to relocate the vRanger installation simply by installing the application in another location, and pointing the Install Wizard to the existing database.

Sizing the catalog database

The vRanger catalog process collects and records metadata and path information for files updated since the last backup and catalog entry. Depending on the number of VMs protected, and the number of files in each VM, the catalog database may grow rapidly.

Actual database growth varies depending on the Guest OS and the number of files changed between backups, but the following information can be used as an approximate guide.

- With default filtering, the full catalog of a generic Windows Server® 2012 VM is approximately 500 files, or approximately 0.2 MB.

NOTE: Many Windows® files are not cataloged due to filtering; for more information about catalog filtering, see the *Quest vRanger User's Guide*. An amount of data equal to a standard Windows Server® 2012 installation results in a larger catalog footprint.

- Incremental and differential backups only catalog changed files, making the catalog record for these backups considerably smaller. Using incremental or differential backups, or both, allows you to store catalog data for many more savepoints than if you used only full backups.

Installing the vRanger virtual appliance (VA)

The vRanger VA can process backup and restore tasks in addition to replication tasks. This setup allows you to scale backup, restore, and replication activity across multiple hosts or clusters, while maintaining central scheduling and reporting control from a single vRanger server.

While the deployment and configuration of the VA are covered in the *Quest vRanger User's Guide*, the following information might help you understand the usage of the VA.

VA usage

The vRanger VA can be used to perform the following operations. For each of these operations, the processing activity occurs on the VA.

- Backup: network and LAN-free (HotAdd)
- Restore: network and LAN-free (HotAdd)
- Linux® file-level restore
- Replication

Deployment locations

The locations to which the vRanger VA or VAs should be deployed depend on the specifics of the virtual environment in question. Some general guidelines for VA deployment are:

- You may share a single VA among the hosts within a cluster. You may install a VA to some or all hosts within a cluster as well. If a VA is not detected on the host, vRanger determines whether the host is part of a cluster, and then if that cluster has a VA available.
- You must have a VA deployed on any VMware® ESXi™ host or cluster that is used for replication and backup. This requirement is true regardless of whether the host or cluster is used as the source or target of the replication task.
- When using the VA for replication, both the source and target host or cluster must use a VA.

NOTE: The vRanger VA is now bundled with vRanger, and can be found in: **C:\Program Files\Quest\vRanger**

Creating a vRanger repository

Designed for ease-of-use in recovery operations, repositories eliminate the need for countless backup locations and endless configurations. With vRanger, you can configure a repository once, and use it forever.

vRanger supports the following options for repository connections.

NOTE: Any storage device or appliance that supports CIFS or NFSv3 is expected to be compatible with vRanger.

- Common Internet File System (CIFS)
- Network File System (NFS) (version 3)
- NetVault SmartDisk
- EMC® Data Domain® Boost (DD Boost™)
- Quest DR Series Disk Backup Appliance (Quest Rapid Data Access [RDA])
- Quest QoreStor (Quest Rapid Data Access [RDA])

A repository is essentially a directory on a supported file system that vRanger uses to store savepoints—backup archives. When viewed from outside vRanger, through Windows® Explorer, for example, a repository consists of a configuration file—**GlobalManifest.metadata**—and directories for each savepoint.

Any time you add a repository in vRanger a **GlobalManifest.Metadata** XML file is created in the selected folder. It is the presence of that manifest file that tells vRanger that a repository exists in that folder.

Repository location, along with the configuration of jobs to those repositories, plays a significant role in the performance of vRanger. Use the following recommendations to aid on planning your repository configuration.

Repository storage devices

Slow disk performance has been shown to negatively impact the backup performance of vRanger. When configuring repositories, special attention should be paid to the type of storage devices used.

The use of SAS (Serial Attached SCSI) disk drives are recommended. SAS drives typically offer a 30% performance improvement over SATA drives.

The use of external USB drives or low quality NAS devices is not recommended. If these types of storage are used, the vRanger configuration settings must be adjusted to accommodate the slow devices. Recommended configuration settings for slower repositories are shown in the following list. These configurations can be made on the **vRanger Configuration Options** dialog box, available on the **Tools > Options** menu.

- Maximum number of tasks running off a LUN = **3**
- Maximum number of tasks running off a host = **1**
- Maximum number of tasks running per repository = **2**

If no errors are received with these settings, increment the tasks per repository value by 1 to find the best fit for your environment.

Bandwidth to repositories

While performance varies based on environmental factors, data throughput during a single backup task can reach up to 100 MB/s. If you assume a standard case of a repository connected by using a Gigabit network, as little as 10 concurrent jobs can saturate the link to that repository.

Although there is no ability to throttle data transmissions from a source server, vRanger can limit the number of simultaneous backup tasks on a per-repository level.

NOTE: This configuration is a global configuration, meaning that it applies to all repositories.

Repository size

There is no limit to the number of savepoints that can be stored in a vRanger repository. There are, however, environmental limits on the size of a single directory. The available options, and their limits, are described in the following list.

NOTE: The volume limitations described in this topic are limitations within the Windows® environment.

- **Default configuration**: A standard volume, with an MBR partition on a basic disk, has a limit of 2 TB. This configuration is the default for Windows Server® 2003. In this configuration, the vRanger repository cannot exceed 2 TB.
- **Dynamic disks**: Dynamic disks contain dynamic volumes, including simple volumes, spanned volumes, striped volumes, mirrored volumes, and RAID-5 volumes. A repository on dynamic disk volumes can be as large as 64 TB.
- **GPT volumes**: GUID partition table (GPT) volumes provide a more flexible mechanism for partitioning disks than the older Master Boot Record (MBR) partitioning scheme that has been common to PCs. GPT partitions are supported on Windows Server 2003, SP1 and later, and can reach up to 256 TB. For more information, see http://www.microsoft.com/whdc/device/storage/GPT_FAQ.mspx

Configuring vCenter permissions

vRanger requires a VMware® vCenter™ account to function properly. To comply with security best practices, Quest recommends creating a vCenter user account with the minimum required permissions for vRanger to use.

