Quest

Quest® vRanger® 7.7

Integration Guide for Quest® DR Series Disk Backup Appliance

© 2018 Quest Software Inc.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

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

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

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

Patents

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

Trademarks

Quest, the Quest logo, Foglight, NetVault, vRanger, and Join the Innovation are trademarks and registered trademarks of Quest Software Inc. vCenter, vSphere, vMotion, VMware, and ESXi are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions. Active Directory, Hyper-V, SharePoint, SQL Server, Windows, and Windows Server are registered trademarks of Microsoft Corporation in the United States and/or other countries. Data Domain and DD Boost are trademarks or registered trademarks of EMC Corporation in the United States and other countries. 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

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

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

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

vRanger Integration Guide for Quest® DR Series Disk Backup Appliance
Updated - November 2018
Software Version - 7.7

Contents

2

Getting started

- vRanger integration quick start for Quest® DR Series
- Product overviews

IMPORTANT: The information in this topic is intended only to provide an overview of the steps and information required to configure vRanger and the Quest DR Series appliance. Before implementing this solution, review the full vRanger and Quest DR Series documentation.

vRanger integration quick start for Quest® DR Series

Integrating vRanger with a Quest DR Series appliance is achieved by adding the DR Series appliance to vRanger as a Quest Rapid Data Access (RDA) repository. The following steps describe the integration process at a high level, and provide links to the remaining topics for more exploration. Before implementing this solution in a production environment, read this information thoroughly.

1. **Confirm integration requirements**: Before starting the integration, confirm that you are using supported versions of vRanger and the DR Series software. For more information, see Product requirements for integration.
2. **Install and configure the DR Series**: To install your DR Series and integrate with vRanger, perform the following operations:
   - **Install the DR Series hardware**: Assemble the rails, and install and connect the DR Series to your infrastructure.
   - **Log in and initialize the DR Series**: Log in to the DR Series system CLI by using a local console keyboard-video-mouse (KVM) connection or an iDRAC connection. Configure your system network settings using the Initial System Configuration Wizard.
   - **Configure network settings**: Ensure that you have an active network connection and a fully configured IP address.
   - **Register and configure your DR Series**: Log in to the web interface and complete the registration process and Initial System Configuration Wizard, which includes password administration, Active Directory connection, and additional network configuration.
   - **Create a storage container**: Containers function like a shared file system, which can be assigned a connection type of None (to be defined later), NFS/CIFS, or RDA (includes Rapid Data Storage [RDS] clients). Containers can then be accessed using Network File System (NFS), Common Internet File System (CIFS), or RDA.

     IMPORTANT: For integration with vRanger, create an RDA container, with the RDA Type setting as RDS.
3. **Install vRanger:** Using the vRanger installer, install vRanger on a machine meeting the vRanger system requirements. For a high-level overview of the vRanger installation process, see Installing vRanger. For more information, see the *Quest vRanger Installation/Upgrade Guide*.

4 **Create a Quest RDA repository**: After vRanger is installed, add the DR Series to vRanger as a Quest RDA repository. Any backup written to this repository is deduplicated according to your DR Series configuration.

Product requirements for integration

To integrate vRanger with a DR Series appliance, you must be using one of the following supported product versions:

- vRanger:
  - 7.1 or later—for RDA integration
  - 7.0—for CIFS/NFS only
- DR Series systems:
  - DR4x00
  - DR6x00
- DR Series software:
  - 4.0.3 or later—for RDA integration
  - 4.0.3 or later —for CIFS/NFS only

Product overviews

The following topics provide an overview of vRanger and the Quest DR Series appliances, and important information about the licensing required to integrate the two products.

What is vRanger?

vRanger is the leading VMware® data protection solution that also backs up and recovers Windows® physical servers and files with blazing speed and minimal storage requirements. With vRanger, you get comprehensive protection for both virtual and physical environments that you can manage from one intuitive interface.

vRanger has historically supported the Quest DR Series systems as repositories, but required that the Quest DR Series system was configured as an NFS share. vRanger extends this functionality to support the more advanced functionality offered by the DR Series, and allow direct configuration of Quest RDA repositories.

vRanger licensing

For virtual machine (VM) backup, a license for vRanger controls the number of source CPUs that you can configure for backup. For licensing purposes, a multi-core processor is counted as a single CPU. For physical backup, each server protected consumes one physical backup license.

Every VMware® ESXi™ host for which vRanger is expected to provide protection must be properly licensed, both by VMware and in the vRanger Host Licensing tab.

IMPORTANT: A Quest vRanger license is required for integration with the Quest DR Series. vRanger Standard Edition (SE) and vReplicator are not supported by Quest DR Series. This topic uses “vRanger” for simplicity, but only vRanger Backup & Replication is supported for use with Quest DR Series.

Quest DR Series overview

The DR Series system is a high-performance, disk-based backup and recovery appliance that is simple to deploy and manage, and offers unsurpassed Total Cost of Ownership benefits. Features such as innovative firmware and an all-inclusive licensing model ensure optimal functionality and the assurance of no hidden costs for desired future features.

Using Quest deduplication and compression algorithm technology, this system can achieve data reduction levels averaging 15:1. This reduction in data results in less incremental storage needs and a smaller backup footprint. By removing redundant data, the system provides deduplication and compression that delivers:

- Fast, reliable backup and restore functionality.
- Reduces media usage and power and cooling requirements.
- Improves overall data protection and retention costs.
- Reduces overall network traffic—as only unique data is transmitted.
- Allows for increased scalability through the addition of more RDA capable devices.

The benefits of data deduplication can be extended across the enterprise—through the deduplicated replication function—to provide a complete backup solution for multi-site environments.

Shorter Recovery Time Objectives (RTO) and more attainable Recovery Point Objectives (RPO) can be assured as critical backup data remains on disk and online longer. Capital and administrative costs are diminished at the same time as internal service-level agreements (SLAs) are more easily met.

