Quest

Rapid Recovery Version 6.2.1

System Requirements Guide

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 - August 2018
Version - Version 6.2.1

Contents

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, regardless of origin. Rapid Recovery can also archive to the cloud, to a DL series backup and recovery appliance, or to a supported system of your choice. 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).
- **Instant recovery**. Our Live Recovery feature allows you to access critical data first, while remaining restore operations complete in parallel.
- **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 Core Console.
- **Virtual support**. Rapid Recovery supports one-time virtual export, letting you generate a bootable VM from a recovery point; and virtual standby, in which the bootable VM you generate is continually updated after each backup. You can even perform virtual export to Microsoft 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 5.5 and higher with no agent software 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 Agent is built with application support for Microsoft Exchange, SQL Server, and Oracle. When you protect these application servers in your Core, the backup snapshots 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 (for SQL Server) and database integrity DBVERIFY checks (for Oracle). Application awareness also extends to agentless protection for SQL Server and Exchange Server.
  For penultimate sentence, use this version for 7.0: Specific application features are supported, including checks for SQL attachability (for SQL Server), database integrity DBVERIFY checks (for Oracle), and database checksum and mountability (for Exchange Server).

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/.

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 which replaced the Central Management Console in Rapid Recovery release 6.2.

In previous releases, system requirements for Rapid Recovery appeared in several technical product documents, but now appear only in this *Rapid Recovery 6.2 System Requirements Guide*.

Topics include:

Recommended network infrastructure

For running Rapid Recovery, Quest requires a minimum network infrastructure of 1 gigabit Ethernet (GbE) for efficient performance. 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.

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 8.1, Windows 10; Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016.
- **Linux:** All supported versions of Linux.

Rapid Recovery also supports the protection and recovery of Resilient File System (ReFS) volumes for Windows 10, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016.

Support for dynamic and basic volumes

Rapid Recovery supports taking snapshots of all dynamic and basic volumes. Rapid Recoveryy 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 Recoveryy 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, you must have installed the Rapid Recovery Agent software 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	2007 Single Copy Cluster (SCC) 2007 Cluster Continuous Replication (CCR)	2008 R2
	2010 Database Availability Group (DAG)	2008 R2
	2013, 2016 DAG	2008 R2 SP1, 2012, 2012 R2
Microsoft SQL Server	2005	2008 R2
	2008, 2008 R2 SCC	2008 R2, 2012, 2012 R2
	2012, 2014 SCC	2008 R2, 2012, 2012 R2
	2012, 2014, 2016, 2017 Availability Groups	2012, 2012 R2, 2016

NOTE: If using SQL Server 2012 or higher with always-on Availability Groups, you must have .NET Framework 3.5 SP1 enabled on the protected server.

NOTE: As of Rapid Recovery 6.2, Windows 2008 is no longer supported. However, protection of a Windows 2008 cluster is supported if it has a release 6.1.x Rapid Recovery Agent installed.

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

Support for Cluster-Shared Volumes

For Agent-based support, Rapid Recovery only supports direct protection and restore of cluster-shared volumes (CSVs) running on Windows Server 2008 R2.

Rapid Recovery 6.1 and later offers agentless support 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 2012, Windows Server 2012 R2, and Windows Server 2016.

In addition, Rapid Recovery release 6.1 and later supports virtual export to Hyper-V CSVs installed on Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016. For information about supported hypervisors, see Hypervisor requirements.

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

Table 2: Rapid Recovery support for VMs on cluster-shared volumes

Operating System	**Protect[1] and Restore[2] VMs on a Hyper-V CSV**			**Virtual Export to Hyper-V CSV**			**Protect[1] and Restore[3] of CSV**		
CSV Operating System	Rapid RecoveryVersion			Rapid Recovery Version			Rapid Recovery Version		
	6.0.x	6.1.x	6.2.x	6.0.x	6.1.x	6.2.x	6.0.x	6.1.x	6.2.x
Windows Server 2008 R2	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes
Windows Server 2012	No	Yes	Yes	Yes	Yes	Yes	No	No	No
Windows Server 2012 R2	No	Yes	Yes	Yes	Yes	Yes	No	No	No
Windows Server 2016	No	Yes	Yes	No	Yes	Yes	No	No	No

[1] Protect includes protection, replication, rollup, mount, and archiving.

