Quest

Rapid Recovery 6.9

System Requirements Guide

Revision1 April 2025

© 2025 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

4 Polaris Way

Aliso Viejo, CA 92656

Refer to our Web site (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, and Join the Innovation are trademarks and registered trademarks of Quest Software Inc. 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

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

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

Rapid Recovery System Requirements Guide
Updated - April 2025
Version - 6.9

Contents

Introduction to Rapid Recovery **1**

Rapid Recovery system requirements **3**

Recommended network infrastructure 3

General Data Protection Regulation compliance 4

UEFI and ReFS support 5

Support for dynamic and basic volumes 5

Supported applications and cluster types 6

Support for Cluster Shared Volumes 7

Rapid Recovery Core installation requirements 8

Rapid Recovery operating system installation and compatibility matrix 9

Microsoft Windows operating systems 9

Linux operating systems 10

Rapid Recovery Core requirements 12

Rapid Recovery Agent software requirements 13

Rapid Recovery Local Mount Utility software requirements 16

Rapid Snap for Virtual agentless protection 17

Agentless protection of SQL Server machines 17

Protecting older operating systems with older Agent versions or Agentlessly 17

Rapid Snap for Virtual (agentless protection) support limitations 18

Hypervisor requirements 18

VMware Workstation 19

VMware vCenter/ESXi Microsoft Hyper-V 19

Microsoft Hyper-V 20

Oracle VM VirtualBox 21

DVM repository requirements 21

License requirements 22

Quest Support policy 22

About us **23**

Technical support resources 23

1

Introduction to Rapid Recovery

Rapid Recovery is a backup, replication, and recovery solution that offers near-zero recovery time objectives and recovery point objectives. Rapid Recovery offers data protection, disaster recovery, data migration and data management. You have the flexibility of performing bare-metal restore (to similar or dissimilar hardware), and you can restore backups to physical or virtual machines (VMs), regardless of origin. Rapid Recovery lets you create backup archives to a wide range of supported systems including archiving to the cloud. With Rapid Recovery, you can replicate to one or more targets for added redundancy and security.

Rapid Recovery offers:

- **Flexibility**. You can perform universal recovery to multiple platforms, including restoring from physical to virtual, virtual to physical, virtual to virtual, and physical to physical.
- **Cloud integration**. You can export a VM, archive and replicate to the cloud, and perform bare metal restore from archives in the cloud. Compatible cloud services include Microsoft Azure, Amazon Web Services (AWS), any OpenStack-based provider (including Rackspace), and Google Cloud. US government-specific platforms include AWS GovCloud (US) and Azure Government.
- **Intelligent deduplication**. You can reduce storage requirements by storing data once, and referencing it thereafter (once per repository or encryption domain).
- **Live Recovery**. Using the Live Recovery feature of Rapid Recovery Agent, you have instant access to critical data first, while remaining restore operations complete in parallel. You can use Live Recovery to restore data from a recovery point of any non-system volume of a Windows machine, physical or virtual. Live Recovery is not supported for agentlessly protected machines, Linux machines, or cluster-shared volumes.
- **File-level recovery**. You can recover data at the file level on-premises, from a remote location, or from the cloud.
- **File-level search**. Using criteria you specify, you can search a range of recovery points for one or more files. From the search results, you can then select and restore the files you want to the local Core machine directly from the Rapid Recovery Core Console.
- **Virtual machine export**. Rapid Recovery supports one-time virtual export, letting you generate a VM from a recovery point; and virtual standby, in which the VM you generate is continually updated after each backup. Compatible VM hypervisors include VMware vCenter/ESXi, VMware Workstation, Microsoft Hyper-V, Oracle VM VirtualBox, and Microsoft Azure. You can even perform virtual export to Hyper-V cluster-shared volumes.
- **Rapid Snap for Virtual support**. Enhanced support for virtualization includes agentless protection for vCenter/ESXi VMs and for Hyper-V VMs. Rapid Snap for Virtual includes protection and autodiscovery for VMware ESXi 6.0 and higher with no software agent installed. Host-based protection supports installing Rapid Recovery Agent on a Microsoft Hyper-V host only, letting you agentlessly protect all its guest VMs.

- **Application support**. Rapid Recovery is built with application support. When you protect SQL Server or Microsoft Exchange machines (whether using Rapid Recovery Agent or agentless protection), the backup snapshots captured are automatically application-aware; open transactions and rolling transaction logs are completed and caches are flushed to disk before creating snapshots. Specific application features are supported, including SQL attachability checks (for SQL Server) and database checksum and mountability checks (for Exchange Server). If you protect Oracle 12c or 18c servers with Rapid Recovery Agent, you can also perform DBVERIFY database integrity checks.

See the following resources for more information about Rapid Recovery.

- The Rapid Recovery product support website at https://support.quest.com/rapid-recovery/.
- The documentation website at https://support.quest.com/rapid-recovery/technical-documents/.

2

Rapid Recovery system requirements

This document describes the system and license requirements for installing the Core and Agent components of Rapid Recovery. It also describes requirements for installing the Quest QorePortal.

Topics include:

- Recommended network infrastructure
- General Data Protection Regulation compliance
- UEFI and ReFS support
- Support for dynamic and basic volumes
- Supported applications and cluster types
- Support for Cluster Shared Volumes
- Rapid Recovery Core installation requirements
- Rapid Recovery operating system installation and compatibility matrix
- Rapid Recovery Core requirements
- Rapid Recovery Agent software requirements
- Rapid Recovery Local Mount Utility software requirements
- Rapid Snap for Virtual agentless protection
- Hypervisor requirements
- DVM repository requirements
- License requirements
- Quest Support policy

Recommended network infrastructure

Rapid Recovery requires a minimum network infrastructure of 1 gigabit Ethernet (GbE). Quest recommends 10GbE networks for robust environments. 10GbE networks are also recommended when protecting servers featuring large volumes (5TB or higher).

If multiple network interface cards (NICs) are available on the Core machine that support NIC teaming (grouping several physical NICs into a single logical NIC), and if the switches on the network allow it, then using NIC teaming on the Core may provide extra performance. In such cases, teaming up spare network cards that support NIC teaming on any protected machines, when possible, may also increase overall performance.