The DR Series includes the following:

- Advanced data protection and disaster recovery.
- Simple management interface—using the system GUI.
- Wide variety of data backup installations and environments.

The Quest DR Series contains data backup and management software preinstalled on a Quest hardware appliance, which provides you with a robust disk-based data backup capability installed on a deduplication-enabled appliance.

The system supports two interface types, and the system software manages the storage containers using the following interfaces:

- A command line interface (CLI)
- A graphical user interface (GUI)

3

Understanding the Quest DR Series

- Available DR Series configurations
- DR Series features and concepts

IMPORTANT: The information presented in this topic is a summary of the full documentation. For more information, see the vRanger and Quest DR Series documentation.

Available DR Series configurations

The Quest DR Series system is a solution designed to reduce your backup data footprint using several comprehensive backup and deduplication operations that optimize storage savings.

The DR Series system consists of the following components:

- **Software:** The system software supports record linkage and context-based lossless data compression methods.
- **Hardware/VM:** Following are the hardware and virtual appliance (VA) types that support the DR Series:
  - DR2000v system: A VM template in various capacities for VMware® ESXi™ and Hyper-V® that can be deployed on our existing VM infrastructure.
  - DR Series appliance: A rack-based appliance available in various configurations.
  - Expansion shelf: The hardware system appliance supports the addition of external Quest PowerVault MD1200 data storage expansion shelf enclosures.

DR Series features and concepts

This topic provides an overview of the primary features and concepts in the Quest DR Series appliance.

- Deduplication and compression
- Replication
- Supported protocols
- Rapid Data Access (RDA)

Deduplication and compression

The DR Series design uses various data-reduction technologies, including advanced deduplication algorithms, in addition to the generic and custom compression solutions that prove effective across many differing file types. Data deduplication and compression is addressed in the following areas:

- **DR Series appliances:** The DR Series backup and recovery appliances provide both efficient and high-performance disk-based data protection to leverage the advanced deduplication and compression capabilities in the DR Series software. Based on technology that is now part of the Quest Data Protection

strategy, the DR Series provides a key component that performs backup, recovery, and data protection operations.

- **Deduplication**: This technology eliminates redundant copies of data and in the process it decreases disk capacity requirements and reduces the bandwidth needed for data transfer. Deduplication can be a major asset for companies that are dealing with increasing data volumes and require a means for optimizing their data protection.
- **Compression**: This technology reduces the size of data that is stored, protected, and transmitted. Compression helps companies improve their backup and recovery times while helping reduce infrastructure and network resource constraints.

In general, the DR Series appliances are Purpose Built Backup Appliances (PBBA) that offer advanced deduplication and compression capabilities to reduce the time and cost associated with backing up and restoring data. Based on deduplication and compression technology, the DR Series eliminates the need to maintain multiple copies of the same data. This product lets customers keep more data online longer and reduce the need for tape backup dependency.

Using its deduplication and compression technology, the DR Series can help achieve an expected data reduction ratio of 15:1. Achieving this reduction in data means that you need fewer incremental storage operations to run and it provides you with a smaller backup footprint. By removing redundant data, the DR Series deliver fast reliable backup and restore functionality, reduce media usage and power and cooling requirements, and improve your overall data protection and retention costs.

You can extend the benefits of data deduplication across the enterprise as well—using the DR Series deduplication replication function—to provide a complete backup solution for multi-site environments. With 32:1 deduplicated replication, up to 32 DR Series appliances can be replicated simultaneously to separate, individual containers on one central DR Series appliance. The DR Series uses compression with replication to shrink the data that is needed to be moved across the wire to a container.

Replication

Replication is the process by which the same key data is saved from multiple storage locations, with the goal being to maintain consistency between redundant resources in data storage environments. Data replication improves the level of fault-tolerance, which improves the reliability of maintaining saved data and permits accessibility to the same stored data. The DR Series system uses an active form of replication that lets you configure a primary-backup scheme. During replication, the system processes data storage requests from a specified source to a specified replica target, which acts as a replica of the original source data. This replica can then be cascaded optionally to a third location called a Cascaded replica for an additional copy.

NOTE: It is important to distinguish the difference between data that has been processed by backup, and data that has been processed by replication. This distinction is because backup saves a copy of data that generally remains unchanged for a long time.

Replicas and Cascaded replicas are read-only and are updated with new or unique data during scheduled or manual replications. The DR Series system can be considered to act as a form of a storage replication process in which the backup and deduplication data is replicated in real time or using a scheduled window in a network environment. In a replication relationship between two or three DR Series systems, this configuration means that a relationship exists between several systems. One system acts as the source and the other as a replica, with an optional third cascaded replica if you have chosen to keep two instances of replicated data in your backup workflow.

Supported protocols

The DR Series supports the following file system protocols:

- Network File System (NFS)
- Common Internet File System (CIFS)
- Rapid Data Access (RDA)

- Rapid Data Storage (RDS)

NOTE: The DR Series supports three container connection types: NFS, CIFS, and RDA. RDS provides a logical disk interface that can be used with network storage devices to store data and support data storage operations.

Rapid Data Access (RDA)

RDA is developed by Quest and provides a logical disk interface for use with network storage devices. RDS allows for better coordination and integration between DR Series backup, restore, and optimized duplication operations with vRanger and Quest NetVault Backup.

The DR Series and vRanger integration is done using the Rapid OFS (ROFS) plug-in developed by Quest. The ROFS plug-in allows vRanger control over backup image creation, deletion, and duplication. RDS allows deduplication operations to happen on the client-side so that network traffic can be reduced.

The RDS protocol allows the supported backup applications to communicate directly with the DR Series and determine whether a specific chunk of data exists on the system. If the data exists, only the pointers need to be updated on the DR Series, and the duplicate chunk of data does not need to be transferred to the system. This process provides two benefits: it improves the overall backup speed, and also reduces the network load.

