Rev. A00

Dell Data Protection | Rapid Recovery 6.1.1 Release Notes

February 2017

These release notes provide information about the Dell Data Protection | Rapid Recovery release, build 6.1.1.137.

These release notes specifically address the Rapid Recovery 6.1.1 maintenance release. For specific information about the Rapid Recovery 6.1 parent release, see Rapid Recovery 6.1 Release Notes.

Topics:

About Dell Data Protection | Rapid Recovery 6.1.1

Dell Data Protection | Rapid Recovery software delivers fast backups with verified recovery for your VMs and physical servers, on-premises or remote. Dell™ Rapid Recovery is software built for IT professionals who need a powerful, affordable, and easy-to-use backup, replication, and recovery solution that provides protection for servers and business-critical applications like Microsoft® SQL Server®, Microsoft Exchange, and Microsoft SharePoint®. Using Rapid Recovery, you can continuously back up and protect all your critical data and applications from a single web-based management console.

Rapid Recovery release 6.1.1 is a minor release that includes enhancements and defect fixes (described in Resolved issues). For information on the new features, enhanced functionality, or changes for other components that were introduced in release 6.1, see Rapid Recovery 6.1 Release Notes.

Previously named AppAssure, Rapid Recovery has been rebranded in release 6 to reflect the next step in its evolution. The new name applies to Rapid Recovery Core, as well as the Rapid Recovery Agent software you can install on machines to protect their data.

Some other components were rebranded for consistency. For more information on rebranding, see the Enhancements topic in **Rapid Recovery 6.0.1 Release Notes**.

Repository upgrade advisory

Upgrading the Core software to release 6.1.x from any earlier version (for example, Rapid Recovery 6.0x, AppAssure 5.x) changes the schema in your repository. The updates let you use new features in the latest release, including the ability to protect guests on a Microsoft Hyper-V host without installing Rapid Recovery Agent on each guest.

Anytime you change the structure of your repository through an upgrade, you cannot downgrade the version of Core. Should you determine in the future that you want to use an earlier version of Core after upgrade to this release, you will need to archive the data in your repository. You could then re-import the information manually, which can be a substantial effort.

System requirements documentation advisory

For each software release, we review and update the system requirements for Rapid Recovery software and components. If using localized versions of product documentation, always refer to the release notes for the most current system requirements. Release notes are sometimes updated and re-issued in a release cycle.

Enhancements

Rapid Recovery release 6.1.1 is a minor release, with enhanced functionality and defect fixes.

NOTE: To see new features, enhancements, deprecations, and other changes in Rapid Recovery release 6.1, see **Rapid Recovery 6.1 Release Notes**.

The following is a list of enhancements implemented in Rapid Recovery release 6.1.1.

Limited support for vSphere/ESXi 6.5

Limited support for vSphere/ESXi 6.5

Beginning with release 6.1, Rapid Recovery provides limited support for vSphere/ESXi 6.5. Unless otherwise indicated, functions supported for ESXi 6 now work for ESXi 6.5. Read the following details carefully for a full understanding.

The following functions are supported:

- Protection of virtual machines on ESXi 6.5
- Replication of recovery points from ESXi 6.5
- Virtual export of recovery points to ESXi 6.5

The following limitations exist:

- You cannot export a virtual machine to vCenter/ESXi 6.5 if the source machine uses the Secure Boot option.
- When protecting virtual machines agentlessly on ESXi 6.5, you cannot protect encrypted VMs, which require VDDK 6.5. This limitation does not apply if the VM has the Agent software installed. Support for

this feature is expected in Rapid Recovery release 7.0.0 and later, which includes an upgrade to VDDK 6.5.

- When protecting virtual machines agentlessly on ESXi 6.5, transfer does not work if the transport mode is set to SAN (storage area network). The SAN transport mode option is only available for agentless protection.

In general, new features specific to ESXi 6.5 may not function and are not supported until the VDDK is updated and tested in a future release of Rapid Recovery.

Resolved issues

Issues resolved in this release are listed below.

Table 1. Core and Windows resolved issues

Resolved Issue	Issue ID	Functional Area
After upgrading Core from release 6.0.2 to 6.1.x, the metadata for a protected machine was not available. When viewing the Summary page for the protected machine, the error "Unable to get details for '[AgentName]' appears. In logs, error "Object reference not set to an instance of an object" appeared.	100989	Agent summary information
Cancel feature on the Events page of Core Console resulted in failure of the cancel job function, displaying error message: "Invalid method. Parameter name: DELETE."	101172	Cancel job
This defect affected Rapid Recovery Core on an appropriate Windows server set for localization in simplified Chinese. When attempting to protect a Hyper-V server agentlessly using the Protect Multiple Machines wizard, a System.FormatException error appeared preventing users from installing Agent on the Hyper-V server.	101207	Agentless protection
Rollup of recovery points for extended volumes failed with error message: "The offset is invalid."	101230	Rollup
Using Rapid Recovery version 6.1.0, virtual export of recovery points to ESXi 6.5 failed. When using the virtual export wizard, the export process failed, displaying the error "The value 'xx' for 'CPU count' is invalid. It must be in the range from '1' to '0'."	101245	Virtual export to ESXi
When using DL appliances, ESXi exports eventually failed in some cases, displaying error: System.OutOfMemoryException.	101246	Virtual export to ESXi

Table 2. DocRetriever resolved issues

Resolved issue	Issue ID	Functional area
DocRetriever failed to connect to the SharePoint front-end server with the error "The socket connection was aborted" when the DocRetriever Console was installed on a machine running Windows Server 2012 R2.	100870	Transfers

Known issues

The following is a list of issues, including those issues attributed to third-party products, known to exist at the time of release.

