QUEST SOFTWARE®

vRanger®

Version 5.4.1

Installation and Setup Guide

© 2012 Vizioncore, 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 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 products. EXCEPT AS SET FORTH IN QUEST'S TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST 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 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 HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest 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 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 World Headquarters
LEGAL Dept
5 Polaris Way
Aliso Viejo, CA 92656
www.quest.com
email: legal@quest.com

Refer to our Web site (*www.quest.com*) for regional and international office information.

Patents

Protected by U.S. Patents 8,046,550; 8,060,476; and 8,135,930.Additional patents pending.

Trademarks

Quest, Quest Software, the Quest Software logo, AccessManager, ActiveRoles, Aelita, Akonix, Benchmark Factory, Big Brother, BridgeAccess, BridgeAutoEscalate, BridgeSearch, BridgeTrak, BusinessInsight, ChangeAuditor, CI Discovery, Defender, DeployDirector, Desktop Authority, Directory Analyzer, Directory Troubleshooter, DS Analyzer, DS Expert, Foglight, GPOADmin, Help Desk Authority, Imceda, IntelliProfile, InTrust, Invirtus, iToken, JClass, JProbe, LeccoTech, LiteSpeed, LiveReorg, LogADmin, MessageStats, Monosphere, NBSpool, NetBase, NetControl, Npulse, NetPro, PassGo, PerformaSure, Point, Click, Done!, Quest vToolkit, Quest vWorkSpace, ReportADmin, RestoreADmin, ScriptLogic, SelfServiceADmin, SharePlex, Sitraka, SmartAlarm, Spotlight, SQL Navigator, SQL Watch, SQLab, Stat, StealthCollect, Storage Horizon, Tag and Follow, Toad, T.O.A.D., Toad World, vAutomator, vConverter, vEcoShell, VESI, vFoglight, vPackager, vRanger, vSpotlight, vStream, vToad, Vintela, Virtual DBA, VizionCore, Vizioncore vAutomation Suite, Vizioncore vEssentials, Vizioncore vWorkflow, WebDefender, Webthority, Xaffire, and XRT are trademarks of Quest Software, Inc. and its subsidiaries. For a complete list of Quest Software trademarks, see *www.quest.com/legal/trademarks.aspx*. All other trademarks are property of their respective owners.

Installation and Setup Guide
Version 5.4.1 - Private Release
Mary 2012

Table of Contents

Introduction to this Guide **6**
About vRanger 7
vRanger Documentation Suite 7
About Quest Software, Inc. 7
Contacting Quest Software 8
Contacting Quest Support 8

Before You Install **9**
Before Installing vRanger 10
vRanger Licensing Levels 10
vRanger Installation Options 11
Installing the vRanger Server 11
Installing vRanger in a Virtual Machine 12
Installing vRanger on a Physical Server 15
Installing The vRanger Database 17
Database options 17
Installing the Databases 17
Installing the vRanger Virtual Appliance 18
Creating a vRanger Repository 19
Repository Storage Devices 20
Bandwidth to Repositories 20
Repository Size 20
Configuring vCenter Permissions 21
vSphere 5 21
vSphere 4.x 23

Upgrading vRanger **26**
Before Upgrading vRanger 27
Licensing Changes in vRanger 27
vRanger Editions 27
Upgrading a Previous vRanger Installation 27
Upgrading the vRanger Virtual Appliance 31
Upgrading a Previous vReplicator Installation 32
Upgrading from vRanger Pro 3.x 33

Installing vRanger 34
vRanger Installation Overview 35
Installing vRanger 35
Install vRanger on a New Instance of SQL Express 2005 35
Install vRanger on an Existing SQL 2005/2008 Server 41
Install vRanger Catalog Manager 47

Configuring vRanger 51
Configuration Overview 52
Configuration through the Startup Wizard 52
Select a License 53
VirtualCenter and Host Information 54
Host Licensing Information 57
Virtual Appliance Information 58
Add Repositories 58
Set up Mail Server Information/Add Email Addresses 60
Configuration without Using the Startup Wizard 62
Add a VirtualCenter 62
Add an ESX Server 62
Add a Repository 63
Configure an SMTP Server 63
Configure Virtual Appliances 65
Import License File 66
Manage Host Licensing 67
Manage Job Configuration Settings 68
Cataloging Options 69
Configuring Linux File Level Restoration 70
Configuration Options 71
Catalog Filtering 73
Supplemental Instructions - Additional Repository Types 73
Adding an NFS Repository 74
Adding an FTP Repository 75
Adding an SFTP Repository 76
Adding an NVSD Repository 77
Adding an EMC Data Domain Boost (DDB) Repository 77

Configuring the Virtual Appliance 81
The vRanger Virtual Appliance 82
Virtual Appliance Overview 82
The Virtual Appliance Scratch Disk 82
Deploying the Virtual Appliance 85
Deploying Multiple Virtual Appliances 85

Configuring the Virtual Appliance 86
Deploying Multiple VAs From a Template - VI Client 90
Deploying Multiple VAs From a Template - PowerCLI 91
Disabling DRS for the vRanger Appliance 94
Adding the Virtual Appliance to vRanger 94
Changing Virtual Appliance Configuration 96
Increasing The VA Scratch Disk Size 98
Disabling DRS for the vRanger Appliance 99

Appendix: Using the VI Editor 100
VI Editor Overview 100
Starting VI 100
Changing Modes 100
Editing Commands 101
Moving the Cursor 101
Inserting Text 102
Deleting Text 102
Saving Your Changes 102

Index 104

Introduction to this Guide

This chapter provides information about what is contained in *Installation and Setup Guide*. It also provides information about the vRanger documentation suite and Quest.

This chapter contains the following sections:

About vRanger 7
vRanger Documentation Suite 7
About Quest Software, Inc. 7

About vRanger

vRanger is the market-leading backup, recovery and backup management solution for virtual environments. Featuring a new platform technology, vRanger reduces the backup window, provides smarter backup options, and offers more scalability features while using fewer resources.

vRanger Capabilities:

- Performs incremental, differential or full image backups of virtual machines.
- Quickly restores the entire virtual machine or just specific files.
- Manages disaster recovery strategies and protects critical data in virtual environments.
- Offers the ability to replicate virtual machines to more than one destination, thus allowing users to accomplish multiple High Availability and Disaster Recovery objectives based on their specific needs.

vRanger Documentation Suite

The documentation suite is made up of the core set plus documents intended for advanced configurations. Documentation is provided in a combination of online help and PDF.

- **Online Help:** You can access online help through Help in the Menu bar on the four main screens of the interface.
- **PDF:** The *Getting Started Guide*, *What's New Guide*, *System Requirements Guide, Installation and Setup Guide,* and *User Guide*, are provided as PDF files. The PDF guides are included in the zip file downloaded from Quest. Adobe® Reader® is required.

About Quest Software, Inc.

Quest Software simplifies and reduces the cost of managing IT for more than 100,000 customers worldwide. Our innovative solutions make solving the toughest IT management problems easier, enabling customers to save time and money across physical, virtual and cloud environments. For more information about Quest go to *www.quest.com.*

Contacting Quest Software

Email	*info@quest.com*
Mail	Quest Software, Inc. World Headquarters 5 Polaris Way Aliso Viejo, CA 92656 USA
Web site	*www.quest.com*

Refer to our web site for regional and international office information.

Contacting Quest Support

Quest Support is available to customers who have a trial version of a Quest product or who have purchased a Quest product and have a valid maintenance contract. Quest Support provides unlimited 24x7 access to our support portal. Visit our support portal at: *www.quest.com/support.*

From our support portal, you can do the following:

- Retrieve thousands of solutions from our Knowledge Base
- Download the latest releases and service packs
- Create, update and review Support cases

View the Global Support Guide for a detailed explanation of support programs, online services, contact information, policies and procedures. The guide is available at: *www.quest.com/support.*

Before You Install

This chapter provides information on vRanger installation options, as well as required permissions.

This chapter contains the following sections:

Before Installing vRanger 10
vRanger Installation Options 11
Installing the vRanger Server 11
Installing The vRanger Database 17
Installing the vRanger Virtual Appliance 18
Creating a vRanger Repository 19
Configuring vCenter Permissions 21

Before Installing vRanger

Before installing vRanger, you will need to decide the best architectural option for your environment. In addition, there are some preliminary configurations that should be made in order to get the most out of vRanger. The sections in this chapter provide some basic information that you will need in order to decide where and how to deploy vRanger. For more detailed information, please consult the *vRanger Deployment Guide*.

Note If you are upgrading a previous vRanger version, please see Upgrading vRanger.

vRanger Licensing Levels

There are three levels of vRanger Licensing, each with different available features:

- vRanger Standard
- vRanger Pro
- vReplicator

	vRanger Standard	vRanger Pro	vReplicator
Backup	X	X	
Restore	X	X	
VA-Based Backup/Restore		X	
Replication		X	X
CBT	X	X	X
ABM	X	X	X
LAN Free (SAN)*		X	
LAN Free (HotAdd)	X	X	
Catalog		X	
Windows FLR	X	X	
Linux FLR		X	

*Note that in the vRanger UI, “LAN Free” is used to encompass both traditional LAN-Free (with vRanger on a physical proxy connected to your Fibre SAN) and LAN-Free via HotAdd (with vRanger in a VM). Traditional LAN-Free operations are restricted to vRanger Pro licenses only. vRanger Standard can still perform LAN-Free backups and restores via VMware’s HotAdd API.

A license for vRanger controls the number of source CPUs that you can configure for backup. For licensing purposes, a dual-core processor is counted as a single CPU. Therefore, one ESX Server with two dual-core processors would use two CPUs of a license.

Trial License

You may evaluate vRanger using the trial license included with the product. The trial provides license is limited to 30 CPUs, and will expire 90 days after installation. The trial license provides vRanger Pro functionality. In order to continue using vRanger past the trial period, you must import the new license key provided to you by Quest Software. If you have not received your license key, please go to *https://support.quest.com/LicenseKey.aspx.*

Single License Limitation

vRanger is available in three versions: vRanger SE, vRanger Pro, and vReplicator. Please note that only one version of vRanger can be installed on a machine at any one time. For example, you cannot install vRanger SE and vReplicator on the same machine.

vRanger Installation Options

A complete vRanger installation includes four components: the vRanger server; the vRanger database; the vRanger virtual appliances; and at least one repository. The sections below provide information on the options available for each component.

- Installing the vRanger Server
- Installing The vRanger Database
- Installing the vRanger Virtual Appliance
- Creating a vRanger Repository

Installing the vRanger Server

vRanger can be installed either on a physical server or in a virtual machine. As long as the vRanger machine meets the specifications detailed in the *vRanger System Requirements Guide*, application performance should be similar regardless of which option is chosen.

- **Virtual Machine** - When installing vRanger in a virtual machine, you eliminate the need for dedicated hardware while maintaining high performance. Due to the lower cost and increased flexibility, this is the recommended approach. For information on installing in a virtual machine, see Installing vRanger in a Virtual Machine
- **Physical Server** - The primary benefit of installing vRanger on a physical server is that the resource consumption of backup activity is off-loaded from the virtual environment to the physical proxy. Of course, this configuration requires a dedicated server, and LAN-free backups require a more complex configuration. For more information on installing on a physical server, see Installing vRanger on a Physical Server.

Regardless of which approach you chose, vRanger can leverage the vRanger virtual appliances to perform backup, restore, and replication tasks. This provides greater scalability while distributing the resource consumption of data protection activities across multiple hosts. See Installing the vRanger Virtual Appliance for more information.

Installing vRanger in a Virtual Machine

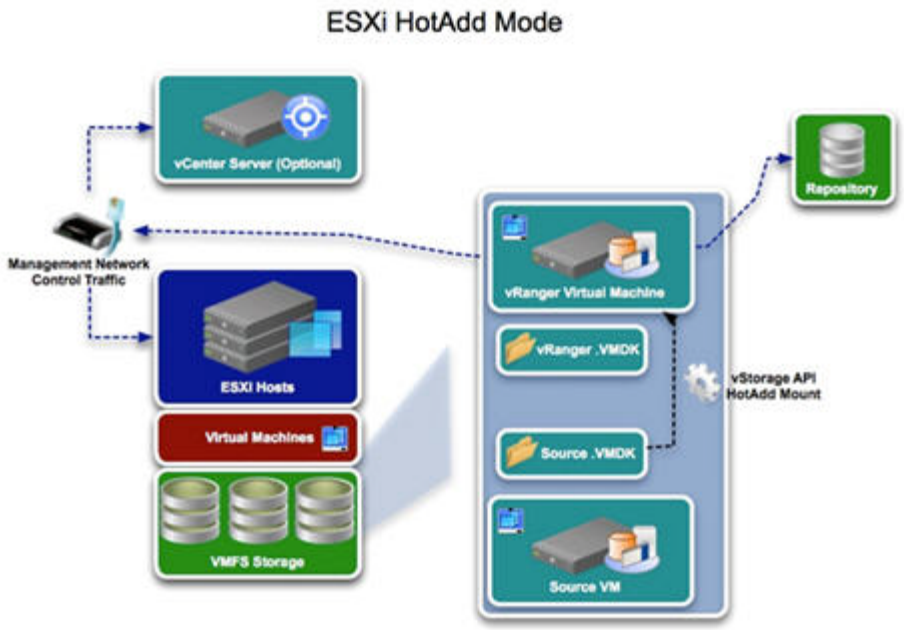
When vRanger is installed in a virtual machine, you can perform backups and restores either over the network or in a LAN-Free mode which uses your fibre infrastructure. The sections below provide a summary of each method. Note that replication tasks are always performed over the network.

Note You have the option of deploying the vRanger virtual appliances for backup and restore activity. See Installing the vRanger Virtual Appliance for more information.

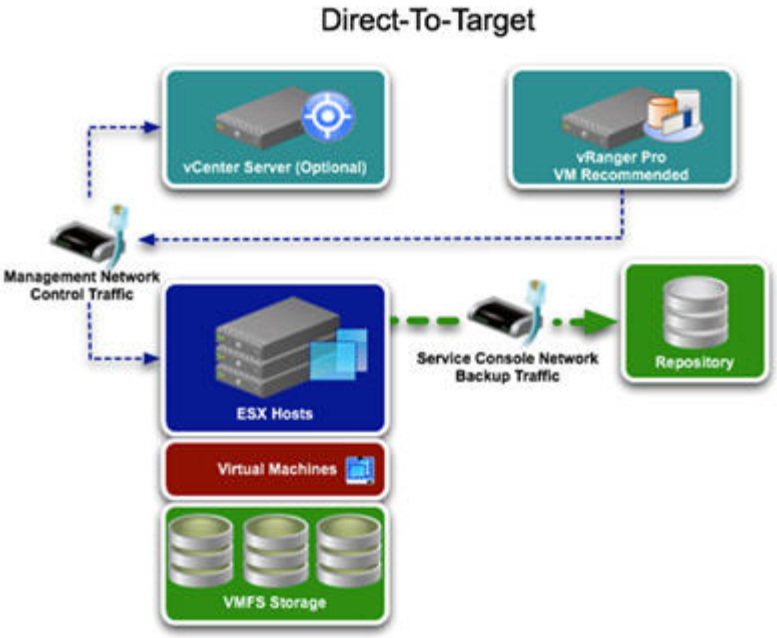
Network Backups

Network backups and restores are the default option in vRanger, as they are supported in all configurations and require no additional set-up to work. With vRanger installed in a VM, network backups can be processed either of two ways, depending on the source host configuration.

- When the source VM is on an ESXi host, there is no service console to process the backup activity. In this configuration the VMDK(s) of the source VM are attached (via HotAdd) to the vRanger machine, yielding direct access to source data which is then sent over the network to the repository.



- For network-based backups when using ESX, the backup data flows “direct to target” from the ESX Host to the target repository. This means that the vRanger server does not process any of the backup traffic.

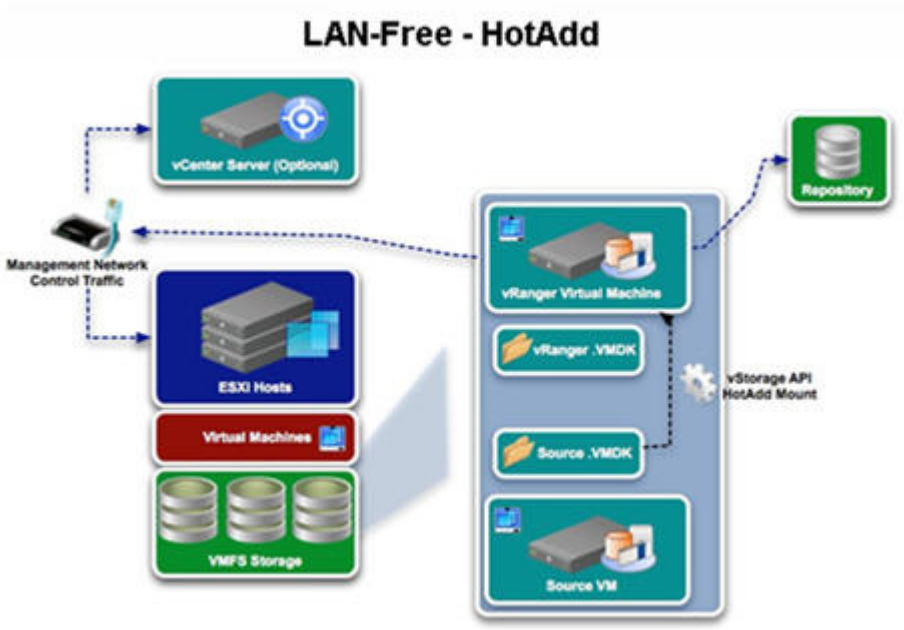


Note Generally speaking, network backups and restores will be slower than LAN-Free. If your environment supports LAN-Free backups, use that option whenever possible. See LAN-Free Backups for more information.