If the Core uses iSCSI or Network Attached Storage (NAS), Quest recommends using separate NIC cards for storage and network traffic, respectively.

Use network cables with the appropriate rating to obtain the expected bandwidth. Quest recommends testing your network performance regularly and adjusting your hardware accordingly.

These suggestions are based on typical networking needs of a network infrastructure to support all business operations, in addition to the backup, replication, and recovery capabilities Rapid Recovery provides.

General Data Protection Regulation compliance

The General Data Protection Regulation (GDPR) is legislation crafted to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU, which makes it relevant to software manufacture in the US and other countries. It updates rules governing the handling of individuals' personal data. GDPR is being widely adopted throughout the software industry.

To comply with the GDPR, the collection of any personally identifiable information (PII) by Rapid Recovery has been carefully considered. Data collection has been streamlined, and the information collected and how it is used is clearly documented.

When installing the Rapid Recovery Core or running the Rapid Recovery Info Gathering Tool, you are provided a description of the information Rapid Recovery collects and our purposes for collecting the information.

If you accept the stated use of personal data, you can then associate a license (running in standard "phone-home" mode) with your Core. If you choose to decline the use of personal data described in the privacy policy, you must request a special "non-phone-home" license. After you receive that license and associate it with your Core, your PII will not be used, and certain functions (auto update, and enabling integration between the Core and the QorePortal) are disabled.

Regardless of the privacy option you selected during installation, from the Core *Agree to use of personal data* General setting, you can update your privacy setting at any time. To switch between phone-home and non-phone-home modes in either direction, you must have access to the appropriate license at the time you make this change.

For more information about the GDPR, see the EU General Data Protection Regulation website at https://eugdpr.org/the-regulation/. For more information about managing your privacy, see the following topics in the *Rapid Recovery User Guide*:

- Certain business rules apply when changing between phone-home and non-phone-home mode using the *Agree to use of personal data* general setting. For more information, see the topic "Configuring Core general settings."
- To see what information Rapid Recovery collects, in which circumstances, and why the information is collected, see "How Rapid Recovery uses personal information."
- To see what functions you cannot perform when using a non-phone-home license, see the topic "Non-phone-home license restrictions."
- To download a phone-home license, log into the Rapid Recovery License Portal. From the navigation menu, click **Licensing**, and from the drop-down menu on the top right, select **License Key.**
- To learn how to obtain a license in non-phone-home mode, see the topic "Obtaining and using non-phone-home licenses."

UEFI and ReFS support

Unified Extensible Firmware Interface (UEFI) is a replacement for Basic Input/Output System (BIOS). For Windows systems, UEFI uses the Extensible Firmware Interface (EFI) system partitions that are handled as simple FAT32 volumes.

Protection and recovery capabilities are available in Rapid Recovery for EFI system partitions with the following operating systems:

- **Windows:** Windows versions 10, 11; Windows Server versions 2016, 2019, 2022.

  NOTE: Operating systems marked * have reached EOL; support is limited.

- **Linux:** All supported versions of Linux.

  NOTE: Some versions of Linux have limited support. For more information, see Rapid Recovery operating system installation and compatibility matrix.

Rapid Recovery also supports the protection and recovery of Resilient File System (ReFS) volumes for Windows 10, Windows 11, Windows Server versions , 2016, 2019, and 2022.

NOTE: When using ReFS volumes for Windows Server 2019, use only the latest version of Windows Server 2019 with the most recent Windows updates. Rapid Recovery Core may block volumes that use older versions of Windows Server 2019 from protection.

Support for dynamic and basic volumes

Rapid Recovery supports taking snapshots of all dynamic and basic volumes. Rapid Recovery also supports exporting simple dynamic volumes that are on a single physical disk. As their name implies, simple dynamic volumes are not striped, mirrored, spanned, or RAID volumes.

The behavior for virtual export of dynamic disks differs, based on whether the volume you want to export is protected by the Rapid Recovery Agent software, or is a VM using agentless protection. This is because non-simple or complex dynamic volumes have arbitrary disk geometries that cannot be fully interpreted by Rapid Recovery Agent.

When you try to export a complex dynamic disk from a machine with the Rapid Recovery Agent software, a notification appears in the user interface to alert you that exports are limited and restricted to simple dynamic volumes. If you attempt to export anything other than a simple dynamic volume using Rapid Recovery Agent, the export job fails.

In contrast, dynamic volumes for VMs you protect agentlessly are supported for protection, virtual export, restoring data, and BMR, and for repository storage, with some important restrictions. For example:

- **Protection:** In the case when a dynamic volume spans multiple disks, you must protect those disks together to maintain the integrity of the volume.

- **Virtual export:** You can export complex dynamic volumes such as striped, mirrored, spanned, or RAID volumes from an ESXi or Hyper-V host using agentless protection. However, the volumes are exported at the disk level, with no volume parsing. For example, if exporting a dynamic volume spanned across two disks, the export will include two distinct disk volumes.

  CAUTION: When exporting a dynamic volume that spans multiple disks, you must export the dynamic disks with the original system volumes to preserve the disk types.

- **Restoring data:** When restoring a dynamic volume that spans multiple disks, you must restore the dynamic disks with the original system volumes to preserve the disk types. If you restore only one disk, you will break the disk configuration.
- **Repository storage:** Additionally, Rapid Recovery supports the creation of repositories on complex dynamic volumes (striped, mirrored, spanned, or RAID). The file system of the machine hosting the repository must be NTFS or ReFS.

Supported applications and cluster types

To protect your cluster properly, the Rapid Recovery Agent software must be installed on each of the machines or nodes in the cluster. Rapid Recovery supports the application versions and cluster configurations listed in the following table.

Table 1: Supported application versions and cluster configurations

Application	Application Version and Related Cluster Configuration	Windows Failover Cluster
Microsoft Exchange Server[1]	Exchange 2013, 2016[2], 2019	Windows Server 2012[2], 2012 R2, 2022
Microsoft SQL Server	SQL Server 2012, 2014 SCC	Windows Server 2012[2], 2012 R2
	SQL Server 2012[2], 2014, 2016[2], 2017, 2019 Availability Groups	Windows Server 2012, 2012 R2, 2016[2], 2019, 2022

[1] Microsoft Exchange support includes both standalone and Database Availability Group (DAG) for all versions listed.

