Rapid Recovery 6.1.3 Release Notes

August 2017

These release notes provide information about the Rapid Recovery release, build 6.1.3.100.

Topics include:

About this release

Rapid Recovery software delivers fast backups with verified recovery for your VMs and physical servers, on-premises or remote. 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.

Since Rapid Recovery 6.1.3 is a maintenance release, the enhancements and defect fixes are unique to this release. Only the known issues are cumulative. For information on new features, enhanced functionality, resolved issues, known issues, or component changes for other releases, see release notes for the appropriate version of Rapid Recovery on our technical documentation website. For example:

- To see information specific to the most recent major release, Rapid Recovery 6.0, see Rapid Recovery 6.0.1 Release Notes.
- To see information specific to the most recent minor release, Rapid Recovery 6.1, see Rapid Recovery 6.1 Release Notes.
- To see information specific to the most recent prior maintenance release, Rapid Recovery 6.1.2, see Rapid Recovery 6.1.2 Release Notes.

NOTE: The default view of the technical documentation website shows documentation for the most recent generally available version of the Rapid Recovery software. Using the filters at the top of the page, you can view documentation for a different software release or for a Quest DL series backup and recovery appliance. You can also filter the view by guide category.

Rebranding

Release 6.1.3 includes full rebranding of the Rapid Recovery user interface installed on the DL Appliance to reflect the Quest Software brand. For more information about Quest, see About us.

Repository upgrade advisory

Upgrading the Core software to release 6.1.x from any earlier version (for example, Rapid Recovery 6.0x, or 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.

After 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, refer to the release notes for the most current system requirements. Release notes are sometimes updated and re-issued in a release cycle.

Rapid Recovery release designations

Rapid Recovery release designations consist of up to four parts. Each part consists of a set of numerals separated by decimal points.

- **Major releases** are specified by the first numeral. These releases include dramatic changes to UI, the repository, or application behavior.
- **Minor releases** are specified by the second numeral, which follows the first decimal point. Minor releases introduce new functionality that is smaller in scope than the types of changes included in major releases.
- **Maintenance releases** are specified by the third numeral, which follows the second decimal point. For release numbers at this point and in the future, if the third numeral is greater than 0, it is a maintenance release. Maintenance releases correct previously identified defects or behaviors.
- **Build numbers** (typically 3 or 4 digits) are specified by the fourth set of numerals. This part is used to differentiate version of the software program generated during the development process.
    - For the Rapid Recovery Agent software, build numbers may differ between Windows and Linux versions. If the first three parts of the release number are identical, interoperability between the Core and Agent with different build numbers is not affected.
    - Updated builds of the same software release may be made available on to the License Portal within a release cycle. Therefore, if your Core is set to automatically update the Agent version on protected machines, you may see differences in build numbers for a single release. These differences will not negatively influence functionality.
    - Build numbers may also differ between software-only versions of the Core and the versions used on the Quest DL series backup and recovery appliances.
    - Build numbers will differ between the Core and the Add-on for Kaseya component.
    - Difference in build numbers do not affect replication.

For release 6.1.3.100, the first digit (6) is the major release. The second digit (1) represents the minor release. The third digit (3) indicates that this is the third maintenance release to 6.1, containing defect fixes. In this case, the maintenance release also contains rebranding for Quest DL appliances. The build number (100) is last and is generally only referenced in release notes.

Resolved issues

Customer-facing issues resolved in this release are listed below.

Table 1. Central Management Console resolved issue

Resolved Issue Description	Issue ID	Functional Area
Was unable to authorize to Central Management Console on a single customer environment due to specific configuration of domain controller, groups and accounts.	101227	Authentication

Table 2. Core and Windows resolved issues

Resolved Issue Description	Issue ID	Functional Area
The Dismiss All button on the Event page for a protected machine removed all alerts for the Core instead of for the specific machine.	103386	Events
After executing the Get-UnprotectedVolumes PowerShell command for specific machines, protected volumes displayed instead of unprotected volumes.	103302	PowerShell
A CIFS repository went offline at random times dues to multiple connections.	103240	Repositories
The Core certificate contained two Common Names (CNs) hostname/localhost inside the issuer, instead of one CN hostname.	103233	Certification
A Core certificate with one CN hostname was not secure in Chrome 58.	103303	Certification
Archive compression speed for archives saved in 6.1.x decreased by as much as 50% over the speed attained in AppAssure release 5.4.3.	103229	Archive
The compression ratio of archives was too small after an upgrade from AppAssure 5.4.3 to Rapid Recovery 6.1.2.	103212	Upgrade
Retention policy logic does not account for specific cases that could result in skipping generation of a monthly recovery point during rollup. For example, when an error occurs during capture of an incremental snapshot, or if nightly jobs runs over and causes rollup not to run, then when the rollup policy enforces the logic to keep one recovery point per month, in rare cases, the monthly recovery point may not be created. This is as designed.	103165	Retention policy
If a Hyper-V Cluster was agentlessly protected, the Core System Events logs were spammed by a "DCOM" error.	103021	Agentless protection
The archive recycle actions "Erase completely" and "Replace this Core" did not function correctly.	102803	Archive

Resolved Issue Description	Issue ID	Functional Area
Repository mount failed with error, "Failed to mount repository because it is currently in use by another Core," because the damaged/not valid dfs.mbr file was not rewritten after a Repository Check job.	102719	Repositories
ESXi export job failed with permissions error for a protected machine that has disks with identical UUIDs.	102685	ESXi export
Base images were taken instead of incrementals for a volume with Hyper-V virtual disk files on a Windows Server 2016 Hyper-V protected machine.	102617	Hyper-V protection
Disks and volumes were not detected for VMs protected agentlessly if FIPS 140-2 protocol was enabled on Core.	102508	Agentless protection
Core could not create a DVM repository greater in size than 16TB when write caching was enabled.	102507	DVM repository
When using replication, the Core could not consume a seed drive named "AABackup."	102506	Replication, seed drive
In a unique environment, replication transferred all data instead of incremental because 'Recalculate deduplication cache for repository' failed. In the specific environment, this behavior is as designed.	102297	Replication
Local Hyper-V export failed on Windows Server 2016 with error: "WMI class "MsvmVirtualSystemGlobalSettingData" or error "properties in class 'MsvmVirtualSystemGlobalSettingData' was not found."	102223	Virtual export
Hyper-V agentless protection for all nodes in a cluster failed with error: "Unrecognized Guid Format" due to the specific state of a VM hosted on a cluster.	102221	Hyper-V agentless
Checking archive job was canceled if storage was corrupted, instead of failing with appropriate informative error.	102207	Archiving
For replicated protected machines, the nightly job setting for 'Check recovery points integrity' set to default (enabled) even if the setting on the source was changed to disabled before replicating.	102105	Replication
If you tried to perform a one-time export of a recovery point on a protected machine to Azure, errors appeared when you tried to specify a new cloud service name in the Deploy page of the Virtual Machine Export Wizard. The error was "Object reference not set to an instance of an object."	101819	VM export
There was no warning message that rollup was not performed for recovery points on a seed drive that had not yet been consumed. This was only relevant for environments that used replication with an outstanding seed drive.	35823	Replication
If a USBB device was connected to the Core machine and went into an unknown B state, the error "Failed to call Create File on disk '\\.\PhysicalDrive' - The specified network resource or device is no longer available" displayed and blocked the GUI, because the Core could not gather metadata.	35765	Protection