LAN-Free Backups

When vRanger is installed in a virtual machine, LAN-Free backups are made possible by VMware’s HotAdd disk transport. This configuration that requires vRanger to be installed on a virtual machine residing on an ESX(i) host connected to your fibre or iSCSI network.

During backups with HotAdd, the source VM’s disks are mounted to the vRanger virtual machine, allowing vRanger direct access to the VM’s data through VMware’s I/O stack. Backup processing occurs on the vRanger VM, with the data then being send to the configured repository.



Requirements for a LAN Free - HotAdd Configuration

In order to use vRanger with HotAdd, vRanger must be installed in a VM, and that VM must be able to access the target VM's datastore(s). In addition, all hosts that the vRanger VM could be vMotioned to must be able to see the storage for all VMs that vRanger will be configured to back up.

Configuring vRanger for HotAdd

When using HotAdd, make sure to disable automount on the vRanger machine. This will prevent Windows on the vRanger VM from assigning a drive letter to the target VMDK. To disable automount:

- From the start menu, select "run" and enter `diskpart`.
- Run the `automount disable` command to disable automatic drive letter assignment.
- Run the `automount scrub` command to clean any registry entries pertaining to previously mounted volumes.

Considerations for Installing vRanger in a Virtual Machine

Please read and the notes below regarding limitations and considerations about installing vRanger in a VM:

- When installing vRanger in a VM, it is not supported to perform a machine-based backup of the vRanger VM. In other words, the vRanger VM cannot back itself up. You may, however, perform a VA-based backup of the vRanger VM.
- When creating the virtual machine for vRanger, it is recommended to create a fresh VM rather than cloning an existing VM or template.

In recent versions of Windows, volumes are recognized by a serial number assigned by Windows. When VMs are cloned, the serial number for each VM volume is cloned as well. During normal operations, this is not an issue, but when vRanger is cloned from the same source or template as a VM being backed up, the vRanger volume will have the same serial number as the source volume.

For backup operations using HotAdd, source disk volumes are mounted to the vRanger VM. If the source VM volumes have the same disk serial number as the vRanger volume (which will be the case with cloned VMs), the source VM's serial number will be changed by Windows when mounted to the vRanger VM. When restoring from these backups, the boot manger will not have the expected serial number, causing the restored VM not to boot until the boot information is corrected.

Installing vRanger on a Physical Server

Installing vRanger on a physical server provides a method to off-load backup resource consumption from the ESX/ESXi host and network. While you can perform Network Backups in this configuration, LAN-Free Backups are the primary driver for using vRanger in a physical server.

Note With vRanger installed on a physical server, you can still take advantage of the vRanger virtual appliances for backup and restore activity. See Installing the vRanger Virtual Appliance for more information.

LAN-Free Backups

The LAN Free configuration is identical whether ESX or ESXi is used, providing the best mix of performance and compatibility for protecting your data, especially if your environment has a mix of VMware hypervisors.

In order to perform LAN Free backups, vRanger must be installed on a physical system attached to your SAN environment. This is a high performance configuration that requires vRanger to be connected to your fibre or iSCSI network. In addition, the VMFS volumes containing the VMs to be protected must also be properly zoned/mapped to the vRanger proxy server.

Configuring vRanger for LAN-Free

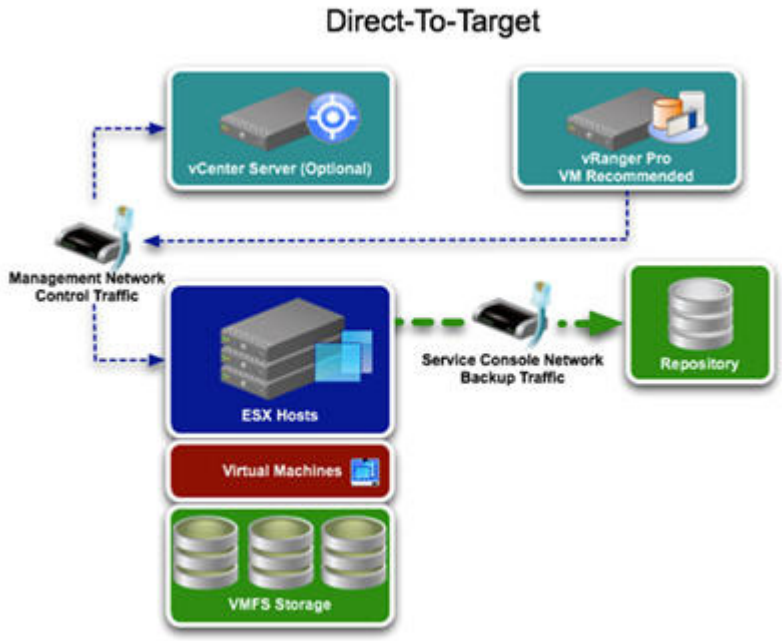
With vRanger will be installed on a physical proxy server, the following configurations must be made:

- Disable automount on the vRanger machine:
  - From the start menu, select "run" and enter `diskpart`.
  - Run the `automount disable` command to disable automatic drive letter assignment.
- Run the **`automount scrub`** command to clean any registry entries pertaining to previously mounted volumes.
- On your storage device, zone your LUNs so that the vRanger HBA (or iSCSI initiator) can see and read them.

- Only one proxy should see a set of VMFS LUNs at one time. For backups only, The proxy server should have only **read-only** access to the LUNs. In order to perform LAN-Free restores, please ensure that the vRanger server has Read + Write access to any zoned VMFS LUNs to which you wish to restore.

Network Backups

Network Mode within vRanger can be configured one of two ways, depending on whether you are using ESX or ESXi as your hypervisor. For network-based backups when using ESX, the backup data flows “direct to target” from the ESX Host to the target repository. This means that the vRanger server does not process any of the backup traffic. Network-based, Direct-To-Target backups use the ESX Service Console and the Service Console NIC to process and send data to a repository.



- When the source VM is on an ESXi host, there is no service console to process the backup activity. In this configuration the data is transferred from the VM to the vRanger server using VMware’s VDDK transport. The data is then sent to the repository over the network.

Generally, this configuration will yield the slowest performance, and should be avoided if possible. A better option would be to deploy a virtual appliance to any ESXi servers, and use that virtual appliance for backup and restore tasks.

Installing with Other Applications

Customers often want to install vRanger on the same server as another application. Due to the wide variety of factors that may impact performance, it is impossible to make blanket recommendations. Some key concerns to keep in mind:

- Many customers, in an effort to maximize their hardware investment, want to install vRanger on the same server as VMware vCenter. This practice is not recommended.
- During testing, many customers install vRanger with other Quest products. In this case it is not recommended to install vRanger on the same machine as vFoglight.
- Only one version of vRanger may be installed on a machine at one time. For example, you may not install vRanger SE and vReplicator on the same machine.

Installing The vRanger Database

vRanger utilizes a SQL database to store application and task configuration data. The database can be either the embedded SQL Express instance (the default option)or a SQL database running on your own SQL Server or SQL Express instance.

Database options

The database deployment occurs during the initial installation of vRanger. The default option installs a SQL Express database on the vRanger server. You may, if desired, install vRanger using a separate SQL Server instance. If you are going to use your own SQL instance and wish to use the vRanger cataloging feature, the SQL instance must be installed on the vRanger server. For more information, see Installing the Databases

Default

The Installation Wizard will default with a selection to install vRanger with the embedded SQL Express 2005 database. The SQL Express database can only be installed on the vRanger server.

Note While the embedded SQL Express database is free and simple to install, there is a size limit of 4GB per database.

External SQL Instance

The Installation Wizard will guide you through configuring vRanger with an external SQL database. There is also an option in the Install Wizard to configure the database connection manually, but the guided approach is recommended.

Important See the *vRanger System Requirements Guide* for a list of supported SQL database versions.

Installing the Databases

When installing vRanger, consider the database selection carefully as migrating from a SQL Express installation to an external SQL database carries a risk of corrupting application data.

The cataloging function of vRanger requires that the application and catalog database be installed on the vRanger server. There are two options to accomplish this:

- Use the default SQL Express 2005 installation, which will install vRanger, the vRanger database, and the Catalog database on the same machine. While this is the most straight forward option, SQL Express 2005 databases are limited in size to 4 GB.
- If you don't want to use the default SQL Express database, you can also install a supported Microsoft SQL Server version on the vRanger machine, and install the vRanger databases on that instance. While there is no hard-coded limit to database size, this is a more complicated installation.

If you will ***not*** be using cataloging, in order to provide the most flexibility, it is recommended to install vRanger using an external SQL database server. This will allow you to relocate the vRanger installation simply by installing the application in another location, and pointing the Install Wizard to the existing database.

Sizing the Catalog Database

The vRanger catalog process collects and records metadata and path information for files updated since the last backup and catalog entry. Depending on the number of VMs protected, and the number of files in each VM, the catalog database may grow quite rapidly.

Actual database growth will vary depending on the Guest OS and the number of files changed between backups, but the information below can be used as an approximate guide.

- With default filtering, the full catalog of a generic Windows 2008 VM is approximately 500 files, or approximately 0.2 MB.

  Note Many Windows files are not cataloged due to filtering (see Catalog Filtering). An amount of data equal to a standard Windows 2008 installation will result in a larger catalog footprint.

- Incremental and differential backups will only catalog changed files, making the catalog record for these backups considerably smaller. Using incremental and/or differential backups will allow you to store catalog data for many more savepoints than if you used only full backups.

Installing the vRanger Virtual Appliance

Starting with vRanger 5.4, the virtual appliance can now process backup and restore tasks in addition to replication tasks. This allows you to scale backup, restore, and replication activity across multiple hosts or clusters, while maintaining central scheduling and reporting control from a single vRanger server.

While the deployment and configuration of the virtual appliance are covered in more detail in Configuring the Virtual Appliance, the information below should help you understand the usage of the virtual appliance.

Virtual Appliance Usage

The vRanger virtual appliance can be used to perform the following operations. For each of these operations, the processing activity occurs on the VA.

- Backup - network and LAN-Free (HotAdd)
- Restore - network and LAN-Free (HotAdd)

- File-level restore
- Linux file-level restore
- Replication

Deployment Locations

The locations to which the vRanger virtual appliance(s) should be deployed depend on the specifics of the virtual environment in question.Some general guidelines for VA deployment are:

- Starting with vRanger 5.4, you may share a single virtual appliance among the hosts within a cluster.
  - You may install a virtual appliance to some or all hosts within a cluster as well. If a VA is not detected on the host, vRanger will check if the host is part of a cluster, and then if that cluster has a VA available.
- You must have a virtual appliance deployed on any ESXi host or cluster that will be used for replication. This is true regardless of whether the host or cluster will be used as the source or target of the replication task.
- When using the virtual appliance for replication, both the source and target host or cluster must use a virtual appliance.

Creating a vRanger Repository

Designed for ease-of-use in recovery operations, repositories eliminate the need for countless backup locations and endless configurations. With vRanger, you can configure a repository once, and use it forever.

Repositories can be one of the formats below:

- CIFS
- NFS (version 3)
- FTP
- SFTP
- NetVault SmartDisk
- EMC Data Domain Boost

A repository is essentially a directory on a supported file system that vRanger uses to store savepoints (backup archives). When viewed from outside vRanger (through Windows Explorer, for example), a repository consists of a configuration file (GlobalManifest.metadata) and root level directories for each protected object.

Any time you add a repository in vRanger a GlobalManifest.Metadata XML file is created in the selected folder. It is the presence of that manifest file that tells vRanger that a repository exists in that folder.

Repository location, along with the configuration of jobs to those repositories, plays a significant role in the performance of vRanger. Use the recommendations below to aid on planning your repository configuration.

Repository Storage Devices

Slow disk performance has been shown to negatively impact the backup performance of vRanger. When configuring repositories, special attention should be paid to the type of storage devices used.

The use of SAS (Serial Attached SCSI) disk drives are recommended. SAS drives typically offer a 30% performance improvement over SATA drives.

The use of external USB drives or low quality NAS devices is not recommended. If these types of storage are used, the vRanger configuration settings must be adjusted to accommodate the slow devices. Recommended configuration settings for slower repositories are shown below. These configurations can be made in the vRanger Configuration Options dialogue, available on the **Tools>Options** menu.

- Maximum number of tasks running off a LUN = **3**
- Maximum number of tasks running off a host = **1**
- Maximum number of tasks running per repository = **2**

If no errors are received with these settings, increment the tasks per repository value by 1 to find the best fit for your environment.

Bandwidth to Repositories

While performance varies based on environmental factors, data throughput during a single backup task can reach up to 100 MB/s. If we assume a standard case of a repository connected via a Gigabit network, then as little as ten concurrent jobs can saturate the link to that repository.

Although there is no ability to throttle data transmissions from an ESX(i) host, vRanger can limit the number of simultaneous backup tasks on a per-repository level.

Note This configuration is a global configuration, meaning that it applies to all repositories.

Repository Size

There is no limit to the number of savepoints that can be stored in a vRanger repository. There are, however, environmental limits on the size of a single directory. The available options, and their limits, are described below.

Note The volume limitations described in this section are limitations within the Microsoft Windows environment.

- **Default Configuration**- A standard volume, with an MBR partition on a basic disk, has a limit of 2 TB. This is the default configuration for Windows Server 2003. In this configuration, the vRanger repository cannot exceed 2 TB.

- **Dynamic Disks** - Dynamic disks contain dynamic volumes, including simple volumes, spanned volumes, striped volumes, mirrored volumes, and RAID-5 volumes. A repository located on dynamic disk volumes can be as large as 64 TB. For more information, see the Microsoft TechNet article: *http://technet.microsoft.com/en-us/library/cc773268(WS.10).aspx*
- **GPT Volumes** - GPT provides a more flexible mechanism for partitioning disks than the older Master Boot Record (MBR) partitioning scheme that has been common to PCs. GPT partitions are supported on Windows Server 2003, SP1 and later, and can reach up to 256 TB. For more information, see *http://www.microsoft.com/whdc/device/storage/GPT_FAQ.mspx*

Configuring vCenter Permissions

vRanger requires a vCenter account to function properly. To comply with security best practices, Quest recommends creating a vCenter user account with the minimum required permissions for vRanger to use.

The procedures differ slightly depending on which version of vCenter you are using. For vSphere 5.x, see the section below. For vCenter 4.0, please see vSphere 4.x.

vSphere 5

The permissions required for backup and restore operations in a vSphere 5 environment differ slightly from the permissions required for previous versions of vCenter. If you have migrated to vSphere 5 after creating a vRanger user account, please update the permissions accordingly to avoid job interruption.