[2]Rapid Recovery does not support cluster shared volumes (CSVs) for all Windows versions. For more information, see Support for Cluster Shared Volumes.

Live migration is a Hyper-V feature of Windows Server which lets users move running VMs from one Hyper-V host to another. Rapid Recovery supports Hyper-V live migration when moving VMs between nodes in a cluster. Live migration between separate hosts (a Hyper-V 2016 feature) is not supported with Rapid Recovery.

If using Rapid Snap for Virtual agentless protection, a supported version of Rapid Recovery Agent must be installed on the Hyper-V host. If using agent-based protection, Rapid Recovery Agent must be installed on each node in a protected Hyper-V cluster, but is not required on the host.

If using Rapid Snap for Virtual agentless protection, a supported version of Rapid Recovery Agent must be installed on the Hyper-V host. If using agent-based protection, Rapid Recovery Agent must be installed on each node in a protected Hyper-V cluster, but is not required on the host.

The supported disk types include:

- GUID partition table (GPT) disks greater than 2 TB
- Master Boot Record (MBR) disks less than 2 TB

The supported mount types include:

- Shared drives that are connected as drive letters (for example, D:)
- Simple dynamic volumes on a single physical disk (not striped, mirrored, or spanned volumes)
- Shared drives that are connected as mount points

NOTE: Rapid Recovery Core does not support mount types of complex dynamic disks for agentless protection.

Support for Cluster Shared Volumes

Direct protection and restore of the actual cluster-shared volumes (CSVs) themselves in Rapid Recovery is only possible with Windows Server 2008 R2 SP1[1], and is deprecated. This feature is not expected to be supported in future releases of Rapid Recovery.

Currently supported versions of Rapid Recovery offer agentless support only of virtual machines *residing on* Hyper-V CSVs (not of the CSVs themselves).

Any feature listed as supported below requires Rapid Recovery Agent to be installed on each node of the cluster. You can then agentlessly protect and restore supported VMs hosted on Hyper-V clusters installed on Windows Server versions 2008 R2 SP1[1], 2012, 2012 R2, 2016, and 2019.

In addition, Rapid Recovery Core supports virtual export to Hyper-V CSVs installed on currently supported Windows operating systems, including Windows Server versions 2012, 2012 R2, 2016, 2019, and 2022. For information about supported hypervisors, see Hypervisor requirements.

The following table depicts current Rapid Recovery support for cluster-shared volumes.

Operating System	**Protect[2] and Restore[3] VMs on a Hyper-V CSV**			**Virtual Export to Hyper-V CSV**			**Protect[2] and Restore[4] CSV Directly**		
CSV Operating System	**Rapid Recovery Version**			**Rapid Recovery Version**			**Rapid Recovery Version**		
	6.7	**6.8**	**6.9**	**6.7**	**6.8**	**6.9**	**6.7**	**6.8**	**6.9**
Windows Server 2012	Limited[5]	Limited[5]	Limited[5]	Yes	Yes	Yes	No	No	No
Windows Server 2012 R2	Limited[5]	Limited[5]	Limited[5]	Yes	Yes	Yes	No	No	No
Windows Server 2016	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No
Windows Server 2019	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No
Windows Server 2022	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No

Notes:

[1] Microsoft discontinues support for Windows Server 2008 R2 on January 14, 2020. After this date, Rapid Recovery continues limited support for Windows Server 2008 R2 (SP1 only) in release 6.9. Customers are advised to migrate to newer supported versions to continue backing up data using Rapid Recovery.
[2] Protect includes protection, replication, rollup, mount, and archiving.
[3] Restore includes file-level restore, volume-level restore, bare metal restore, and virtual export.
[4] Restore includes file-level restore, volume-level restore, and bare metal restore.
[5] These Windows Server versions have reached standard end of life. Support for these OS is therefore limited.

Rapid Recovery Core installation requirements

Servers should not have any other applications, roles, or features installed that are not related to Rapid Recovery. For example, do not use the Core server as a high-traffic web server; and do not run Active Directory as a domain controller on the Core server. If possible, do not run server applications such as Exchange Server, Oracle, SharePoint Server, or SQL Server on the Core machine. If SQL Server is required on the Core machine – for example, if you are using Rapid Recovery DocRetriever for SharePoint–make sure you allocate more resources, in addition to those needed for efficient Core operations.

Depending on your license and your environment requirements, you may need to install multiple Cores, each on a dedicated server. Licensed Rapid Recovery users with an active maintenance agreement can manage two or more Cores from the QorePortal, which can be accessed at https://qoreportal.quest.com/.

Before installing or upgrading Rapid Recovery Core on your Core server, ensure that your system meets the following minimum hardware and software requirements. For additional guidance for sizing your hardware, software, memory, storage, and network requirements, see knowledge base article 185962, "Sizing Rapid Recovery Deployments."

CAUTION: Microsoft offers Server Core editions of their Windows Server products, which have a smaller footprint and limited server roles. Quest does not support running Rapid Recovery Core on these minimal installations of the Windows Server operating systems. Quest only supports Rapid Recovery Core on the standard (or "Desktop Experience") versions of supported Windows Server operating systems.

NOTE: Quest does not recommend installing Rapid Recovery Core on an all-in-one server suite such as Microsoft Small Business Server or Microsoft Windows Server Essentials.

CAUTION: Quest does not recommend running the Rapid Recovery Core on the same physical machine that serves as a hypervisor host.

Rapid Recovery operating system installation and compatibility matrix

Microsoft Windows operating systems

Rapid Recovery Core must be installed on an appropriately sized server running a supported 64-bit Microsoft Windows operating system. The following table and notes list each Windows operating system and describes compatibility for each Rapid Recovery component or feature. Rapid Recovery Core does not support Windows Server core editions.

NOTE: This matrix is provided to educate users on compatibility. Quest does not support operating systems that have reached end of life.