Resolved Issue Description	Issue ID	Functional Area
If a user tried to mount a volume with the single-instance storage (SIS) feature on the volume, even if the feature was disabled and a new base image was taken, the error "The current OS does not support Single Instance Storage and cannot be used to mount volumes" displayed and the volume would not mount.	35718	Mounting
Specific volumes were not mounted after virtual export of Linux machine. This defect applied only to customers with LVM volumes on an iSCSI Dell EqualLogic machine.	35288	Virtual export (ESXi)
During a repository check, the status for a repository appeared on the Core Console Home page as red.	34904	Repositories

Table 3. DL Appliance resolved issues

Resolved Issue Description	Issue ID	Functional Area
In a specific customer environment, the Provisioning appliance page was unavailable, with an error: "CIM Chassis error" due to a storage pool that referenced an enclosure that did not exist.	102495	GUI
User could launch several remount jobs simultaneously on DL Appliance.	102322	Storage Provisioning
FTBU failed when trying to start a Core service that was already in a "Starting" state.	101554	FTBU
There was an incorrect default value of Repository name field on the Add New Repository Wizard.	101348	Storage Provisioning
If the server was rebooted during FTBU, then the Compatibility Mode of the browser prevented the first launch of the Core after FTBU from performing successfully.	101313	FTBU
RASR failed to start with fatal exception on DL1300 and DL4300 with new ID modules.	101051	Storage Provisioning
If a repository name contained three dots in a row, the provisioning job failed with an error and the repository was not created.	100913	Provisioning
Parameters in 'Expand Existing Repository' pop-up did not reflect true available space for repository expansion on internal controller on DL1300 after upgrade via RUU#3.1.	100908	Windows Backup
Storage Provisioning and Restore the Provisioning Configuration jobs could be launched simultaneously in spite of incompatibility for launching of these jobs.	100907	Storage Provisioning
RASR USB could not be created on the server after upgrade using RUU if server was restored from Windows backup.	100905	Storage Provisioning
Core interface became unavailable if forced to collect Core and Appliance logs.	100904	RASR

Resolved Issue Description	Issue ID	Functional Area
The LSI Provider installation failed if the User Policy was set to Restricted.	99997	RUU
RUU hung after several double-clicks on the RUU window.	98537	RUU
Monitor Active Task hung at 95% during creation of RASR USB job.	35531	Storage Provisioning
Job "Restore the provisioning configuration" failed on a specific environment.	35137	RASR
Sometimes error "invalid state; already open" appeared on the Virtual Standby page for DL4x00 Appliances.	31477	Storage Provisioning

Table 4. DocRetriever resolved issue

Resolved Issue Description	Issue ID	Functional Area
DocRetriever did not restore the "Content Editor" web parts in SharePoint 2013.	103241	Restore
Old documents are not overwritten after a restore with the options "Merge containers" and "Overwrite" selected.	102616	Restore

Table 5. Documentation resolved issue

Resolved Issue Description	Issue ID	Functional Area
Context-sensitive help found in-product for Rapid Recovery Core was re-branded as of release 6.1.2 to reflect its ownership by Quest Software. Other than rebranding, no content changes appeared for help files in that release.	70130	Context-sensitive help

Table 6. Kaseya Add-On resolved issues

Resolved Issue Description	Issue ID	Functional Area
In some cases, credentials for Cores and Agents in the Kaseya Server were stored in unencrypted text in the AppRecoveryParams.json file.	102096	Authentication

Table 7. Linux resolved issues

Resolved Issue Description	Issue ID	Functional Area
Was unable to protect an Ubuntu Linux Agent if it contained a "non fs data" partition type.	102284	Metadata

Table 8. Local Mount Utility resolved issues

Resolved Issue Description	Issue ID	Functional Area
For mounted recovery points on a Windows Server 2016 machine, the "Explore" button was disabled.	101860	Mounts

Table 9. Mailbox Restore resolved issues

Resolved Issue Description	Issue ID	Functional Area
When Mailbox Restore loaded mailboxes from an Exchange 2016 CU5 database, the error "Property Blob version is invalid" displayed.	102696	Exchange databases
The "From" field incorrectly contained Asian characters in the message preview.	102586	Localization
MailboxRestore could not restore a message containing emoticon symbols such as unamused face (ASCII symbol "😒").	102360	Restoring

Known issues

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

Table 10. Core and Windows known issues

Known Issue Description	Issue ID	Functional Area
After an upgrade from release 6.1.1 to release 6.1.2 on an environment with a specific security policy, the Core Console does not open. **Workaround:** Complete the following steps: 1. Find the file Web.config at C:\Program Files\AppRecovery\Core \CoreService\coreadmin folder and open it in Notepad. 2. Change the value from "localhost" to "charon." For example, <add key="CoreHostName" value="charon" />. 3. In the Web.config file, turn in-memory hosting on by changing the value from "false" to "true." For example, <add key="InMemoryHosting" value="false" />. 4. Restart the Core service.	103783	GUI
In the Spanish translation of the product, agentless virtual machines (VMs) do not display on the Virtual Machines page. **Workaround:** To view the VMs, change the language of the Core from Spanish to another language in the Core Settings.	103782	GUI
The Agent service on a cluster may crash when attempting to collect SQL metadata of a database with the FileAttributes.ReparsePoint attribute. **Workaround:** Contact Support to request a patch that addresses this issue.	103740	Agent

Known Issue Description	Issue ID	Functional Area
A queued replication job begins after the scheduled start time has passed.	103702	Replication
The ability to restore ReFS volumes fails for Windows Server 2016. **Workaround:** Move the existing repository to a Windows 2012 or Windows 2012 R2 operating system, and then perform the restore.	103698	Restore
There is no ability to add a new cloud account to the Azure Government cloud. **Workaround:** None.	103683	Azure
The Core exhibits poor performance and high system resources usage when mounting a recovery point from an attached Azure archive. **Workaround:** Contact Support to request a patch that addresses this issue.	103670	Azure
MongoDB cannot connect to the Rapid Recovery servers due to an insufficient quantity of available ports. **Workaround:** None.	103664	Connectivity
It is possible to restore a recent Core configuration with a backup of an outdated Core version. **Workaround:** None.	103632	Core
The setting for maximum concurrent exports does not enforce the limitation if the setting is changed to '1' while two or more exports are in progress. **Workaround:** None.	103515	Core settings
During a successful repository check, a 'Placeholder mismatch' error displays in the Phase area of the Monitor Active Task details of the job. **Workaround:** None.	103492	Repository check
ESXi export fails when the Quest NetVault Backup with BMR plugin is installed on the same machine as the Rapid Recovery Core. **Workaround:** Complete the following steps: 1. Copy the following .dlls from Coreservice\vddk\bin to Coreservice folder: ◦ glib-2.0 ◦ gobject-2.0 ◦ gvmomi ◦ iconv ◦ intl ◦ libcurl ◦ libxml2 ◦ vixDiskLibVim 2. Restart the Core service.	103477	Virtual export
If the dedupe cache is on a disk with a sector size of 4KB, resizing the dedupe cache fails with the error "cache_io_engine: windows error 87."	103469	Repository

