Rapid Recovery 6.1.3

Installation and Upgrade Guide

Table of 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 archive and replicate to the cloud, using cloud storage vendors that support both proprietary and open-source platforms.

- **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-premise, from a remote location, or from the cloud.

- **Virtual support**. Enhanced support for virtualization includes agentless protection and autodiscovery for VMware ESXi 5 and higher, and export to Microsoft Hyper-V cluster-shared volumes.

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 section describes the system and license 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.

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,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 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 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.

Support for Cluster Shared Volumes

Rapid Recovery release 6.1 and later includes the Rapid Snap for Virtual feature. With the Rapid Recovery Agent installed on each node, you can protect and restore supported VMs hosted on Hyper-V cluster-shared volumes (CSVs) installed on 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.

Rapid Recovery only supports protection and restore of CSV volumes running on Windows Server 2008 R2.

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

Table 1. Rapid Recovery support for 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 Recovery Version		Rapid Recovery Version		Rapid Recovery Version	
	6.0.x	6.1.x	6.0.x	6.1.x	6.0.x	6.1.x
Windows Server 2008 R2	No	No	Yes	Yes	Yes	Yes
Windows Server 2012	No	No	Yes	Yes	No	No
Windows Server 2012 R2	No	Yes	Yes	Yes	No	No
Windows Server 2016	No	Yes	No	Yes	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. 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 the topic "Understanding Rapid Snap for Virtual" in the *Rapid Recovery User Guide*.

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.

> ℹ **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.)

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.

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

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

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

Windows OS	Core/ Central Management Console	Agent	Agent-less	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[2]
Windows 7 SP1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes[2]
Windows 8	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes[2]
Windows 8.1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes[2]
Windows 10	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes[2]

Windows OS	Core/ Central Management Console	Agent	Agent- less	LMU	MR	DR	URC Restore	VM Export to Azure
Windows Server 2003	No	No	Yes	No	No	No	Yes[1]	No
Windows Server 2008	No	No	Yes	No	No	No	Yes[1]	Yes[2]
Windows Server 2008 SP2	Yes	Yes	Yes	Yes	Yes	Yes	Yes[1]	Yes[2]
Windows Server 2008 R2	No	No	Yes	No	No	No	Yes	Yes[2]
Windows Server 2008 R2 SP1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes[2]
Windows Server 2012	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes[2]
Windows Server 2012 R2	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes[2]
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] 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 3. 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.

Windows OS	Core/ Central Management Console	Agent	Agentless
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 - 7.3	Yes	Yes	Yes
CentOS Linux 6.3 - 6.8	Yes	Yes	Yes
CentOS Linux 7.0 - 7.3	Yes	Yes	Yes
Debian Linux 7, 8	Yes	Yes	Yes
Oracle Linux 6.3 - 6.8	Yes	Yes	Yes

Windows OS	Core/ Central Management Console	Agent	Agentless
Oracle Linux 7.0 - 7.3	Yes	Yes	Yes
Ubuntu Linux 12.04 LTS, 12.10	Yes	Yes	Yes
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 (SLES) 11 SP2 or later	Yes	Yes	Yes
SLES 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 with service pack 4 or later, and versions 15.10 or later. SLES versions 12 and 12 SP1 have older kernel versions, and so Rapid Recovery does not support their implementations of BTRFS.

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 4. Rapid Recovery Core and Central Management Console requirements

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

Requirement	Details
	any Linux distribution. Rapid 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).
	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.

i	**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.

i	**NOTE:** The 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 User Guide*.

Table 5. 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, 7.3 • CentOS Linux 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 7.0, 7.1, 7.2, 7.3 • Oracle Linux 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 7.0, 7.1, 7.2, 7.3 • 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
	i **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.

Requirement	Details
	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 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.
	i **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 Server support	Microsoft SharePoint 2007, 2010, 2013, 2016 **i** **NOTE:** Support for "SharePoint" refers to fully licensed versions of Microsoft SharePoint Server for the versions listed above.
Storage	Direct attached storage, storage area network or network attached storage
Network	1 gigabit Ethernet (GbE) minimum **i** **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.

Requirement	Details
Network hardware	Use network cables with the appropriate rating to obtain the expected bandwidth. ℹ **NOTE:** Quest recommends testing your network performance regularly 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 Core Console or the Rapid Recovery License Portal.

Table 6. Local Mount Utility software requirements

Requirement	Details
Operating system	The Rapid Recovery Local Mount Utility software supports 32-bit and 64-bit Windows operating systems, including the following: • Microsoft Windows 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* ℹ **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 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

Requirement	Details
Network	1 gigabit Ethernet (GbE) minimum **i** | **NOTE:** Quest recommends a 10GbE network backbone for robust environments.
Network hardware	Use network cables with the appropriate rating to obtain the expected bandwidth. **i** | **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 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 Framework version 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.

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 7. 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, 6.5 **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. **NOTE:** Secure Boot is a new ESXi 6.5 feature. Rapid Recovery support for this feature is planned for the near future. At this time, Rapid Recovery does not support virtual export to vCenter/ESXi 6.5 if the source machine uses the Secure Boot option. Microsoft Hyper-V:

Requirement	Details
	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
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 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 on each guest. 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 8. 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, 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 support for this feature is planned for the near future. At this time, Rapid Recovery does not support virtual export to vCenter/ESXi 6.5 if the source machine uses the Secure Boot option.
	
	    • ESXi 6.5 introduced support for encrypted VMs. However, that feature requires Virtual Disk Development Kit (VDDK) version 6.5. Support for VDDK 6.5 for agentless protection is planned for Rapid Recovery version 7.0.0 and later. Until that change, agentless protection of encrypted VMs in ESXi version 6.5 or higher by Rapid Recovery is not supported.
	
	    • Transfer for VMs agentlessly protected on ESXi 6.5 does not work if the transport mode is set to SAN (storage area network).
	
	ⓘ **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

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. 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.

> **i** | **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."

License requirements

Before you can install Rapid Recovery components, you must register at the Rapid Recovery License Portal, create an account, and obtain a license key or file, which is required to download the Rapid Recovery Core and Rapid Recovery Agent software and to configure and protect machines. To register the Core with the license portal, the server must have internet connectivity, and be able to check in with the license portal on a regular basis.

For more information about the Rapid Recovery License Portal, obtaining a license key, and registering for an account, 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 lifecycle (PLC) support policy on its Support website (visit https://support.quest.com/ rapid-recovery/, click **Policies & PLC,** and then expand **Software Product Support Lifecycle Policy**). To understand full support, limited support, and discontinued support, consult the policy referenced above.

Installing Rapid Recovery

Before you begin installing Rapid Recovery, consider which components are necessary for your implementation, as not all components are required. At minimum, plan to install Rapid Recovery Core on a dedicated Windows server. You may also need to install the Rapid Recovery Agent software on the Windows or Linux machines you want to protect. If your environment consists of only VMware vCenter/ESXi or Hyper-V virtual machines (VMs), you can opt to protect those machines without installing the Rapid Recovery Agent on every machine. This option is called Rapid Snap for Virtual, or agentless protection. Optionally, if you plan to set up and manage multiple Cores from one interface, you can install the Rapid Recovery Central Management Console service.

> **i** **NOTE:** When using Hyper-V agentless protection, the Rapid Recovery Agent software is installed only on the Hyper-V Server or on each node of Hyper-V cluster.

The steps you must follow to install Rapid Recovery are:

- **Step 1:** Register at the Rapid Recovery License Portal at https://licenseportal.com, create an account, and obtain a software license. A license key or license file is necessary to download the Rapid Recovery Core and Rapid Recovery Agent software and to configure and protect machines. For more information about obtaining a license key or file, or registering and creating a Rapid Recovery License Portal account, see the *Rapid Recovery License Portal User Guide*.

- **Step 2:** Review and ensure that the system requirements have been met for the servers and machines on which you plan to install Rapid Recovery components. For more information, see Rapid Recovery system requirements.

- **Step 3:** Install the Rapid Recovery Core software on each Windows machine you plan to use as a Core. For more information, see Installing the Rapid Recovery Core. Before you use the Core to protect machines, you must also specify a storage location in which to configure a repository that stores your data. For detailed information, see the "Working with repositories" in the *Rapid Recovery User Guide*.

- **Step 4:** Install the Rapid Recovery Agent software on the Windows or Linux machines you plan to protect. For more information, see Installing the Rapid Recovery Agent software on Windows machines and About installing the Agent software on Linux machines. You can also protect virtual machines on a VMware vCenter/ESXi or Hyper-V host without installing the Agent software on every VM. Some important exclusions apply. For more information, see the topic Understanding Rapid Snap for Virtual in the *Rapid Recovery User Guide*.

- **Step 5:** If you need to manage multiple Rapid Recovery Cores in your environment, install and configure the Rapid Recovery Central Management Console. For more information about installing the Central Management Console, see Installing the Rapid Recovery Central Management Console. For more information about configuring the Central Management Console, see "Configuring the Rapid Recovery Central Management Console" in the *Rapid Recovery User Guide*.

  > **i** **NOTE:** After you have installed all necessary components, you must create a repository and define storage locations for your protected data. You can do this as a separate process, or as part the workflow when using the Protect Machine Wizard.

Optionally, you may want to perform other configuration tasks, such as setting encryption keys, configuring event notification, or replicating recovery points from a source Core to a target Core. Each of these configuration tasks is included in the Quick Start Guide feature of Rapid Recovery Core. You can read more information about the Quick Start Guide or performing these tasks independently in the *Rapid Recovery User Guide*. That document also contains information about tasks such as configuring an SMTP server for notification messages, changing the data retention policy, or configuring SQL attachability.

Understanding Rapid Recovery components

This section describes the Rapid Recovery components available for backup, replication, and recovery. The purpose of this section is to help you gain an understanding of the components that you may install in your Rapid Recovery environment and how they work together to help protect your data.

- **Rapid Recovery Core.** The central component of the Rapid Recovery architecture, the Core provides the essential services for backup, recovery, retention, replication, archiving, and management. The Core manages the repositories that store your backup data. It contains the settings that change behavior, manages schedules for backups, replication and archives, provides security, and enforces your data retention policy. After the Core is installed, you access it using the web-based interface called the Rapid Recovery Core Console. The Rapid Recovery Core must be installed on a dedicated Windows server. Depending on your license and your environment requirements, you may need to install multiple Cores.

- **Rapid Recovery Central Management Console.** This optional component is a web portal that simplifies the process of managing multiple Rapid Recovery Cores. Using the Central Management Console on a Windows server, you can group and manage multiple Cores in your environment through a single web-based interface. You can also generate reports for multiple Cores from one UI. If you install multiple Rapid Recovery Cores, you can install this separate service to manage them.

- **Rapid Recovery Agent.** This component is the primary provider of the services and software that let you protect your data. You install Rapid Recovery Agent software on the Windows and Linux machines in your environment (for example, on an Exchange server, SQL Server, Windows and Linux desktop and laptop machines, and so on). After you add a machine with the Agent software as a protected machine in the Rapid Recovery Core, the Agent software tracks changed data blocks on the disk volume of the machine and creates snapshot images of the data which it sends to the Core, based on the backup schedule. You manage protected machines using the Core Console of the associated Core, including establishing or changing the frequency of backups.

  > **i** | **NOTE:** If your Core and the machines you want to protect are all ESX or ESXi virtual machines on a VMware Workstation host, and if all of the VMs use a supported Windows operating system, then you do not need to install the Agent software. Likewise, if the machines that you want to protect are all Hyper-V virtual machines, you need only install the Agent software on the Hyper-V host server or cluster node host. This agentless protection feature for VMs is called Rapid Snap for Virtual.

- **Rapid Recovery Command Line Management utility.** The Rapid Recovery Command Line Management utility, cmdutil.exe, provides third-party access to manage system functionality. This tool permits scripting of the Rapid Recovery Core management functions. In previous versions of the product (AppAssure), this tool was called AACMD.

- **Rapid Recovery PowerShell Module.** The Rapid Recovery PowerShell Module is a Windows utility that lets users interact with the Core server by using Windows PowerShell scripts. This module offers some of the same functionality that the Rapid Recovery Core Console graphic user interface (GUI) provides. For example, the Rapid Recovery PowerShell Module can mount recovery points or force a snapshot of a protected machine.

About installing the Rapid Recovery Core

Because the Rapid Recovery Core manages the backups of all protected machines in your environment, you should install the Rapid Recovery Core on a dedicated server. Depending on your license and your environment requirements, you may need to install multiple Cores.

To use Rapid Recovery Core, you must register it with the Rapid Recovery License Portal. This requires you to create a license portal account, if you do not already have one. The email address you use to register your license portal account is used in the future for important communication. To register, or to access the license portal, visit https://licenseportal.com.

Many users start with a trial license. Once the trial period expires, the Rapid Recovery Core stops taking snapshots until you obtain and register an updated license. Once you have upgraded or purchased your Rapid Recovery license, you will receive by email either a license file or a license key.

For information about obtaining a license key, see the *Rapid Recovery License Portal User Guide*.

For information about managing licenses from the Core, see the topic Managing Licenses in the *Rapid Recovery User Guide*.

The license portal identifies a Rapid Recovery Core by its Core ID. For this reason, to avoid a conflict between managing Core IDs, Quest recommends not cloning machines with Rapid Recovery Core installed. In the event you have already done so, then remove the Rapid Recovery Core software on the cloned machine, and then reinstall it. This results in a new Core ID being assigned to the cloned machine.

When installing the Rapid Recovery Core, you can choose to automatically update the Rapid Recovery Core software. You can also choose to be notified about or to ignore updates. Once installation is complete, these settings can be changed at any time. For more information on changing automatic update settings, see the topic Configuring update settings in the *Rapid Recovery User Guide*.

i | **NOTE:** For optimal performance, it is recommended that you install the Rapid Recovery Core on more recent operating systems such as Windows 8.1 or Windows Server 2012 R2.

The Rapid Recovery Core requires a 64-bit Windows platform; 32-bit systems and Linux systems are not supported. For more information, see Rapid Recovery Core installation requirements. In addition, on Windows 8, Windows 8.1, Windows 10, Windows Server 2012, and Windows Server 2012 R2 operating systems, you must have the ASP.NET 4.5 feature installed on the server. If you do not have the feature installed, the GUI will not load correctly.

After you install the Rapid Recovery Core, you can download the Rapid Recovery Agent installer from the Core or the Rapid Recovery License Portal for each machine that you want to protect using the Rapid Recovery Agent software.

