Rapid Recovery 6.3 Release Notes

May 2019

These release notes provide information about the Rapid Recovery release, build 6.3.0.5309.

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, Oracle Database 12c, Microsoft Exchange, and Microsoft SharePoint. Using Rapid Recovery, you can continuously back up and protect all your critical data and applications from a single web-based management console.

Rapid Recovery 6.3 is a minor release, with new features and functionality. See New features and Enhancements for details.

NOTE: For more information about how major, minor, and maintenance releases are differentiated, see Rapid Recovery release designations.

Some features, previously integrated software tools, or platforms are no longer supported. For more information on these items, see Deprecated features.

As a minor release, defect fixes and known issues listed in this document are not cumulative.

For information relevant for any other release, please see the edition of release notes specific to that release on the Quest technical documentation website.

Topics in this section include:

Double license consumption corrected for release 6.3

Rapid Recovery Core consumes one license from your license pool per central processor unit (CPU) socket, or one per machine protected by Rapid Recovery Agent. In the past (as represented by Rapid Recovery License Portal defect 6682), if protecting the same hypervisor in 2 Cores, twice the number of licenses were consumed.

If you protect guest VMs from the same VMware host in two separate Rapid Recovery 6.3 Cores, only a single set of licenses from your license pool (one per socket) are now consumed. This improvement in license consumption assumes the following:

- Both Cores are part of the same Rapid Recovery License Portal group
- Both Cores are running Rapid Recovery Core release 6.3.0 or later

If your business needs require you to protect the same VMware host in 2 separate Cores in the same license portal group, and want to reduce your license consumption, then Quest recommends upgrading both Cores to release 6.3.

Portal rebranding advisory

The QorePortal is the new name for the web portal formerly called the Quest Data Protection Portal.

The QorePortal is a web-based portal that lets organizations monitor and manage multiple Rapid Recovery Cores and protected machines from a single interface. You can monitor tasks and events, view repository status, monitor commands and system health, generate reports that span multiple Cores, and download Rapid Recovery software. QorePortal is integrated with the Rapid Recovery License Portal and vFoglight.

Licensed users of Rapid Recovery can access the QorePortal using the web address https://qoreportal.quest.com/.

Repository upgrade advisory

Upgrading the Core software to release 6.3 from any earlier version (for example, Rapid Recovery 6.2.x, 6.1.x, 6.0x, or AppAssure 5.x) changes the structure of your DVM repository. The updates let you use new features in the latest release, such as application support for Oracle Database 12c, agentless protection, and so on.

After you change the structure of your DVM 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 uninstall the new version, re-install the older version, and then re-import the information manually from the archive, which can be a substantial effort.

Automatic Update advisory

If upgrading from Rapid Recovery release 6.2 or later, you can use the Automatic Update feature to upgrade to this release, if it is enabled in your Core. Use of this feature requires you to consent to Quest using a limited amount of your personal data. For more details, see the topic "How Rapid Recovery uses personal information" in the *Rapid Recovery 6.3 User Guide*.

Due to parameters included as part of GDPR compliance in Rapid Recovery release 6.2 and later, customers using Rapid Recovery versions prior to 6.2 will not be able to use the Automatic Update feature to upgrade. You must manually upgrade the software one time instead. Once you have upgraded to Rapid Recovery release 6.2 or later and consented to the use of personal data, you can resume using the Automatic Upgrade feature.

Replication conflicts with agentlessly protected virtual machines on SMB shares

In specific cases, users cannot set up replication between 6.1.3 and 6.3 Cores. Users attempting to establish replication from a source Core running Rapid Recovery Core 6.1.3 to a target Core running version 6.2.0 or higher will fail if the target Core has recovery points from an agentlessly protected machine that had shared VHDX disks placed on a network shared volume using the Server Message Block (SMB) protocol.

If using such a configuration, all attempts to set up replication will fail (not only protection of agentless VMs). At this time, Quest does not expect to backport a fix. To resolve, upgrade your source Core to release 6.2.0 or later.

Content differences between context-sensitive help and technical documentation

Rapid Recovery Core includes in-product context-sensitive help. Help topics are derived from the *Rapid Recovery 6.3 User Guide*. To view help topics in a web browser, from the Rapid Recovery Core Console, click Help or , and from the resulting drop-down menu, select **Help**.

Due to publication schedules, sometimes there are content differences between content in the in-product help and in the *User Guide*, with the latter document being the most recent. In such cases, these differences are typically documented in the Documentation section of the Known issues topic.

Since Rapid Recovery release 6.2, the "REST APIs" appendix appears only in the HTML and PDF versions of the *User Guide*. This topic, which describes how to download and work with Rapid Recovery REST APIs, does not appear in context-sensitive help. Likewise, as in previous releases, the help topic "Third-party contributions" appears only in context-sensitive help, or from the **About** menu. This topic does not appear in HTML or PDF versions of the *User Guide*.

Rapid Recovery release designations

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

- **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 numeral following the first decimal point. If this number is greater than 0, it is part of a minor release. 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 numeral following the second decimal point. If this number is greater than 0, it is a maintenance release. Maintenance releases correct previously identified defects or behaviors. Maintenance releases may also reflect changes (additions and deprecations) in supported operating system or application platforms.
- **Build numbers** (typically between 3 and 5 digits) are specified by the fourth set of numerals. This part is used to differentiate versions of the software program generated during the development process.
    - For the 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 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.
    - Difference in build numbers does not affect replication when the target Core has the same or a more recent build installed than the source Core.

The release designation for this release, 6.3.0.5309, therefore represents the following: The first digit shows this version as part of the 6.x major release. The digit after the first point (3) shows this release as the fourth minor version in 6.x. The 0 after the second point shows this is the first generally available release within 6.3 (a 1 or higher would signify a maintenance release). Finally, the build number identifies the release down to the lowest level and is generally only referenced in release notes.

Support policy

Quest policy is to provide technical support to customers with an active maintenance agreement for specific current software versions.

Customers should familiarize themselves with Quest product life cycle support policies. These policies, listed on the Quest Support website, apply across the board to all the Quest products.

A primary component of the policy is Quest's commitment to support the current software version (N) and the prior version (N-1). Support is offered at varying service levels, including full, limited, and discontinued support. The website also describes an option for continuing support, and descriptions of each service level.

To see Quest general product life cycle support policies, view the Support website as follows:

1. Navigate to https://support.quest.com/rapid-recovery/.
2. Click **Product Life Cycle & Policies**.

3. Scroll down to the **Product Support Policies** heading and expand the link **Product Support Life Cycle Policy**.
   This content details the Quest-wide N-1 product support life cycle policy. It describes aspects of full, limited, and discontinued support levels and describes an option for continuing support.

Some products—including Rapid Recovery—offer higher support levels and commitments than the generic Quest product support life cycle. For more information, see Differentiation between standard Quest and Rapid Recovery service levels.

Differentiation between standard Quest and Rapid Recovery service levels

Quest Data Protection Support is committed to providing customers that have a current maintenance contract with assistance and advice for supported releases.

Quest strives to put resources behind the most recent product releases so that we can continually improve and enhance the value of our solutions. As new versions are released, interoperability testing is conducted only between those new versions and the releases that will be in full or limited support when the new version becomes generally available. Other versions are no longer tested, even if they are expected to be interoperable.