Table 2: Rapid Recovery components and features compatible with Windows operating systems.

OS Version	Core	Agent	Agentless	LMU	MR	DR	URC Restore	URC Driver Injection	VM Export to Azure
Windows 8	No	No	Limited	No[1]	Yes[1]	Yes[1]	Limited	Limited	Limited[2]
Windows 8.1	No	Limited	Yes	No	No	No	Limited	Limited	Limited[2]
Windows 10	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes[2]
Windows 11	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes[2]
Windows Server 2012	No	No	Limited	No	No	No	No	No	Limited
Windows Server 2012 R2	No	No	Limited	No	No	No	No	No	Limited
Windows Server 2016	Yes[3]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes[2]
Windows Server 2019	Yes[3]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Windows Server 2022	Yes[3]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Windows installation and support notes:

[1] Follow guidance in Microsoft KB 3033929. Install hotfix per Microsoft KB 2921916. Silent installation of Core is not supported.

[2] VM export to Azure works only for x64 editions of operating systems listed.

[3]Rapid Recovery Core cannot be installed on Windows Core operating systems, which offer limited server roles and have no GUI. This includes all Server Core editions for all currently supported Windows Server operating systems.

Linux operating systems

Linux operating systems are supported as protected machines in a Rapid Recovery Core. You can use agentless protection, or install the Rapid Recovery Agent. The following table and notes list each supported Linux operating system and distribution, and describes support for each Rapid Recovery component or feature.

Table 3: Compatible Rapid Recovery components and features by Linux operating system

OS Version or distribution	Agent	Agentless	Live DVD	VM Export to Azure
AlmaLinux 8.3	Limited[2]	Limited[2]	Limited[2]	Limited[2]
AlmaLinux 9	Yes	Yes	Yes	Yes
CentOS Linux 6.4 - 6.10	Limited[2]	Limited[2]	Limited[2]	Limited[2]
CentOS Linux 7.0 - 7.9	Yes	Yes	Yes	Yes
CentOS Linux 8.0 - 8.6	Yes	Yes	Yes	Yes
CentOS Linux 9.0	Yes	Yes	Yes	Yes
Debian Linux 9	Yes	Yes	Yes	Yes
Debian Linux 10	Limited[2]	Limited[2]	Limited[2]	Limited[2]
Debian Linux 11	Yes	Yes	Yes	Yes
Debian Linux 12	Yes	Yes	Yes	Yes
Oracle Linux 6.4 - 6.10	Yes	Yes	Yes	Yes
Oracle Linux 7.0 - 7.9	Yes	Yes	Yes	Yes
Oracle Linux 8.0 - 8.3	Yes	Yes	Yes	Yes
Oracle Linux 9.0	Yes	Yes	Yes	Yes
Red Hat Enterprise Linux (RHEL) 6.4 - 6.10	Limited[2]	Limited[2]	Limited[2]	Limited[2]
RHEL 7.0 - 7.9	Yes	Yes	Yes	Yes
RHEL 8.0 - 8.6	Yes	Yes	Yes	Yes

OS Version or distribution	Agent	Agentless	Live DVD	VM Export to Azure
RHEL 9 - 9.3	Yes	Yes	Yes	Yes
Rocky Linux 8	Limited[4]	Limited[4]	Limited[4]	Limited[4]
Rocky Linux 9	Yes	Yes	Yes	Yes
SUSE Linux Enterprise Server (SLES) 11 SP4[3]	Limiteds[2]	Limited[2]	Limited[2]	Limited [2]
SLES 12 SP3[3]	Limited[2]	Limited[2]	Limited[2]	Limited[2]
SLES 12 SP4[3]	Limited[2]	Limited[2]	Limited[2]	Limited[2]
SLES 12 SP5 (No BMR)[3]	Yes	Yes	Yes	Yes
SLES 15 SP1[3], SP2[3]	Yes	Yes	Yes	Yes
SLES 15 SP3, SP4	Yes	Yes	Yes	Yes
SLES 15 SP5	Yes	Yes	Yes	Yes
Ubuntu Linux 16.04 LTS (April 2016)	Limited[2]	Limited[2]	Limited[2]	Limited[2]
Ubuntu Linux 18.04 LTS	Yes	Yes	Yes	Yes
Ubuntu Linux 19.04, 19.10	Limited[2]	Limited[2]	Limited[2]	Limited[2]
Ubuntu Linux 20.04 LTS	Yes	Yes	Yes	Yes
Ubuntu Linux 20.10	Yes	Yes	Yes	Yes
Ubuntu Linux 21.04, 21.10	Yes	Yes	Yes	Yes
Ubuntu Linux 22.04, 22.10	Yes	Yes	Yes	Yes
Ubuntu Linux 23.04, 23.10	Yes	Yes	Yes	Yes
Ubuntu Linux 24.04	Limited	Limited	Limited	Limited

Linux installation and support notes:

[1] B-tree file system (BTRFS) is supported only on operating systems with kernel version 3.7 or later. The earliest versions of compliant operating systems include Ubuntu 14.04, Debian 8, CentOS/Oracle Linux/RHEL 7, and SLES 12.

[2] This operating system distribution has reached end of life, and is therefore no longer tested. Support for this operating system is therefore limited.

[3] This operating system distribution (and SUSE Linux Desktop) fully supported when using listed service packs; versions using earlier SPs are in limited support only.

[4] This operating system distribution was tested only for platform detection, not for functionality.

For more information on Linux versions supported by Rapid Recovery, including kernel versions, file systems and restrictions, see Rapid Recovery Agent software requirements

Rapid Recovery Core requirements

Requirements for the Rapid Recovery Core are described in the following table.

