Quest

Rapid Recovery 6.1.3

Third-Party Integration Guide

Table of Contents

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.

Introduction to Rapid Recovery Add-on for Kaseya

Rapid Recovery Add-on for Kaseya features increase third-party integration with Kaseya Virtual System Administrator (VSA). Kaseya VSA is a broad-based information technology (IT) system management framework for IT departments and managed service providers (MSPs).

Topics include:

- About the Rapid Recovery Add-on for Kaseya
- Rapid Recovery Add-on for Kaseya system requirements
- Preparing to protect machines using the Rapid Recovery Add-on for Kaseya
- Installing the Rapid Recovery Add-on for Kaseya
- Navigating the Rapid Recovery Add-on for Kaseya

About the Rapid Recovery Add-on for Kaseya

The Rapid Recovery Add-on for Kaseya is a software plug-in that integrates with the Kaseya Virtual System Administrator (VSA) system management interface. Kaseya VSA is broad-based information technology (IT) system management framework for IT departments and managed service providers (MSPs) to install and monitor machines protected by the Rapid Recovery Core.

With the Rapid Recovery Add-on for Kaseya, you can do the following:

- Deploy the Rapid Recovery Agent and Core software
- Protect machines
- Set up replication
- Add or change repository storage locations
- View recovery points
- Perform consolidated reporting

The Add-on for Kaseya is a means of managing Rapid Recovery environments from the Kaseya VSA user interface. Not all Rapid Recovery features are available from the Add-on for Kaseya. For example, to restore data, you must use the Rapid Recovery Core Console. For more information about using the Rapid Recovery Core Console, see the *Rapid Recovery User Guide*.

Rapid Recovery Add-on for Kaseya system requirements

The system requirements for the Rapid Recovery Add-on for Kaseya relate to the version of Kaseya VSA with which the Add-on for Kaseya is installed. The Rapid Recovery Add-on for Kaseya is compatible with the following Kaseya VSA releases:

- Kaseya VSA v7.x
- Kaseya VSA R8
- Kaseya VSA R9.0

For information about preparing your environment and installing Rapid Recovery, see Rapid Recovery system requirements.

Preparing to protect machines using the Rapid Recovery Add-on for Kaseya

After you install the Rapid Recovery Add-on for Kaseya, there is a multi-step process for preparing the environment to protect machines with Rapid Recovery.

To prepare the Rapid Recovery Add-on for Kaseya for protecting machines, complete the following tasks:

- Go to the Rapid Recovery License Portal at https://licenseportal.com to create an account and download the Rapid Recovery installation packages. For more information, see the *Rapid Recovery License Portal User Guide*.
- Use the license key you obtained from the Rapid Recovery License Portal to create a license.
- Create and assign a repository for storing the backed-up data.
- Deploy the Rapid Recovery installation deployment packages.
- Set up the credentials for the Core and protected machines.
- Enjoy using the Add-on for Kaseya to protect and manage your machines.

Related concepts

See also: Managing credentials for Rapid Recovery Core and Agent
See also: Configuring repositories
See also: About protecting machines using the Rapid Recovery Add-on for Kaseya

Related tasks

See also: Installing the Rapid Recovery Add-on for Kaseya
See also: Adding a Rapid Recovery license to the Add-on for Kaseya

Related references

See also: Installing Rapid Recovery using the Add-on for Kaseya

Installing the Rapid Recovery Add-on for Kaseya

The installation of the Rapid Recovery Add-on for Kaseya involves installing the Rapid Recovery Add-on for Kaseya software on your Kaseya server as described in this section, and then installing and deploying the Rapid Recovery Core and Agent services on Windows machines.

NOTE: The Rapid Recovery Add-on for Kaseya requires Kaseya server version 7 or later.

1. To download the Rapid Recovery Add-on for Kaseya, navigate to the URL you received from Quest or to https://licenseportal.com.
2. Navigate to and double-click the Rapid Recovery Add-on for Kaseya installer file on your system. The InstallShield Wizard starts.
   - **If you experience an Open File — Security Warning window, click Run to continue.**
3. On the **Welcome** page, click **Next** to continue with the installation.
4. On the **License Agreement** page, select **I accept the terms in the license agreement**, and then click **Install**.

   NOTE: In the rare case that your instance of Microsoft Internet Information Services (IIS) serves other websites, those sites are temporarily unavailable until the Rapid Recovery installation completes.

   A page appears showing the status and progress of the installation.
5. Click **Finish**.

   You can now log on to Kaseya to select the Rapid Recovery Add-on for Kaseya and deploy the Rapid Recovery software to your compatible servers.

Related concepts

See also: Rapid Recovery system requirements

Related references

See also: Installing Rapid Recovery using the Add-on for Kaseya

Navigating the Rapid Recovery Add-on for Kaseya

The Rapid Recovery Add-on for Kaseya lets you perform several Rapid Recovery functions directly from the Kaseya VSA Management Console. Use the navigation tree in the Rapid Recovery Server Backup column of the console to access the various Rapid Recovery pages.