At a minimum, Quest commits company-wide to supporting the current software version (N) and the prior version (N-1). Rapid Recovery customers with an active maintenance agreement are entitled to higher service levels from Quest Data Protection Support under the following terms:

- Rapid Recovery software versions supported follow the **N-2 policy**.
  - **N** represents the major and minor release numbers (for example, 6.3, 6.2, 6.1, 6.0, 5.4) of the most recent generally available software release. For more information about parsing a Rapid Recovery release number, see Rapid Recovery release designations.
  - **N - 1** refers to the most recent prior release, considering major and minor versions only. For example, in release 6.3, N-1 refers to release 6.2.
  - **N - 2** refers to the penultimate major/minor release. For example, in release 6.3, N-2 refers to release 6.1.
- For each release, some versions are eligible for full support; some for limited support; and for some versions, support is discontinued.
  - The current version (N) and the most recent maintenance release (N-1) are fully supported.
  - For N-2 (6.1), the latest maintenance release (6.1.3) is in limited support. Patches or fixes are not written for releases in limited support; however, once identified and confirmed, software defects can be expected to be corrected in the most recent version of the software.
  - Support for all other versions is discontinued. Support for earlier maintenance releases is discontinued because viable, easy-to-upgrade alternatives are available. For example, users of release 6.2.0 can upgrade directly to release 6.2.1, which is fully supported. Users of 6.1.1 or 6.1.2 can upgrade to 6.1.3 (in limited support) or to 6.2.1 (in full support).
- Limited support can be offered to other versions by exception. As of the date of publication, no Rapid Recovery releases currently are supported by exception.

If you are using a release that is in limited support and you request assistance from Quest Data Protection Support, you may be asked to upgrade. If you are using a release in discontinued support, you will first be asked to upgrade.

For each product on the Quest Support website, in the Product Life Cycle section, you can view a chart showing recent software versions, and the service levels and dates applicable to those service levels. For example, to see Rapid Recovery- specific product life cycle support information, do the following:

1. Navigate to https://support.quest.com/rapid-recovery/.
2. Click **Product Life Cycle & Policies**.
   The resulting matrix shows the product-specific list of supported releases. For example, dates are included for each Rapid Recovery release to specify the support status (full, limited, or discontinued) for each release shown.

New features

The following new features have been added to Rapid Recovery in release 6.3, or were not previously documented in earlier releases.

Rapid Recovery support for Azure Stack

As of release 6.2, Quest Rapid Recovery supports Azure Stack. It is available in the Azure Marketplace items available for Azure Stack listed under "Quest Rapid Recovery Core."

Azure Stack is Microsoft's proprietary answer to the open source OpenStack platform. Essentially, Azure Stack is a hybrid cloud software solution (based on the Azure cloud platform) that organizations can use in their own data centers. In other words, it is an on-premises cloud service instead of a service hosted in Microsoft's cloud. In practice, users could seamlessly move from their private cloud to the Azure public cloud if needed.

Azure and Azure Stack share a standardized architecture, including the same portal, a unified application model, and common tools.

Support for Azure Resource Manager, Core cloud account types, and Azure storage accounts

For some time, Microsoft supported two sets of APIs: the original Azure deployment technology, Azure Service Management (ASM, known as the Classic deployment model), and its replacement, Azure Resource Manager (ARM). New to Rapid Recovery in this release is support for ARM.

When using ARM with Rapid Recovery, additional steps are required for your Azure account. These prerequisites are fully addressed in the topic "Before virtual export to Azure" in the *Rapid Recovery 6.3 User Guide*.

Microsoft announced that support for ASM is retired as of June 30, 2018. Accordingly, in release 6.3, Rapid Recovery no longer supports ASM for virtual export. Instead, Rapid Recovery virtual export to Azure exclusively supports ARM.

Rapid Recovery Core also includes the ability to archive recovery points to Azure. For both virtual export to Azure and archiving to Azure, you must first create a cloud account in the Rapid Recovery Core Console to connect your Core and Azure accounts. In this release, cloud account requirements differ for these two functions.

Virtual export to Azure

When setting up an Azure cloud account in Rapid Recovery Core release 6.3 for use with virtual export to Azure, select the cloud account type **Microsoft Azure Resource Management (for Virtual Export)**.

Customers already using virtual export to Azure before upgrade to this release are advised to remove the Rapid Recovery virtual exports from their Azure accounts and perform fresh virtual exports after upgrading to release 6.3.

For more information about performing one-time or continual virtual export to Azure, see the *Rapid Recovery 6.3 User Guide*.

Archive to Azure

When setting up an Azure cloud account in Rapid Recovery Core release 6.3 for use with archiving recovery points to Azure, select the cloud account type **Microsoft Azure (for Archive)**.

NOTE: In previous releases, this cloud type was simply called **Microsoft Azure**.

For more information about archiving recovery points (on demand or continually, based on a schedule), see the *Rapid Recovery 6.3 User Guide*.

Azure storage account types

Azure supports storage accounts created using ARM. When viewing these storage accounts in Azure, the account type shown in the Azure GUI is simply **Storage account**. This is the recommended storage account type.

At the time of publication, Azure continues to support storage accounts created using ASM. When viewing these storage accounts in Azure, the account type shown in the Azure GUI is **Storage account (classic)**. Note that you can no longer create a classic storage account using ASM.

When performing archive to Azure in this release, you can use storage accounts created using either deployment method, ARM or ASM, as long as the cloud account type is **Microsoft Azure (for Archive)**.

However, the use of classic Azure storage accounts in Rapid Recovery Core is deprecated, and support in Rapid Recovery Core is expected to be removed in a future release. As a best practice, Quest recommends creating storage accounts using ARM and using this fully supported storage account type for both virtual export and archiving recovery points. For more details in these Release Notes, see Azure Service Management features deprecated.

For more information about Microsoft ending support for ASM, please see Microsoft blogs, knowledge base articles, and online Azure documentation, including the following:

- Microsoft's blog post: Deprecating Service Management APIs support for Azure App Services
- MSDN Q&A topic: Will removing Support to ASM on June 30 2018 also mean that a Cloud Service (Classic) cannot be deployed through PowerShell commands?

Credentials Vault

Credentials Vault is a new Rapid Recovery usability feature that manages account login credentials used within the Rapid Recovery Core Console.

When performing operations such as adding a machine or cluster to protection, setting up virtual export or replication, connecting to a repository, archiving or restoring archived recovery points, and so on, you are prompted to enter account credentials. For each account, credentials include the user name, password, and a description parameter where you can identify the account. After you enter your credentials, if you choose to, you can add them to the Credentials Vault.

Thereafter, the next time you want to perform an operation in the Core Console that uses the same account, instead of manually entering your user name and password, you can select the account from a drop-down menu.

The Credentials Vault simplifies management of your passwords. For example, if your organization has a security policy mandating password changes at frequent intervals, one visit to the Credentials Vault page can let you easily update your password for each user account accessed from the Rapid Recovery Core Console.

The Credentials Vault is unobtrusive. Sections of the Core Console UI that are enabled for the Credentials Vault include a **+** sign next to the **User name** text box when prompted for credentials. When you place your cursor over it, you see a hint that reads "Save account to Credentials Vault." To add an account to the vault, click the **+** sign to open the *Add New Account* dialog box, then enter the user name, password, and a meaningful text description. Then click **OK** to save the account to the vault.

NOTE: Unlike most descriptions, the text you enter describing each account in the Credentials Vault is functional. Passwords, once entered into the vault, are not displayed. Thus, the combination of the user name and this description uniquely identifies each account in the vault. This value can later be edited.

After accounts have been added to the Credentials Vault, when prompted to authenticate, you can view the list of accounts and select an account with one click, rather than manually entering your account user name and password.

From a location on the Rapid Recovery Core Console in which you are asked for credentials, click the downward-facing arrow in the **User name** text box. The view expands to show a drop-down grid, with each row representing one account in the Credentials Vault.

Scroll through the list to identify the account for which you want to enter credentials. Then click on the row for the appropriate account.

The Credentials Vault drop-down grid appears. Each row shows the user name and description associated with an account held in the vault. The grid closes, and the account information is passed to the window or dialog box. Since passwords are hidden, the password parameter is not shown.

From the Rapid Recovery Core Console, you can also view and manage all accounts in the vault. From the More menu, select **Credentials Vault.** The *Credentials Vault* page appears. For each account, the user name, description, and utilization appears. You can do the following:

- Click in any row to select that account. From the last row, click More and then select **Edit** to update the user name, refresh the password, or edit the text description.

