Quest™

DL4300 Appliance

Release Notes

Table of Contents

Introduction

This document describes important product information and additional information on the Quest DL4300 Appliance.

NOTE: For more information on the new features in this release see the Quest DL4300 Appliance Deployment Guide at quest.com/support/manuals.

About Rapid Recovery Software

The Rapid Recovery software offers near-zero recovery time objectives and recovery point objectives. More than disaster recovery, Rapid Recovery software offers data solutions for data migration and 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. The Rapid Recovery software can also archive to the cloud, to a Quest DL series backup and recovery appliance, or to a supported system of your choice. With the Rapid Recovery software, you can replicate to one or more targets for added redundancy and security.

For more information, see: https://support.quest.com.

Parent topic

Other information you may need

NOTE: Always check for updates on support.quest.com and read the updates first because they often supersede information in other documents.

NOTE: For documentation related to Dell OpenManage Server Administrator, see dell.com/support.

You product documentation includes:

Getting Started Guide

Provides an overview of system features, setting up your system, and technical specifications. This document is also shipped with your system.

Owner's Manual

Provides information about system features and describes how to troubleshoot the system and install or replace system components.

Deployment Guide

Provides information on hardware deployment and the initial deployment of the appliance.

User's Guide

Provides information about configuring and managing the system.

OpenManageServer Administrator User's Guide

Provides information about using Dell OpenManage Server Administrator to manage your system.

System Placemat

Provides information on how to set up the hardware and install the software on your solution.

NOTE: The system placemat information is included in the Getting Started Guide.

Resource Media

Any media that ships with your system that provides documentation and tools for configuring and managing your system, including those pertaining to the operating system, system management software, system updates, and system components that you purchased with your system.

Interoperability Guide

Provides information on supported software and hardware for the DL4300 appliance as well as usage considerations, recommendations, and rules.

Parent topic

Known issues and limitations

Table 1. Known issues and limitations

The following table lists the known issue, workaround, old issue ID, new issue ID, functional area, and Siebel ID.

Known Issue	Old Issue ID	New Issue ID	Functional Area	Siebel ID
The "Start VM / Network Adapters" buttons should be all set in a disabled state if ESX(i)/ Hyper-V export of the machine was launched on the appliance. Workaround: Do not click these buttons until the corresponding VM export is complete.	30989	96366	Virtual Machine Management	--
Sometimes the error message" invalid state; already open" appears on the virtual standby tab on DL4x00 appliances. Workaround: Close error message. If issue still presents, reload the page by clicking F5.	31477	96797	Virtual Machine Management	--
VD disk provisioning fails with return code 4 if storage pool has not consistent empty space Workaround: Contact support.	34937	99967	Storage Provisioning	3882937-1
Wrong translation of 'State' some localization in table (section "Items	35031	100061	Localization	--

Known Issue	Old Issue ID	New Issue ID	Functional Area	Siebel ID
Backed Up") on "Backup" tab. Workaround: No workaround.				
Monitor Active Task is hanging on 95% during creation of a RASR USB job. Workaround: The job doesn't hang. It completes successfully. However, sometimes the GUI popup does not reflect the fact that the job is done. Refresh the GUI.	35531	100551	RASR	--
The GUI should be disabled immediately after confirmation of the remount process. Workaround: Wait for a few minutes and refresh the Core Console page.	35579	100599	Storage Provisioning	--
VMM actions are available when the ESXi host is set in maintenance mode. Workaround: Do not perform any VM operations from the "Virtual Standby" tab if ESXi host is in the maintenance mode.	35740	100758	Virtual Machine Management	--
Incorrect behavior of provisioning size determining logic. Workaround: When doing provisioning, specify the size a few GB smaller than the available space.	35770	100787	Storage Provisioning	--

