Dell Data Protection | Rapid Recovery™ 6.0.2

Release Notes

2016 - 06

June 2016

These release notes provide information about the Dell Data Protection | Rapid Recovery™ release, build 6.0.2.144.

Topics:

About Dell Data Protection | Rapid Recovery 6.0.2

Dell Data Protection | Rapid Recovery software delivers fast backups with verified recovery for your VMs and physical servers, on-premise 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 6.0.2 is a minor release, with enhanced features. See Enhancements.

Previously named AppAssure, Rapid Recovery has been rebranded in release 6.0.x 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 have been rebranded for consistency. For more information on rebranding, see the Enhancements topic in *Rapid Recovery 6.0.1 Release Notes*.

Upgrade advisory for AppAssure Replication Target for Azure

For Rapid Recovery 6.0.x users that want to replicate on-premise Cores to the cloud, a new Azure VM is available. For more information, see the *Dell Data Protection | Rapid Recovery Replication Target for Microsoft Azure Setup Guide* available on the Dell Software website. There is an upgrade path for users of AppAssure Replication Target for Azure (release 5.4.3)

If you are using AppAssure Replication Target for Azure (release 5.4.3) and plan to upgrade your on-premise source Core, you can upgrade your target Core on Azure. See the updated *Setup Guide* for upgrade information.

⚠ CAUTION: **You must upgrade your target Core before upgrading your source Core. The target Core to which you replicate must be the same version or higher than the source Core, or your cloud replica will cease to replicate.**

Enhancements

Rapid Recovery 6.0.2 is a minor release, with enhanced features and functionality, and defect fixes.

The following is a list of enhancements implemented in Rapid Recovery release 6.0.2.

- Localization
- Adding Deferred Delete to nightly jobs
- Rapid Recovery Agent Debian 7 and 8 Support (Linux)
- Separating VDDK calls into the VMware Proxy Service
- Operating system support changes
- Documentation updates and changes

ⓘ NOTE: AppAssure 5.x users take note: Rapid Recovery release 6.0.1 was a major release. New features included agentless protection for VMware VMs on an ESXi™ host; autodiscovery of new VMware VMs; direct mount of archives; BMR from cloud archives; duplicate block reclamation; support for SNMP 1.0; and the introduction of a software development kit (SDK) for Rapid Recovery APIs.

Additionally, release 6.0.x brought many other enhancements from release 5.4.x, such as rebranding from AppAssure to Rapid Recovery. Other changes included UI enhancements; OS support changes for Windows and Linux agents; virtual export and virtual standby to Microsoft Hyper-V cluster-shared volumes (CSV) running Windows Server 2012 or Windows Server 2012 R2 machines; importing archives on a schedule; and more. For detailed information on these changes, see Rapid Recovery 6.0.1 Release Notes.

See also:

- Resolved issues

Localization

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

ⓘ NOTE: While the locale you can select from the Rapid Recovery Core Console is listed as Spanish (Spain), the localized content is actually a generalized international Spanish translation, and is not specific to Spain. This designation will be corrected in future localized versions.

Adding Deferred Delete to nightly jobs

Recovery point data are stored in Recovery Point File System (RPFS) files in the repository. When you manually specify the deletion of a recovery point, or when the Core enforces rollup to merge or delete a recovery point, the specified recovery points are marked for deletion. This action creates a "Deleting of Index RPFS File" job on the Core. The relevant recovery points are immediately removed from the Core Console user interface.

The deletion job is immediately queued and then starts running in the background, concurrent with other Core operations. Deletion of recovery points is a processor-intensive task that may take hours. This delay in the removal of marked recovery points is known as the *deferred delete* feature of Rapid Recovery Core. This feature was first introduced in AppAssure release 5.4.1.

In Core environments under heavy load (such as undersized Cores, or environments with slow network speeds or infrastructure) performance of transfer jobs can be slow when performed concurrently with deferred delete jobs.

As an enhancement in release 6.0.2, Core now includes a new Deferred Delete option in nightly jobs. This option controls a single parameter: the ability to configure a maximum execution time for deferred delete during nightly jobs. The new deferred delete nightly job option is disabled by default.