To create a vRanger user on vSphere 6 or later:

1. Navigate to **Administration > Roles**.
2. Select **Add Role**.
3. Enter a name for the role, such as **vRanger Non-Admin**.
4. In the **Privileges** section, set the permissions according to the following table:

Section	Privileges
Cryptographic operations	• Add disk • Direct Access • Encrypt • Encrypt New • Manage KMS • Manage encryption policies • Migrate
Datastore	• Allocate space • Browse datastore • Low level file operations • Remove file
Global	• • Licenses • Log event
Host > Local Operations	• Create virtual machine • Reconfigure virtual machine
Host > Inventory	• Modify Cluster
Network	• Assign network • Configure
Profile-driven storage	• Profile-driven storage view
Resource	• Assign vApp to resource pool • Assign virtualmachine to resource pool
vApp	• Add virtual machine • Assign resource pool • Create • Delete • Import • Move • Power Off • Power On • Rename
Virtual Machine > Configuration	• Select all privileges in this section
Virtual Machine > Interaction	• Configure CD media • Configure floppy media • Console interaction • Device connection • Power Off • Power On • VMware Tools Install
Virtual Machine > Inventory	• Create new • Remove •

Section	Privileges
Virtual Machine > Provisioning	• Allow disk access • Allow read-only disk access • Allow virtualmachine download • Allow virtualmachine files upload • Clone template •
Virtual Machine > Service Configuration	• Modify service configuration
Virtual Machine > Snapshot management	• • Select all privileges in this section

5 Navigate to the **Inventory** view.

6 Right-click the applicable level to grant user permission, such as the main vCenter level, and click **Add Permission**.

7 Add and locate the applicable user account, select the recently created User Role, and click **Add**.

8 Click **OK**.

NOTE: When you add the vCenter to the vRanger inventory, use this account for authentication.

3

System requirements and compatibility

- Requirements for the vRanger machine
- Supported platforms
- Feature-level requirements
- Configuration requirements
- Compatibility with other applications

Requirements for the vRanger machine

To maximize application performance, and to ensure error-free operation, you must ensure that the machine on which vRanger is installed meets the requirements as documented in this topic.

Requirements for the vRanger machine are divided among these topics:

- Minimum hardware requirements
- Supported operating systems for installation

Review each of these topics thoroughly before installing vRanger.

NOTE: For LAN-free and HotAdd installation requirements, see Physical backup and restore.

Minimum hardware requirements

The minimum hardware requirements to run vRanger can vary widely based on several factors. Therefore, you should not do a large-scale implementation without first completing a scoping and sizing exercise.

vRanger: physical machine

The following describes the hardware recommendations for the vRanger physical machine:

Table 1. Requirements for a installing vRanger on a physical machine

CPU	Any combination equaling four cores of CPUs are recommended. Example one quad-core CPU; two dual-core CPUs.
RAM	4 GB RAM is required.
Storage	At least 4 GB free hard disk space on the vRanger machine.
HBA	For LAN-free, Quest recommends that you use two HBAs—one for read operations and one for writing.

vRanger: virtual machine (VM)

The following describes the hardware recommendations for using vRanger in a VM:

Table 2. Requirements for a installing vRanger on a virtual machine

CPU	Four vCPUs.
RAM	4 GB RAM is recommended.
Storage	At least 4 GB free hard disk space on the vRanger machine.

Requirements for physical backup and restore

When backing up from and restoring to a physical server, vRanger uses a client run on that server to perform backup and restore operations. To process the backup workload effectively, the physical server must meet the following requirements:

Table 3. Requirements for physical backup and restore

CPU	Any combination equaling four cores of CPUs are recommended. Example one quad-core CPU; two dual-core CPUs.
RAM	2 GB RAM is required.

Supported operating systems for installation

The following operating systems are supported for installation of vRanger.

Table 4. Supported operating systems

Operating system	Service pack level	Bit level
Windows Server 2012[b]	All service packs	x64
Windows Server 2012 R2[ba]	All service packs	x64
Windows Server 2016[b]	All service packs	x64
Windows Server 2019[b]	All service packs	x64
Windows Server 2022[b]	All service packs	x64
Windows Server 2025	All service packs	x64

a. Before installing vRanger on Windows Server 2012 R2, the updates listed in Additional required software must be installed.

Additional required software

In addition to a supported version of Windows® and a supported VMware® Infrastructure, you may need some additional software components, depending on your configuration.

- **Microsoft® .NET Framework**: vRanger requires the .NET Framework 4.5. The vRanger installer installs it if not detected.
- **SQL Server**: [Optional] vRanger utilizes two SQL Server® databases for application functionality. vRanger can install a local version of SQL Express 2019 SP3 or you can choose to install the vRanger databases on your own SQL instance.
- **Windows PowerShell 3 or above.**If you are installing vRanger on Windows 2008 R2 SP1, you will need to install Windows PowerShell 3 or above before installing vRanger

- **vRanger virtual appliance (VA)**: The vRanger VA is a small, pre-packaged Linux® distribution that serves as a platform for vRanger operations away from the vRanger server. vRanger uses the VA for the following functions:
  - Replication to and from VMware® ESXi™ hosts.
  - File-level restore (FLR) from Linux machines.
  - Optionally for backups and restores.
- **Updates for Windows Server 2012 R2**: Before installing vRanger on Windows Server 2012 R2, ensure that the Windows updates listed below are installed:
  - KB2939087
  - KB2975061
  - KB2919355
  - KB2999226

Supported SQL Server versions

The default is to install vRanger with the SQL Server® Express 2014 SP3 database, but you may use your own SQL Server instance if you prefer.

If you chose to use your own SQL Server instance, and want to use the vRanger Cataloging function, you must install the SQL Server instance on the vRanger server as the Catalog database must be local to vRanger. The following versions of Microsoft SQL Server are supported by vRanger.

Table 5. Supported versions of SQL Server

Version	Service pack level
SQL Server 2012 (all editions)	All service packs
SQL Server 2014 Express (embedded option)	SP 3
SQL Server 2014 (all editions)	All service packs
SQL Server 2016 (all editions)	All service packs
SQL Server 2017 (all editions)	All service packs
SQL Server 2019 (all editions)	All service packs

Supported platforms

The following topics list the platforms and operating systems supported for backup, restore, and replication operations.

Supported vSphere versions

vRanger supports backup, restore, and replication operations against the following versions of VMware® Infrastructure:

Table 6. vSphere versions

Component	Supported versions
VMware® ESXi™	• 7.0 • 7.0.2 • 7.0.3 • 8.0 • 8.0.1 • 8.0.2 • 8.0.3 **NOTE:** ESXi replication requires the use of the vRanger virtual appliance (VA).
VMware® vCenter™	• 7.0 • 7.0.2 • 7.0.3 • 8.0 • 8.0.1 • 8.0.2 • 8.0.3
VMware® vSphere® license	vRanger supports vSphere editions except for the free versions of ESXi. The free versions do not provide the necessary APIs for vRanger to function.

Equivalent version support policy

In addition to what is listed in this document, vRanger supports VMware® versions where the following criteria have been met:

NOTE: The naming convention used in this policy topic follows the standard product release version scheme of Major.Minor.Update.Patch.