4

Installing and configuring your Quest DR Series

Installing the DR Series hardware

IMPORTANT: The information in this topic is a summary of that found in the Quest DR Series documentation. Procedures in this topic are abbreviated to provide a high-level overview of the installation process. Before installing your Quest DR Series system, review the full set of documentation, including:

- *Setting Up Your Quest DR Series System*
- *Quest DR Series Systems Getting Started Guide*
- *Quest DR Series Owner's Manual*
- *Quest DR Series System Administrator Guide*

Prerequisites

Before installing the DR Series appliance, ensure that the following requirements have been met:

- You must use a supported version of vRanger and the DR Series system. For more information, see Product requirements for integration.
- An active network with available Ethernet cables and connections.
- If the system has a 1 GbE network interface card (NIC), connect all NIC ports on the NIC daughter card. If the system has a 10 GbE NIC, connect both the 10 GbE ports on the NIC daughter card. Do not connect to 1 GbE ports if there is a 10 GbE NIC available on the system.
- Network values required are IP addressing, network mask, default gateway, DNS suffix, primary (and optional) DNS server, and host name. If DHCP is selected, these values are populated based on your DHCP configuration. If DHCP is not selected, the values must be manually configured.
- Defaults for the DR Series are:
  - **Default Static System IP:** 10.77.88.99

    NOTE: Default static system IP is used only when there is no DHCP server. The default IP can be used to configure the system using a point-to-point NIC connection.
  - **Subnet mask IP:** 255.0.0.0
  - **Default iDRAC IP:** 192.168.0.120

    NOTE: For iDRAC connection, the login name is **root** and password is **calvin**.

- On the first boot, you must set up the network and the host name for the Quest DR Series system.
- Connect the Quest DR Series system to a keyboard and monitor when you set up the system for the first time. After the operating system and network are configured, the system can be managed using a remote browser interface.
- To set up the Quest DR Series system, use an account with administrator privileges.

Installing the DR Series

To install the DR Series appliance:

1. Unpack your rack system and identify each part.
2. Assemble the rails, and install the system in the rack following the safety instructions and the rack installation instructions provided with your system.
3. [Optional] Connect the keyboard, mouse, and monitor.

   The connectors on the back of your system have icons indicating which cable to plug into each connector. Be sure to tighten any screws on the monitor's cable connector.
4. Connect the system's power cable or cables to the system, and, if a monitor is used, connect the monitor's power cable to the monitor.
5. Bend the system power cable or cables, as shown in the *Quest DR Series Getting Started Guide*, and attach to the cable strap.
6. Plug the other end of the power cable or cables into a grounded electrical outlet or a separate power source such as an uninterruptible power supply (UPS) or a power distribution unit (PDU).
7. Press the power button on the system.

   The power indicator should light.
8. [Optional] Install the bezel.

Initializing the DR Series

Before you can start using the DR Series system GUI for the first time, you must properly initialize the system. To initialize the DR Series system, complete the following:

1. Log in to the DR Series system CLI by using a local console KVM connection or an iDRAC connection.
2. Configure your system network settings using the **Initial System Configuration Wizard**.

   This wizard lets you configure the following network settings to complete a first-time initialization of your system:

   - IP addressing mode
   - Subnet mask address
   - Default gateway address
   - DNS suffix address
   - Primary DNS server IP address
   - [Optional] Secondary DNS server IP address
   - Host name for system

Configuring local console connections

To configure a local console connection, you must make the following two back chassis cable connections:

- VGA port and your video monitor
- USB port and your keyboard

IMPORTANT: For more information, including port diagrams, see the *Quest DR Series System Administrator Guide*.

To make local console cable connections for the DR Series appliances:

1 Locate the VGA monitor port and the USB ports on the back of your system.

1 Connect the video monitor to the VGA port on the back of your system.

2 Connect the USB keyboard to one of the two USB ports on the back of your system.

You are now ready to perform initialization using the DR Series system CLI login process.

Configuring the iDRAC connection

The iDRAC connection requires a network connection between the integrated Quest Remote Access Control (iDRAC) management port on the DR Series system and another computer running the iDRAC remote console session in a supported browser. The iDRAC provides remote console redirection, power control, and the out-of-band (OOB) system management functions for the DR Series system. iDRAC connections are configured using console redirection and the iDRAC6/7 web interface. The login values you can use for making iDRAC connections are:

- Default username: root
- Default password: calvin
- Default static IP address: 192.168.0.120

NOTE: For information on how to configure the iDRAC, see the *Dell RACADM Command Line Reference Guide* at http://www.dell.com/support/home.

When the Quest DR Series System splash screen is displayed, you are ready to begin initialization using the DR Series system CLI login process.

Logging in and initializing the DR Series

Use the DR Series system CLI and the **Initial System Configuration Wizard** to log in to and initialize the system. After completing a local console or iDRAC connection, log in to the DR Series system CLI:

1 Launch a terminal emulator application, such as PuTTY, and type the default IP address, 10.77.88.99, for the DR Series system, if you are not using iDRAC or a local console.

2 At the **login as:** prompt, type **administrator**, and press **Enter**.

3 At the **administrator@<system_name> password:** prompt, type the default administrator password, **St0r@ge!**, and press **Enter**.

4 To configure the network settings, type **y** (for yes), and press **Enter**.

When completed, a successful initialization message is displayed.

NOTE: For complete information on configuring networking, see “Logging in and Initializing the DR Series System” in the *Quest DR Series System Administrator Guide*.

5 At the prompt, type **exit**, and press **Enter** to end the DR Series system CLI session.

You are now ready to log in to the system using the DR Series system GUI.

NOTE: Before you log in to the system using the DR Series system GUI, make sure to register it in the local Domain Name System (DNS) for your network so that it is a DNS-resolvable entry.

Registering and configuring your DR Series

To log in to and register the DR Series system using a browser-based connection, complete the following topics.

NOTE: This procedure describes the login process from a first-time perspective, starting with the Customer Registration and Notification page, the completion of the Initial System Configuration Wizard process, and the Initial Software Upgrade page. For more information, see the *Quest DR Series System Administrator Guide*.