- To merge two accounts, select an account, click More and then select **Merge to account**. From the **Target account** text box, select the other account with which you want to merge this account record, and then click **Merge**.
- To remove an account from the Credentials Vault, click More and then select **Remove**.

Rapid Recovery encrypts credentials in the vault using the Microsoft Data Protection API (DPAPI) using local machine scope.

For detailed information about this feature, including step-by-step procedures, see the "Credentials Vault" section of the *Rapid Recovery 6.3 User Guide*.

Active Block Mapping

Active Block Mapping (ABM) is a feature developed to optimize image-based data protection by keeping inactive blocks out of managed images. This addition brings critical performance advantages for capturing incremental backups (specifically for virtual machines).

While not available on the Core, ABM can be configured on two levels as follows:

- **Protected VM container (hypervisor level)**. On this level, the user can specify settings to be applied by default for all protected VMs within the container.
- **Individual VM level.** You can override default settings for any individual virtual machine.

ABM is implemented as a query to the volume's file system header (MFT for NTFS), which returns a list of active blocks in the image. ABM can be used by itself to read only active blocks from a VM during a backup process. ABM can also be combined with Changed Block Tracking (CBT) to read only active and changed blocks when capturing incremental backups specifically of virtual machines.

Implementation is based on the integration with DiskUtils library, which is already used within the Core for multiple features including Agentless protection of ESXi and Hyper-V VMs.

VMware VM configuration backup and restore

Rapid Recovery Core release 6.3 introduces a new feature, the ability to back up and restore VMware VM configurations, including the option to include VM configurations during virtual export to VMware/ESXi virtual machines.

Backup. Rapid Recovery Core release 6.3 and later automatically saves agentlessly protected ESXi virtual machine configurations in each volume image when snapshots are captured. VMware virtual machine configurations are stored in .vmx files (and related BIOS settings are stored in .nvram files). The relevant files are saved in the custom metadata for each relevant VM volume, and includes hypervisor version information to ensure compatibility.

Restore. Optionally, when restoring data from a recovery point of an agentlessly protected ESXi machine, you can choose whether to include in the VM all VM configurations and data, or only the data. This choice is presented in the UI through the **Restore all configuration data** check box. This option appears only for VMware machines protected agentlessly (replacing the **Show advanced options** check box that is relevant only for machines protected by Rapid Recovery Agent). When the option is selected, all VM configurations for volumes being recovered are restored. When the option is cleared, only data (and not VM configurations) are restored for those volumes.

Virtual export. Optionally, when performing virtual export from a recovery point of an agentlessly protected ESXi machine to VMware/ESXi, you can choose whether to export all VM configurations and data, or export only the data. This choice is presented in the UI through the **Restore all configuration data** check box. This option

appears only for agentlessly protected ESXi machines. When the option is selected, all VM configurations for volumes being exported to a VM are included in the exported VM. When the option is cleared, only data (and not VM configurations) are included in the exported VM.

Based on the restore or virtual export type, The **Restore all configuration data** option is selected by default in the following situations:

- When restoring data or performing virtual export from a recovery point to the same agentless virtual machine.
- When performing virtual export to a different server .There is no backward compatibility between hypervisor versions.

Otherwise, the **Restore all configuration data** option is not selected by default, although you can change the default option by selecting or clearing this setting.

Improved Linux suport for BMR of LVM and software-based RAID volumes

Logical Volume Management (LVM) and software-based Redundant Array of Independent Disks (RAID) are complex virtual volume types, similar in nature to spanned or striped complex Windows volumes. These volume types can be composed from different parts of other disks and partitions.

You can continue to protect machines running supported Linux distributions in the Rapid Recovery Core, both using Rapid Recovery Agent, and agentlessly using Rapid Snap for Virtual.

Rapid Recovery release 6.3 expands bare metal restore (BMR) support of protected Linux machines. In previous versions, if you wanted to perform BMR of a Linux machine using automatic volume mapping, and if the volumes on the original protected Linux machine contained LVM volumes or software-based RAID volumes, the restore produced simple volumes instead of LVM or RAID volumes. Now, if you specify automatic volume mapping, the restored volumes will automatically be created, matching the volumes from your recovery point to the appropriate virtual volumes on the BMR target machine. This new capability includes LVM volumes and RAIDs; LVMs and RAIDs with partitions; and complex LVMs and RAIDs.

NOTE: These complex Linux volume types are supported only when using automatic volume mapping.

Supported LVM types include linear, striped, mirrored, RAID1, thin, ThinPool.

For RAID volumes, Rapid Recovery supports Common RAID Disk Data Format (DDF). Supported RAID types include linear, striped, mirrored, RAID4, RAID5, RAID6, and RAID10.

Support for restore of software RAIDs on Linux machines

If you have a software RAID on a Linux machine protected by Rapid Recovery Agent, you can restore the software RAID from a recovery point.

NOTE: This feature, not previously documented, was introduced in Rapid Recovery Agent release 6.2.1 and is not compatible for snapshots taken using earlier Agent versions. If you upgrade Linux machines with software RAIDS to Rapid Recovery Agent release 6.2.1 or later and then capture snapshots in your Rapid Recovery Core, you can thereafter restore the software RAID from the new snapshots.

This is a feature unique to Rapid Recovery Agent on Linux machines and is not available to agentlessly protected software RAIDs.

Managing virtual environments from your Core

With Quest's departure from manufacturing or supporting new hardware-based appliances that run Rapid Recovery Core, some appliance-like features have been ported to the Rapid Recovery Core software to increase our customers' ability to integrate with hypervisors and their guest VMs.

If your Core is installed on a Hyper-V or vCenter/ESXi virtual machine, you have access to a new *Virtual Environments* page, accessible from the ••• (More) menu on the icon bar.

If protecting Hyper-V or vCenter/ESXi hosts or virtual machines in your Core, you can now perform the following tasks from the new *Virtual Environments* page:

- **Manage hypervisor credentials.** On the *Virtual Storage* sub-page, you can manage the credentials for Hyper-V or vCenter/ESXi hypervisor hosts added to or protected on your Core. If you add a hypervisor host and enter your credentials, Rapid Recovery caches them for future use.
- **Manage hypervisor host storage locations.** You can add, edit, or remove storage locations for hypervisor hosts added to your Core.
- **Monitor virtual disks.** From the *Attached Disk*s sub-page, you can view and monitor all virtual disks currently attached to the virtual machine, including the subset of disks not specifically defined as storage locations in the *Virtual Storage* sub-page.

  NOTE: For this reason, the number of disks listed on the *Attached Disks* sub-page may exceed the number of volumes shown on the *Virtual Storage* sub-page.
- **Define repositories or volumes.** On the *Provisioning* sub-page, you can create a new repository for your Hyper-V or ESXi protected machines. You can also add an empty volume for your virtual environments.

  NOTE: Creation of either a repository or a virtual volume requires a storage location to be defined on the *Virtual Storag*e sub-age as a prerequisite.

Enhancements

The following enhancements have been added to Rapid Recovery 6.3, or were not previously documented in earlier releases.

Support for Windows Server 2019

Rapid Recovery release 6.3 supports Windows Server 2019, except for volumes using the using Resilient File System (ReFS).

Rapid Recovery users can protect, restore, and export Windows 2019 servers and clusters.

NOTE: Following our standards, the operating system on the Core must be greater than or equal to the OS version on protected machines, for both Agent-based and agentless protection. For more information, see the *Rapid Recovery 6.3 Release Notes* topic "Rapid Recovery Core and Agent compatibility."

Rapid Recovery does not support ReFS volumes on Windows Server 2019. Because ReFS is not supported, Rapid Recovery release 6.3 does not allow protection of ReFS volumes on Windows Server 2019 machines. If you upgrade an already-protected machine to Windows Server 2019, Quest recommends removing ReFS volumes from protection.