- VMware updates or patches to a supported major or minor release are also supported, unless otherwise stated.
- Major or minor versions that are newer than what is listed in this documentation are not supported and require a separate qualification effort, unless otherwise stated.

vRanger and VM snapshots

The vRanger backup and replication functionality requires the ability to create a snapshot. In certain circumstances, the creation of VM snapshots is not supported by VMware®. In these cases, backup and replication of these VMs or disks is not possible. Some common examples are:

- RDM Disks in physical compatibility mode
- Disks in independent mode
- Fault-tolerant VMs

NOTE: This list is not exhaustive. Any configuration in which snapshots are not supported by VMware, or not possible, is not supported by vRanger.

Supported Hyper-V versions

vRanger supports backup and restore operations against the following versions of Hyper-V® Server:

Table 7. Hyper-V versions

Component	Supported versions
Hyper-V Servers	Windows Server 2012 Full Server and Server Core Windows Server 2012 R2 Full Server and Server Core Windows Server 2016 Full Server and Server Core Windows Server 2019 Full Server Windows Server 2022 Full Server Windows Server 2025 Full Server
System Center Virtual Machine Manager (VMM)	Windows Server 2012 Full Server and Server Core Windows Server 2012 R2 Full Server and Server Core Windows Server 2016 Full Server and Server Core
Support for Microsoft Storage Spaces Direct (S2D)[a]	Windows Server 2019 Full Server

a. Microsoft Storage Spaces Direct (S2D) is supported in virtual environments only.

Supported platforms for physical machine backup

vRanger supports backup and restore operations against the following operating systems:

Table 8. Supported platforms

Operating system	Bit level
Windows Server 2008 R2 SP1 and above	x64
Windows Server 2012	x64
Windows Server 2012 R2	x64
Windows Server 2016	x64
Windows Server 2019	x64
Windows Server 2022	x64
Windows Server 2025	x64

Supported virtual appliance (VA) versions

vRanger 7.8.7 supports VA 7.6.3 or later.

IMPORTANT: For more information on upgrading your virtual appliance to the latest version, see Upgrading the vRanger virtual appliance (VA).

Supported disk types and file systems

The following topics list the disk types and file systems supported by vRanger.

Supported disk types

The following table details the support status of the listed disk types for the documented vRanger functions.

Table 9. Supported disk types

Disk types	Backup and restore	Catalog	File-level restore (FLR)
Windows® virtual machines (VMs)			
MBR	Supported	Supported	Supported
GPT	Supported	Supported	Supported[a]
Dynamic	Supported	Not supported	Not supported
Windows physical machines			
MBR	Supported	Supported	Supported
GPT	Supported	Supported	Supported[a]
Dynamic	Not supported	Not supported	Not supported
Linux® virtual machines (VMs)[b]			
LVM	Supported	Not supported	Supported
MBR	Supported	Not supported	Not supported
GPT	Supported	Not supported	Supported
Dynamic	Supported	Not supported	Not supported

a. FLR supported for 2012 or later systems only when performing FLR on 2012 or newer systems. Older systems may not show data on GPT disks.

b. FLR for Hyper-V® Linux VMs is not supported.

Supported file systems

The following table details the support status of the listed file systems for the documented vRanger functions.

Table 10. Supported file systems

File system types	Backup and restore	Catalog	File-level restore (FLR)
Windows® virtual machines (VMs)			
NTFS	Supported	Supported	Supported
FAT32	Supported	Not supported	Not supported
exFAT	Supported	Not supported	Not supported
ReiserFS[a]	Supported	Not supported	Supported[ab]
Windows physical machines			
NTFS	Supported	Supported	Supported
FAT32	Supported	Not supported	Not supported
exFAT	Supported	Not supported	Not supported
ReiserFS[a]	Supported	Not supported	Supported[ab]
Linux® virtual machines (VMs)			
ext2	Supported	Not supported	Supported
ext3	Supported	Not supported	Supported
ext4	Supported	Not supported	Supported
JFS	Supported	Not supported	Supported
XFS	Supported	Not supported	Supported

Table 10. Supported file systems

File system types	Backup and restore	Catalog	File-level restore (FLR)
ReiserFS	Supported	Not supported	Supported
LVM (one physical disk)	Supported	Not supported	Supported

a. FLR is not supported on ReFS on Windows Server 2019.
b. FLR supported for 2012 and 2016 systems only when performing FLR on 2012 or 2016 systems.

Feature-level requirements

Some vRanger features and functions have requirements or limitations that do not apply to the rest of the product. Review this list to ensure that all requirements are understood. The features and functions described here are:

- Standard backup, restore, and replication
- Physical backup and restore
- HotAdd
- File-level restore (FLR): Windows
- FLR: Linux
- Microsoft Volume Shadow Copy Service (VSS)

Standard backup, restore, and replication

For basic backup and replication functions, vRanger supports any Guest OS that is supported by VMware. For a complete list, see the VMware *Guest Operating System Installation Guide*.

For advanced functions, such as file-level restore (FLR) or additional application consistency, see the requirements in the following topics:

- File-level restore (FLR): Windows
- FLR: Linux
- Microsoft Volume Shadow Copy Service (VSS)

Additional replication requirements

The following limitations and requirements apply to replication:

- vRanger replication does not operate with servers that are behind a network address translation (NAT) firewall. To replicate through a NAT firewall properly, you must have an IP tunnel in place between two NATed subnets. Contact your ISP provider to see if this option is available to you.
- The VM hardware cannot be changed during replication. For this reason, the VM must be at a hardware version level that is compatible with both the source and target servers. The VMware® ESXi™ version of the source and target hosts does not matter, as long as the VM hardware is supported on both ESXi versions. For more information on VM hardware versions and compatibility, see the VMware documentation at https://www.vmware.com/support/pubs/.
- A continuous connection between source and target sites is required when replication is taking place.
- Excessive network packet loss could result in replication failure. Replication does work with links having average packet loss of less than 2%. Replication is not designed to work in replication environments where packet loss exceeds commercially accepted limits.
- Networks having 99% uptime and availability generally provide for good Replication performance.

Physical backup and restore

- Ensure that the physical server is running a supported operating system. Refer to Supported platforms for physical machine backup for more information.
- Ensure that the physical server is not booting into UEFI. The vRanger Boot CD does not support UEFI.