[2] Restore includes file-level restore, volume-level restore, bare metal restore, and virtual export.

[3] Restore includes file-level restore, volume-level restore, and bare metal restore.

Rapid Recovery Core installation requirements

Install the Rapid Recovery Core on a dedicated Windows 64-bit server.

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 support contract can manage two or more Cores from the QorePortal.

For each physical machine you want to protect in a Rapid Recovery Core, install the Rapid Recovery Agent software version appropriate to that machine's operating system. You can also protect virtual machines (VMs) on your Core after installing using the Agent software. Optionally, you can use the Rapid Snap for Virtual feature to protect VMs agentlessly. This approach has some limitations. For more information, see the topic "Understanding Rapid Snap for Virtual" in the *Rapid Recovery User Guide*.

Before installing Rapid Recovery, 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: Quest does not support running the Rapid Recovery Core on Windows Core operating systems, which offer limited server roles. This includes all editions of Windows Server 2008 Core, Windows Server 2008 R2 Core, Windows Server 2012 Core, Windows Server 2012 R2 Core, and Windows Server 2016 Core.

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. (This recommendation does not apply to Quest DL series backup and recovery appliances.)

Rapid Recovery release 6.2.1 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 3: Rapid Recovery components and features compatible with Windows operating systems.

Windows OS	Core	Agent	Agent-less	LMU	MR	DR	URC Restore	VM Export to Azure
Windows 7 SP1	No	No	Limited	No	No	No	Limited	Limited[1]

Windows OS	Core	Agent	Agent-less	LMU	MR	DR	URC Restore	VM Export to Azure
Windows 8	No	No	Limited	Yes [2]	Yes [2]	Yes [2]	Limited	Limited[1]
Windows 8.1	No	Limited	Yes	Yes	Yes	Yes	Yes	Yes[1]
Windows 10	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes[1]
Windows Server 2008 R2 SP1	Yes[2]	Yes[2]	Yes	Yes [2]	Yes	Yes	Yes	Yes[1]
Windows Server 2012	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes[1]
Windows Server 2012 R2	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes[1]
Windows Server 2016	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Windows installation and support notes:

[1] VM export to Azure works only for x64 editions of operating systems listed. EFI is not supported. Azure VMs do not support Generation 2 Hyper-V VM features. For more information about these features, see "Generation 2 Virtual Machine Overview" in the Microsoft Technet article at https://technet.microsoft.com/library/dn282285.aspx.

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

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 4: Compatible Rapid Recovery components and features by Linux operating system

OS or distribution	Agent	Agentless	Live DVD	VM Export to Azure	Standard / Extended End of Life
Red Hat Enterprise Linux 6.3 - 6.9	Yes	Yes	Yes	Yes	November 2020 / TBD
Red Hat Enterprise Linux 7.0 - 7.2	Yes	Yes	Yes	Yes	June 2024 / TBD
Red Hat Enterprise Linux 7.3 - 7.4	Yes	Yes	Yes	Yes	June 2024 / TBD
CentOS Linux 6.3 - 6.9	Yes	Yes	Yes	Yes	November 2020
CentOS Linux 7.0 - 7.2	Yes	Yes	Yes	Yes	June 2024
CentOS Linux 7.3 - 7.4	Yes	Yes	Yes	Yes	June 2024
Debian Linux 7	Limited [2]	Limited[2]	Limited [2]	No	May 2018
Debian Linux 8	Yes	Yes	Yes	Yes	May 20208