> **NOTE:** Rapid Recovery has migrated to a new issue tracking tool. When applicable, previous issue ID numbers are found in the Old issue ID column. Numbers associated with the new tracking tool are found in the New issue ID column.

Table 3. Central Management Console known issue

Known Issue	Old Issue ID	New Issue ID	Functional Area
Users are unable to sign in to the Central Management Console on environments with a specific configuration of the domain controller, groups, and accounts. **Workaround:** Contact Support and request the custom binary that addresses this issue.	N/A	101227	Authentication

Table 4. Core and Windows known issues

Known Issue	Old Issue ID	New Issue ID	Functional Area
Virtual export fails with the error "No physical extents have been found for cluster offset '19626746' cluster length '520.' Extent disk #'1' LCL '19627264' LCF '0' PSF '264192'" after specific steps. **Workaround:** Take a new base image, and then attempt the export again.	35626	100646	VM export
There is incorrect validation for the "Maximum connection pooling size" and "Minimum connection pooling size" fields for the connection to MongoDB. **Workaround:** Since validation on these fields is not functioning, take care to specify the correct values for the "Maximum connection pooling size" and "Minimum connection pooling size" fields.	35607	100627	GUI
In the Settings page of the Core Console, validation in the client timeout fields sometimes work incorrectly, showing the error "Uncaught Error." **Workaround:** Refresh the page.	35572	100592	GUI
In the Korean translation of the user interface, the Pause button has the incorrect translation of 일지 중지. **Workaround:** The Korean translation of the Pause button should read as 일시 중지.	35557	100577	Localization
On the Schedule page of the Archive wizard, the tooltip text is wrong in all translations.	35556	100576	Localization

Known Issue	Old Issue ID	New Issue ID	Functional Area
Workaround: This is a cosmetic issue that does not require a workaround.			
In the Protect Machine wizards, the "Encrypt data using Core-based encryption with an existing key" option is highlighted when it is not selected. **Workaround:** This is a cosmetic issue that does not require a workaround.	35554	100574	GUI
Volumes are not available after a recovery point from an attached archive created from an agentless Windows Server 2008 R2 protected machine is mounted as Writable. **Workaround:** Import the archive to the repository, and then mount the recovery point as Writable.	35542	100562	Agentless protection
The email notification template reverts to the default after the Core service restarts. **Workaround:** Contact Support and request the custom binary that addresses this issue.	35483	100503	GUI
Replication to a second target Core does not start if volumes are missing from the source Core. **Workaround:** On the Summary page for the affected protected machine, remove the missing volume from protection.	35358	100378	Replication
On a specific environment, the GPT volume on an agentlessly protected virtual machine cannot be opened from a mount point mounted in Read-only mode. **Workaround:** Create another mount type, or mount the volume using the Local Mount Utility on a machine running Windows Server 2012.	35100	100129	Agentless protection
A base image is taken whenever the NTFS Boot Sector is changed. **Workaround:** Contact Support and request the custom binary that addresses this issue.	34981	100011	Filter driver
Unexpected base images are generated for the ESXi virtual machines that have snapshots with quiescing enabled. **Workaround:** Disable quiescing.	34916	99946	Transfers
When viewing the Core Console in the Dashboard view in languages other than English, the word "Transfer" is not translated when searching for all transfer events using the Transfer Job per Machine widget. **Workaround:** This is a cosmetic issue that does not require a workaround.	34774	99804	Localization
Export rate is slow for recovery points from repositories that have high fragmentation. **Workaround:** Option 1: Pause machine protection, archive all recovery points for that machine, remove the repository, create a new	34758	99788	Repository