Known Issue Description	Issue ID	Functional Area
Workaround: Contact Support to request a patch that addresses this issue.		
Agentless protection of an ESXi VM fails with the error "An item with hthe same key has already been added" for the vCenter server. **Workaround:** Contact Support to request a patch that addresses this issue.	103426	Agentless
The Dashboard Transfer Job widget does not track jobs that expire while queued. **Workaround:** None.	103412	Reporting
A Core set to display in Portuguese fails to communicate with the license portal, because the DateTime was not recognized. **Workaround:** Set the Core to another language.	103371	Licensing
The error message "The specified display name is already in use by another agent" displays during agentless protection if the VM exceeded the maximum number of permitted snapshots. **Workaround:** Delete snapshots for the VM so that it has fewer than the maximum number of snapshots allowed.	103334	Protection
Transfer failed due to the absence of retries during the CleanupSnapshotInternal stage of the transfer during a brief network outage. **Workaround:** Attempt another backup.	103310	Transfers
A Core certificate with on CN (Common Name) hostname is not secure in Chrome 58.0. **Workaround:** Use a different browser.	103303	Security
When a scheduled archive is set with the option "Include only the recovery points in the date range ...," a base image is archived. **Workaround:** There is no workaround for this issue at this time.	103283	Archiving
A DVM repository stored on a Common Internet File System (CIFS) shared volume randomly goes offline with error: "Multiple connections error occurred while trying to map share." **Workaround:** Contact Support to request a patch that addresses this issue.	103240	Repository
When database files are located on a quorum disk for a protected SQL Server cluster, log truncation does not occur, with error: "SQL log truncation for the protected has been skipped, because there aren't any SQL databases in protection group." **Workaround:** Move the SQL Database on a different volume. Alternatively, schedule SQL log truncation separately using a post-transfer script or a scheduled job.	103225	SQL log truncation
Archives created in Rapid Recovery Core releases 6.0.2 and later have lower performance than archives created in earlier releases, relative to both speed and compression ratio. Not a defect in 6.0.1. This defect first appeared in release 6.02, and recurs in releases 6.1.0, 6.1.1, and 6.1.2.	103212	Archive

Known Issue Description	Issue ID	Functional Area
Workaround: Contact Support to request a patch that addresses this issue.		
Deploy to Azure fails if you specify a cloud service name in Fully Qualified Domain (FQDN) format. **Workaround:** Specify service name using hostname format.	102756	Azure
The export postprocessing step can sometimes take a long time to complete the dismount operation. **Workaround:** Increase the protection interval.	102742	Exporting
Sometimes there is no ability to protect a cluster with the same hostname as a protected cluster from a different domain. **Workaround:** Complete the following steps: 1. Protect the first cluster. 2. Stop the Core service. 3. Navigate to registry HKEY_LOCAL_MACHINE\SOFTWARE\AppRecovery\Core\Agents\f0ca6c1d-0000-0000-0000-000000000000 and copy the GUID. 4. Change the value of the GUID to 1. 5. In the registry, find records with the old GUID and change those values to 1. 6. Start the Core service. 7. Protect the second cluster.	102702	Protection
Incremental Virtual Standby Hyper-V export fails if the location or name of the exported VM includes Chinese symbols. **Workaround:** Replace the Chinese symbols with English characters in the location and name of the exported VM.	102589	Virtual export
The following warning about a nonexistent writer on a SQL Server or Exchange protected machine displays during log truncation: VSS full snapshot was taken with excluded VSS writers "Microsoft Exchange Writer has state" error. **Workaround:** Ignore the warning, as it does not prevent the truncation job from completing.	102567	Log truncation
Slow incremental images are captured for volumes with specific write activity. **Workaround:** Contact Support to request a patch that addresses this issue.	102493	Backups
Deferred delete cancels after rollup job when localization is set to a French OS. **Workaround:** Contact Support to request a patch that addresses this issue.	102436	Localization, deletion
Sometimes the drive letters of an exported machine do not match the drive letters of the source machine. **Workaround:** Contact Support to request a patch that addresses this issue.	102390	Virtual export
On the Recovery Points page of the Core Console, users are unable to navigate multiple pages of recovery points by using a menu. **Workaround:** Use existing navigation.	101736	UI

Known Issue Description	Issue ID	Functional Area
Seed drive job fails with error: "Write data task has failed."	101617	Replication
When Secure boot option is enabled on Windows Server 2016, installation of some drivers are blocked during Agent installation, displaying error: "The transfer failed." **Workaround:** Contact Support to request a patch that addresses this issue.	101573	Installer
After a few weeks, VM export fails. TCP/IP event 4227 appears in system log, with message "TCP/IP failed to establish an outgoing connection because the selected local endpoint was recently used to connect to the same remote endpoint." This error typically occurs when outgoing connections are opened and closed at a high rate, causing all available local ports to be used and forcing TCP/IP to reuse a local port for an outgoing connection. **Workaround:** Temporarily increase dynamic port range, and restart the server periodically.	101485	Virtual export
ESXi Virtual Standby fails with error: "An entry with the same key already exists" on a system test environment.	100868	Virtual export
"Maximum connection pooling size" and "Minimum connection pooling size" fields for the MongoDB connection are not validated, allowing users to set a maximum value below the minimum value. **Workaround:** Set a "Minimum connection pooling size" value that is less than the "Maximum connection pooling size" value.	35607	Core settings
A base image is captured instead of an incremental image on a Windows Server 2012 R2 protected machine when NTFS Boot Sector copy was changed. This defect only affects users who installed third-party software that changed in the NTFS Boot Sector copy. **Workaround:** None.	34981	Backups
Unexpected base images captured in ESXi VMs that have snapshots with quiescing enabled. Defect affects users who protect vCenter virtual machines that have SAN snapshots with quiescing enabled. Workaround: Disable quiescing.	34916	Virtual export
Virtual standby performance is slow when performing export of multiple concurrent protected machines (for example, 36). **Workaround:** Decrease the number of concurrent export jobs allowed.	34434	Virtual export
Warning message: "Information about allocated space for some volumes is unavailable... " displays on the Summary page for a protected machine if the VM is located on a Network File System (NFS) datastore. **Workaround:** None. This is a limitation of VMs stored on an NFS datastore.	33551	Summary information
Replication rate becomes extremely slow if a virtual export job is started concurrent to the replication job. **Workaround:** Use schedule to avoid replication and export run simultaneously.	33230	Virtual export, replication, resource consumption