When this new option is enabled, then after other nightly jobs have completed, a "Deleting records previously flagged for deletion" job is given the highest priority on the Core. Any new jobs for transfer, replication, and so on are queued behind the deferred delete job. In this way, Core processing is dedicated to removing deferred delete jobs, which complete much more quickly since other jobs are not running. When all marked recovery points are deleted, or when the maximum execution time period specified has passed, nightly jobs are completed, and the Core resumes normal operations. Transfers and other operations resume, and deletion of any remaining marked recovery points continues as a background job.

The default period for the maximum execution time for deferred delete is four hours. You can customize this timeout threshold in hours and minutes, from a minimum of 5 minutes to a maximum of 23 hours and 59 minutes. The amount of time for dedicated deletions should be determined based on load on your Core and the number of recovery points that are typically in the queue to be deleted.

Dell recommends using the default setting for this option (disabled) unless you are encountering transfer performance issues related to queued recovery point deletions. If you enable this new option, Dell recommends reviewing your Core jobs to ensure most recovery points marked for deletion are removed from the repository within a one-week period. This approach helps to balance maximum transfer performance with maximum reclamation of repository space.

For more detailed information on deferred delete, see Dell Knowledge Base article 198715, Understanding Deferred Delete in Nightly Jobs.

Rapid Recovery Agent Debian 7 and 8 Support (Linux)

In addition to the Linux operating systems supported since Rapid Recovery release 6.0.1, the following Linux operating systems are now supported for Rapid Recovery Agent:

- Debian ® Linux 7, 8

ⓘ NOTE: These Linux distributions use the apt package manager.

For a full set of software requirements for Rapid Recovery Agent, including other supported Linux operating systems and distributions, see the topic Rapid Recovery Agent software requirements.

Separating VDDK calls into the VMware Proxy Service

Rapid Recovery release 6.0.2 includes improved integration with the VMware Virtual Disk Development Kit (VDDK) for creating and accessing VMware virtual disk storage. Rapid Recovery calls to the VDDK application program interfaces (APIs) have been separated into a VMware Proxy Service. As a result, if an API hangs (such as if a requested connection is temporarily unavailable), the process is terminated, and a new VDDK wrapper process is started.

This enhancement increases the likelihood that slow-responding or failed VMware API calls can be retried and likely performed. This affects setting or customizing the VMware proxy service port; changing timeout settings for the proxy; restarting the proxy service; and cleaning up snapshots when a repository is full.

Operating system support changes

The following Microsoft operating systems have recently reached end-of-life (EOL) and are no longer supported by Dell:

- Windows Server® 2003 extended support ended on July 14, 2015.
- Windows XP® extended support ended on April 8, 2014.

EOL applies to any service pack and any edition of the specified operating systems. When operating systems achieve the EOL phase, the software manufacturer stops supporting it. As a result, Dell does not support operating systems that have reached EOL.

If you protect machines in an AppAssure or Rapid Recovery Core that use an OS that has reached EOL, you do so at your own risk. If you experience problems recovering data from these machines, addressing these issues is outside the scope or responsibility of Dell Support.

In release 6.0.x, Microsoft Windows® 10 support includes the following exceptions:

- Virtual exports of Windows 10 protected machines to Oracle® VirtualBox are missing SCSI controller drivers.
- The Rapid Recovery Add-on for the Kaseya® Management Console is not currently supported on Windows 10 machines.

Detailed information is now available about the operating systems supported by Rapid Recovery. See the following resources:

- Rapid Recovery release 6.0.2 operating system installation and compatibility matrix
- Rapid Recovery Core and Central Management Console requirements
- Rapid Recovery Agent software requirements

Documentation updates and changes

Rapid Recovery Release 6.0.2 includes updates to the following product documentation.