HotAdd

To perform backup/restore/replication tasks using HotAdd, vRanger must be installed on a VM. Also:

- HotAdd only works on SCSI and SATA disks. IDE disks and vRDMs are not supported.
- Datastores for the target VMs must be accessible to the vRanger VM.
- vRanger can only perform operations on VMs within the same data center.
- HotAdd cannot be used if the VMFS block size of the datastore containing the VM folder for the target VM does not match the VMFS block size of the datastore containing the vRanger VM. For example, if you back up a virtual disk on a datastore with 1 MB blocks, the proxy must also be on a datastore with 1 MB blocks.
- Backing up thick disk requires the maximum disk size to be available. When backing up a thick disk, the vRanger VM's datastore must have at least as much space available as the maximum configured disk size for the VM to be backed up.
- When using vRanger with machine based HotAdd to backup encrypted VMs, the vRanger VM must also be encrypted.
- When using vRanger with VA-based HotAdd to backup and replicate encrypted VMs, the VA must also be encrypted.

File-level restore (FLR): Windows

To perform FLR from a Windows® VM, the VM must be a supported disk type. For more information, see Supported disk types.

FLR: Linux

Review the following information to understand the functions and limitations of the vRanger Linux® FLR feature.

- Linux FLR requires the vRanger VA.
- vRanger requires you to recover the Linux files to an intermediate Windows® machine. When you recover Linux files to a Windows machine, you lose the file permissions.
- The source VM properties need to show the operating system (OS) type as Linux. If this feature is not configured properly, vRanger cannot identify the savepoint as a Linux VM.
- For a list of supported file systems, see Supported disk types and file systems.

Configuration requirements

HotAdd disk requirements

When using the HotAdd transport, the following disk restrictions and requirements apply.

- HotAdd only works on SCSI and SATA disks. IDE disks and vRDMs are not supported.
- HotAdd cannot be used if the VMFS block size of the datastore containing the VM folder for the target VM does not match the VMFS block size of the datastore containing the vRanger VM. For example, if you back up a virtual disk on a datastore with 1 MB blocks, the proxy must also be on a datastore with 1 MB blocks.

Password security setting policy

Weak passwords compromise system security. When you create and update passwords in vRanger, follow as many of these guidelines as your environment allows:

- A password should not include a significant portion of a user or account name. A password should be at least six characters long and should contain several characters from these categories:
  - Uppercase letters in English—A to Z
  - Lowercase letters in English—a to z
  - Digits—0 to 9
  - Non-alphabetic characters—for example, $, !, #, %

Port requirements

The following table lists the ports used by each of the vRanger components.

Table 11. Ports

Port number	Protocol	Direction
22	TCP	vRanger to VMware® ESXi™ Host vRanger to VA VA to VA
53	TCP	vRanger/VA/ESXi Host to DNS Server
135	TCP	vRanger server to guest VM. Used for push install of vRanger VSS tools.
137	TCP	vRanger/VA/ESXi Host to CIFS Repository
137	UDP	vRanger/VA/ESXi Host to CIFS Repository
138	UDP	vRanger/VA/ESXi Host to CIFS Repository
139	TCP	vRanger/VA/ESXi Host to CIFS Repository
443	TCP	vRanger and VA to ESXi hosts vRanger and VA to VMware® vCenter™
445	TCP	vRanger/VA/ESXi Host to CIFS Repository vRanger to VA
445	TCP	vRanger server to guest VM. Used for push install of vRanger VSS tools.

Table 11. Ports

Port number	Protocol	Direction
902	TCP	vRanger to Hosts VA to Hosts
2049	TCP	vRanger/VA/ESXi Host to NFS Repository
2049	UDP	vRanger/VA/ESXi Host to NFS Repository
37453	TCP	vRanger/VA/ESXi Host to NetVault SmartDisk Repository
10011	TCP	RDA Control Channel
11000	TCP	RDA Data Channel
49152-65535 (Dynamic Port Range)	TCP	vRanger server to guest VM. Used for push install of vRanger VSS tools.
51000	TCP	Physical Backup: vRanger to physical server

Additional port requirements

- For the VA designated for Linux® FLR, the firewall must be configured to allow ICMP (ping) packets.
- For physical backups to function correctly, the firewall must be configured to allow WMI connections.

Compatibility with other applications

vRanger can be used with various applications to provide additional functionality. The following table summarizes which applications are supported by the most recent versions of vRanger.

Table 12. Compatibility

Company	Application	Application version	vRanger version								Support details
			7.6.3	7.6.4	7.6.5	7.6.6	7.7	7.7.1	7.8	7.8.7	
Quest	NetVault SmartDisk	2.0.1									
		10.0	X								
		11.4.5		X	X	X	X	X	X	X	
	QoreStor	For QoreStor and vRanger interoperability information, please refer to the *QoreStor Interoperability Guide*.									
EMC®	DD OS[a]	7.2							X	X	
		7.7							X	X	
		7.10							X	X	
		7.13							X	X	
		8.3								X	
		8.6								X	

a. Data Domain® operating system

Microsoft Volume Shadow Copy Service (VSS)

vRanger uses the Microsoft Volume Shadow Copy Service (VSS) to provide application consistency. To leverage VSS, the following conditions must be met:

The source server must be running an operating system that supports VSS quiescing. The following lists the supported guest operating systems:

- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

  NOTE: As per VMware KB article 60395, quiescing is not supported for Windows Server 2019.

- Windows Server 2022
- Windows Server 2025

- For application consistency, the application must support VSS quiescing. As shown in the following table, application consistency is not always available with the basic quiescing options. In these situations, you may use the vRanger VSS Tools for application-level consistency.

Table 13. File-level quiescing

Server version	ESXi 7.0	ESXi 8.0
Windows Server 2012 **Windows Server 2012 R2**	VMware VSS	VMware VSS
Windows Server 2016	VMware VSS	VMware VSS
Windows Server 2019	VMware VSS	VMware VSS
Windows Server 2022	VMware VSS	VMware VSS
Windows Server 2025	VMware VSS	VMware VSS

Table 14. Application-level quiescing

Server version	ESXi 7.0	ESXi 8.0
Windows Server 2012 **Windows Server 2012 R2**	VMware VSS	VMware VSS
Windows Server 2016	VMware VSS	VMware VSS
Windows Server 2019	VMware VSS	VMware VSS
Windows Server 2022	VMware VSS	VMware VSS
Windows Server 2025	VMware VSS	VMware VSS

IMPORTANT: Application-consistent backups and replications are not available for encrypted VMs.

4

Installing vRanger

- vRanger installation overview
- Installing vRanger
- Installing the vRanger Catalog Service later

vRanger installation overview

This version of the software can be installed on a physical or virtual machine (VM). When you complete one of these processes, three services are installed: Quest vRanger Service, Quest vRanger API Service, and Quest vRanger File Level Restore Service. The optional Quest vRanger Catalog Service may also be installed, based on your selections.