Known Issue Description	Issue ID	Functional Area
When archiving 2 or more jobs simultaneously, if the target network storage device runs out of space, 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	Archiving
After virtual export of a WinXPx86 machine protected agentlessly, or virtual export of any machine protected on an ESXi host, the resulting VM is not bootable. Issue relates to controller drivers for SCSI and IDE controllers not present in the exported VM. **Workaround:** None.	31705	Virtual export
After virtual export of RHEL 6 or 7 with the LVM or RAID volumes and more than eight HDDs from an ESXi host, the resulting VM is not bootable. **Workaround:** To let the export be created with all disks on one single disk controller and let the machine boot successfully after export, use less than nine disks on one disk controller.	31277	Virtual export
ESXi agentless restore or virtual export using SAN transport mode fails with the error, "One of the parameters was invalid." **Workaround:**Use Network Transport mode for restoring data.	29508	VMware agentless, restoring data
If using auto disk mapping for VM export from ESXi, in rare cases an error occurs with an uninformative message: "Task 'ReconfigVM_Task' failed: Invalid configuration for device '0'." **Workaround:** Try the operation again and it should succeed.	27309	Virtual export

Table 11. DL Appliance known issues

Known Issue Description	Issue ID	Functional Area
After a factory reset, the Core may fail to restore the configuration for some services during the Remount Volumes job, but the Core shows the job as being successfully completed. **Workaround:** Perform another Remount Volumes job.	104043	Restore
The MongoDB service cannot establish a connection to the Core, because there are not enough available ports. **Workaround:** None.	103664	Connection
Sometimes "Internal Server Error" appears on Backup page. **Workaround:** Ignore and close the error message.	102379	Storage Provisioning
After an upgrade to release 6.1.2, repository maintenance failed after a restore of the provisioning configuration. **Workaround:** Contact Support.	102340	Windows Backup
Remount job does not restore Core's localization.	101316	Storage Provisioning

Known Issue Description	Issue ID	Functional Area
Workaround: Manually change Core localization from Core Settings.		
Jobs are failing with error: "System.OutOfMemoryException" on DL Appliances after running for some time. **Workaround:** Install the latest Windows updates and reboot the appliance. If this problem persists, contact Support.	101246	Storage Provisioning
Statuses of volumes are displayed as 'Not valid' if a letter is assigned to 'Recovery' partition. **Workaround:** Wait until the RASR USB creation job completes or, if the driver letter was manually assigned to the Recovery partition, remove the drive letter.	101224	Virtual Export
Windows Backup failed when necessary volume letters were changed. **Workaround:** Remove current policy with mixed/changed letters for partitions and create a new policy with heterogeneous volume labels.	100985	RASR
Main Appliance status receives a red state without the ability to resolve if Windows Backup was forced on the server with old Winbackups with volume size of 75GB and without free space on Internal controller. **Workaround:** Clear the Windows Backup logs as follows: 1) Open event viewer. 2) Go to Applications and Services Logs. 3) Navigate under Microsoft -> Windows -> Backup. 4) Right click on the Operational channel and select Save and Clear (or, if you don't want to save, select Clear).	100887	UI
Restore the provisioning configuration job fails with an uninformative error: "Cannot mount volume to the folder 'I:\' because it contains files or folders" if the virtual disk has a letter assigned that was already used before remount. **Workaround:** Remove assigned letters from attached virtual media via disk manager. Perform Volumes Remount job again from Appliance Provisioning page.	35805	Provisioning
Incorrect behavior of provisioning size determining logic. **Workaround:** When performing provisioning, specify the intended sizea few GB smaller than the available space.	35770	Windows Backup
VMM actions are available when ESXi host is in maintenance mode. **Workaround:** Do not perform any VM operations from the Virtual Standby page if an ESXi host is in Maintenance mode.	35740	Storage Provisioning
The GUI should be disabled immediately after confirmation of the remount process. **Workaround:** Wait for a few minutes and refresh Core Console page.	35579	Virtual Machine Management
On the Backups page, incorrect translation of 'State' appears in the 'Items Baced Up' section for some non-English language. **Workaround:** None.	35031	Storage Provisioning
VD disk provisioning fails with return code 4 if storage pool does not have consistent empty space.	34937	Localization

Known Issue Description	Issue ID	Functional Area
Workaround: Contact Support.		
"Start VM / Network Adapters" buttons remain enabled when an ESXi or Hyper-V export of a machine is launched on DL Appliances. **Workaround:** Do not click these buttons until the corresponding VM export is complete.	30989	Virtual Machine Management

Table 12. DocRetriever known issues

Known Issue Description	Issue ID	Functional Area
DocRetriever fails to open a SharePoint 2016 database when several sites have a similar identifier. **Workaround:** Contact Support to request a patch that addresses this issue.	103710	Databases
DocRetriever restore operations fail on 32-bit versions of Windows operating systems due to the absence of a necessary registry key. **Workaround:** On the protected machine, manually create the following key in the registry: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NETFramework \AssemblyFolders\SharePoint.	102522	Restore

Table 13. Documentation known issues

Known Issue Description	Issue ID	Functional Area
The components ANTLR 3.3.3 and ANTLR 4.0.2 appear in the list of third-party components found in the product, even though they were not used in Rapid Recovery 6.1.3. **Workaround:** The component will be removed from the Third-Party Contributions list in a future release.	104031	Context-sensitive help
The component MongoDB 2.6 appears in the list of third-party components found in the product, even though it was not used in Rapid Recovery 6.1.3. **Workaround:** The component will be removed from the Third-Party Contributions list in a future release.	104030	Context-sensitive help
The component Microsoft Windows Azure Storage 7.2.1 does not appear in the list of third-party components found in the product. An outdated version of the component appears in its place. **Workaround:** Microsoft Windows Azure Storage 7.2.1 uses the Apache 2.0 license, which can be found in the Third-Party Contributions list in the in-product Help and hyperlinked from the About Rapid Recovery page.	102504	Context-sensitive help
The component DataGridViewImageAnimator 1.0 appears in the list of third-party components found in the product, even though it was not used in Rapid Recovery 6.1.3. **Workaround:** The component will be removed from the Third-Party Contributions list in a future release.	102503	Context-sensitive help