See also: Installing the Rapid Recovery Core
See also: Installing the Rapid Recovery Agent software on Windows machines
See also: About installing the Agent software on Linux machines

Installing the Rapid Recovery Core

Before you begin, see About installing the Rapid Recovery Core .

Complete the procedure below to install or upgrade the Rapid Recovery Core.

i | **NOTE:** Quest recommends retaining the binary installer file for any currently installed Rapid Recovery software product.

1. Download the Rapid Recovery Core installer file from the Rapid Recovery License Portal; for example:

```
Core-X64-6.x.x.xxxx.exe
```

2. Double-click on the executable Rapid Recovery Core installer file to start the installer.

   Depending on the configuration of your machine, the **User Account Control** window or the **Open File - Security Warning** window may appear.

3. If prompted for permission, confirm that you want to run the installer and make changes to the system.

   For more information, see Rapid Recovery Core installation requirements.

4. If .NET components are missing or need to be upgraded, accept the prompts to download and install the framework.

5. In the **Setup** dialog box, from the language field, select the appropriate language and then click **OK**.

6. Choose from one of the following:

   - **If this is the first time the Rapid Recovery Core software is being installed on this machine, the installer prepares the installation, and then the Rapid Recovery Core Installation Wizard appears. Proceed to Step 7.**

   - **If this machine has an earlier version of the AppAssure Core or Rapid Recovery Core software installed, you will see a message asking if you want to upgrade to the current version.**

     1. Click **Yes**.

        The Rapid Recovery Core Installation Wizard appears, and displays the **Update Options** page.

     2. Skip to Step 13.

7. In the Rapid Recovery Core Installation Wizard, on the **Welcome** page, click **Next** to continue with the installation.

   The **License Agreement** page appears.

8. On the **License Agreement** page, select **I accept the terms in the license agreement**, and then click **Next**.

   The **Prerequisites** page appears.

9. The Rapid Recovery Core installer verifies the existence of the prerequisite files.

   - **If the prerequisites do not exist, the installer identifies which files are needed and displays the results accordingly. Click Install Prerequisites.**

   - **If the prerequisite files exist, a message appears indicating that all prerequisites are installed on the machine.**

10. Once the installation of the prerequisite files is completed, click **Next**.

    The **Installation Options** page appears.

11. On the **Installation Options** page, review the installation options. If necessary, modify them as described below.

    - **In the Destination Folder text field, review the destination folder for the installation. If you want to change the location, do the following:**

      ▪ Click the folder icon.

      ▪ In the **Browse to Destination Folder** dialog box, select a new location.

      ▪ Click **OK**.

    - **In the Core port number text field, enter a port number to use for communication between the Rapid Recovery Core and its protected machines.**

i **NOTE:** The default value is 8006. If you change the port number, be sure to make note of it in the event that you need to adjust configuration settings at a later time.

• **In the VMware Proxy port number text field, enter a port number to use for communication between the Rapid Recovery Core and the VMware Virtual Disk Development Kit (VDDK) libraries used for creating and accessing VMware virtual disk storage.**

i **NOTE:** The default value is 8016. If you change the port number, be sure to make note of it in the event that you need to adjust configuration settings at a later time.

• **Optionally, in the Select optional components area, if you want to install Mailbox Restore, select Mailbox Restore for Exchange.**

Mailbox Restore for Microsoft Exchange is a comprehensive email recovery program that works with Rapid Recovery and the Rapid Recovery Local Mount Utility (LMU) to recover Exchange items from a full data store to a single email message. For more information about Mailbox Restore, see the *Mailbox Restore for Microsoft Exchange using Rapid Recovery User Guide*.

• **Select Allow Core to automatically send diagnostic and usage information to Quest Inc. to share this type of information (in aggregate) with Quest. If you do not want to send this information, clear this option.**

12. Once you are satisfied with the installation options, click **Next**.

The **Update Options** page appears.

13. On the **Update Options** page, choose from one of the options described in the following table.

Table 9. Update options for Rapid Recovery Core

This table lists options for updating the Core, and describes the results of selecting each option.

Option	Description
Automatically install updates (recommended)	If you select this option, the Rapid Recovery Core will automatically compare your version of the Core with the latest version available, once weekly. If a minor update is available (for example, upgrade to 6.0.2 from 6.0.1), the updated version is installed automatically after the nightly jobs have completed. If a major upgrade is available (for example, upgrade to 6.1 from 5.4.x, or 6.1 from 6.0.2), you will see an alert at the top of the Rapid Recovery Core Console when a newer version is available, including a link to download the update.
	When using replication, configuring your system to install updates automatically could result in upgrading the source core before the target core. Updating cores in this sequence may result in replication failure or the inability to set up new replication between cores.
	For replication users, Quest recommends administrators apply automatic upgrades only to the target core, and then manually upgrade the source core, and lastly upgrade the protected machines.
Notify me about updates, but do not install them automatically	If you select this option, you will see an alert at the top of the Rapid Recovery Core Console when a newer version is available, including a link to download the update.
Never check for updates	If you select this option, you will not be notified when a newer version is available.

If you choose to install automatic updates or to be notified about them, then the software version on the Rapid Recovery Core is checked against available software updates on a weekly basis. If a new version is detected, and if you selected the option to automatically update, then the updated version of the Core is installed after other scheduled nightly jobs have completed.

You can change how frequently the system checks for updates (options include daily, weekly, monthly, or never) at any time by configuring the update settings for the Core in the Rapid Recovery Core Console.

From the icon bar, click ⚙ (Settings), and then navigate to **Updates**. For more information on how to change these settings, see the topic Configuring update settings in the *Rapid Recovery User Guide*.

14. Once you are satisfied with the update options in the installer, click **Install**, or if upgrading, click **Next**.

    The **Progress** page appears and includes a status bar that lets you monitor the progress of the installation.

    When the installation is complete, the **Completed** page appears.

15. Click **Finish** to close the installer.

    ℹ **NOTE:** The first time you open the Rapid Recovery Core, you will need to enter your license information.

    ℹ **NOTE:** You can protect virtual machines on a VMware vCenter/ESXi host without installing the Agent software. However, some important exclusions apply. For more information, see the topic Understanding agentless protection in the *Rapid Recovery User Guide.*

    For information on configuring the Rapid Recovery Core and protecting and managing your data, see the *Rapid Recovery User Guide*.

Installing the Rapid Recovery Agent software

For agent-based protection, install the Rapid Recovery Agent software on machines that you want to protect with Rapid Recovery Core release 6.1, using the criteria specified below.

If upgrading a Linux machine from AppAssure Agent to Rapid Recovery Agent, perform these basic steps:

1. Optionally, back up the agent ID information associated with that protected machine.
   For more information, see Backing up and restoring the AppAssure agent ID.
2. Remove the AppAssure Agent version of the software from the machine using a shell script.
   For more information, see Uninstalling the AppAssure Agent software from a Linux machine.
3. Install Rapid Recovery Agent.
   For more information, see About installing the Agent software on Linux machines.
4. Configure the upgraded Rapid Recovery machine.
   For more information, see Configuring the Rapid Recovery Agent on a Linux machine.
5. Restore the agent ID.
   This process is also described in the topic Backing up and restoring the AppAssure agent ID.

   ℹ **NOTE:** After updating Rapid Recovery Agent, the first snapshot will result in a base image, creating a new recovery point chain.

For new installations, or if the drivers in the version of the Rapid Recovery Agent software you are upgrading to have changed, you are prompted to restart your system.

ℹ **NOTE:** You can also protect VMware vCenter/ESXi virtual machines on a host using agentless protection. This method uses the ESX agent client and APIs without installing Rapid Recovery Agent software on each VM. Likewise, you can protect Hyper-V virtual machines by installing the Agent on only the Hyper-V server or cluster node, rather than on every virtual machine. Agentless protection offers some advantages, but also some restrictions. For example, Quest does not advise agentless protection for Microsoft SQL or Microsoft Exchange servers because the metadata is not collected without the Rapid Recovery software. Before deciding to use agentless protection, see the topic "Understanding Rapid Snap for Virtual" in the *Rapid Recovery User Guide*.

Install the Rapid Recovery Agent software on machines that you want to protect using the following criteria:

- Install Rapid Recovery Agent software on every physical machine in your environment.

- Install Rapid Recovery Agent software on every VirtualBox virtual machine you want to protect.

- Install Rapid Recovery Agent software on every Hyper-V virtual machine you want to protect with the Agent, instead of agentlessly.

- Install Rapid Recovery Agent software on every VMware vCenter/ESXi virtual machine you want to protect with the Agent, instead of agentlessly.

Review the methods to obtain the Rapid Recovery Agent software and determine which method you will use. Then obtain the software, and install on the machines you want to protect on the Rapid Recovery Core. Finally, add the machines to protection on your Core.

> **i** | **NOTE:** Quest recommends retaining the binary installer file for any currently installed Rapid Recovery software product.

Related tasks
See also: Installing the Rapid Recovery Agent software on Windows machines
See also: Installing the Agent software on Windows Server Core Edition machines
Related references
See also: Obtaining the Rapid Recovery Agent software
See also: Installing the Agent software on Linux machines

Obtaining the Rapid Recovery Agent software

You can obtain the Agent software using one of the following methods:

- **Download from the Rapid Recovery Core Console.** If the Rapid Recovery Core is installed, you can log into the Rapid Recovery Core Console and download the software to the machine you want to protect. From the icon bar, click **More** and then select **Downloads.** From the Downloads page, you can download the web installer for the Agent component.

- **Download from the License Portal.** If you have already registered your software in the Rapid Recovery License Portal, you can log into the portal at https://licenseportal.com and download the software to the machine you want to protect.

  For more information about the Rapid Recovery License Portal, including obtaining a license key or registering and creating a License Portal account, see the *Rapid Recovery License Portal User Guide*.

- **Deploy the Agent software when protecting a machine.** If the Rapid Recovery Core is installed, you can deploy the Agent software to the machine you want to protect from the Protect Machine Wizard. For more information about using this wizard, see the topic Protecting a Machine in the *Rapid Recovery User Guide*.

- **Deploy the Agent software when protecting to multiple machines.** If the Rapid Recovery Core is installed, you can deploy the Agent software to multiple machines using the Protect Multiple Machines Wizard. For more information about using this wizard, see the topic About protecting multiple machines in the *Rapid Recovery User Guide*.

- **Use the Deploy Agent Software feature.** If the Rapid Recovery Core is installed, you can deploy the Agent software to one or multiple machines using the Deploy Agent Software option, accessed from the Protect drop-down menu on the Rapid Recovery Core Console. For more information about using this feature, see the topic Deploying Agent to multiple machines simultaneously from the Core Console in the *Rapid Recovery User Guide*.

Installing the Rapid Recovery Agent software on Windows machines

Deploy the Rapid Recovery Agent installer file to the machine you want to protect using one of the methods described in Installing the Rapid Recovery Agent software. Then launch the installer program as described below to install or upgrade the software on each Windows machine you want to protect in the Rapid Recovery Core.

> **ⓘ** | **NOTE:** You must run the installer with local administrator privileges.

The procedure for installing on Windows Server Core editions differs than other versions of Windows, since that version describes how to install from the command line. For more information, see Installing the Agent software on Windows Server Core Edition machines.

1. From the machine you want to protect, double-click on the executable Rapid Recovery Agent installer file to start the installer.

    Depending on the configuration of your machine, the **User Account Control** window or the **Open File - Security Warning** window may appear.

2. If prompted for permission, confirm that you want to run the installer and make changes to the system.

3. If .NET components are missing or need to be upgraded, accept the prompts to download and install the framework.

4. In the **Setup** dialog box, from the language field, select the appropriate language and then click **OK**.

5. Choose from one of the following:

    - **If this is the first time the Rapid Recovery Agent software is being installed on this machine, the installer prepares the installation, and then the Rapid Recovery Agent Installation Wizard appears. Proceed to Step 6.**

    - **If this machine has an earlier version of the AppAssure Agent or Rapid Recovery Agent software installed, you will see a message asking if you want to upgrade to the current version.**

        1. Click **Yes**.

            The Rapid Recovery Agent Installation Wizard appears, showing the **Progress** page of the wizard. The application downloads to the destination folder, with progress displayed in the progress bar. When finished, the wizard automatically advances to the **Completed** page.

        2. Skip to Step 12.

6. In the Rapid Recovery Agent Installation Wizard, on the **Welcome** page, click **Next** to continue with the installation.

    The **License Agreement** page appears.

7. On the **License Agreement** page, select **I accept the terms in the license agreement**, and then click **Next**.

    The **Prerequisites** page appears.

8. The Rapid Recovery Agent Installer verifies the existence of the prerequisite files.

    - **If the prerequisite files exist, a message appears indicating that all prerequisites are installed on the machine.**

    - **If the prerequisite files do not exist, the Rapid Recovery Agent Installer identifies which files are needed and displays the results accordingly. Click Install Prerequisites.**

9. When the installation of the prerequisite files is completed, click **Next**.

The **Installation Options** page appears.

10. On the **Installation Options** page, review the installation options. If necessary, modify them as described below.

- **In the Destination Folder text field, review the destination folder for the installation. If you want to change the location, do the following:**

  ▪ Click the folder icon.

  ▪ In the **Browse to Destination Folder** dialog box, select a new location.

  ▪ Click **OK**.

- **In the Port Number text field, enter a port number to use for communication between the Agent software on the protected machine and the Rapid Recovery Core.**

  ℹ **NOTE:** The default value is 8006. If you change the port number, be sure to make note of it in the event that you need to adjust configuration settings at a later time.

- **Select Allow Agent to automatically send diagnostic and usage information to Quest Inc. to share this type of information (in aggregate) with Quest. If you do not want to send this information, clear this option.**

11. Once you are satisfied with the installation options, click **Install**.

   The **Progress** page appears, and includes a status bar that lets you monitor the progress of the installation.

   When the installation is complete, the **Completed** page appears. Skip to Step 12.

12. On the **Completed** page, if you see a message indicating that the system must be restarted before the installation takes effect, perform one of the following steps:

- **To restart now, select Yes, I want to restart my computer now.**

- **To restart later, clear the Yes, I want to restart my computer now option.**

13. On the **Completed** page, click **Finish.**

   The installer wizard closes, and the Agent installation is complete. If you designated this option, the machine may restart if necessary.

