Dell Data Protection | Rapid Recovery™ 6.0

Installation and Upgrade Guide

Legend

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

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

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

Rapid Recovery Installation and Upgrade Guide
2016 - 05
Version - 6.0.2

Rev. A00

Contents

1

Introduction to Dell Data Protection | Rapid Recovery

Dell Data Protection | 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 Dell 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 Dell Rapid Recovery product support website at https://support.software.dell.com/rapid-recovery/
- The documentation website at https://support.software.dell.com/rapid-recovery/release-notes-guides/

2

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.

Topics:

Recommended network infrastructure

A decade ago, the standard backbone infrastructure featured speeds of 100 megabits per second. Demands for network traffic and input and output have increased steadily and substantially. As a result, standards for network backbones have increased to meet demand. Modern network backbones support speeds such as gigabit Ethernet (GbE), which transfers Ethernet frames at 1 gigabit per second, or 10GbE, which is ten times faster.

For running Rapid Recovery, Dell requires a minimum network infrastructure of 1GbE for efficient performance. Dell 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), Dell recommends using separate NIC cards for storage and network traffic, respectively.

Use network cables with the appropriate rating to obtain the expected bandwidth. Dell 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). UEFI is used in the Windows 8, Windows 8.1, Windows 10, Windows Server® 2012, and Windows Server 2012 R2 operating systems. For Windows systems, UEFI uses the Extensible Firmware Interface (EFI) system partitions that are handled as simple FAT32 volumes. Protection and recovery capabilities are available in Rapid Recovery for EFI system partitions.

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

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

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 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

In Rapid Recovery release 6.x, as in AppAssure release 5.4.x, support for cluster-shared volumes (CSV) is limited to native backup of CSVs running Windows Server 2008 R2. You can also restore CSV volumes running Windows Server 2008 R2 from a recovery point, or perform virtual export to a Hyper-V CSV running Windows Server 2008 R2. You cannot perform virtual export of a cluster-shared volume. New as of Rapid Recovery release 6.0 is the ability to perform virtual export to a Hyper-V CSV running Windows Server 2012 or Windows Server 2012 R2.

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

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

Table 1. AppAssure and Rapid Recovery support for cluster-shared volumes

Rapid Recovery Cluster Shared Volumes Support	Protect, Replicate, Rollup, Mount, Archive			Restore CSV Volumes			Virtual Export to Hyper-V CSV		
Rapid Recovery or AppAssure version	5.3	5.4	6.0	5.3	5.4	6.0	5.3	5.4	6.0
Windows Server 2008 R2	No	Yes	Yes	No	Yes	Yes	No	Yes	Yes
Windows Server 2012	No	No	No	No	No	No	No	No	Yes
Windows Server 2012 R2	No	No	No	No	No	No	No	No	Yes

While Rapid Recovery may let you protect some other operating systems on cluster-shared volumes, you do so at your own risk. Only the configurations in the table above are supported by Dell.

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 Dell 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 Dell Data Protection | DocRetriever for SharePoint – make sure you allocate more resources, in addition to those needed for efficient Core operations.

Depending on your license and your environment requirements, you may need to install multiple Cores, each on a dedicated server. Optionally, for remote management of multiple Cores, you can install the Rapid Recovery Central Management Console on a 64-bit Windows computer.

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

Before installing Rapid Recovery release 6.0.2, 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 Dell Data Protection | Rapid Recovery knowledge base article 185962, "Sizing Rapid Recovery Deployments."

CAUTION: Dell 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, and Windows Server 2012 R2 Core. Excluding Windows Server 2008 Core, these Core edition operating systems are supported for running the Rapid Recovery Agent software.

NOTE: Dell 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: Dell 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 Dell DL series of backup and recovery appliances.)

Rapid Recovery release 6.0.2 operating system installation and compatibility matrix

Microsoft Windows operating systems

Rapid Recovery Core must be installed on an appropriately sized server running a supported 64-bit Microsoft Windows operating system. The following table and notes list each Windows operating system and describes compatibility for each Rapid Recovery component or feature.