Known Issue Description	Issue ID	Functional Area
The component SimpleRestServices 1.3.0.3 does not appear in the list of third-party components found in the product. An outdated version of the component appears in its place. **Workaround:** SimpleRestServices 1.3.0.3 is used in Rapid Recovery 6.1.3. The component uses the MIT N/A license. A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.	102502	Context-sensitive help
The component OpenStack.NET 1.4.0.2 does not appear in the list of third-party components found in the product. An outdated version of the component appears in its place. **Workaround:** OpenStack.NET 1.4.0.2 was used in Rapid Recovery 6.1.3. The component uses the MIT N/A license. A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.	102501	Context-sensitive help
The component NLog 3.2.1 does not appear in the list of third-party components found in the product. An outdated version of the component appears in its place. **Workaround:** NLog 3.2.1 was used in Rapid Recovery 6.1.3. The component uses the BSD - Kowalski 2011 license, Copyright (c) 2004-2011 Jaroslaw Kowalski <jaak@jkowwalski.net>. A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.	102500	Context-sensitive help
The component AWS SDK for .NET 3.3.1.2 does not appear in the list of third-party components found in the product. An outdated version of the component appears in its place. **Workaround:** AWS SDK for .NET 3.3.1.2 uses the Apache 2.0 license, which can be found in the Third-Party Contributions list in the in-product Help and hyperlinked from the About Rapid Recovery page.	102499	Context-sensitive help
The *Rapid Recovery User Guide* procedure "Deploying a virtual machine in Azure" for release 6.1.x 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...".	101859	Azure export
The *Rapid Recovery User Guide* procedure "Setting up continual export to Azure" for release 6.1.x 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).	101858	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 may not be immediately visible in the wizard. This behavior is not reflected in the appropriate procedures in the *Rapid Recovery User Guide*.	101853	Azure export

Known Issue Description	Issue ID	Functional Area
Workaround: If you create a container from the Virtual Machine Export Wizard, and that container is not accessible in the wizard UI, 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.		
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 release 6.1.x 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).	101837	Azure export

Table 14. Linux protection known issues

Known Issue Description	Issue ID	Functional Area

After a successful virtual export, a machine running Debian 7.11 with a root on a RAID does not start.
Workaround: Complete the following steps:
1. Load liveDVD.
2. Chroot to the new /dev/sdc disk and install grub on it:
`mount --bind /dev /mnt/dev`
`mount --bind /proc /mnt/proc`
`mount --bind /sys /mnt/sys`
`chroot /mnt /bin/bash`
`grub-install /dev/sd*`
	103558	Virtual export

Protection of volumes created with LVM-based storage pools fails. **Workaround:** Contact Support to request a patch that addresses this issue.	103488	Protection
Transfer from Core failed on SLES 11.4 x32 with the error, "The partition size is incorrect, please shrink the volume." **Workaround:** Use a different release of SLES or a different Linux distribution.	103300	Transfers
It is possible to select Linux system folders for a rollback restore. **Workaround:** None.	103178	Restore
Unable to use Transport Layer Security (TLS) 1.2 protocol with Linux Agent. **Workaround:** Disable TLS 1.0 and/or SSL3.	101279	Security
There is no warning message indicating that the Agent service cannot be started if it was installed on a Linux machine using an init system other than the originally installed system. For example, Debian 8 uses SysD by default. If SysD is removed and SysV installed, the Agent does not start.	35818	Notifications

Known Issue Description	Issue ID	Functional Area
Workaround: No workaround is required since the defect only describes the absence of a notification.		
Agentlessly protected Ubuntu machine is not bootable after BMR. **Workaround:** Use the Rapid Recovery Agent on Ubuntu instead of using agentless protection.	31206	BMR bootability

Table 15. Mailbox Restore known issues

Known Issue Description	Issue ID	Functional Area
The MAPI dialog does not display during a restore if the Exchange server uses a self-signed certificate, which causes the restore to fail. **Workaround:** Add the certificate to local storage of trusted certificates on local machine by clicking "View Certificate," and then "Install Certificate" when the dialog displays.	102765	Security
During restore of permissions for a public folder, an uninformative error message displays if user was not found in the Global Address List. **Workaround:** No workaround is required since the defect only describes an error message which can be ignored.	102018	Restoring

Rapid Recovery system requirements

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

Topics include:

- Recommended network infrastructure
- UEFI and ReFS support
- Support for dynamic and basic volumes
- Support for Cluster Shared Volumes
- Rapid Recovery Core installation requirements
- Rapid Recovery release 6.1 operating system installation and compatibility matrix
- Rapid Recovery Core and Central Management Console requirements
- Rapid Recovery Agent software requirements
- Rapid Recovery Local Mount Utility software requirements
- Rapid Snap for Virtual agentless protection
- Hypervisor requirements
- DVM repository requirements
- License requirements
- Quest Support policy

Recommended network infrastructure

For running Rapid Recovery, Quest requires a minimum network infrastructure of 1 gigabit Ethernet (GbE) for efficient performance. Quest recommends 10GbE networks for robust environments. 10GbE networks are also recommended when protecting servers featuring large volumes (5TB or higher).

If multiple network interface cards (NICs) are available on the Core machine that support NIC teaming (grouping several physical NICs into a single logical NIC), and if the switches on the network allow it, then using NIC teaming on the Core may provide extra performance. In such cases, teaming up spare network cards that support NIC teaming on any protected machines, when possible, may also increase overall performance.

If the core uses iSCSI or Network Attached Storage (NAS), Quest recommends using separate NIC cards for storage and network traffic, respectively.

Use network cables with the appropriate rating to obtain the expected bandwidth. Quest recommends testing your network performance regularly and adjusting your hardware accordingly.

These suggestions are based on typical networking needs of a network infrastructure to support all business operations, in addition to the backup, replication, and recovery capabilities Rapid Recovery provides.

UEFI and ReFS support

Unified Extensible Firmware Interface (UEFI) is a replacement for Basic Input/Output System (BIOS). For Windows systems, UEFI uses the Extensible Firmware Interface (EFI) system partitions that are handled as simple FAT32 volumes.

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

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

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

Support for dynamic and basic volumes

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

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

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

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

- **Protection:** In the case when a dynamic volume spans multiple disks, you must protect those disks together to maintain the integrity of the volume.
- **Virtual export:** You can export complex dynamic volumes such as striped, mirrored, spanned, or RAID volumes from an ESXi or Hyper-V host using agentless protection. However, the volumes are exported at the disk level, with no volume parsing. For example, if exporting a dynamic volume spanned across two disks, the export will include two distinct disk volumes.

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

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

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

Support for Cluster Shared Volumes

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

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

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

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

Table 16. Rapid Recovery support for cluster-shared volumes

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

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

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

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

Rapid Recovery Core installation requirements

Install the Rapid Recovery Core on a dedicated Windows 64-bit server. Servers should not have any other applications, roles, or features installed that are not related to Rapid Recovery. As an example, do not use the Core machine to also serve as a hypervisor host (unless the server is an appropriately sized Quest DL series backup and recovery appliance).