Table 4: Rapid Recovery Core requirements

Requirement	Details
Operating system	Rapid Recovery Core does not run on 32-bit Windows systems or any Linux distribution. Rapid Recovery Core requires one of the following 64-bit Windows operating systems (OS): • Microsoft Windows 10 , 11 • Microsoft Windows Server versions 2016, 2019, 2022 [1] The Rapid Recovery Core supports all x64 editions of the Windows Server OS versions listed. However, the Rapid Recovery Core does not support Windows Server core editions [2] Quest provides only limited support for OS versions after their manufacturers end extended support. **General Notes:** Windows operating systems require the Microsoft .NET Framework version 4.8 to be installed to run the Rapid Recovery Core service. For optimal performance, it is recommended that you install the Rapid Recovery Core on more recent operating systems.
Architecture	64-bit only
Memory	8GB RAM or more. This is a requirement of Rapid Recovery Core. Quest highly recommends using Error Checking & Correction (ECC) memory, to ensure optimum performance of Rapid servers.
Processor	**NOTE**: Rapid Recovery 6.9 or newer supports processor family Sandy Bridge or newer. **Nehalem (2008)** - This architecture introduced the concept of Turbo Boost. **Westmere (2009)** - An update to Nehalem with minor architectural improvements and higher clock speeds. **Sandy Bridge (2011)** - A major architecture leap, introducing improved graphics processing (Intel HD Graphics) and integrated memory controller. **Ivy Bridge (2012)** - Updated version of Sandy Bridge with enhanced performance and further improvements to the integrated graphics. **Haswell (2013)** - Continued refinements of the Sandy Bridge architecture, focusing on power efficiency and battery life for mobile devices. **Broadwell (2014)** - Introduced a new transistor design, aiming for even greater energy efficiency but faced production issues initially. **Skylake (2015)** - A significant architectural change, bringing updated security features, improved integrated graphics, and support for DDR4 memory.
Storage	The amount of storage required differs based on your needs. Storage requirements typically increase over time and should be revisited at least annually. Rapid Recovery supports primary storage in a DVM repository. Characteristics and

Requirement	Details
	requirements include the following: • DVM repositories can be extended by adding new storage locations. • Each volume you define as a storage location must have a minimum of 1GB of free space available on it. Quest recommends minimum storage of 100GB per storage volume. • For your repository storage, Quest strongly recommends a configuration of RAID 6 with 4 usable drives or better, for a change rate per hour of up to 10GB. Use more drives for additional capacity or higher change rates. • Suggested random input/output per second (IOPS) of 300 or better (based on 4 usable drives each capable of 75 IOPS measured at 32KB with 75% reads with 60 random I/O). • There are no specific I/O controller requirements. However, speed is the most important factor for DVM repository storage. • Quest recommends locating your DVM repository on direct attached storage (DAS), storage area network (SAN), or network attached storage (NAS) devices (listed in order of preference). • If installing on a NAS, Quest recommends limiting the repository size to 6TB. Any storage device must meet the minimum IOPS requirements.
	See Quest knowledge base article 185962, "Sizing Rapid Recovery Deployments," for additional guidance for sizing your hardware, software, memory, storage, and network requirements.
Network	1 gigabit Ethernet (GbE) minimum **NOTE:** Quest recommends a 10GbE network backbone for robust environments. .
Network hardware	Use network cables with the appropriate rating to obtain the expected bandwidth. **NOTE:** Quest recommends testing your network performance regularly and adjusting your hardware accordingly.

Rapid Recovery Agent software requirements

For each physical machine you want to protect in a Rapid Recovery Core, install the Rapid Recovery Agent software. The Agent software must be compatible with that machine's OS and file system, as detailed in the following matrix.

You can also protect virtual machines (VMs) on your Core. You can use Agent-based protection by installing Rapid Recovery Agent on each VM, as appropriate. Or you can protect VMs on supported hypervisor hosts using Rapid Snap for Virtual agentless protection. There are tradeoffs between using Agent-based and agentless protection. When configured properly, fewer licenses are consumed from your license pool when using Rapid Snap for Virtual. However, you may prefer using Agent-based protection for VMs (for example, when protecting Oracle servers,

dynamic volumes, or if you need Live Recovery). For more information, see the topic "Understanding Rapid Snap for Virtual" in the *Rapid Recovery User Guide*.

Requirements for the Rapid Recovery Agent software are described in the following table. Review carefully for each release, as requirements change. Snapshot data for each protected machine must be saved to a DVM repository only. Tiering is not supported in this release.

You cannot use the Rapid Recovery Add-on for Kaseya to deploy Rapid Recovery Agent to a Linux machine you want to protect in your Core. If using the Add-on, manually install Rapid Recovery Agent on each Linux machine. For more information on installing Agent, see the *Rapid Recovery Installation and Upgrade Guide*.

Table 5: Rapid Recovery Agent software requirements

Requirement	Details
Operating system	Windows operating systems require the Microsoft .NET Framework version 4.8 to be installed to run the Rapid Recovery Agent service. The Rapid Recovery Agent software supports 32-bit and 64-bit Windows and Linux operating systems, including the following: • Microsoft Windows version 10, 11[1] • Microsoft Windows Server versions 2016[1], 2019[1,5], 2022. • AlmaLinux 8.3,9 • CentOS Linux 6.4 - 6.10[3], 7.0 - 7.9, 8.0 - 8.6 • Debian Linux 9, 10, 11 , 12 • Oracle Linux 6.4 - 6.10[3], 7.0 - 7.9, 8.0 - 8.3, 9 • Red Hat Enterprise Linux (RHEL) 6.4- 6.10[3], 7.0- 7.8, 8.0-8.6, 9.0 - 9.3 • Rocky Linux 8, 9 • SUSE Linux Enterprise Server (SLES) 11 (SP4 and later)[6], 12 (SP3 and later)[6], 15 (SP1 and later)[6], 15 SP5 • Ubuntu Linux 16.04 LTS[3], 18.04 LTS, 19.04[3], 19.10[3], 20.04 LTS, 20.10, 21.04[4], 21.10, 22.04, 22.10, 23.04, 23.10, 24.04 [1] Requires the ASP .NET 4.8 role or feature. When installing or upgrading the Rapid Recovery Agent software, the installer checks for the ASP .NET 4.8 role or feature. If required, the installer installs or activates this component and then reboots. [2] Follow guidance in Microsoft KB 3033929. For silent installation, see Microsoft KB 2921916. [3] This operating system has reached end of life, and is therefore no longer tested. Support for this operating system is therefore limited. [4] This operating system distribution was tested only for platform detection, not for functionality. [5] ReFS volumes supported for protection only on most recent update of Windows Server 2019. [6] SUSE Linux Enterprise with the listed service packs are fully supported. Older versions are on limited support. SUSE Linux Enterprise Desktop is supported at the same version level.
	Additional operating systems are supported for agentless protection only. For more information, see Rapid Snap for Virtual agentless protection. The Rapid Recovery Agent software supports Windows Server Core edition installations for Windows Server version, 2016, 2019, and 2022. The Rapid Recovery Agent software supports the Linux distributions included in this list.