NOTE: This information is provided to educate users on compatibility. Operating systems that have reached end of life are not supported by Dell.

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

Windows OS	Core	Agent	Agentless	LMU	MR	DR	Boot CD
Windows XP SP3	No	No	Yes	No	No	No	No
Windows Vista™	No	No	Yes	No	No	No	No
Windows Vista SP2	No	Yes	Yes	Yes	Yes	Yes	Yes[1]
Windows 7	No	No	Yes	No	No	No	No
Windows 7 SP1	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Windows 8	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Windows 8.1	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Windows 10	Yes[3]	Yes[3]	Yes[3]	Yes	Yes	Yes	Yes
Windows Server 2003	No	No	Yes	No	No	No	No
Windows Server 2008	No	No	Yes	No	No	No	No
Windows Server 2008 SP2	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Windows Server 2008 R2	No	No	Yes	No	No	No	No
Windows Server 2008 R2 SP1	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Windows Server 2012	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Windows Server 2012 R2	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Windows installation and support notes:

[1] The boot CD supports bare metal restore of Vista SP2, but does not support driver injection.

[2] In general, AppAssure 5.4 and Rapid Recovery 6.0 components work on Windows 10, with the exception that the Rapid Recovery Add-on for Kaseya® cannot be installed on Windows 10.

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 Linux operating system and describes support for each Rapid Recovery component or feature.

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

Linux OS or distribution	Agent	Agentless	Live DVD
Red Hat Enterprise Linux 6.3 - 6.7	Yes	Yes	Yes
Red Hat Enterprise Linux 7.0 - 7.2	Yes	Yes	Yes
CentOS Linux 6.3 - 6.7	Yes	Yes	Yes
CentOS Linux 7.0 - 7.2	Yes	Yes	Yes
Debian Linux 7, 8	Yes	Yes	Yes
Oracle Linux 6.3 - 6.7	Yes	Yes	Yes
Oracle Linux 7.0 - 7.2	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	Yes	Yes
Ubuntu Linux 15.04, 15.10	Yes	Yes	Yes
Ubuntu Linux 16.04 LTS	Yes	Yes	Yes
SUSE Linux Enterprise Server 11 SP2 or later	Yes	Yes	Yes
SUSE Linux Enterprise Server 12	Yes[1]	Yes[1]	Yes[1]

Linux installation and support notes:

[1] Btrfs is not supported. This is the default file system on SUSE 12.

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 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) 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 Dell highly recommends using Error Checking & Correction (ECC) memory, to ensure optimum performance of Rapid Recovery Core servers.
Processor	Quad-core or higher
Storage	Dell 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, Dell recommends limiting the repository size to 6TB. Any storage device must meet the minimum input/output requirements. See Dell knowledge base article 185962, "Sizing Rapid Recovery Deployments" for guidance in sizing your hardware, software, memory, storage, and network requirements.

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

Table 5. Rapid Recovery Agent software requirements

Requirement	Details
Operating system	The Rapid Recovery Agent software supports 32-bit and 64-bit Windows and Linux operating systems, including the following: • Microsoft Windows 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* • Red Hat Enterprise Linux (RHEL) 6.3, 6.4, 6.5, 6.6, 6.7, 7.0, 7.1, 7.2 • CentOS Linux 6.3, 6.4, 6.5, 6.6, 6.7, 7.0, 7.1, 7.2 • Oracle Linux 6.3, 6.4, 6.5, 6.6, 6.7, 7.0, 7.1, 7.2 • Debian Linux 7, 8 • Ubuntu Linux 12.04 LTS, 12.10, 13.04, 13.10, 14.04 LTS, 14.10, 15.04, 15.10, 16.04 LTS • SUSE Linux Enterprise Server (SLES) 11 (SP2 and later), 12
	NOTE: Windows operating systems require the Microsoft .NET framework version 4.5.2 to be installed to run the Rapid Recovery Agent service. Operating systems listed above that are marked with * also require the ASP .NET 4.5.x role or feature. When installing or upgrading the Rapid Recovery Agent software, the installer checks for these components, and installs or activates them automatically if required. Additional operating systems are supported for agentless protection only. For more information, see Rapid Snap for Virtual agentless protection.