Logging in to the web interface

1. In a supported web browser, type the IP address or host name of the system in the browser Address bar, and press **Enter**.

   NOTE: If you want to reset your login password, click **Reset Password** on the **DR Series System Login** page. The **Reset Password** dialog box is displayed. The reset options displayed depend on the password reset option you configured earlier. By default, the service tag option is displayed. In Service Tag, enter the service tag number ID for the system, and click Reset Password to reset the system password back to its default—or click Cancel to return to the DR Series System Login page.

2. In **Password**, type **St0r@ge!**, and click **Log in** or press **Enter**.

   The **Customer Registration and Notification** page is displayed.

Registering your DR Series

Before you can begin using the DR Series system GUI, you need to register the system with Quest. In addition, this page also allows you to sign up for notifications about appliance alerts and system software updates.

1. In the **Settings** pane of the **Customer Registration and Notification** page, complete the following:
   - In **Contact Name**, enter a system contact name.
   - In **Relay Host**, enter a host name or IP address for the relay host.
   - In **Email Address**, enter an email address for the contact.
   - To be notified about system appliance alerts, select **Notify me of DR Series appliance alerts**.
   - To be notified about system software updates, select **Notify me of DR Series software updates**.
   - To be notified about container statistics daily, select **Notify me of *<DR Series>* daily container stats reports**.
   - To prevent display of the **Customer Registration and Notification** page again, select **Don't show me this again**.
2. Click **Confirm** to have the DR Series system accept your settings—or click **Skip** without configuring any settings—to proceed with initialization.

   The **Initial System Configuration Wizard** page is displayed.

Changing your password

1 To start the initial system configuration process, click **Yes**.

> **NOTE:** If you click No, you bypass the initial system configuration process, and the DR Series System Dashboard page is displayed. However, when you next log in to the DR Series system, you are prompted to perform the initial system configuration process again with the Initial System Configuration Wizard page is displayed.

2 In the **Settings** pane of the **Initial Configuration — Change Administrator Password** page, complete the following:

- In **Current Password**, enter the current administrator password.
- In **New Password**, enter the new administrator password.
- In **Retype New Password**, enter the new administrator password again to confirm it.

3 Click **Next** to continue with the initial configuration process.

The **Initial Configuration — Networking** page is displayed.

Configuring your DR Series system

For detailed configuration information, see the “Configuring the DR Series System Settings” topic in the *Quest DR Series System Administrator Guide*. The “Configuring the DR Series System Settings” topic addresses topics such as:

- Configuring network settings.
- Managing the DR Series system password.
- Configuring Active Directory settings.
- Configuring date and time settings.

The information presented in Managing storage containers is specific to the integration with vRanger. For more information on integrating vRanger with a Quest DR Series system Rapid Data Access (RDA) repository, see the *Quest vRanger User’s Guide*.

Managing storage containers

After initialization, the DR Series system contains a single default container named **backup**. Containers function like a shared file system, which can be assigned a connection type of None (to be defined later), NFS/CIFS, or RDA (includes RDS clients). Containers can then be accessed using NFS, CIFS, or RDA.

> **IMPORTANT:** For the most beneficial integration with vRanger, an RDA connection should be used.

Creating a storage container

By default, the DR Series system provides a container named **backup** for your use after you complete the basic system configuration and initialization process. You can create additional containers to store your data as needed.

> **NOTE:** NOTE: The DR Series system does not support creating container names that begin with a 0 (zero). In addition, many of the DR Series system GUI and CLI operations do not work when a container name begins with a 0.

Containers function like a shared file system that can be accessed using the following connection types:

- NFS/CIFS
- NFS

- CIFS
- RDA
- RDS
- None (an unassigned connection type)

Choosing the **None** or unassigned connection type lets you create containers that can be configured later as needed. To modify a container configured with a **None** connection type, select the container, click **Edit**, and start configuring it as applicable.

Creating an RDS connection type container

To create an RDS connection type container:

1 Select **Storage > Containers**.

The **Containers** page displays all existing containers.

2 Click **Create**.

3 In **Container Name** on the **Create New Container** dialog box, type the name of the container.

Container names cannot exceed 32 characters in length, and can be composed of any combination of the following characters:

- A to Z (uppercase letters)
- a to z (lowercase letters)
- 0 to 9 (numbers)
- Dash (-) or underscore (_) special characters

NOTE: The DR Series system does not support the use of the following special characters in container names: /, #, or @. In addition, the first container name cannot be a number.

4 In **Marker Type**, select **Auto**.

Selecting Auto marker type enables all marker types to be detected. As a best practice, if you have only one type of DMA with traffic directed to a container, it is best to select the corresponding marker type. As a best practice, if you have traffic from a DMA that is not one of the supported marker types, it is best to disable marker detection for the container by selecting the None marker type.

5 In **Connection Type**, select **RDA**.

6 In **RDA** type on the **RDA** pane, select **RDS**.

7 In **Capacity**, select one of the following options allowed per container:

NOTE: When RDS is selected, by default, **Unlimited** is selected. Under **Capacity**, the **Size** field is inactive.

- **Unlimited:** This option defines the allowed amount of incoming raw data per container—based on the physical capacity of the container.
- **Size:** This option defines a set limit in Gigabytes (GiB) for incoming raw data allowed per container.

8 Click **Create a New Container**, or click Cancel to display the Containers page.

After creating the container, the Containers page is displayed and includes a **Successfully Added** dialog box. The list of containers in the Containers summary table is updated with your new container—and its new status is reflected as N/A in the Replication column of this table.

NOTE: There are many more configurations that may be required for proper operation of the DR Series appliance in your environment. For complete information on configuring your DR Series, see the *Quest DR Series System Administrator Guide*.