OS or distribution	Agent	Agentless	Live DVD	VM Export to Azure	Standard / Extended End of Life
Debian Linux 9	Yes	Yes	Yes	Yes	June 2022
Oracle Linux 6.3 - 6.9	Yes	Yes	Yes	Yes	May 2021
Oracle Linux 7.0 - 7.4	Yes	Yes	Yes	Yes	July 2024
Ubuntu Linux 12.04 LTS	Limited [2]	Limited[2]	No	Yes	April 2017
Ubuntu Linux 12.10, 13.04, 13.10	Limited [2]	Limited[2]	No	Yes	October 2014
Ubuntu Linux 14.04 LTS	Yes[1]	Yes[1]	Yes[1]	Yes	April 2019
Ubuntu Linux 14.10, 15.04, 15.10	Limited [2]	Limited[2]	Limited [2]	Yes	October 2016
Ubuntu Linux 16.04 LTS	Yes[1]	Yes[1]	Yes[1]	Yes	April 2021
Ubuntu Linux 16.10	Yes[1]	Yes[1]	Yes[1]	Yes	October 2017
Ubuntu Linux 17.04 LTS	Yes[1]	Yes[1]	Yes[1]	Yes	April 2018
Ubuntu Linux 17.10	Limited [1, 2]	Limited[1, 2]	Limited [1, 2]	Yes	October 2018
Ubuntu Linux 18.04 LTS	Yes[1]	Yes[1]	Yes[1]	Yes	April 2023
SUSE Linux Enterprise Server (SLES) 11 SP2 (or later SP)	Yes	Yes	Yes	Yes	March 2019 / March 2022
SLES 12, 12 SP1 (or later SP)	Yes[1]	Yes[1]	Yes[1]	Yes	October 2024 / October 2027

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 OS distribution has reached end of life, and is therefore no longer tested. Support for this OS is therefore limited.

Rapid Recovery Core requirements

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

Table 5: 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 8.1* • Microsoft Windows 10

Requirement	Details
	• Microsoft Windows Server 2008 R2 SP1* (except Core editions) • Microsoft Windows Server 2012, 2012 R2* (except Core editions) • Microsoft Windows Server 2016 (except Core editions) Windows operating systems require the Microsoft .NET Framework version 4.6.2 to be installed to run the Rapid Recovery Core service. Additionally, any OS marked with * requires the ASP .NET 4.6.2. role or feature. When installing or upgrading the Core, the installer checks for these components based on the OS of the Core server, and installs or activates them automatically if required. Installing or upgrading .NET software typically requires a system reboot. The Rapid Recovery Core supports all x64 editions of the Windows OS listed, unless otherwise indicated. The Rapid Recovery Core does not support Windows Server core editions. If any operating system listed specifies a service pack (for example, Windows Server 2008 R2 SP1), then the OS with the specified service pack is the minimum requirement. If an operating system is listed without a service pack (for example, Windows 8.1), then the base operating system is supported. Any subsequent SP for a listed OS is also supported, unless explicitly excluded. For optimal performance, it is recommended that you install the Rapid Recovery Core on more recent operating systems such as Windows 8.1 (or later) and Windows Server 2012 (or later).
Architecture	64-bit only
Memory	8GB RAM or more. Quest highly recommends using Error Checking & Correction (ECC) memory, to ensure optimum performance of Rapid servers.
Processor	Quad-core or higher
Storage	The amount of storage required differs based on your needs and choice of repository technology type. Rapid Recovery supports two primary technology types: **DVM repositories**. Rapid Recovery supports primary storage in a classic DVM repository. Characteristics and 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. • Requires a configuration of RAID 6 with 4 usable drives or better for a change rate per hour of up to 10GB. More drives are required 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.

NOTE: This feature is deprecated. Tiering repositories will not be supported in Rapid Recovery7.0 or later releases.

Requirement	Details
	NOTE: This feature is deprecated. Tiering repositories will not be supported in Rapid Recovery7.0 or later releases. See Quest knowledge base article 185962, "Sizing Rapid Recovery Deployments" for additional guidance in 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

Requirements for the Rapid Recovery Agent software are described in the following table.

NOTE: Rapid Recovery Agent cannot be deployed to a machine with a Linux operating system installed using the Add-on for Kaseya. If using that add-on, you must install the Agent on a Linux machine manually. For more information, see the *Rapid Recovery 6.2 User Guide*.

Table 6: Rapid Recovery Agent software requirements

Requirement	Details
Operating system	The Rapid Recovery Agent software supports 32-bit and 64-bit Windows and Linux operating systems, including the following: • Microsoft Windows 8.1[1, *] • Microsoft Windows 10 • Microsoft Windows Server 2008 R2 SP1 (all editions except Windows Server 2008 Core). Follow guidance in Microsoft KB 3033929. • Microsoft Windows Server 2012, 2012 R2* • Microsoft Windows Server 2016* • Red Hat Enterprise Linux (RHEL) 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9, 7.0, 7.1, 7.2, 7.3, 7.4 • CentOS Linux 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9, 7.0, 7.1, 7.2, 7.3, 7.4 • Oracle Linux 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9, 7.0, 7.1, 7.2, 7.3, 7.4 • Debian Linux 7, 8, 9