The Rapid Recovery navigation tree includes the following root nodes:

- **Welcome to Rapid Recovery.** An overview of the product.
- **Rapid Recovery Deployment.** Upload Rapid Recovery software packets, manage Rapid Recovery user licenses, and deploy the Rapid Recovery software.
- **Configure Management.** View and manage credentials, repositories, and protected machine volume information.
- **Manage Protection.** Protect machines using the Rapid Recovery software, manage their protection, and view recovery points.
- **Manage Replication.** Begin replicating the protected machines from a source Core to a target Core for disaster recovery preparation.
- **Monitor.** View the machines and the events that the Core and Agent software performs.
- **Reports.** Create, view, and send reports of machine information and events.

Introduction to Rapid Recovery and installing it using the Add-on for Kaseya

This section provides a brief overview of Rapid Recovery. It also provides the system requirements necessary for installing the Rapid Recovery Core and Agent, and how to install those products using the Add-on for Kaseya.

Topics include:

- Introduction to Rapid Recovery
- Rapid Recovery system requirements
- Installing Rapid Recovery using the Add-on for Kaseya

Introduction to Rapid Recovery

Rapid Recovery is a backup, replication, and recovery solution that offers near-zero recovery time objectives and recovery point objectives. Rapid Recovery offers data protection, disaster recovery, data migration and data management. You have the flexibility of performing bare-metal restore (to similar or dissimilar hardware), and you can restore backups to physical or virtual machines, regardless of origin. Rapid Recovery can also archive to the cloud, to a DL series backup and recovery appliance, or to a supported system of your choice. With Rapid Recovery, you can replicate to one or more targets for added redundancy and security.

Rapid Recovery offers:

- **Flexibility**. You can perform universal recovery to multiple platforms, including restoring from physical to virtual, virtual to physical, virtual to virtual, and physical to physical.
- **Cloud integration**. You can archive and replicate to the cloud, using cloud storage vendors that support both proprietary and open-source platforms.
- **Intelligent deduplication**. You can reduce storage requirements by storing data once, and referencing it thereafter (once per repository or encryption domain).
- **Instant recovery**. Our Live Recovery feature allows you to access critical data first, while remaining restore operations complete in parallel.
- **File-level recovery**. You can recover data at the file level on-premise, from a remote location, or from the cloud.
- **Virtual support**. Enhanced support for virtualization includes agentless protection and autodiscovery for VMware ESXi 5 and higher, and export to Microsoft Hyper-V cluster-shared volumes.

See the following resources for more information about Rapid Recovery.

- The Rapid Recovery product support website at https://support.quest.com/rapid-recovery/
- The documentation website at https://support.quest.com/rapid-recovery/technical-documents/

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
- 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
- DVM repository requirements

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.

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 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 1. 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

Requirement	Details
	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 **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 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 2. 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 3. 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, 15.10, and 16.04. SLES versions 12 and 12 SP1 have older kernel versions, and so Rapid Recovery does not support their implementations of BTRFS.

Rapid Recovery 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 4. 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. Additional operating systems are supported for agentless protection only. For more information, see . 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.

Requirement	Details
	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.
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.

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."

Installing Rapid Recovery using the Add-on for Kaseya

The Rapid Recovery Core stores and manages the backups of all protected machines or servers in your environment on which the Rapid Recovery Agent is installed.

To install Rapid Recovery using the Add-on for Kaseya, complete the following tasks.

NOTE: The Rapid Recovery Add-on for Kaseya supports versions 6.0.1 and later of the Rapid Recovery Core and Agent.

- Download the Rapid Recovery from the Rapid Recovery License Portal at https://licenseportal.com.
- Upload the Rapid Recovery deployment package to the Kaseya server.
- Deploy the Rapid Recovery Core to the machine or machines that you want to have function as the Core and run the Core Console.
- Install the Rapid Recovery Agent software on the machine or machines that you want to protect.
- Verify that the Rapid Recovery software installation completed.

Related tasks

See also: Downloading the Rapid Recovery deployment package
See also: Uploading a Rapid Recovery installation package to the Kaseya server
See also: Installing the Rapid Recovery Core from the Add-on for Kaseya
See also: Installing Rapid Recovery Agent software from the Add-on for Kaseya

Downloading the Rapid Recovery deployment package

To begin installing Rapid Recovery using the Add-on for Kaseya, you must first download the Rapid Recovery Core Web and Agent Web installer packages from the Rapid Recovery License Portal. Save this file on your system in an accessible location so you can later upload it to the Kaseya Server.

1. Go to https://licenseportal.com.
2. From the main page of the License Portal, click **Downloads**.
3. On the **Downloads** page, click **Rapid Recovery**.
4. In the Windows Based Applications table, do the following:
   - **To download the software for the Rapid Recovery Core, in the Core Web Installer row, click Download.**
   - **To download the software for the Rapid Recovery Agent, in the Windows Agent Web Installer row, click Download.**
5. As necessary, follow the prompts specific to your operating system and web browser to save the package or packages in an accessible location.