Known Issue	Old Issue ID	New Issue ID	Functional Area
repository, assign the protected machine to the new repository, import the archive to the new repository, and then resume protection. Option 2: Contact Support and request the custom binary that addresses this issue.			
Performance on the Virtual Standby page is slow when there are several export jobs in the queue or in progress. **Workaround:** Decrease the number of concurrent export jobs allowed.	34434	99466	Performance
On the Events page and the Delete Recovery Points Range window, the date and time pickers work incorrectly. **Workaround:** Refresh the page.	34347	99380	GUI
Information about allocated space for some volumes is unavailable. A warning message appears on the Summary page for a protected machine if it is a virtual machine located on an NFS datastore. **Workaround:** There is no workaround at this time. There are issues with gathering metadata on the NFS.	33551	98697	GUI
There is no ability to inject drivers from the Rapid Recovery Universal Recovery Console (URC) after restoring data for older operating systems (such as Windows Server 2003, Windows Server 2008, Windows Vista) to a successfully boot-restored machine. **Workaround:** Restore on hardware with included driver support. Use x86 boot CD from 5.4.3.106 build. Install the OS, install the Rapid Recovery Agent software, then restore the volumes.[1]	33359	98524	URC
Replication rate becomes extremely slow if you start a virtual export job while replication job is running. **Workaround:** Configure jobs so they do not run in parallel.	33230	70064	Replication
Disk metadata size skews progress tracking during archive. For example, if there are many databases on a volume, the progress bar stays at 1% for too long, then speeds up. **Workaround:** There is no workaround at this time.	32044	97307	Archive
When the target network storage volume runs out of space, if more than one archive job is in progress, then all running archive jobs fail with error: "There is not enough space on the disk." **Workaround:** Create different schedules for running each archive so that the archives do not run simultaneously in the network share.	31827	97116	Archive
WinXPx86 machine is not bootable after virtual export. Issue relates to controller drivers for SCSI and IDE controllers not present in the exported VM. **Workaround:** There is no workaround at this time.	31705	97005	VM export
ESXi agentless restore or virtual export using SAN transport mode fails with the error, "One of the parameters was invalid."	29508	95042	VMware agentless

Known Issue	Old Issue ID	New Issue ID	Functional Area
Workaround: Use Network Transport mode for rollback.			
ESXi virtual export with auto disk mapping fails with unclear error. An error message for ESXi virtual export with auto disk mapping does not clearly describe the issue. **Workaround:** Use manual disk mapping.	27309	93141	ESXi export

[1]Investigation concluded that this issue describes functionality of the URC as it was designed. The workaround is expected to be included in future editions of the **Rapid Recovery User Guide** and the issue removed from future versions of the release notes.

Table 5. DocRetriever **known issues**

Known Issue	Old Issue ID	New Issue ID	Functional Area
The error "Cannot find the original destination..." appears after trying to perform an in-place restore of a site from the "Farm" backup. **Workaround:** Perform an out-of-place restore and manually specify the appropriate restore location.	35614	100634	Restoring

Table 6. Documentation **known issues**

Known Issue	Old Issue ID	New Issue ID	Functional Area
When performing virtual export to Azure, the Rapid Recovery Core uses Azure storage and containers created using the Classic management model. Containers created in Azure using the newer Resource Manager deployment model are not recognized by the Core. The **Rapid Recovery User Guide** procedure "Creating a container in an Azure storage account" for releases 6.1 and 6.1.1 does not specify that the Classic management model is required. Future versions of documentation are to be modified accordingly. **Workaround:** Use the Classic management model to create storage accounts and containers for virtual export. If you already have a storage account created using the Classic model, any new containers created for it will automatically use the correct model (Classic).	N/A	101837	Azure export
Containers created in Azure are used to store virtual machines exported from the Rapid Recovery Core to your associated Azure account. If you create a specific container prior to performing virtual export, the Virtual Machine Export Wizard typically displays that container as one of the choices in the Container name field of the Destination window. If you create the container by typing a valid container name into the Container name field as part of the process of defining a virtual export, the container is not immediately visible in the wizard. This behavior is not reflected in the appropriate procedures in the **Rapid Recovery User Guide**. **Workaround:** If you create a container from the Virtual Machine Export Wizard, that container is not accessible to the API used to connect to	N/A	101853	Azure export

Known Issue	Old Issue ID	New Issue ID	Functional Area
your Azure account. Simply close the wizard, and launch it again, and you should then be able to access the newly created container. Future versions of documentation are to be modified accordingly.			
The **Rapid Recovery User Guide** procedure "Setting up continual export to Azure" for releases 6.1 and 6.1.1 contains unnecessary steps. Future versions of documentation are to be modified accordingly. **Workaround:** When following this procedure, disregard Steps 4 and 5. Since you are defining ongoing continual export, you are not prompted to select a recovery point. Likewise, there is no Summary page at the end of the wizard. On the Volumes page of the wizard, click Finish (instead of Next).	N/A	101858	Azure export
The **Rapid Recovery User Guide** procedure "Deploying a virtual machine in Azure" for releases 6.1 and 6.1.1 contains unnecessary steps. Future versions of documentation are to be modified accordingly. **Workaround:** When following this procedure, disregard Steps 4 through 8. The step currently numbered Step 9 should start with "On the Destination page...".	N/A	101859	Azure export

Table 7. Linux protection known issues

Known Issue	Old Issue ID	New Issue ID	Functional Area
TLS 1.2 is not compatible with the Linux® Agent. **Workaround:** There is no workaround at this time. Security protocols are determined by the version of Mono used in the Rapid Recovery Linux Agent software. The versions currently used are compatible only with SSL and TLS 1.	N/A	101279	Encryption
An exported Linux machine with an EFI partition is not bootable on VMware ESXi, because specific volumes are not mounted after the export of the Linux machine. **Workaround:** There is no workaround at this time.	35288	100311	ESXi export
Users who have 'safenet' encrypted file partitions are unable to protect Linux machines using the Rapid Recovery Agent. **Workaround:** Contact Support and request the custom binary that addresses this issue.	35226	100254	Protection
Red Hat® Enterprise Linux® (RHEL) protected machine is not bootable after VirtualBox export of ESXi Agentless machine. **Workaround:** There is no workaround at this time.	31277	96616	VirtualBox export
Agentlessly protected ESXi Ubuntu machine is not bootable after BMR. **Workaround:** Use the Rapid Recovery Agent on Ubuntu instead of using agentless protection.	31206	70052	VMware agentless

Rapid Recovery system requirements

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

Recommended network infrastructure

For running Rapid Recovery, Dell requires a minimum network infrastructure of 1 gigabit Ethernet (GbE) 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). For Windows systems, UEFI uses the Extensible Firmware Interface (EFI) system partitions that are handled as simple FAT32 volumes.