You need the following to install vRanger:

- A physical machine or VM to host the installation.
- Administrator access to the machine on which the software is installed.

Installing vRanger

The processes described in the following topics assume that you have already downloaded the vRanger software and saved it to an accessible location.

- Setting up vRanger
- Entering vRanger service credentials
- Installing the vRanger database
- Entering vRanger database runtime credentials
- Installing the vRanger Catalog Service
- Completing the installation

Setting up vRanger

1. Double-click the vRanger installation executable.
2. When the **vRanger Backup & Replication** dialog box appears, select the language for the interface from the **Language** list, and click **Next**.

   NOTE: This setting applies to both the vRanger installation process and the product interface.

3. When the **License Agreement** dialog box appears, read the license terms, accept the agreement, and click **Next**.

Entering vRanger service credentials

The **vRanger Services Information** dialog box appears. Use this dialog box to configure the credentials that are used to run the services installed by vRanger.

CAUTION: The user account needed for this step must have administrator privileges on the vRanger machine.

1. In the **Domain** field, enter the domain in which the user account is located.

   To use an account on the local machine, leave this field blank.

2. In the **Username** field, enter the username for the account.

   IMPORTANT: If you choose to install the Quest vRanger Service with an account other than the account with which you are currently logged in, select **Mixed-Mode** authentication when installing the vRanger database.

3. In the **Password** field, enter the password for the account.
4. In the **Choose Components** dialog box, click **Next**.

Installing the vRanger database

vRanger utilizes a SQL Server® database to store application and task configuration data. The database can be either the embedded SQL Server Express instance—the default—or a SQL Server database running on your own SQL Server or SQL Server Express instance. For more information on the vRanger database and configuration options, see Installing the vRanger database.

NOTE: This step is omitted if an existing SQL Server instance is detected.

1. When the **vRanger Database Installation** dialog box appears, do one of the following:
   - To proceed with the default, leave **Install a new local instance of SQL Server Express** selected, and proceed to Step 3.
   - To install vRanger on an existing SQL Server instance, clear **Install a new local instance of SQL Server Express**, and click **Next**.
2. Select a server authentication mode:
   - **Windows authentication mode:** When a user connects through a Windows® user account, SQL Server validates the account name and password using information in the Windows operating system. Windows Authentication uses Kerberos security protocol, provides password policy enforcement (complexity validation for strong passwords), supports account lockout, and supports password expiration.
   - **Mixed Mode (SQL Server and Windows authentication and SQL Server Authentication):** Enter and confirm the system administrator (sa) password when you select Mixed Mode authentication. Setting strong passwords is essential to the security of your system. Never set a blank or weak sa password.

     IMPORTANT: If you chose an account for the Quest vRanger Service installation other than the account with which you are currently logged in, select **Mixed Mode**.

   If you selected **Mixed Mode**, you are prompted to enter a password for the system administrator (sa) account. If you selected **Windows authentication mode**, the installation continues using the account specified in Entering vRanger service credentials.
3. Click **Next.**

Entering vRanger database runtime credentials

The **vRanger Database Runtime Credentials** dialog box appears. This dialog box allows you to configure different credentials for database installation and for normal runtime operations. In addition, this dialog box is where you configure a connection to an existing SQL Server® database.

1 To select an external database, select the server and database name in the drop-down lists.

> **TIP:** If the applicable server is not visible, click the refresh icon to perform another discovery.

When using an external SQL Server, ensure that the following configurations are made.

- The external SQL Server must have **Named Pipes** and **TCP/IP** enabled in SQL Server Configuration Manager. **Named Pipes** is found under **SQL Server Network Configuration**, while **TCP/IP** is under **Protocols for Database_Instance_Name**. If you update these settings, restart SQL Server.
- SQL Server Browser services must be running for vRanger to discover the external database.

2 Configure the credentials for your database installation and connection as follows:

- **Database Installation Credentials**: If you select **Windows**, the database installs using the credentials chosen in Entering vRanger service credentials. If you are using SQL Server authentication, the credentials used must have administrative privileges on the SQL Server instance.
- **Runtime DB Connection Credentials**: You may choose different credentials for use during normal vRanger operations.
  - If you select **Windows**, the database installs using the credentials chosen in Entering vRanger service credentials.
  - If you select **SQL Server**, enter and confirm the system administrator (sa) password when you select Mixed Mode authentication. Setting strong passwords is essential to the security of your system. Never set a blank or weak sa password.

3 Click **Next**.

Installing the vRanger Catalog Service

The Quest vRanger Catalog Service provides a searchable catalog of files in cataloged backups. This feature enables faster searches during FLR.

1 When the **vRanger Catalog Service** dialog box appears, do one of the following:

- To install the Catalog Service, select **Install vRanger Catalog Service**.
- To proceed without installing the Catalog Service, clear the check box, click **Next**, and proceed to Completing the installation.

> **NOTE:** If you have previously installed the Catalog Service, you cannot clear the check box.

2 Choose the credentials to use for the database installation.

Select **Use the same credentials as vRanger Database**, or configure the credentials for the Catalog database per the following options:

- **Database Installation Credentials**: If you select **Windows**, the database installs using the credentials chosen in Entering vRanger service credentials. If you are using SQL Server® authentication, the credentials used must have administrative privileges on the SQL Server instance.
- **Runtime DB Connection Credentials**: You may choose different credentials for use during normal vRanger operations.

- If you select **Windows**, the database installs using the credentials chosen in Entering vRanger service credentials.
- If you select **SQL Server**, enter the credentials for vRanger to use when connecting to the vRanger database. If the account entered does not exist, it is created.

3 Click **Next**.

Completing the installation

The **Ready to Install** dialog box appears.

1 Review and confirm your selected configurations.

2 To change any configuration, click **Back**; to continue, click **Install**.

3 After the installation is complete, click **Finish**.

> **NOTE:** For procedures on completing the vRanger Startup Wizard or performing other configurations, see the *Quest vRanger User's Guide*.

Installing the vRanger Catalog Service later

If you want to install the Catalog Manager after vRanger Backup & Replication is already installed, you may modify your installation with the standard vRanger installer.

1 Double-click the installer file.

2 When the Setup Wizard appears, select **Modify the installation**, and click **Next**.

3 Click **Next** to proceed through the **vRanger Services Information and vRanger Database Runtime Credentials** dialog box.

4 When the **vRanger Catalog Service** dialog box appears, select **Install vRanger Catalog Service**, and click **Next**.