As another example, do not use the Core server as a high-traffic web server. If possible, do not install and run Microsoft Exchange Server, SQL Server, or Microsoft SharePoint on the Core machine. If SQL Server is required on the Core machine – for example, if you are using Rapid Recovery DocRetriever for SharePoint – make sure you allocate more resources, in addition to those needed for efficient Core operations.

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

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

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

CAUTION: Quest does not support running the Rapid Recovery Core on Windows Core operating systems, which offer limited server roles. This includes all editions of Windows Server 2008 Core, Windows Server 2008 R2 Core, Windows Server 2012 Core, Windows Server 2012 R2 Core, and Windows Server 2016 Core. Excluding Windows Server 2008 Core, these Core edition operating systems are supported for running the Rapid Recovery Agent software.

NOTE: Quest does not recommend installing Rapid Recovery Core on an all-in-one server suite such as Microsoft Small Business Server or Microsoft Windows Server Essentials.

CAUTION: Quest does not recommend running the Rapid Recovery Core on the same physical machine that serves as the Hyper-V host. (This recommendation does not apply to Quest DL series of backup and recovery appliances.)

Rapid Recovery release 6.1 operating system installation and compatibility matrix

Microsoft Windows operating systems

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

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

Table 17. Rapid Recovery components and features compatible with Windows operating systems

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

Windows OS	Core/ Central Management Console	Agent	Agent-less	LMU	MR	DR	URC Restore	VM Export to Azure
Windows XP SP3	No	No	Yes	No	No	No	Yes[1]	No
Windows Vista	No	No	Yes	No	No	No	Yes[1]	No
Windows Vista SP2	No	Yes	Yes	Yes	Yes	Yes	Yes[1]	No
Windows 7	No	No	Yes	No	No	No	Yes	Yes[2]
Windows 7 SP1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes[2]
Windows 8	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes[2]
Windows 8.1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes[2]
Windows 10	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes[2]
Windows 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 18. Compatible Rapid Recovery components and features by Linux operating system

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

Windows OS	Core/ Central Management Console	Agent	Agentless
Linux OS or distribution	Agent	Agentless	Live DVD
Red Hat Enterprise Linux 6.3 - 6.8	Yes	Yes	Yes
Red Hat Enterprise Linux 7.0 - 7.3	Yes	Yes	Yes
CentOS Linux 6.3 - 6.8	Yes	Yes	Yes
CentOS Linux 7.0 - 7.3	Yes	Yes	Yes
Debian Linux 7, 8	Yes	Yes	Yes
Oracle Linux 6.3 - 6.8	Yes	Yes	Yes
Oracle Linux 7.0 - 7.3	Yes	Yes	Yes
Ubuntu Linux 12.04 LTS, 12.10	Yes	Yes	Yes
Ubuntu Linux 13.04, 13.10	Yes	Yes	Yes
Ubuntu Linux 14.04 LTS, 14.10	Yes[1]	Yes[1]	Yes[1]
Ubuntu Linux 15.04, 15.10	Yes[1]	Yes[1]	Yes[1]
Ubuntu Linux 16.04 LTS	Yes[1]	Yes[1]	Yes[1]
SUSE Linux Enterprise Server (SLES) 11 SP2 or later	Yes	Yes	Yes
SLES 12	Yes[1]	Yes[1]	Yes[1]

Linux installation and support notes:

[1] B-tree file system (BTRFS) is supported only on operating systems with kernel version 4.2. or later. Compliant operating systems currently include Ubuntu versions 14.04.4 with service pack 4 or later, and versions 15.10 or later. SLES versions 12 and 12 SP1 have older kernel versions, and so Rapid Recovery does not support their implementations of BTRFS.

Rapid Recovery Core and Central Management Console requirements

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

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

Table 19. Rapid Recovery Core and Central Management Console requirements

Requirement	Details
Operating system	The Rapid Recovery Core and Central Management Console require one of the following 64-bit Windows operating systems (OS). They do not run on 32-bit Windows systems or any Linux distribution. Rapid Recovery Core requires one of the following x64 Windows operating systems: • Microsoft Windows 7 SP1 • Microsoft Windows 8, 8.1* • Microsoft Windows 10 • Microsoft Windows Server 2008 SP2, 2008 R2 SP1 (except Core editions) • Microsoft Windows Server 2012, 2012 R2* (except Core editions) • Microsoft Windows Server 2016* (except Core editions) Windows operating systems require the .NET Framework 4.5.2 to be installed to run the Rapid Recovery Core service. Additionally, any OS marked with * requires the ASP .NET 4.5x role or feature. When installing or upgrading the Core, the installer checks for these components based on the OS of the Core server, and installs or activates them automatically if required. The Rapid Recovery Core supports all x64 editions of the Windows OS listed, unless otherwise indicated. The Rapid Recovery Core does not support Windows Server core editions. If any operating system listed specifies a service pack (for example, Windows 7 SP1), then the OS with the specified service pack is the minimum requirement. If an operating system is listed without a service pack (for example, Windows 8), then the base operating system is supported. Any subsequent SP for a listed OS is also supported, unless explicitly excluded. For optimal performance, it is recommended that you install the Rapid Recovery Core on more recent operating systems such as Windows 8.1 (or later) and Windows Server 2012 (or later).
Architecture	64-bit only
Memory	8GB RAM or more Quest highly recommends using Error Checking & Correction (ECC) memory, to ensure optimum performance of Rapid Recovery Core servers.
Processor	Quad-core or higher
Storage	Quest recommends locating your repository on direct attached storage (DAS), storage area network (SAN), or network attached storage (NAS) devices (listed in order of preference). **NOTE:** If installing on a NAS, Quest recommends limiting the repository size to 6TB. Any storage device must meet the minimum input/output requirements. See Quest knowledge base article 185962, "Sizing Rapid Recovery Deployments" for guidance in sizing your hardware, software, memory, storage, and network requirements.
Network	1 gigabit Ethernet (GbE) minimum

Requirement	Details
	NOTE: Quest recommends a 10GbE network backbone for robust environments.
Network hardware	Use network cables with the appropriate rating to obtain the expected bandwidth. **NOTE:** Quest recommends testing your network performance regularly and adjusting your hardware accordingly.

Rapid Recovery Agent software requirements

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

NOTE: The Rapid Recovery Agent cannot be deployed to a machine with a Linux operating system installed using the Add-on for Kaseya. If using that add-on, you must install the Agent on a Linux machine manually. For more information, see the *Rapid Recovery User Guide*.