Requirement	Details
	• Ubuntu Linux 12.04 LTS, 12.10, 13.04, 13.10, 14.04 LTS, 14.10, 15.04, 15.10, 16.04 LTS, 16.10, 17.04, 18.04 LTS[2, 3] • SUSE Linux Enterprise Server (SLES) 11 (SP2 and later), 12 (SP1 and later) [1] Only limited support for Agent as of this release in DVM repositories. Agentless protection is also supported. [2] BTRFS is supported on kernels 3.7 and later. [3] Since Ubuntu Linux versions 12.04 LTS, 12.10, 13.04, 13.10, 14.10, 15.04, 15.10 have reached end of life and are no longer tested, support is limited. * Any OS marked with * requires the ASP .NET 4.6.2 role or feature.
	NOTE: Windows operating systems require the Microsoft .NET Framework version 4.6.2 to be installed to run the Rapid Recovery Agent service. Operating systems listed above that are marked with * also require the ASP .NET 4.6.2. role or feature. When installing or upgrading the Rapid Recovery Agent software, the installer checks for these components, and installs or activates them automatically if required. Installing or upgrading .NET software typically requires a system reboot. Additional operating systems are supported for agentless protection only. For more information, see Rapid Snap for Virtual agentless protection. If any operating system listed specifies a service pack (for example, Windows 2008 R2 SP1), then the OS with the specified service pack is the minimum requirement. If an operating system is listed without a service pack (for example, Windows 8.1), then the base operating system is supported. Any subsequent SP for a listed OS is also supported, unless explicitly excluded. The Rapid Recovery Agent software supports Windows Server Core edition installations for Windows Server 2008 R2 , Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016. For Windows Server 2008 R2 Core only, you must have SP1 or later. The Rapid Recovery Agent software supports the Linux distributions included in this list. Most of the released kernel versions have been tested. File systems supported include ext2, ext3, ext4, and xfs. BTRFS is also supported (only on SLES 12, SLES 12 SP1, and SLES 12 SP2 with kernel version 3.7 or later). For more information, see the Rapid Recovery release 6.2.1 operating system installation and compatibility matrix. Agents installed on Microsoft Hyper-V Server 2012, 2012 R2, and 2016 operate in the Core edition mode of the relevant Windows Server OS. **NOTE:** Native backup of cluster shared volumes is supported on Windows 2008 R2 (SP1 and later) protected machines only.
Architecture	32-bit or 64-bit
Memory	4GB or higher
Processor	Single processor or higher
Microsoft Exchange Server support	Microsoft Exchange Server 2007 SP1 Rollup 5 or later, Exchange Server 2010, Exchange Server 2013, or Exchange Server 2016.

Requirement	Details
	NOTE: End of life for Exchange Server 2007 was April 11, 2017. This application will not be supported in future releases. Users are advised to move to a current version of Exchange Server.
Microsoft SQL Server support	Microsoft SQL Server 2008, SQL Server 2008 R2, SQL Server 2012, SQL Server 2014, SQL Server 2016, SQL Server 2017 are supported on Windows machines only (no Linux support). **NOTE:** End of life for SQL Server 2008 and 2008 R2 is July 9, 2019. Users are advised to move to a current version of SQL Server that is supported by both Microsoft and Quest in advance of that date.
Microsoft SharePoint Server support	Microsoft SharePoint 2007, 2010, 2013, 2016 **NOTE:** Support for "SharePoint" refers to fully licensed versions of Microsoft SharePoint Server for the versions listed above.
Oracle relational database support	Oracle 12c database using Rapid Recovery6.2.1 or later on 64-bit servers running Windows Server 2012 R2 or Windows Server 2016. Oracle support includes application awareness. You can perform database integrity checks against our volume images using DBVERIFY (a native Oracle utility). Protection of Oracle12c databases is limited to using Volume Snapshot Service (VSS) in the ARCHIVELOG mode. For more information, see "About protecting Oracle database servers" in the . *Rapid Recovery 6.2 User Guide*
Storage	Direct attached storage, storage area network or network attached storage
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 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://dataprotection.quest.com/settings/downloads), or theRapid Recovery License Portal (at https://licenseportal.com/Downloads).