Requirement	Details
	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 2008 R2, 2012, and 2012 R2. 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. Only ext2, ext3, ext4, and xfs file systems are supported. Agents installed on Microsoft Hyper-V Server 2012 operate in the Core edition mode of Windows Server 2012. NOTE: Native backup of cluster shared volumes is supported on Windows 2008 R2 (SP2 and later) protected machines only.
Architecture	32-bit or 64-bit
Memory	4GB or higher
Processor	Single processor or higher
Microsoft Exchange Support	Microsoft Exchange 2007 SP1 Rollup 5 or later, Microsoft Exchange 2010, or Microsoft Exchange 2013
Microsoft SQL Support	Microsoft SQL Server 2005 or higher (excluding preview versions)
Microsoft SharePoint	Microsoft SharePoint 2007, 2010, 2013
Storage	Direct attached storage, storage area network or network attached storage
Network	1 gigabit Ethernet (GbE) minimum NOTE: Dell recommends a 10GbE network backbone for robust environments. Dell does not recommend protecting machines over a wide-area network (WAN). If you have multiple networked sites, Dell recommends installing a Core at each site. To share information, you can replicate between the Cores located at different sites. Replication between Cores is WAN-optimized. The data transmitted is compressed, deduplicated, and encrypted during transfer.
Network hardware	Use network cables with the appropriate rating to obtain the expected bandwidth. NOTE: Dell 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 Dell Data Protection | Rapid Recovery License Portal. Requirements for the Local Mount Utility are described in the following table.

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*
	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 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 2012 and 2012 R2. Windows Server 2008 Core edition and Windows Server 2008 R2 Core edition are not supported.
Architecture	32-bit or 64-bit
Memory	4GB or higher
Processor	Single processor or higher
Network	1 gigabit Ethernet (GbE) minimum NOTE: Dell recommends a 10GbE network backbone for robust environments.

Requirement	Details
Network hardware	Use network cables with the appropriate rating to obtain the expected bandwidth. NOTE: Dell 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 a VMware ESXi host without installing the Rapid Recovery Agent software. This feature, Rapid Snap for Virtual, is also called agentless protection.

Agentless protection 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. (Agentless protection does let you capture snapshots on dynamic volumes at the disk level.) Before using agentless protection, ensure that you understand both the benefits and restrictions. For more information, see the topic "Understanding agentless protection" in the *Dell Data Protection | Rapid Recovery User Guide*.

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

Agentless support for other operating systems

Rapid Recovery release 6.x uses Microsoft .NET 4.5.2, which is not supported by Windows XP SP3, Windows Vista (prior to SP2), Windows Server 2003, and Windows Server 2008. If you protected machines with these operating systems in an earlier Core version (such as AppAssure Core 5.4.3), the corresponding version of AppAssure Agent (which used an earlier version of .NET) was supported.

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

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

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

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

VMware ESXi environments are compatible with some operating systems that Dell 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. Dell 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 6.0.2 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. Dell strongly encourages users to review system requirements and release notes prior to installing any software version.

Dell 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 Dell Support representative. Reporting such difficulties lets Dell 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 standby feature of Rapid Recovery, you can perform a one-time virtual export, or define requirements for continual virtual export. This process can be performed from any protected machine, physical or virtual. Exporting your data to a virtual standby machine provides you with a high availability copy of the data. If a protected machine goes down, you can boot up the virtual machine to 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