Related concepts
    See also: Rapid Recovery system requirements
Related tasks
    See also: Installing the Agent software on Windows Server Core Edition machines
Related references
    See also: Installing the Rapid Recovery Agent software

Installing the Agent software on Windows Server Core Edition machines

Complete the steps in the following procedure to install the Agent software on a Windows Server Core machine.

ℹ **NOTE:** The following procedure installs the Agent software in console mode. To install in silent mode instead, append `/silent` to the installer file name on the command line. For example, `Agent-X64-6.X.X.xxxxx.exe /silent`.

1. Download the Rapid Recovery Agent installer file from the Rapid Recovery License Portal or from the Rapid Recovery Core.

2. From a command prompt, navigate to the directory containing the Rapid Recovery Agent installer file and enter the installer file name to begin the installation:

       Agent-X64-6.x.x.xxxxx.exe

The installation program installs the Agent software and displays progress in the console. Upon completion, new installations trigger an automatic restart of the machine, whereas Agent upgrades may not require a machine restart.

About installing the Agent software on Linux machines

When installing the Rapid Recovery Agent software on Linux machines that you want to protect, use the following prerequisites and guidance.

Prerequisites for installation on Linux machines

Prerequisites:

- If AppAssure Agent was previously installed, then before installing Rapid Recovery Agent, remove the AppAssure Agent from the machine using a shell script. For more information, see Uninstalling the AppAssure Agent software from a Linux machine.

- The operating system on the Linux machine must be a supported distribution, as listed in Rapid Recovery Agent software requirements.

Deploying and installing the Agent software on Linux machines from the Core Console

The following items are prerequisites for deploying Agent to Linux machines when you select Deploy Agent Software from the Protect drop-down menu

- SSH Server must be running on the Linux machine you want to protect. You can confirm on the Linux machine from the root account by entering the command: `netstat -antp |grep ssh`.

- The firewall on the Linux machine you want to protect must be disabled, or not blocking port 22.

- The current Linux user must be a non-root user account with sudo privileges. To confirm, make sure that your user account is a member of the sudo, wheel, or root group by entering the command: `groups <username>`.

- The wget utility must be installed on the Linux machine you want to protect. To confirm, run the command: `which wget`.

Guidelines for installation on Linux machines

The method for installing and removing the Agent software on Linux machines has changed. As of release 6.0.1, the following factors apply:

- Earlier versions of Rapid Recovery used shell scripts to install or remove the Agent software from Linux machines.

- As of release 6.x, a single Linux archive package is used to set up a Rapid Recovery software repository on the local Linux machine.

- Rapid Recovery now uses a package manager (such as yum, zypper or apt) to install or remove Rapid Recovery Agent on Linux machines from this repository.

  > **i** | **NOTE:** The software repository is used for staging files for the relevant package managers. This repository is not related to the Rapid Recovery repository.

- Installations of Agent on a Linux machine with access to the internet are called **online installations**.

- Installations of Agent on a Linux machine with no access to the Internet (such as air-gapped or secured standalone machines) are called **offline installations**. For offline installations, you must first download an installation package from a Linux machine with Internet access. Then, move those installation files to the secured computer for installation.

The various supported Linux distributions use different package managers for online installation. Thus, the procedure for installing, upgrading, or removing Agent on any supported Linux OS depends on the package manager used. The package managers, and the Linux distributions they support, are described in the following table.

Table 10. Package managers and the Linux distributions they support

This table lists the package managers used for installing Rapid Recovery on a Linux machine. The first column lists the package manager name. The second column lists the relevant Linux distributions each package manager supports.

Package Manager	Linux Distribution
yum	Linux distributions based on Red Hat Enterprise Linux (RHEL), including RHEL, CentOS, and Oracle Linux.
zypper	SUSE Linux Enterprise Server (SLES) versions 11, 12
apt	Linux distributions based on Debian, including Debian 7 or 8, and Ubuntu 12.04 and later

As a one-time setup step for each Linux machine, you must configure your local software repository to point to the location where the package manager obtains Rapid Recovery installation files.

> **i** **NOTE:** This process is represented by steps 1 through 4 in each of the installation procedures. When upgrading future editions of the Rapid Recovery Agent on a Linux machine with the software repository configured, you do not need to perform these steps.

After you configure a software repository on your Linux machine, the package manager is able to retrieve and install the packages needed for installation or removal of Rapid Recovery Agent software and related components, such as local_mount, rapidrecovery-vdisk, and Mono.

For each package manager, you can run the appropriate command at the command line to determine if it is configured to download Rapid Recovery packages. These commands are listed in the following table.

Table 11. Command to show package manager repository configuration

This table lists the commands each package manager runs to determine if it is configured to download Rapid Recovery on a Linux machine. The first column lists the package manager name. The second column lists the relevant command to enter at the command line.

Package Manager	Command to list configured repositories
yum	yum replolist
zypper	zypper repos
apt	ls /etc/apt/sources.list.d

Previous versions of the AppAssure Agent software must be removed from a Linux machine before installing the Rapid Recovery Agent version and protecting the Linux machine using the Rapid Recovery Core. This requirement applies to both online and offline installations. Removing AppAssure Agent employs the use of shell scripts. The uninstall instructions differ, depending on the Linux distribution you are using. For more information on uninstalling AppAssure Agent from a Linux machine, see Uninstalling the AppAssure Agent software from a Linux machine.

> **i** **NOTE:** Removal of the new Rapid Recovery Agent software uses the package manager for each distribution. Therefore, if uninstalling a version of Rapid Recovery Agent, see the appropriate procedure under the topic Uninstalling the Rapid Recovery Agent software from a Linux machine.

If installing Rapid Recovery Agent on a Linux machine that has never had AppAssure Agent installed, determine the appropriate package manager from the preceding table. Then follow the appropriate installation procedure.

After configuring the newly installed Agent software on a Linux machine, you must restart the machine. Restarting ensures that the proper kernel driver version is used to protect your machine.

Thus, the installation process when upgrading from AppAssure to Rapid Recovery involves:

- Removing the AppAssure Agent software (not required for first-time installations)

- Follow the procedure for installing Rapid Recovery Agent on the Linux machine. Each procedure includes (as steps 1 through 4) the process for configuring the software repository locally.

- Run the configuration utility to set ports, configure users, add firewall exclusions, install the kernel module, and start the Agent service.

- Restart the Linux machine

The instructions for installing the Agent software on a Linux machine differ slightly depending on the Linux distribution you are using. For more information about preparing for and installing the Agent software for a Linux machine connected to the Internet, see the appropriate topic. You can choose from the following sections:

- Installing the Rapid Recovery Agent software on Debian or Ubuntu

- Installing the Rapid Recovery Agent software on Red Hat Enterprise Linux, CentOS, or Oracle Linux

- Installing the Rapid Recovery Agent software on SUSE Linux Enterprise Server

For more information about preparing for and installing the Agent software for a Linux machine that is not connected to the Internet, see the topic:

- Installing the Agent software on offline Linux machines

See the following important information before you begin installation of Agent software.

- Downloading the Linux distribution

- About security

- Location of Linux Agent files

- Agent dependencies

- Linux scripting information

After installation on Linux machines

After installing Rapid Recovery Agent, configure the Agent software as described in the topic Configuring the Rapid Recovery Agent on a Linux machine.

> ⚠ **CAUTION: After configuring the newly installed Agent software on a Linux machine, restart the machine. Restarting ensures that the proper kernel driver version is used to protect your machine.**

Downloading the Linux distribution

You must download the distribution-specific 32-bit or 64-bit installer on every Linux machine that you want to protect. You can download the installers from the Rapid Recovery License Portal at https://licenseportal.com. For more information, see the *Rapid Recovery License Portal User Guide*.

About security

Linux uses the Pluggable Authentication Module (PAM) to manage security. Once a user is authenticated through libpam, the user is only authorized to protect the machine if the user is in one of the following groups: sudo, admin, recovery, or wheel. For information on protecting a machine, see the section "Protecting a Machine" in the *Rapid Recovery User Guide*.

Location of Linux Agent files

There are several files required to support the Rapid Recovery Agent software on a Linux machine. For all supported Linux distributions, these files are located in the following directories:

- mono:

  ```
  /opt/apprecovery/mono
  ```

- agent:

  ```
  /opt/apprecovery/agent
  ```

- local mount:

  ```
  /opt/apprecovery/local_mount
  ```

- rapidrecovery-vdisk and aavdctl:

  ```
  /usr/bin/aavdisk
  ```

- configuration files for rapidrecovery-vdisk:

  ```
  /etc/apprecovery/aavdisk.conf
  ```

- wrappers for agent and local_mount

  ```
  /usr/bin/agent
  /usr/bin/local_mount
  ```

- autorun scripts for agent and rapidrecovery-vdisk:

  ```
  /etc/init.d/rapidrecovery-agent
  /etc/init.d/rapidrecovery-vdisk
  ```

Agent dependencies

The following dependencies are required and are installed as part of the Agent installer package:

- For Debian 7 and Ubuntu 12.xx and 14.xx:
  - The rapidrecovery-agent requires:

    ```
    lsscsi, libblkid1, e2fslibs, libpam0g, libc6, libpcre3, perl, make, e2fsprogs, xfsprogs,
    ```
  - The apprecovery-dkms requires:

    ```
    module-init-tools, gcc, build-essential, coreutils (>= 7.4), patch
    ```
- For Debian 8 and Ubuntu 15.xx and 16.xx
  - The rapidrecovery-agent requires:

    ```
    lsscsi, libblkid1, e2fslibs, libpam0g, libc6, libpcre3, perl, make, e2fsprogs, xfsprogs,
    ```
  - The apprecovery-dkms requires:

    ```
    module-init-tools, gcc, build-essential, coreutils (>= 7.4), patch
    ```
- For Red Hat Enterprise Linux 6, CentOS 6, and Oracle Linux 6:
  - The rapidrecovery-agent requires:

    ```
    lsscsi, make, gcc, pam, pcre, glibc, python, perl, e2fsprogs, apprecovery-dkms, rapidreco
    ```
  - The nbd requires:

    ```
    apprecovery-dkms
    ```
  - The apprecovery-dkms requires:

```
coreutils, cpio, findutils, gawk, gcc, grep, gzip, sed, tar, bash > 1.99, module-init-too
```

- For Red Hat Enterprise Linux 7, CentOS 7, and Oracle Linux 7:
    - ◦ The rapidrecovery-agent requires:
      ```
      lsscsi, make, gcc, pam, pcre, glibc, python, perl, e2fsprogs, apprecovery-dkms, rapidreco
      ```
    - ◦ The nbd requires:
      ```
      apprecovery-dkms
      ```
    - ◦ The apprecovery-dkms requires:
      ```
      bash > 1.99, coreutils, cpio, findutils, gawk, gcc, grep, gzip, kmod, sed, systemd, tar,
      ```
- For SUSE Linux Enterprise Server 11:
    - ◦ The rapidrecovery-agent requires:
      ```
      lsscsi, make, libblkid1, libext2fs2, pam, pcre, glibc, xfsprogs, python, perl, apprecover
      ```
    - ◦ The apprecovery-dkms requires:
      ```
      coreutils, cpio, findutils, gawk, gcc, grep, gzip, sed, tar, bash > 1.99, module-init-too
      ```
- For SUSE Linux Enterprise Server 11:
    - ◦ The rapidrecovery-agent requires:
      ```
      lsscsi, make, libblkid1, libext2fs2, pam, pcre, glibc, xfsprogs, python, perl, apprecover
      ```
    - ◦ The apprecovery-dkms requires:
      ```
      bash > 1.99, coreutils, cpio, findutils, gawk, gcc, grep, gzip, kmod, sed, systemd, tar,
      ```

Linux scripting information

Information about Bourne Shell scripting supporting Linux protected machines is included in the *Rapid Recovery User Guide*. See the appendix "Scripting," including the topic "Using Bourne Shell and Bash scripting with Rapid Recovery."

Installing the Rapid Recovery Agent software on Debian or Ubuntu

The Rapid Recovery Agent .deb file is an archive containing repository information specific to the apt package manager. Complete the following steps to install the Rapid Recovery Agent on Debian or Ubuntu machines for an online installation.

> **i**   **NOTE:** This procedure applies to a Linux machine that is connected to the internet. For offline installation of Rapid Recovery Agent on any Linux machine, see Installing the Agent software on offline Linux machines.

1. Open a terminal session with root access.
2. Determine your present working directory by entering `pwd` and pressing **Enter**. For example, assume your directory is `/home/rapidrecovery/`.
3. Download the appropriate Rapid Recovery Agent .deb installation file from the License Portal at https://licenseportal.com to your present working directory.

   For more information about the license portal, see the *Rapid Recovery License Portal User Guide*.

4. To establish a persistent connection between your Linux machine and the remote Quest software repository in which Rapid Recovery software and components are stored, type the following command:
   ```
   dpkg -i <.deb installation file you downloaded>
   ```

For example, if the installer file is named rapidrecovery-repo-6.1.0.999.deb in the directory `/home/rapidrecovery/`, type the following command, and then press **Enter**:

```
dpkg -i rapidrecovery-repo-6.1.0.999.deb
```

Any missing packages or files required by the Agent will be downloaded from the remote software repository and installed automatically as part of the script.

> **ⓘ** **NOTE:** For more information on dependencies for installing on a Linux machine, see Agent dependencies.

5. Install the Rapid Recovery Agent by invoking the apt package manager, updating the repository manager. Type the following command, and then press **Enter**:

```
apt-get update
```

6. Instruct the package manager to install the Rapid Recovery Agent software. Type the following command, and then press **Enter**:

```
apt-get install rapidrecovery-agent
```

7. The package manager prepares to install all dependent files. If prompted to confirm installation of unsigned files, enter **y** and then press **Enter**.

The Rapid Recovery Agent files are installed.

Installing the Rapid Recovery Agent software on Red Hat Enterprise Linux, CentOS, or Oracle Linux

The Rapid Recovery Agent .rpm file is an archive containing repository information specific to Red Hat Enterprise Linux (RHEL), CentOS, or Oracle Linux. These distributions use the yum package manager. Complete the following steps to install the Rapid Recovery Agent on RHEL, CentOS, or Oracle Linux.

> **ⓘ** **NOTE:** This procedure applies to a Linux machine that is connected to the internet. For offline installation of Rapid Recovery Agent on any Linux machine, see About installing the Agent software on Linux machines.

1. Open a terminal session with root access.
2. Determine your present working directory by entering `pwd` and pressing **Enter**. For example, assume your directory is `/home/rapidrecovery/`.
3. Download the appropriate Rapid Recovery Agent .rpm installation file from the License Portal at https://licenseportal.com to your present working directory.