To create a vRanger user on vSphere 5:

1. Navigate to Administration > Roles.
2. Select **Add Role**.
3. Enter a name for the Role, such as “vRanger Non-Admin”.
4. In the Privileges section, set the permissions according the table below:

Section	Privileges
Datastore	• Allocate space • Browse Datastore • Low level file operations • Remove file

Section	Privileges
Global	• Cancel task • Disable methods • Enable methods • Licenses • Log event

Host	• Local Operations
	  • Create virtual machine
	  • Reconfigure virtual machine

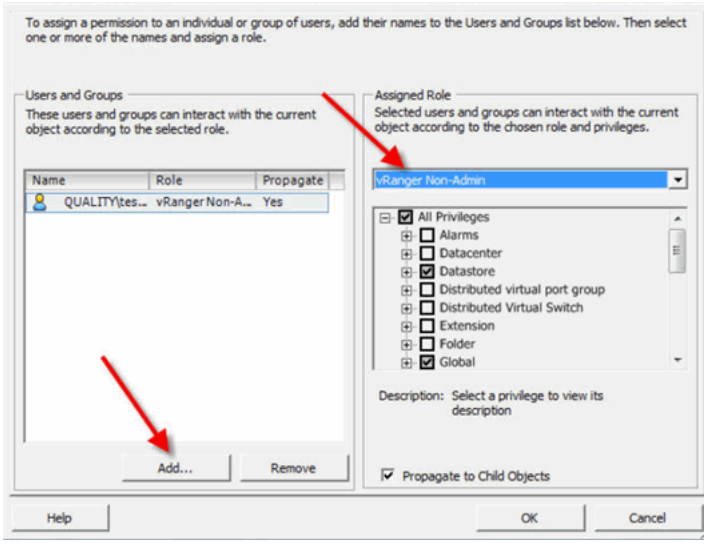
Network	• Assign network
Resource	• Assign vApp to resource pool • Assign virtual machine to resource pool
Tasks	• Create task • Update task

Virtual Machine	• Configuration
	  • Select all privileges in this section
	• Interaction
	  • Configure CD media
	  • Configure floppy media
	  • Device connection
	  • Power Off
	  • Power On
	• Inventory
	  • Create new
	  • Register
	  • Remove
	  • Unregister
	• State
	  • Create snapshot
	  • Remote snapshot
	  • Revert to snapshot

5 Navigate to the Inventory view

6 Right-click the desired level to grant user permission, such as the main vCenter level. Click **Add Permission**.

7 Add and locate the desired user account, and select the recently created User Role. Click **Add**.



8 Click **OK**.

Note When you add the vCenter to vRanger's inventory, use this account for authentication.

vSphere 4.x

To create a vRanger user on vSphere 4:

1 Navigate to Administration > Roles.

2 Select **Add Role**.

3 Enter a name for the Role, such as "vRanger Non-Admin".

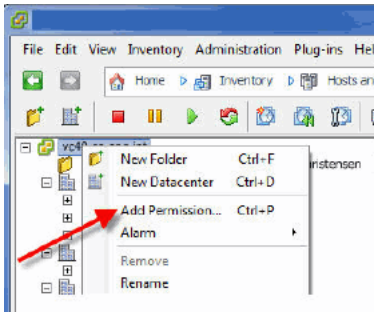
4 In the Privileges section, set the permissions according the table below:

Section	Privileges
Datastore	• Allocate Space • Browse Datastore
Global	• Licenses • Log Event
Host > Local Operations	• Create Virtual Machine • Reconfigure Virtual Machine
Network	• Assign Network
Resource	• Assign virtual machine to resource pool

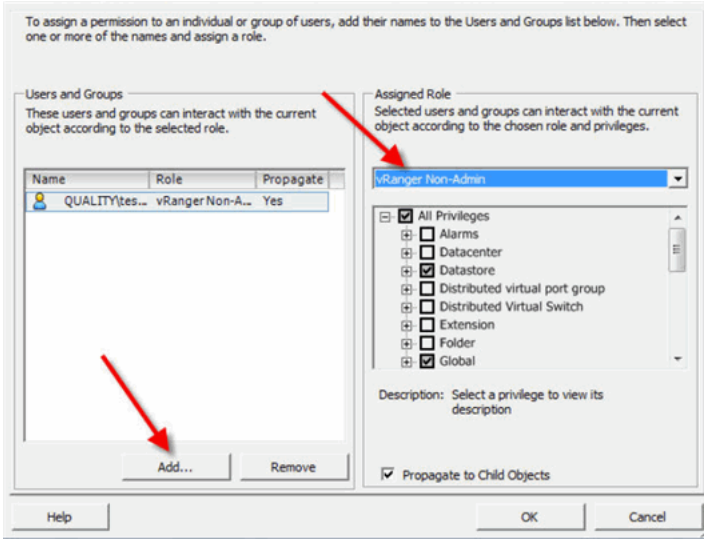
Virtual Machine > Configuration	• Select all options in this section.
Virtual Machine > Interaction	• Configure CD Media • Configure floppy media • Device Connection • Power Off • Power On
Virtual Machine > Inventory	• Create new
Virtual Machine > Provisioning	• Allow disk access • Allow read-only disk access • Allow virtual machine download • Allow virtual machine files upload • Mark as template • Mark as virtual machine
Virtual Machine > State	• Create Snapshot • Remove Snapshot

5 Navigate to the Inventory view

6 Right-click the desired level to grant user permission, such as the main VC level.Click **Add Permission**.



7 Add and locate the desired user account, and select the recently created User Role and click Add.



8 Click OK.

Note When you add the vCenter to vRanger's inventory, use this account for authentication.

Upgrading vRanger

This chapter guides you through the process of upgrading a previous vRanger installation.

This chapter contains the following sections:

Before Upgrading vRanger 27
Upgrading a Previous vRanger Installation 27
Upgrading a Previous vReplicator Installation 32
Upgrading from vRanger Pro 3.x 33

Before Upgrading vRanger

Before you upgrade an existing vRanger installation, please refer to the sections below for important information.

Licensing Changes in vRanger

vRanger 5.2 and above uses a new license key that differs from previous vRanger versions. The license key file for versions 5.2 and above ends in *.asc* where the prior license key files ended in *.lic* and will not work with this version.

If you are upgrading from vRanger 5.1 or earlier, you will need a new license key. If you have not received your license key, please go to *https://support.quest.com/LicenseKey.aspx.*

vRanger Editions

With replication now integrated into vRanger, and vRanger being offered in multiple versions, there are several upgrade options available.

- **Current vRanger customers** - see Upgrading a Previous vRanger Installation.
- **Current vReplicator customers** - see Upgrading a Previous vReplicator Installation.
- **Customers of both vRanger and vReplicator** - the upgrade procedures differ depending on whether you want to manage replication from the D/R site, or combine backup and replication management on the production site.
  - **D/R site** - if you want to manage replication from the D/R site (to ease failover), then follow both of the procedures referenced above, upgrading the vRanger installation on the production side and the vReplicator installation on the D/R site. You may use a combined license file for both installations, provided that the combined CPU count for each protection type (backup and replication) for both sites does not exceed the total licensed number of CPUs.
  - **Production site** - when both backup and replication will be managed from the production site, start with Upgrading a Previous vRanger Installation, then skip to Step 4 of the Upgrading a Previous vReplicator Installation procedures.

If you purchase vRanger -Standard Edition, you can purchase an upgrade to vRanger Pro. Similarly, you can also purchase an upgrade from vReplicator 5.0 to vRanger Pro 5.4.

Upgrading a Previous vRanger Installation

You may upgrade a previous vRanger installation to the latest version by running the vRanger Upgrade installer. If you are upgrading from a vRanger 3.x installation, see the section:Upgrading from vRanger Pro 3.x.

Note Do not use the full installer to upgrade an existing installation.

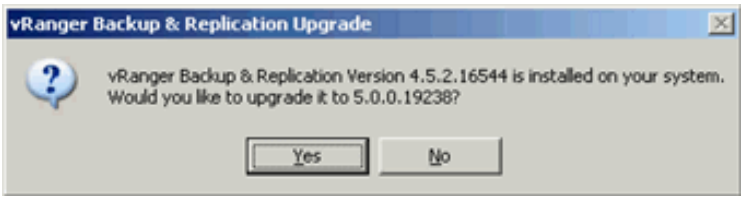
The vRanger Upgrade installer supports upgrading from vRanger Pro versions 4.0 or later.

Upgrade from Beta versions is not supported, nor is operating a GA version in parallel with a Beta version. The beta version must be uninstalled before upgrading a previous GA version or performing a full installation.

Note It is recommended that you backup your vRanger Pro database before upgrading the application.

To upgrade a vRanger Pro installation:

1 Double-click the vRanger Upgrade executable. A confirmation prompt displays:



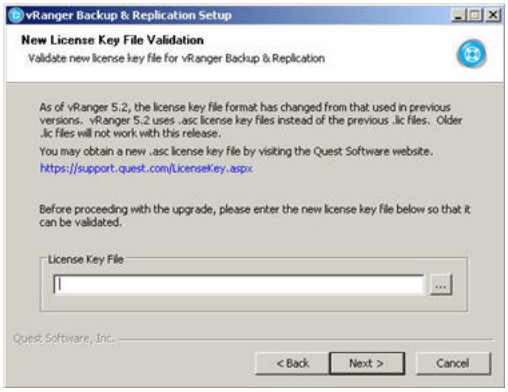
2 Click **Yes** to upgrade. A backup reminder prompt appears. Click **Yes**.

3 The Welcome Screen appears. Click **Next**.

4 The License Agreement dialog appears. Click **I Agree**.

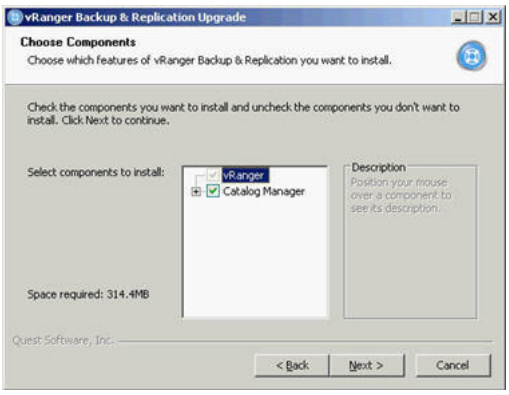
5 The License Key Validation dialog appears.

Note This screen will only show if you are upgrading from vRanger 4.x, 5.0, or 5.1 to vRanger 5.4. If upgrading from version 5.2 to 5.4, this dialog will not appear.



This screen prevents you from continuing with the upgrade process if you do not have a valid vRanger 5.4 license. Import your vRanger 5.4 license, and click **Next**.

6 The Choose Components dialog appears.



vRanger includes a cataloging feature that requires an additional database and other components. The Catalog Manager installation is enabled by default. Click **Next**.

or

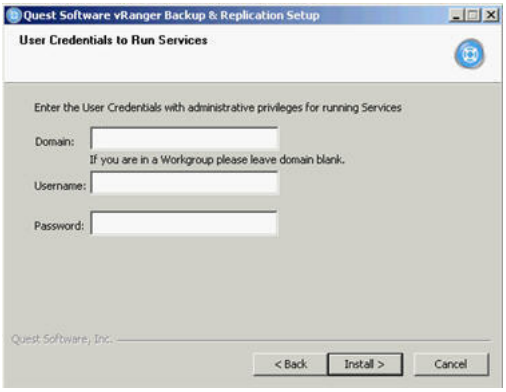
To disable the installation of the Catalog Manager, clear the checkbox. Click **Next**. You may install the components later by re-running the vRanger Upgrade installer.

7 If you are upgrading from vRanger 4.x, a prompt displays. Click **Ok**.

The prompt states that some files will be relocated as part of the upgrade. To view the details, see *C:\Program Files\Quest Software\vRanger\Upgradelog.log*

Note On x64 systems, the path will be *C:\Program Files (x86)\Quest Software\vRanger\Upgradelog.log*

8 The User Credentials dialog displays. The user account needed for this step must have administrator privileges on the local machine.



a In the **Domain** field, enter the domain in which the user account is located.

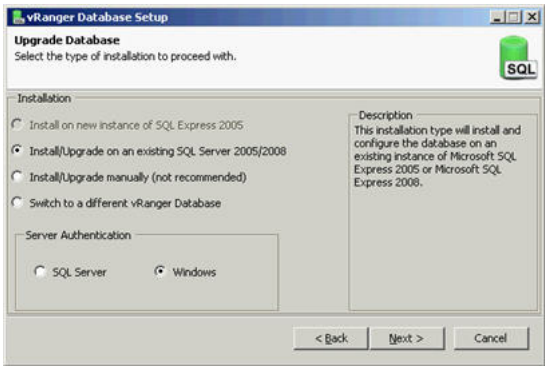
b In the **Username** field, enter the username for the account.

c In the **Password** field, enter the password for the account.

d Click **Next.**

9 The installation process continues. The Database Setup Wizard appears. Click **Next**.

10 The Upgrade Database dialog appears.



The installer will find the existing vRanger database, and default to **Install/Upgrade on an existing SQL Server 2005/2008**.

Select the Server Authentication method and click **Next**.

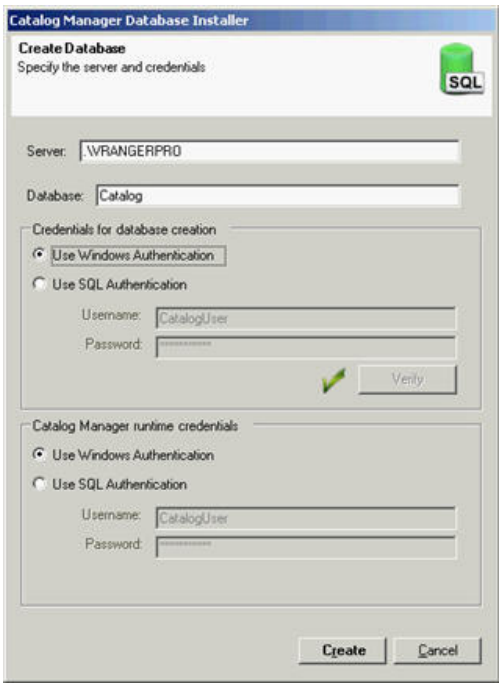
11 The Installation Database Credentials dialog appears. Click **Verify**.

Click **Ok** to close the confirmation dialog. Click **Next**.

12 A confirmation dialog appears. Click **Yes**.

13 Click the **Automatic Setup** button. The database upgrade will complete.

14 The Catalog Manager Database Installer dialog appears.



Select the desired authentication method. You mach use the method chosen in Step 11, or select a new method. Click **Verify**. Click **Create**.

Note If the Instance name on the machine is different, you should change the sever name to the instance name on the local machine. “vRangerPro” is the default created instance when using SQL Express 2005.

15 The installation completes.

Upgrading the vRanger Virtual Appliance

vRanger 5.4 uses a new version of the virtual appliance (version 1.5.0) to support vRanger's automated deployment feature.

Maintaining Your Scratch Disk

The second disk (scratch disk) on your virtual appliance(s) contains a hash file for each replicated virtual machine. vRanger uses this file to identify changed data blocks during replication. When upgrading the virtual appliance, consider migrating the scratch disk from your legacy VA to the upgraded version. This will ensure that your hash files are maintained. See Upgrading Your Virtual Appliance for more information.

Important If you do not migrate the scratch disk to your updated virtual appliances, vRanger will need to re-create each hash file which requires a full scan of the replicated virtual machine. While only the changed data will be sent, the re-scan of the VM may take up to 1 minute per GB of hard disk space.

For more information about the scratch disk, see The Virtual Appliance Scratch Disk.

Checking the Version of Your Virtual Appliance

To check the version of your virtual appliance:

1 Login to the virtual appliance.

2 At the prompt, enter the command

```
cat /etc/vzvaversion
```

Upgrading Your Virtual Appliance

There is no method to perform an in-place upgrade of the virtual appliance. The previous version must be replaced with the new version. To update your virtual appliance(s), follow the steps described below:

- Deploy the new virtual appliance version according to the instructions documented in Deploying the Virtual Appliance.

  Note If you want to maintain the scratch disk from your existing virtual appliances, deploy a virtual appliance without a scratch disk.

3 Migrate your scratch disk as described in Migrate Existing Scratch Disk.

- Remove your previous VAs from vRanger. To do this, browse to the Virtual Appliance Configuration dialog via **Tools > Options > Virtual Appliance Configuration**. Select the virtual appliances s to remove, and click **Remove**.

  Note If you are going to attach your existing scratch disk to your upgraded virtual appliance, do so before removing the old VA.

Migrate Existing Scratch Disk

The Virtual Appliance Deployment Wizard gives you the option of deploying a virtual appliance with or without a scratch disk. When deploying a new VA to upgrade an existing virtual appliance used for replication, do not create a scratch disk during the deployment process. You can add the existing scratch disk to the new virtual appliance, as described below:

1. From the VI Client, right-click on the new virtual appliance, and select **Edit Settings**.
2. On the Hardware tab, click **Add**.
3. Select **Hard Disk**. Click **Next.**
4. Select **Use an existing virtual disk**.
5. Browse to the location of your existing scratch disk. Select the VMDK for the scratch disk and click **OK**.
6. Using the console in the VI client, login to the virtual appliance. Restart the VM by typing `reboot` at the prompt.

Upgrading a Previous vReplicator Installation

vReplicator 3.x customers current on maintenance can migrate to vRanger 5.4 - Replication Only.

Due to the differences in application architecture, there is no upgrade path from vReplicator 3.x to vRanger 5.4. vRanger 5 will need to be installed fresh (using the full installer) and replication jobs will need to be re-created.

The high-level process for migrating from vReplicator to vRanger 5.4 is as follows:

1. Request a new vRanger 5.4 license.

   A new license is required for vReplicator customers migrating to vRanger 5.4. Please request one using the Quest Software Licence Request form at: *https://support.quest.com/LicenseKey.aspx.*

   Note Current vReplicator 3.x customers who are also vRanger customers may want to request a combined license file that includes backup and replication licensing.

2. Download and install vRanger using the Full installer. See Installing vRanger for the installation procedures.

   Caution If you will be re-creating your replication jobs, do not uninstall vReplicator 3.x. You may install and run vRanger on the same machine as vReplicator 3.x without issue.

3. Configure vRanger as appropriate. See "Configuration through the Startup Wizard for more information.

4. Re-create replication jobs to match your vReplicator configuration.

   vRanger replication jobs can re-use the existing target VMs created by the vReplicator jobs. This eliminates the need to perform a full synchronization to start the new replication jobs. When configuring jobs, ensure that the host and datastore configuration matches the original job. vRanger will recognize the existing target VM and resume replication without sending the full VM.