Table 20. Rapid Recovery Agent software requirements

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

Requirement	Details
Operating system	The Rapid Recovery Agent software supports 32-bit and 64-bit Windows and Linux operating systems, including the following: • Microsoft Windows Vista SP2 • Microsoft Windows 7 SP1 • Microsoft Windows 8, 8.1* • Microsoft Windows 10 • Microsoft Windows Server 2008 SP2, 2008 R2 SP1 (all editions except Windows Server 2008 Core) • Microsoft Windows Server 2012, 2012 R2* • Microsoft Windows Server 2016* • Red Hat Enterprise Linux (RHEL) 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 7.0, 7.1, 7.2, 7.3 • CentOS Linux 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 7.0, 7.1, 7.2, 7.3 • Oracle Linux 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 7.0, 7.1, 7.2, 7.3 • Debian Linux 7, 8 • Ubuntu Linux 12.04 LTS, 12.10, 13.04, 13.10, 14.04 LTS, 14.10, 15.04, 15.10, 16.04 LTS • SUSE Linux Enterprise Server (SLES) 11 (SP2 and later), 12
	NOTE: Windows operating systems require the Microsoft .NET framework version 4.5.2 to be installed to run the Rapid Recovery Agent service. Operating systems listed above that are marked with * also require the ASP .NET 4.5.x role or feature. When installing or upgrading the Rapid Recovery Agent software, the installer checks for these components, and installs or activates them automatically if required.

Requirement	Details
	Additional operating systems are supported for agentless protection only. For more information, see Rapid Snap for Virtual agentless protection. If any operating system listed specifies a service pack (for example, Windows 7 SP1), then the OS with the specified service pack is the minimum requirement. If an operating system is listed without a service pack (for example, Windows 8), then the base operating system is supported. Any subsequent SP for a listed OS is also supported, unless explicitly excluded. The Rapid Recovery Agent software supports Windows Server Core edition installations for Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016. For Windows Server 2008 R2 Core only, you must have SP1 or later. Windows Server 2008 Core edition is not supported. The Rapid Recovery Agent software supports the Linux distributions included in this list. Most of the released kernel versions have been tested. File systems supported include ext2, ext3, ext4, and xfs. BTRFS is also supported (only on certain Linux operating systems with kernel version 4.2. or later). For more information, see the Rapid Recovery release 6.1 operating system installation and compatibility matrix. Agents installed on Microsoft Hyper-V Server 2012 operate in the Core edition mode of Windows Server 2012. **NOTE:** Native backup of cluster shared volumes is supported on Windows 2008 R2 (SP2 and later) protected machines only.
Architecture	32-bit or 64-bit
Memory	4GB or higher
Processor	Single processor or higher
Microsoft Exchange Server support	Microsoft Exchange Server 2007 SP1 Rollup 5 or later , Exchange Server 2010, Exchange Server 2013, or Exchange Server 2016
Microsoft SQL Server support	Microsoft SQL Server 2008 or higher
Microsoft SharePoint Server support	Microsoft SharePoint 2007, 2010, 2013, 2016 **NOTE:** Support for "SharePoint" refers to fully licensed versions of Microsoft SharePoint Server for the versions listed above.
Storage	Direct attached storage, storage area network or network attached storage
Network	1 gigabit Ethernet (GbE) minimum **NOTE:** Quest recommends a 10GbE network backbone for robust environments. Quest does not recommend protecting machines over a wide-area network (WAN). If you have multiple networked sites, Quest recommends installing a Core at each site. To share information, you can replicate between the Cores located at different sites. Replication between Cores is WAN-optimized. The data transmitted is compressed, deduplicated, and encrypted during transfer.

Requirement	Details
Network hardware	Use network cables with the appropriate rating to obtain the expected bandwidth. **NOTE:** Quest recommends testing your network performance regularly and adjusting your hardware accordingly.

Rapid Recovery Local Mount Utility software requirements

The Local Mount Utility (LMU) is included with Rapid Recovery. You can obtain the LMU installer from the **Downloads** page from either the Core Console or the Rapid Recovery License Portal.

Table 21. Local Mount Utility software requirements

Requirement	Details
Operating system	The Rapid Recovery Local Mount Utility software supports 32-bit and 64-bit Windows operating systems, including the following: • Microsoft Windows Vista SP2 • Microsoft Windows 7 SP1 • Microsoft Windows 8, 8.1* • Microsoft Windows 10 • Microsoft Windows Server 2008 SP2, 2008 R2 SP1 (all editions except Windows Server 2008 Core and Windows Server 2008 R2 Core) • Microsoft Windows Server 2012, 2012 R2* • Microsoft Windows Server 2016*
	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

Requirement	Details
	NOTE: Quest recommends a 10GbE network backbone for robust environments.
Network hardware	Use network cables with the appropriate rating to obtain the expected bandwidth. **NOTE:** Quest recommends testing your network performance regularly and adjusting your hardware accordingly.

Rapid Snap for Virtual agentless protection

The Rapid Snap for Virtual feature of Rapid Recovery lets you protect virtual machines (VMs) on specific hypervisor platforms without installing the Rapid Recovery Agent on each guest machine.

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

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

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

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

Agentless support for other operating systems

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

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

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

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

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

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

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

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

Rapid Snap for Virtual (agentless protection) support limitations

For a list of supported operating systems, see Rapid Recovery release 6.1 operating system installation and compatibility matrix. Any known limitations are included in these matrices, or as notes to the software requirements tables for the Core or the Agent, respectively. If a defect precludes the use of specific features temporarily, this information is typically reported in the release notes for any specific release. Quest strongly encourages users to review system requirements and release notes prior to installing any software version.

Quest does not fully test with unsupported operating systems. If using agentless protection to protect virtual machines with an OS not supported by the Rapid Recovery Agent software, do so at your own risk. Users are cautioned that some restrictions or limitations may apply. These restrictions may include:

- An inability to perform virtual export (one-time or continual)
- An inability to save to an archive or restore from an archive
- An inability to restore to a system volume using bare metal restore

For example, if agentlessly protecting a machine with Windows 95, attempts at virtual export to Hyper-V will fail. This failure is due to restrictions in Hyper-V support of that older operating system.

To report specific difficulties, you can contact your Quest Support representative. Reporting such difficulties lets Quest potentially include specific incompatibilities in knowledge base articles or future editions of release notes.

Hypervisor requirements

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

Using the virtual export feature of Rapid Recovery, you can perform a one-time virtual export, or define requirements for continual virtual export known as virtual standby. This process can be performed from any protected machine, physical or virtual. If a protected machine goes down, you can boot up the virtual machine to restore operations, and then perform recovery.