   For more information about the license portal, see the *Rapid Recovery License Portal User Guide*.

4. To establish a persistent connection between your Linux machine and the remote Quest software repository in which Rapid Recovery software and components are stored, type the following command:

```
rpm -ivh <.rpm installation file you downloaded>
```

For example, if the installer file is named rapidrecovery-repo-6.1.0.999.rpm in the directory `/home/rapidrecovery/`, type the following command, and then press **Enter**:

```
rpm -ivh rapidrecovery-repo-6.1.0.999.rpm
```

Any missing packages or files required by the Agent will be downloaded from the remote software repository and installed automatically as part of the script.

> **ⓘ** **NOTE:** For more information on dependencies for installing on a Linux machine, see Agent dependencies.

5. Install the Rapid Recovery Agent by invoking the yum package manager, updating the repository manager. Type the following command, and then press **Enter**:

```
yum clean all
```

6. Instruct the package manager to install the Rapid Recovery Agent software. Type the following command, and then press **Enter**:

Installation and Upgrade Guide
Installing the Rapid Recovery Agent software on Red Hat Enterprise Linux, CentOS, or Oracle Linux

36

```
yum install rapidrecovery-agent
```

7.   The package manager prepares to install all dependent files. If prompted to confirm installation of unsigned files, enter **y** and then press **Enter**.

The Rapid Recovery Agent files are installed.

Installing the Rapid Recovery Agent software on SUSE Linux Enterprise Server

The Rapid Recovery Agent .rpm file is an archive containing repository information for SUSE Linux Enterprise Server (SLES) . This distribution uses the zypper package manager. Complete the following steps to install the Rapid Recovery Agent on SLES.

> **i** **NOTE:** This procedure applies to a Linux machine that is connected to the internet. For offline installation of Rapid Recovery Agent on any Linux machine, see Installing the Agent software on offline Linux machines.

1.   Open a terminal session with root access.

2.   Determine your present working directory by entering `pwd` and pressing **Enter**. For example, assume your directory is `/home/rapidrecovery/`.

3.   Download the appropriate Rapid Recovery Agent .rpm installation file from the License Portal at https://licenseportal.com to your present working directory.

For more information about the license portal, see the *Rapid Recovery License Portal User Guide*.

4.   To establish a persistent connection between your Linux machine and the remote Quest software repository in which Rapid Recovery software and components are stored, type the following command:

```
rpm -ivh <.rpm installation file you downloaded>
```

For example, if the installer file is named rapidrecovery-repo-6.1.0.999.rpm in the directory `/home/rapidrecovery/`, type the following command, and then press **Enter**:

```
rpm -ivh rapidrecovery-repo-6.1.0.999.rpm
```

Any missing packages or files required by the Agent will be downloaded from the remote software repository and installed automatically as part of the script.

> **i** **NOTE:** For more information on dependencies for installing on a Linux machine, see Agent dependencies.

5.   Install the Rapid Recovery Agent by invoking the zypper package manager, updating the repository manager. Type the following command, and then press **Enter**:

```
zypper refresh 'rapidrecovery repository'
```

6.   Instruct the package manager to install the Rapid Recovery Agent software. Type the following command, and then press **Enter**:

```
zypper install rapidrecovery-agent
```

7.   The package manager prepares to install all dependent files. If prompted to confirm installation of unsigned files, enter **y** and then press **Enter**.

The Rapid Recovery Agent files are installed.

Installing the Agent software on offline Linux machines

This task requires access to an online Linux machine, removable storage media, and access to the final offline Linux machine. If AppAssure Agent is installed on the offline Linux machine, you must first uninstall it before installing Rapid Recovery Agent. For more information, see Uninstalling the AppAssure Agent software from a Linux machine.

When installing the Agent software on Linux machines that do not have access to the Internet, follow this procedure. After installation is complete, configure the Agent as described in the topic Configuring the Rapid Recovery Agent on a Linux machine.

> **ℹ NOTE:** If installing on multiple Linux distributions, perform this procedure once for each distribution.

1. From a Linux machine with access to the Internet, download the shell script for off-line Agent installation from the license portal:
   a. Browse to https://licenseportal.com.
   b. Log into the license portal and click **Downloads**.
   c. Under Linux-Based Applications, scroll down to the **Downloader script for off-line Agent installation**, and click **Download**.

   The shell script downloads to your current directory.

   d. Using removable storage media compatible with both machines, transfer the shell script file to the home directory of the appropriate offline Linux machine.

2. Run the shell script by executing the following command:

   ```
   bash packages-downloader.sh
   ```

   The script executes and prompts you to select a specific Linux distribution and architecture.

3. Type the index of the installation package you want and press **Enter**.

   For example, to obtain an installation package for Red Hat Enterprise Linux 7, enter 3 and press Enter.

   The appropriate installer is extracted into the `~/rapidrecovery.packages/` directory.

   > **ℹ NOTE:** The tilde ~/ characters represent your home directory.

4. Copy the packages for Rapid Recovery Agent to removable media. The specific location of your removable media can differ based on Linux distribution. Type the following command and then press **Enter**:

   ```
   cp -R ~/rapidrecovery.packages/ <your_removable_media>
   ```

   For example, if using a removable USB drive that is mounted to location /media/USB-drive-1, type the following command and then press Enter:

   ```
   cp -R ~/rapidrecovery.packages /media/USB-drive-1
   ```

   All the necessary files are copied to the removable medium.

5. Take the removable medium to the offline Linux machine and mount the drive.

6. Copy the data from the mounted device to your home directory or other desired location. For example, type the following command and then press **Enter**:

   ```
   cp -R /media/USB-drive-1 ~/rapidrecovery.packages
   ```

7. Change to the Rapid Recovery directory. For example, type the following command and then press **Enter**:

   ```
   cd ~/rapidrecovery.packages
   ```

8. Run the installation of Agent with root privileges. This command differs based on Linux distribution.

   - **For Red Hat, SLES, Oracle, and CentOS, type the following command and then press Enter:**

     ```
     sudo rpm -i *.rpm
     ```

   - **For Debian and Ubuntu, type the following command and then press Enter:**

     ```
     sudo dpkg -i *.deb
     ```

   The local package manager runs the installation of Rapid Recovery Agent.

After installation is complete, configure the Agent as described in the topic Configuring the Rapid Recovery Agent on a Linux machine.

> ⚠ **CAUTION:** After configuring the newly installed Agent software on a Linux machine, you must restart the machine. Restarting ensures that the proper kernel driver version is used to protect your machine.

Configuring the Rapid Recovery Agent on a Linux machine

Run the Rapid Recovery Configuration utility after installing Rapid Recovery Agent software on a Linux machine. This compiles and installs the kernel module on the Linux machine you want to protect in your Core.

The configuration utility offers several configuration options, and provides hints in the numbered steps of the instructions when it detects your specific configuration information.

Complete the steps below to configure the Rapid Recovery Agent software on any Linux machine. Some configuration options differ based on the Linux distribution you are installing.

1. Open a terminal session with root access.
2. Launch the configuration utility by typing the following command, and then press Enter:

   ```
   sudo /usr/bin/rapidrecovery-config
   ```

   The configuration utility starts. This lists several configuration options, each with an index number to enter for the appropriate configuration step.

3. Configure the port for this protected machine by typing the following command, and then press Enter. The default port is 8006.

   ```
   1 <agent_port>
   ```

   For example, if using the default port, type the command:

   ```
   1 8006
   ```

4. Configure users available for protection, by typing the following command, and then press Enter:

   ```
   1 <user_names_separated_by_comma>
   ```

   For example, if using usernames michael, administrator, and test_user1, type the command:

   ```
   2 michael,administrator,test_user1
   ```

5. Configure firewall rules to select a firewall configuration manager. This establishes firewall exceptions for the port designated in step 1.

   If the utility detects one or more firewall configuration managers (such as lokkit or firewalld), each is listed in the utility in line 3. Select the appropriate configuration manager and enter it, starting with the command number (3), and then press Enter:

   ```
   3 <firewall_configuration>
   ```

   For example, if using firewalld, type the command:

   ```
   3 firewalld
   ```

6. Query the list of compatible kernel modules from the utility by entering the command number, and then press Enter:

   ```
   4
   ```

   A sub-shell returns all kernel modules compatible for installation. For example, the following could be returned:

   ```
   Searching for all available for installation kernels.
   This might take a while, depending on the Internet connection speed.
   Kernels compatible for module installation:
    0 - linux-image-3.16.0.23-generic
    1 - linux-image-3.16.0.31-generic
    2 - linux-image-3.16.0.33-generic
   ```

```
    3 - linux-image-3.16.0.34-generic
  Input indices of the kernel modules you wish to install, delimited by space; use 'all' to ins
```

7. Configure the appropriate Rapid Recovery kernel module.

   For example, to enter kernel modules for 3.16.0-23 and 3.16.0-34, enter `1 4` and press Enter.

   To enter all kernel modules, enter `all` and press Enter.

8. After configuring the newly installed Agent software, restart the machine. Restarting ensures that the proper kernel driver version is used to protect your machine.

After completing this process, the local repository has been configured on this Linux machine. The Agent software is installed and the kernel module is loaded.

Your next step is to protect the machine on the Rapid Recovery Core.

Starting and stopping the Linux Agent Daemon

After installing or upgrading the Agent software on a Linux machine, you should configure the Agent, and then restart. Restarting ensures that the Rapid Recovery Agent services start automatically, which is required to protect your Linux machine.

If for any reason you need to manually start or stop the Agent services, use the following procedure.

You can manually start, stop, and view the status of the Rapid Recovery Agent software and rapidrecovery-vdisk in all supported distributions by using the default commands as described in the following tables, respectively.

Table 12. Starting the Linux Agent Daemon

This table lists the command to start the agent service or rapidrecovery-vdisk manually from the command line.

To start the...	Use the following command...
agent service	sudo service rapidrecovery-agent start
rapidrecovery-vdisk	sudo service rapidrecovery-vdisk start

Table 13. Stopping the Linux Agent Daemon

This table lists the command to stop the agent service or rapidrecovery-vdisk manually from the command line.

To stop the...	Use the following command...
agent service	sudo service rapidrecovery-agent stop
rapidrecovery-vdisk	sudo service rapidrecovery-vdisk stop

Table 14. Viewing status for the Linux Agent Daemon

This table lists the command to view the status of the agent service or rapidrecovery-vdisk manually from the command line.

To view the status of...	Use the following command...
agent service	sudo service rapidrecovery-agent status
rapidrecovery-vdisk	sudo service rapidrecovery-vdisk status

Installing the Rapid Recovery Central Management Console

The Rapid Recovery Central Management Console is an optional component intended for environments with two or more Rapid Recovery Cores. This component is a web portal providing a central interface where you can group, manage, and generate reports for multiple Cores.

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.

After installation, you must configure the Central Management Console by adding Cores you want to manage, either individually, or as part of Core groups.

> **i** | **NOTE:** You must run the installer with local administrator privileges.

The Windows 8, 8.1, and 10, and Windows Server 2012 and 2012 R2 operating systems must have the ASP.NET 4.5 role installed on the server for proper loading of the GUI. This configuration is included for you as part of the Rapid Recovery installer.

For more information about configuring this component, see the topic "Configuring the Central Management Console" in the *Rapid Recovery User Guide*.

For more information about understanding the UI of this component, see the topic "Understanding the Rapid Recovery Central Management Console" in the *Rapid Recovery User Guide*.

Complete the steps in the following procedure to install the Central Management Console.

> **i** | **NOTE:** Quest recommends retaining the binary installer file for any currently installed Rapid Recovery software product.

1. Download the Rapid Recovery Central Management Console installer file from the Rapid Recovery License Portal; for example:

   ```
   CentralConsole-X64-6.X.X.xxxx.exe
   ```

   > **i** | **NOTE:** The Rapid Recovery Central Management Console requires a 64-bit Windows platform.

2. Double-click on the executable Rapid Recovery Central Management Console installer file to start the installer.

   Depending on the configuration of your machine, the User Account Control window or the Open File — Security Warning window could appear.

3. If prompted for permission, confirm that you want to run the installer and make changes to the system.

   The Setup dialog box appears. The installer checks that the Microsoft .NET Framework 4.5.2 is installed on your system.

4. If .NET components are missing or must be upgraded, accept the prompts to download and install the framework.

5. In the language field, select the appropriate language and then click **OK**.

   The installer prepares the installation, and then the Rapid Recovery Central Management Console Installation Wizard appears.

6. In the Rapid Recovery Central Management Console Installation Wizard, on the Welcome page, click **Next** to continue with the installation.

The License Agreement page appears.

7. On the License Agreement page, click **I accept the terms in the license agreement**, and then click **Next**.

The Prerequisites page appears.

8. The Rapid Recovery Central Management Console installer verifies the existence of the prerequisite files.

- **If the prerequisites do not exist, the installer identifies which files are needed and displays the results accordingly. Click Install Prerequisites.**

- **If the prerequisite files exist, a message appears indicating that all prerequisites are installed on the machine.**

9. Once the installation of the prerequisite files is completed, click **Next**.

The Installation Options page appears.

10. On the Installation Options page, review the installation options. If necessary, modify them as described below.

- **In the Destination Folder text field, review the destination folder for the installation. If you want to change the location, do the following:**

  ▪ Click the folder icon.

  ▪ In the Browse to Destination Folder dialog box, select a new location.

  ▪ Click **OK**.

- **In the Port Number text field, enter a port number to use for communication between the** Rapid Recovery **Central Management Console and each Core.**

  ℹ | **NOTE:** The default value is 8006. If you change the port number, be sure to make note of it in case you must adjust configuration settings later.

11. Once you are satisfied with the installation options, click **Install**.

The Progress page appears and includes a status bar that lets you monitor the progress of the installation.

When the installation is complete, the Completed page appears.

12. Click **Finish**.

The installer closes. You must configure the Rapid Recovery Central Management Console before use.

Automatically installing updates

When installing the Rapid Recovery Core, you can choose to automatically update the Rapid Recovery Core software. For specific steps on selecting these options, see Installing the Rapid Recovery Core.

You can also choose to be notified when an updated version of the Core software is available, or to ignore updates. Once installation is complete, these settings can be changed at any time. For more information on changing automatic update settings, see "Configuring Update Settings" in the *Rapid Recovery User Guide.*

If you choose automatic updates, or if you choose to be notified about updates, then the software on the Rapid Recovery Core is checked against new versions available from the Rapid Recovery License Portal periodically.