Related tasks

See also: Uploading a Rapid Recovery installation package to the Kaseya server

Related references

See also: Installing Rapid Recovery using the Add-on for Kaseya

Uploading a Rapid Recovery installation package to the Kaseya server

After you install the Rapid Recovery Add-on for Kaseya, you can use it to deploy the Rapid Recovery Core and Agent to the machines you want to use and protect.

NOTE: The Rapid Recovery Add-on for Kaseya supports versions 6.0.1 and later of the Rapid Recovery Core and Agent.

1. Navigate to the Rapid Recovery Deployment section in Kaseya, and then click **Upload Packages**.
2. To locate and open the Rapid Recovery Core-Web or Agent-Web installation package file on your system, click **Browse for a file**.
3. In the dialog box, select the installation package on your system, and then click **Open**.
4. Click **Upload File**.

   The package file appears in the table as Core or Agent, depending on which package you uploaded. The release build number for the package appears in the Installation Package Version column of the table.

Related tasks

See also: Downloading the Rapid Recovery deployment package
See also: Installing the Rapid Recovery Core from the Add-on for Kaseya
See also: Installing Rapid Recovery Agent software from the Add-on for Kaseya

Installing the Rapid Recovery Core from the Add-on for Kaseya

Before you can complete this task, you must first upload the Rapid Recovery Core installation package and add the license to the Manage Licenses page.

You can use the Rapid Recovery Add-on for Kaseya interface to deploy and install the Rapid Recovery Core to networked servers. Complete the following procedure to deploy the Rapid Recovery Core.

NOTE: When upgrading a machine to a newer version of AppAssure or to Rapid Recovery, always upgrade the Core before the protected machine. If you have replication enabled, it is important that you upgrade in the following order: target Core, then source Core, and then protected machines.

1. In the left navigation tree, expand the Rapid Recovery Deployment section, and then click **Install Cores** .
2. On the Install Rapid Recovery Cores page, select the machine that you want to use as the Core machine, and then click **Install/Reinstall**.

   The **Install/Reinstall** window opens.
3. Specify the following options to define when and how to install the Rapid Recovery software.

Table 5. Rapid Recovery installation options

Option	Description
Run on	Select this option to run the installation on the date and time specified in the text box.
Run now	Select this option to run the installation immediately.
Stagger by	Optional. Enter the amount of minutes to wait between deploying the Rapid Recovery Core to multiple machines to even the load on file servers and the network connection.
Skip if machine offline	Optional. Select this option when installing the package at a specified time. If the machine is offline, the Add-on for Kaseya attempts the installation again during the next stagger interval. Keep this check box clear to install the update as soon as the machine is online, regardless of the specified time.
Choose Rapid Recovery installation package	Use the drop-down list to select the upload version of Rapid Recovery Core that you want to install. **NOTE:** When upgrading, verify the Core that protects each protected machine and that you are not upgrading a protected machine before a Core, by viewing the Protect Machines page in the navigation tree.
Choose a license	Use the drop-down list to select the appropriate license for this installation of the Rapid Recovery Core.

4. Click **OK**.

   The Rapid Recovery Core software is sent to and installed on the selected machines.

Related concepts

See also: Managing your Rapid Recovery licenses

Related tasks

See also: Uploading a Rapid Recovery installation package to the Kaseya server

See also: Installing Rapid Recovery Agent software from the Add-on for Kaseya

Installing Rapid Recovery Agent software from the Add-on for Kaseya

Before you can complete this task, you must first upload the Rapid Recovery Agent installation package and have installed the Rapid Recovery Core on a dedicated machine.

This section describes the steps for installing and deploying the Rapid Recovery Agent software to the machines in your environment.

NOTE: If the Rapid Recovery Core or Agent software is already installed on the target machine, an upgrade or repair is performed. Also note that downgrading an installation to a previous version is not supported.

NOTE: When upgrading a machine to a newer version of AppAssure or Rapid Recovery, always upgrade the Core before the protected machine. If you have replication enabled, it is important that you upgrade in the following order: target Core, then Source Core, then protected machines.

1. In the left navigation tree, expand the Rapid Recovery Deployment section, and then click **Install Agents** .
2. On the Install Rapid Recovery Agents page, select the machine or machines that you want to protect, and then click **Install/Reinstall**.

   The **Install/Reinstall** window opens.
3. Specify the following options to define when and how to install the Rapid Recovery software.

Table 6. Rapid Recovery installation options

Option	Description
Run on	Select this option to run the installation on the date and time specified in the text box.
Run now	Select this option to run the installation immediately.
Stagger by	Optional. Enter the amount of minutes to wait between deploying the Agent to multiple machines to even the load on file servers and the network connection.
Skip if machine offline	Optional. Select this option when installing the package at a specified time. If the machine is offline, the Add-on for Kaseya attempts the installation again during the next stagger interval. Keep this check box clear to install the update as soon as the machine is online, regardless of the specified time.
Choose Rapid Recovery installation package	Use the drop-down list to select the upload version of Rapid Recovery Agent that you want to install. **NOTE:** When upgrading, verify the Core that protects each protected machine and that you are not upgrading a protected machine before a Core, by viewing the Prepare Replication page in the navigation tree.