Requirement	Details
	Additionally, note the following: **Linux kernel.** Rapid Recovery supports Linux kernel versions 2.6.32 and later. **FIle systems and restrictions.** Supported file systems include ext2, ext3, ext4, xfs, and BTRFS. The following restrictions apply: • ext2 is supported only on kernel version 3.6.0 or later. • BTRFS is supported on Linux operating systems with kernel 3.7 or later. This minimum kernel version is included beginning with Ubuntu 14.04, Debian 8, CentOS/Oracle Linux/RHEL 7, and SLES 12. If the kernel on earlier versions of these OS is upgraded to 3.7 or later, BTRFS is supported. For more information, see the Rapid Recovery operating system installation and compatibility matrix. Agents installed on Microsoft Hyper-V Server versions, 2016 and 2019 operate in the Core edition mode of the relevant Windows Server OS.
Architecture	32-bit or 64-bit
Memory	4GB or higher
Processor	Single processor or higher
Microsoft Exchange Server support	Rapid Recovery supports Microsoft Exchange Server versions 2013, 2016, and 2019.
Microsoft SQL Server support	The following Microsoft SQL Server versions are supported on Windows machines only (no Linux support): 2012, 2014, 2016, 2017, and 2019.
Microsoft SharePoint Server support	Microsoft SharePoint versions 2016 and 2019 **NOTE:** Support for "SharePoint" refers to fully licensed versions of Microsoft SharePoint Server for the versions listed above.
Oracle relational database support	Rapid Recovery Agent supports the following versions of Oracle relational database management systems (RDBMS): • Oracle 18c RDBMS u[']/[sing Rapid Recovery 6.4.0 or later on 64-bit servers running Windows Server 2016 only. • Oracle 12c RDBMS using Rapid Recovery 6.2 or later on 64-bit servers running Windows Server 2016. Protection of Oracle12c and 18c databases is limited to using Volume Snapshot Service (VSS) in the ARCHIVELOG mode. Agentless protection is not supported. Oracle Agent-based support includes application awareness. You can perform database integrity checks against our volume images using DBVERIFY (a native Oracle utility). For more information, see "About protecting Oracle database servers" in the *Rapid Recovery User Guide*.
Storage	Direct attached storage, storage area network or network attached storage
Network	1 gigabit Ethernet (GbE) minimum

Requirement	Details
	NOTE: Quest recommends a 10GbE network backbone for robust environments. Quest does not recommend protecting machines over a wide-area network (WAN). If you have multiple networked sites, Quest recommends installing a Core at each site. To share information, you can replicate between the Cores located at different sites. Replication between Cores is WAN-optimized. The data transmitted is compressed, deduplicated, and encrypted during transfer.
Network hardware	Use network cables with the appropriate rating to obtain the expected bandwidth. **NOTE:** Quest recommends testing your network performance regularly (at least once annually) and adjusting your hardware accordingly.

Rapid Recovery Local Mount Utility software requirements

The Local Mount Utility (LMU) is included with Rapid Recovery. You can obtain the LMU installer from the *Downloads* page from either the Rapid Recovery Core Console, the QorePortal (at https://qoreportal.quest.com/), or the Rapid Recovery License Portal (at https://licenseportal.com/Downloads).

Table 6: Local Mount Utility software requirements

Requirement	Details
Operating system	The Rapid Recovery Local Mount Utility software supports 32-bit and 64-bit Windows operating systems, including the following: • Microsoft Windows version 10[1], 11 • Microsoft Windows Server versions 2016[1], 2019[1], 2022
	[1] Requires the ASP .NET 4.8 role or feature. When installing or upgrading the LMU, the installer checks for the ASP .NET 4.8 role or feature. If required, the installer installs or activates this component and then reboots. The LMU software supports Windows Server Core edition installations for Windows Server versions 2016, 2019, and 2022. Windows Server 2008 R2 Core edition is not supported.
Architecture	32-bit or 64-bit
Memory	4GB or higher
Processor	Single processor or higher
Network	1 gigabit Ethernet (GbE) minimum **NOTE:** Quest recommends a 10GbE network backbone for robust environments.. Quest does not recommend protecting machines over a wide-area network (WAN). If you have multiple networked sites, Quest recommends installing a Core at each site. To share

Requirement	Details
	information, you can replicate between the Cores located at different sites. Replication between Cores is WAN-optimized. The data transmitted is compressed, deduplicated, and encrypted during transfer.
Network hardware	Use network cables with the appropriate rating to obtain the expected bandwidth. **NOTE:** Quest recommends testing your network performance regularly (at least once annually) and adjusting your hardware accordingly.

Rapid Snap for Virtual agentless protection

The Rapid Snap for Virtual feature of Rapid Recovery lets you protect virtual machines (VMs) on specific hypervisor platforms without installing the Rapid Recovery Agent software on each guest machine.

When using this feature on the Hyper-V hypervisor platform, you only install Agent on the Hyper-V host. When using this feature on VMware ESXi, the ESXi host uses native APIs to extend protection to its guest machines.

Since the Agent software is not required to be installed on every VM, this feature is known in the industry as *agentless protection*. On Hyper-V, we also refer to this as *host-based protection*.

Rapid Snap for Virtual offers several benefits, and also some restrictions. As an example, you cannot capture snapshots of dynamic volumes (such as spanned, striped, mirrored, or RAID volumes) at the volume level. You can, however, capture snapshots on dynamic volumes at the disk level. Ensure that you understand both the benefits and restrictions before using this feature. For more information, see the topic "Understanding Rapid Snap for Virtual " in the *Rapid Recovery User Guide* .