Known Issue	Old Issue ID	New Issue ID	Functional Area	Siebel ID
Core interface becomes unavailable if force collecting Core and Appliance logs. Workaround: Refresh page to make GUI available again.	N/A	100904	UI	--
Storage Provisioning and Restore the Provisioning Configuration jobs could be launched simultaneously in spite of the incompatibility when launching these jobs. Workaround: 1) Remove the created Repository 2 Virtual Disk using OMSA. 2) Restart the Core service.	N/A	100907	Storage Provisioning	--
Windows Backup could not be created due to inappropriate determining of the necessary volume items for backup, if volume name letters were changed. Workaround: Remove current policy with mixed/ changed letters for partitions and create a new policy.	N/A	100985	Windows Backup	--
Statuses of volumes are displayed as "Not valid" if a letter is assigned to the "Recovery" partition.	N/A	101224	Storage Provisioning	--

Known Issue	Old Issue ID	New Issue ID	Functional Area	Siebel ID
Workaround: Wait until the RASR USB creation job is finished.				
Jobs are failing with "System.OutOfMemoryException" on DL appliance message after it has been running for some time. Workaround: Contact support.	N/A	101246	Virtual Export	3830465-1, 3791536-1, 3825434-1
Remounting the job does not restore the core's localization. Workaround: Manually change the Core localization from Core Settings.	N/A	101316	Storage Provisioning	--
Restore the provisioning configuration job fails with an uninformative error "Cannot mount volume to the folder 'I:\' because it contains files or folders" if the virtual disk has the letter that already was used before the remount. Workaround: Remove assigned letters from attached virtual media by using the disk manager. Perform the Volumes Remount job again from the Appliance Provisioning page.	35805	100822	Storage Provisioning	--
"Restrictions" error appears after including the appliance	35828	100845	DL Appliance Configuration Wizard	--

Known Issue	Old Issue ID	New Issue ID	Functional Area	Siebel ID
into the domain and completing FTBU if trying to sign in with the local administrator credentials. Workaround : Login to the OS using the domain administrator credentials.				
The provisioning job fails with an error if the repository name contains three dots in a row. Workaround: Do not use three dots in a row when creating a repository name.	N/A	100913	Storage Provisioning	--
The first launch of Core after FTBU could not be performed successfully due to Compatibility Mode in the browser if the server has been rebooted during FTBU. Workaround: Close browser and launch Core again	N/A	101313	DL Appliance Configuration Wizard	--
The FTBU crashes on launch if a bootable media is used with a system EFI partition connected to the server. Workaround: Do not connect any external media to the Appliance server until the FTBU has finished successfully.	N/A	101457	DL Appliance Configuration Wizard	--

Known Issue	Old Issue ID	New Issue ID	Functional Area	Siebel ID
Core opens with an error indicating some services have failed to initialize after FTBU on DL1300. Workaround: Restart Server.	N/A	101487	DL Appliance Configuration Wizard	--
The FTBU fails when trying to start the Core service that is already in "starting" state. Workaround: Restart the server.	N/A	101554	DL Appliance Configuration Wizard	--

Rapid Recovery system requirements

This section describes the system requirements for installing the Rapid Recovery Core, Rapid Recovery Agent, and Rapid Recovery Central Management Console.

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.

Parent topic

UEFI and ReFS support

Unified Extensible Firmware Interface (UEFI) is a replacement for Basic Input/Output System (BIOS). UEFI is used in the Windows 8, Windows 8.1, Windows 10, Windows Server® 2012, Windows Server 2012 R2, and Windows Server 2016 operating systems. 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.

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

Rapid Recovery also supports UEFI for protected machines with the Linux® distributions we support. These include Red Hat® Enterprise Linux® (RHEL®), CentOS™, Debian ®, Ubuntu®, SUSE® Enterprise Linux (SLES®), and Oracle® Linux.

Parent topic

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 the 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 with the 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.

Parent topic

Support for Cluster Shared Volumes

Rapid Recovery release 6.1 lets you protect, restore, replicate, and archive virtual machines hosted on cluster-shared volumes (CSVs) running on Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 with the Rapid Recovery Agent software.