4. Click **OK**.

   The Rapid Recovery Agent software is sent to and installed on the selected machines.

Related tasks

See also: Uploading a Rapid Recovery installation package to the Kaseya server
See also: Installing the Rapid Recovery Core from the Add-on for Kaseya

Using the Rapid Recovery Add-on for Kaseya

This section includes topics that describe how to use the Rapid Recovery Add-on for Kaseya after it is installed and the Rapid Recovery Core and Agent software applications have been deployed to their respective machines.

Topics include:

- Managing your Rapid Recovery licenses
- Managing credentials for Rapid Recovery Core and Agent
- Configuring repositories
- About protecting machines using the Rapid Recovery Add-on for Kaseya
- Managing replication in the Rapid Recovery Add-on for Kaseya
- Monitoring Rapid Recovery activity in the Add-on for Kaseya
- Managing Rapid Recovery Core reports in the Add-on for Kaseya

Managing your Rapid Recovery licenses

Before you download the Rapid Recovery Core and Agent installation packages, you must log on to the Rapid Recovery License Portal at https://licenseportal.com and register for an account. You can then download the installer and obtain a license key to enable the software. For more information about the Rapid Recovery License Portal, see the *Rapid Recovery License Portal User Guide*, found on the Rapid Recovery documentation website at https://support.quest.com/rapid-recovery/technical-documents.

After you install the Rapid Recovery Core, you can download the Rapid Recovery Agent installer from the Core or the Rapid Recovery License Portal for each machine that the Core protects.

Adding a Rapid Recovery license to the Add-on for Kaseya

Complete the following procedure to enter the license key necessary to deploy the Rapid Recovery software from Kaseya.

1. In the left navigation tree, expand the Rapid Recovery Deployment section, and then click **Manage Licenses**.
2. On the **Manage Rapid Recovery Licenses** page, click **Add**.
3. In the **Add License Key** window, enter the following information for your license.

Table 7. License information

Text Box	Description
License name	A descriptive name to identify the license.
License key	The license key you received from the Quest Software Group licensing team.
Description	Optional. A description for this license key.

4. Click **Add**.
5. Repeat Step 2 through Step 4 for each license you want to enter.

   The licenses added appear in the table on the Manage Rapid Recovery Licenses page.

Related tasks

See also: Removing Rapid Recovery licenses from the Add-on for Kaseya

Removing Rapid Recovery licenses from the Add-on for Kaseya

Complete the following procedure to remove one or more licenses from the Rapid Recovery Add-on for Kaseya.

1. Navigate to the Rapid Recovery Deployment section, and then select **Manage Licenses**.
2. In the table, select the license or licenses that you want to delete.
3. Click **Remove**.
4. In the **Confirmation** dialog box, click **Yes**.

Related tasks

See also: Adding a Rapid Recovery license to the Add-on for Kaseya

Managing credentials for Rapid Recovery Core and Agent

A Rapid Recovery Core provides the essential services for backup, replication, archiving, and management. A protected machine is a machine on which the Rapid Recovery Agent software is installed that is managed and protected by a specific Core. Repositories are set up through the Core to store the snapshots that are captured from the protected machines. Repositories are configured by specifying a storage location associated with the Core server to store the data.

Managing Agent credentials

You must set credentials for all machines on which the Rapid Recovery Agent is installed for the Add-on for Kaseya to communicate with them. Complete the following steps to set the credentials for a Rapid Recovery protected machine.

1. Navigate to the Configure Management section, and then click **Manage Agent Credentials**.
2. Select a machine from the table, and then click **Set credentials**.
3. Enter the information for your Rapid Recovery protected machine described in the following table.

Table 8. Agent credentials and information

Text Box	Description
Login	Enter the user name used to connect to this machine; for example, administrator.
Password	Enter the password associated with the login.
Domain	Enter the domain for this machine, if applicable. If the machine is not in a domain, leave this text box empty.

4. Click **OK**
5. To confirm whether the saved credentials are correct and have the required privileges to communicate with the protected machine, select a machine, and the click **Verify**.

Related tasks

See also: Managing Core credentials

Managing Core credentials

You must set credentials for all machines on which the Rapid Recovery Core is installed for the Add-on for Kaseya to communicate with them. Complete the following steps to set the credentials for a Rapid Recovery Core machine.

1. Navigate to the Configure Management section, and then click **Manage Core Credentials**.
2. Select a machine from the table, and then click **Set credentials**.
3. Enter the information for your Rapid Recovery Core machine described in the following table.

Table 9. Core credentials and information

Text Box	Description
Login	Enter the user name used to connect to this machine; for example, administrator.
Password	Enter the password associated with the login.
Domain	Enter the domain for this machine, if applicable. If the machine is not in a domain, leave this text box empty.

4. Click **OK**
5. To confirm whether the saved credentials are correct and have the required privileges to communicate with the Core machine, select a machine, and the click **Verify**.

Related tasks

See also: Managing Agent credentials

Configuring repositories

A repository is used to store the snapshots that are captured from the protected servers. Before creating a repository, verify that you have set the credentials for logging on to the associated Rapid Recovery Core.