- If you choose automatic updates, then when a new version is detected, the version on the Core is updated after other scheduled nightly jobs have completed.

- If you choose to be notified about updates, then when a new version is detected, a message appears on the Core Console under the button bar indicating that a new version is available. The message includes a link to obtain the update.

Quest recommends using the automatic update option.

The default setting for automatic updates is to check for updates weekly. You can change how frequently the system checks for updates (options include daily, weekly, monthly, or never) at any time by configuring the update settings for the Core on the Settings page of the Rapid Recovery Core Console. For more information on how to change these settings, see the topic "Configuring Update Settings" in the *Rapid Recovery User Guide.*

If using replication, the recommended order of upgrading components is to always upgrade the target Core first, then upgrade the source Core, and lastly update the Agent software on protected machines.

Uninstalling the Rapid Recovery Core

Complete the steps in this procedure to uninstall the Rapid Recovery Core. The same steps apply to uninstall an AppAssure Core. Only the version number will be different.

1. On the Windows server from which you want to uninstall the Rapid Recovery Core, open the Control Panel, click **Programs**, and then click **Uninstall a Program**.

2. In the **Programs and Features** window, double-click the installed Rapid Recovery Core instance; for example:

   ```
   Core-X64-6.0.x.xxxxx.exe
   ```

   If uninstalling the Appassure Core, the version number will be different, for example:

   ```
   Core-X64-5.4.x.xxxxx.exe
   ```

3. Do one of the following:

   - **If the version of Rapid Recovery Core installed does not include support for localization, then the Rapid Recovery Core Installation Wizard appears, showing the Repair/Remove page. Skip to Step 4.**

   - **If the version of Rapid Recovery Core installed includes support for localization, then the Setup dialog box appears.**

     ▪ In the **Setup** dialog box, from the **Choose your language** drop-down menu, select the appropriate display language, and then click **OK**.

       For example, select **English**.

     ▪ Proceed to Step 4.

       The Rapid Recovery Core Installation Wizard appears, showing the **Repair/Remove** page.

4. On the **Repair/Remove** page of the Rapid Recovery Core Installation wizard, select **Remove**, and then click **Next**.

   The **Remove Options** page appears.

5. Do one of the following:

   - **To remove your repository, as well as all recovery points and change logs, select Uninstall configuration settings and data including all backup images and change logs, and then click Uninstall.**

     ℹ **NOTE:** If you select this option, you will delete all data in the repository, including the repository folder and all subfolders. This option is appropriate for typical installations where the repository is installed on an otherwise empty volume. If you have other data on the directory where your repository is located, do not select this option.

   - **To leave your repository but remove the Rapid Recovery Core software, clear this option and then click Uninstall.**

     The **Progress** page appears. You can view the progress of the uninstall action on the Progress page. When the uninstall is complete, the **Completed** page box appears.

6. Click **Finish** to close the wizard and exit.

Uninstalling the Rapid Recovery Agent software

When you remove a machine from protection on the Rapid Recovery Core, the Agent software is not affected. To remove the Rapid Recovery Agent software from a machine, perform the steps described in the following sections, based on the operating system of the machine.

Regardless of the operating system, you must restart the machine to complete the removal of the Rapid Recovery Agent software.

Related tasks
See also: Uninstalling the Rapid Recovery Agent software from a Windows machine
Related references
See also: Uninstalling the Rapid Recovery Agent software from a Linux machine

Uninstalling the Rapid Recovery Agent software from a Windows machine

Complete the steps described in this procedure to uninstall the Rapid Recovery Agent software from a Windows machine.

> **i** | **NOTE:** If uninstalling the AppAssure Agent software from a Windows machine, the steps are the same except for the product name in the control panel or uninstall wizard.

1. On the computer from which you want to uninstall the Rapid Recovery Agent software, open the Control Panel, click **Programs**, and then click **Uninstall a Program**.

2. In the **Programs and Features** window, double-click the installed version of the Rapid Recovery (or AppAssure Agent) software.

    The Rapid Recovery Agent Installation Wizard appears, showing the Repair/Remove page.

3. Select **Remove**, and then click **Next**.

    The **Remove Options** page appears.

4. To remove all data and settings installed by the Rapid Recovery Agent software, select **Uninstall the configuration settings and data, including all backup images and change logs** and then click **Uninstall**.

    > **!** | **CAUTION: If you select this option, one setting that is removed is the agent ID, a unique identifier assigned to this protected machine. If you remove the agent ID, and install Rapid Recovery Agent on this machine in the future, you will not be able to connect to existing recovery points saved in the repository. If you want to protect this machine with all of the previous settings and be able to access the existing recovery points in the future, do not select this option.**

    The **Progress** page appears. You can view the progress of the uninstall action on the Progress page.

    When the removal is complete, the **Completed** page appears.

5. On the **Completed** page, you see a message indicating that the system must be restarted before the configuration changes take effect. Take one of the following actions, and then click **Finish**:

    *   **To restart now, select Yes, I want to restart my computer now.**

    *   **To restart later, clear the Yes, I want to restart my computer now option.**

i **NOTE:** You must restart your system to complete the removal of the Agent software.

Uninstalling the Rapid Recovery Agent software from a Linux machine

The method for removing the Agent software on Linux machines has changed. As of release 6.0.1, instead of using shell scripts, the process of uninstalling the Agent software uses the package manager relevant to the Linux distribution on the protected machine.

To uninstall an earlier version, such as AppAssure Agent release 5.4.3, see the topic Uninstalling the AppAssure Agent software from a Linux machine.

Because the various supported Linux distributions use different package managers, the procedure for removing Rapid Recovery Agent on any supported Linux OS depends on the package manager used. The package managers, and the Linux distributions they support, are described in the following table.

Table 15. Package managers and the Linux distributions they support

This table lists the package managers used for installing Rapid Recovery on a Linux machine. The first column includes the package manager supported. The second column lists the relevant Linux distributions each package manager supports.

Package Manager	Linux Distribution
yum	Linux distributions based on Red Hat Enterprise Linux (RHEL), including RHEL, CentOS, and Oracle Linux.
zypper	SUSE Linux Enterprise Server (SLES) versions 11, 12
apt	Linux distributions based on Debian, including Debian 7 or 8, and Ubuntu 12.04 and later

As a one-time setup step for each Linux machine, you must configure your local software repository to point to the location where the package manager obtains Rapid Recovery installation files.

i **NOTE:** This process is represented by steps 1 through 4 in each of the installation procedures. When upgrading future editions of the Rapid Recovery Agent on a Linux machine with the repository configured, you will not need to perform these steps.

After you configure a software repository on your Linux machine, the package manager is able to retrieve and install the packages needed for installation or removal of Rapid Recovery Agent software and related components, such as aamount (now called local mount), aavdisk (now called rapidrecovery-vdisk), and Mono (an open source, Ecma standard-compliant, .NET Framework-compatible tool set used for porting the Agent software to Linux platforms).

For each package manager, you can run the appropriate command at the command line to determine if it is configured to download Rapid Recovery packages. These commands are listed in the following table.

Table 16. Command to show package manager repository configuration

This table lists the commands for each package manager to run to determine if it is configured to download Rapid Recovery on a Linux machine. The first column includes the package manager supported. The second column lists the relevant command to enter at the command line.

Package Manager	Command to list configured repositories
yum	yum replolist

Package Manager	Command to list configured repositories
zypper	zypper repos
apt	ls /etc/apt/sources.list.d

The uninstall instructions differ, depending on the Linux distribution you are using. For more information on uninstalling Rapid Recovery Agent from a Linux machine, see the following topics:

See also:

Uninstalling the Rapid Recovery Agent software from Debian and Ubuntu systems

To remove Rapid Recovery Agent from a Debian or Ubuntu machine, the Agent must be installed, and your local software repository be configured to point to the location where the package manager obtains Rapid Recovery installation files.

The Rapid Recovery Agent .deb file is an archive containing repository information specific to the apt package manager. Complete the following steps to remove the Rapid Recovery Agent from a Debian or Ubuntu Linux machine.

1. Open a terminal session with root access.
2. If you want to remove the configuration file for the software repository, as well as remove Agent and related files, skip to Step 4.
3. If you want to remove Agent and related files, leave the configuration for the software repository, then type the following command, and then press **Enter**:

   ```
   apt-get remove rapidrecovery-agent rapidrecovery-mono
   ```

   The package manager removes the Agent application and related files.
4. If you want to remove the configuration file for the software repository, as well as remove Agent and related files, then type the following command, and then press **Enter**:

   ```
   apt-get remove rapidrecovery-agent rapidrecovery-mono rapidrecovery-repo
   ```

   The package manager removes the application, related files and the software repository.
5. To remove files that are dependencies of the Agent software (including dkms, gcc, and so on), type the following command, and then press **Enter**:

   ```
   apt-get autoremove
   ```

   The dependent files are removed from the Linux machine.

Uninstalling the Rapid Recovery Agent software from RHEL, CentOS, or Oracle Linux

To remove Rapid Recovery Agent from a RHEL, CentOS, or Oracle Linux machine, the Agent must be installed, and your local software repository be configured to point to the location where the package manager obtains Rapid Recovery installation files.

The Rapid Recovery Agent .rpm file is an archive containing repository information specific to the yum package manager. Complete the following steps to remove the Rapid Recovery Agent on RHEL, CentOS, or Oracle Linux.

1. Open a terminal session with root access.
2. If you want to remove the configuration file for the software repository, as well as remove Agent and related files, skip to Step 4.
3. If you want to remove Agent and related files, leave the configuration for the software repository, then type the following command, and then press **Enter**:

   ```
   yum remove rapidrecovery-agent rapidrecovery-mono
   ```

   The package manager removes the Agent application and related files.
4. If you want to remove the configuration file for the software repository, as well as remove Agent and related files, then type the following command, and then press **Enter**:

   ```
   yum remove rapidrecovery-agent rapidrecovery-mono rapidrecovery-repo
   ```

   The package manager removes the application, related files and the software repository.
5. To remove files that are dependencies of the Agent software (including dkms, gcc, and so on), type the following command, and then press **Enter**:

   ```
   yum autoremove
   ```

   The dependent files are removed from the Linux machine.

Uninstalling the Rapid Recovery Agent software from SUSE Linux Enterprise Server

To remove Rapid Recovery Agent from a SUSE machine, the Agent must be installed, and your local software repository be configured to point to the location where the package manager obtains Rapid Recovery installation files.

The Rapid Recovery Agent .rpm file is an archive containing repository information specific to the zypper package manager. Complete the following steps to remove the Rapid Recovery Agent from a SUSE Linux machine.

1. Open a terminal session with root access.
2. If you want to remove the configuration file for the software repository, as well as remove Agent and related files, skip to Step 4.
3. If you want to remove Agent and related files, leave the configuration for the software repository, then type the following command, and then press **Enter**:

   ```
   zypper remove rapidrecovery-agent rapidrecovery-mono
   ```

   The package manager removes the Agent application, related files, and Agent dependencies (including dkms, gcc, and so on).
4. If you want to remove the configuration file for the software repository, as well as remove Agent and related files, then type the following command, and then press **Enter**:

   ```
   zypper remove rapidrecovery-agent rapidrecovery-mono rapidrecovery-repo
   ```

   The package manager removes the application, related files, the software repository, and Agent dependencies (including dkms, gcc, and so on).

Uninstalling the AppAssure Agent software from a Linux machine

If upgrading from AppAssure Agent to Rapid Recovery Agent on a Linux machine, you must first uninstall AppAssure Agent.

If you want the Linux machine to be able to connect to existing recovery points, before uninstalling, Quest recommends first backing up the unique agent ID. For more information, see Backing up and restoring the AppAssure agent ID.

The process to remove the AppAssure Agent software from a Linux machine uses a shell script. The uninstall instructions differ depending on the Linux distribution you are using.

> **i** **NOTE:** As of Rapid Recovery release 6.0.1, instead of using a shell script, uninstalling the Agent software from a Linux machine uses the package manager relevant to the Linux distribution on the protected machine. The same package manager is required for online installation of Rapid Recovery Agent. For more information on which package manager is appropriate for a specific supported Linux distribution, see About installing the Agent software on Linux machines.

Complete the steps in the following topics to uninstall the AppAssure Agent software from a Linux machine, based on the distribution.

Related tasks

See also: Uninstalling the AppAssure Agent software on Ubuntu systems
See also: Uninstalling the AppAssure Agent software on Red Hat Enterprise Linux, CentOS, and Oracle Linux systems
See also: Uninstalling the AppAssure Agent software on SUSE Linux Enterprise Server systems

Backing up and restoring the AppAssure agent ID

When you remove the AppAssure Agent software in preparation for installing the new Rapid Recovery version of the Agent, you also remove the unique identification number associated with that machine. This removal results in the inability to connect to the recovery points saved to the Core for that protected Linux machine.

Before removing AppAssure Agent, you can back up the agent ID values. Then you can install Rapid Recovery Agent and restore the settings.

Use the following procedure to back up agent ID values, and then to restore them afterward.

1. On the Linux machine from which you intend to remove AppAssure Agent, open a command prompt. Type the following command and then press **Enter**:

   ```
   sudo cp -p /root/.mono/registry/CurrentUser/software/apprecovery/agent/agentid/values.xml ~/v
   ```

   A file named values-backup.xml containing your unique agent ID is saved to the specified location.

2. Remove AppAssure Agent following the steps specific to the appropriate Linux distribution. For more information, see Uninstalling the AppAssure Agent software from a Linux machine.

3. Install Rapid Recovery Agent online using the appropriate package manager, or offline using the appropriate steps. For more information, see About installing the Agent software on Linux machines.

4. Run the appropriate configuration steps for the updated Linux machine. For more information, see Configuring the Rapid Recovery Agent on a Linux machine.

5. Copy the `values-backup.xml` file to the new location by typing the following command and then pressing **Enter**:

   ```
   sudo mv ~/values-backup.xml /root/.mono/registry/CurrentUser/software/apprecovery/agent/agent
   ```

6. Restart the rapidrecovery-agent service or reboot the machine.

   The original agent ID for that machine is now associated with the updated Rapid Recovery Agent software.

Check the Rapid Recovery Core to see if the machine appears. If not, use the Protect Machine wizard to add the upgraded machine to protection in the Core.

> **i** **NOTE:** After updating Rapid Recovery Agent, the first snapshot will result in a base image, creating a new recovery point chain.