Table 7: 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 8.1* • Microsoft Windows 10 • Microsoft Windows Server 2008 R2 SP1 (all editions except Windows Server 2008 R2 Core) • Microsoft Windows Server 2012, 2012 R2* • Microsoft Windows Server 2016* **NOTE:** Windows operating systems require the Microsoft .NET Framework version 4.6.2 to be installed to run the Local Mount Utility service. Operating systems listed above that are marked with * also require the ASP .NET 4.6.2. role or feature. When installing or upgrading the LMU, the installer checks for these components, and installs or activates them automatically if required. Installing or upgrading .NET software typically requires a system reboot. If any operating system listed specifies a service pack (for example, Windows Server 2008 R2 SP1), then the OS with the specified service pack is the minimum requirement. If an operating system is listed without a service pack (for example, Windows 8.1), then the base operating system is supported. Any subsequent SP for a listed OS is also supported, unless explicitly excluded. The LMU software supports Windows Server Core edition installations for Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016. 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.
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 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 6.2 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 6.2, 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 4.6.2 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 releases 6.1.3 and 6.0.2 run Microsoft .NET Framework version 4.5.2, which supports some older Microsoft operating systems. You can protect machines running these versions of Agent in a Rapid Recovery 6.2 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 Core6.2.1. 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 6.2 Release Notes*.

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

You can protect VMware ESXi virtual machines running operating systems that do not support .NET Framework version 4.5.2, such as Windows XP SP3, Windows Vista (prior to SP2), Windows Server 2003, and Windows Server 2008.

You can also protect VMware ESXi virtual machines running operating systems that do not support .NET Framework version 4.6.2, such as Windows 7 SP1, Windows 8, Windows Server 2008 SP2.

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 current or 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 release 7.0.0 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 the *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.

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 to restore operations, and then perform recovery.

Rapid Recovery lets you perform virtual export to VM hosts described in the following table.

Table 8: Hypervisor requirements supporting virtual export

Requirement	Details
Virtual machine host	VMware: • VMware Workstation 7, 8, 9, 10, 11, 12

NOTE: For virtual export to any Hyper-V host, .NET 4.6.2 and .NET 2.0 are required on the Hyper-V host.

Requirement	Details

	• First generation:
	  • Hyper-V running on Microsoft Server versions 2008 SP2, 2008 R2 SP1, 2012, 2012 R2, 2016
	  • Hyper-V running on Microsoft Windows 8, 8.1, 10 with Hyper-V
	• Second generation:
	  • Hyper-V running on Microsoft Server 2012 R2, 2016
	  • Hyper-V running on Microsoft Windows 8.1, Windows 10
	Quest recommends installing Hyper-V Integration Services on VMs you want to protect on Hyper-V hosts.
	NOTE: Only protected machines with the following Unified Extensible Firmware Interface (UEFI) operating systems support virtual export to Hyper-V second-generation hosts:
	  • Windows 8 (UEFI)
	  • Windows 8.1 (UEFI)
	  • Windows 10 (UEFI)
	  • Windows Server 2012 (UEFI)
	  • Windows Server 2012 R2 (UEFI)
	  • Windows Server 2016 (UEFI)
	Hyper-V export to second-generation VM can fail if the Hyper-V host does not have enough RAM allocated to perform the export.
	Oracle VirtualBox:
	• VirtualBox 5.1 and higher
	NOTE: When exporting to ESXi, Hyper-V, or VMware Workstation, you must use the full licensed versions of those hypervisors, not free versions.

Guest (exported) operating system	**Volumes under 2TB.** For protected volumes under 2TB, the VM (guest) can use the same supported operating systems described in the topic Rapid Recovery Agent software requirements. **Volumes over 2TB.** If you want to perform virtual export on a system for which the protected volumes exceed 2TB, use a Hyper-V host running Windows 2012 R2, Windows Server 2016, VMware ESXi 5.5, or VMware ESXi 6.0. Earlier operating systems are not supported. Both Hyper-V generation 1 and generation 2 VMs are supported. **NOTE:** Not all operating systems are supported on all hypervisors.
Storage	The storage reserved on the host must be equal to or larger than the storage in the guest VMs.
Architecture	32-bit or 64-bit

Rapid Recovery lets you protect VM hosts without installing the Rapid Recovery Agent software on each guest. This is known as agentless protection. For more information, including exclusions for agentless protection, see the*Rapid Recovery 6.2 User Guide* topic "Understanding Rapid Snap for Virtual."