When using agentless or host-based protection, your VMs have the same minimum requirements for base operating system, RAM, storage, and network infrastructure as machines protected with the Rapid Recovery Agent software. For details, see the topic Rapid Recovery Agent software requirements.

Agentless protection of SQL Server machines

Rapid Recovery supports agentless protection for all supported SQL Server versions. As of release 6.3, this includes agentless support of SQL Server 2017.

Protecting older operating systems with older Agent versions or Agentlessly

Quest does not support software that has reached end of life (EOL). Agent-based protection in release 6.2 and later requires the OS of the protected machine to support Microsoft .NET Framework version 4.8 and SHA-2.

To protect machines in a Core running older operating systems, consider running an older supported version of Rapid Recovery Agent. For example, Rapid Recovery Agent release 6.1.3 runs Microsoft .NET Framework version 4.5.2, which supports some older Microsoft operating systems. You can protect machines running Agent version 6.1.3 in a Rapid Recovery 6.3 Core. For details on versions supported, see Quest Support policy.

Protected machines with these operating systems cannot be upgraded past release 6.2. Additionally, support for other operating systems have been discontinued in Core 6.9. For information on supported operating systems, see Rapid Recovery OS installation and compatibility matrix. For information on which platforms have been discontinued, refer to the Deprecations section of *Rapid Recovery Release Notes*.

Another option is to protect machines agentlessly on Hyper-V or VMware ESXi. For more information, see Hypervisor requirements.

For machines running unsupported operating systems, proceed with agentless protection at your own risk. While Quest Data Protection Support can attempt to answer questions for releases under limited support, any required software corrections or patches can only be applied to fully supported software releases, respectively.

Rapid Snap for Virtual (agentless protection) support limitations

For a list of supported operating systems and the Rapid Recovery components supported for each, see Rapid Recovery operating system installation and compatibility matrix. Any known limitations are included in these matrices, or as notes to the software requirements tables for the Core or the Agent, respectively. If a defect precludes the use of specific features temporarily, this information is typically reported in the release notes for any specific release. Quest strongly encourages users to review system requirements and release notes prior to installing any software version.

For a list of features that have recently been deprecated or are now only under limited support, see the latest edition of *Rapid Recovery Release Notes*.

Quest does not fully test with unsupported operating systems. If using agentless protection to protect virtual machines with an OS not supported by the Rapid Recovery Agent software, do so at your own risk. Users are cautioned that some restrictions or limitations may apply. These restrictions may include:

- An inability to perform virtual export (one-time or continual)
- An inability to save to an archive or restore from an archive
- An inability to restore to a system volume using bare metal restore

For example, if agentlessly protecting a machine with Windows 95, attempts at virtual export to Hyper-V will fail. This failure is due to restrictions in Hyper-V support of that older operating system.

To report specific difficulties, you can contact your Quest Data Protection Support representative. Reporting such difficulties lets Quest potentially include specific incompatibilities in knowledge base articles or future editions of release notes.

Hypervisor requirements

A hypervisor creates and runs virtual machines (guests) on a host machine. Each guest has its own operating system, which can differ from the OS of the host machine.

Two main integration points between Rapid Recovery and hypervisors relate to virtual export, and agentless protection.

Virtual export. Using the virtual export feature of Rapid Recovery, you can perform a one-time virtual export, or define requirements for continual virtual export (this feature is also called "virtual standby"). This process can be performed from any protected machine, physical or virtual. If a protected machine goes down, you can boot up the virtual machine and use it to continue day-to-day operations.

When exporting to ESXi, Hyper-V, or VMware Workstation, you must use the full licensed versions of those hypervisors, not free versions.

Rapid Recovery lets you perform virtual export to VM hosts described in the matrices below.

Agentless protection. Agentless protection for hypervisors is supported as described in the matrices below.

Rapid Recovery explicitly supports the following hypervisors:

- VMware Workstation
- VMware vCenter/ESXi
- Microsoft Hyper-V
- Oracle VM VirtualBox

VMware Workstation

Rapid Recovery lets you perform virtual export to the following VMware Workstation hosts. There is no agentless support for VMware Workstation.

Table 7: Rapid RecoverySupport for VMware Workstation

VMware Workstation Version	Rapid Recovery Support (as VM Export Target)	End of General Support by VMware
VMware Workstation 15.x[1]	Limited support	March 2021
VMware Workstation 16 Pro	Limited support	December 2022

[1] These Workstation versions have passed the end of general support with VMware. Rapid Recovery support for these versions is listed above.

[2] Full support provided until end of general support date listed; thereafter, only limited support is provided in that Rapid Recovery release.

Quest strongly recommends running on the most recent supported VMware product version.

VMware vCenter/ESXi Microsoft Hyper-V

Rapid Recovery lets you perform virtual export to supported VMware vCenter/ESXi hosts, and supports protection in a Rapid Recovery Core of vCenter/ESXi guest VMs. The following vCenter/ESXi versions are supported:

Table 8: Rapid Recovery Support for vCenter/ESXi

ESXi Version	Rapid Recovery Support (as VM Export Target)	Rapid Recovery Support (Agentless Protection)	End of General Support by VMware
vCenter/ESXi 6.7	Full support	Full support	November 15, 2021
vCenter/ESXi 7.0	Full support	Full support	April, 2025
vCenter/ESXi 8.0	Full support	Full support	October 11, 2027

[1] Full support provided until end of general support date listed; thereafter, only limited support is provided in that Rapid Recovery release.

Quest strongly recommends running on the most recent supported VMware product version.

Quest recommends installing the most recent version of VMware Tools on protected VMs on vSphere or ESXi hosts.

Rapid Recovery supports only licensed versions of ESXi for agentless protection. Users of ESXi Free edition must use Agent-based protection and Agent-based licensing (socket-based licensing is not available to users of ESXi Free).