Reporting changes

A new report, the Core Nostalgia Report, was introduced in Rapid Recovery Core release 6.2.0.

In release 6.3, this report has been renamed the Classic Summary Report, to more accurately reflect the information depicted in the report. For more information on this report, see the following topics in the *Rapid Recovery 6.3 User Guide*:

- For information about the information included in this report, see "Understanding the Classic Summary Report."
- For information about generating this or any Rapid Recovery report one time on demand, see "Generating a Core report on demand."
- For information about generating this or any Rapid Recovery report repeatedly on a schedule you define, see"Managing scheduled reports from the Core Console."

No other changes to reporting were introduced in this release.

Support for SQL Server 2017

Rapid Recovery now supports SQL Server 2017. You can protect a SQL Server with Rapid Recovery Agent or agentlessly, taking advantage of application support such as truncating SQL logs (identifying available space on the protected server) and performing SQL attachability checks (verifying the integrity of recovery points containing SQL databases, and ensuring that all supporting data and log files are available in the backup snapshot).

For more information about recent support changes for SQL Server software with Rapid Recovery, see SQL Server support changes.

Limited support for live migration

Live migration is a Hyper-V feature of Windows Server which lets users move running VMs from one Hyper-V host to another with no visible downtime. This provides flexibility to hypervisor administrators in managing VMs.

This feature is included in Windows Server OS from Windows Server 2008 R2 and later versions. Windows Server 2016 is the first OS to support this feature without failover clustering.

Live migration is a Hyper-V feature of Windows Server which lets users move running VMs from one Hyper-V host to another. Rapid Recovery supports Hyper-V live migration when moving VMs between nodes in a cluster. Live migration between separate hosts (a Hyper-V 2016 feature) is not supported with Rapid Recovery.

If using Rapid Snap for Virtual agentless protection, a supported version of Rapid Recovery Agent must be installed on the Hyper-V host. If using agent-based protection, Rapid Recovery Agent must be installed on each node in a protected Hyper-V cluster, but is not required on the host.

Improvements in mounts for Core and LMU

Rapid Recovery Core captures snapshots from volumes on machines protected in the Core, and saves them in the designated repository as recovery points. From the Rapid Recovery Core Console (or using the Local Mount Utility), you can browse recovery points, and choose to mount one in the Core.

You can browse through the data in a mounted recovery point (also referred to as simply a "mount"). For example, you can recover individual files, or use the mount as a source for a restore action (such as restoring whole volumes). When viewing a mount, you can restore in place (to the original machine location, or to bare metal.

Historically, Rapid Recovery assigned a physical address (such as `C:\mounts\backup1vol2`) for each mount, from which you can access the data.

As of Rapid Recovery 6.3, when mounting a recovery point (whether from the Rapid Recovery Core Console or using the LMU), you can choose to assign an as-yet unreserved drive letter (such as `f:\`) to the mount instead of a physical address.

This new functionality is also supported by PowerShell and Command Line commands. An example of the usefulness of this feature is when mounting using the command line, since there is no longer a need to verify in advance which volumes are available.

NOTE: For more information on these commands, see the latest edition of the *Rapid Recovery Commands and Scripting Reference Guide*.

Deprecated features

The following is a list of features that are no longer supported starting with Rapid Recovery 6.3.

Rapid Recovery support for Exchange Server 2007 is deprecated

In April of 2017, Microsoft Exchange Server 2007 reached end of life. Microsoft no longer supports that version of Exchange Server.

Accordingly, Rapid Recovery support of Exchange Server 2007 is deprecated.

- Exchange Server 2007 is not supported by Rapid Recovery release 6.3.
- Customers with a current maintenance agreement using supported prior versions of Rapid Recovery (as of General Availability for release 6.3, these include releases 6.1.3 and 6.2.1) are entitled to limited support for Exchange Server. If customers encounter issues, Quest Data Protection Support will apply their best effort to provide known work-arounds or fixes. However, no coding effort will be applied to issues discovered in Exchange Server 2007 in relation to our software.

Quest recommends migrating to newer, supported versions of Exchange if you want to continue protecting your data using Rapid Recovery.

Tiering recovery points to the DR appliance deprecated and not supported in release 6.3

A tiering repository is a secondary repository (located on a DR Series deduplication appliance) defined on your Core into which recovery points in Rapid Recovery Core versions 6.1.x and 6.2.x were relocated from a primary DVM repository.

NOTE: In release 6.2, tiering was only supported on DR Series deduplication appliances running OS 4.0.

Recovery points are deleted from your primary DVM repository after they are moved. The Core continued to manage the relocated recovery points until they were eventually rolled up and deleted.

As indicated previously, the tiering feature is discontinued and is no longer supported by Rapid Recovery Core.

Rapid Recovery customers who want to continue tiering must remain on Rapid Recovery Core version 6.2.1 or 6.1.3. These customers cannot take advantage of new features of Rapid Recovery Core or Agent.

Azure Service Management features deprecated

Microsoft announced that support for Azure Service Management (ASM) is retired as of June 30, 2018.

Accordingly, in release 6.3, Rapid Recovery no longer supports ASM for virtual export. Instead, Rapid Recovery virtual export to Azure exclusively supports Azure Resource Manager (ARM). When setting up a cloud type for your Azure account, use cloud type **Microsoft Azure Resource Manager (Virtual Export)**.

NOTE: When using ARM with Rapid Recovery, additional steps are required for your Azure account. These prerequisites are fully addressed in the topic "Before virtual export to Azure" in the *Rapid Recovery 6.3 User Guide*.

When archiving recovery points to Azure in Rapid Recovery release 6.3, you can use Azure storage accounts created using either ARM or ASM, as long as the Rapid Recovery cloud account type is **Microsoft Azure (for Archive)**.

However, the use of classic Azure storage accounts in Rapid Recovery Core is deprecated, and support in Rapid Recovery Core is expected to be removed in a future release. As a best practice, Quest recommends creating storage accounts using ARM and using this fully supported storage account type for both virtual export and archiving recovery points.

You are no longer required to associate Azure management certificates with your Rapid Recovery Core, or to refresh or delete them. You are also no longer required to obtain or load your Azure Publish Settings File. These setup steps were required exclusively for configuring ASM with your Core.

Correspondingly, the following topics have been removed from the *Rapid Recovery 6.3 User Guide*:

- Working with Azure management certificates associated with your Core
- Obtaining the Publish Settings file for your Azure account
- Loading an Azure management certificate
- Refreshing or deleting Azure management certificates

For more details in these Release Notes, see Support for Azure Resource Manager, Core cloud account types, and Azure storage accounts.

SQL Server support changes

Rapid Recovery customers are advised of the following changes in support for SQL Server.

- Support for SQL Server 2005 is discontinued
- Support for SQL Server 2008 and 2008 R2 is deprecated

Support for SQL Server 2005 is discontinued

In April of 2017, Microsoft SQL Server 2005 reached end of life. Microsoft no longer supports that version of Exchange Server..

Accordingly, Rapid Recovery support of Exchange 2007 is deprecated. As indicated in *Rapid Recovery 6.2.1 Release Notes*, customers are reminded that Rapid Recovery no longer supports SQL Server 2005. References to this version of SQL Server are removed from documentation in this release.

Support for SQL Server 2008 and 2008 R2 is deprecated

Mainstream support by Microsoft for SQL Server 2008 and SQL Server 2008 R2 ended on July 8, 2014. Extended support by Microsoft for these versions ends in July of 2019.

Customers are advised that support in Rapid Recovery for SQL Server 2008 and 2008 R2 is deprecated. In a future release of Rapid Recovery Core (after July 2019), support for these versions of SQL Server will be removed. Notification is provided so that customers can plan in advance accordingly.

Quest recommends migrating to newer, supported versions of SQL Server if you want to continue protecting your data using Rapid Recovery.