Requirement	Details
Virtual machine host	VMware • VMware Workstation 7.0, 8.0, 9.0, 10, 11 • VMware vSphere on ESX or ESXi 4.0, 4.1, 5.0, 5.1, 5.5, 6.0 NOTE: Dell recommends running on the most recent supported VMware version. Microsoft Hyper-V • Hyper-V running on Microsoft Server 2008 SP2, 2008 R2 SP1, 2012, 2012 R2 • Hyper-V running on Microsoft Windows 8, 8.1 with Hyper-V, Windows 10 NOTE: For virtual export to any Hyper-V host, .NET 4.5.2 is required on the Hyper-V host. Oracle • Oracle 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 or VMware ESX(i) 5.5. Earlier OS are not supported based on an inability of the host to connect to the virtual hard disk (VHD). Both Hyper-V Gen 1 and Gen 2 VMs are supported. NOTE: Not all operating systems are supported on all hypervisors.
Storage	The storage reserved on the host must be equal to or larger than the storage in the guest VMs.
Architecture	32-bit or 64-bit

Rapid Recovery lets you protect VM hosts without installing the Rapid Recovery Agent software. This is known as agentless protection. For more information, including exclusions for agentless protection, see the Dell Data Protection | Rapid Recovery User Guide topic "Understanding agentless protection."

Agentless protection is supported as described in the following table.

Table 8. Hypervisor requirements supporting agentless protection

Requirement	Details
Virtual machine host	VMware • VMware vSphere on ESX or ESXi 5.0 (build 623860 or later), 5.1, 5.5, 6.0. • You should also install the latest VMware Tools on each guest.

Requirement	Details
	NOTE: Dell strongly recommends running on the most recent supported VMWare version.
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.

Dell 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, Dell 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 *Dell Data Protection | 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).

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

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

NOTE: You can generate an on-demand or scheduled report to monitor the size and health of your repository. For more information on generating a Repository report, see the topic Generating a report from the Core Console in the *Dell Data Protection | 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 *Dell Data Protection | Rapid Recovery User Guide*. For more information on managing Dell Data Protection | Rapid Recovery licenses, see the *Dell Data Protection | Rapid Recovery License Portal User Guide*. For more information on sizing your hardware, software, memory, storage, and network requirements, see the *Dell Data Protection | 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 Dell Data Protection | 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 Dell Data Protection | Rapid Recovery License Portal, obtaining a license key, and registering for an account, see the *Dell Data Protection | Rapid Recovery License Portal User Guide*.

3

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 virtual machines, you can opt to protect those machines without Rapid Recovery Agent. 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.

The steps you must follow to install Rapid Recovery are:

- **Step 1:** Register at the Dell Data Protection | 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 Dell Data Protection | Rapid Recovery License Portal account, see the Dell Data Protection | 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 *Dell Data Protection | 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 host without installing the Agent software. Some important exclusions apply. For more information, see the topic "Understanding agentless protection" in the *Dell Data Protection | 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 Central Management Console" in the *Dell Data Protection | Rapid Recovery User Guide*.

  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 *Dell Data Protection | 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.

Topics:

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.

  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. This new agentless protection feature for VMs is called Rapid Snap for Virtual. Future versions of Rapid Recovery are expected to include agentless protection for other supported VM platforms.
- **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.

Installing the Rapid Recovery Core

About this task

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 Dell Data Protection | 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 *Dell Data Protection | Rapid Recovery License Portal User Guide*.

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

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 Dell Data Protection | Rapid Recovery License Portal for each machine that you want to protect using the Rapid Recovery Agent software.

For more information about the Rapid Recovery Agent installer and about installing the Agent software on Windows machines, see Installing the Rapid Recovery Agent software on Windows machines. For information about installing the Agent software on Linux machines, see About installing the Agent software on Linux machines.

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

Steps

1. Download the Rapid Recovery Core installer file from the Dell Data Protection | 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 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, click **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 **Port Number** text field, enter a port number to use for communication between the Rapid Recovery Core and its protected machines.

  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.

- 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 diagnosis and user information to Dell Inc.** to send diagnostic and user information to Dell. 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 following options:

Table 9. Update options for Rapid Recovery Core

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 an update is available, the updated version is installed after the nightly jobs have completed. 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, Dell 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 *Dell Data Protection | 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.

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

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 *Dell Data Protection | Rapid Recovery User Guide*.