For CSVs running on Windows Server 2008 R2, Rapid Recovery supports native backup. You can restore CSVs from a recovery point, or perform virtual export to a Hyper-V CSV. There is no support for cluster-shared volumes running on earlier Windows operating systems, such as Windows 2008.

Rapid Recovery does not support virtual export of a cluster-shared volume protected using Rapid Recovery Agent.

In contrast, in Rapid Recovery release 6.1, you can perform virtual export to a Hyper-V CSV running Windows Server 2012, Windows Server 2012 R2, or Windows Server 2016.

For other operating systems, the Rapid Recovery Agent service can be run on all nodes in a cluster, and the cluster can be protected as a cluster within the Rapid Recovery Core. However, CSVs do not display in the Core Console and are not available for protection. All local disks (such as the operating system volume) are available for protection.

The following table depicts current support in Rapid Recovery Core for cluster-shared volumes protected with Rapid Recovery Agent.

Table 2. Rapid Recovery support for cluster-shared volumes on machines protected with Rapid Recovery Agent

The following table depicts current support in Rapid Recovery Core for cluster-shared volumes protected with Rapid Recovery Agent.

Rapid Recovery Cluster Shared Volumes Support	Protect, Replicate, Rollup, Mount, and Archive		Restore CSV Volumes		Virtual Export to Hyper-V CSV	
Rapid Recovery version	6.0.x	6.1	6.0.x	6.1	6.0.x	6.1
Windows Server 2008 R2	Yes	Yes	Yes	Yes	Yes	Yes
Windows Server 2012	No	No	No	No	Yes	Yes
Windows Server 2012 R2	No	No	No	No	Yes	Yes
Windows Server 2016	No	No	No	No	No [1]	Yes

[1] Windows Server 2016 was not tested on Rapid Recovery release 6.0.x and is therefore not supported.

If using Hyper-V host-based protection, Rapid Recovery release 6.1 supports protection of VMs on Hyper-V cluster-shared volumes running Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016. The VMs themselves are protected, not the volumes.

Table 3. Support for cluster-shared volumes using host-based protection on Hyper-V

The following table depicts current levels of support in Rapid Recovery Core for cluster-shared volumes protected using host-based protection on Hyper-V guests.

	Windows Server 2012	Windows Server 2012 R2	Windows Server 2016
Protect, Replicate, Rollup, Mount, and Archive VMs on CSV	No [1]	Yes	Yes
Restore VMs hosted on CSV	No [1]	Yes	Yes
Virtual Export from	No [1]	Yes	Yes

	Windows Server 2012	Windows Server 2012 R2	Windows Server 2016
Hyper-V CSV			
Virtual Export to Hyper-V CSV	No [1]	Yes	Yes

[1] Windows Server 2012 is not supported in this scenario. Full support (and future functionality) for CSVs using Hyper-V host-based protection is planned primarily for Windows Server 2012 R2 and later operating systems.

Parent topic

Hypervisor support in Rapid Recovery

In general, Rapid Recovery protects virtual machine guests hosted on a hypervisor (such as KVM or XenServer) using the Rapid Recovery Agent software.

Each protected machine hosted on a hypervisor must meet or exceed documented system requirements. See for OS, architecture, memory, processor, server application, storage, network, and network hardware requirements.

Individual hypervisors may also restrict support to specific operating systems. See appropriate documentation for each relevant hypervisor.

For successful use of Rapid Recovery, the overarching requirement is that Cores are properly sized, and have sufficient resources and infrastructure to support backup, replication, and other features you need. These resources are in addition to any requirements for the original purpose of the machines. For guidance for sizing your hardware, software, memory, storage, network, and network hardware, see knowledge base article 185962, "Sizing Rapid Recovery Deployments."

Agentless support for hypervisors in Rapid Recovery release 6.0.2 is limited to VMware/ESXi. Guest machines must meet other requirements such as installation of VMware Tools. Rapid Recovery release 6.1 agentless support includes host-based support for Hyper-V, in which the Agent software is required only on the host. For more information about agentless support, see Rapid Snap for Virtual agentless protection.