- *Dell Data Protection | Rapid Recovery DocRetriever for SharePoint User Guide* has been completely updated. Content changes reflect the current UI and workflow for this product and some content has been reorganized. Content related to creating user accounts has been clarified. Images have been updated to reflect product rebranding.
- *Dell Data Protection | Rapid Recovery Mailbox Restore for Exchange User Guide* has been completely updated. It reflects the most recent changes made to the UI, particularly concerning restore procedures (which are no longer determined by Microsoft Exchange version). This document now includes the addition of the Eseutil.exe command line utility function. Graphics are updated, and minor updates are included to improve the appearance of tables in XML format.
- *Dell Data Protection | Rapid Recovery Third-Party Integration Guide* has been completely updated to reflect the most recent changes to the Add-on for Kaseya UI. It also includes the latest system requirements and Kaseya VSA compatibility. The document has been reorganized to improve workflow and navigation. Updates also reflect product rebranding, and includes minor updates to improve the appearance of tables in XML format.
- The *Dell Data Protection | Rapid Recovery User Guide* includes minor updates to improve the appearance of tables in XML format. Supported release versions have been updated.

Context-sensitive help is generated from this document, and is accessed from the Rapid Recovery Core. Some minor edits or additions that appeared in the *Dell Data Protection | Rapid Recovery User Guide* release 6.0.1 but not in help files have now been updated. Help files also include minor updates to improve the appearance of tables in XML format. Information about third-party components, previously included in release notes, is accessible in release 6.0.x in contact-sensitive help. In the Rapid Recovery Core console, from the **Help** menu, select **About**, and then click **Third-party contributions**.

- The *Dell Data Protection | Rapid Recovery Installation and Upgrade Guide* has been updated to include updated system requirements information (such as support of the Agent software on Debian Linux versions 7 and 8). Supported release versions have been updated. Installation procedures are updated to include localization steps. Minor updates are included to improve the appearance of tables in XML format.
- As always, the *Dell Data Protection | Rapid Recovery Release Notes* provides the latest information regarding product enhancements, system requirements, issues resolved since the last release, and known issues.

The following documentation has been discontinued:

- The *Dell AppAssure Command Line Management Reference Guide* has been discontinued. Information about the Rapid Recovery Command Line Management utility, now called cmdutil.exe, appears as an appendix to the *Dell Data Protection | Rapid Recovery User Guide*. This content addresses scripting of the Core management functions. This utility was previously called AACMD.
- The *Dell AppAssure PowerShell Module Reference Guide* has been discontinued. Information about the updated Rapid Recovery PowerShell Module is included as an appendix to the *Dell Data Protection | Rapid Recovery User Guide*.

Additional information about APIs is available in HTML files included in the SDK, in the form of reference materials and samples. You can obtain the SDK from the **Downloads** page of the Dell Data Protection | Rapid Recovery License Portal.

Resolved issues

Issues resolved in this release are listed below.

Table 1. Central Management Console resolved issues

Resolved issue	Issue ID	Functional area
Rapid Recovery Central Management Console did not display images correctly if installed on any machine without the AppAssure or Rapid Recovery Core service.	32532	MCMP
The Rapid Recovery Central Management Console failed to start on a domain controller with the error 'An error occurred during the request execution.'	32123	MCMP
Rapid Recovery Central Management Console did not display images correctly for any core server if the Core service was not running on the Central Management Console.	32093	GUI

Table 2. Core and Windows resolved issues

Resolved issue	Issue ID	Functional area
When the number of concurrent agentless transfers was increased from default of 3 to 10, performance of agentless transfer decreased, and frequency of transfer failures increased.	33286	Agentless protection
Repository did not mount after upgrade to Rapid Recovery 6.0 if record mode for RPFS record was changed to 0. In rare circumstances, the record mode for RPFS records may be changed to an invalid value due to defects in builds prior to 5.4.1.	32974	Repository
CSV reports were incorrectly formatted.	32966	Reporting
Migration step did not start for Background Job Settings.	32670	Backward compatibility
There was no ability to modify SQL metadata gathering timeout when using UseSqlQuery option.	32639	Metadata
Cores with a non-default deduplication cache size displayed an incorrect free space calculation during upgrade.	32608	Installer