5

Installing vRanger

- vRanger system requirements
- Installing vRanger
- Configuring vRanger
- Adding a Quest Rapid Data Access (RDA) repository

IMPORTANT: The information in this topic is intended only to provide an overview of the steps and information required to configure vRanger and the Quest DR Series appliance. Before implementing this solution, see the full vRanger and Quest DR Series documentation.

vRanger system requirements

Before installing vRanger and the DR Series appliance, ensure that you read and understand the requirements and operation of both products. The following topics summarize the system requirements for vRanger. The information is a summary only. Before implementing vRanger, review the *Quest vRanger Installation/Upgrade Guide*.

IMPORTANT: You must use a supported version of vRanger and the DR Series system. For more information, see Product requirements for integration.

Minimum hardware requirements

The minimum hardware requirements to run vRanger can vary widely based on several factors. Therefore, you should not do a large-scale implementation without first completing a scoping and sizing exercise.

vRanger: physical machine

The following describes the hardware recommendations for the vRanger physical machine:

Table 1. Requirements for a installing vRanger on a physical machine

CPU	Any combination equaling four cores of CPUs are recommended. Example one quad-core CPU; two dual-core CPUs.
RAM	4 GB RAM is required.
Storage	At least 4 GB free hard disk space on the vRanger machine.
HBA	For LAN-free, Quest recommends that you use two HBAs—one for read operations and one for writing.

vRanger: virtual machine (VM)

The following describes the hardware recommendations for using vRanger in a VM:

Table 2. Requirements for a installing vRanger on a virtual machine

CPU	Four vCPUs.
RAM	4 GB RAM is recommended.
Storage	At least 4 GB free hard disk space on the vRanger machine.

Requirements for physical backup and restore

When backing up from and restoring to a physical server, vRanger uses a client run on that server to perform backup and restore operations. To process the backup workload effectively, the physical server must meet the following requirements:

Table 3. Requirements for physical backup and restore

CPU	Any combination equaling four cores of CPUs are recommended. Example one quad-core CPU; two dual-core CPUs.
RAM	2 GB RAM is required.

Additional requirement for repository replication

If you set up repository replication, increase the Task Timeout setting beyond the default 24 hours for the initial synchronization. If the initial synchronization involves the transfer of many terabytes of data, you might need to increase the task timeout to over a hundred hours.

1. On the Main toolbar, click **Tools > Options**.
2. Under the My Jobs node, click **Configuration**.
3. In the **Timeout** section, change the **Task Timeout** field to **100** or more, depending on the size of the environment.

   After the initial synchronization of the repositories is finished, you can update this field to an appropriate number.
4. Click **OK**.

Supported operating systems for installation

The following operating systems are supported for installation of vRanger.

Table 4. Supported operating systems

Operating system	Service pack level	Bit level
Windows Server 2008 R2[ab]	SP1 or later	x64
Windows Server 2012[b]	All service packs	x64
Windows Server 2012 R2[bc]	All service packs	x64
Windows Server 2016[b]	All service packs	x64

a. Windows 2008 R2 SP1 requires Windows Management Framework 3.0. Refer to Known Issue VR-177 in the vRanger Release Notes for more information.
b. The Windows Storage Server edition is not supported as an installation platform for vRanger.
c. Before installing vRanger on Windows Server 2012 R2, the updates listed in Additional required software must be installed.

Additional required software

In addition to a supported version of Windows® and a supported VMware® Infrastructure, you may need some additional software components, depending on your configuration.

- **Microsoft® .NET Framework**: vRanger requires the .NET Framework 4.5. The vRanger installer installs it if not detected.
- **SQL Server**: [Optional] vRanger utilizes two SQL Server® databases for application functionality. vRanger can install a local version of SQL Express 2008 R2 or you can choose to install the vRanger databases on your own SQL instance.
- **Windows PowerShell 3 or above.**If you are installing vRanger on Windows 2008 R2 SP1, you will need to install WIndows PowerShell 3 or above before installing vRanger
- **vRanger virtual appliance (VA)**: The vRanger VA is a small, pre-packaged Linux® distribution that serves as a platform for vRanger operations away from the vRanger server. vRanger uses the VA for the following functions:
  - Replication to and from VMware® ESXi™ hosts.
  - File-level restore (FLR) from Linux machines.
  - Optionally for backups and restores.
- **Updates for Windows Server 2012 R2**: Before installing vRanger on Windows Server 2012 R2, ensure that the Windows updates listed below are installed:
  - KB2939087
  - KB2975061
  - KB2919355
  - KB2999226

Installing vRanger

The installation of vRanger has several options. Unless you have a valid reason not to, accept the defaults wherever possible. The installation follows this sequence:

1. Launch the installer, and accept the vRanger license.

   The install process does not continue until the license is accepted.
2. Enter the credentials under which the vRanger services should run.

   The credentials used need to have local administrator privileges on the vRanger machine.
3. Choose an installation directory.
4. Select the vRanger database.

   You may choose to install vRanger with a new instance of SQL Server® Express or on an existing SQL Server.
5. Configure the runtime credentials for the vRanger Database.
6. [Optional] Install the vRanger Catalog Service.

   The installation completes.

For more information, see the *Quest vRanger Installation/Upgrade Guide*.

Configuring vRanger

vRanger requires some basic configuration before data protection can begin. The bulk of this configuration is driven by the Startup Wizard which starts the first time the application is opened. For more information, see the *Quest vRanger Installation/Upgrade Guide*.

The following lists the primary configurations you need to make.

- **Add source servers:** Before you can begin backups, you must add one or more source objects to the vRanger inventory. Source objects can include VMware® vCenter™ or ESXi™ hosts, Hyper-V® clusters or hosts, or physical machines.
- **Add vRanger virtual appliances (VAs):** vRanger VAs allow you to distribute the backup workload and gain direct access to target VM's storage for improved performance.

  IMPORTANT: To be able to run in Deduplication Mode, the vRanger VA should be configured with four vCPUs and 2 GB of RAM. This configuration lets you run four backup jobs per VA.

- **Add repositories:** Repositories are where vRanger stores the savepoints created by each backup job. For the purposes of this integration, a Quest Rapid Data Access (RDA) repository should be used.