Resolved issues

This topic contains resolved issues in the following categories:

- Core and Windows resolved issues
- DL appliance resolved issues
- Documentation resolved issues
- Linux resolved issues

The following is a list of issues addressed in this release.

Table 1: Core and Windows resolved issues

Issue ID	Resolved Issue Description	Functional Area
6682	Double license consumption corrected for release 6.3. Rapid Recovery Core consumes one license from your license pool per processor or CPU socket. In earlier releases, if protecting the same hypervisor in 2 Cores, twice the number of	License consumption

Issue ID	Resolved Issue Description	Functional Area
	licenses were consumed. Now, if you protect guest VMs from the same VMware host in two separate Rapid Recovery6.3 Cores, only a single set of licenses from your license pool (one per socket) are consumed. Requirements: Both Cores must be part of the same Rapid Recovery License Portal group and both Cores must be version 6.3.0 or greater.	
108313	Upgrade, Deploy and other web-installer dependent jobs were failing due error code: 3002. Message: "The certificate for MSI issued to Quest Software Inc is invalid."	Installer
108264	Partial backup data was not deleted from repository after failed transfer.	Repository
108098	Mount for recovery points from attached archive failed with error: 'The index xxxxxx is greater than the maximum valid index, which is one less than the capacity yyyyyy' if the volume had been shrunk.	Mounts, Archive
108085	When Core service was not shut cleanly and an archive was attached, the GUI did not load, with error "Oops.. Looks like something went completely wrong."	Core service, Archive
108064	Agent protection failed with error "GetResponse timed out (stuck on collecting metadata)" on specific environment.	Core service, Archive
108006	In a specific environment, when a scheduled archive was canceled and the incomplete archive deleted, the next scheduled archive did not include the deleted recovery points, and the resulting archive could not be imported. To correct this issue, the archive structure is refreshed after a scheduled archive is canceled, and subsequent archives are valid.	Scheduled archive
107976	Scheduled archives failed, with error "Value cannot be null. Parameter name: source" after upgrade from 6.1.3 to 6.2.x.	Scheduled archive, Upgrade
107971	Core service hung; GUI did not load, with error "Oops.. Looks like something went completely wrong" in specific cases.	Core service
107941	Replication rate for huge base images were extremely slow due to small write buffer size on the target Core.	Replication
107933	Archive to the Amazon Glacier failed after minor network interruption due to the absence of retry logic that has subsequently been added.	Archive to Amazon Glacier
107785	There was no ability to archive cluster nodes without adding cluster volumes to an archive.	Archive, Clusters
107768	Rollup failed with error "cannot find the recovery point with the id __" on a system test environment.	Rollup

Issue ID	Resolved Issue Description	Functional Area
107764	No virtual machines were displayed on the Virtual Machines page of a protected vCenter/ESXi server when a protected VM with Agent installed was added for agentless protection, and the VM was associated with its parent host.	Protection of ESXi. Linking
107568	Data was lost on disk located on Scale Out File Server (SOFS) if you added some data to the disk and evicted active SOFS cluster node.	Hyper-V, agentless protection, clusters
106296	Unexpected base images occurred for cloned disks during Hyper-v agentless transfers.	Hyper-V, agentless protection
105606	Replication was not paused after upgrading Target Core from release 5.4.3 to release 6.2.x.	Replication
105560	Not all disks were exported after VirtualBox export of ESXi agentless VM based on Windows 8.1 x86 and Windows 8.1 x64.	Virtual exports
103783	Core GUI would not launch after upgrade from 6.1.1 to 6.1.2 on specific environment.	Core Console
102521	Azure Market Place Offer used "dell_software" in the URI.	Azure
102321	Core GUI hung for Agent Settings page when maintaining repository was in progress.	Repository, Maintenance Job, GUI

Table 2: DL appliance resolved issues

Issue ID	Resolved Issue Description	Functional Area
107303	Retention policy settings became disabled on DL1000 and DL1300 after upgrade to 6.2.0.	Retention policy

Table 3: Documentation resolved issues

Issue ID	Resolved Issue Description	Functional Area
N/A	License and copyright information for the following components (missing from release 6.2 in-product help) appears as expected in the Rapid Recovery Core in-product help topic "Third-party components": • ANTLR 3.3.3 • bash-completion 2.1	Third-party components, licensing, copyright

Issue ID	Resolved Issue Description	Functional Area
	• btrfs-tools 4.4.1 • ca-certificates 2016.10.04 • casper 1.376 • Castle Windsdor 2.5.3 • Chromium 57 • cURL 7.47 • docutils 0.14 • efibootmgr 0.12-4 • fakeroot 1.20.2 • gcc 5.3.1 • gdisk 1.0.1 • Google APIs Client Library for .NET 1.32.2 • htop 2.0.1-1 • JavaScriptEngineSwitcher 2.4.10 • jQuery 1.9.2 • Newtonsoft.Json 11.0.2, 4.0.8 • jsTree 3.1.0 • Linux-libc-dev 4.4.0 • libc6-dev-2.23 • libc-dev-bin 2.2.3 • libesdb 2015409 • libext2fs1.43.4 • libfakeroot 1.20.2 • libreadline5 5.2 • lsscsi 0.27-3 • lupin-casper 0.57 • lvm2 2.02.167 • make 4.1 • mc 4.8.15-2 • mdadmin 3.3-2ubuntu7 • Microsoft Windows Azure Storage 8.2.0 • Mono 5.2 • openssh-server 7.2p2	

Issue ID	Resolved Issue Description	Functional Area
	• Oracle ManagedDataAccess 12.2.1100 • parted 3.2-15 • PuTTy 0.70 • screen 4.3.1-2build1 • Select2 4.03 • SSH.Net 2016.1.0 • zlib 1.2.8 • python minimal 2.7.11 Additionally, this section contains substantial updates to ensure all third-party components are identified as required.	
108327	For agentlessly protected machines only, web help contains a link on the protected virtual machine's *System Information* page that shows an incorrect topic, "Viewing system information for the Core." The link has been corrected and now points to the topic "Understanding system information for a protected machine."	In-product help
107985	Support for SQL Server 2005 was discontinued in Rapid Recovery Core release 6.2.1. Accordingly, references to this version no longer appear in documentation for release 6.3.	Supportability
106264	Rapid Recovery 6.3 User Guide correctly indicates that log truncation for Oracle is disabled by default and must be enabled if users want this function.	Oracle log truncation
101859	*Rapid Recovery 6.3 User Guide* topic "Deploying a virtual machine in Azure" has been modified. It contains no unnecessary steps.	Virtual export to Azure
101858	*Rapid Recovery 6.3 User Guide* topic "Setting up continual export to Azure" has been modified. It contains no unnecessary steps.	Virtual export to Azure
101853	In release 6.3 and later, to export a VM to Azure, you can use an existing container or (using Advanced storage options), you can define an export container or deployment container.	Virtual export to Azure
101837	Steps for creating a container in classic Azure Service Management mode for Azure were included in the *Rapid Recovery 6.2 User Guide*. Note that as of release 6.3, containers must be created using Azure Resource Management.	Supportability

Table 4: Linux resolved issues

Issue ID	Resolved Issue Description	Functional Area
107966	Ubuntu 16 and 18 on Hyper-V hung when taking snapshots.	Linux

Go to the top of this topic.