Resolved issue	Issue ID	Functional area
Core Console GUI did not display after upgrade if Core had any custom groups established.	32488	Core
Core install fails with the error "Application catch an exception System.NullReferenceException depth 0: Object reference not set to an instance of an object. (0x80004003)" when installing in silent mode.	32100	Installer
A restore of the Core settings with repositories could not be performed in the "Restore Repositories" pop-up after fixing the path for the repository.	31990	GUI
Checkdisk of system volume fails after restore in ESXi Agentless.	31981	VMware agentless
Several check jobs (including SQL Attachability, Exchange Mountability, Exchange Checksum, Recovery point checks) in some circumstances had caused deadlock during execution which could not be cancelled.	31881	Core
Sometimes the Core service crashes during simultaneous deploy of multiple Linux agents when upgrading agents.	31878	Bulk deploy
Full virtual standby export occured in place of incremental exports after an incremental snapshot. This event occurred if the Core ran on a VM located on the same ESXi server to which virtual standby export was established.	31877	Virtual standby
Transfer failed if any disk on VM used format ...-000001.vmdk in ESXi agentless protection.	31738	VMware agentless
Transfers for ESXi agentless machines were stuck on a specific environment.	31352	VMware agentless
Replication failed with error "...Failed to synchronize the lists of consumed and outstanding seed drives" if upgrading source and target Cores from release 5.4.3 with outstanding seed drives on the source Core.	30339	Replication
The "Background Job Delayed" event created high load on Mongo DB, which led to delays in email notifications.	29450	Alerts
Replication in old (pre-5.4.1) replication mode tried (and failed) to transfer volume images to the target Core that were already replicated.	25648	Replication
There was no ability to schedule Deferred Delete jobs.	04739	Deferred delete

Table 3. DocRetriever for SharePoint resolved issues

Resolved issue	Issue ID	Functional area
Links are duplicated on the top link bar if restoring only subsites during an out-of-place restore.	31629	GUI

Table 4. Linux resolved issues

Resolved issue	Issue ID	Functional area
Protected Linux machines crashed on startup if the machine contained devices that were not listed in the LVM configuration.	32880	Linux Agent
Rapid Recovery Agent service failed to start on Linux machines if the volume group name containing the swap volume contained a hyphen.	32715	Linux Agent
SLES 12 was not bootable after BMR.	31762	Linux Live DVD
Agent fails to take next snapshot after a previous snapshot fails because the new generated data was larger than the size of the datastore.	31695	Linux Agent

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.

Table 5. Central Management Console known issues

Known issue	Issue ID	Functional area
Error: "Sequence contains no elements" appears when adding a domain user or group to access in the Central Management Console. **Workaround:** Back up Windows registry and then modify registry by setting AccountManagementAlgorithm to 1 at HKEY_LOCAL_MACHINE\SOFTWARE \AppRecovery\Mcmp\AccountManagementAlgorithm.	33459	MCMP
Impossible to repair or remove Rapid Recovery Agent or Central Management Console from Control Panel "Programs and Features" after uninstalling Core. **Workaround:** Repair or remove Rapid Recovery Agent or Central Management Console using installer programs.	30747	Installer

Table 6. Core and Windows known issues

Known issue	Issue ID	Functional area
Information about allocated space for some volumes is unavailable. Warning message appears on the Summary page for a protected machine if VM is located on the NFS datastore. This is a VMware issue caused by metadata gathering on NFS. **Workaround:** There is no known workaround.	33551	GUI
Machines with a specific PCIe application accelerator flash drive (SanDisk Fusion ioMemory™ SX350) cannot be protected; the serialization exception error appears: "Replay.ServiceHost.Implementation.Hosting.ServiceHost ... Service Host Error: Service error while handling request...: Enum value '2046' is invalid for type 'Replay.Common.Contracts.Metadata.Storage.StorageBusType' and cannot be serialized." **Workaround:** Disable or remove the device. A custom binary is available to address this issue. If you encounter this issue, please contact Support.	33532	Protection
When using agentless protection, the hypervisor host consumes a license on the License Portal. **Workaround:** There is no known workaround.	33525	Agentless protection
Unclear error message appears if you perform a Hyper-V virtual export to a node for which the cluster service is stopped. **Workaround:** If the cluster is valid, start the cluster service. Otherwise, remove the invalid or unnecessary cluster.	33511	Hyper-V export
For very large databases performing a mountability check job, cancel actions are ignored and job may hang. **Workaround:** If mountability check jobs hang when you want to cancel, restart the Core service.	33462	Mountability check
Sometimes virtual exports hang for virtual standby jobs during postprocessing. **Workaround:** Cancel unsuccessful export job.	33460	Virtual Standby
In some cases, if replication fails due to a temporary connection problem, automatic retries are not performed. There should be 2 attempted retries before a replication job terminates.	33423	Replication