   Caution Disable the vReplicator job before enabling its vRanger counterpart.

5 After validating that all replication jobs have been properly migrated and are working correctly, uninstall vReplicator.

Upgrading from vRanger Pro 3.x

vRanger 5.2 and later versions do not support importing legacy jobs or restoring legacy archives. If you are a vRanger Pro 3.x customer and want to migrate to the current platform, you will need to first upgrade to an intermediate build such as vRanger 5.0.

Installing vRanger

This chapter guides you through the process of installing vRanger using the application installer.

This chapter contains the following sections:

vRanger Installation Overview 35
Installing vRanger 35
Install vRanger Catalog Manager 47

vRanger Installation Overview

This version of the software can be installed on a physical or virtual machine. When you complete one of these processes, three services will be installed: vRanger service, vRanger vAPI service, and vRanger FLR service.

You will need the following to install vRanger:

- A physical or virtual machine to host the installation.
- Administrator access to the machine on which the software will be installed.
- Administrator access to the source VMs.

Installing vRanger

The vRanger Installer includes several options for database configuration. The procedures are included below.

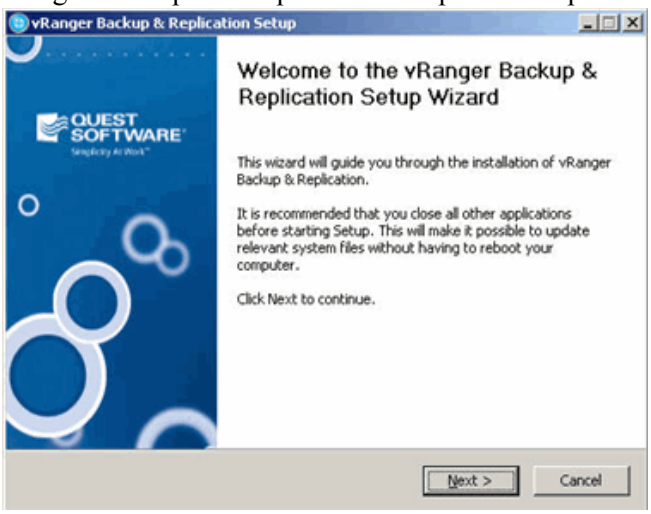
Install vRanger on a New Instance of SQL Express 2005

This procedure assumes that you have already downloaded the vRanger software and saved it to an accessible location.

Step 1: vRanger Setup

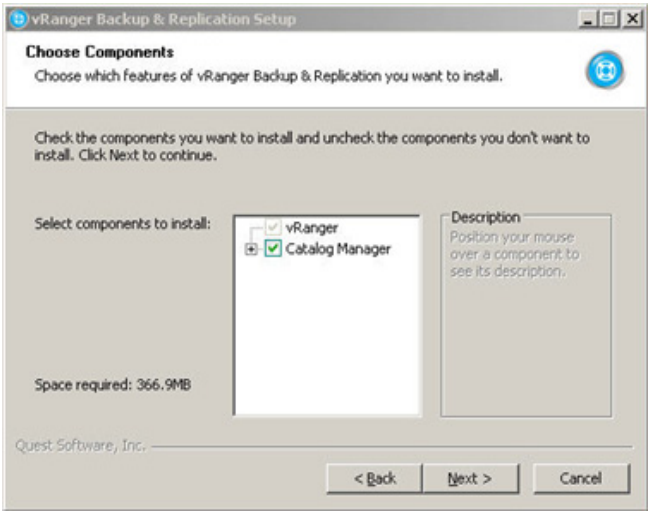
1 Double-click the *vRanger-5.4-Setup.exe* file.

The vRanger Backup and Replication Setup Wizard opens. Click **Next.**



2 The License agreement screen displays. Click **I Agree**.

3 The Choose Components screen displays.

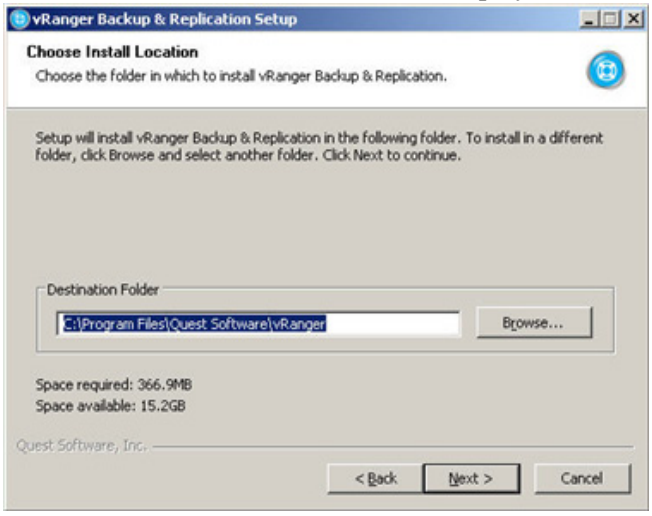


4 Select the components you wish to install.

Note Both **vRanger** and **Catalog Manager** are selected by default. You can choose to deselect catalog manager, and install it separately at a later time, if you wish.

5 Click **Next**.

6 The Choose Install Location screen displays.

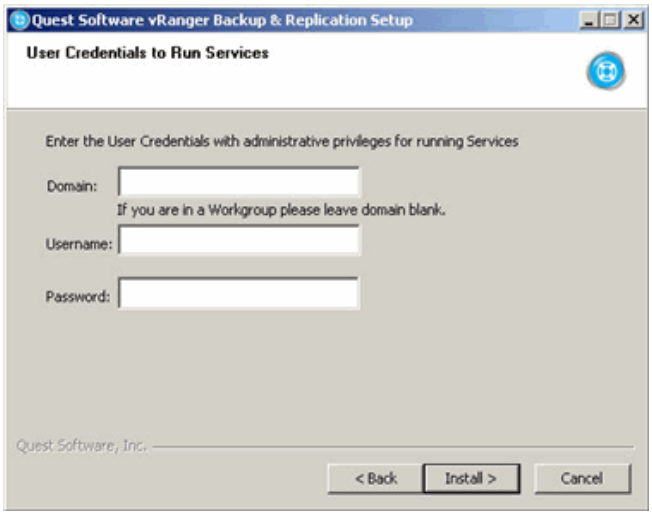


7 You can accept the default folder, or browse to another location of your choice. Press **Next**.

Step 2: User Credentials

The User Credentials dialog displays. This configures the account that will be used to run the services installed by vRanger.

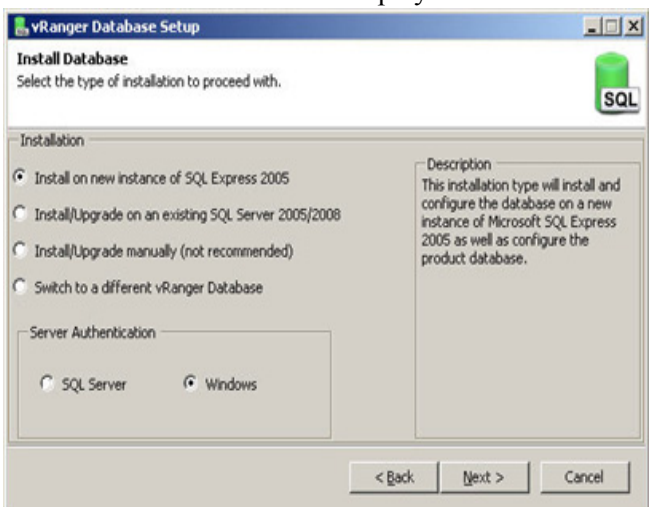
Caution The user account needed for this step must have administrator privileges on the vRanger machine.



1. In the **Domain** field, enter the domain in which the user account is located.
2. In the **Username** field, enter the username for the account.
3. In the **Password** field, enter the password for the account.
4. Click **Install.**

Step 3: Install Database

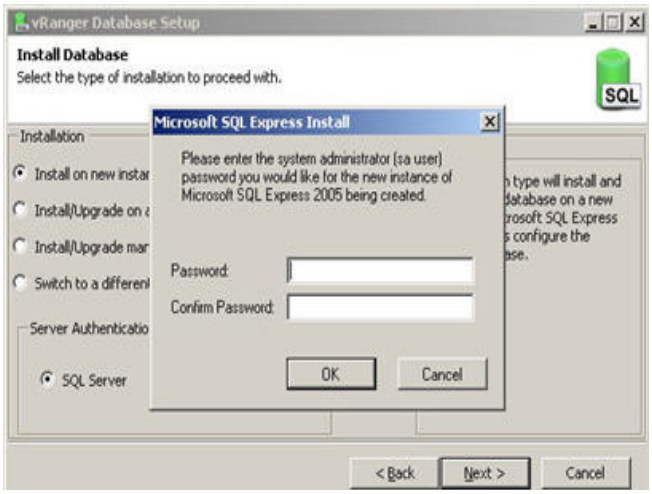
1. The vRanger Database Setup screen displays. Press **Next.**
2. The **Install Database** screen displays.



3. Click **Install on new instance of SQL Express 2005.**
4. Select a server authentication method.

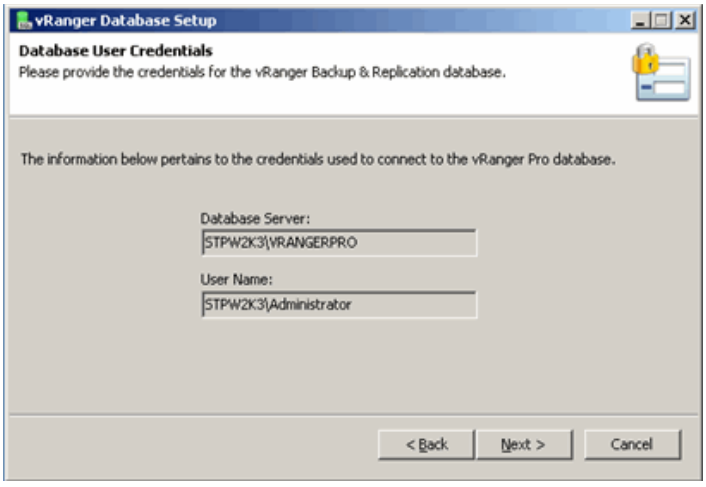
- **SQL Server:** Enter and confirm the system administrator (sa) password when you select Mixed Mode authentication. Setting strong passwords is essential to the security of your system. Never set a blank or weak sa password.
- **Windows**: When a user connects through a Windows user account, SQL Server validates the account name and password using information in the Windows OS. Windows Authentication uses Kerberos security protocol, provides password policy enforcement (complexity validation for strong passwords), provides support for account lockout, and supports password expiration.

5 If you selected SQL Server, you will be prompted to enter a password for the SA account.



or

If you selected Windows, the installation will continue using the account specified in Step 2: User Credentials.

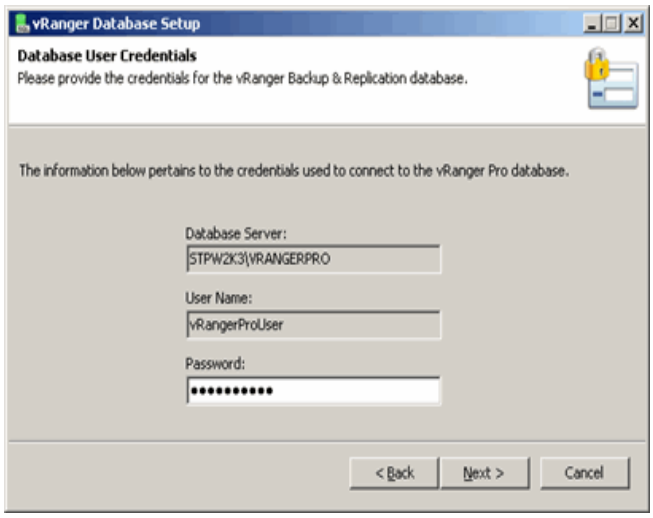


6 Click **Verify** to test connectivity to the database.

7 When the **Connection Successful** display, click **OK.**

8 Click **OK** or **Next,** depending on your authentication method.

The Database User Credentials dialog displays.

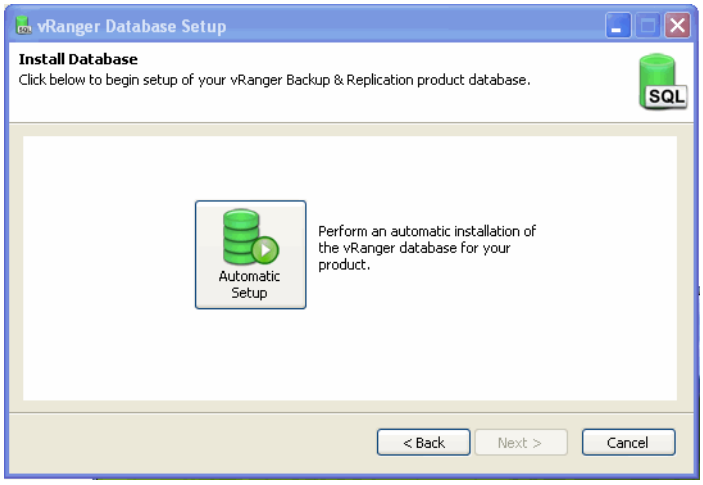


Note vRanger creates an account to connect to the Quest database. This account uses a default password of “V!ZionC0re”. Quest Software recommends changing this default password. You may enter a new password on this screen.

9 Click **Next.**

Step 4: Automatic Setup

The Install Database dialog displays.



1 Click **Automatic Setup.**

The database is installed.

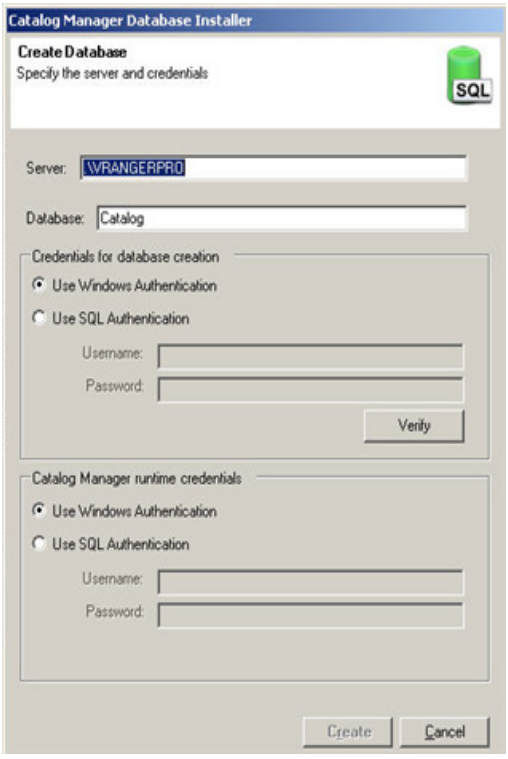
2 When the installation is completed, click **Next.**

3 Click **Finish.**

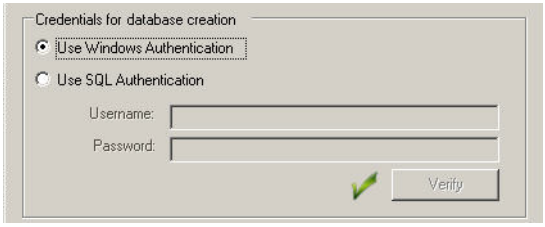
Step 5: Catalog Manager Database Installer

Note If you de-selected the Catalog Manger option during initial installation, Step 5 (catalog Manager Database Installer) will not appear.

The installation continues until the **Catalog Database** screen displays.



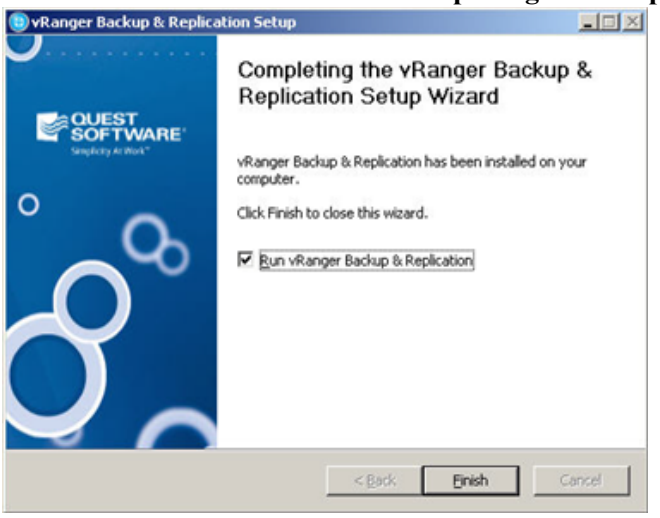
1. You can accept the default server name, or enter an alternate.
2. If you are using **Windows Authentication,** click **Verify.** A check mark appears next to the verify box.