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

- **Windows:** Windows 8,Windows 8.1, Windows 10; Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016.
- **Linux:** All supported versions of Linux.

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

Support for dynamic and basic volumes

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

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

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

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

- **Protection:** In the case when a dynamic volume spans multiple disks, you must protect those disks together to maintain the integrity of the volume.
- **Virtual export:** You can export complex dynamic volumes such as striped, mirrored, spanned, or RAID volumes from an ESXi or Hyper-V host using agentless protection.

  However, the volumes are exported at the disk level, with no volume parsing. For example, if exporting a dynamic volume spanned across two disks, the export will include two distinct disk volumes.

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

- **Restoring data:** When restoring a dynamic volume that spans multiple disks, you must restore the dynamic disks with the original system volumes to preserve the disk types. If you restore only one disk, you will break the disk configuration.

Repository storage: Additionally, Rapid Recovery supports the creation of repositories on complex dynamic volumes (striped, mirrored, spanned, or RAID). The file system of the machine hosting the repository must be NTFS or ReFS.

Support for Cluster Shared Volumes

Rapid Recovery release 6.1 and later includes the Rapid Snap for Virtual feature. With the Rapid Recovery Agent installed on each node, you can protect and restore supported VMs hosted on Hyper-V cluster-shared volumes (CSVs) installed on Windows Server 2012 R2 and Windows Server 2016.

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

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

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

Table 8. Rapid Recovery **support for cluster-shared volumes**

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

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

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

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

Hypervisor support in Rapid Recovery

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

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

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

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

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

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

Virtual export hypervisor license requirements

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

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

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

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

Before installing Rapid Recovery release 6.1, ensure that your system meets the following minimum hardware and software requirements. For additional guidance for sizing your hardware, software, memory, storage, and network requirements, see knowledge base article 185962, "Sizing Rapid Recovery Deployments."

CAUTION: 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, Windows Server 2012 R2 Core, and Windows Server 2016 Core. Excluding Windows Server 2008 Core, these Core edition operating systems are supported for running the** Rapid Recovery **Agent software.**

NOTE: 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 6.1 operating system installation and compatibility matrix

Microsoft Windows operating systems

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

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

Table 9. Rapid Recovery **components and features compatible with Windows operating systems**

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

Windows OS	Core/ Central Management Console	Agent	Agentless	LMU	MR	DR	URC Restore	VM Export to Azure
Windows XP SP3	No	No	Yes	No	No	No	Yes[1]	No
Windows Vista™	No	No	Yes	No	No	No	Yes[1]	No
Windows Vista SP2	No	Yes	Yes	Yes	Yes	Yes	Yes[1]	No
Windows 7	No	No	Yes	No	No	No	Yes	Yes[2]
Windows 7 SP1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes[2]
Windows 8	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes[2]
Windows 8.1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes[2]
Windows 10	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes[2]
Windows Server 2003	No	No	Yes	No	No	No	Yes[1]	No
Windows Server 2008	No	No	Yes	No	No	No	Yes[1]	Yes[2]
Windows Server 2008 SP2	Yes	Yes	Yes	Yes	Yes	Yes	Yes[1]	Yes[2]
Windows Server 2008 R2	No	No	Yes	No	No	No	Yes	Yes[2]
Windows Server 2008 R2 SP1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes[2]
Windows Server 2012	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes[2]
Windows Server 2012 R2	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes[2]
Windows Server 2016	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Windows installation and support notes:

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

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

Linux operating systems

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

Table 10. Compatible Rapid Recovery components and features by Linux operating system

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

Windows OS	Core/ Central Management Console	Agent	Agentless
Linux OS or distribution	Agent	Agentless	Live DVD
Red Hat Enterprise Linux 6.3 - 6.8	Yes	Yes	Yes
Red Hat Enterprise Linux 7.0 - 7.2	Yes	Yes	Yes
CentOS™ Linux 6.3 - 6.8	Yes	Yes	Yes
CentOS Linux 7.0 - 7.2	Yes	Yes	Yes
Debian® Linux 7, 8	Yes	Yes	Yes
Oracle® Linux 6.3 - 6.8	Yes	Yes	Yes
Oracle Linux 7.0 - 7.2	Yes	Yes	Yes
Ubuntu Linux 12.04 LTS, 12.10	Yes	Yes	Yes
Ubuntu Linux 13.04, 13.10	Yes	Yes	Yes
Ubuntu Linux 14.04 LTS, 14.10	Yes[1]	Yes[1]	Yes[1]
Ubuntu Linux 15.04, 15.10	Yes[1]	Yes[1]	Yes[1]
Ubuntu Linux 16.04 LTS	Yes[1]	Yes[1]	Yes[1]
SUSE® Linux Enterprise Server (SLES®) 11 SP2 or later	Yes	Yes	Yes
SLES 12	Yes[1]	Yes[1]	Yes[1]