Known issue	Issue ID	Functional area
Workaround: Force replication manually		
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, the Rapid Recovery agent, then restore the volumes.	33359	URC
Archive certificates validation on both Cores and protected machines should be removed from the archive check job, since certificates are not used when importing an archive. **Workaround:** Do not delete the certificates from archives.	33354	Archive
Rarely, on very busy systems, virtual standby export fails to start with incorrect RPFS file size error. **Workaround:** Wait for a period of time for workload to reduce. The next export job will start without an issue.	33308	Virtual Standby
Error: "Sequence contains no matching element" repeatedly appears in the Core log during mountability check. **Workaround:** Change logging configuration to handle larger files.	33301	Mountability check
Sometimes export for Agentless fails with "Object reference" error on post-processing step. **Workaround:** Force another export	33291	Agentless protection
Incorrect failure reason displays in UI if job fails with specific errors. **Workaround:** Check logs for actual cause of failure.	33242	Logging
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	Replication
Security corrections of SNMP protocol are required. There is no current ability to disable SNMP and then configure Community type. **Workaround:** Block SNMP port using a firewall.	33185	SNMP support
MongoDB service is configured to use an insecure REST interface. **Workaround:** Remove "--rest" portion of key manually, and then restart services.	33171	Mongo
There is no validation process when configuring a retention policy with using the API. **Workaround:** Check parameters carefully. Use UI to configure retention policy and to verify the settings.	33168	REST API
Heartbeat fails with error "Unable to contact licensing server" with authentication problem (such as AD or LDAP outage, incorrect credentials, or corrupt Exchange installation). **Workaround:** Repair whatever is causing the Exchange account to work incorrectly. Disable metadata settings on License portal or fix gathering SQL / Exchange metadata.	33151	Licensing
Agentless protection of machines with virtual RDMs does not work. The protected machine fails to protect, or shows no disk information. **Workaround:** Install the Rapid Recovery Agent software instead of using agentless protection.	33039	Agentless protection

Known issue	Issue ID	Functional area
Replication fails with uninformative error message when the source Core does not receive a proper response from the target (often caused by networking issues between the Cores). **Workaround:** Improve the network connectivity between the 2 cores to improve the communication between them.	32995	Replication
It is possible to start a VMware ESXi virtual export for a hard disk drive with 4096 bytes per sector. VMware only supports disks with 512 bytes per sector; thus, export of a 4096 bytes-per-sector disk should not be possible. **Workaround:** There is no workaround at this time.	32972	ESXi export
Windows System State backup does not work properly when Rapid Recovery Agent is installed on the machine. **Workaround:** A custom binary is available to address this issue. If you encounter this issue, please contact Support.	32967	Software conflict
RecoveryPointsInfo and MasterCoreInfo properties were removed from the Get-ReplicatedServers PowerShell cmdlet. This change to the cmdlet was intentional. Please update scripts to work without these properties. **Workaround:** A custom binary is available to address this issue. If you encounter this issue, please contact Support.	32954	PowerShellModule
If one of the ESXi hosts added to vCenter is offline, ESXi export fails for all agents with error "FormatException..." . **Workaround:** Bring ESXi host back online before performing virtual export.	32897	ESXi export
After upgrading from AppAssure 5.4.3 to Rapid Recovery 6.0 with notifications already configured, sometimes notifications do not work properly. **Workaround:** Add HKEY_LOCAL_MACHINE\SOFTWARE\AppRecovery\Core\Agents_ID_\EventsService\AgentAlertingPolicy registry branch for protected machines where this key is missed. Run script https://s3.amazonaws.com/appassure_patches/MigrateTo601.zip. A custom binary is available to address this issue. If you encounter this issue, please contact Support.	32879	Backward compatibility
After upgrade from 5.4.3, error: "Object reference not set to an instance of an object" appears on the Boot CDs tab if boot CDs were created prior to upgrade. **Workaround:** Remove HKEY_LOCAL_MACHINE\SOFTWARE\AppRecovery\Core\IsoDatabase\Entries\0 (1,2,3 etc) registry branch(es). A custom binary is available to address this issue. If you encounter this issue, please contact Support.	32878	Backward compatibility
Migration steps do not start during a clean install of Rapid Recovery if a previous HKLM/Software/AppRecovery registry branch is present. **Workaround:** 1. Delete registry keys which are not being used in the current version, or 2. Install previous version of Core and then upgrade to new version.	32863	Installer
Incorrect behavior of archive creation process if the previous archive attempt was interrupted and the "erase completely" recycle action was selected. **Workaround:** Choose different folder for archive.	32780	Archive
In rare cases, PreHyperVAgentScript does not run on the Hyper-V host during VM export. See Microsoft KB https://support.microsoft.com/en-us/kb/2779204 for details. **Workaround:** A custom binary is available to address this issue. If you encounter this issue, please contact Support.	32712	Hyper-V export
Replication fails with error: "Unable to read data contract from stream due to incorrect RPFS file size" if metadata for a recovery point or volume image was not written successfully due to environmental issues such as low memory or full repository.	32226	Transfers