3. If you are using **SQL Authentication,** enter the **username and password** for the database, and click **Verify.** A check mark appears next to the verify box.
4. If you are using **Windows Authentication** for the **Catalog Manager runtime credentials**, click **Create.**
5. If you are using **SQL Authentication** for the **Catalog Manager runtime credentials**, enter the **username and password** for the database, and click **Create.**

Step 5: Complete the Installation

The installation continues until the **Completing the Setup Wizard Dialog** displays.



1 Select **Run vRanger Backup & Replication** to launch the application immediately.

2 Click **Finish**.

Install vRanger on an Existing SQL 2005/2008 Server

This procedure assumes that you have already downloaded the vRanger software and saved it to an accessible location.

Step 1: vRanger Setup

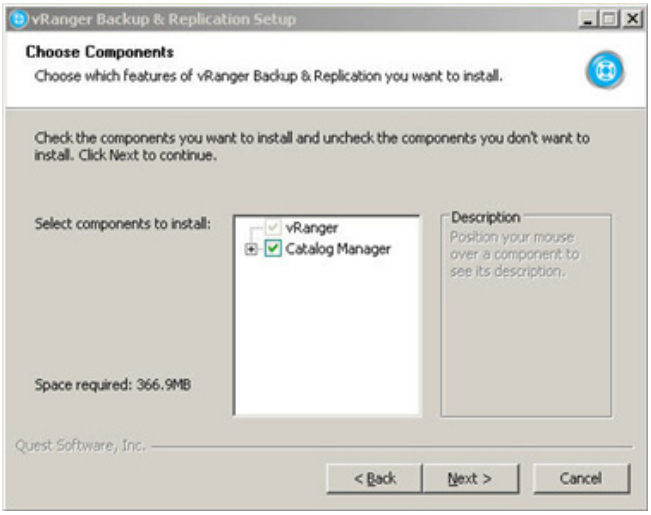
1 Double-click the *vRanger-5.4-Setup.exe* file.

The vRanger Backup and Replication Setup Wizard opens. Click **Next**.



2 The License agreement screen displays. Click **I Agree**.

3 The Choose Components screen displays.

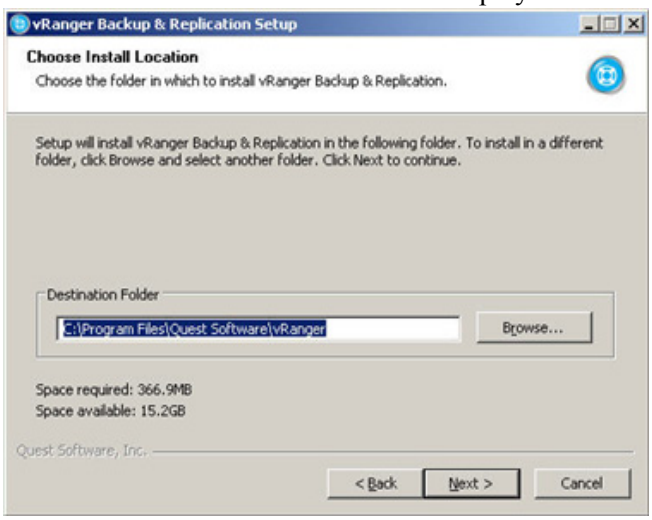


4 Select the components you wish to install.

Note Both **vRanger** and **Catalog Manager** are selected by default. You can choose to deselect catalog manager, and install it separately at a later time, if you wish.

5 Click **Next**.

6 The Choose Install Location screen displays.

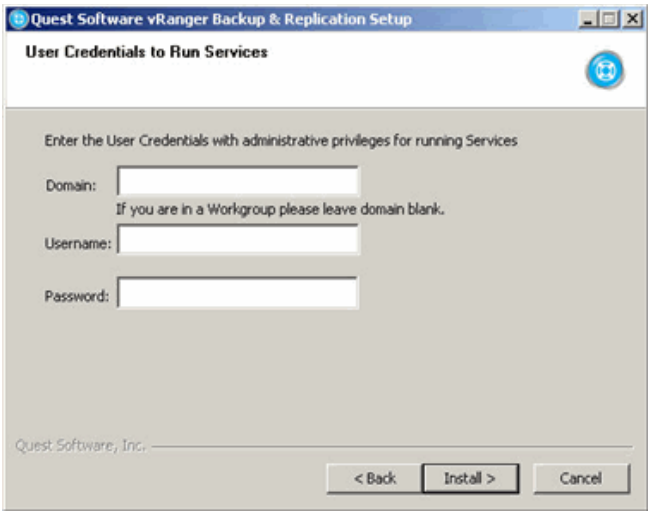


7 You can accept the default folder, or browse to another location of your choice. Press **Next**.

Step 2: User Credentials

The User Credentials dialog displays. This configures the account that vRanger will use to run the vRanger Service. The user account needed for this step must have administrator privileges on the local machine.

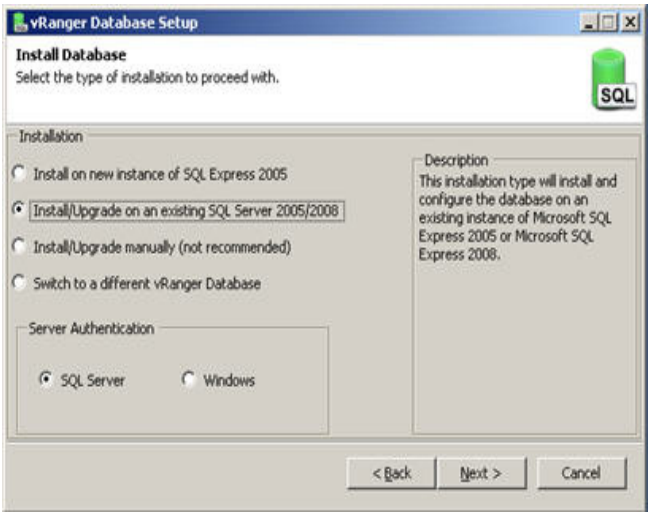
If you plan on using Windows Authentication for your SQL database, the account configured here will be used.



1. In the **Domain** field, enter the domain in which the user account is located.
2. In the **Username** field, enter the username for the account.
3. In the **Password** field, enter the password for the account.
4. Click **Install.**

Step 3: Install Database

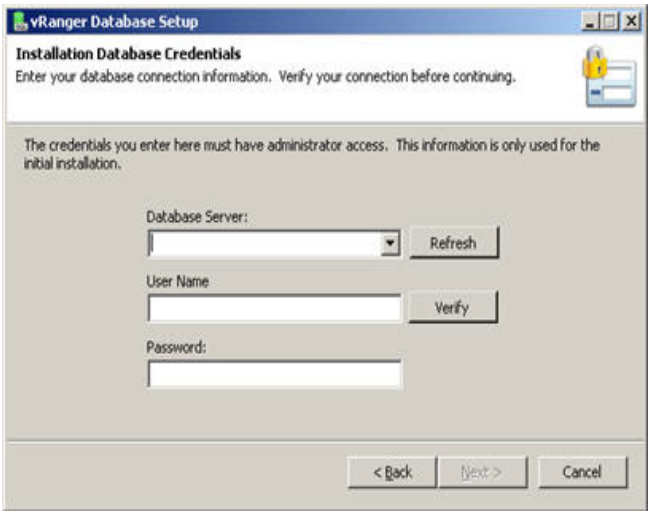
1. The vRanger Database Setup screen displays. Press **Next.**
2. The **Install Database** screen displays



3. Click **Install/Upgrade on an existing SQLS Server 2005/2008.**
4. Select a server authentication method.

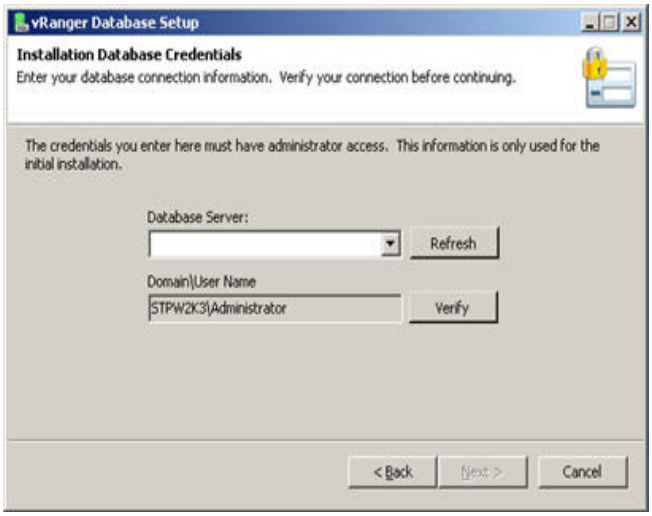
- **SQL Server:** Enter and confirm the system administrator (sa) password when you select Mixed Mode authentication. Setting strong passwords is essential to the security of your system. Never set a blank or weak sa password.
- **Windows**: When a user connects through a Windows user account, SQL Server validates the account name and password using information in the Windows OS. Windows Authentication uses Kerberos security protocol, provides password policy enforcement (complexity validation for strong passwords), provides support for account lockout, and supports password expiration.

5 Enter your database connection information. Click **Next**. If you selected SQL Authentication, you will see the screen below:



or

If you selected Windows Authentication, you will be prompted to select a SQL server. The credentials configured in Step 2: User Credentials. will be used.

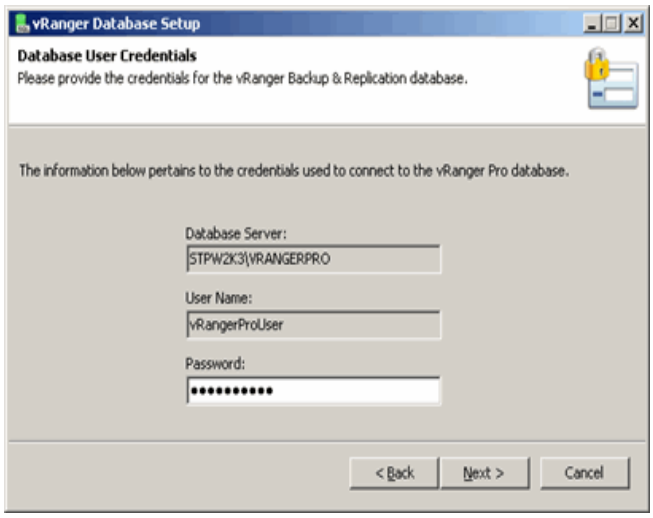


6 Click **Verify** to test connectivity to the database.

7 When the **Connection Successful** display, click **OK.**

8 Click **OK** or **Next,** depending on your authentication method.

The Database User Credentials dialog displays.

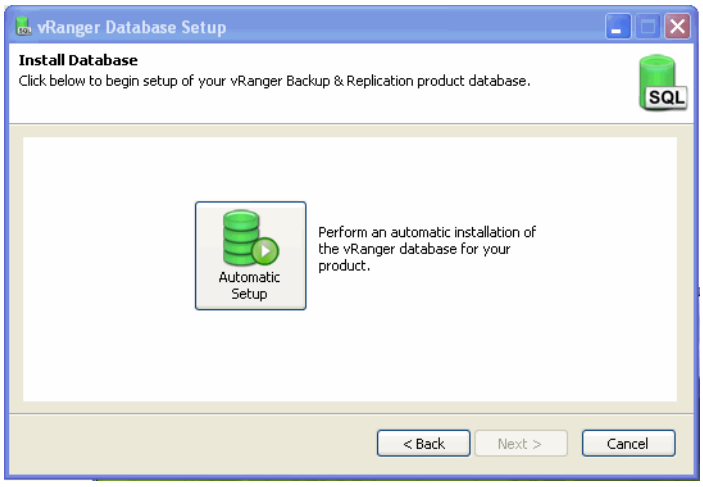


Note vRanger creates an account to connect to the Quest database. This account uses a default password of “V!ZionC0re”. Quest Software recommends changing this default password. You may enter a new password on this screen.

9 Click **Next.**

Step 4: Automatic Setup

The Install Database dialog displays.



1 Click **Automatic Setup.**

The database is installed.

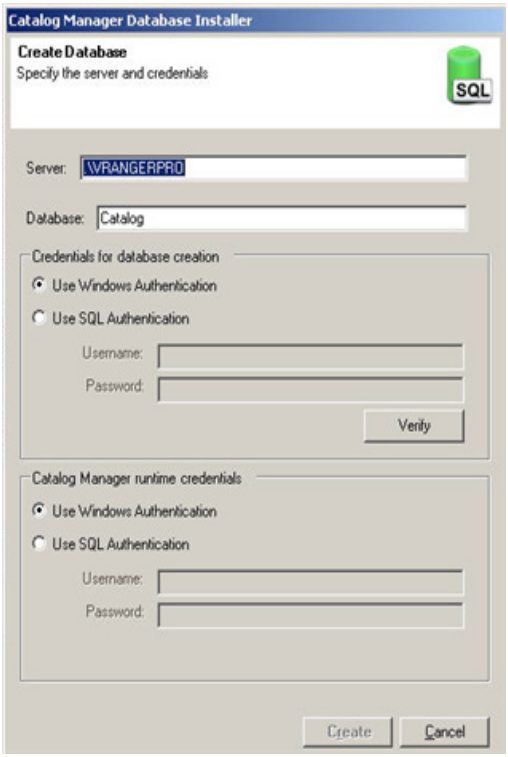
2 When the installation is completed, click **Next.**

3 Click **Finish.**

Step 5: Catalog Manager Database Installer

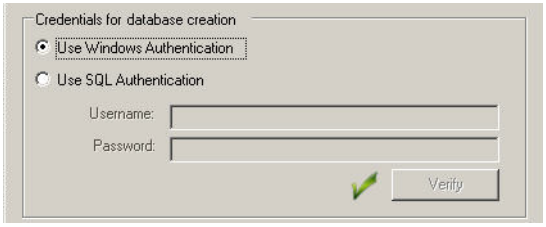
Note If you de-selected the Catalog Manger option during initial installation, Step 5 (catalog Manager Database Installer) will not appear.

The installation continues until the **Catalog Database** screen displays.



1 The Server field must be the same as your SQL instance. This should populate correctly by default.

2 If you are using **Windows Authentication,** click **Verify.** A check mark appears next to the verify box.



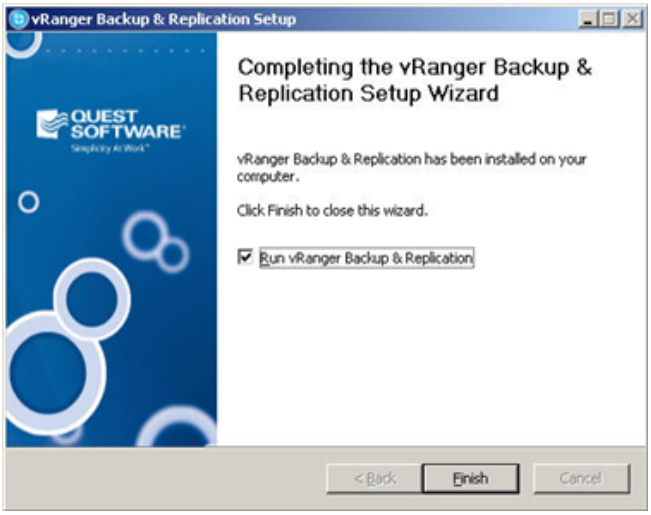
3 If you are using **SQL Authentication,** enter the **username and password** for the database, and click **Verify.** A check mark appears next to the verify box.

4 If you are using **Windows Authentication** for the **Catalog Manager runtime credentials**, click **Create.**

5 If you are using **SQL Authentication** for the **Catalog Manager runtime credentials**, enter the **username and password** for the database, and click **Create.**

Step 5: Complete the Installation

The installation continues until the **Completing the Setup Wizard Dialog** displays.



1 Select **Run vRanger Backup & Replication** to launch the application immediately.

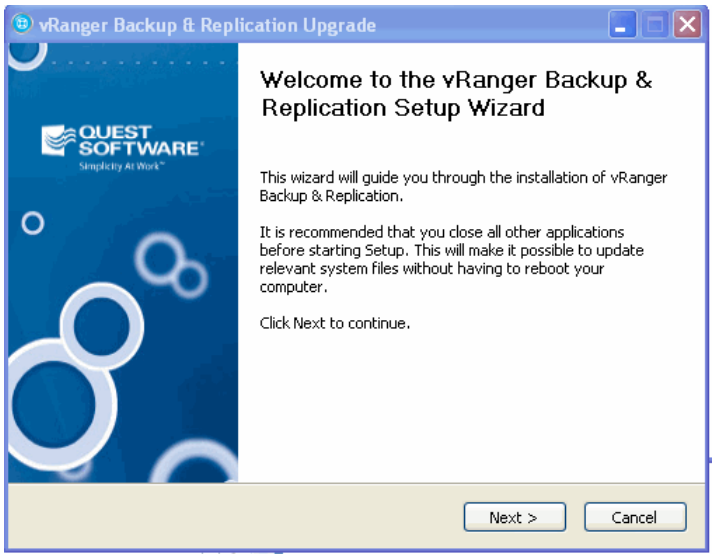
2 Click **Finish**.