Uninstalling the AppAssure Agent software on Ubuntu systems

Complete the steps below to uninstall the Appassure Agent software on Ubuntu systems.

i | **NOTE:** The following steps apply to both 32-bit and 64-bit environments.

1. Open a terminal session with root access.
2. Change to the directory that includes the Appassure installation script, for example:

   `cd /home/appassure/`
3. Run the following command to identify the specific build number of the Agent software you want to remove:

   `/opt/appassure/mono/bin/mono /opt/appassure/aagent/Agent.Service.Mono.exe 2>dev/null`
4. Run the following command, modifying it to specify the build number you identified:

   `./appassure-installer_ubuntu_amd64_5.x.x.xxxxx.sh -u`

   For example, if uninstalling Agent Version 5.4.3.106, the modified command is:

   `./appassure-installer_ubuntu_amd64_5.4.3.106.sh -u`

   The system removes the Appassure Agent files and directories.

After completing this process, the Agent software is removed from the system. To protect your machine in the Rapid Recovery Core, install the Rapid Recovery Agent software or use agentless protection.

Uninstalling the AppAssure Agent software on Red Hat Enterprise Linux, and CentOS systems

Complete the steps below to uninstall the AppAssure Agent software on RHEL, or CentOS systems.

i | **NOTE:** The following steps apply to both 32-bit and 64-bit environments.
For 32-bit RHEL, and CentOS systems, the file extension in the steps below will change from "x86_64" to "i386".

1. Open a terminal session with root access.
2. Change to the directory that includes the AppAssure installation script, for example:

   `cd /home/AppAssure/`
3. Run the following command to identify the specific build number of the Agent software you want to remove:

   `/opt/AppAssure/mono/bin/mono /opt/AppAssure/aagent/Agent.Service.Mono.exe 2>dev/null`
4. Run the following command, modifying it to specify the build number you identified:

   `./AppAssure-installer_rhel_amd64_5.x.x.xxxxx.sh -u`

   For example, if uninstalling Agent Version 5.4.3.106, the modified command is:

   `/AppAssure-installer_rhel_amd64_5.4.3.106.sh -u`

   The system removes the AppAssure Agent files and directories.

After completing this process, the Agent software is removed from the system. To protect your machine in the Rapid Recovery Core, install the Rapid Recovery Agent software or use agentless protection.

Installation and Upgrade Guide
Uninstalling the AppAssure Agent software on Red Hat Enterprise Linux, and CentOS systems

49

Uninstalling the AppAssure Agent software on SUSE Linux Enterprise Server systems

Complete the steps below to uninstall the AppAssure Agent software on SUSE Linux Enterprise Server (SLES) systems.

> **i** **NOTE:** The following steps apply to both 32-bit and 64-bit environments.

1. Open a terminal session with root access.
2. Change to the directory that includes the AppAssure installation script, for example:
   ```
   cd /home/appassure/
   ```
3. Run the following command to identify the specific build number of the Agent software you want to remove:
   ```
   /opt/appassure/mono/bin/mono /opt/appassure/aagent/Agent.Service.Mono.exe 2>dev/null
   ```
4. Run the following command, modifying it to specify the build number you identified:
   ```
   ./appassure-installer_sles_amd64_5.x.x.xxxxx.sh -u
   ```

   For example, if uninstalling Agent Version 5.4.3.106, the modified command is:
   ```
   ./appassure-installer_sles_amd64_5.4.3.106.sh -u
   ```

   The system removes the AppAssure Agent files and directories.

After completing this process, the Agent software is removed from the system. To protect your machine in the Rapid Recovery Core, install the Rapid Recovery Agent software or use agentless protection.

Uninstalling the Rapid Recovery Central Management Console

Complete the steps in this procedure to uninstall the Rapid Recovery Central Management Console.

1. On the Windows server from which you want to uninstall the Rapid Recovery Central Management Console, open the Control Panel, click **Programs**, and then click **Uninstall a Program**.
2. In the Programs and Features window, double-click the installed Rapid Recovery Central Management Console instance; for example:
   ```
   Central Console-X64-5.x.x.xxxxx.exe
   ```

   The Rapid Recovery Central Management Console Installation Wizard appears, showing the Repair/Remove page.

3. Select **Remove**, and then click **Next**.

   The **Remove Options** page appears.

4. Select **Uninstall configuration settings and data including all backup images and change logs,** and then click **Uninstall**.

   The **Progress** page appears. You can view the progress of the uninstall action on the Progress page.

   When the uninstall is complete, the **Completed** page appears.

5. Click **Finish** to close the wizard and exit.

About the Local Mount Utility

The Local Mount Utility (LMU) is a downloadable Windows-based application that lets you mount a Rapid Recovery recovery point in any of the three available modes on any compatible Windows machine. The light-weight utility can be installed on the same 32-bit and 64-bit Windows operating systems as the Rapid Recovery Agent software, but it does not have to be installed on the same machine as the Agent. The LMU includes the rapidrecovery-vdisk (formerly aavdisk) and aavstor drivers, but it does not run as a service. When you install the utility, by default, it is installed in the directory `C:\Program Files\AppRecovery\Local Mount Utility` and a shortcut appears on the machine's desktop.

While the utility was designed for remote access to a Rapid Recovery Core machine, you can also install the LMU on the same machine as a Rapid Recovery Core. When it runs on a Core, the application recognizes and displays all mounts from that Core, including mounts performed through the Rapid Recovery Core Console. Likewise, mounts performed on the LMU also appear in the Core Console.

When the LMU is installed on the same machine as Mailbox Restore, the LMU automatically launches Mailbox Restore when you use it to open an Exchange database. Mailbox Restore is the Rapid Recovery application used to restore Microsoft Exchange data stores and items. You can install it upon installation of the LMU or the Rapid Recovery Core. For more information about Mailbox Restore, see the *Rapid Recovery Mailbox Restore for Microsoft Exchange User Guide.*

> **i** | **NOTE:** Linux machines use a command-line utility, local_mount, to query the Core for protected machines and their corresponding recovery points. Similarly, that tool lets users remotely mount a recovery point volume; lets users explore the volume contents at the file levels; and lets users restore a individual files or an entire volume from the recovery point, including BMR of the system volume. For more information, see the *Rapid Recovery User Guide*.

Downloading the Local Mount Utility

There are two ways to download the Local Mount Utility. You can download the web installer version of the software directly from the Rapid Recovery Core Console, which is practical if you are installing the LMU on the Core. You can also download either 32-bit or 64-bit executable installer files for the LMU from the Rapid Recovery License Portal.

This section includes the following topics:

- Downloading the LMU from the Rapid Recovery Core Console
- Downloading the LMU from the Rapid Recovery License Portal

Downloading the LMU from the Rapid Recovery Core Console

Complete the following steps to download the Local Mount Utility from the Rapid Recovery Core Console.

1. From the machine on which you want to install the LMU, access the Rapid Recovery Core Console by entering the console URL into your browser and logging on with your user name and password.
2. From the Rapid Recovery Core Console, in the icon bar, click ⋮ (More), and then select **Downloads**.
3. Under Local Mount Utility, click **Download web installer**.
4. From the **Opening LocalMountUtility-Web.exe** window, click **Save File**.

    The file saves to the local Downloads folder. In some browsers, the folder automatically opens or a pop-up message gives you the option to run the installation.

Downloading the LMU from the Rapid Recovery License Portal

If you have already registered your Rapid Recovery Core software in the Rapid Recovery License Portal, do the following:

1. From the machine on which you want to install the LMU, open a web browser and log in to the license portal at https://licenseportal.com.

2. From the left navigation menu of the license portal, click **Downloads**.

3. From the **Downloads** page, scroll down to Windows-Based Applications. From the Local Mount Utility section, based on the architecture of the machine on which you are installing the utility (64-bit systems or 32-bit systems on the x86 architecture), click **Download**.

   The file saves to the local Downloads folder. In some browsers, the folder automatically opens or a pop-up message gives you the option to run the installation.

i | **NOTE:** For more information about managing the Rapid Recovery License Portal from the Rapid Recovery Core Console, see the *Rapid Recovery User Guide*. For complete documentation of the license portal, see the *Rapid Recovery License Portal User Guide*.

Installing the Local Mount Utility

The Local Mount Utility (LMU) can be installed using the web installer, or using an executable installation file specific to the architecture of the machine on which it is being installed. The process is the same regardless of which installer you use. Follow the procedure below to install or upgrade the Local Amount Utility.

1. From the machine on which you want to install the LMU, locate the executable installation file.

   ◦ If you downloaded the installer from the Core, the install file uses the web installer, which is named LocalMountUtility-Web.exe.

   ◦ If you downloaded from the License Portal, the installer name includes the architecture of your operating system, for example LocalMountUtility-X32-6.X.X.xxxx.exe or LocalMountUtility-X64-6.X.X.xxxx.exe.

2. Double-click on the executable LMU installer file to start the installer.

   Depending on the configuration of your machine, the **User Account Control** window or the **Open File - Security Warning** window may appear.

3. If prompted for permission, confirm that you want to run the installer and make changes to the system.

4. If .NET components are missing or need to be upgraded, accept the prompts to download and install the framework.

5. In the **Setup** dialog box, from the language field, select the appropriate language and then click **OK**.

6. Choose from one of the following:

   • **If this is the first time the Rapid Recovery LMU software is being installed on this machine, the installer prepares the installation, and then the Rapid Recovery Local Mount Utility Installation Wizard appears. Proceed to Step 7.**

   • **If this machine has an earlier version of the Rapid Recovery Local Mount Utility software installed, you will see a message asking if you want to upgrade to the current version.**

     1. Click **Yes**.

        The Rapid Recovery **Local Mount Utility Installation Wizard** appears, showing the **Progress** page of the wizard. The application downloads to the destination folder, with progress displayed in the progress bar. When finished, the wizard automatically advances to the **Completed** page. Skip to Step 13.

7. In the Rapid Recovery Local Mount Utility Installation Wizard, on the **Welcome** page, click **Next** to continue with the installation.

The **License Agreement** page appears.

8. On the **License Agreement** page, select **I accept the terms in the license agreement**, and then click **Next**.

   The **Prerequisites** page appears.

9. The Rapid Recovery LMU Installer verifies the existence of the prerequisite files.

   - **If the prerequisites do not exist, the Installer identifies which files are needed and displays the results accordingly. Click Install Prerequisites.**

   - **If the prerequisite files exist, a message appears indicating that all prerequisites are installed on the machine.**

10. Once the installation of the prerequisite files is completed, click **Next**.

    The **Installation Options** page appears.

11. On the **Installation Options** page, review the installation options. If necessary, modify them as described below.

    - **In the Destination Folder text field, review the destination folder for the installation. If you want to change the location, do the following:**

      ▪ Click the folder icon.

      ▪ In the **Browse to Destination Folder** dialog box, select a new location.

      ▪ Click **OK**.

    - **Optionally, in the Select optional components area, if you want to install Mailbox Restore, select Mailbox Restore for Exchange. If you do not wish to install Mailbox Restore, clear this option.**

      Mailbox Restore for Microsoft Exchange is a comprehensive email recovery program that works with Rapid Recovery and the Rapid Recovery LMU to recover Exchange items from a full data store to a single email message. For more information about Mailbox Restore, see the Rapid Recovery Mailbox Restore for Microsoft Exchange User Guide.

      i | **NOTE:** You can install Mailbox Restore only on 64-bit machines.

    - **Select Allow Local Mount Utility to automatically send diagnostic and user information to Quest Inc. to share this type of information (in aggregate) with Quest. If you do not want to send this information, clear this option.**

12. Once you are satisfied with the installation options, click **Install**.

    The **Progress** page of the wizard appears, and the application downloads to the destination folder, with progress displayed in the progress bar. When finished, the wizard automatically advances to the **Completed** page.

13. On the **Completed** page, click **Finish** to close the wizard.

Uninstalling the Local Mount Utility

Complete the steps in this procedure to uninstall the Rapid Recovery Local Mount Utility.

1. On the Windows server from which you want to uninstall the Rapid Recovery Local Mount Utility, open the Control Panel, click **Programs**, and then click **Uninstall a Program**.

2. In the Programs and Features window, double-click the program you want to remove.

3. Do one of the following:

   - **If the version of Rapid Recovery LMU installed does not include support for localization, then the Rapid Recovery Local Mount Utility Installation Wizard appears, showing the Repair/ Remove page. Skip to Step 4.**

   - **If the version of Rapid Recovery LMU installed includes support for localization, then the Setup dialog box appears.**

     - In the Setup dialog box, from the Choose your language drop-down menu, select the appropriate display language, and then click **OK**.

       For example, select **English**.

     - Proceed to Step 4.

       The Rapid Recovery Local Mount Utility Installation Wizard appears, showing the Repair/Remove page.

4. On the Repair/Remove page of the Rapid Recovery Local Mount Utility Installation wizard, select **Remove**, and then click **Next**.

   The Remove Options page appears.

5. Do one of the following:

   - **To remove the LMU application and any supporting log files, select Uninstall the configuration settings and data including all backup images and change logs, and then click Uninstall.**

   - **To leave LMU log files on this machine but remove the Rapid Recovery LMU software, clear this option and then click Uninstall.**

     The Progress page appears. You can view the progress of the uninstall action on the Progress page. When the uninstall is complete, the Completed page box appears.

6. Click **Finish** to close the wizard and exit.

Upgrading to Rapid Recovery

This topic describes how to upgrade an installation of AppAssure Core or Agent from AppAssure release 5.2.x, 5.3.x, or 5.4.x to the rebranded Rapid Recovery release 6.1.

This topic also describes how to upgrade from an earlier supported version Rapid Recovery to the current version.

Read this chapter in its entirety before deciding whether to upgrade to Rapid Recovery release 6.1.

Upgrading to the latest release of Rapid Recovery ensures that your environment is equipped with the latest features, fixes and enhancements available. For a summary, see the *Rapid Recovery Release Notes*. Release notes and other Rapid Recovery technical documents are available on the Quest documentation website at https://support.quest.com/rapid-recovery/technical-documents/.

Upgrade only after careful consideration about the effect it may have on your machines. For example:

- Quest requires users to carefully review the release notes for each release, and system requirements for that release, prior to upgrading. This process helps to identify and preclude potential issues.

- Most work environments expand over time, adding computer systems and complexity. Quest recommends customers review their environments before upgrading and adjust accordingly. Quest also recommends performing this review at least once annually, whether or not you are upgrading.

- To help determine that enough resources are dedicated to sufficiently protect your environment with Rapid Recovery, review the *Rapid Recovery 6.0 Sizing Guide 3.0*.