Known issue	Issue ID	Functional area
Workaround: Remove problematic volume or recovery point using 'Delete range' on Source Core and then force 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	Archive
When the target network storage volume runs out of space, all running archive jobs fail with error: "There is not enough space on the disk" if more than one archive job is in progress.	31827	Archive
In rare cases, most commonly caused by environmental issues on an Exchange agent, the mountability queue breaks the order of the Virtual Standby export queue, causing a full export (instead of an incremental). **Workaround:** 1. Resolve the environmental issue on the Exchange agent (usually low memory) or 2. Disable automatic mountability check. A custom binary is available to address this issue. If you encounter this issue, please contact Support.	31803	Jobs
If users of ESXi Agentless protection perform virtual export of BusLogic Parallel controller-based machines to ESXi and VMware, the exported machines are not bootable. **Workaround:** Change controller type in configurations already exported to ESXi machine, and then boot it. Alternatively, perform the export to a Hyper-V server.	31775	VM Export
WinXPx86 machine is not bootable after export. Issue relates to controller drivers for SCSI and IDE controllers not present in the exported VM.	31705	VM Export
There is no link to "fix path" on a repository that has been opened using the "open existing repository" option. **Workaround:** Delete the repository path, and then fix the path while reopening the repository.	31473	GUI
There is no ability to change Snapshot Cleaning Timeout on the Settings page for a protected machine. **Workaround:** If you encounter this issue, please contact Support.	31460	GUI
Sometimes new volumes are not taken under protection automatically after metadata refreshes using agentless ESXi auto protection.	30968	VMware agentless
Mountability check fails with error: "Mandatory database was not found" if more than two Exchange 2013 databases are located on the same mounted volume. **Workaround:** Move the databases to separate mounted volumes. A custom binary is available to address this issue. If you encounter this issue, please contact Support.	30818	Mountability check
Impossible to repair or remove Rapid Recovery Agent or Central Management Console from Control Panel "Programs and Features" after uninstalling Core. **Workaround:** Repair or remove Rapid Recovery Agent or Central Management Console using installer programs.	30747	Installer
Server error "Object '/...rem' has been disconnected or does not exist at the server" appears when opening Core or protected machine settings. **Workaround:** Reduce workload on Core.	30629	Core
Boot CD starts with random IP even if user specifies a particular IP during creation of the Boot CD image. **Workaround:** If you need a correct IP address, you can configure your network to temporarily use DHCP. Alternatively, you can log in to the boot CD image with a keyboard and monitor, and assign the IP address while performing a bare metal restore.	30365	URC