Install vRanger Catalog Manager

If you wish to install the Catalog Manager after vRanger Backup & Replication is already installed, download the vRanger Upgrade file, and save it to an accessible location.

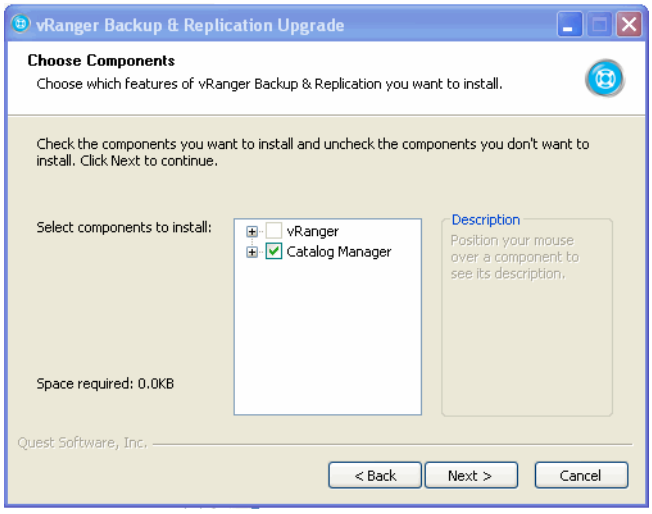
Step 1: vRanger Setup

1 Double-click the *vRanger-5.4-Upgrade-Setup.exe* file. The Upgrade screen Displays. Click **Next**.

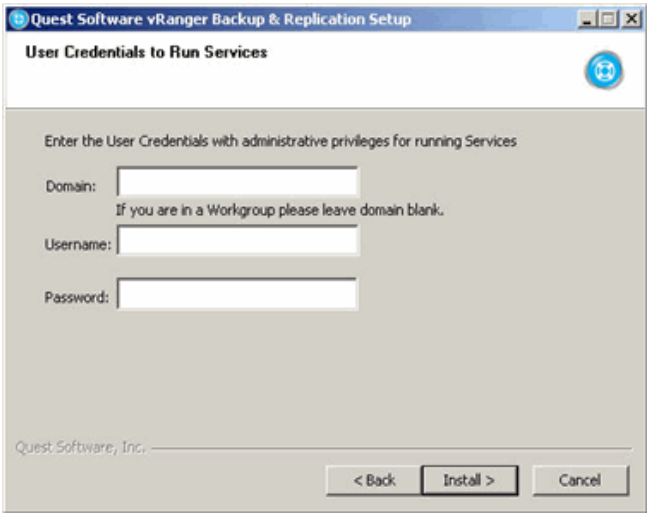


2 The License Agreement screen displays. Click **I Agree**.

3 The Choose Components screen displays. Select **Catalog Manager,** and click **Next.**

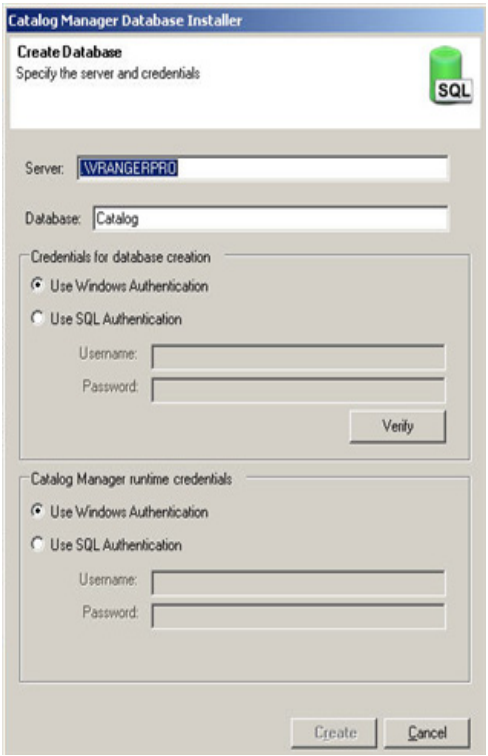


4 The User Credentials Screen displays.



1. In the **Domain** field, enter the domain in which the user account is located.
2. In the **Username** field, enter the username for the account.
3. In the **Password** field, enter the password for the account.
4. Click **Install.**

The installation continues until the **Catalog Database** screen displays.



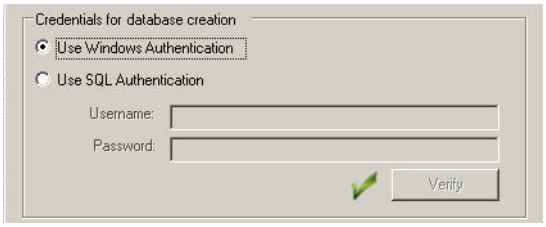
1. The Server field must be the same as your local SQL instance.

This value will populate to the default “VRANGERPRO” value. If you used the default SQL Express database, you can leave the default.

or

If you installed your own SQL instance on the vRanger server, you will need to change the **Server** field to the instance name.

2 If you are using **Windows Authentication,** click **Verify.** A check mark appears next to the verify box

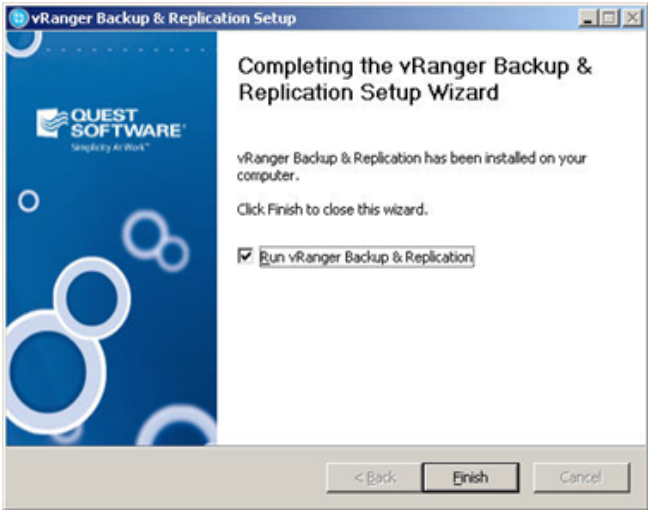


3 If you are using **SQL Authentication,** enter the **username and password** for the database, and click **Verify.** A check mark appears next to the verify box.

4 If you are using **Windows Authentication** for the **Catalog Manager runtime credentials**, click **Create.**

5 If you are using **SQL Authentication** for the **Catalog Manager runtime credentials**, enter the **username and password** for the database, and click **Create.**

6 The installation continues until the **Completing the Setup Wizard Dialog** displays.



7 Select **Run vRanger Backup & Replication** to launch the application immediately.

8 Click **Finish**.

Configuring vRanger

This chapter outlines the process of starting vRanger for the first time, licensing the application, and configuring connections with the Virtual Infrastructure.

This chapter contains the following sections:

Configuration Overview 52
Configuration through the Startup Wizard 52
Configuration without Using the Startup Wizard 62
Configuration Options 71
Catalog Filtering 73
Supplemental Instructions - Additional Repository Types 73

Configuration Overview

Before you begin configuring vRanger, confirm that you have access to all user names, passwords, and root passwords for the ESX hosts that you intend to use.

vRanger requires some basic configurations to ensure that the software functions properly. You complete the initial configuration through the Startup Wizard, which launches when you first install vRanger. If you would rather configure settings through the menu commands and icons on the main vRanger screen, you can do so. In either case, you can revise the settings at any time.

After completing the basic configuration process, you can use either the **Startup Wizard** or the **Configuration Options** dialog to manage your settings. Although the **Configuration Options** dialog offers some functionality that the **Startup Wizard** does not, you can use either dialog to manage host licensing or email server data. Only the **Configuration Options** dialog lets you manage resources on the task level. Given the role that tasks play in making backup and restore jobs, this resource is vital.

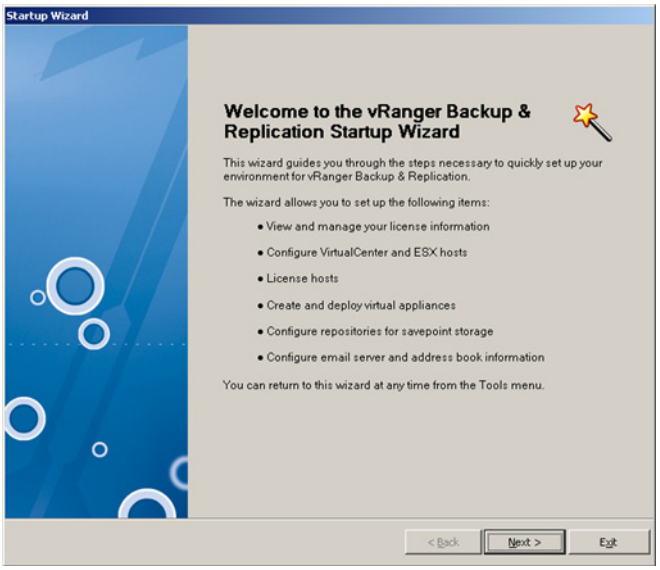
- Configuration through the Startup Wizard
- Configuration without Using the Startup Wizard
- Configuration Options

Configuration through the Startup Wizard

You must have an email SMTP server set up to enable notification during job creation. Later in this process, on the **Email Notification Selection** dialog, you will have the option of choosing recipients. A plain text email will be sent when the job completes. The notification will include the job results, if you select that option.

- Select a License
- VirtualCenter and Host Information
- Host Licensing Information
- Virtual Appliance Information
- Add Repositories
- Set up Mail Server Information/Add Email Addresses

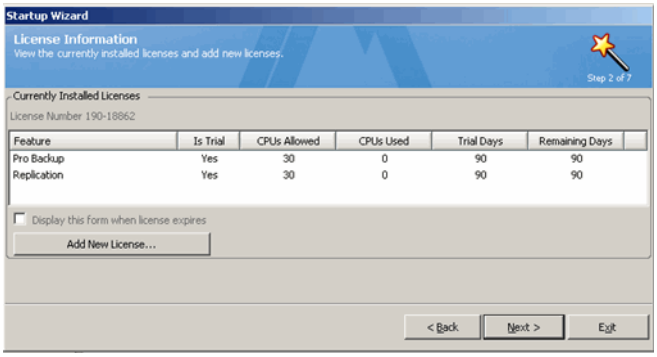
1 If you have just installed the software, click **Next** on the Startup Wizard. If not, access it through **Tools-->Startup Wizard.**



2 Click **Next.**

Select a License

The **Licenses** dialog displays.

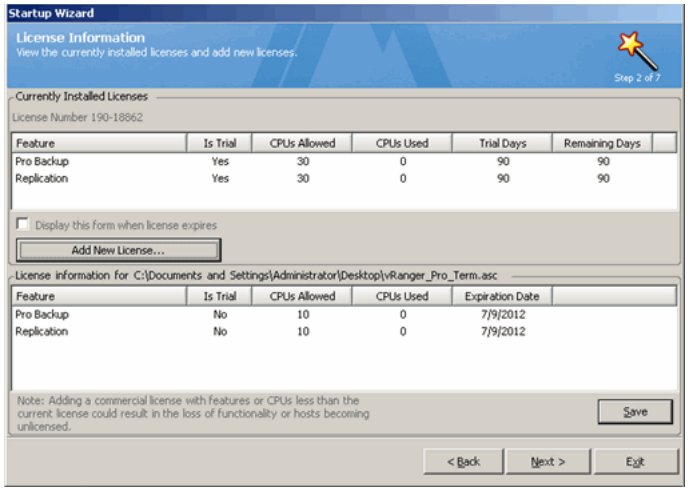


1 Click **Add New License.**

Note Starting with vRanger 5.2. the license file is different from those used in version 5.1 and 5.0. Do not use a license file for previous versions of this software. License files for vRanger 5.2 and later end in *.asc*.

2 Select the license.

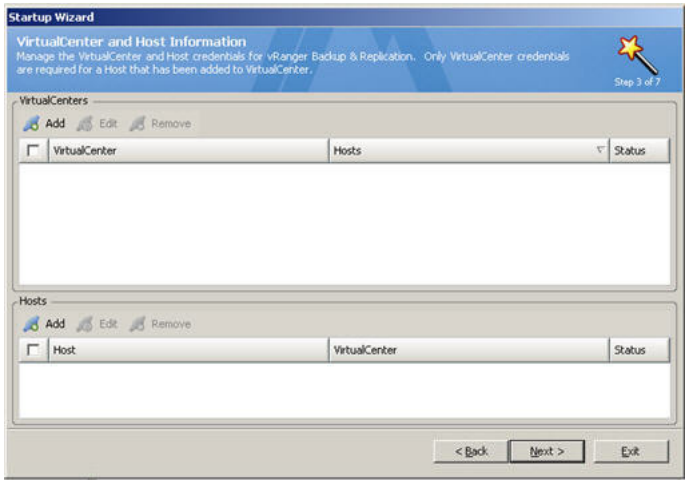
3 Click **Open.**



4 Click **Save.** Then, click **Next.**

VirtualCenter and Host Information

The **VirtualCenter and Host Information** dialog displays. Before vRanger can add source objects to the **My Inventory** pane, you must configure a connection to a vCenter and/or an ESX(i) Server.



Step 1: Adding a vCenter

1 In the VirtualCenters section, click Add.

2 In the **DNS Name** or **IP** field, enter the FQDN or IP address of the vCenter server.

3 In the **User Name** field, enter the user name of an account with privileges on the vCenter server. See the chapter "Configuring vCenter Permissions" for the required permissions for a vRanger vCenter account.

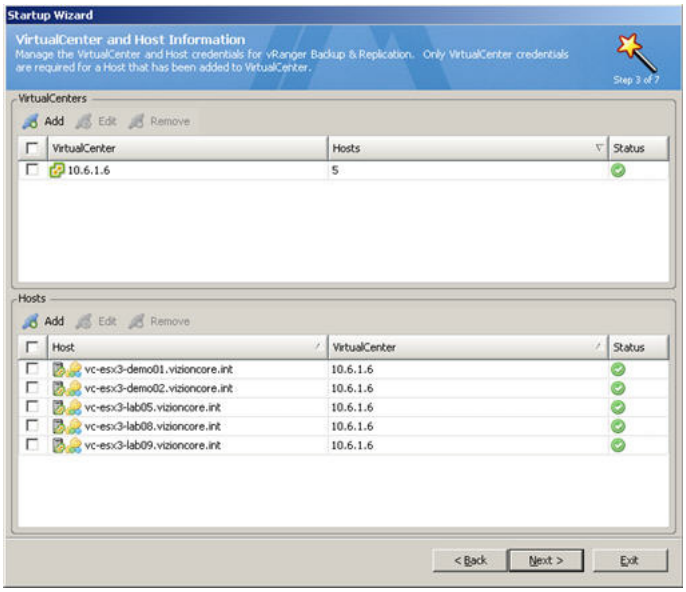
Caution The user name for the vCenter credential should be entered in the "username@domain" format, rather than "domain\username". Please avoid special characters in the user name.

4 In the **User Password** field, enter the password for the account used above.

Caution Please avoid special characters in the password.

5 Click **Save**.

The vCenter will display in the VirtualCenters section and on the **VirtualCenter and Host Information** dialog. The Hosts managed by that vCenter will display in the Hosts section.



Note that the hosts displayed show the icon . There are 4 key indicators shown in the icon:

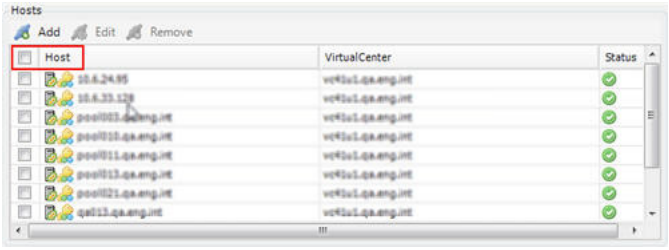
- The large gold key indicates that the host has been issued a vRanger license.
- The green dot indicates that the host has been assigned a backup license.
- The blue dot indicates that the host has been assigned a replication license.
- The authentication method for the host is indicated by the icon superimposed on the host icon:
  - if the host is authenticated with vCenter credentials only, the vCenter icon will appear superimposed over the host icon: 
  - If the host is authenticated with host credentials, a gold key will be superimposed over the host icon: 

Caution vCenter credentials are sufficient for operations that use only the vStorage API. You will need to credential each host in order for backup and replication operations to utilize the Service Console.

Step 2: Host Credentials

1 In the Hosts section, select one or more hosts. To select all hosts, select the upper-most check box.

Note You do not need to supply credentials for ESXi hosts.



2 Click **Edit.**

3 The Host Connections dialog appears. If you have selected multiple hosts, the DNS Name or IP section will display "[multiple connections]"

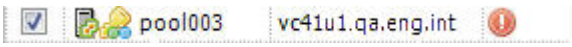
4 In the **User Name** field, enter an account for the host. You may use the root account if connections via root are enabled, or a non-root account. If the account does not yet exist on the host, select **Add user if user does not exist**.