NOTE: Rapid Recovery repositories should 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.

For more information about repositories, see the topic “Understanding Repositories” in the *Rapid Recovery User Guide*.

Adding a repository

Complete the steps in this procedure to add a repository.

1. Navigate to the Configure Management section, and then click **Manage Core Repositories**.
2. In the list of machines on this page, select the Core machine to which you want to add a repository.
3. Click **Add new repository**.
4. Enter the information in the text boxes as described in the following table.

Table 10. Repository information

Text Box	Description
Repository Name	Enter the display name of the repository. By default, this text box consists of the word Repository and an index number, which corresponds to the number of the new repository. You can change the name as needed, and you can enter up to 150 characters.
Concurrent Operations	Define the number of concurrent requests that the repository supports. By default, the value is 64.
Comments	(optional) When configuring repositories, network and local storage locations must be similar and not a combination of local and network file locations. Configure the storage location for the repositories as either all local or all network. Enter a descriptive note about this repository.

5. Click **Add Storage Location** to define a specific location or volume for the repository.

   NOTE: If the Rapid Recovery repository that you are creating in this step is later removed, all files at the storage location of your repository are also deleted. If you do not define a dedicated folder to store the repository files, then those files are stored in the root. Deleting the repository also deletes the entire contents of the root, resulting in catastrophic data loss.

   NOTE: Rapid Recovery repositories should 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.

   The **Add Storage Location** dialog box appears.
6. Specify how to add the file for the storage location and where. You can choose to add the file on local disk or on CIFS share.

   NOTE: When configuring repositories, you cannot intermix network and local locations for a repository. The storage location must contain either all local files or all network files.

   - **Click Add file on local disk to specify a local machine and then enter the information as described in the following table.**

Table 11. Local disk paths

Text Box	Description
Metadata Path	Enter the location for storing the protected metadata. For example, type: `X:\Repository\Metadata`.

Text Box	Description
	When specifying the path, use only alphanumeric characters, the hyphen, and the period (only to separate host names and domains). The letters a to z are case-insensitive. Do not use spaces. No other symbols or punctuation characters are permitted.
Data Path	Enter the location for storing the protected data. For example, type: `X:\Repository\Data`. The same limitations to the path apply; use only alphanumeric characters, hyphen, or period, with no spaces or special characters.

- **Or, click Add file on CIFS share to specify a network share location and then enter the information as described in the following table.**

Table 12. CIFS share information

Text Box	Description
UNC Path	Enter the path for the network share location. If this location is at the root, define a dedicated folder name (for example, `Repository`). The path must begin with \\. When specifying the path, use only alphanumeric characters, the hyphen, and the period (only to separate host names and domains). The letters a to z are case-insensitive. Do not use spaces. No other symbols or punctuation characters are permitted.
User Name	Specify a user name for accessing the network share location.
Password	Specify a password for accessing the network share location.

7. In the More Details pane, enter the details for the storage location as described in the following table.

Table 13. Storage location details

Text Box	Description
Bytes per Sector	Specify the number of bytes you want each sector to include. The default value is 512.
Average Bytes per Record	Specify the average number of bytes per record. The default value is 8192.
Write Caching Policy	The write caching policy controls how the Windows Cache Manager is used in the repository and helps to tune the repository for optimal performance on different configurations. Set the value to one of the following: • On • Off • Sync If set to On, which is the default, Windows controls the caching. **NOTE:** Setting the write caching policy to On could result in faster performance. If you are using a version of Windows Server older than Server 2012, the recommended setting is Off. If set to Off, Rapid Recovery controls the caching.

Text Box	Description
	If set to Sync, Windows controls the caching as well as the synchronous input/ output.
Size	Set the size or capacity for the storage location. The default is 250 GB. You can choose from the following: • GB • TB **NOTE:** The size that you specify cannot exceed the size of the volume. If the storage location is a New Technology File System (NTFS) volume using Windows XP or Windows 7, the file size limit is 16TB. If the storage location is an NTFS volume using Windows 8, 8.1 or Windows Server 2012, 2012 R2, the file size limit is 256TB. **NOTE:** For Rapid Recovery to validate the operating system, Windows Management Instrumentation (WMI) must be installed on the intended storage location.

8. Click **Save**.

   The Repositories page displays the newly added storage location.

9. Repeat Step 5 through Step 8 to add additional storage locations for the repository.
10. Click **Create** to create the repository.
    - **If you need to edit the storage location, click Edit.**
    - **If you need to delete the storage location, click Delete.**

Performing a repository audit

Performing a repository audit is helpful for getting and viewing information about the repositories configured for a Rapid Recovery Core.

1. Navigate to the Configure Management section, and then click **Manage Core Repositories**.
2. Select the machine for the audit, and then click **Get Rapid Recovery Core Repositories**.
3. To confirm the selection and acknowledge that this task queries all selected Core machines for their repository parameters, click **Yes**.

   Any associated repositories, including allocated size (in GB or TB), appears in the Repositories column for the selected machine.