Known issue	Issue ID	Functional area
Volume letters are not assigned during BMR for GPT partitions. **Workaround:** Assign drive letters using diskpart.	30319	URC
Functionality for archives has changed to allow recovery points to be archived without a full recovery point chain. The default behavior is to select the "Build recovery points chains (fix orphans)" option in the Options page of the Archive Wizard. **Workaround:** Reduce the workload on the Core. A custom binary is available to address this issue. If you encounter this issue, please contact Support.	30297	Repository
Core hangs during generation of HTML report for Core with greater than 300,000 event records. **Workaround:** Generate reports in PDF, CSV, XLS, or XLSX format instead of HTML format.	29788	Reporting
In some cases, when a Core contains more than 300,000 event records, reports fail to generate with error "Failed to generate report file." **Workaround:** Restart Core and MongoDB services.	29786	Reporting
Restore or virtual export of an ESXi agentlessly protected machine using SAN transport mode fails with error: "One of the parameters was invalid." **Workaround:** Use Network transport mode for rollback.	29508	VMware agentless
On specific environments, Deferred Delete jobs are slowed down when a DVM flush action is called too frequently. **Workaround:** Reduce the workload on the Core. A custom binary is available to address this issue. If you encounter this issue, please contact Support.	29420	DVM
PDF and HTML reports do not export for a Core with more than 300,000 event records. **Workaround:** Export to CSV or Excel format instead.	29265	Reporting
Nightly recovery points integrity check is not performed for some protected machines if one or more have no volumes protected. **Workaround:** Exclude any agent with no protected volumes from nightly recovery point integrity check. A custom binary is available to address this issue. If you encounter this issue, please contact Support.	28741	Nightly job
Replication stays paused after completing "Copy to seed drive" job if the same job was previously interrupted.	27749	Replication
Error message is unclear for ESXi export with auto disk mapping. **Workaround:** There is no workaround at this time.	27309	ESXi export
Error: "DvmBadRecord" appears if an agent volume was extended during a backup. **Workaround:** Do not extend volumes while backups are in progress.	26579	Repository
In rare cases (when hundreds of SQL databases exist on a volume), SQL Writer goes from stable to failed "nonretryable" state when Rapid Recovery takes a snapshot. **Workaround:** 1. Reduce the number of databases on the volume. 2. See KBs https://support.software.dell.com/appassure/kb/119513, https://support.software.dell.com/appassure/kb/120829, and https://support.software.dell.com/appassure/kb/151899. 3. A custom binary is available to address this issue. If you encounter this issue, please contact Support.	22155	Core

Table 7. DocRetriever for SharePoint known issues

Known issue	Issue ID	Functional area
DocRetriever Console does not open singular site collection backup in SharePoint 2013.	17238	DR

Table 8. Linux known issues

Known issue	Issue ID	Functional area
Product documentation: The procedure "Installing the Agent software on off-line Linux machines" in the *Installation and Upgrade Guide* versions 6.0.1 and 6.0.2 contains incorrect information about where to obtain the downloader script. **Workaround:** Instead of using the URL described in step 1 of that procedure, replace step 1 with the following information. Then resume the documented procedure with step 2. 1. From a Linux machine with access to the Internet, download the shell script for off-line Agent installation from the Dell Data Protection | Rapid Recovery License Portal as follows: a. Log in to the license portal. b. Click **Downloads**. c. When prompted for your product, select **Rapid Recovery**. d. Under Linux-Based Applications, scroll down to the Downloader script for off-line Agent installation, and click **Download**. e. Using removable storage media compatible with both machines, transfer the shell script file to the home directory of the appropriate offline Linux machine.	33628	Linux
Product documentation: Update installation commands for SLES to use Zypper. Two commands shown in the *Installation and Upgrade Guide* for installing Rapid Recovery Agent software on SUSE Linux Enterprise Server (SLES) are incorrect. SLES uses the Zypper package manager, but the commands shown for steps 5 and 6 are apt commands. **Workaround:** Use the command: "zypper refresh 'rapidrecovery repository'" in place of "apt-get update" to refresh the local repository in step 5. Use the command "zypper install rapidrecovery-agent" instead of "apt-get install rapidrecovery-agent" in step 6 to install Agent.	33583	Linux
5.4 Linux Agent software installation fails when installing on non-English locales. **Workaround:** Change shell locale temporarily to English before running the Agent installer.	33042	Linux
In some cases, the controller type for a Linux protected machine cannot not be detected, resulting in failure of virtual export with error: "System.InvalidOperationException: Sequence contains more than one matching element." **Workaround:** A custom binary is available to address this issue. If you encounter this issue, please contact Support.	32938	Linux
Ubuntu x32 machine is not bootable after Hyper-V export. **Workaround:** There is no workaround at this time.	31307	VMware agentless
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	VirtualBox export
Agentless protected ESX Ubuntu machine is not bootable after BMR. **Workaround:** Use the Rapid Recovery Agent on Ubuntu instead of using agentless protection.	31206	VMware agentless