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

Table 22. Hypervisor requirements supporting virtual export

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

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

Requirement	Details
	NOTE: For virtual export to any Hyper-V host, .NET 4.5.2 and .NET 2.0 are required on the Hyper-V host. • First generation: ◦ Hyper-V running on Microsoft Server versions 2008 SP2, 2008 R2 SP1, 2012, 2012 R2, 2016 ◦ Hyper-V running on Microsoft Windows 8, 8.1 with Hyper-V, Windows 10 • Second generation: ◦ Hyper-V running on Microsoft Server 2012 R2, 2016 ◦ Hyper-V running on Microsoft Windows 8.1, Windows 10 **NOTE:** Only protected machines with the following Unified Extensible Firmware Interface (UEFI) operating systems support virtual export to Hyper-V second-generation hosts: • Windows 8 (UEFI) • Windows 8.1 (UEFI) • Windows Server 2012 (UEFI) • Windows Server 2012 R2 (UEFI) • Windows Server 2016 (UEFI) **NOTE:** Hyper-V export to second-generation VM can fail if the Hyper-V host does not have enough RAM allocated to perform the export. Oracle VirtualBox: • VirtualBox 4.2.18 and higher
Guest (exported) operating system	**Volumes under 2TB.** For protected volumes under 2TB, the VM (guest) can use the same supported operating systems described in the topic Rapid Recovery Agent software requirements. **Volumes over 2TB.** If you want to perform virtual export on a system for which the protected volumes exceed 2TB, use Windows 2012 R2, Windows Server 2016, VMware ESXi 5.5, or VMware ESXi 6.0. Earlier operating systems are not supported based on an inability of the host to connect to the virtual hard disk (VHD). Both Hyper-V generation 1 and generation 2 VMs are supported. **NOTE:** Not all operating systems are supported on all hypervisors.
Storage	The storage reserved on the host must be equal to or larger than the storage in the guest VMs.
Architecture	32-bit or 64-bit

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

Agentless protection is supported as described in the following table.

Table 23. Hypervisor requirements supporting agentless or host-based protection

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

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

DVM repository requirements

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

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

Quest recommends locating your repository on direct attached storage (DAS), storage area network (SAN), or network attached storage (NAS) devices. These are listed in order of preference. If installing on a NAS, Quest recommends limiting the repository size to 6TB. Any storage device must meet the minimum input/output requirements. For these requirements, and for additional guidance for sizing your hardware, software, memory, storage, and network requirements, see the *Rapid Recovery Sizing Guide* referenced below.

When creating a DVM repository, you are required to specify the repository size on a volume. Each DVM repository supports up to 4096 repository extents (additional storage volumes).

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

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

NOTE: You can generate an on-demand or scheduled report to monitor the size and health of your repository. For more information on generating a Repository report, see the topic Generating a report from the Core Console in the *Rapid Recovery User Guide*.

Always create your repository in a dedicated folder or directory, not the root folder on a volume. For example, if installing on a local path, use `D:\Repository\` instead of `D:\`. The best practice is to create separate directories for data and metadata. For example, `D:\Repository\Data` and `D:\Repository\Metadata`.

For more information on using Rapid Recovery, see the *Rapid Recovery User Guide*. For more information on managing Rapid Recovery licenses, see the *Rapid Recovery License Portal User Guide*. For more information on sizing your hardware, software, memory, storage, and network requirements, see the *Rapid Recovery Sizing Guide* referenced in knowledge base article 185962, "Sizing Rapid Recovery Deployments."

License requirements

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

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

Quest Support policy

For customers with a valid support agreement, Quest provides call-in or email support for the current major and minor release, when patched to the latest maintenance release. That release is known as N. Quest also fully supports N - 1 and N - 2. Intermediate versions receive limited support.

Quest describes its product lifecycle (PLC) support policy on its Support website (visit https://support.quest.com/rapid-recovery/, click **Policies & PLC,** and then expand **Software Product Support Lifecycle Policy**). To understand full support, limited support, and discontinued support, consult the policy referenced above.

Product licensing

To use and manage any version of Rapid Recovery, AppAssure, or Quest 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 Quest 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 Quest 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 *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 *Rapid Recovery User Guide*.

To enable a trial DL appliance license:

Each Quest 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 *Rapid Recovery User Guide*.

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

Getting started with Rapid Recovery

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

Topics include:

- Rapid Recovery Core and Agent compatibility
- Upgrade and installation instructions
- Additional resources

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 6.1.3.

Table 24. 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 6.1.2 Core	Rapid Recovery 6.1.3 Core
AppAssure 5.4.3 Agent[1]	Fully compatible	Fully compatible[2]	Fully compatible[2]	Fully compatible[2]
Rapid Recovery 6.0.2 Agent	Not compatible	Fully compatible	Fully compatible[3]	Fully compatible[2]
Rapid Recovery 6.1.2 Agent	Not compatible	Not compatible	Fully compatible	Fully compatible
Rapid Recovery 6.1.3 Agent	Not compatible	Not compatible	Not compatible	Fully compatible

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

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

The matrix shows releases that have been fully tested with this release, and represent fully supported releases, plus the most recent prior release (6.1.2). Other software versions in limited support status (such as releases 6.0.1, 6.1, and 6.1.1) have not been tested for interoperability, but are also expected to work.

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

Upgrade and installation instructions

Quest recommends users carefully read and understand the *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, Quest 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 *Rapid Recovery User Guide*.

Quest Software policy is to support two previous major/minor releases of Rapid Recovery. 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 6.1.2 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 *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 *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 *Rapid Recovery User Guide*.
- For complete details on licensing, see the *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 *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 *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
- 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 requires the Microsoft .NET 4.5.2 Framework. 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 are in English only.
- The Rapid Recovery Add-On for Kaseya is in English only.
- Technical product documentation for this release is in English only, except for Release Notes, which are available in all of the languages listed above.

About us

We are more than just a name

We are on a quest to make your information technology work harder for you. That is why we build community-driven software solutions that help you spend less time on IT administration and more time on business innovation. We help you modernize your data center, get you to the cloud quicker and provide the expertise, security and accessibility you need to grow your data-driven business. Combined with Quest's invitation to the global community to be a part of its innovation, and our firm commitment to ensuring customer satisfaction, we continue to deliver solutions that have a real impact on our customers today and leave a legacy we are proud of. We are challenging the status quo by transforming into a new software company. And as your partner, we work tirelessly to make sure your information technology is designed for you and by you. This is our mission, and we are in this together. Welcome to a new Quest. You are invited to Join the Innovation™.

Our brand, our vision. Together.

Our logo reflects our story: innovation, community and support. An important part of this story begins with the letter Q. It is a perfect circle, representing our commitment to technological precision and strength. The space in the Q itself symbolizes our need to add the missing piece — you — to the community, to the new Quest.

Contacting Quest

For sales or other inquiries, visit https://www.quest.com/contact.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request.
- View Knowledge Base articles.
- Sign up for product notifications.
- Download software and technical documentation.
- View how-to videos.
- Engage in community discussions.
- Chat with support engineers online.
- View services to assist you with our product

MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc., Attn: LEGAL Dept., 4 Polaris Way, Alisa Viejo, CA 92656.

Refer to our website (https://www.quest.com) for regional and international office information

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at https://www.quest.com/legal.

Trademarks

Quest, the Quest logo, and Join the Innovation are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit https://www.quest.com/legal/trademark-information.aspx. All other trademarks and registered trademarks are property of their respective owners.

Legend

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

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

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