5 In the **User Password** field, enter the password for the account used above.

6 In the **Root Password** field, enter the root password for the selected hosts. If you hosts use different root passwords, you will need to configure them in like groups based on the root password.

7 Click **Connect**. The icon next to the host will change to , showing that the vCenter icon has been replaced with a key.

If there is an authentication problem, such as connections via the root account being disabled, the status icon will display an alarm:



If this happens, you will need to edit the host connection to use a non-root user account. Make sure that the Add user if user does not exist option is selected.

Note ESXi requires the use of the root account. You cannot use a non-root account with ESXi.



8 When all connections have been made and verified, click **Next.**

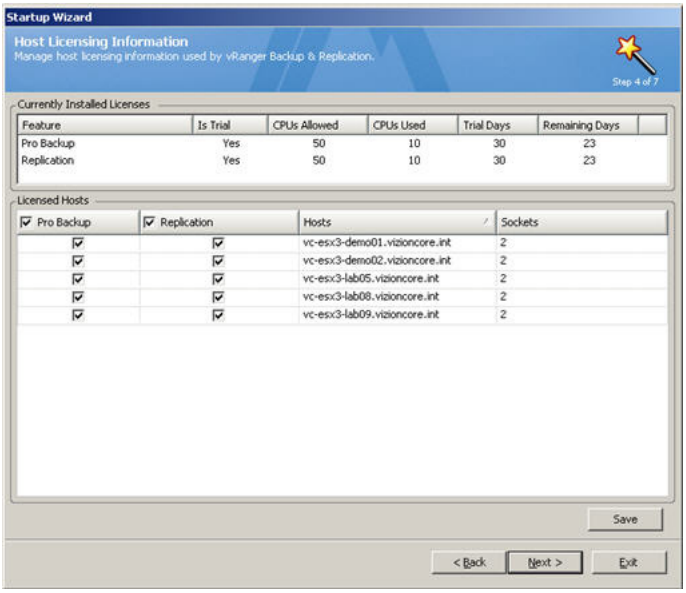
Step 3: Adding Hosts [Optional]

If you have hosts that are not managed by a vCenter, you can add them individually.

1. In the Host section, click **Add.**
2. In the **DNS Name** or **IP** field, enter the FQDN or IP address of the Host.
3. In the **User Name** field, enter an account for the host. You may use the root account if connections via root are enabled, or a non-root account. If the account does not yet exist on the host, select **Add user if user does not exist**.
4. In the **User Password** field, enter the password for the account used above.
5. In the **Root Password** field, enter the password for the root account.
6. Click **Connect**. The Host will be display in the Hosts section.

Host Licensing Information

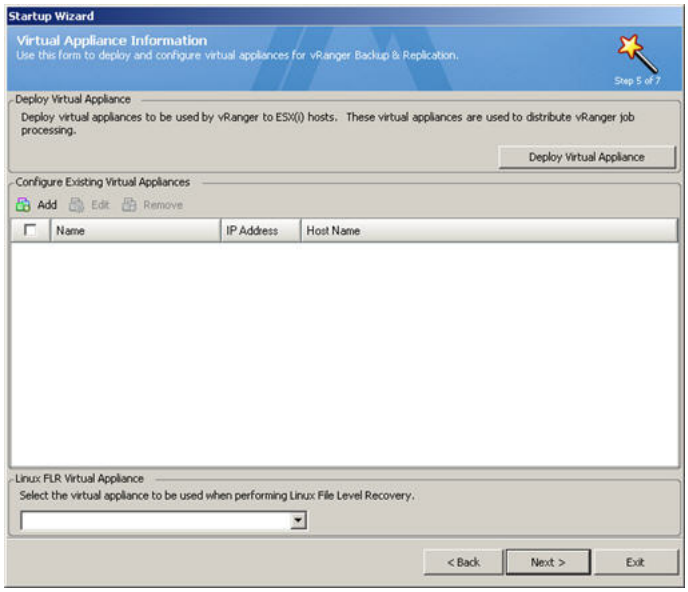
The **Host Licensing Information** dialog displays. It displays total licensed sockets, used sockets and the remaining days left in a trial period.



1. View the **CPUs Allowed** value to confirm the number of sockets that are licensed for protection. The number of licenses currently allocated is shown in the **CPUs Used** column.
2. The Licensed Hosts section lists the managed hosts, the number of sockets for each host, and the licensed features for that host.
   a. The **Sockets** column indicates the license "cost" of each ESX Host.
   b. In the **Pro Backup and**/or **Replication** column, select or deselect ESX Hosts until you have used all of the available licenses, or until all of your ESX Hosts are protected.
3. Click **Save.**
4. Click **Next.**

Virtual Appliance Information

vRanger uses a virtual appliance for both Linux file-level recovery and for replication to and from VMware ESXi servers.



To simplify the startup procedure, the instructions for deploying and configuring the virtual appliances have been moved to Configuring the Virtual Appliance.

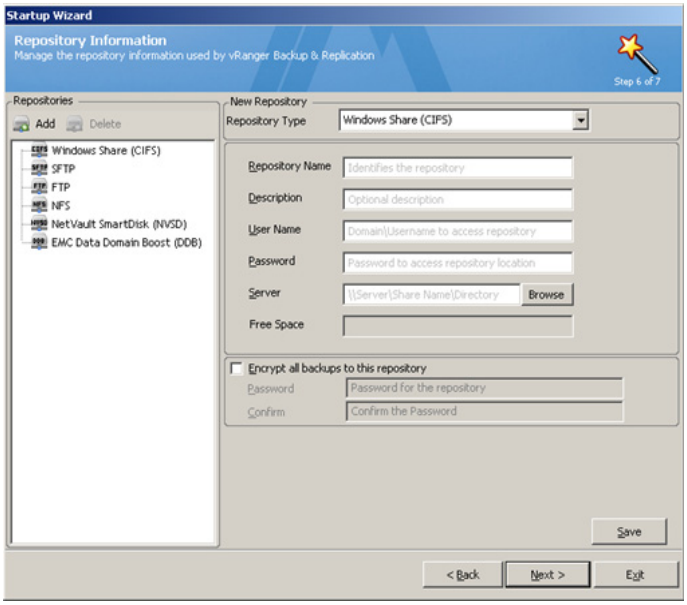
You may skip the virtual appliance configuration step now and continue with the Startup Wizard. You may access the Virtual Appliance Configuration dialog at any time via the **Tools>Options** menu.

Add Repositories

vRanger uses repositories to store backup archives. Repositories can be either a CIFS, NFS (version 3), FTP, or SFTP share. In addition, s you may also deduplicate your backups by using a NetVault SmartDisk (v1.5 or later) instance or Data Domain system with DD Boost as a repository.

Note For more information on **NetVault SmartDisk**, see the SmartDisk page of the Quest Software website: *http://www.quest.com/netvault-smartdisk/.* For more information on Data Domain's **DD Boost** technology, see the Data Domain website: *http://www.datadomain.com/products/dd-boost.htAdminiml*

The procedure below shows mounting a CIFS share to the My Repositories pane. The procedures for the other repository types are described in Supplemental Instructions - Additional Repository Types.



1. To add a CIFS repository, navigate to the My Repositories pane. Right-click anywhere in the My Repositories pane. Select **Add--> CIFS.**
2. If the repository you want to add is listed on the left of the screen, click it to populate the fields on the right.Click **Update** and **Next.** If it is not listed, follow the steps below.
3. In the **Repository Type** section, select **Windows Share (CIFS),** if necessary**.**
4. Populate the **Repository Name** field.

   This value will display in the **My Repositories** pane.
5. Populate the **Description** field.
6. Enter a username and password in the appropriate fields.
7. In the **Server** field, type the UNC path to the desired 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.

Caution If you wish to use the **Encrypt all backups** feature**, make certain to retain** the password you enter in the following steps. There is no back-door or admin-level password. If the password is unknown, the backups will not be usable.

8. Select **Encrypt all backups to this repository** if you wish these backups to be password-protected.

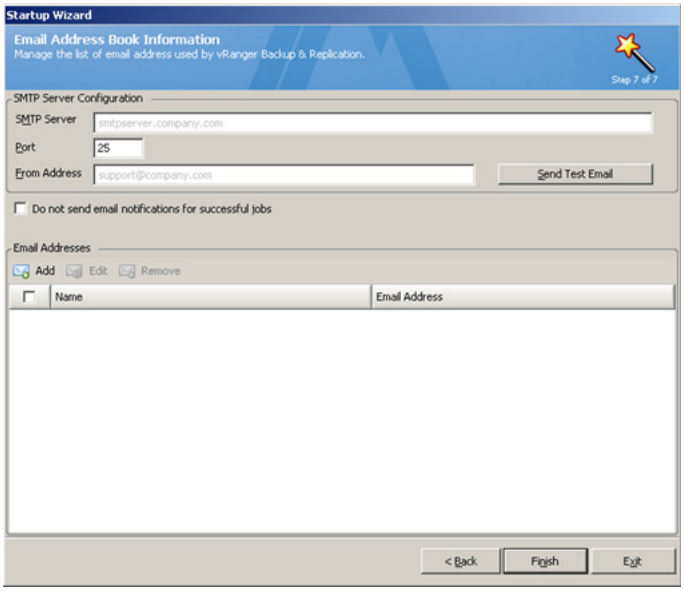
   Note Encryption is not supported for NetVault SmartDisk and Data Domain Boost repositories.
9. Enter a Password for the encrypted repository -- confirm the password by re-entering it.
10. Click **Save** -- the connection to the repository is tested and the repository is added to the My Repositories pane and the **Repository Information** dialog.
11. vRanger will check the configured repository location for existing manifest data to identify existing savepoints. If any are found, you will be prompted to take one of three actions:

- Import as Read-Only - with this option, all savepoint data will be imported into the vRanger database, but only for restores. You will not be able to backup to this repository.
- Import -all savepoint data will be imported into the vRanger database. vRanger will be able to use the repository for backups and restores. vRanger requires read and write access to the directory.
- Overwrite - the savepoint data will be retained on the disk, but will not be imported into vRanger. vRanger will ignore the existence of the existing savepoint data and treat the repository as new.

12 Click **Next**.

Set up Mail Server Information/Add Email Addresses

The Mail Server Information dialog displays. When you configure an SMTP server, select one that does not require authentication so that there are no obstacle to email notification transmission**.**



Step 1: SMTP Server

1 In the **SMTP Server** field, enter the DNS name or IP of an SMTP server.

2 In the **From Address** field, enter the email address that vRanger should use.

Note Make sure that you use a valid email account registered to the SMTP server that you added.

3 Click **Send Test Email.**

4 If desired, select **Do not send email notifications for successful jobs**.

Step 2: Address Book

1 To add recipients, click **Add.**

2 Populate the **Name** and **Email Address** fields.

3 Click **Save** to add the information to the Email Addresses list.

4 Repeat steps 1-3 to include additional contacts.

5 Click **Finish.**

Configuration without Using the Startup Wizard

These instructions describe the process for configuring vRanger without using the Startup Wizard. During this process you will:

- Add a VirtualCenter
- Add an ESX Server
- Add a Repository
- Configure an SMTP Server
- Add Email Address
- Configure Virtual Appliances
- Import License File
- Manage Host Licensing
- Manage Job Configuration Settings
- Configuring Linux File Level Restoration

Note To configure multiple hosts under the same vCenter, the system retains the data you entered to add credentials for the first host.

Add a VirtualCenter

1. To add a VirtualCenter, navigate to the **My Inventory** view. From the **Add icon** , select **VirtualCenter.**
2. On the **VirtualCenter Credentials** dialog, populate the **DNS Name or IP, User Name,** and **User Password** fields. Leave the **Port Number default** (443) as is. Click **Connect.**

   Note The user name for the vCenter credential should be entered in the “username@domain” format, rather than “domain\username”. Please avoid special characters in the user name and password.

   vRanger attempts to connect to the vCenter using the current configuration. If it is successful, the vCenter displays in the **My Inventory** pane.

Add an ESX Server

1. From the **My Inventory** view, select the **Add Icon-->ESX Host.**

   Note If the connection is unsuccessful, confirm that the configuration settings are correct and that the vCenter is visible to the computer where vRanger is installed.

2. On the **Add Host Credentials** dialog, populate the **DNS Name or IP, User Name, User Password,** and **Root Password** fields. Leave the **Port Number** default (22). Click **Connect.**

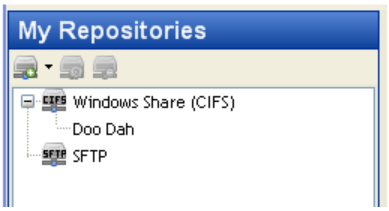
   The host is added to the tree structure under the vCenter. Confirm this noting that a gold key icon displays adjacent to it in the **My Inventory** pane.

Add a Repository

1 To add repository, navigate to the My Repositories pane. Click to highlight the desired repository type. Right-click the node and select **Add-->Windows Share CIFS.**

Note These instructions describe the process for adding a CIFS repository. The procedures for the other repository types are described in Supplemental Instructions - Additional Repository Types.

2 On the **Add Repository** dialog, populate the **Repository Name, DNS Name or IP, Target Directory, User Name,** and **User Password** fields. The Description field is optional**.**



3 In the **Server** field, type the name of the server you want.

Caution If you wish to use the **Encrypt all backups** feature**, make certain to retain** the password you enter in the following steps. There is no back-door or admin-level password. If the password is unknown, the backups will not be usable.

4 Select **Encrypt all backups to this repository** if you wish these backups to be password-protected.

5 Enter a Password for the encrypted repository -- confirm the password by re-entering it.

6 Click **Update** -- the connection to the repository is tested and the repository is added to the My Repositories pane and the Repository Information dialog.

7 Click **OK**.

Configure an SMTP Server

1 Select **Tools-->Options.**

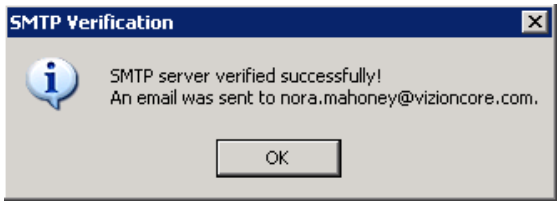
2 Under the General node on the Configuration Options dialog, click **Email Configuration.**

3 Populate the **SMTP Server** field.

4 Leave the default (25) in the **Port** field.

5 In the **From Address** field, enter an email address from which notifications should be sent.

6 Click **Send Test Email.**
The confirmation message confirms the server connection and successful transmission to the email address you entered.



7 Click **OK.**

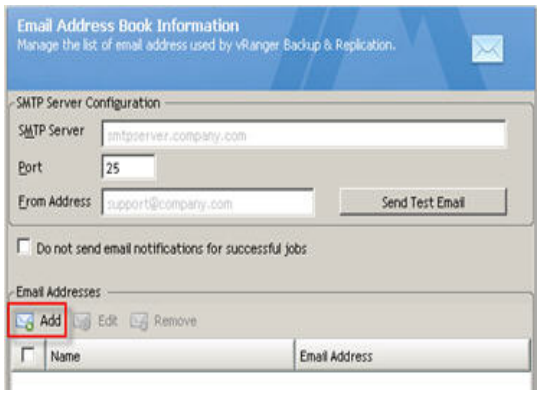
8 If desired, select **Do not send email notifications for successful jobs**.

Add Email Address

1 Select **Tools-->Options.**

2 Under the General node on the Configuration Options dialog, click **Email Configuration.**

3 In the **Email Addresses** section, click **Add.**



4 Click the **Add** button.

5 Enter the contact name and email address, and click **OK.**

Edit Email Address

1 Select **Tools-->Options.**

2 Under the **General** node, click **Email Configuration.**

3 In the **Email Addresses** section, select the email address that you want to edit. Click **Edit**.

4 Update the information and click **Update.**

5 The information is updated and moved to the **Email Addresses** section.

6 Click **OK.**

Remove Email Address

1 Select **Tools-->Options.**

2 Under the General node on the Configuration Options dialog, click **Email Configuration.**

3 In the **Email Addresses** section, select the email address that you want to delete.

4 Click **Remove.** The listing is deleted.

5 Click **OK.**

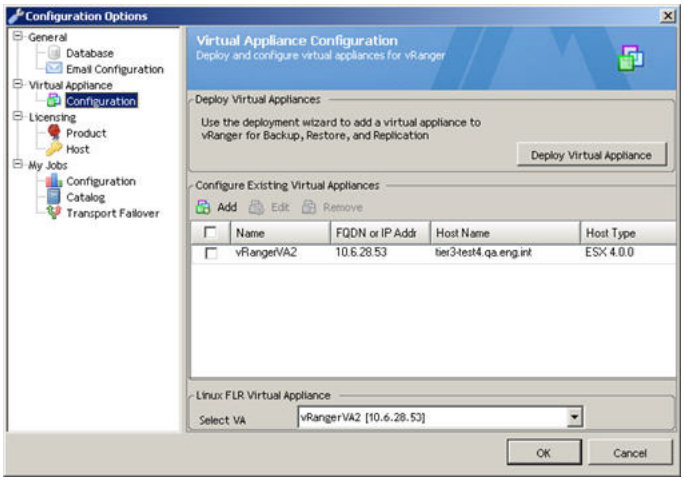
Configure Virtual Appliances

vRanger uses a virtual appliance for both Linux file-level recovery and for replication to and from VMware ESXi servers. The Virtual Appliance Configuration dialogue allows you to add a configured VA to vRanger, and select the VA to use for Linux FLR. Virtual appliances deployed using the Virtual Appliance Deployment Wizard will be added to vRanger automatically.