Linux installation and support notes:

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

Rapid Recovery Core and Central Management Console requirements

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

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

Table 11. Rapid Recovery **Core and Central Management Console requirements**

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

Requirement	Details
Operating system	The Rapid Recovery Core and Central Management Console require one of the following 64-bit Windows operating systems (OS). They do not run on 32-bit Windows systems or any Linux distribution. Rapid Recovery Core requires one of the following x64 Windows operating systems: • Microsoft Windows 7 SP1 • Microsoft Windows 8, 8.1* • Microsoft Windows 10 • Microsoft Windows Server 2008 SP2, 2008 R2 SP1 (except Core editions) • Microsoft Windows Server 2012, 2012 R2* (except Core editions) • Microsoft Windows Server 2016* (except Core editions) Windows operating systems require the .NET Framework 4.5.2 to be installed to run the Rapid Recovery Core service. Additionally, any OS marked with * requires the ASP .NET 4.5x role or feature. When installing or upgrading the Core, the installer checks for these components based on the OS of the Core server, and installs or activates them automatically if required. The Rapid Recovery Core supports all x64 editions of the Windows OS listed, unless otherwise indicated. The Rapid Recovery Core does not support Windows Server core editions. If any operating system listed specifies a service pack (for example, Windows 7 SP1), then the OS with the specified service pack is the minimum requirement. If an operating system is listed without a service pack (for example, Windows 8), then the base operating system is supported. Any subsequent SP for a listed OS is also supported, unless explicitly excluded. For optimal performance, it is recommended that you install the Rapid Recovery Core on more recent operating systems such as Windows 8.1 (or later) and Windows Server 2012 (or later).
Architecture	64-bit only
Memory	8GB RAM or more 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 12. Rapid Recovery **Agent software requirements**

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

Requirement	Details
Operating system	The Rapid Recovery Agent software supports 32-bit and 64-bit Windows and Linux operating systems, including the following: • Microsoft Windows Vista SP2 • Microsoft Windows 7 SP1 • Microsoft Windows 8, 8.1* • Microsoft Windows 10 • Microsoft Windows Server 2008 SP2, 2008 R2 SP1 (all editions except Windows Server 2008 Core) • Microsoft Windows Server 2012, 2012 R2* • Microsoft Windows Server 2016* • Red Hat Enterprise Linux (RHEL) 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 7.0, 7.1, 7.2 • CentOS Linux 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 7.0, 7.1, 7.2 • Oracle Linux 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 7.0, 7.1, 7.2 • Debian Linux 7, 8 • Ubuntu Linux 12.04 LTS, 12.10, 13.04, 13.10, 14.04 LTS, 14.10, 15.04, 15.10, 16.04 LTS • SUSE Linux Enterprise Server (SLES) 11 (SP2 and later), 12
	NOTE: Windows operating systems require the Microsoft .NET framework version 4.5.2 to be installed to run the Rapid Recovery Agent service. Operating systems listed above that are marked with * also require the ASP .NET 4.5.x role or feature. When installing or upgrading the Rapid Recovery Agent software, the installer checks for these components, and installs or activates them automatically if required. Additional operating systems are supported for agentless protection only. For more information, see Rapid Snap for Virtual agentless protection.

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 Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016. For Windows Server 2008 R2 Core only, you must have SP1 or later. Windows Server 2008 Core edition is not supported. The Rapid Recovery Agent software supports the Linux distributions included in this list. Most of the released kernel versions have been tested. File systems supported include ext2, ext3, ext4, and xfs. BTRFS is also supported (only on certain Linux operating systems with kernel version 4.2. or later). For more information, see the Rapid Recovery release 6.1 operating system installation and compatibility matrix. Agents installed on Microsoft Hyper-V Server 2012 operate in the Core edition mode of Windows Server 2012. **NOTE:** Native backup of cluster shared volumes is supported on Windows 2008 R2 (SP2 and later) protected machines only.
Architecture	32-bit or 64-bit
Memory	4GB or higher
Processor	Single processor or higher
Microsoft Exchange Server Support	Microsoft Exchange Server 2007 SP1 Rollup 5 or later , Exchange Server 2010, Exchange Server 2013, or Exchange Server 2016
Microsoft SQL Server Support	Microsoft SQL Server 2008 or higher
Microsoft SharePoint	Microsoft SharePoint 2007, 2010, 2013, 2016
Storage	Direct attached storage, storage area network or network attached storage
Network	1 gigabit Ethernet (GbE) minimum **NOTE:** 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 Rapid Recovery License Portal.