Known issues

This topic contains known issues in the following categories:

- Core and Windows known issues
- Documentation known issues
- Linux known issues
- Obsolete known issues

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

Table 5: Core and Windows known issues

Issue ID	Known Issue Description	Workaround	Functional Area
27309 93141	ESXi virtual export with automatic disk mapping using default configuration for the VM configuration location fails with unclear error. The Failure Reason is "Task 'ReconfigVM_Task' failed: Invalid configuration for device '0'."	Reduce the number of concurrent exports.	Virtual exports, ESXi
106545	When upgrading a Core (in languages other than English) that protects machines with Agent version earler than 5.4.3.106, the *Compatibility* page of the Rapid Recovery Core Installer wizard incorrectly shows Agent version 7 in the message instead of Agent 6.2 or Agent 6.3 (based on the installer being used).	None available. Disregard the version number. Protected machines with supported operating systems will be upgraded to Rapid Recovery Agent version 6.3.	Installer, localization
105830	Rollup job does not merge replicated recovery points according to the retention policy if seed drive for older recovery points was not consumed.	None available.	Rollup jobs, replication, seed drive
105445	Trustedinstaller process called during every metadata request from Agent, consuming about 100MB of additional RAM.	Contact Quest Data Protection Support for a patch to address this issue.	Metadata
104393	In a specific environment, when a shadow copy has a specific path, agentless backup fails with "Invalid URI: The hostname could not be parsed" error.	Contact Quest Data Protection Support for a patch to address this issue.	Agentless
103945	After upgrade from release 5.4.3 to release 6.1 and later, all task events convert to service events, and are no longer visible on	None available.	Upgrading

Issue ID	Known Issue Description	Workaround	Functional Area
	the Tasks page.		
103477	If the Quest NetVault Backup with BMR plugin is installed on the same server as the Rapid Recovery Core, then ESXi exports fail.	Copy the following DLLs from Coreservice\vddk\bin to the Coreservice folder, and then restart the Core service: • glib-2.0 • gobject-2.0 • gvmomi • iconv • intl • libcurl • libxml2 • vixDiskLibVim	Virtual exports
102756	A deploy to Azure fails if the cloud service name is specified in FQDN format.	Specify only the hostname (without periods) in the Cloud service name text box. For example, instead of specifying companycloudhost.cloudapp.net, enter companycloudhost.	Azure
102390	Drive letters are not assigned on an exported machine that is identical to the original machine.	Assign drive letters manually, or contact Support for a script to run on the exported machine that solves the issue.	Virtual exports
101736	Add menu for switching between pages with recovery points on the top of the Recovery Points page.	None available. This item is an enhancement request.	Recovery Points, GUI
100569	EC2 Export job fails with exception: 'Amazon.EC2.AmazonEC2Exception: The key pair '{key_name}' does not exist.' for replicated Agent from another region.	Before performing virtual export, import agent machine's key manually to the region in which the target Core machine is deployed. The key should have the same name as origin.	Virtual exports, Amazon E2C
97451	Volume letters are not assigned after BMR for GPT partitions of ESXi Agentless VM.	Assign drive letters manually.	BMR, ESXi agentless
97017	Exported CentOS7 isn't bootable on ESXi when it has more than 6 system volumes and root volume with the 'xfs' filesystem.	Perform VM export of 6 volumes; use restore for remaining volumes.	Virtual exports, Linux, XFS

Table 6: Documentation known issues

Issue ID	Known Issue Description	Workaround	Functional Area
108934	The following corrections were made to the *Rapid Recovery 6.3 User Guide* but not in the in-product help: One of the introductory paragraphs in the topic "Protecting multiple machines on a VMware vCenter/ESXi virtual host" is duplicated in the in-product help. A hypertext link in the topic "Protecting vCenter/ESXi virtual machines using agentless protection" is broken in the in-product help. Some minor formatting errors also appear. Some formatting errors appear in the topic "Protecting vCenter/ESXi virtual machines using agentless protection" in the in-product help. A hypertext link in the topic "Factors when choosing agent-based or agentless protection" is broken in the in-product help. A clarification regarding Active Block Mapping was added to the User Guide after in-product help was published. For the ABM setting "Exclude subdirectories," the text "Lets you exclude specific folders and files" was replaced with the following text: "Lets you exclude specific files by specifying '<file name>' or '<folder>\<subfolder>\<file name>'. Only the files will be excluded. The folders or subfolders that contained excluded files are included in the mount point, with no contents." This change appears in three topics: • Protecting vCenter/ESXi virtual machines using agentless protection • Protecting Hyper-V virtual machines using host-based protection • Changing ABM settings Malformed or missing hypertext links appear in step 13 of the topic "Protecting multiple machines manually" in the in-product help. In the topic "Generating a Core report on demand," the note under step 6 should begin "In all cases." Additionally, various formatting updates were applied to topics when necessary.	These errors have been fixed in the *Rapid Recovery 6.3 User Guide* and the correction will appear in the next release of in-product help.	In-product help
108327	For agentlessly protected machines only, web help contains a link on the protected virtual machine's *System Information* page that shows an incorrect topic, "Viewing system information for the Core."	Please disregard this help topic. This link is expected to be removed in a future version of	Agentless protection, In-product help

Issue ID	Known Issue Description	Workaround	Functional Area
		Rapid Recovery.	
108288	In release 6.3, a link to in-product help for the new Active Block Mapping feature is present only for protected hypervisor hosts, and is not yet available for agentlessly protected virtual machines.	The in-product help topic "Changing ABM settings" and its parent topic, "Understanding Active Block Mapping," are available to users when they open in-product help independently, and in the *Rapid Recovery 6.3 User Guide*.	Agentless protection, ABM, machine-level settings, In-product help

Table 7: Linux known issues

Issue ID	Known Issue Description	Workaround	Functional Area
108290	Linux Live DVD does not recognize disks on a specific environment.	Contact Quest Data Protection Supportfor a patch to address this issue.	Linux, Live DVD
108395	There is no ability to protect a Linux machine with more than 2000 disk devices attached.	Contact Quest Data Protection Support for a patch to address this issue.	Linux
31277, 96616	Red Hat virtual machines that are hosted in ESXi are not bootable when exported to VirtualBox. This occurs only with agentless protect and either large hard drives or LVM volumes.	None available.	ESXi, agentless protection, Linux

Table 8: Obsolete known issues

The issues listed in this table are previously known issues that are obsolete. Unless otherwise indicated, these issues relate to features that are no longer supported. Thus, these issues will not be fixed, nor tracked further in *Release Notes*.

Issue ID	Known Issue Description	Workaround	Functional Area
105997	Customer requested a decrease in the number of events created during agentless backup on vCenter.	This is an enhancement request, not a defect, and therefore will no longer be tracked in *Release Notes*. To request enhancements or new features, access the Quest Ideation Portal at https://ideas.labs.quest.com/.	Events monitoring, notifications
104825	There is no ability to create Tiering repository using the Add-on for Kaseya.	Tiering recovery points is no longer supported, and the Add-On for Kaseya is discontinued. This issue will no longer be tracked.	Tiering, Kaseya Add-On
104812	It is impossible to set GDPR if the user tries to install Core using the Add-on for Kaseya.	After installing using the 6.2 Kaseya Add-On, set GDPR (set the "Agree to use of personal data" setting) using General Settings in the Core Console. GDPR compliance was added after the last version of the Kaseya Add-On was provided. This issue will no longer be tracked.	Core settings, privacy setings, GDPR, Kaseya VSA
103412	Dashboard Transfer Job widget doesn't track jobs which are expired in the queue.	If experiencing this issue, review the status using other aspects of the Core Console UI, or using PowerShell scripts. This is not actually a defect, but reflects behavior as designed by the application. This item will no longer be tracked.	Core Console, dashboard widget
100061, 35031	In Rapid Recovery 6.0 and later, some non-English languages (namely French, Japanese, and Korean) use incorrect translations of the word "state" on the *Backup* page in the "Items Backed Up" section. The correct translation relates to the current condition.	This issue will no longer be tracked.	DL appliance, Backups page, localization
106200	Relocate recovery points to Virtual DR fails with error 'Job fails with RDS service exception. Error code: 'ConnectionResetByPeer.'	Tiering recovery points is no longer supported.	Tiering
104856	Add-on for Kaseya displays only 10 Kaseya Agents within different tabs.	The last release for the Add-on for Kaseya was 6.2. This	Kaseya Add-On

Issue ID	Known Issue Description	Workaround	Functional Area
		product is discontinued. This issue will no longer be tracked.	