For information on configuring the Rapid Recovery Core and protecting and managing your data, see the *Dell Data Protection | 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 6.0.2, 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.

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.

NOTE: You can also protect VMware vCenter/ESX(i) 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, Dell 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 *Dell Data Protection | 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 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.

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.

Related Links

Obtaining the Rapid Recovery Agent software
Installing the Rapid Recovery Agent software on Windows machines
Installing the Agent software on Windows Server Core Edition machines
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.Installing the Rapid Recovery Core
- **Download from the License Portal.** If you have already registered your software in the Dell Data Protection | Rapid Recovery License Portal, you can log into the License Portal at https://licenseportal.com and download the software to the machine you want to protect.

  For more information about the Dell Data Protection | Rapid Recovery License Portal, including obtaining a license key or registering and creating a License Portal account, see the Dell Data Protection | 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 Dell Data Protection | 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 Protecting Multiple Machines in the Dell Data Protection | 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 to Multiple Machines in the Dell Data Protection | Rapid Recovery User Guide.

Installing the Rapid Recovery Agent software on Windows machines

About this task

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.

Steps

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 could 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 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, click **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; for example, CRT 2013 (x64) ENU (distributable code for Microsoft Visual Studio®), or Microsoft System CLR Types for SQL Server 2008 R2 (x64). 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.

  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 Dell Inc.** to send diagnostic and usage information to Dell. 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.

Related Links

Installing the Rapid Recovery Agent software
Installing the Agent software on Windows Server Core Edition machines
Rapid Recovery system requirements

Installing the Agent software on Windows Server Core Edition machines

About this task

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

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`.

Steps

1. Download the Rapid Recovery Agent installer file from the Dell Data Protection | 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 Agent software on Linux machines that you want to protect, use the following guidance. 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, restart the machine. Restarting ensures that the proper kernel driver version is used to protect your machine.

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

- One set of instructions applies to installations of Agent on a Linux machine with current access to the Internet. This is referred to as online installation. Instead of using shell scripts, package managers are used to install or remove the Rapid Recovery software from a repository referenced on the local Linux machine.

  NOTE: The repository is used for staging of files for the relevant package managers. This repository is not related to the Rapid Recovery repository.
- If installing Agent on a Linux machine with no access to the Internet (such as an air-gapped or secured standalone machine), this is referred to as offline installation. For this process, you must first download an installation package from a Linux machine with Internet access, and then move those installation files to the secured computer for installation.

Because the various supported Linux distributions use different package managers for online installation, 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

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 Dell Rapid Recovery installation files.

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 11. Command to show package manager repository configuration

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 completely removed from a Linux machine before installing the Rapid Recovery Agent version and protecting the Linux machine using the Rapid Recovery Core. This is true for online or 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.

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)
- Determine the relevant package manager for your Linux distribution
- Follow the procedure for installing Rapid Recovery Agent on the Linux machine, including configuring the software repository (steps 1 through 4 of the installation procedure)
- Run the configuration utility to set port, 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

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 Dell Data Protection | Rapid Recovery License Portal at https://licenseportal.com. For more information, see the *Dell Data Protection | Rapid Recovery License PortalUser 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 *Dell Data Protection | 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 and Ubuntu:
  - The rapidrecovery-agent requires:
    ```
    dkms, gcc, make, linux-headers-‘uname-r‘
                    libc6 (>=2.7-18), libblkid1, libpam0g, libpcre3
    ```
  - The rapidrecovery-mono requires:
    ```
    libc6 (>=2.7-18)
    ```
- For Red Hat Enterprise Linux, CentOS, and Oracle Linux:
  - The nbd-dkms requires
    ```
    dkms, gcc, make, kernel-headers-‘uname-r‘ kernel-devel-‘uname-r‘
    ```
  - The rapidrecovery-agent requires:
    ```
    dkms, gcc, make, kernel-headers-‘uname-r‘ kernel-devel-‘uname-r‘,
                    nbd-dkms, libblkid, pam, pcre
    ```
  - The rapidrecovery-mono requires:
    ```
    glibc >=2.11
    ```
- For SUSE Linux Enterprise Server:
  - The nbd-dkms requires:
    ```
    dkms, gcc, make, kernel-syms
    ```
  - The rapidrecovery-agent requires:
    ```
    dkms, kernel-syms, gcc, make, libblkid1, pam, pcre
    ```
  - The rapidrecovery-mono requires:
    ```
    glibc >= 2.11
    ```