Table 13. Local Mount Utility software requirements

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

Requirement	Details
Operating system	The Rapid Recovery Local Mount Utility software supports 32-bit and 64-bit Windows operating systems, including the following: • Microsoft Windows Vista SP2 • Microsoft Windows 7 SP1 • Microsoft Windows 8, 8.1* • Microsoft Windows 10 • Microsoft Windows Server 2008 SP2, 2008 R2 SP1 (all editions except Windows Server 2008 Core and Windows Server 2008 R2 Core) • Microsoft Windows Server 2012, 2012 R2* • Microsoft Windows Server 2016*
	NOTE: Windows operating systems require the Microsoft .NET framework version 4.5.2 to be installed to run the Local Mount Utility service. Operating systems listed above that are marked with * also require the ASP .NET 4.5.x role or feature. When installing or upgrading the LMU, the installer checks for these components, and installs or activates them automatically if required. If any operating system listed specifies a service pack (for example, Windows 7 SP1), then the OS with the specified service pack is the minimum requirement. If an operating system is listed without a service pack (for example, Windows 8), then the base operating system is supported. Any subsequent SP for a listed OS is also supported, unless explicitly excluded. The LMU software supports Windows Server Core edition installations for Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016. Windows Server 2008 Core edition and Windows Server 2008 R2 Core edition are not supported.
Architecture	32-bit or 64-bit
Memory	4GB or higher
Processor	Single processor or higher
Network	1 gigabit Ethernet (GbE) minimum **NOTE:** 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 specific hypervisor platforms without installing the Rapid Recovery Agent on each guest machine.

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

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

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

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

Agentless support for other operating systems

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

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

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

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

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

VMware ESXi environments are compatible with some operating systems that 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 6.1 operating system installation and compatibility matrix. Any known limitations are included in these matrices, or as notes to the software

requirements tables for the Core or the Agent, respectively. If a defect precludes the use of specific features temporarily, this information is typically reported in the release notes for any specific release. 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 export feature of Rapid Recovery, you can perform a one-time virtual export, or define requirements for continual virtual export known as virtual standby. This process can be performed from any protected machine, physical or virtual. If a protected machine goes down, you can boot up the virtual machine to restore operations, and then perform recovery.

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

Table 14. Hypervisor requirements supporting virtual export

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

Requirement	Details
Virtual machine host	VMware • VMware Workstation 7.0, 8.0, 9.0, 10, 11, 12 • VMware vSphere on ESXi 5.0, 5.1, 5.5, 6.0, 6.5 **NOTE:** Dell recommends running on the most recent supported VMware version. Future major releases of our software are not expected to support ESXi 5.0 and 5.1. **NOTE:** Secure Boot is a new ESXi 6.5 feature. Rapid Recovery support for this feature is planned for the near future. At this time, Rapid Recovery does not support virtual export to vCenter/ESXi 6.5 if the source machine uses the Secure Boot option. Microsoft Hyper-V

Requirement	Details

	NOTE: For virtual export to any Hyper-V host, .NET 4.5.2 and .NET 2.0 are required on the Hyper-V host.
	• First generation
	  ◦ Hyper-V running on Microsoft Server versions 2008 SP2, 2008 R2 SP1, 2012, 2012 R2, 2016
	  ◦ Hyper-V running on Microsoft Windows 8, 8.1 with Hyper-V, Windows 10
	• Second generation
	  ◦ Hyper-V running on Microsoft Server 2012 R2, 2016
	  ◦ Hyper-V running on Microsoft Windows 8.1, Windows 10
	NOTE: Only protected machines with the following Unified Extensible Firmware Interface (UEFI) operating systems support virtual export to Hyper-V second-generation hosts:
	• Windows 8 (UEFI)
	• Windows 8.1 (UEFI)
	• Windows Server 2012 (UEFI)
	• Windows Server 2012 R2 (UEFI)
	• Windows Server 2016 (UEFI)
	NOTE: Hyper-V export to second-generation VM can fail if the Hyper-V host does not have enough RAM allocated to perform the export.
	Oracle VirtualBox
	• VirtualBox 4.2.18 and higher

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

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

Agentless protection is supported as described in the following table.

Table 15. Hypervisor requirements supporting agentless or host-based protection

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

Requirement	Details
Virtual machine host	VMware • VMware vSphere on ESXi 5.0 (build 623860 or later), 5.1, 5.5, 6.0, 6.5. • You should also install the latest VMware Tools on each guest. **NOTE:** The following limitations apply to agentless protection using vSphere/ESXi version 6.5: • Secure Boot is a new ESXi 6.5 feature. Rapid Recovery support for this feature is planned for the near future. At this time, Rapid Recovery does not support virtual export to vCenter/ESXi 6.5 if the source machine uses the Secure Boot option. • ESXi 6.5 introduced support for encrypted VMs. However, that feature requires Virtual Disk Development Kit (VDDK) version 6.5. Support for VDDK 6.5 for agentless protection is planned for Rapid Recovery version 7.0.0 and later. Until that change, agentless protection of encrypted VMs in ESXi version 6.5 or higher by Rapid Recovery is not supported. • Transfer for VMs agentlessly protected on ESXi 6.5 does not work if the transport mode is set to SAN (storage area network). **NOTE:** Dell strongly recommends running on the most recent supported VMware version. Future major releases of our software are not expected to support ESXi 5.0 and 5.1. Microsoft Hyper-V • Windows Server 2012 R2 • Windows Server 2016 • Windows 8 x64 • Windows 8.1 x64 • Windows 10 x64
Operating system	For volume-level protection, volumes on guest VMs must have GPT or MBR partition tables. If other partition tables are found, protection occurs at the disk level, not at the volume level.
Storage	The storage reserved on the host must be equal to or larger than the storage in the guest VMs.
Architecture	32-bit or 64-bit

DVM repository requirements

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

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

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**.