Viewing Agent volume information in the Rapid Recovery Add-on for Kaseya

You can view information about the volumes for machines that are being protected by the Rapid Recovery software. To get updated Rapid Recovery Agent volume information, verify that you have set the credentials for logging on to the protected machine.

1. Navigate to the Configure Management section, and then click **Agent Volumes Information**.
2. To refresh the information in the list about known Rapid Recovery Agent volumes, click **Get Rapid Recovery Agent Volumes**.

About protecting machines using the Rapid Recovery Add-on for Kaseya

You can protect the volumes of data from the machines and Windows Servers on which you have installed the Rapid Recovery Agent software. When a machine is protected, full and incremental snapshots of data are captured from and stored in the repository associated with the Core.

From the Rapid Recovery Add-on for Kaseya, you can protect a machine, update the protection and replication status of a machine, and remove a machine from protection.

Related tasks

See also: Protecting a machine using the Rapid Recovery Add-on for Kaseya
See also: Updating protection and replication status
See also: Removing a machine from the Rapid Recovery Add-on for Kaseya

Protecting a machine using the Rapid Recovery Add-on for Kaseya

Before you protect a machine, be sure to have on hand the information for the machine volumes and the Rapid Recovery Core repositories.

Complete the following steps to protect a machine with Rapid Recovery.

1. Navigate to the Manage Protection section, and then click **Protect Machines**.
2. In the table, click the **Protect Agent** icon for the machine that you want to protect.

   The Protect Machine dialog box opens.
3. On the Select Core page, select the Core that protects and manages this machine, and then click **Next**.
4. On the Options page, use the **Repositories** drop-down list to select a repository for storing the backed up data.

   A message appears in the Managed by Core column, alerting you that the setup of protection is in progress. After the setup, the name of the Core appears in this column. The default interval for protection is one hour.
5. Under **Volumes**, select the volumes on the machine that you want to protect.
6. Click **Protect**.

Related tasks

See also: Installing Rapid Recovery Agent software from the Add-on for Kaseya
See also: Managing Agent credentials
See also: Viewing Agent volume information in the Rapid Recovery Add-on for Kaseya
See also: Viewing machine activity in the Rapid Recovery Add-on for Kaseya

Related references

See also: Managing replication in the Rapid Recovery Add-on for Kaseya

Updating protection and replication status

When you update the protection and replication status for a machine, you get the latest status of all protected machines associated with the known Cores. This feature is helpful if you need to verify that you have the latest version of protected data.

1. Navigate to the Manage Protection section, and then click **Protect Machines**.
2. Click **Update Protection and Replication Status**.

Editing a protected machine in the Rapid Recovery Add-on for Kaseya

Complete the following steps to make changes to the settings of a machine protected by the Rapid Recovery Core from the Add-on for Kaseya.

1. Navigate to the Manage Protection section, and then click **Protect Machines**.
2. In the table, click the **Edit** icon for the machine that you want to edit.

   The Agent Volumes dialog box opens.
3. Select the volumes that you want to protect or clear the volumes that you no longer want to protect.
4. Click **Protect**.

Removing a machine from the Rapid Recovery Add-on for Kaseya

When you remove a machine from protection, Rapid Recovery stops collecting backups of the machine in the repository.

NOTE: This task removes a machine from protection, but it does not uninstall Rapid Recovery Agent software from the machine.

1. Navigate to the Manage Protection section, and then click **Protect Machines**.
2. In the list of machines on this page, click the **Remove** icon for the machine that you want to remove.

   The confirmation dialog box opens.
3. To remove the machine, in the confirmation dialog box, click **Yes**.

   A message displays in the Managed by Core column for the selected machine to indicate that the removal is in progress.

Related tasks

See also: Protecting a machine using the Rapid Recovery Add-on for Kaseya
See also: Editing a protected machine in the Rapid Recovery Add-on for Kaseya
See also: Updating protection and replication status

Managing replication in the Rapid Recovery Add-on for Kaseya

Replication is the managing and transference of data (recovery points) between a source and target core. A snapshot of the recovery points on the source core is captured and then transmitted to a target core for redundancy. There are multiple ways in which replication can be configured; for example, between two cores at the same site or across two locations on a per machine basis. Rapid Recovery asynchronously transmits the snapshot of the replicated data (recovery points) to the target core for storage. Outbound replication can also be configured to a Managed Service Provider (MSP) providing off-site backup and disaster recovery service, or to a self-managed core.

The Rapid Recovery Add-on for Kaseya supports two types of replication. Replication by request is useful when you know the name but do not know the credentials for the Core to which you want to replicate; for example, an MSP-hosted core. On-demand replication is replication for a self-managed core, that is, a core that you own.

In the Rapid Recovery Add-on for Kaseya, the following list describes the replication tasks you can perform:

- When you prepare for replication, you create a link between two cores, that is, one source and one target. For more information, see Preparing for replication.
- When you establish replication, you establish on-demand replication. For more information, see Establishing replication.
- When viewing pending requests, you can accept or deny replication requests. For more information, see Viewing pending replication requests in the Rapid Recovery Add-on for Kaseya.
- You can also remove replication. For more information, see Removing replication in the Rapid Recovery Add-on for Kaseya.