Linux scripting information

Information about Bourne Shell scripting supporting Linux protected machines is included in the *Dell Data Protection | Rapid Recovery User Guide*. See the appendix "Extending Rapid Recovery jobs using scripting," including the topic "Using Bourne Shell scripting in Rapid Recovery."

Installing the Rapid Recovery Agent software on Debian or Ubuntu

About this task

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.

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.

Steps

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 *Dell Data Protection | Rapid Recovery License Portal User Guide*.
4. To establish a persistent connection between your Linux machine and the remote Dell 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-6.0.2.999.deb in the directory **/home/rapidrecovery/**, type the following command, and then press **Enter**:

   ```
   dpkg -i rapidrecovery-repo-6.0.2.999.deb
   ```

   Any missing packages or files required by the Agent will be downloaded from the remote 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

About this task

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.

Steps

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 *Dell Data Protection | Rapid Recovery License Portal User Guide*.
4. To establish a persistent connection between your Linux machine and the remote Dell 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-6.0.2.999.rpm in the directory **/home/rapidrecovery/**, type the following command, and then press **Enter**:

   ```
   rpm -ivh rapidrecovery-repo-6.0.2.999.rpm
   ```

   Any missing packages or files required by the Agent will be downloaded from the remote 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**:

   ```
   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

About this task

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.

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.

Steps

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 *Dell Data Protection | Rapid Recovery License Portal User Guide*.
4. To establish a persistent connection between your Linux machine and the remote Dell 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-6.0.2.999.rpm in the directory **/home/rapidrecovery/**, type the following command, and then press **Enter**:

   ```
   rpm -ivh rapidrecovery-repo-6.0.2.999.rpm
   ```

   Any missing packages or files required by the Agent will be downloaded from the remote 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 zypper 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 Agent software on offline Linux machines

Prerequisites

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.

About this task

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.

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

Steps

1. From a Linux machine with access to the Internet, open a terminal window and type the following command:

   ```
   wget http://s3.amazonaws.com/repolinux/6.0.2/packages-downloader.sh
   ```

   The shell script downloads to your current directory.
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.

   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.

Next steps

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

About this task

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.

Steps

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 install into all supported kernels, or 'q' to quit.
```

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

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

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

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

About this task

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.

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 *Dell Data Protection | 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 *Dell Data Protection | Rapid Recovery User Guide*..

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

Steps

1 Download the Rapid Recovery Central Management Console installer file from the Dell Data Protection | Rapid Recovery License Portal; for example:

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

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 need to 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.

  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.

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 *Dell Data Protection | 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 Dell Data Protection | Rapid Recovery License Portal on a weekly basis.

- 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.

Dell 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 *Dell Data Protection | 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

About this task

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.

Steps

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**.

  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 Links

Uninstalling the Rapid Recovery Agent software from a Windows machine
Uninstalling the Rapid Recovery Agent software from a Linux machine

Uninstalling the Rapid Recovery Agent software from a Windows machine

About this task

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

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.

Steps

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.

     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

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 Dell Rapid Recovery installation files.

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

Package Manager	Command to list configured repositories
yum	yum replolist
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:

Backing up and restoring the AppAssure agent ID

Prerequisites

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.

Steps

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 ~/values-backup.xml
   ```

   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/agentid/values.xml
   ```
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.

Next steps

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.

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

Uninstalling the Rapid Recovery Agent software from Debian and Ubuntu systems

Prerequisites

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 Dell Rapid Recovery installation files.

About this task

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.

Steps

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

Prerequisites

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 Dell Rapid Recovery installation files.

About this task

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.