5 Choose the credentials to use for the database installation.

Select **Use the same credentials as vRanger Database**, or configure the credentials for the Catalog database per the following options:

- **Database Installation Credentials**: If you select **Windows**, the database installs using the credentials chosen in Entering vRanger service credentials. If you are using SQL Server® authentication, the credentials used must have administrative privileges on the SQL Server instance.
- **Runtime DB Connection Credentials**: You may choose different credentials for use during normal vRanger operations.
  - If you select **Windows**, the database installs using the credentials chosen in Entering vRanger service credentials.
  - If you select **SQL Server**, enter the credentials for vRanger to use when connecting to the vRanger database. If the account entered does not exist, it is created.

6 Click **Next**.

7 When the **Ready to Install** dialog box appears, click **Install**.

5

Upgrading vRanger

- Before upgrading vRanger
- Backing up the vRanger database
- Upgrading a previous vRanger installation
- Upgrading the vRanger Database
- Upgrading the vRanger virtual appliance (VA)
- Upgrading a previous vReplicator installation

Before upgrading vRanger

Before you upgrade an existing vRanger installation, review the following topics for important information.

- Deprecated repository types
- vRanger editions
- Upgrading a previous vRanger installation

Deprecated repository types

Starting with vRanger 7.6, FTP and SFTP repositories will not be supported. If your existing vRanger installation has either of these repository types configured, the upgrade will not proceed. To upgrade, you will need to:

- [Optional] Migrate content from existing FTP and SFTP repositories to a supported repository type.
- Remove the FTP and/or SFTP repository from vRanger.
- Run the vRanger 7.6 installer to upgrade.
- Edit any existing backup jobs for FTP or SFTP repositories and configure the jobs to use one of the supported repository types

Migrating content from an FTP or SFTP repository

You can migrate content from one repository (or repository type) to another simply by copying the repository contents to the new location.

To migrate a repository:

1. For each repository, identify the GlobalManifest.metadata file. This file serves as a master index to the repository contents. Ensure that this file is moved to the new repository along with the savepoint data.
2. Using the file transfer method of your choice, copy all of these files to the new repository location.
3. Remove the FTP or SFTP repository from vRanger.

   IMPORTANT: Do not select **Delete all savepoints in this repository.** By not selecting this option, you will remove the repository from vRanger but maintain the data in the repository location.

4 When all FTP and SFTP repositories are removed, you will be able to upgrade vRanger to the latest version.

5 When the upgrade is completed, you can add the new repository to vRanger. Refer to the instructions in the “Configuration” chapter of the *vRanger User’s Guide* if necessary.

> **NOTE:** When adding the new repository, you will be prompted with the options to Import as Read-Only, Import, or Overwrite. Select **Import.**

6 Please note that the imported savepoints will not be linked to any backup jobs. You will need to edit existing backup jobs to point to the new repository as required.

vRanger editions

With replication now integrated into vRanger, and vRanger being offered in multiple versions, there are several upgrade options available.

- **Current vRanger customers**: See Upgrading a previous vRanger installation.
- **Current vReplicator customers**: See Upgrading a previous vReplicator installation.
- **Customers of both vRanger and vReplicator**: The upgrade procedures differ depending on whether you want to manage replication from the disaster recovery (DR) site, or combine backup and replication management on the production site.
  - **DR site**: If you want to manage replication from the DR site to ease failover, follow both of the preceding procedures, upgrading the vRanger installation on the production side and the vReplicator installation on the DR site. You may use a combined license file for both installations, if the combined CPU count for each protection type—backup and replication—for both sites does not exceed the total licensed number of CPUs.
  - **Production site**: When both backup and replication are managed from the production site, start with Upgrading a previous vRanger installation, and skip to Step 4 of the Upgrading a previous vReplicator installation procedures.

If you purchase vRanger SE, you can purchase an upgrade to vRanger Backup & Replication. Similarly, you can also purchase an upgrade from vReplicator 5.0 to vRanger Backup & Replication 7.8.7.

Supported upgrade paths

Due to architectural differences, a direct upgrade to vRanger 7.8.7 from older vRanger versions may not be possible.

- **Supported for direct upgrade**: If you are using one of the following vRanger versions, you may upgrade directly to vRanger 7.8.7.
  - vRanger 7.7
  - vRanger 7.7.1
  - vRanger 7.8.0
  - vRanger 7.8.2
  - vRanger 7.8.3
  - vRanger 7.8.4
  - vRanger 7.8.5
  - vRanger 7.8.6
- **Requires intermediate upgrade**: The following versions are not supported for direct upgrade to vRanger 7.8.7. If you are using one of these versions, you must first upgrade to vRanger 7.6.x before upgrading to the latest version.
  - vRanger 7.2.x

- vRanger 7.3.x
- vRanger 7.5.x

Backing up the vRanger database

vRanger utilizes a SQL Server® database to store application and task configuration data. The database can be either the embedded SQL Server Express instance—the default—or a SQL Server database running on your own SQL Server or SQL Server Express instance. If you want to back up the SQL Server database before installing an upgrade, you must use SQL Server Management Studio.

1. Start SQL Server Management Studio, and log in using either the system administrator (sa) or Windows credentials.
2. Expand the list of databases.
3. Right-click **vRangerPro Database**, select **Tasks**, and then select **Backup**.
4. In the **Back Up Database Wizard**, verify that the **Disk** option is selected in the **Destination** section.
5. If you need to point to a different destination, complete the following steps:
    a. Click **Add**.
    b. Verify that the default path to the SQL Server backup folder is acceptable; if not, point to a different location.
    c. After identifying the applicable path, enter **vRangerPro.bak** after the last backward slash in the path name, and click **OK**.
6. To run the backup process for the database, click **OK**.
7. To verify that the backup was created, go to the selected location, and look for the **vRangerPro.bak** file.

Upgrading a previous vRanger installation

You may upgrade a previous vRanger installation to the latest version by running the standard vRanger installer. For information on which versions of vRanger are supported for upgrade, see Supported upgrade paths.

NOTE: Starting with vRanger 7.0, there is no longer a separate installer for upgrades.

Upgrade from Beta versions is not supported, nor is operating a GA version in parallel with a Beta version. The Beta version must be uninstalled before upgrading a previous GA version or performing a full installation.

NOTE: Quest recommends that you back up your vRanger database before upgrading the application.

To upgrade a vRanger installation:

1. Double-click the vRanger installation executable.
2. When the **vRanger Backup & Replication** dialog box appears, select the language for the interface from the **Language** list, and click **Next**.

    NOTE: This setting applies to both the vRanger installation process and the product interface.

3. When the **License Agreement** dialog box appears, read the license terms, accept the agreement, and click **Next**.

4 When the **vRanger Services Information** dialog box appears, enter the credentials you want to use to run the services installed by vRanger.