Microsoft Hyper-V

Rapid Recovery lets you perform virtual export to Microsoft Hyper-V hosts, and supports protection in a Rapid Recovery Core of Hyper-V guests on the following Hyper-V operating systems:

Table 9: Rapid Recovery Support for Hyper-V

Hyper-V Operating System	Rapid Recovery Support (as VM Export Target)[1]	Rapid Recovery Support (Agentless Protection)[2]	End of Mainstream Support by Microsoft
Windows Server 2016	Full support	Full support	January 11, 2022
Windows Server 2019	Full support	Full support	January 9, 2024
Windows Server 2022	Full support	Full support	October 13, 2026
Windows 8[3]	Limited support	Limited support	January 14, 2014
Windows 8.1[3]	Limited support	Full support	January 14, 2014
Windows 10	Limited support	Full support	October 13, 2020
Windows 11	Limited support	Full support	October 10, 2023

[1] For virtual export to any Hyper-V host, .NET v.4.6.2 or later and .NET 2.0 or later are required on the Hyper-V host. If experiencing crashes of the Rapid Recovery Core with System.AccessViolationException, try upgrading the .NET Framework to version 4.7.2 or later.
[2] Since Rapid Recovery Agent software must be installed on the Hyper-V host, but not on Hyper-V guest VMs, Quest also refers to this type of agentless support as host-based support.
[3] These operating systems have passed the end of mainstream support with Microsoft. Rapid Recovery support for these versions is listed above.

Quest recommends installing Hyper-V Integration Services on VMs you want to protect on Hyper-V hosts.

Protected machines with Unified Extensible Firmware Interface (UEFI) operating systems support virtual export to Hyper-V second-generation hosts.

Oracle VM VirtualBox

Rapid Recovery lets you perform virtual export to the following Oracle VM VirtualBox versions, on both Windows and Linux platforms. There is no agentless support for VirtualBox .

Table 10: Rapid Recovery Support for Oracle VM VirtualBox

VirtualBox Version	Rapid Recovery Support (as VM Export Target)[1]	End of Mainstream Support by Microsoft
VirtualBox 5.1[3]	Limited support	April 2018
VirtualBox 5.2[3]	Limited support	July 2020
VirtualBox 6.0	Full support	December 2023
VirtualBox 7.0	Full support	NA

DVM repository requirements

When you create a Deduplication Volume Manager (DVM) repository, you can specify its location on a local storage volume or on a storage volume on a Common Internet File System (CIFS) shared location. If creating the repository locally on the Core server, you must allocate resources accordingly.

DVM repositories must be stored on primary storage devices. Archival storage devices such as Data Domain are not supported due to performance limitations. Similarly, repositories should not be stored on NAS filers that tier to the cloud, as these devices tend to have performance limitations when used as primary storage.

Questrecommends locating your repository on direct attached storage (DAS), storage area network (SAN), or network attached storage (NAS) devices. These are listed in order of preference. If installing on a NAS, Quest recommends limiting the repository size to 6TB when using the CIFS protocol, since CIFS is not designed as a high-I/O storage protocol. Any storage device must meet the minimum input/output requirements. For these requirements, and for additional guidance for sizing your hardware, software, memory, storage, and network requirements, see the *Rapid Recovery Sizing Guide* referenced below.

When creating a DVM repository, you are required to specify the repository size on a volume. Each DVM repository supports up to 4096 repository extents (additional storage volumes).

Questdoes not support installing a Rapid Recovery Core or a repository for a Core on a cluster shared volume (CSV).

You can install multiple DVM repositories on any volume on a supported physical or virtual host. The installer lets you determine the size of a DVM repository.

NOTE: You can generate an on-demand or scheduled report to monitor the size and health of your repository. For more information on generating a Repository report, see the topic "Generating a report from the Core Console" in the *Rapid Recovery User Guide*.

Always create your repository in a dedicated folder or directory, not the root folder on a volume. For example, if installing on a local path, use `D:\Repository\` instead of `D:\`. The best practice is to create separate directories for data and metadata. For example, `D:\Repository\Data` and `D:\Repository\Metadata`.

For more information about using Rapid Recovery, see the *Rapid Recovery User Guide*. For more information about managing Rapid Recovery licenses from the Core Console, see the "Managing licenses" topic in the *Rapid Recovery Installation and Upgrade Guide*. For more information about administering license groups or licenses on the license portal, see the *Rapid Recovery License Portal User Guide*. For more information on sizing your

hardware, software, memory, storage, and network requirements, see the *Rapid Recovery Sizing Guide* referenced in knowledge base article 185962, “Sizing Rapid Recovery Deployments.”

License requirements

New Core users must purchase a long-term subscription or perpetual license to use Rapid Recovery.

Some Rapid Recovery Core users start with a trial license, which uses a temporary license key for the duration of the trial. After the trial period expires, you can continue to restore from existing backups, but cannot perform new backups or replication until you purchase a long-term subscription or perpetual license. You must then activate the license on the Rapid Recovery License Portal, download Rapid Recovery license files, and associate them with your Core.

For more information about licensing, see the following resources:

- For information about activating your new license and obtaining Rapid Recovery license files for your Core, see the topic "Product licensing" in the *Rapid Recovery Release Notes* .
- For information about managing licenses from the Rapid Recovery Core, including uploading license files to associate them with the Core, see the topic "Managing Rapid Recovery licenses" in the *Rapid Recovery Installation and Upgrade Guide.*
- For information about managing license subscriptions and license groups on the license portal, see the *Rapid Recovery License Portal User Guide*.

Quest Support policy

Full support: For customers with a current maintenance contract, Quest Data Protection Support provides call-in or email support for the current major and minor release, when patched to the latest maintenance release. That release is known as N. Quest also fully supports N - 1. For Rapid Recovery, Quest also provides limited support for N - 2. For more information, see "Rapid Recovery support levels" in the *Rapid Recovery Release Notes*.

Limited support: Quest Data Protection Support may attempt to answer questions on other versions of our products, provided resources are available. However, if you are using an unsupported or discontinued version, no new patches or code fixes will be created for those versions. In such cases, we encourage you to upgrade to a currently supported version of the product.

Product support life cycle: Quest describes its product life cycle (PLC) support policy on its Support website (visit https://support.quest.com/rapid-recovery/, click **Product Life Cycle & Policies,** and then expand the topic **Product Support Life Cycle Policy**). To understand full support, limited support, and discontinued support, consult the detailed policy on the website referenced above.

About us

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Office 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. 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