Virtual export is supported only for VMware/ESXI, Hyper-V, and VirtualBox hypervisors and on the Azure platform.

Parent topic

Virtual export hypervisor license requirements

Rapid Recovery Core supports virtual export to a variety of hypervisor platforms. When exporting to ESXi, Hyper-V, or VMware Workstation, you must use the full licensed versions of those hypervisors, not free versions.

Parent topic

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. As an example, do not use the Core machine to also serve as a hypervisor host (unless the server is an appropriately sized Quest DL series backup and recovery appliance).

As another example, do not use the Core server as a high-traffic web server. If possible, do not install and run Microsoft Exchange Server, SQL Server®, or Microsoft SharePoint® 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. Optionally, for remote management of multiple Cores, you can install the Rapid Recovery Central Management Console on a 64-bit Windows computer.

For each machine you want to protect in a Rapid Recovery Core, install the Rapid Recovery Agent software version appropriate to that machine's operating system. Optionally, you can protect virtual machines on a VMware ESXi host without installing the Rapid Recovery Agent. This agentless protection has some limitations. For more information, see Rapid Snap for Virtual agentless protection.

Before installing Rapid Recovery release 6.1, 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. Excluding Windows Server 2008 Core, these Core edition operating systems are supported for running the Rapid Recovery Agent software.

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 the Hyper-V host. (This recommendation does not apply to Quest DL series of backup and recovery appliances.)

Parent topic

Rapid Recovery release 6.1 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.

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

Table 4. Rapid Recovery components and features compatible with Windows operating systems

This table lists each supported Windows OS and the Rapid Recovery components compatible with it.

Windows OS	Core/ Central Management Console	Agent	Agentless	LMU	MR	DR	URC Restore	VM Export to Azure
Windows XP SP3	No	No	Yes	No	No	No	Yes[1]	No
Windows Vista™	No	No	Yes	No	No	No	Yes[1]	No
Windows Vista SP2	No	Yes	Yes	Yes	Yes	Yes	Yes[1]	No
Windows 7	No	No	Yes	No	No	No	Yes	Yes[3]
Windows 7 SP1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes[3]
Windows 8	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes[3]
Windows 8.1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes[3]
Windows 10	Yes[2]	Yes[2]	Yes[2]	Yes	Yes	Yes	Yes	Yes[3]
Windows Server 2003	No	No	Yes	No	No	No	Yes[1]	No
Windows Server 2008	No	No	Yes	No	No	No	Yes[1]	Yes[3]
Windows Server 2008 SP2	Yes	Yes	Yes	Yes	Yes	Yes	Yes[1]	Yes[3]
Windows Server 2008 R2	No	No	Yes	No	No	No	Yes	Yes[3]
Windows Server 2008 R2 SP1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes[3]

Windows OS	Core/ Central Management Console	Agent	Agentless	LMU	MR	DR	URC Restore	VM Export to Azure
Windows Server 2012	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes[3]
Windows Server 2012 R2	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes[3]
Windows Server 2016	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Windows installation and support notes:

[1] The boot CD supports bare metal restore, but does not support driver injection.

[2] In general, AppAssure 5.4.x and Rapid Recovery 6.x components work on Windows 10, with two exceptions:

- SCSI controller drivers are missing in Windows 10 machines exported to VirtualBox hypervisor.

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

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 5. Compatible Rapid Recovery components and features by Linux operating system

This table lists each supported Linux distribution and the Rapid Recovery components compatible with it.

Linux OS or distribution	Agent	Agentless	Live DVD
Red Hat Enterprise Linux 6.3 - 6.8	Yes	Yes	Yes
Red Hat Enterprise Linux 7.0 - 7.2	Yes	Yes	Yes
CentOS Linux 6.3 - 6.8	Yes	Yes	Yes
CentOS Linux 7.0 - 7.2	Yes	Yes	Yes
Debian Linux 7, 8	Yes	Yes	Yes
Oracle Linux 6.3 - 6.8	Yes	Yes	Yes
Oracle Linux 7.0 - 7.2	Yes	Yes	Yes
Ubuntu Linux 12.04 LTS, 12.10	Yes	Yes	Yes