Steps

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

Prerequisites

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 Dell Rapid Recovery installation files.

About this task

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.

Steps

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, Dell 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.

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 Links

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

Uninstalling the AppAssure Agent software on Ubuntu systems

About this task

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

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

Steps

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.

Next steps

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

About this task

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

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".

Steps

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.

Next steps

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 SUSE Linux Enterprise Server systems

About this task

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

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

Steps

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.

Next steps

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

About this task

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

Steps

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 RemoveOptions 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.

4

Upgrading to Rapid Recovery

This chapter 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 6.0.2.

This chapter 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 6.0.2.

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 *Dell Data Protection | Rapid Recovery Release Notes*. Release notes and other Rapid Recovery technical documents are available on the Dell documentation website at https://support.software.dell.com/rapid-recovery/release-notes-guides/.

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

- Dell 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. Dell recommends customers review their environments before upgrading and adjust accordingly. Dell 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 *Dell Data Protection | Rapid Recovery 6.0 Sizing Guide 3.0*.

Topics:

Dell Support policy

Dell Software policy is to support two previous releases of software products. As of Rapid Recovery release 6.0.2, Dell continues to support the full range of Rapid Recovery release 6.0.1 Core and Agent features, and AppAssure Core and Agent in release 5.4.3. If you want to take advantage of new features, upgrade to the latest release, Rapid Recovery release 6.0.2.

The following table provides a visual guide, by Agent version, of compatibility between AppAssure and Rapid Recovery Agents and Cores.

Table 17. Compatibility between AppAssure and Rapid Recovery Agents and Cores

Agent	AppAssure 5.4.1 Core	AppAssure 5.4.2 Core	AppAssure 5.4.3 Core	Rapid Recovery 6.0.1 Core	Rapid Recovery 6.0.2 Core
5.4.1 Agent	Supported	Supported	Supported	Not Supported	Not Supported
5.4.2 Agent	Not Supported	Supported	Supported	Supported	Not Supported
5.4.3 Agent	Not Supported	Not Supported	Supported	Supported	Supported
6.0.1 Agent	Not Supported	Not Supported	Not Supported	Supported	Supported
6.0.2 Agent	Not Supported	Not Supported	Not Supported	Not Supported	Supported

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 6.0.2, 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 6.0.1 or 6.0.2.
- Dell tests the compatibility of transfers between machines protected with AppAssure Agent 5.3.7 and Rapid Recovery Core release 6.0.1 and 6.0.2. For full supportability of any other functions, Dell suggests you upgrade the Agent software on your protected machines to AppAssure Agent release 5.4.3, or Rapid Recovery Agent release 6.0.1 or 6.0.2.
- 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 Dell Data Protection | 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 Dell Data Protection | 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 Dell Data Protection | 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). 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.

  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 6.0.2 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 release 6.0.1 was available in English only. If upgrading from a localized AppAssure Core 5.4.3, upgrading to release 6.0.2 supports uninterrupted use of a localized Core Console user interface. If upgrading from Rapid Recovery Core release 6.0.1, you can now change your locale to the desired language to view the Core Console in that language.

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 from Rapid Recovery 6.0.1

Upgrading from Rapid Recovery Core or Agent release 6.0.1 is fast and easy. Simply download the new installers from the license portal or the Core, and run them on any machine with Rapid Recovery Core or Agent release 6.0.1.

After installing Rapid Recovery Core release 6.0.2, if you want to view the Core Console in a supported language other than English, simply change the locale in the general Core setting. For more information, see the topic Configuring Core general settings in the *Dell Data Protection | Rapid Recovery User Guide*.

Upgrading 5.2x, 5.3.x, or 5.4.x to Rapid Recovery

Upgrading AppAssure Core or Rapid Recovery Core

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

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

If upgrading from AppAssure Core 5.4.3 to Rapid Recovery Core release 6.0.1 or 6.0.2, 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 a release 5.4.1 or 5.4.2 AppAssure Core, 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 6.0.1 or 6.0.2 installer for the Rapid Recovery Core or Agent component, respectively.