Agentless protection is supported as described in the following table.

Table 9: Hypervisor requirements supporting agentless or host-based protection

Requirement	Details

Virtual machine host	**VMware:**
	• VMware vSphere on ESXi 5.5, 6.0, 6.5.
	• You should also install the latest VMware Tools on each guest.
	• **NOTE:** The following limitations apply to agentless protection using vSphere/ESXi version 6.5:
	  ◦ Secure Boot is a new ESXi 6.5 feature. Rapid Recovery release 6.2 and later supports this feature, including virtual export to vCenter/ESXi 6.5 if the source machine uses the Secure Boot option. The source Virtual Machine must have an Extensible Firmware Interface (EFI) system partition, and the target exported VM must be ESXi 6.5 or later.
	  ◦ ESXi 6.5 introduced support for encrypted VMs, which requires Virtual Disk Development Kit (VDDK) version 6.5. Support for VDDK 6.5 for agentless protection is included inRapid Recovery release 6.2 and later. Agentless protection of encrypted VMs in ESXi version 6.5 or later by earlier Rapid Recovery releases is not supported.
	• **NOTE:** Quest strongly recommends running on the most recent supported VMware version.
	Microsoft Hyper-V:
	• Windows Server 2012 R2
	• Windows Server 2016
	• Windows 8 x64
	• Windows 8.1 x64
	• Windows 10 x64

Operating system	For volume-level protection, volumes on guest VMs must have GPT or MBR partition tables. If other partition tables are found, protection occurs at the disk level, not at the volume level.
Storage	The storage reserved on the host must be equal to or larger than the storage in the guest VMs.
Architecture	32-bit or 64-bit

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.

Quest recommends 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).

Quest does 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 6.2 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 6.2 User Guide*. For more information about managing Rapid Recovery licenses from the Core Console, see the "Managing licenses" topic in the *Rapid Recovery 6.2 User Guide* or the *Rapid Recovery 6.2 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."

Tiering repository requirements

A tiering repository is a secondary repository defined on your Core into which recovery points can be relocated from a primary DVM repository. Once they are moved, recovery points are deleted from your primary DVM repository. The Core continues to manage the relocated recovery points until they are eventually rolled up and deleted.

In release 6.2, tiering is only supported on DR Series deduplication appliances running OS 4.0. The repository requires RDS services native to the DR appliance.

The tiering feature, supported in releases 6.1 and 6.2 only, is deprecated. This feature is not expected to be included in future releases.

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 licenses for your Core, see the topic "Licensing Rapid Recovery software and appliances" in the *Rapid Recovery 6.2 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 licenses" in the *Rapid Recovery 6.2 User Guide* or the *Rapid Recovery 6.2 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

For customers with a valid support agreement, Quest 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 and N - 2. Intermediate versions receive limited support.

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 Product Support Life Cycle Policy). To understand full support, limited support, and discontinued support, consult the policy referenced above.

About us

We are more than just a name

We are on a quest to make your information technology work harder for you. That is why we build community-driven software solutions that help you spend less time on IT administration and more time on business innovation. We help you modernize your data center, get you to the cloud quicker and provide the expertise, security and accessibility you need to grow your data-driven business. Combined with Quest's invitation to the global community to be a part of its innovation, and our firm commitment to ensuring customer satisfaction, we continue to deliver solutions that have a real impact on our customers today and leave a legacy we are proud of. We are challenging the status quo by transforming into a new software company. And as your partner, we work tirelessly to make sure your information technology is designed for you and by you. This is our mission, and we are in this together. Welcome to a new Quest. You are invited to Join the Innovation™.

Our brand, our vision. Together.

Our logo reflects our story: innovation, community and support. An important part of this story begins with the letter Q. It is a perfect circle, representing our commitment to technological precision and strength. The space in the Q itself symbolizes our need to add the missing piece — you — to the community, to the new Quest.

Contacting Quest

For sales or other inquiries, visit www.quest.com/contact.

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