Adding a Quest Rapid Data Access (RDA) repository

The Quest DR Series disk-based data protection appliances optimize storage utilization and reduce network bandwidth requirements with in-line deduplication, server-side compression, and compressed and deduplicated replication.

The Quest DR Series supports CIFS, NFS, and RDA protocols. The RDA protocol provides a logical disk interface for the DR Series system. The RDA protocol also enables better coordination and integration between vRanger and the DR Series system and provides for client-side deduplication of vRanger backups.

NOTE: Quest recommends that you use the RDA protocol when using a Quest DR Series system as a repository.

For more information about the Quest DR Series systems, see the *Quest DR Series System Administrator Guide*.

This topic describes the process for adding a Quest Rapid Data Access (RDA) repository. The following procedure assumes that:

- You have a properly configured the Quest DR Series appliance that is accessible to the vRanger machine.
- You created at least one storage container to be used as a Logical Storage Unit. When creating the storage container, use the options:
  - Connection type: RDA
  - RDA type: RDS
- You have designated an RDA User account.
- You configured your firewall to enable the following TCP ports.
  - 9904
  - 9911
  - 9915
  - 9916
  - 9920

NOTE: For information on setting up the preceding configurations, see your Quest DR Series documentation.

To add a Quest DR Series system as a Quest RDA repository:

1. In the **My Repositories** pane, right-click anywhere, and click **Add > Quest Rapid Data Access (RDA)**.
2. In the **Add Quest Rapid Access Repository** dialog box, complete the following fields:
   - **Repository Name**: Enter a descriptive name for the repository.
   - **Description**: [Optional] Enter a long-form description for the repository.
   - **DNS Name or IP**: Enter the DNS name or IP address of the Quest DR Series system.
   - **RDA Username**: Enter a user account that can be used to log in to the device. On the Quest DR Series system, only one user account exists, and the user ID for that account is **backup_user**. You can only change the password for this account; you cannot create an account or delete the existing account.
   - **RDA Password**: Enter the password for the user account—the default is: **St0r@ge!**
   - **Logical Storage Unit**: Enter the name of the storage container. Ensure that the container is created before you add the device. You cannot add the device if the specified container does not exist on the device. When creating the storage container, use the options:
     - Connection type: RDA
     - RDA type: RDS
   - **Port Number**: Leave this value at 0 to use the default.
3. Click **OK**.

   The connection to the repository is tested and the repository is added to the **My Repositories** pane and the **Repository Information** dialog box.

   vRanger checks the configured repository location for existing manifest data to identify existing savepoints.
4. If vRanger finds existing savepoints, click the applicable button:
   - **Import as Read-Only:** To import all savepoint data into the vRanger database, but only for restores, click this button. You cannot back up data to this repository.
   - **Import:** To import all savepoint data into the vRanger database, click this button. vRanger is able to use the repository for backups and restores. vRanger requires read and write access to the directory.
   - **Overwrite:** To retain the savepoint data on the disk and not import it into vRanger, click this button. vRanger ignores the existence of the existing savepoint data and treats the repository as new.

Configuring repository replication

Replication is configured through the My Repositories pane of the vRanger interface.

TIP: For more information on repository replication, see the *Quest DR Series System Administrator Guide*.

The following procedure assumes that:

- You have configured at least one Quest RDA repository in vRanger.
- At least one other Quest DR Series appliance with RDA is available in your environment to serve as the replication target. You do not have to add this device to vRanger.

To configure Replication:

1. In the **My Repositories** pane, right-click the Quest Rapid Data Access (RDA) repository, and select **Configure Replication**.
2. In the **Configure Replication** dialog box, complete the following fields:
   - **Repository Name**: Enter a descriptive name for the repository.
   - **Description**: [Optional] Enter a long-form description for the repository.
   - **DNS Name or IP**: The DNS name or IP address of the Quest DR Series system.
   - **RDA Username**: Enter a user account that can be used to log in to the device. On the Quest DR Series system, only one user account exists, and the user ID for that account is **backup_user**. You can only change the password for this account; you cannot create an account or delete the existing account.
   - **RDA Password**: Enter the password for the user account.
   - **Logical Storage Unit**: Enter the name of the storage container. Ensure that the container is created before you add the device. You cannot add the device if the specified container does not exist on the device. When creating the storage container, use the options:
     - Connection type: RDA
     - RDA type: RDS
   - **Port Number**: Leave this value at 0 to use the default.
3. Click **OK**.

   The connection to the device is tested and the device is added as a repository is added to the **My Repositories** pane and the **Repository Information** dialog box.

After replication is configured for a repository, the **Configure Replication** option is disabled for that repository.

IMPORTANT: After a repository is configured for replication, you must select a synchronization method before replication occurs. For more information, see Managing repository replication.

Editing a replication configuration

You may edit an existing replication configuration to update credentials or timeout values. You may also use the **Edit Repository Details** dialog box to view free space for the repository.

1. In the **My Repositories** pane, right-click the Quest Rapid Data Access (RDA) repository, and select **Edit Replication Configuration**.
2. In the **Edit Quest Rapid Data Access (RDA)** dialog box, edit any of the following fields:
   - **Repository Name**
   - **User Name**
   - **Password**
3. Alternatively, view the **Free Space** field for up-to-date information about this repository.
4. If you edited any of the fields, click **Update**.

Managing repository replication

vRanger supports repository replication. Repositories configured for replication can be synchronized in one of three ways:

- Automatically, after a successful backup task to that repository.
- As a separate job on a scheduled basis.

- Manually, using the Synchronize option.

Configuring a repository for automatic replication

When a managed repository is configured for savepoint replication, and a backup task completes successfully, each savepoint is also replicated to the replication repository.

To enable automatic savepoint replication:

1. From the **Tools** menu on the vRanger toolbar, select **Options**.
2. Under the **Repositories** node, select **Replication**.

   TIP: You may also right-click the target repository in the **My Repositories** pane, and select **Repository Replication Options**.