If upgrading from AppAssure Core 5.3x to Rapid Recovery Core, you must use a two-step process. First, upgrade to AppAssure release 5.4.3. Finally, upgrade to Rapid Recovery Core.

If upgrading from AppAssure Core 5.2x 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.

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.**

- If you choose not to install this version, and are using AppAssure release 5.3.6 or earlier, Dell Software recommends upgrading to Rapid Recovery 5.3.7 to take advantage of the latest fixes. For more information on Rapid Recovery 5.3.7, see the Rapid Recovery 5.3.7 Release Notes.

Upgrading AppAssure Agent or Rapid Recovery Agent

When upgrading the Agent software on protected Windows machines from Rapid Recovery Agent release 6.0.1 or AppAssure Agent release 5.4.3, 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 (in this case, Rapid Recovery Agent release 6.0.1) or the one prior (AppAssure Agent release 5.4.3). After upgrading to the intermediate version, you can then run the Rapid Recovery Agent release 6.0.2 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 to release 6.0.2, 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

About this task

This topic provides an overview for upgrading your AppAssure environment to Rapid Recovery release 6.0.1 or 6.0.2.

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

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 *Dell Data Protection | 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 6.0.2 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 installer is only supported from machines with one of the prior two releases installed (in this case, Rapid Recovery Core release 6.0.1 or 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.x Core from a version of AppAssure Core older than two releases, you need to use a two-step or three-step upgrade process, as detailed in the topic Upgrading 5.2x, 5.3.x, or 5.4.x to Rapid Recovery.

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 *Dell Data Protection | 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 Rapid Recovery release 6.0.1 or release 6.0.2 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 *Dell Data Protection | Rapid Recovery User Guide*.

9 Direct upgrade of the Rapid Recovery Agent software using the Agent installer is only supported from machines with one of the prior two releases installed (in this case, Rapid Recovery Agent release 6.0.1 or AppAssure Agent release 5.4.3). If using these releases, you can use the Agent installer program 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 releases, first upgrade to AppAssure Agent release 5.4.3, and then upgrade to Rapid Recovery Agent release 6.0.1 or 6.0.2, as applicable. For more information, see Upgrading 5.2x, 5.3.x, or 5.4.x to Rapid Recovery.

- 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 6.0.1) to a newer version of Agent (such as release 6.0.2). 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.

> 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:

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

2 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.

NOTE: You can also protect VMware vCenter/ESX(i) 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, Dell 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 *Dell Data Protection | 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. Dell supports compatibility with two prior versions of our software. In the case of Rapid Recovery release 6.0.2, 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 6.0.2 installer, as applicable.

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 6.0.2 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.

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.

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

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 Dell Rapid Recovery installation files.

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

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

About this task

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 8, or on Ubuntu 12.04, 13.04 or 14.04.

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.

Steps

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

About this task

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.

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.

Steps

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 *Dell Data Protection | 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

About this task

Rapid Recovery Agent software

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: 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.

Steps

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

About this task

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 Dell 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 Dell Software sales representative or fill out the contact form at https://software.dell.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.

Steps

1. Register for an account at the Dell Software License Portal at http://license.appassure.com. Ensure that you register using the email address that is on file with your Dell 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.

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 Dell

Dell listens to customers and delivers worldwide innovative technology, business solutions, and services they trust and value. For more information, visit http://software.dell.com.

Contacting Dell

For sales or other inquiries, visit http://software.dell.com/company/contact-us.aspx or call + 1-949-754-8000.

Technical support resources

Technical support is available to customers who have purchased Dell software with a valid maintenance contract and to customers who have trial versions. To access the Support Portal, go to https://support.software.dell.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. In addition, the Support Portal provides direct access to product support engineers through an online Service Request system.

The Support Portal enables you to:

- Create, update, and manage Service Requests (cases).
- View Knowledge Base articles.
- Obtain product notifications.
- Download software. For trial software, go to http://software.dell.com/trials.
- Engage in community discussions.