Go to the top of this topic.

Where to find Rapid Recovery system requirements

For every software release, Quest reviews and updates the system requirements for Rapid Recovery software and related components. This information is exclusively available in the release-specific *Rapid Recovery System Requirements Guide*. Use that document as your single authoritative source for system requirements for each release.

You can find system requirements and all other documentation at the technical documentation website at https://support.quest.com/rapid-recovery/technical-documents/.

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 filter the view by document type.

Product licensing

Before you use and manage any version of Rapid Recovery, AppAssure, or DL series backup appliance, you must first obtain a software license. To purchase a license for the first time, contact the Quest Data Protection Sales team by completing the web form at https://www.quest.com/register/95291/. A sales representative will contact you and arrange for the license purchase.

If you need to renew or purchase additional licenses, please contact the Quest Support Renewals team by completing the web form at https://support.quest.com/contact-us/renewals.

After each license purchase, you must activate the license on the Rapid Recovery License Portal. From this portal, you can then download your Rapid Recovery license files.

When you initially install Rapid Recovery Core, you are prompted to upload these license files the first time you open the Rapid Recovery Core Console.

Some users start with a trial license, which has limited capabilities. Once a trial period expires, the Rapid Recovery Core stops taking snapshots. For uninterrupted backups, upgrade to a long-term subscription or perpetual license before the trial period expires. If you purchase a license after backups are interrupted, performing this procedure resumes your backup schedule.

When using a software license in standard phone-home mode, the Rapid Recovery Core Console frequently contacts the Rapid Recovery License Portal server to remain current with any changes made in the license portal. This communication is attempted once every hour. If the Core cannot reach the license portal after a grace period, the Core stops taking snapshots for non-trial licenses. The grace period (10 days by default) is configurable (from 1 to 15 days) in the license group settings on the license portal.

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

Use of phone-home licenses requires Rapid Recovery users to accept a limited use of personal information, as described in the privacy policy shown when you install Core software. For more information, see the topic "General Data Protection Regulation compliance" in the *Rapid Recovery 6.3 User Guide*.

NOTE: When registering or logging into the license portal, 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 Sales representative for assistance.

Complete the following steps to license your Rapid Recovery software.

1. **Open your registration email.** When you first purchase a license from Quest, you receive an email from the Quest licensing system. The email includes your license entitlements, expiration date (if relevant), registered email address, andQuest license number. The license number is typically 9 digits, in format 123-456-789. Other formats are supported, as described in the topic "Understanding Rapid Recovery licenses" in the *Rapid Recovery 6.3 Installation and Upgrade Guide*.
2. **New users: Register for the Rapid Recovery License Portal.** If you have not previously created an account on the Rapid Recovery License Portal, then do the following:
    a. **Sign up for an account.** In a web browser, access the license portal registration URL, https://rapidrecovery.licenseportal.com/User/Register.
    The *Sign Up* page appears.
    b. **Complete the form.** Enter the information requested, review and accept the privacy policy and terms of use, and click **Sign Up**.
    The *Confirm Email* page appears.
    c. **Verify your account information.** Check your email and verify your account information by clicking **Verify email address**.
    The *Add License Numbers* page appears.
    d. **Proceed to step 4**.
3. **Existing users: Log into the Rapid Recovery License Portal.** If you previously registered a license portal account to use with AppAssure or Rapid Recovery, then do the following:
    a. **Use existing credentials.** Log into the Rapid Recovery License Portal.
    b. **Open the License Numbers dialog box.** On the *Licensing* page, underneath your license pool information, click the **License Numbers** link.
    The *License Numbers* dialog box appears.
    c. **Proceed to step 4**.
4. **Enter your license numbers.** For each Quest license number included in your welcome email, click in the **License Number** text box and enter or paste your license number. Then click **+ Add License Numbers**. When satisfied, click **Close**.
The *License Number* dialog box closes.
5. **Review updated license information.** Review license type and license pool information displayed on the *Licensing* page.

Getting started with Rapid Recovery

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

Rapid Recovery Core and Agent compatibility

The following table provides a visual guide of the compatibility between supported versions of Rapid Recovery Core and Rapid Recovery Agent.

Table 9: Compatibility between supported Core and Agent versions

Version	6.1.3 Core	6.2.1. Core	6.3.0 Core
6.1.3 Agent	Fully compatible	Fully compatible	Fully compatible
6.2.1 Agent	Not compatible	Fully compatible	Fully compatible
6.3.0 Agent	Not compatible	Not compatible	Fully compatible

Previous editions of this topic depicted compatible versions of Rapid Recovery Core and Rapid Recovery Agent, regardless of whether the release versions shown were currently supported.

The following hybrid chart shows supportability (using the color coding explained in the legend) as well as compatibility between Core and Agent versions since release 5.4.3.

NOTE: Future editions of this topic will only include the simplified supportability information shown in the preceding chart.

Table 10: Hybrid chart: Compatibility between Core and Agent versions and supportability by color code

Version	5.4.3 Core[1]	6.0.2 Core	6.1.3[3] Core	6.2.1 Core	6.3.0x Core
5.4.3 Agent[1, 2]	Compatible	Compatible[3]	Compatible[3]	Compatible[3]	Compatible[3]
6.0.2 Agent[1, 2]	Not applicable	Compatible	Compatible[3]	Compatible[3]	Compatible[3]
6.1.3[4] Agent	Not applicable	Not applicable	Compatible	Compatible [3]	Compatible[3]
6.2.1 Agent	Not applicable	Not applicable	Not applicable	Compatible	Compatible[3]
6.3.0x Agent	Not applicable	Not applicable	Not applicable	Not applicable	Compatible[3]
	Color Legend:	Full Support	Limited Support	Discontinued	Never Supported

[1] While not currently supported, AppAssure 5.4.3 and Rapid Recovery 6.0.2 are shown in this chart to convey interoperability. See note 4.

[2] Protected machines with EFI partitions must be upgraded to Rapid Recovery release 6.0.x or later to successfully restore data, perform bare metal restore, or perform virtual export. To receive assistance from Quest

Data Protection Support, Quest recommends upgrading to a supported release (generally, the latest release), as detailed in note 4.

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

[4] As shown in this chart, Rapid Recovery supports the current version (6.3.0x), and the latest maintenance release of the last two major/minor versions (6.2.1 and 6.1.3, respectively). When a new maintenance release becomes generally available, it becomes fully supported. The prior version goes into limited support. For detailed information, see the "Product Life Cycle and Policies" section of the Rapid Recovery Support website at https://support.quest.com/rapid-recovery/.

Only the latest maintenance releases for the last two major/minor versions (N-1 and N-2 releases shown in table 11) are supported. For example, in release 6.3.0x, these versions include only releases 6.2.1 and 6.1.3. With the general availability of this release, other versions (such as releases 6.2.0, 6.1.2, 6.1.1, and so on) are now outside of the support policy. While Quest expects these versions to function, they may not have been tested for interoperability with the current version. If you have a current maintenance agreement, Quest Data Protection Support can attempt to answer your questions. However, if you call for support for an unsupported version, expect to be asked to upgrade.

Other factors affect interoperability. For example, the Rapid Snap for Virtual feature was first introduced in Rapid Recovery 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. Release 6.2 introduced agentless application support for protected machines running Exchange Server and SQL Server. Logically, users of Core version 5.4.3 cannot agentlessly protect any VMs. Users of Core version 6.0 cannot protect VMs on Hyper-V without installing the Agent software. And Cores earlier than release 6.2 have limited agentless support for Exchange and SQL Server, as detailed in the user guide topic "Understanding Rapid Snap for Virtual agentless protection" or "Understanding agentless protection" for each relevant release.