3. Select **Enable savepoint replication for a successful backup job task, and c**lick **Ok**.

Scheduling repository synchronization

When using scheduled repository synchronization, savepoints are replicated to the replication repository according to a configured schedule.

NOTE: When scheduling repository synchronization, ensure that the synchronization activity does not occur at the same time as backup jobs using the synchronized repository.

To schedule a repository synchronization:

1. From the **Tools** menu on the vRanger toolbar, select **Options**.
2. Under the **Repositories** node, select **Replication**.
3. In the **Repository Replication Configuration** pane, find the **Repository Name** column, and select the applicable repository.

   The repositories listed are the target repositories.
4. Select **Schedule repository synchronization**.
5. Configure the replication schedule as desired, using the following information as a guide.
   a. **Start**: In the drop-down list, select the time for the replication task to begin.
   b. **Recurrence Pattern**: Establish how often the changes should be synchronized. There are five options within this section:
      - **Daily**: The daily option can be scheduled to synchronize the repository every weekday or every *x* number of days.
      - **Weekly**: Repository synchronization can be configured to run on weekly intervals, from every week to every 99 weeks. The day of the week on which to run synchronization tasks can be configured.
      - **Monthly**: The monthly option offers the following configurations:
        - **Day *[x]* of every *[y]* month:**

          x can be any value from 1 to 31. This value determines the day of the month on which the synchronization job occurs.

          y can be any value from 1 to 99. This value determines the monthly interval—for example, every two months sets the job to run every other month.
        - **The *[f]* *[d]* of every *[y]* month(s)**:

          f can be either: first, second, third, fourth or last.

d can be: weekday, weekend day, Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday.

y can be any value from 1 to 99. This value determines the monthly interval—for example, every two months sets the synchronization task to run every other month.

- **Yearly**: The yearly option offers the following configurations:
  - **Every *[m] [x]***:

    m is any month of the year. This value determines the month of the year in which the synchronization occurs.

    x can be any value from 1 to 31. This value determines the day of the month on which the synchronization occurs.
  - **The *[f] [d]* of *[m]***:

    f can be either: first, second, third, fourth, or last.

    d can be: day, weekday, weekend day, Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday.

    m is any month of the year. This value determines the month of the year in which the synchronization occurs.
- **Interval**: The interval option lets you select the number of days, hours, and minutes that should pass between synchronization jobs. The interval selected must be greater than or equal to five minutes.

6 Click **OK** to schedule the job.

Synchronizing a repository manually

1 In the **My Repositories** pane, right-click the source or replication repository, and select **Synchronize**.

2 When the confirmation prompt appears, click **Yes**.

Disabling repository replication

To disable repository replication:

1 Do one of the following:

- From the **Tools** menu on the vRanger toolbar, select **Options**. Under the **Repositories** node, select **Replication**.
- Right-click the replication repository, and select **Repository Replication Options**.

2 Clear the check box for **Enable savepoint replication for a successful backup job task** or **Schedule repository synchronization**, or both**.**

3 Click **OK**.

Replication is disabled as indicated by a red circle icon containing a white exclamation point.

Changing a replication repository to a primary repository

If your primary repository becomes corrupt or otherwise unavailable, you can quickly change your replication repository to a primary repository to continue backup and recovery operations.

To change a replication repository to a primary repository:

1 In the **My Repositories** pane, right-click the replication repository, and click **Remove**.

IMPORTANT: Ensure that **Delete all savepoints in this repository** is not selected.

2 Click **OK**.

3 In the **My Repositories** pane, click **Add**.

4 Select the applicable repository type.

5 Complete the **Add Repository** dialog box, and click **OK**.

6 When vRanger detects that the repository being added contains savepoint data and displays the **Warning: Existing Repository Found** dialog box, click **Import** to reconfigure the repository as a primary repository.

Removing a Quest Rapid Data Access (RDA) repository

The process for removing a Quest Rapid Data Access (RDA) repository is the same as removing any other repository type.

To remove a Quest Rapid Data Access (RDA) repository:

1 In the **My Repositories** pane, right-click the Quest Rapid Data Access (RDA) repository, and select **Remove**.

The **Remove Repository** dialog box appears, showing the savepoints in the selected repository.

When removing a repository, you have the option of keeping the savepoints on disk or deleting them. To remove the storage unit associated with the repository, you need to remove the savepoints. If replication is configured for this repository, you are also given the option to delete the savepoints in the replicated repository.

2 Select **Delete all savepoints in this repository**.

CAUTION: This step deletes the savepoints from the repository disk, not just the vRanger database. Exercise caution when deleting savepoints.

3 To delete the savepoints in a replicated repository, select **Delete all savepoints in replication repository**.

4 Click **OK**.

5 When the **Delete Savepoints** dialog box appears, click **OK**.

The savepoints are deleted, along with the storage unit associated with the repository.

Adding a Quest DR Series system as a CIFS repository

NOTE: Adding a Quest DR Series system as a CIFS repository does not take advantage of the full function of the DR Series system. Quest recommends adding the DR Series as an RDA repository.

To add a Quest DR Series system as a CIFS repository:

1 In the **My Repositories** pane, right-click anywhere, and click **Add > Windows Share (CIFS)**.

2 In the **Add Windows Network Share Repository** dialog box, complete the following fields:

- **Repository Name**: Enter a name for the repository.
- **Description**: [Optional] Enter a long-form description for the repository.
- **User Name** and **Password**: Enter the credentials for accessing the CIFS share.
- **Security Protocol**: Select a protocol, **NTLM** (default) or **NTLMv2**.
- **Server**: Enter the UNC path to the applicable repository directory. Alternatively, you may enter a partial path and click **Browse** to find the target directory.

NOTE: You must enter a valid username and password before using the browse functionality.

IMPORTANT: Do *not* select **Encrypt all backups to this repository.** Using encryption or compression with deduplicated repositories limits or disables deduplication. Encryption and compression should not be used with any repository type that provides deduplication.