Linux OS or distribution	Agent	Agentless	Live DVD
Ubuntu Linux 13.04, 13.10	Yes	Yes	Yes
Ubuntu Linux 14.04 LTS, 14.10	Yes[1]	Yes[1]	Yes[1]
Ubuntu Linux 15.04, 15.10	Yes[1]	Yes[1]	Yes[1]
Ubuntu Linux 16.04 LTS	Yes[1]	Yes[1]	Yes[1]
SUSE Linux Enterprise Server 11 SP2 or later	Yes	Yes	Yes
SUSE Linux Enterprise Server 12	Yes[1]	Yes[1]	Yes[1]

Linux installation and support notes:

[1] B-tree file system (BTRFS) is supported only on operating systems with kernel version 4.2. or later. Compliant operating systems currently include Ubuntu versions 14.04.4, 15.10, and 16.04. SUSE Linux Enterprise Server versions 12 and 12 SP1 have older kernel versions, and so Rapid Recovery does not support their implementations of BTRFS.

Parent topic

Rapid Recovery Core and Central Management Console requirements

Requirements for the Rapid Recovery Core and the Central Management Console (CMC) are described in the following table.

Operating system requirements for the Central Management Console are identical to the requirements for the Rapid Recovery Core. These components can be installed on the same machine or on different machines, as your needs dictate.

Table 6. Rapid Recovery Core and Central Management Console requirements

The first column of the following table lists the requirement, including operating system, architecture, memory, processor, storage, network and network hardware. The second column includes specific details for each.

Requirement	Details
Operating system	The Rapid Recovery Core and Central Management Console require one of the following 64-bit Windows operating systems (OS). They do not run on 32-bit Windows systems or any Linux distribution. Rapid

Requirement	Details
	Recovery Core requires one of the following x64 Windows operating systems: • Microsoft Windows 7 SP1 • Microsoft Windows 8, 8.1* • Microsoft Windows 10 • Microsoft Windows Server 2008 SP2, 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 .NET Framework 4.5.2 to be installed to run the Rapid Recovery Core service. Additionally, any OS marked with * requires the ASP .NET 4.5x 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. 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 7 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), 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 Recovery Core servers.
Processor	Quad-core or higher
Storage	Quest recommends locating your repository on direct attached storage (DAS), storage area network (SAN), or network attached storage (NAS) devices (listed in order of preference).

Requirement	Details
	NOTE: If installing on a NAS, Quest recommends limiting the repository size to 6TB. Any storage device must meet the minimum input/output requirements. See Quest knowledge base article 185962, "Sizing Rapid Recovery Deployments" for 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.

Parent topic

Rapid Recovery Agent software requirements

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

Table 7. Rapid Recovery Agent software requirements

The first column of the following table lists Agent software requirements, including operating system, architecture, memory, processor, Exchange Server, SQL Server, SharePoint, storage, network and network hardware. The second column includes specific details for each.

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 Vista SP2 • Microsoft Windows 7 SP1 • Microsoft Windows 8, 8.1* • Microsoft Windows 10 • Microsoft Windows Server 2008 SP2, 2008 R2 SP1 (all editions except Windows Server 2008 Core) • 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, 7.0, 7.1, 7.2 • CentOS Linux 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 7.0, 7.1, 7.2 • Oracle Linux 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 7.0, 7.1, 7.2 • Debian Linux 7, 8 • Ubuntu Linux 12.04 LTS, 12.10, 13.04, 13.10, 14.04 LTS, 14.10, 15.04, 15.10, 16.04 LTS • SUSE Linux Enterprise Server (SLES) 11 (SP2 and later), 12 NOTE: Windows operating systems require the Microsoft .NET framework version 4.5.2 to be installed to run the Rapid Recovery Agent service. Operating systems listed above that are marked with * also require the ASP .NET 4.5.x 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. 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 7 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), 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

Requirement	Details
	must have SP1 or later. Windows Server 2008 Core edition is not supported. 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 certain Linux operating systems with kernel version 4.2. or later). For more information, see the Rapid Recovery release 6.1 operating system installation and compatibility matrix. Agents installed on Microsoft Hyper-V Server 2012 operate in the Core edition mode of Windows Server 2012. NOTE: Native backup of cluster shared volumes is supported on Windows 2008 R2 (SP2 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
Microsoft SQL Server Support	Microsoft SQL Server 2008 or higher
Microsoft SharePoint	Microsoft SharePoint 2007, 2010, 2013, 2016
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.