Product licensing

To use and manage any version of Rapid Recovery, AppAssure, or Dell DL series backup and recovery appliance software, you need two items:

- **An account on the Rapid Recovery License Portal**.

  License portal accounts are free. If you are a new user, register at https://licenseportal.com. When you register, use the email address that is on file with your Dell sales representative. If upgrading from a trial version, use the email address associated with the trial version. If you need to use a different email address, contact your Dell sales representative for assistance.

  > **NOTE:** This license portal was recently rebranded. If you previously registered a license portal account to use with AppAssure or Rapid Recovery, then use that account information. Previous license portal users do not need to register a new account for Rapid Recovery.

For more details about the license portal, please see the **Dell Data Protection | Rapid Recovery License Portal User Guide** on our documentation website.

- **A software license.** Use of Rapid Recovery requires a license. You can use a trial license, which has a limited lifetime; or you can use a long-term (non-trial) license. After a trial license expires, the Rapid Recovery Core stops taking snapshots until you obtain and register a valid long-term license.

  If you registered for a trial version of Rapid Recovery, the installer is configured with a trial license which you can use immediately. This temporary license is valid for 14 days, and can be extended one time by the group administrator to a 28-day license.
  If you purchased a DL backup and recovery appliance, your appliance is configured with a 30-day temporary license that is activated automatically the first time you start the Core on the appliance.
  After you purchase software or a DL appliance, you receive by email a long-term (non-trial) license file or license number. If specified on the sales order, the license is sent to the end user email address. Otherwise, the long-term license is sent to the contact email address on the sales order.

To enable a trial software license:

When you register for a trial version, a trial license is written into the Rapid Recovery Core software installer. Simply log in to your license portal account and download the Rapid Recovery Core software. Carefully review the Rapid Recovery system requirements, and install a Rapid Recovery Core. You can begin protecting machines and backing up immediately.

To enable a purchased commercial software license (without a trial license):

If you purchased a software license and did not start with a trial license, then you are prompted for the license from the Core Console after you install the Rapid Recovery Core. Enter the license number, or browse and locate the license file provided to you by email in your sales order. For more information, see the topic Updating or changing a license in the **Dell Data Protection | Rapid Recovery User Guide**.

To enable a trial DL appliance license:

Each Dell DL series appliance contains a 30-day license that is activated automatically the first time you start the Core on the appliance.

To upgrade a trial license:

For uninterrupted backups, upgrade to a long-term license before the trial period expires. Once a trial license expires, the Rapid Recovery Core stops taking snapshots. To resume backups interrupted by the lack of a license, obtain a long-term license and enter the license information into the Core Console.

If a Core does not contact the license portal for 20 days after the grace period, it will be removed from the license pool automatically. If the Core subsequently connects to the license portal, it will be restored automatically on the license portal.

To request a license upgrade, contact your sales representative by completing the Contact Sales web form at https://www.quest.com/register/95291/. Once you have upgraded or purchased your long-term Rapid Recovery license through your Sales representative, you receive an email that includes your new license key or file. Enter this license information in the Core Console. For more information, see the topic Updating or changing a license in the **Dell Data Protection | Rapid Recovery User Guide**.

To add a license to a DL series backup and recovery appliance, see the topic Adding a license in the **Dell Data Protection | Rapid Recovery User Guide**.

Getting started with Rapid Recovery

The following topics provide information you can use to begin protecting your data with Rapid Recovery.

Rapid Recovery Core and Agent compatibility

The following table provides a visual guide of the interoperability between Core and Agent software versions. This table lists versions tested for release 6.1.1.

Table 16. Tested interoperability between Core and Agent versions

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

	AppAssure **5.4.3 Core**	Rapid Recovery **6.0.2 Core**	Rapid Recovery **6.1.0 Core**	Rapid Recovery **6.1.1 Core**
AppAssure 5.4.3 Agent[1]	Interoperability tested, fully compatible	Interoperability tested, fully compatible	Interoperability tested, fully compatible	Interoperability tested, fully compatible[2, 3]
Rapid Recovery 6.0.2 Agent	Not compatible	Interoperability tested, fully compatible	Interoperability tested, fully compatible	Interoperability tested, fully compatible[3]
Rapid Recovery 6.1.0 Agent	Not compatible	Not compatible	Interoperability tested, fully compatible	Interoperability tested, fully compatible[3]
Rapid Recovery 6.1.1 Agent	Not compatible	Not compatible	Not compatible	Interoperability tested, fully compatible

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

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

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

The matrix shows releases that have been fully tested with this release, and represent fully supported releases, plus the most recent release (6.1.0). Other software versions, in limited support status, are also expected to work.