Rapid Recovery Core and Agent compatibility

The following table provides a visual guide of the interoperability between Core and Agent software versions. This table lists versions tested for release 6.1.2.

Table 17. Interoperability between Core and Agent versions

This table explicitly lists compatibility between specific Agent and Core software versions.

	AppAssure 5.4.3 Core	Rapid Recovery 6.0.2 Core	Rapid Recovery 6.1.1 Core	Rapid Recovery 6.1.2 Core
AppAssure 5.4.3 Agent[1]	Fully compatible	Fully compatible	Fully compatible[2, 3]	Fully compatible[2, 3]
Rapid Recovery 6.0.2 Agent	Not compatible	Fully compatible	Fully compatible[3]	Fully compatible[3]
Rapid Recovery 6.1.1 Agent	Not compatible	Not compatible	Fully compatible	Fully compatible[3]
Rapid Recovery 6.1.2 Agent	Not compatible	Not compatible	Not compatible	Fully compatible

[1] EFI partitions on protected machines must be upgraded to Rapid Recovery Agent release 6.0.x or later to successfully restore data, perform bare metal restore, or perform virtual export.

[2] Release 6.1 release notes erroneously indicated that 5.4.3 Agent in 6.1.0 Core was not supported. This configuration is tested and supported. See Note 1.

[3] Users can protect machines using older versions of the Agent software in a newer Core. Logically, newer features provided in more recent versions of Rapid Recovery Agent are not available for machines protected with older versions of Agent installed.

The matrix shows releases that have been fully tested with this release, and represent fully supported releases, plus the most recent prior release (6.1.1). Other software versions in limited support status (such as releases 6.0.1 and 6.1) have not been tested for interoperability, but are also expected to work.

Other factors affect interoperability. For example, the Rapid Snap for Virtual feature was first introduced in Rapid Recovery Core version 6.0, letting you protect VMware ESXi VMs agentlessly. Rapid Recovery release 6.1.0 expanded this support to host-based protection for Hyper-V VMs. Logically, users of Core version 5.4.3 cannot agentlessly protect any VMs. And users of Core version 6.0 cannot protect VMs on Hyper-V without installing the Agent software.

Upgrading factors to consider

When upgrading from AppAssure to Rapid Recovery on your machines, or upgrading from one version of Rapid Recovery to another, it is important to be mindful of the following best practices:

- If upgrading to Rapid Recovery Core release 6.x, you can continue to protect machines with older versions of Agent, including AppAssure Agent release 5.4.3. If you want to use any new features or enhancements in the Agent software, you can upgrade to Rapid Recovery Agent release 6.x.

- Quest tests the compatibility of transfers between machines protected with AppAssure Agent 5.3.7 and Rapid Recovery Core release 6.x. For full supportability of any other functions, Quest suggests you upgrade the Agent software on your protected machines to AppAssure Agent release 5.4.3, or Rapid Recovery Agent release 6.x.

- Rapid Recovery installers (for both the Core and Agent software) can be used for first-time installation or for upgrading. Installers can be downloaded from the Rapid Recovery License Portal at https://licenseportal.com.

- You can install or upgrade Rapid Recovery Core from the Core Installer or the web installer. The Core Installer downloads the executable file in one task. The Core Web Installer streams a download of the latest version of the Rapid Recovery Core installer, which runs directly from the web and lets you pause and resume the process as needed. From a compatibility perspective, there is no difference between using the Core Installer or the web installer. Both versions are available for download from the Rapid Recovery License Portal.

- Before upgrading, verify that your system meets operating system, memory, processor, storage, and network requirements. For additional guidance for sizing your hardware, software, memory, storage, and network requirements, see Rapid Recovery knowledge base article 118407, "Sizing AppAssure and Rapid Recovery Deployments."

- Always upgrade the Core before upgrading protected machines with the Rapid Recovery Agent software.

- The Core machine can run a version of Rapid Recovery that is the same as, or more recent than, the version installed on protected machines.

- Protected machines must not run a version of the Agent software that is more recent than the version installed on the Core. This guideline only applies to the first three digits in a release name (for example, 5.4.2, 5.4.3, 6.0.1, 6.0.2, 6.1.0). For example, the build number for a supported Linux Agent version (5.4.3.5651) can be greater than the corresponding build number for the Core (5.4.3.106). Both build numbers in this example are for release 5.4.3.

> **i** | **NOTE:** Within a release, it is acceptable to use different build numbers. For example, if using the automatic update feature to install the latest versions of Agent on protected machines, there may be minor differences between Agent software versions, or between the Agent and the Core version.

- If using replication, always upgrade the target Core first, then upgrade the source Core, and lastly upgrade protected machines.

- The source Core must not run a version of Rapid Recovery more recent than the target Core.

> **!** | **CAUTION: If you see a message in the Core Console of a source Core indicating that a newer version of the Core software is available, but the message indicates that a replicated (target) Core has an earlier version, do not click Update Now. Instead, update the target Core first, and then update the source Core.**

- If using cross replication (when two Cores are replicating recovery points from each other's protected machines), replication must be paused on both Cores first. Then both Cores should be upgraded prior to resuming replication functions.

Consider localization before upgrading

Rapid Recovery release 6.1 is an international release. In addition to availability in English, this release is localized into simplified Chinese, French, Korean, German, Japanese, Brazilian Portuguese, and international Spanish. When a localized version is installed, you can see or change the current display language set for the Core Console in the general settings for the Core.

Rapid Recovery beta program considerations

Customers who participated in the Rapid Recovery beta program did so with the requirement that the beta software be installed in a lab environment, not a production environment. There is no direct upgrade path from a beta release to the generally available release. Interoperability of beta releases and production releases is not supported.

If you participated in the beta program, do not attempt to upgrade the beta version of the Rapid Recovery Core. Instead, if using the same server, perform the following steps:

- Delete your repository or repositories.

- Perform a full uninstall of the Rapid Recovery Core using the installer or from Control Panels, Add/Remove.

- Obtain the production version of the Core installer or Core web installer from the license portal and perform a clean install of the Core.

Upgrading AppAssure 5.x Core to Rapid Recovery Core

Before upgrading the AppAssure Core to Rapid Recovery Core, verify if you have any custom binaries applied, and note the binaries used. Doing so can increase the ability of Quest Support to assist you in the event of upgrading difficulties. For more information, see knowledge base article 132353.

Quest Software policy is to support two previous releases of software products.

If upgrading from AppAssure Core 5.4.3 to Rapid Recovery Core release 6.x, you can download the new installers from the license portal or the Core, and run them on your 5.4.3 Core as an in-place upgrade.

If you want to upgrade from AppAssure Core 5.3.x or 5.4.1 or 5.4.2, best practice is to perform a two-step upgrade process. The first step is to upgrade to the oldest supported release (in this case, to AppAssure 5.4.3).

You can then run the Rapid Recovery release 6.x installer for the Rapid Recovery Core or Agent component, respectively.

If upgrading from AppAssure Core 5.2.x to Rapid Recovery Core, you must use a three-step process. First, upgrade to AppAssure Core 5.3.7. Then upgrade to AppAssure release 5.4.3. Finally, upgrade to Rapid Recovery Core.

Additionally, be aware of the following information when upgrading from AppAssure 5.3.x and later:

- Recovery points are represented differently in AppAssure release 5.4.x and later, as part of the changes made to improve application performance. When upgrading from AppAssure 5.3.x to AppAssure 5.4.x, existing recovery points are converted to the new representation, which is not backward-compatible. You cannot downgrade an AppAssure release 5.4.x installation to 5.3 (or a Rapid Recovery release) unless you recreate your repository.

- When launching the Core for the first time after upgrading from versions prior to Rapid Recovery 5.4.1, the conversion of existing recovery points will take approximately twice as long as loading the same recovery points under previous versions. After this initial conversion, however, loading recovery points will be significantly faster than with previous versions.

  i | **NOTE:** When upgrading from AppAssure 5.3.x to 5.4.x, ensure that you factor extra time for converting recovery points into your planning before your upgraded environment is ready for use.

- After upgrading from versions prior to Rapid Recovery 5.4.1, if you attempt to set up a retention policy on a replicated target Core that differs from the replication policy on the source Core, you will first be prompted to perform a repository Integrity Check Job. The same requirement applies if you want to set up a custom retention policy for a replicated agent. Running this job can preemptively identify inconsistencies in replicated recovery points, providing the opportunity to replace those with error-free recovery points.

  ! | **CAUTION: Running the Integrity Check Job is expected to take an extended period of time. The time required differs for each environment, based on the quantity and type of data in your repository and also based on the underlying storage system. While the job is running, no other transactions can be performed in that repository, including transfers (snapshot and base image backups, and replication), nightly jobs, and so on. Ensure that you factor extra time for completing a lengthy Integrity Check Job into your planning if these situations apply to you.**

Upgrading AppAssure Agent or Rapid Recovery Agent

When upgrading the Agent software on protected Windows machines from Rapid Recovery Agent release 6.x, you can install the new version without removing the old version. If you want to upgrade a version older than two releases, best practice is to first upgrade to the last release or the one prior. After upgrading to the intermediate version, you can then run the Rapid Recovery Agent release 6.x Agent installer.

When upgrading the Agent software on Linux machines from any AppAssure release to Rapid Recovery Agent, first remove the old Agent software version. Then perform a clean install of Rapid Recovery Agent. When upgrading the Agent software on Linux machines from Rapid Recovery Agent release 6.0.1 or later, you can use the appropriate package manager.

When removing AppAssure Agent on Linux machines, the correct process is to use shell scripts. For more information, see Uninstalling the AppAssure Agent software from a Linux machine. When removing Rapid Recovery Agent release 6.0.1 or later on Linux machines, the correct process is to use the package manager appropriate for your distribution of Linux. For more information, see Uninstalling the Rapid Recovery Agent software from a Linux machine.

Upgrading steps overview

This topic provides an overview for upgrading your AppAssure environment to Rapid Recovery release 6.0x or 6.1x.

When upgrading AppAssure to Rapid Recovery, perform the following steps:

1. Review upgrading factors such as compatibility, replication scenarios, and best practices as described in this document. Factors include the following:

   - **Review the operating system of the Core machine and any machines you want to protect. For more information, see Rapid Recovery system requirements.**

   - **Ensure the Core you want to upgrade is sized appropriately. To help determine that enough resources are dedicated to sufficiently protect your environment with Rapid Recovery, review the** *Rapid Recovery 6.0 Sizing Guide 3.0*.

   - **If using replication, be sure to follow the upgrade order described in the topic Upgrading factors to consider.**

2. Verify that your Cores can contact the license server. The UI may differ slightly based on the version of Rapid Recovery or AppAssure Core you are using, but the following is a guideline:

   a. Navigate to the Core Console.

   b. On the icon bar, click ⚙ **Settings** and then select **Licensing**.

   c. Scroll down to the **License Server** pane and click **Contact Now**.

   After a brief pause, you can briefly see a message indicating that the license server was contacted.

3. From the Core machine or machines you want to upgrade, navigate to the license portal to download the Rapid Recovery release 6.0.1 or release 6.1 Core installer program, as applicable, but do not launch it yet. The steps include:

   a. Log into the license portal at https://licenseportal.com.

   b. From the License Portal navigation menu on the left side of the page, click **Downloads**.

   c. From the Windows-based Applications table, click **Download** to obtain the Core Installer or the Core Web Installer, but do not launch the installer yet.

4. Direct upgrade of the Core using the Core installer is fully supported from machines with the prior release installed (6.1.1). Upgrade of the Core is also fully supported from the latest build of the last two major/minor versions (in other words, Rapid Recovery release 6.0.2, and AppAssure Core release 5.4.3). If using these releases, you can use the Core installer or the Core web installer program without removing a prior version or without an interim upgrade. If upgrading to Rapid Recovery release 6.1x Core from a version of AppAssure Core older than two major/minor releases, you need to use a two-step or three-step upgrade process, as detailed in the topic Upgrading AppAssure 5.x Core to Rapid Recovery Core.

5. For each Core you want to upgrade, pause and disable all data transfer activities, including replication, snapshots, and nightly jobs. Doing so expedites the Core Service shut-down process during the upgrade. For information on how to pause activities, see the *Rapid Recovery User Guide*.

6. Run the installer programs on each Core you want to upgrade. If using replication, be sure to follow the upgrade order described in the topic Upgrading factors to consider. For specific instructions on using the Core installer, see Installing the Rapid Recovery Core.

7. Apply new license keys on each Core as appropriate. For more information, see the topic Applying a new license key or file.

8. You can protect older versions of AppAssure Agent on a Rapid Recovery release 6.x Core. Optionally, to take advantage of new features, update each protected machine with the latest Rapid Recovery Agent software. Consider the following options:

   - **For each protected machine, you can download the Agent software from the Downloads page of the license portal.**

   - **You can deploy the software to multiple machines simultaneously using the Deploy Agent Software option from the Rapid Recovery Core Console. This option is accessible from the Protect drop-down menu on the button bar. For more information, see the topic Deploying the Rapid Recovery Agent software to one or more machines in the** *Rapid Recovery User Guide.*

9. Direct upgrade of the Agent software using the Agent installer is fully supported from machines with the prior release installed (6.1.1). Upgrade of the Agent is also fully supported from the latest build of the last

two major/minor versions (in other words, Rapid Recovery release 6.0.2, and AppAssure Agent release 5.4.3). If using these releases, you can use the Agent installer without removing a prior version or without an interim upgrade. If upgrading to Rapid Recovery release 6.x Agent from a version of AppAssure Agent older than two major/minor releases, you need to use a two-step or three-step upgrade process, as detailed in the topic Upgrading AppAssure 5.x Core to Rapid Recovery Core.

- **For upgrading Windows machines with the AppAssure Agent to Rapid Recovery, use the same installer and perform the same steps as a clean installation. See Installing the Rapid   Recovery Agent software on Windows machines.**

- **You cannot directly upgrade a Linux machine that is currently protected with AppAssure Agent. You must uninstall AppAssure Agent, and then perform a clean install of Rapid Recovery release 6.x Agent.**

- **You can directly upgrade a Linux machine from Rapid Recovery release 6.x Agent (such as release 6.0.2) to a newer version of Agent (such as release 6.1.2). Linux installations now use a package manager specific to your Linux distribution. If the local software repository on the Linux machine is configured, then to upgrade a Linux machine from one version of Rapid Recovery Agent to a newer version of Agent, see About installing the   Agent software on Linux machines.**

- **Before installing Rapid Recovery Agent on a Linux machine that was previously protected with AppAssure Agent, you must uninstall AppAssure Agent. For more information, see Uninstalling the   AppAssure Agent software from a Linux machine.**

10. Run the installer programs on each Core you want to upgrade. If using replication, be sure to follow the upgrade order described in the topic Upgrading factors to consider. For specific instructions on using the Core installer, see Installing the Rapid Recovery Core.