CAUTION: The user account needed for this step must have administrator privileges on the vRanger machine.

- In the **Domain** field, enter the domain in which the user account is located.
- In the **Username** field, enter the username for the account.
- In the **Password** field, enter the password for the account.

5 Click **Next**.

The **vRanger Database Runtime Credentials** dialog box appears. This dialog box allows you to configure different credentials for database installation and for normal runtime operations. In addition, this dialog box is where you configure a connection to an existing SQL Server® database.

6 To select an external database, select the server and database name in the drop-down lists.

TIP: If the applicable server is not visible, click the refresh icon to perform another discovery.

7 Configure the credentials for your database installation and connection as follows:

- **Database Installation Credentials**: If you select **Windows**, the database installs using the credentials chosen in Entering vRanger service credentials. If you are using SQL Server authentication, the credentials used must have administrative privileges on the SQL Server instance.
- **Runtime DB Connection Credentials**: You may choose different credentials for use during normal vRanger operations.
  - If you select **Windows**, the database installs using the credentials chosen in Entering vRanger service credentials.
  - If you select **SQL Server**, enter and confirm the system administrator (sa) password when you select Mixed Mode authentication. Setting strong passwords is essential to the security of your system. Never set a blank or weak sa password.

8 When the **vRanger Catalog Service** dialog box appears, do one of the following:

- To install the Catalog Service, select **Install vRanger Catalog Service**.
- To proceed without installing the Catalog Service, clear the check box, and proceed to Step 9.

NOTE: If you have previously installed the Catalog Service, you cannot clear the check box.

9 Click **Next**.

10 When the **Ready to Install** dialog box appears, click **Install**.

11 After the installation is complete, click **Finish**.

Updating the VSS Tools

Starting with vRanger 7.6.3, the path to required files has changed. Upgrading from a version of vRanger prior to 7.6.3 requires a refresh of the VSS Tools on each VM for which they are configured.

To update the VSS Tools:

1 When viewing the **My Inventory View**, right-click the preferred VM, and select **Configure VSS Tools**.

2 When the **Configure VSS Tools** dialog box appears, enter the name and password for an account with administrative privileges on the VM, and click **Next**.

If the selected VM has more than one disk, the available disks are shown in the **Disk for VSS snapshot section**.

3 Select the disks to quiesce.

4 If preferred, select **Perform application log truncation**.

5 Click **Configure**, and click **Next**.

vRanger performs the following actions:

- Creates the **C:\Program Files\Quest\vRanger\vzShadow** directory, and populates the directory with the **vzShadow** executable and supporting files.
- Creates the **C:\Program Files\VMware\VMware Tools\backupscripts.d** directory, and creates a **freeze.bat** file in that directory that contains the appropriate contents based on your selections.

Upgrading the vRanger Database

Starting with vRanger 7.8.7, the embedded vRanger database version has been changed to SQL Server 2019 SP3 Express. Follow the procedures below to upgrade your vRanger database.

Performing a database upgrade

In order to upgrade the vRanger database, perform the steps described below.

Prerequisites

- Back up all SQL Server database files from the SQL Server instance to be upgraded. Refer to Backing up the vRanger database for more information.
- Run the appropriate Database Console Commands (DBCC) on databases to be upgraded to ensure that they are in a consistent state.
- Estimate the disk space that is required to upgrade SQL Server components in addition to user databases.
- Ensure that all database servers have logon information in the master database. This is important for restoring a database, as system logon information resides in master.
- Disable all startup stored procedures, as the upgrade process will stop and start services on the SQL Server instance being upgraded. Stored procedures processed at startup time might block the upgrade process.
- Quit all applications, including all services that have SQL Server dependencies. Upgrade might fail if local applications are connected to the instance being upgraded.

Upgrading the database (32-bit SQL Server)

To upgrade an older 32bit version of SQL Server to a newer 32bit SQL server

1 Log on to the computer as an Administrator or as a member of the Administrator group and select the installation package that contains the *setup.exe*.

2 Run the program and the **SQL Server Installation Center** wizard is displayed.

3 In the left navigation area, click **Installation** and then click **Upgrade from SQL Server 2005, SQL Server 2008, SQL Server 2008 R2 or SQL Server 2012**.

4 On the **License Terms** page, review the license agreement and, if you agree, select **I accept the license terms**, then click **Next**.

5 In the **Global Rules** window, the setup procedure will automatically advance to the **Product Updates** window if there are no rule errors.

6 The **Microsoft Update** page will appear next if the Microsoft Update check box in **Control Panel>All Control Panel Items>Windows Update>Change settings** is not checked. Putting a check in the Microsoft Update page will change the computer settings to include the latest updates when you scan for Windows Update.

7 On the **Product Updates** page, click **Next** to include the latest SQL Server updates. The **Install Setup Files** page is displayed, where the setup files are copied and then the installation automatically starts.

8 On the **Install Setup Files** page, **Setup** provides the progress of downloading, extracting, and installing the Setup files. If an update for SQL Server Setup is found, and is specified to be included, that update will also be installed.

9 In the **Upgrade Rules** window, the setup procedure will automatically advance to the **Select instance** window if there are no rule errors.

10 On the **Select Instance** page, specify the instance of SQL Server to upgrade.

11 On the **Select Features** page, the features to upgrade will be preselected. A description for each component group appears in the right pane after you select the feature name.

The prerequisites for the selected features are displayed on the right-hand pane. SQL Server Setup will install the prerequisite that are not already installed during the installation step described later in this procedure.

12 On the **Instance Configuration** page, specify the Instance ID for the instance of SQL Server.

- **Instance ID** - By default, the instance name is used as the Instance ID. This is used to identify installation directories and registry keys for your instance of SQL Server. This is the case for default instances and named instances. For a default instance, the instance name and instance ID would be MSSQLSERVER. To use a non-default instance ID, provide a value for the Instance ID textbox.

  All SQL Server service packs and upgrades will apply to every component of an instance of SQL Server.

- **Installed instances** - The grid will show instances of SQL Server that are on the computer where Setup is running. If a default instance is already installed on the computer, you must install a named instance of SQL Server.

13 On the **Server Configuration - Service Accounts** page, the default service accounts are displayed for SQL Server services. The actual services that are configured on this page depend on the features that you are upgrading.

Authentication and login information will be carried forward from the previous instance of SQL Server. You can assign the same login account to all SQL Server services, or you can configure each service account individually.

When you are finished specifying login information for SQL Server services, click **Next**.

14 On the **Full-Text Search Upgrade Options** page, specify the upgrade options for the databases being upgraded.

The **Feature Rules** window will automatically advance if all rules pass.