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

Upgrade and installation instructions

Dell recommends users carefully read and understand the **Dell Data Protection | Rapid Recovery Installation and Upgrade Guide** before installing or upgrading. Specifically, when upgrading, read all topics in the chapter Upgrading to Rapid Recovery. For new installations, read all topics in the chapter Installing Rapid Recovery.

Additionally, Dell requires users to carefully review the release notes for each release, and the Rapid Recovery system requirements for that release, prior to upgrading. This process helps to identify and preclude potential

issues. Since the release notes are updated last of all the product documents for each release, it is your best source for updated system requirements.

If upgrading from AppAssure Core release 5.4.3, or Rapid Recovery Core release 6.0.x or 6.1.x, then run the latest Core installer software on your Core server. If using replication, always upgrade the target Core before the source Core.

To protect machines using the Agent software, if upgrading from AppAssure Core release 5.4.3, or Rapid Recovery Core release 6.0.x or 6.1.x, , run the latest Rapid Recovery Agent installer on each machine you want to protect. For more information, see the subtopic Protection.

You can also use the Rapid Snap for Virtual feature to protect virtual machines on supported hypervisor platforms agentlessly. Important restrictions apply. For more information on benefits or restrictions for agentless protection, see the topic Understanding Rapid Snap for Virtual in the release 6.1 edition of the **Dell Data Protection | Rapid Recovery User Guide**.

Dell Software policy is to support two previous major/minor releases of software products. If you want to upgrade an older version, best practice is to first upgrade to the fully supported release (Rapid Recovery Core release 6.0.2), or the one prior (AppAssure Core release 5.4.3). You can then run the 6.1.1 installer for the appropriate Rapid Recovery software component.

NOTE: Release 6.0.1 did not include localization support. If running a localized AppAssure 5.4.3 Core in a language other than English, upgrade to Rapid Recovery Core release 6.0.2 or later.

For more information, see the **Dell Data Protection | Rapid Recovery Installation and Upgrade Guide**.

When upgrading a protected Linux machine from AppAssure Agent to Rapid Recovery Agent version 6.x, you must first uninstall AppAssure Agent. For more information and specific instructions, see the **Dell Data Protection | Rapid Recovery Installation and Upgrade Guide**.

To download the Rapid Recovery Core software, you must have an account registered on the license portal. Upon successful registration, you can then download the software, carefully review the Rapid Recovery system requirements, and install a Rapid Recovery Core.

Licensing

Trial versions of Rapid Recovery Core may include a temporary license key. A license key is required to perform uninterrupted backups, replication, or data restoration. For more information, see the following resources:

- Basic information about license keys is available in the Product licensing section of these release notes.
- For information about managing licenses from the Rapid Recovery Core, see the topic Managing licenses in the **Dell Data Protection | Rapid Recovery User Guide**.
- For complete details on licensing, see the **Dell Data Protection | Rapid Recovery License Portal User Guide**.

Protection

To protect any physical or virtual machine (except VMs on VMware vSphere), you must install the Rapid Recovery Agent software. You can download Rapid Recovery Agent from the license portal to install on each machine you want to protect. You can also deploy Agent to the machines you want to protect from a properly configured Rapid Recovery Core.

If using a VMware vSphere host for your Core and protected machines, in many cases, you have the option to protect your machines without installing Rapid Recovery Agent. If using agentless protection, some limitations apply (especially for SQL Server or Exchange servers). For more information about these limitations, see the topic Understanding agentless protection in the **Dell Data Protection | Rapid Recovery User Guide**.

Add your machines to protection on the Rapid Recovery Core by using the Protect Machine or Protect Multiple Machines wizard.

NOTE: Before protecting a cluster, you must first create a repository. For more information, see the topic Creating a DVM repository in the in the **Dell Data Protection | Rapid Recovery User Guide**. Although a repository is also required to protect a machine, you have the option to create a repository during the workflow for protecting a machine.

Additional resources

Additional information is available from the following:

- Technical documentation
- Videos and tutorials
- Knowledge base
- Technical support forum
- Training and certification
- Dell Data Protection | Rapid Recovery License Portal

Globalization

This section contains information about installing and operating this product in non-English configurations, such as those needed by customers outside of North America. This section does not replace the materials about supported platforms and configurations found elsewhere in the product documentation.

This release is Unicode-enabled and supports any character set. In this release, all product components should be configured to use the same or compatible character encodings and should be installed to use the same locale and regional options. This release is targeted to support operations in the following regions: North America, Western Europe and Latin America, Central and Eastern Europe, Far-East Asia, Japan. It supports bidirectional writing (Arabic and Hebrew). The release supports Complex Script (Central Asia – India, Thailand).

The release is localized to the following languages: Chinese (Simplified), French, German, Japanese, Korean, Portuguese (Brazil), Spanish.

This release has the following known capabilities or limitations:

- Rapid Recovery release 6.0.1 and later requires Microsoft .NET 4.5.2. AppAssure used an earlier .NET version. There is no downgrade option available. If you upgrade from AppAssure to Rapid Recovery and then subsequently decide to use a prior version of AppAssure, you must perform a new installation of AppAssure Core and Agent.
- Logs and KB articles for Rapid Recovery release 6.1 are in English only.

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.