Known issue	Issue ID	Functional area
Virtual Machine type is displayed as 'Physical' for Linux Agents installed on virtual machines with SATA disks. **Workaround:** There is no workaround at this time.	28583	Linux
RAM consumption grows during transfers of large amounts of data on SLES 11 x64. **Workaround:** A custom binary is available to address this issue. If you encounter this issue, please contact Support.	27509	Linux

Table 9. Local Mount Utility known issues

Known issue	Issue ID	Functional area
LMU hangs if user tries to open "Active mounts" window or to mount recovery points immediately after more than 5 recovery points were dismounted.	31707	Local Mount Tool
If you mount more than 20 recovery points in LMU and then dismount in LMU, dismounted recovery points are still displayed as Remote Mounts in the Core Console.	31706	Local Mount Tool

Table 10. Mailbox Restore known issues

Known issue	Issue ID	Functional area
If there is an incorrect value stored in the database for the mailbox owner's unique mailbox identifier, a restore action to the original location fails with error: "Could not open message store. **Workaround:** Restore to a different location.	33440	MR
Exchange 2016 databases are not currently supported; support is planned for release 6.1. Currently, Exchange 2016 databases are incorrectly identified as Exchange 2013 databases. **Workaround:** There is no workaround at this time.	30924	MR

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). 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 in Rapid Recovery release 6.0.1 and later 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 11. 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.x
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 | Rapid Recovery DocRetriever for SharePoint – make sure you allocate more resources, in addition to those needed for efficient Core operations.

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

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

Before installing Rapid Recovery release 6.0.2, 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 12. 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.x and Rapid Recovery 6.0.x 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 supported Linux operating system and distribution, and describes support for each Rapid Recovery component or feature.

Table 13. 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 14. 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*

Requirement	Details
	- 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.
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 15. 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

Requirement	Details
	- 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. 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.

Requirement	Details
	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 16. 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.
Network hardware	Use network cables with the appropriate rating to obtain the expected bandwidth.

Requirement	Details
	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 17. 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.

Requirement	Details
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 18. 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. 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*.

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:

1. **An account on the Dell Data Protection | 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 previously known as the Dell AppAssure License Portal. If you already have a license portal account that you have used for AppAssure, 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*.

2. **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 Dell 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 Dell 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.

To request a license upgrade, contact your Dell Sales representative by completing the Contact Sales web form at https://software.dell.com/register/57955. 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 Dell 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.

- Dell Support policy
- Upgrade and installation instructions
- Additional resources

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 19. 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

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
6.0.2 Agent	Not Supported	Not Supported	Not Supported	Not Supported	Supported

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.

If upgrading from AppAssure Core release 5.4.3, or Rapid Recovery Core release 6.0.1, then run the new Core installer software on your Core. 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 6.0.1, run the new 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 VMware virtual machines on an ESXi host without the Agent software. Important restrictions apply. For more information on benefits or restrictions for agentless protection, see the topic “Understanding agentless protection” in the *Dell Data Protection | Rapid Recovery User Guide*.

Dell Software policy is to support two previous releases of software products. If you want to upgrade a version older than two releases, best practice is to first upgrade to the last release (Rapid Recovery Core release 6.0.1), or the one prior (AppAssure Core release 5.4.3). You can then run the 6.0.2 installer for the Rapid Recovery Core or Agent component, respectively.

ⓘ NOTE: If running a localized Core in a language other than English, upgrade directly from AppAssure release 5.4.3 to Rapid Recovery Core release 6.0.2.

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 6.0.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 will need to register at the Dell Data Protection | Rapid Recovery 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 6.0.2 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.