Related tasks

See also: Preparing for replication
See also: Establishing replication
See also: Viewing pending replication requests in the Rapid Recovery Add-on for Kaseya
See also: Removing replication in the Rapid Recovery Add-on for Kaseya

Preparing for replication

Use Prepare Replication to configure replication and pair (establish a connection) between two Cores, that is, one source and one target.

1. Navigate to the Manage Replication section, and then click **Prepare Replication**.
2. On the Pair Cores for Replication page, select the machine you want to pair to another Core, and then click **Prepare Replication**.

   The Prepare Replication dialog box opens.
3. On the **Select remote Core** tab, do one of the following:
   - **For replication by request, select I have a subscription to a third-party providing off-site backup and disaster recovery services and wish to replicate my backups to that service (generate replication request), and then enter the information described in the following table.**

Table 14. Replication request settings

Text Box	Description
Host Name	Enter the fully qualified domain name (FQDN) for the Core.

Text Box	Description
Port	Enter the port number that you received from the service provider. The default port number is 8006.

- **For on-demand replication, select I have my own remote Core I wish to replicate to (establish replication on-demand), and then enter the credentials for the target core as they are described in the following table.**

Table 15. On-demand replication settings

Text Box	Description
Host Name	Enter the host name for the target (remote) Core.
Port	Enter the port number. The default port number is 8006.
User Name	The user name for logging on to the Core.
Password	The password associated with this user name.

4. Click **Continue**.
5. If you selected the option for replication by request, in the Prepare Replication Wizard, do the following:
    a. Enter your subscription email address and (optional) customer ID that you received from the service provider.
    b. Click **Finish** to close this dialog box and submit the replication request.

    On the Prepare Replication page, a message displays in the State column indicating that replication by request is in progress, followed by a status of Pending. If the request is approved, this status changes to Established. For replication on demand, the State column displays the text, Pairing.
6. If you selected the option for on-demand replication, proceed to the Establish Replication section.

Related tasks

See also: Establishing replication

Establishing replication

Use Establish Replication to configure on-demand replication when you have credentials for both source and target Cores. For example, you own the Cores and do not need to send a request or get approval to establish replication.

1. Navigate to the Manage Replication section, and then click **Establish Replication**.
2. In the list of machines on this page, select the machine you have prepared for replication and for which you want to establish replication.

    The machine should have the status of Pairing in the State column, or a status of Validated on the Events page.
3. Click the **Review** icon.

The **Establish Replication** dialog box opens.

4. Under **Choose the protected machine(s) whose backups you want to replicate to, and on which repository each Agent should be stored**, do one of the following:
    - **Select Replace an existing replicated Core on, and then select an existing target core from the drop-down list.**
    - **Select Create a new replicated Core on, and then enter the name of the new target core.**
5. In the table, select the protected machine or machines and a repository in which you want to store replicated data from the drop-down list for each machine.
6. Click **Start Replication**.

    On the **Establish Replication** page, the State column for the selected Core machine displays the status of Pending. When replication is established, the status changes to Established.

Viewing pending replication requests in the Rapid Recovery Add-on for Kaseya

If you have protected machines for which others can send replication requests, this page lets you get and view the requests that have been submitted for those protected machines. The list of protected machines includes the following information:

- **Machine.** The name of the machine that has the Core installed.
- **Credentials.** The user name associated with that machine.
- **Source Core.** The Core that protects the machines that have the Agent installed.
- **Target Core.** The Core to whose repository the request wants to send replicated data.
- **Machine.** The means by which you can select a machine.
- **Customer Id.** The identification number for the customer who made the replication request.
- **Email Address.** The contact information for the customer who requested replication to this core.
- **Core Name.** The name of the source core from which the customer wants to replicate.
- **Status.** The state of replication between the cores (for example, Pending or Approved.)

You can then review those requests and accept or deny them as appropriate. If you accept, replication is established and recovery points are sent from the source to the target cores.

1. Navigate to the Manage Replication section, and then click **Pending Requests**.
2. On the Pending Requests page, in the Machine column, expand the Core from which the replication request was sent.
3. To refresh the list, click **Update Status**, and then click Yes in the dialog box to confirm.
4. Select the Core again, and then click **Review**.

    The Pending Request dialog box opens.
5. If you want to approve the request, under Review Replication Request, do the following:
    a. Select the target machine to which you want to replicate, or enter a new remote core for this replication by entering the following information:
        - Core name
        - Subscription email address
        - (Optional) customer ID for this machine
    b. Select the protected machines and associated repositories for the replication.

c. Optionally, enter a comment for the customer to see.
d. Click **Send Response** to establish replication.

6. To deny the request, click **Deny**.

   On the Pending Requests page, the Status column updates to display the status as either Approved or Denied as appropriate.

Removing replication in the Rapid Recovery Add-on for Kaseya

When you remove replication, you stop further replication of recovery points from a protected machine. After you remove replication in the add-on console, the pairing between the source Core and target Core continues to exist. To remove replication completely, you must do so using the Core Console on each core machine. For more information about removing replication from the Rapid Recovery Core Console, see the *Rapid Recovery User Guide*.