Requirement	Details
	NOTE: Quest recommends testing your network performance regularly and adjusting your hardware accordingly.

Parent topic

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 Core Console or the Rapid Recovery License Portal.

Table 8. Local Mount Utility software requirements

The following table lists requirements for the Local Mount Utility included with Rapid Recovery. The first column lists the requirement, including operating system, architecture, memory, processor, network and network hardware. The second column includes specific details for each.

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 Vista SP2 • Microsoft Windows 7 SP1 • Microsoft Windows 8, 8.1* • Microsoft Windows 10 • Microsoft Windows Server 2008 SP2, 2008 R2 SP1 (all editions except Windows Server 2008 Core and 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 4.5.2 to be installed to run the Local Mount Utility service. Operating systems listed above that are marked with * also require the ASP .NET 4.5.x role or feature. When installing or upgrading the LMU, the installer checks for these components, and installs or activates them automatically if required. If any operating system listed specifies a service pack (for example, Windows 7 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), then the base operating system is supported. Any

Requirement	Details
	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 Core edition and Windows Server 2008 R2 Core edition are 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.

Parent topic

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 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 support for other operating systems

Rapid Recovery release 6.x uses Microsoft .NET 4.5.2, which is not supported by Windows XP SP3, Windows Vista (prior to SP2), Windows Server 2003, and Windows Server 2008. If you protected machines with these

operating systems in an earlier Core version (such as AppAssure Core 5.4.3), the corresponding version of AppAssure Agent (which used an earlier version of .NET) was supported.

You can continue to protect these machines in a Rapid Recovery Core, using the earlier Agent version.

However, protected machines with these operating systems cannot be upgraded to Rapid Recovery Agent release 6.x.

Nonetheless, machines with these Windows operating systems can be protected in a Rapid Recovery release 6.x Core using one of the following methods:

- Protect virtual machines on a VMware ESXi host using agentless protection.
- Install and run an earlier compatible version of Agent on a physical or virtual machine you want to protect. For release 6.0.2, the only supported compatible Agent version for these OS is AppAssure Agent 5.4.3.

VMware ESXi environments are compatible with some operating systems that Quest does not support. For example, Windows XP SP3, Windows Vista (prior to SP2), Windows Server 2003, and Windows Server 2008 have all reached end of life with Microsoft.

During testing, the full range of Rapid Recovery features (backup, restore, replication, and export) functioned properly with these specific operating systems.

Nonetheless, use these operating systems at your own risk. Quest Support will not be able to assist you with issues for operating systems that have reached end of life, or that are listed as unsupported for Rapid Recovery Agent.

Rapid Snap for Virtual (agentless protection) support limitations

For a list of supported operating systems, see Rapid Recovery release 6.1 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.

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 Support representative. Reporting such difficulties lets Quest potentially include specific incompatibilities in knowledge base articles or future editions of release notes.

Parent topic

Hypervisor requirements

A hypervisor creates and runs virtual machines (guests) on a host machine. Each guest has its own operating system.

Using the virtual export feature of Rapid Recovery, you can perform a one-time virtual export, or define requirements for continual virtual export known as 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 9. Hypervisor requirements supporting virtual export

The following table lists Hypervisor requirements. The first column lists each requirement: virtual machine host, guest OS, storage, and architecture. The second column specifies details for each requirement.