11. Upon successful account registration, log on to the License Portal, and then click **Downloads** in the left navigation area.

12. To download and install the Core software, on the **Downloads** page, click the **Download** button next to Core Installer or Core Web Installer, as appropriate.

> **i** **NOTE:** The Core Installer downloads the executable file in one task. The Core Web Installer streams a download of the latest version of the Rapid Recovery Core installer, which runs directly from the Web and lets you pause and resume the process as needed. A trial license key is automatically generated and presented for you to use for the Core. The license key also appears in the confirmation email you receive after choosing your download option.

13. Click **Run** in the subsequent dialog boxes to install the software.

14. To download and install the Agent software, on the **Downloads** page, next to the Windows or Linux Agent installer version you want to download, click **Download**.

15. Click **Run** in the subsequent dialog boxes to install the software.

16. After you install the software, launch the Rapid Recovery Core Console to upgrade your trial license to the upgraded or purchased license.

    a. Navigate to the Rapid Recovery Core Console.

    b.
       On the icon bar, click ⚙ (Settings), and then scroll down on the right side of the **Settings** page until you can see the **License Details** heading.

    c. From the License Details area, click **Change License**.

    d. In the **Change License** dialog box, to upload a license file, do the following:

    a. Select **Upload License File** and click **Browse**.

    b. From the File Upload dialog box, locate and select the license file and then click **Open**.

    e. Or, in the **Change License** dialog box, enter a valid license key into the text field and then click **Continue**.

17. Under License Server, click **Contact Now**.

After the license is applied to the license server, any associated agents are automatically updated with the new license.

18. Restart all machines on which you installed the Agent software.

Upgrading the Rapid Recovery Agent software

This topic addresses upgrading the Agent software that protects your machine in a Rapid Recovery Core. Be sure to read this section before you upgrade. If installing the Rapid Recovery Agent software for the first time, see the topic Installing the Rapid Recovery Agent software.

Upgrade the Rapid Recovery Agent software on machines that you want to protect using Rapid Recovery Core version 6.0.2. The same Agent installer executable program can be used for a clean installation or to upgrade an existing version.

For information about getting the appropriate version of the Rapid Recovery Agent software, see Obtaining the Rapid Recovery Agent software. When the upgrade is complete, restart the machines as necessary, and then check the Core to verify that each upgraded machine is being protected.

Install the Rapid Recovery Agent software on machines that you want to protect using the following criteria:

- Install Rapid Recovery Agent software on every physical machine in your environment.

- Install Rapid Recovery Agent software on every Hyper-V or VirtualBox virtual machine you want to protect.

- Install Rapid Recovery Agent software on every VMware vCenter/ESXi virtual machine you want to protect with the Agent, instead of agentlessly.

i | **NOTE:** You can also protect VMware vCenter/ESXi virtual machines on a host using agentless protection. This method uses the ESX agent client and APIs without installing Rapid Recovery Agent software on each VM. Agentless protection offers some advantages, but also some restrictions. For example, Quest does not advise agentless protection for Microsoft SQL or Microsoft Exchange servers because the metadata is not collected without the Rapid Recovery software. Before deciding to use agentless protection, see the topic "Understanding agentless protection" in the *Rapid Recovery User Guide*.

Upgrading on a Windows machine

When upgrading AppAssure Agent to Rapid Recovery Agent, there is no need to uninstall the older version of Agent. Quest supports compatibility with two prior versions of our software. In the case of Rapid Recovery release 6.1, you can run installers on top of Rapid Recovery Agent release 6.0.1 and AppAssure Agent release 5.4.3.

When upgrading a version of AppAssure older than two versions, first update the machine to AppAssure release 5.4.3. Then run the Rapid Recovery release 6.0.1 or release 6.1 installer, as applicable.

i | **NOTE:** This upgrade policy applies to both Agent and Core.

Because there is more than one type of Windows machine, the steps for upgrading depend on the version of Windows installed. Upgrading a Windows machine includes the following options:

- To upgrade Agent on a machine with a standard Windows operating system, see Installing the Rapid Recovery Agent software on Windows machines. Supported Windows operating systems are listed in the topic Rapid Recovery release 6.1 operating system installation and compatibility matrix.

- To upgrade a machine with a Windows Server Core Edition operating system, see Installing the Agent software on Windows Server Core Edition machines.

i | **NOTE:** When upgrading to Rapid Recovery Agent on Windows machines on which the software drivers have changed, you are prompted to restart your system.

Upgrading on a Linux machine

When upgrading a Linux machine from AppAssure Agent to Rapid Recovery Agent, you must first uninstall the AppAssure Agent software. For more information, see Uninstalling the AppAssure Agent software from a Linux machine.

You can run the installer from the package manager to upgrade from a supported earlier release of Rapid Recovery Agent to the current release.

The procedure for upgrading a Linux machine from AppAssure Agent to Rapid Recovery Agent depends on the distribution of Linux installed on the machine. To upgrade a Linux machine, select the appropriate procedure from the following options:

- To upgrade a Linux machine with Red Hat Enterprise Linux (RHEL), CentOs, or Oracle Linux installed, seeUpgrading to Rapid Recovery Agent on Red Hat Enterprise Linux, CentOS, or Oracle Linux.

- To upgrade a Linux machine with SUSE Linux Enterprise Server installed, see Upgrading to Rapid Recovery Agent on SUSE Linux Enterprise Server.

- To upgrade a machine with an Ubuntu distribution of Linux installed, see Upgrading to Rapid Recovery Agent on Debian or Ubuntu.

i | **NOTE:** To ensure that the proper kernel driver version is used to protect your machine, the best practice is to restart the machine after the upgrade to Rapid Recovery Agent is complete.

For more information, see Upgrading Rapid Recovery Agent on a Linux machine.

Upgrading Rapid Recovery Agent on a Linux machine

This topic discusses the upgrade for an existing version of Rapid Recovery Agent on a Linux machine with the local software repository configured.

If the software repository was removed (as described in step 4 of the uninstall procedures for Rapid Recovery), then use the installation procedures specific to your distribution. See the topic About installing the Agent software on Linux machines.

As of release 6.0.1 and later, installing, removing or upgrading Rapid Recovery Agent on a Linux machine uses a new process. A package manager (specific to your distribution of Linux) facilitates the tracking of files needed to install or remove the Agent software.

Because the various supported Linux distributions use different package managers, the procedure for installing, upgrading, or removing Rapid Recovery Agent on any supported Linux OS depends on the package manager used. The package managers, and the Linux distributions they support, are described in the following table.

Table 18. Package managers and the Linux distributions they support

This table lists the package managers used for installing Rapid Recovery on a Linux machine. The first column includes the package manager supported. The second column lists the relevant Linux distributions each package manager supports.

Package Manager	Linux Distribution
yum	Linux distributions based on Red Hat Enterprise Linux (RHEL), including RHEL, CentOS, and Oracle Linux.
zypper	SUSE Linux Enterprise Server (SLES) versions 11, 12

Package Manager	Linux Distribution
apt	Linux distributions based on Debian, including Debian 7 or 8, and Ubuntu 12.04 and later

As a one-time setup step for each Linux machine, you must configure your local software repository to point to the location where the package manager obtains Quest Rapid Recovery installation files.

> **i** **NOTE:** This process is represented by steps 1 through 4 in each of the installation procedures. When upgrading future editions of the Rapid Recovery Agent on a Linux machine with the repository configured, you will not need to perform these steps.

After you configure a software repository on your Linux machine, the package manager is able to retrieve and install the packages needed for installation or removal of Rapid Recovery Agent software and related components, such as local mount (formerly known as aamount), rapidrecovery-vdisk (formerly called aavdisk), and Mono (an open source, Ecma standard-compliant, .NET Framework-compatible tool set used for porting the Agent software to Linux platforms).

For each package manager, you can run the appropriate command at the command line to determine if it is configured to download Rapid Recovery packages. These commands are listed in the following table.

Table 19. Command to show package manager repository configuration

This table lists the commands for each package manager to run to determine if it is configured to download Rapid Recovery on a Linux machine. The first column includes the package manager supported. The second column lists the relevant command to enter at the command line.

Package Manager	Command to list configured repositories
yum	yum replolist
zypper	zypper repos
apt	ls /etc/apt/sources.list.d

If the software repository exists on your Linux machine, you can follow the simplified instructions for upgrading in the section.

Upgrading to Rapid Recovery Agent on Debian or Ubuntu

The Rapid Recovery Agent .deb file is an archive containing repository information specific to the apt package manager. Complete the following steps to install the Rapid Recovery Agent on Debian 7 or higher, or on Ubuntu 12.04 and higher.

> **i** **NOTE:** To ensure that the proper kernel driver version is used to protect your machine, the best practice is to restart the machine after the upgrade to Rapid Recovery Agent is complete.

1. Open a terminal session with root access.
2. Install the Rapid Recovery Agent by invoking the apt package manager, updating the repository manager. Type the following command, and then press **Enter**:

   ```
   apt-get update
   ```
3. Tell the package manager to install the Rapid Recovery Agent software. Type the following command, and then press **Enter**:

```
apt-get install rapidrecovery-agent
```

4. The package manager prepares to install all dependent files. If prompted to confirm installation of unsigned files, enter **y** and then press **Enter**.

The Rapid Recovery Agent files are installed.

Upgrading to Rapid Recovery Agent on SUSE Linux Enterprise Server

The Rapid Recovery Agent .rpm file is an archive containing repository information for SUSE Linux Enterprise Server (SLES) . This distribution uses the zypper package manager. Complete the following steps to install the Rapid Recovery Agent on SLES.

> **i** **NOTE:** To ensure that the proper kernel driver version is used to protect your machine, the best practice is to restart the machine after the upgrade to Rapid Recovery Agent is complete.

1. Open a terminal session with root access.
2. Determine your present working directory by entering PWD and pressing **Enter**. For example, assume your directory is `/home/rapidrecovery/`.
3. Download the appropriate Rapid Recovery Agent .rpm installation file from the License Portal at https://licenseportal.com to your present working directory.

   For more information about the license portal, see the *Rapid Recovery License Portal User Guide*.

4. Install the Rapid Recovery Agent by invoking the zypper package manager, updating the repository manager. Type the following command, and then press **Enter**:

   ```
   apt-get update
   ```

5. Instruct the package manager to install the Rapid Recovery Agent software. Type the following command, and then press **Enter**:

   ```
   apt-get install rapidrecovery-agent
   ```

6. The package manager prepares to install all dependent files. If prompted to confirm installation of unsigned files, enter **y** and then press **Enter**.

   The Rapid Recovery Agent files are installed.

Upgrading to Rapid Recovery Agent on Red Hat Enterprise Linux, CentOS, or Oracle Linux

The Rapid Recovery Agent .rpm file is an archive containing repository information specific to Red Hat Enterprise Linux (RHEL), CentOS, or Oracle Linux. These distributions use the yum package manager. Complete the following steps to install the Rapid Recovery Agent on RHEL, CentOS, or Oracle Linux.

> **i** **NOTE:** To ensure that the proper kernel driver version is used to protect your machine, the best practice is to restart the machine after the upgrade to Rapid Recovery Agent is complete.

1. Open a terminal session with root access.
2. Install the Rapid Recovery Agent by invoking the yum package manager, updating the repository manager. Type the following command, and then press **Enter**:

   ```
   yum clean all
   ```

3. Instruct the package manager to install the Rapid Recovery Agent software. Type the following command, and then press **Enter**:

   ```
   yum install rapidrecovery-agent
   ```

4. The package manager prepares to install all dependent files. If prompted to confirm installation of unsigned files, enter **y** and then press **Enter**.

The Rapid Recovery Agent files are installed.

Applying a new license key or file

When you first sign up to try Rapid Recovery, you are given a trial account. A trial license key is automatically generated when you download the Rapid Recovery Core software from the Quest Software License Portal. This license key is written into the Rapid Recovery Core software installer for you to install the software. To request an upgrade of your license, contact your Quest Software sales representative or fill out the contact form at https:// quest.com/register/57955. After you upgrade or purchase your license, an email is sent to you that includes your new license key or license file. Perform the following procedure to enter this license key or file in the Core Console.

1. Register for an account at the Rapid Recovery License Portal at https://licenseportal.com. Ensure that you register using the email address that is on file with your Quest Software sales representative.

2. Upon successful account registration, log on to the License Portal, and then click **Downloads** in the left navigation area.

3. To download and install the Core software, on the **Downloads** page, click the **Download** button next to Core Installer or Core Web Installer, as appropriate.

   i | **NOTE:** The Core Installer downloads the executable file in one task. The Core Web Installer streams a download of the latest version of the Rapid Recovery Core installer, which runs directly from the Web and lets you pause and resume the process as needed. A trial license key is automatically generated and presented for you to use for the Core. The license key also appears in the confirmation email you receive after choosing your download option.

4. Click **Run** in the subsequent dialog boxes to install the software.

5. To download and install the Agent software, on the **Downloads** page, next to the Windows or Linux Agent installer version you want to download, click **Download**.

6. Click **Run** in the subsequent dialog boxes to install the software.

7. After you install the software, launch the Rapid Recovery Core Console to upgrade your trial license to the upgraded or purchased license.

8. From the icon bar, select ⚙ (Settings) and then click **Licensing**.

   The **License Details** area of the settings appears.

9. From the **License Details** pane, click **Change License.**

10. In the **Change License** dialog box, to upload a license file, do the following:

    • **Select Choose File.**

    • **From the File Upload dialog box, browse the filing system, locate the license file. Click the file and then click Open.**

    The **File Upload** dialog box closes and the filename of the license appears in the license key text field.

11. Or, in the **Change License** dialog box, in the license key text field, enter the license key. and then click **Continue**.

12. From the **Change License** dialog box, with the license key or file name appearing in the license key text field, click **Continue**.

    The **Change License** dialog box closes and the license is applied to the Core.

13. On the Core Settings page, scroll down to the License Server area and click **Contact Now.** The updated license is registered with the license server, and any associated agents are automatically updated with the new license.

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 https://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 our product