1. Navigate to the Manage Replication section, and then click **Remove Replication**.
2. Select the protected machine or machines for which you want to remove replication, and then click **Remove Replication**.

   The **Remove Replication** dialog box opens.
3. To also remove associated recovery points, click **Delete Recovery Points**.
4. Click **Yes**.

Related tasks

See also: Preparing for replication
See also: Establishing replication
See also: Viewing pending replication requests in the Rapid Recovery Add-on for Kaseya

Monitoring Rapid Recovery activity in the Add-on for Kaseya

Within the Rapid Recovery Add-on for Kaseya, you can view pertinent event information about all of the machines in your environment. The pages offer details such as machine name, IP Address, version of Rapid Recovery software, and machine type (Core or Agent), identify each machine, which the start and end times and the status of each event conducted by Rapid Recovery help you monitor relevant activity.

Viewing machine activity in the Rapid Recovery Add-on for Kaseya

Complete the following steps to view the tasks for individual protected machines.

1. Navigate to the Monitor section, and then click **Machines**.
2. To view a list of all associated tasks for a particular machine, expand the machine.
3. To view more information about a particular task, in the Message column, click **View Details** for that task.

Viewing events in the Rapid Recovery Add-on for Kaseya

Complete the following steps to view all events for a Rapid Recovery environment.

1. Navigate to the Monitor section, and then click **Events**.
2. To view the details of a particular event, click the **View Details** icon in the row for that event .

   The Log Details window opens and shows important information regarding the event status and any errors that may have occurred.

Managing Rapid Recovery Core reports in the Add-on for Kaseya

The Rapid Recovery Add-on for Kaseya lets you generate reports for one or more Cores. It does not generate reports for individual protected machines; however, the reports include information about the protected machines that the selected Cores protect.

With the Add-on for Kaseya, you can generate the following reports:

- Core Summary report
- Critical Event report

The Core Summary report provides details about jobs performed and the status of those jobs. It also generates a Core Status report. Together, the reports include the following information:

- **Core.** The Core for which you ran the report.
- **Agent.** The name of the protected machine that the Core protects.
- **Type.** The type of job performed (for example, Transfer).
- **Summary.** A brief description of the actions that the job performed.
- **Status.** The status of the job (for example, Succeeded or Failed).
- **Error.** The type of error that caused the failure if a failure occurred.
- **Start Time.** The time at which the job began.
- **End Time.** The time at which the job ended.
- **Time.** The duration of the job (for example, 2m 16s for 2 minutes and 16 seconds).
- **Total Work.** The amount of data affected. For example, a transfer job could have a Total Work of 53.7MB.

The Critical Event report also generates a Core Status report. Together, the reports include the following information:

- **Core.** The Core for which you ran the report.
- **# of Failures.** The number of jobs that failed to complete for the Core you selected.
- **Type.** The type of job performed. For example, Transfer.
- **Summary.** A brief description of the actions that the job performed.
- **Status.** The status of the job. For example, Succeeded or Failed.
- **Error.** If a failure occurs, the error that caused the failure.
- **Start Time.** The time at which the job began.

The following procedures describe how to create and view reports.

Creating reports in the Rapid Recovery Add-on for Kaseya

The Rapid Recovery Add-on for Kaseya provides a consolidated reporting feature that lets you create summary reports for selected Rapid Recovery Cores and activities for Rapid Recovery protected machines that the Core protects.

1. Navigate to the Reporting section, and then click **Create Report**.
2. Select the Core or Cores for which you want to create the report.
3. (Optional) In the **Description** text box, enter a text description.
4. To designate a time span of data that should be included in the report, use the **Start time** and **End time** calendars.
5. Click **Run report**.
6. In the dialog box, click **OK** to acknowledge that the report has been scheduled.

   In the Most Recent Report Status column, the status of In Progress appears. This status changes to Completed when the report has been created.

Related tasks

See also: Viewing reports in the Rapid Recovery Add-on for Kaseya

Viewing reports in the Rapid Recovery Add-on for Kaseya

The reports you can create for Rapid Recovery Core machines are useful for compliance. They contain information about the Rapid Recovery Core and protected machine activities associated with the Core.

Complete the steps in following procedure to view the summary reports.

1. Navigate to the Reporting section, and then click **View Reports**.
2. Click the link for the report you want to view (for example, View Core Summary Report).

   The View Reports page refreshes with the full report details.

   On the View Reports page, you can view the status of the Core in the report (for example, Available).

Under Core Summary Report, you can view a detailed list of the protected machine activities associated with the Core in the report. These details include the type of activity, summary description, status, start and end time, duration for the activity, and amount of disk space required for the activity.

3. If the report spans multiple pages, click the page numbers or the arrow buttons at the bottom of the report results to page through the results.
4. To export the report results to a different format, select a format for the export from the drop-down list and click **Save**.
    - **Available formats include PDF, XLS, XLSX, CSV, and HTML.**

Related tasks

See also: Creating reports in the Rapid Recovery Add-on for Kaseya

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/company/contact-us.aspx or call + 1-949-754-8000.

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:

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