Requirement	Details
Virtual machine host	VMware • VMware Workstation 7.0, 8.0, 9.0, 10, 11, 12 • VMware vSphere on ESXi 5.0, 5.1, 5.5, 6.0 NOTE: Quest recommends running on the most recent supported VMware version. Future major releases of our software are not expected to support ESXi 5.0 and 5.1. Microsoft Hyper-V NOTE: For virtual export to any Hyper-V host, .NET 4.5.2 and .NET 2.0 are required on the Hyper-V host. • 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 with Hyper-V, Windows 10 • Second generation ◦ Hyper-V running on Microsoft Server 2012 R2, 2016 ◦ Hyper-V running on Microsoft Windows 8.1, Windows 10 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 Server 2012 (UEFI) • Windows Server 2012 R2 (UEFI) • Windows Server 2016 (UEFI) NOTE: 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 4.2.18 and higher

Requirement	Details
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 . Volumes over 2TB. If you want to perform virtual export on a system for which the protected volumes exceed 2TB, use Windows 2012 R2, Windows Server 2016, VMware ESXi 5.5, or VMware ESXi 6.0. Earlier operating systems are not supported based on an inability of the host to connect to the virtual hard disk (VHD). 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. This is known as agentless protection. For more information, including exclusions for agentless protection, see the Rapid Recovery User Guide topic "Understanding Rapid Snap for Virtual."

Agentless protection is supported as described in the following table.

Table 10. Hypervisor requirements supporting agentless or host-based protection

The following table lists Hypervisor requirements specific to agentless (or host-based) protection. The first column lists each requirement: virtual machine host, OS, storage, and architecture. The second column specifies details for each requirement.

Requirement	Details
Virtual machine host	VMware • VMware vSphere on ESXi 5.0 (build 623860 or later), 5.1, 5.5, 6.0. • You should also install the latest VMware Tools on each guest. NOTE: Quest strongly recommends running on the most recent supported VMware version. Future major releases of our software are not expected to support ESXi 5.0 and 5.1. Microsoft Hyper-V • Windows Server 2012 R2 • Windows Server 2016 • Windows 8 x64 • Windows 8.1 x64 • Windows 10 x64

Requirement	Details
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

Parent topic

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. 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 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 on using Rapid Recovery, see the Rapid Recovery User Guide. For more information on managing Rapid Recovery licenses, 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.”

Parent topic

Registering your appliance on the license portal

1. In your web browser, navigate to the License Portal at the website URL that was provided to you in the email you received upon purchase.
2. On the Register page, in the Email Address text box, enter the email address associated with your contract.
3. Enter the license number for your appliance.

   If you have multiple appliances, enter a license number and then press Enter to enter additional numbers.
4. Click Activate.

   If the email address that you entered is not registered on the License Portal (if there was a new License Portal account), you are prompted to create an account in the License Portal using that email address.
5. To create an account in the License Portal, enter the necessary information.

   After you register, you are logged on to the License Portal. An activation email is also sent to your email address.
6. A notification of successful registration appears, which also lists the license key. This notification describes the instructions for you to apply the license key to your appliance as follows:
   a. Launch the Core Console for your appliance.
   b. Go to Configuration → Licensing.
   c. Click Change License.
   d. Copy and paste the software license key included in the successful registration notification message, and then save your changes.
7. Click OK.

For more detailed information, see Quest Software License & Product Agreements at https://www.quest.com/legal/license-agreements.aspx.

NOTE: If the used capacity on your DL Appliance exceeds the capacity for which you have purchased a license, the snapshot functionality is disabled. Please contact your Quest Software Group Account Manager for further assistance.

Getting help

Contacting Quest

NOTE: If you do not have an active Internet connection, you can find contact information on your purchase invoice, packing slip, bill, or Quest product catalog.

Quest provides several online and telephone-based support and service options. If you do not have an active Internet connection, you can find contact information on your purchase invoice, packing slip, bill, or Quest product catalog. Availability varies by country and product, and some services may not be available in your area. To contact Quest for sales, technical support, or customer-service issues, go to quest.com/support.

Parent topic

Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your product.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

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

Parent topic

Parent topic