15 The **Ready to Upgrade** page displays a tree view of installation options that were specified during Setup. To continue, click **Install**. SQL Server Setup will first install the required prerequisites for the selected features followed by the feature installation.

16 During installation, the progress page provides status so that you can monitor installation progress as Setup continues.

17 After installation, the **Complete** page provides a link to the summary log file for the installation and other important notes. To complete the SQL Server installation process, click **Close**.

18 Open **SQL Server Management** and set the compatibility level for the selected database.

Upgrading the database (64-bit SQL Server)

To upgrade an older 32-bit version of SQL Server to a newer 64-bit SQL server

1. Take backups of the **vRangerPro** and **Catalog** Databases. Refer to Backing up the vRanger database.
2. Uninstall the older 32-bit database.
3. Install a fresh 64-bit database.
4. Restore the **vRangerPro** and **Catalog** databases.
5. Open **SQL Server Management** and set the compatibility level for the selected database.

Upgrading the vRanger virtual appliance (VA)

The version of the vRanger VA for this release is listed in Supported virtual appliance (VA) versions. Review the topics that follow for information on checking the version of your deployed VAs, and for procedures on updating them if necessary.

NOTE: The vRanger VA is now bundled with vRanger, and can be found in: **C:\Program Files\Quest\vRanger**

Checking the version of your VA

To check the version of your VA:

1. Log in to the VA.
2. At the prompt, enter the command:

   ```
   cat /etc/vzvaversion
   ```

Upgrading your VA

You can upgrade the vRanger virtual appliance using the Virtual Appliance Configuration dialog box. If your existing VAs have replication scratch disks configured, they are migrated to the upgraded VA as part of this process.

1. Click **Tools**, and then click **Options**.
2. Under the **Virtual Appliance** node on the **Configuration Options** page, click **Configuration**.
3. In the **Configure Existing Virtual Appliance** section, select the VAs to upgrade, and click **Upgrade**.

   IMPORTANT: Only versions 1.9.0 and later of the VA can be upgraded with this method.

4. If not automatically populated, click **Browse**, and browse to the location of the latest Open Virtual Appliance (OVA) file.

   By default, the vRanger virtual appliance OVA files are located in the directory: **C:\Program Files\Quest\vRanger**.

5. Do one of the following:

   - If you want to maintain the existing VAs, select **Do not delete the old virtual appliance**. Selecting this option deploys a new VA in parallel.

- To remove old VAs, do not select this option.

6 Click **OK** to begin the upgrade process.

Maintaining your scratch disk

IMPORTANT: This section is for reference only. The VA scratch disk is migrated automatically by the upgrade process.

The second disk—scratch disk—on your VA contains a hash file for each replicated VM. vRanger uses this file to identify changed data blocks during replication. When upgrading the VA, consider migrating the scratch disk from your legacy VA to the upgraded version. This migration ensures that your hash files are maintained. For more information, see Upgrading your VA.

IMPORTANT: If you do not migrate the scratch disk to your updated VAs, vRanger must re-create each hash file which requires a full scan of the replicated VM. While only the changed data is sent, the re-scan of the VM may take up to one minute per GB of hard disk space.

NOTE: If you are using a VMware® vCenter™ version earlier than 6.0, the ability to change the datastore of the VA scratch disk used for replication is not available.

For more information about the scratch disk, see the *Quest vRanger User's Guide*.

Migrating your existing scratch disk

IMPORTANT: This section is for reference only. The VA scratch disk is migrated automatically by the upgrade process.

The Virtual Appliance Deployment Wizard gives you the option of deploying a VA with or without a scratch disk. When deploying a new VA to upgrade an existing VA used for replication, do not create a scratch disk during the deployment process. You can add the existing scratch disk to the new VA:

1 Power off your existing VA.

2 From the VI Client, right-click the new VA, and select **Edit Settings**.

3 On the **Hardware** tab, click **Add**.

4 Select **Hard Disk**, and click **Next**.

5 Select **Use an existing virtual disk**.

6 Browse to the location of your existing scratch disk.

7 Select the VMDK for the scratch disk, and click **OK**.

8 Using the console in the VI client, log in to the VA.

9 Restart the VM by typing **reboot** at the prompt.

10 After the reboot, use the console to log in and enter the following commands:

```
echo "/dev/sdb /scratch/sdb ext3 defaults 0 0">>/etc/fstab
mkdir /scratch
mkdir /scratch sdb
reboot
```

Upgrading a previous vReplicator installation

Due to the differences in application architecture, there is no upgrade path from vReplicator 3.x to vRanger 7.8.7. vRanger must be installed fresh—using the full installer—and replication jobs must be re-created.

The high-level process for migrating from vReplicator to vRanger 7.8.7 is as follows:

1. Request a new vRanger 7.x license.

   A new license is required for vReplicator customers migrating to vRanger 7.8.7. Request one using the form at: https://support.quest.com/licensing-assistance.

   NOTE: Current vReplicator 3.x customers who are also vRanger customers may want to request a combined license file that includes backup and replication licensing.

2. Download and install vRanger using the installer.

   For the installation procedures, see Installing vRanger.

CAUTION: If you are re-creating your replication jobs, do not uninstall vReplicator 3.x. You may install and run vRanger on the same machine as vReplicator 3.x without issue.

3. Configure vRanger as appropriate.

   For more information, see the topic that discusses using the Startup Wizard in the *Quest vRanger User's Guide*.

4. Re-create replication jobs to match your vReplicator configuration.

   vRanger replication jobs can re-use the existing target VMs created by the vReplicator jobs. This reuse eliminates the need to perform a full synchronization to start the new replication jobs. When configuring jobs, ensure that the host and datastore configuration matches the original job. vRanger recognizes the existing target VM and resume replication without sending the full VM.

CAUTION: Disable the vReplicator job before enabling its vRanger counterpart.

5. After validating that all replication jobs have been properly migrated and are working correctly, uninstall vReplicator.

About Us

Quest provides software solutions for the rapidly-changing world of enterprise IT. We help simplify the challenges caused by data explosion, cloud expansion, hybrid datacenters, security threats, and regulatory requirements. We are a global provider to 130,000 companies across 100 countries, including 95% of the Fortune 500 and 90% of the Global 1000. Since 1987, we have built a portfolio of solutions that now includes database management, data protection, identity and access management, Microsoft platform management, and unified endpoint management. With Quest, organizations spend less time on IT administration and more time on business innovation. For more information, visit www.quest.com.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request.
- View Knowledge Base articles.
- Sign up for product notifications.
- Download software and technical documentation.
- View how-to-videos.
- Engage in community discussions.
- Chat with support engineers online.
- View services to assist you with your product.