For more information about the differences between service levels supported for Rapid Recovery versus support levels generally for Quest products, see "Differentiation between standard Quest and Rapid Recovery service levels" in *Rapid Recovery 6.3 Release Notes*.

Upgrade and installation instructions

Quest recommends users carefully read and understand the *Rapid Recovery 6.3 Installation and Upgrade Guide* before installing or upgrading. See the section "Installing Rapid Recovery" for a step-by-step general installation approach. The approach includes requirements for a software license and for an account on the Rapid Recovery License Portal; adherence to the system requirements; installing a Core; creating a repository; and protecting machines with the Agent software or agentlessly. It also suggests use of the QorePortal.

All existing users should read the section "Upgrading to Rapid Recovery." This content describes upgrading factors, provides an overview of upgrading, and includes procedures upgrading Core, and upgrading Agent on Windows and Linux machines.

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. System requirements are found exclusively in the *Rapid Recovery 6.3 System Requirements Guide*.

When planning an implementation of Rapid Recovery, for guidance with sizing your hardware, software, memory, storage, and network requirements, see knowledge base article 185962, “Sizing Rapid Recovery Deployments".

If upgrading from a currently supported major and minor version of Rapid Recovery Core (6.1x or 6.2x), then run the latest Core installer software on your Core server. If upgrading from a version of AppAssure or Rapid

Recovery Core that is not currently supported, use a two-step upgrade process. First, upgrade using a supported Core installer such as 6.2.1; then run the latest Core installer software.

If using replication, always upgrade the target Core before the source Core.

To protect machines running supported operating systems with the latest Rapid Recovery Agent features, upgrade or install Rapid Recovery Agent on each.

> **CAUTION: Ensure that you check system requirements for compatibility before upgrading. For protected machines with operating systems that are no longer supported, you can continue to run older supported versions of Agent. In some cases, you can protect those machines agentlessly.**

You can use the same installer executable program (standard, or web installer) to perform a clean installation or to upgrade an existing version of Rapid Recovery Core, Rapid Recovery Agent, or the Local Mount Utility. If upgrading from versions earlier than release 5.4.3, you must first upgrade to 5.4.3 and then run a more recent installer on the same machine. For more information, see the *Rapid Recovery 6.3 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 topic "Installing or upgrading Rapid Recovery Agent on a Linux machine" in the *Rapid Recovery 6.3 Installation and Upgrade Guide*.

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 *Rapid Recovery 6.3 User Guide*.

For information on downloading Rapid Recovery software, see Obtaining Rapid Recovery software.

License requirements

New Core users must purchase a long-term subscription or perpetual license to use Rapid Recovery.

Some Rapid Recovery Core users start with a trial license, which uses a temporary license key for the duration of the trial. After the trial period expires, you can continue to restore from existing backups, but cannot perform new backups or replication until you purchase a long-term subscription or perpetual license. You must then activate the license on the Rapid Recovery License Portal, download Rapid Recovery license files, and associate them with your Core.

For more information about licensing, see the following resources:

- For information about activating your new license and obtaining Rapid Recovery license files for your Core, see Product licensing in these release notes.
- For information about managing licenses from the Rapid Recovery Core, including uploading license files to associate them with the Core, see the topic "Managing licenses" in the *Rapid Recovery 6.3 Installation and Upgrade Guide*.
- For information about managing license subscriptions and license groups on the license portal, see the latest edition of the *Rapid Recovery License Portal User Guide*.

More 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
- Quest Data Protection Portal
- In-product help is available from the Rapid Recovery Core Console by clicking  .

Obtaining Rapid Recovery software

You can obtain Rapid Recovery software using the following methods:

- **Download from the QorePortal.** If you have an active maintenance agreement, you can log into the QorePortal at https://qoreportal.quest.com. From the top menu, click **Settings**, and from the left navigation menu, select **Downloads**. Here you will have access to installers for various Rapid Recovery components, including Core, Agent, LMU, DR, and more.
- **Download from the License Portal.** If you have already registered Rapid Recovery in the Rapid Recovery License Portal, you can log into that portal at https://licenseportal.com. From the left navigation menu, click **Downloads**, and download the appropriate software.
- **Download trial software from the Support website.** To download trial software, navigate to the Rapid Recovery Rapid Recovery website at https://support.quest.com/rapid-recovery and from the left navigation menu, click **Software Downloads**. Here you can access trial versions of Rapid Recovery Core, Agent (for Windows or Linux), tools and utilities, and more. Trial versions function for 14 days, after which time you must purchase and register a subscription or perpetual license to continue using Rapid Recovery. To purchase a license, fill out the web form at https://support.quest.com/contact-us/licensing and select **Obtain a license for my product**.
- **Download trial software from the Support website.** To download trial software, navigate to the Rapid Recovery Rapid Recovery website at https://support.quest.com/rapid-recovery and from the left navigation menu, click **Software Downloads**. Here you can access trial versions of Rapid Recovery Core, Agent (for Windows or Linux), tools and utilities, and more. Trial versions function for 14 days, after which time you must purchase and register a subscription or perpetual license to continue using Rapid Recovery. To purchase a license, fill out the web form at https://support.quest.com/contact-us/licensing and select **Obtain a license for my product**.

You can also obtain the Rapid Recovery Agent software from within the Rapid Recovery Core Console using the following methods:

- **Protecting machines with the wizard.** If the Rapid Recovery Core is installed, you can deploy the Agent software to the machine you want to protect from the Protect Machine Wizard or the Protect Multiple Machines Wizard. Using these wizards, you can also choose to add machines to protection using an older installed version of Agent. For more information about these wizards, see the topics "Protecting a Machine" and "About protecting multiple machines" in the *Rapid Recovery 6.3 User Guide*.
- **Use the Deploy Agent Software feature.** If the Rapid Recovery Core is installed, you can deploy the Agent software from the Core to one or multiple machines. This is useful for upgrading Agent to one or more machines simultaneously. From the **Protect** drop-down menu on the Rapid Recovery Core Console, select **Deploy Agent Software** and complete details in the resulting wizard. For more information about using this feature, see the topic "Deploying Agent to multiple machines simultaneously from the Core Console" in the *Rapid Recovery 6.3 User Guide*.

- **Download Agent or LMU from the Rapid Recovery Core Console.** From a network-accessible Windows machine you want to protect, you can log into the Rapid Recovery Core Console and download the Agent software. From the icon bar, click More and then select **Downloads**. From the *Downloads* page, you can download the web installer to install Agent or the Local Mount Utility on Windows machines.

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 in the *Rapid Recovery 6.3 System Requirements Guide*.

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 user interface for this release is localized to the following languages: Chinese (Simplified), French, German, Japanese, Korean, Spanish.

This release has the following known capabilities or limitations:

- QorePortal is in English only.
- Reports are in English only.
- Rapid Recovery release 6.3 requires the . Microsoft .NET Framework version 4.6.2. Earlier releases of Rapid Recovery used different versions of the .NET Framework. There is no downgrade option available. If you upgrade versions of Rapid Recovery to a release using a more recent version of the .NET Framework, and then subsequently decide to return to a prior version, you must perform a new installation of the appropriate Core and Agent software.
- Logs and KB articles for Rapid Recovery are in English only.
- Technical product documentation for this release is in English only.

About us

Quest provides software solutions for the rapidly-changing world of enterprise IT. We help simplify the challenges caused by data explosion, cloud expansion, hybrid datacenters, security threats, and regulatory requirements. We are a global provider to 130,000 companies across 100 countries, including 95% of the Fortune 500 and 90% of the Global 1000. Since 1987, we have built a portfolio of solutions that now includes database management, data protection, identity and access management, Microsoft platform management, and unified endpoint management. With Quest, organizations spend less time on IT administration and more time on business innovation. For more information, visit www.quest.com.

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 your product

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

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

Refer to our Web site (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 and the Quest logo 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.

NOTE: An information icon indicates supporting information.