3 Click **OK**.

The connection to the repository is tested and the repository is added to the **My Repositories** pane and the **Repository Information** dialog box.

vRanger checks the configured repository location for existing manifest data to identify existing savepoints.

4 If vRanger finds existing savepoints, click the applicable button:

- **Import as Read-Only:** To import all savepoint data into the vRanger database, but only for restores, click this button. You cannot back up data to this repository.
- **Import:** To import all savepoint data into the vRanger database, click this button. vRanger is able to use the repository for backups and restores. vRanger requires read and write access to the directory.
- **Overwrite:** To retain the savepoint data on the disk and not import it into vRanger, click this button. vRanger ignores the existence of the existing savepoint data and treats the repository as new.

5 Click **Next**.

Adding a Quest DR Series system as an NFS repository

NOTE: Adding a Quest DR Series system as a Network File System (NFS) repository does not take advantage of the full function of the DR Series system. Quest recommends adding the DR Series as an RDA repository.

To add a Quest DR Series system as an NFS repository:

1 In the **My Repositories** pane, right-click anywhere, and click **Add > NFS**.

2 In the **Add Network File Share Repository** dialog box, complete the following fields:

- **Repository Name**: Enter a descriptive name for the repository.
- **Description**: [Optional] Enter a long-form description for the repository.
- **DNS Name or IP**: Enter the IP or FQDN for the repository.
- **Export Directory**: Specify the export directory, which is similar in concept to a network share. You must create a target subdirectory in the export directory.
- **Target Directory**: Enter a subdirectory of the NFS export directory. This directory is the location to which savepoints are written.

IMPORTANT: Do *not* select **Encrypt all backups to this repository.** Using encryption or compression with deduplicated repositories limits or disables deduplication. Encryption and compression should not be used with any repository type that provides deduplication.

3 Click **OK**.

The connection to the repository is tested and the repository is added to the **My Repositories** pane and the **Repository Information** dialog box.

vRanger checks the configured repository location for existing manifest data to identify existing savepoints.

4 If vRanger finds existing savepoints, click the applicable button:

- **Import as Read-Only:** To import all savepoint data into the vRanger database, but only for restores, click this button. You cannot back up data to this repository.

- **Import:** To import all savepoint data into the vRanger database, click this button. vRanger is able to use the repository for backups and restores. vRanger requires read and write access to the directory.
- **Overwrite:** To retain the savepoint data on the disk and not import it into vRanger, click this button. vRanger ignores the existence of the existing savepoint data and treats the repository as new.

NOTE: For instructions on additional configurations and scheduling backup jobs, see the *Quest vRanger User's Guide*.

6

Maintaining your DR Series appliance

IMPORTANT: The procedures for maintaining the Quest DR Series are covered in the *Quest DR Series System Administrator Guide*. The information provided in the following topic is a summary of common maintenance tasks.

Setting up the DR Series Cleaner

Performing scheduled disk space reclamation operations are recommended as a method for recovering disk space from system containers in which files were deleted as a result of deduplication. The best method is to schedule a time when you can run the Cleaner on your DR Series system with no other planned processes running. Alternately, another method lets the Cleaner process on the DR Series system run whenever it determines that there are no active data ingests.

To schedule Cleaner operations on your system:

1. Select **Schedules > Cleaner Schedule**.
2. Click **Schedule** to create a schedule, or click **Edit Schedule** to modify an existing schedule.
3. Select or modify the **Start Time** and **Stop Time** setpoint values using the **Hour** and **Minutes** drop-down lists to create a Cleaner schedule.

   NOTE: You must set a corresponding Stop Time for every Start Time set in each Cleaner schedule you create. The DR Series system does not support any Cleaner schedule that does not contain a Start Time and Stop Time pair of setpoints—daily or weekly.

4. Click **Set Schedule** for the system to accept your Cleaner schedule, or click **Cancel** to display the **Cleaner Schedule** page.

The current Cleaner Status is represented on the Dashboard page in the System Information pane as one of the three following states:

- **Pending**: Displayed when there is any scheduled window set and the current time is outside the scheduled window for the Cleaner operation.
- **Running**: Displayed when the Cleaner operation is running during a scheduled window.
- **Idle**: Displayed only if there is no Cleaner operation running during a scheduled window.

Quest recommends that you do not schedule the running of any Cleaner operations during the same time period when replication or ingest operations are running. Failure to follow this practice affects the time required to complete the system operations and impacts your DR Series system performance.

Displaying Cleaner statistics

To display additional Cleaner statistics, you can use the DR Series system CLI **stats --cleaner** command to show Cleaner statistics.

For more information about DR Series system CLI commands, see the *Quest DR Series System Command Line Reference Guide*.

Monitoring performance

The **Dashboard** page contains system status indicators for the current state of the DR Series system (**System State**), current hardware state (**HW State**), current number of system alerts (**Number of Alerts**), and current number of system events (**Number of Events**). After backup jobs have run, the DR Series tracks Capacity, Storage Savings, and Throughput on the DR Series dashboard. This information is valuable in understanding the benefits the DR Series.

- **Capacity**: Used space and free space available in percentage and total (in gibibytes or tebibytes).
- **Storage Savings**: Total savings in percentage based on time (in minutes), which can be displayed in 1h (one hour—the default), 1d (one day), 5d (five days), 1m (one month), or 1y (one year) durations.
- **Throughput**: For reads and writes in volume based on time (in minutes), which can be displayed in 1h (one hour—the default), 1d (one day), 5d (five days), 1m (one month), or 1y (one year) durations.

NOTE: Deduplication ratios increase over time, it is not uncommon to see a 2 to 4x reduction (25 to 50% total savings) on the initial backup. As additional full backup jobs complete, the ratios increase. As mentioned previously, backup jobs with 12-week retention average a 15x ratio usually.

For more information on monitoring, see the “Monitoring the DR Series System” topic in the *Quest DR Series System Administrator Guide*.

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:

- 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.