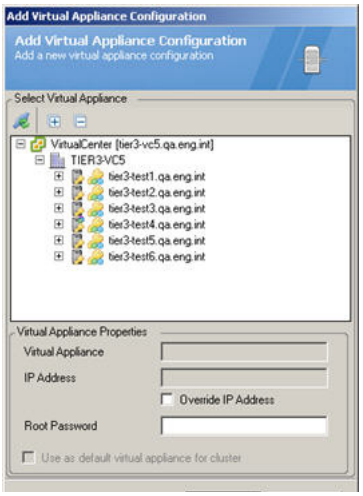
Note You must have deployed and configured at least one virtual appliance before you can add it to vRanger. See Configuring the Virtual Appliance for instructions on virtual appliance deployment.

To add a configured virtual appliance to vRanger:

1 From the **Configuration Options** dialog, select **Virtual Appliance Configuration**.



2 Click **Add**. The **Add virtual appliance configuration** dialog appears, showing the vCenter inventory tree.



3 Browse the inventory tree, and select the virtual appliance.

4 Enter the root password for the virtual appliance, and click **OK**.

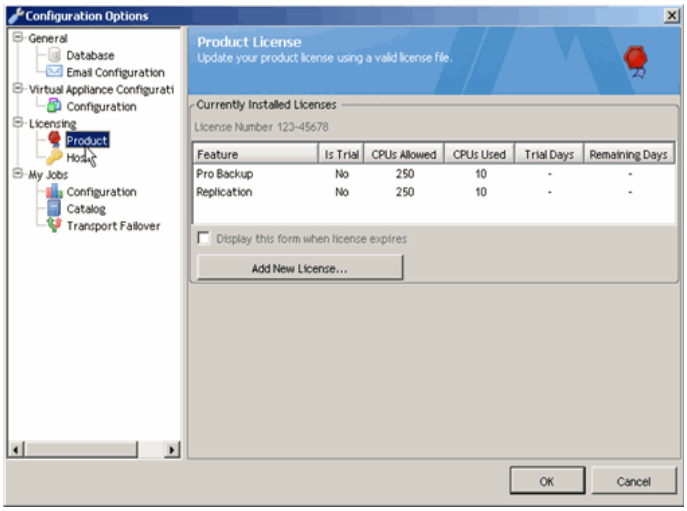
The virtual appliance will appear in the Deployed Virtual Appliances section:

Import License File

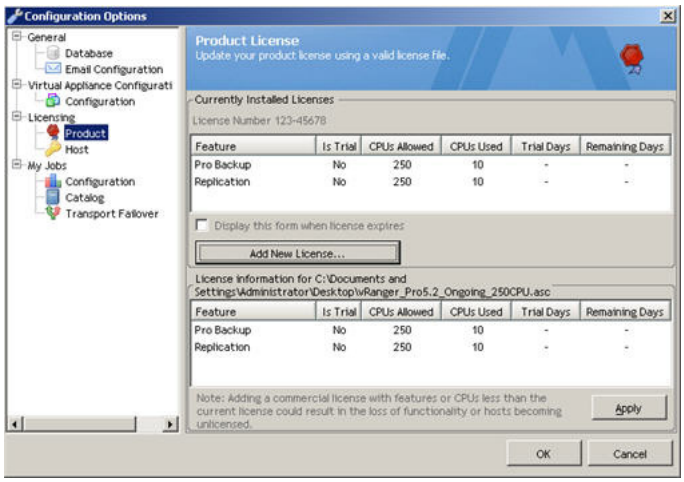
Before you start this process, confirm that you have placed your license file in a location that you can reach easily.

1 Select **Tools-->Options.**

2 Under the **Licensing** node on the **Configuration Options** dialog, click **Product.**



3 Click **Add New License.**



4 Browse to the location where you stored the license file. Click to select it and click **Open.** The new license information is added to the dialog.

Note Starting with vRanger 5.2. the license file is different from those used in version 5.1 and 5.0. Do not use a license file for previous versions of this software. License files for vRanger 5.2 and later end in *.asc*.

5 Click **Apply.**
The dialog refreshes with the new license information added.

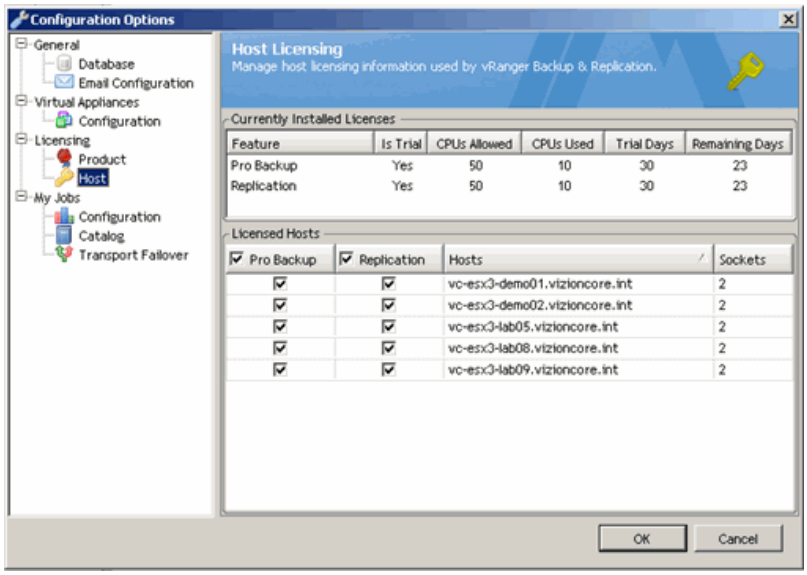
6 Click **OK.**

Manage Host Licensing

Before you start this process, make sure that you have imported the license file and confirmed that it is adequate for managing the hosts that you want to use. The Host Licensing Summary section includes the total number of CPU licenses, the number being used currently, and the number of licenses remaining. These numbers will increment and decrement based on the selections you make on this dialog.

1 Select **Tools-->Options.**

2 Under the **Licensing** node, click **Host.**



3 In the Currently Installed Licenses section, view the **CPUs Allowed** value to confirm the number of sockets that are licensed for protection. The number of licenses currently allocated is shown in the **CPUs Used** column.

4 The Licensed Hosts section lists the managed hosts, the number of sockets for each host, and the licensed features for that host.

   a The **Sockets** column indicates the license "cost" of each ESX Host.

   b In the **Pro Backup and**/or **Replication** column, select or deselect ESX Hosts until you have used all of the available licenses, or until all of your ESX Hosts are protected.

5 Click **OK.**

Manage Job Configuration Settings

Through the **Configuration Options** dialog, you can set limits for the number of tasks running, the time frame for task execution, and the space allowed on a datastore to accommodate snapshot growth.

The maximum number of tasks fields are defined in the table below:

On vRanger	the maximum number of backup, restore and replication tasks running on this instance of vRanger at any one time
off a LUN	the maximum number of tasks allowed on any particular logical storage device
on a host	the maximum number of tasks running on a host at any given time
on each repository	the maximum number of tasks allowed on any specific repository at any specific time

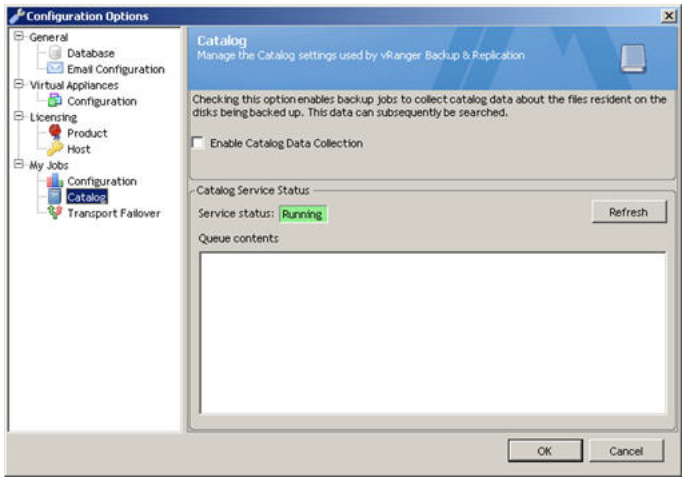
locally	the number of backup and restore tasks that are physically executing on the local vRanger machine.
per VA	the number of replication tasks running on a vRanger virtual appliance.

1. Select **Tools-->Options.**
2. Under the My Jobs node, click **Configuration.**
3. In the **Resource Management** section, set a maximum for the number of tasks that can be run:
   - on vRanger (>=1) -- Default is 100.
   - off a LUN (1-5) -- Default is 3.
   - on a host (1-4) -- Default is 1.
   - on each repository (>=1) -- Default is 3.
   - locally (1 - 20) -- Default is 3.
   - per VA (1 -18) -- Default is 2.
4. In the **Timeout** section, populate the **Task Timeout** (1-999 hours) field -- Default is 24
5. In the **Space needed on host** (in GBs) field, enter a number -- Default is 6.
6. Click **OK.**

Cataloging Options

The vRanger cataloging function must be enabled before data collection can begin. The Catalog dialog includes the option to enable or disable catalog collection, and displays the status of the Catalog Service.

In order for Catalog collections to function, the Catalog Service must display a status of "Running".



1. Select **Tools-->Options.**

2 Under the My Jobs node, click **Catalog.**

3 Select **Enable Catalog Data Collection**.

4 Click OK.

Note Cataloging must also be enabled for each backup job for which you wish to collect catalog data.

Configuring Linux File Level Restoration

To simplify the startup procedure, the instructions for deploying and configuring the virtual appliances have been moved to Configuring the Virtual Appliance.

Configuration Options

Through this dialog you can customize the basic settings that you selected in the Startup Wizard. You can access the Configuration Options dialog through Tools in the menu bar. The left pane of the dialog is set up in a nested structure.

General	• **Database**: displays the database server hosting the vRanger database. • **Delete Jobs data:** In order to reduce the size of your vRanger database, you may delete job data older than the configured date from the database. **Note** Deleted data will no longer be available for reporting. • **Email Server**: On this dialog, you can enter an SMTP server address and verify the connection to the port (default is 25). You can confirm successful transmission to the email address listed in the **From Address** field by clicking the **Send Test Email** button. • **Email Address Book**: Here you can add and manage the email addresses of recipients to whom you would like reports sent. **Note** The **New Email Address Section** becomes the **Edit Email Address** section when you select a listing in the **Email Addresses** section of the dialog.
Virtual Appliances	• **Configuration:** This dialog links to the vRanger virtual appliance, and allows you to add configured VA's for use by vRanger.
Licensing	• **Product License**: On this dialog you can view the current product licensing details and import a license when your current one expires or needs to be replaced. • **Host**: Use this dialog to allocate licensing to the hosts you added to the system. Refer to the **Host Licensing Summary** to view the total number of CPU licenses you are allowed, the number of licenses being used, and the number of licenses that remain.

My Jobs	**Configuration** • **Resource Management**: This section gives you access to task management information. -Maximum number of tasks running on vRanger (>=1) Default is 100. -Maximum number tasks running off of a LUN (1 - 5) Default is 3. -Maximum number tasks running on a host (1- 4) Default is 1. -Maximum number tasks running per repository (>=1) Default is 3. -Maximum number tasks running locally (1 - 20) Default is 3. -Maximum number tasks running per VA (1 - 18) Default is 2. • **Timeout**: In this section, you can set the period of time after which a task times out. The range is between 1 and 999 hours. • **Space needed on Hosts**: You can define the additional datastore space needed for snapshot growth during backup. Populate this field in GB--Minimum space needed on host (in GBs). The snapshot log file grows on the source while the VM is archived and copied to the destination. The default value is 6. Warning: If you allocate insufficient space, VMs on the datastore will power down and you could lose data. **Catalog** • **Catalog Service:** Click the checkbox to enable catalog data collection • **Catalog Service Status:** Status is listed as **Available** or **Unavailable –** click **Refresh** to recheck the status. • **Queue contents:** lists catalog queues. **Transport Failover** Use this screen to set the relative priority for the available transport options. This priority will be used by vRanger to automatically address transport failures. These default options can be changed at the job level.

Catalog Filtering

While there are thousands (or hundreds of thousands) of files in a typical VM, most are not relevant to file level recovery operations. In order to streamline cataloging operations, and reduce impact to the catalog database, vRanger filters files to be indexed in two ways:

- **Path** - by default, vRanger does not catalog any files in the directories listed below. Path filtering is determined by entries in the PathFilterTokens.txt file, located at *C:\Program Files\Quest Software\vRanger\Service\Configuration*.

Program Files	$Txf
Windows	RECYCLER
$Extend	System Volume Informa-
$TxfLog	tion
	I386

- **File** - By default, vRanger does not catalog files of the type below. File filtering is determined by entries in the FilesFilterTokens.txt file, located at *C:\Program Files\Quest Software\CatalogManager\Config\Files*.

.lnk	$Boot	$Reparse
$MFT	$BadClus	$RmMetadata
$Volume	$Secure	$Repair
$AttrDef	$UpCase	$Tops
$BitMap	$Quota	$TxfLog
	$ObjID	

Note File filtering applies to un-filtered paths. If a path is filtered, files in that path do not need to be.

For most situations, the default filtering options will be sufficient. If you want to filter out additional paths or files, simply add the path or file to the appropriate text file.

Supplemental Instructions - Additional Repository Types

The main procedures describe the process for adding a CIFS repository. To add an NFS, SFTP, FTP, or NetVault SmartDisk (NVSD) repository, see the appropriate section below.

- Adding an NFS Repository
- Adding an FTP Repository
- Adding an SFTP Repository
- Adding an NVSD Repository
- Adding an EMC Data Domain Boost (DDB) Repository

Adding an NFS Repository

The section below provides the information required to configure an NFS repository in vRanger.

NFS Requirements

- vRanger supports the NFS3 protocol, which does not provide for authentication. vRanger will use the NFSNobody account to connect to the repository.
- The NFSNobody account must have R,W, X permissions for the target directory.
- Your */etc/exports* file must contain the export directory and a list of the IPs that will connect to the repository. You may list each individually (the vRanger machine and any ESX hosts using direct-to-target) or use a wildcard *. The export directory should be shared with read/write asynchronous access. For an export directory of */backups*, this would look like:

```
[root@NFSServer etc]# cat exports
/backups        *(rw,async)
```

To add an NFS Repository:

1. To add an NFS repository, navigate to the My Repositories pane. Right-click anywhere in the My Repositories pane. Select **Add--> NFS.**
1. On the **Add Network File Share Repository** dialog, populate the fields below:
   a. **Repository Name** - a descriptive name for the repository.
   b. **Description** - a long form description for the repository. This is an optional field.
   c. **DNS Name or IP** - the IP or FQDN for the repository
   d. **Export Directory** - specify the Export directory, which is similar in concept to a network share. You will need to create a target sub-directory in the export directory.
   e. **Target Directory** - this is a sub-directory of the NFS Export directory. This is the location to which savepoints will be written.
2. Select **Encrypt all backups to this repository** if you wish these backups to be password-protected.
3. Enter a Password for the encrypted repository -- confirm the password by re-entering it.

   Caution If you wish to use the **Encrypt all backups** feature**, make certain to retain** the password you enter in the following steps. There is no back-door or admin-level password. If the password is unknown, the backups will not be usable.
4. Click **OK** -- the connection to the repository is tested and the repository is added to the My Repositories pane and the Repository Information dialog.
5. vRanger will check the configured repository location for existing manifest data to identify existing savepoints. If any are found, you will be prompted to take one of three actions:
   - Import as Read-Only - with this option, all savepoint data will be imported into the vRanger database, but only for restores. You will not be able to backup to this repository.
   - Import -all savepoint data will be imported into the vRanger database. vRanger will be able to use the repository for backups and restores. vRanger requires read and write access to the directory.

- Overwrite - the savepoint data will be retained on the disk, but will not be imported into vRanger. vRanger will ignore the existence of the existing savepoint data and treat the repository as new.

Adding an FTP Repository

The process for adding an FTP repository is described below.

To add an FTP Repository:

1. To add an FTP repository, navigate to the My Repositories pane. Right-click anywhere in the My Repositories pane. Select **Add--> FTP.**
2. On the **Add FTP Repository** dialog, populate the fields below:
   a. **Repository Name** - a descriptive name for the repository.
   b. **Description** - a long form description for the repository. This is an optional field.
   c. **DNS Name or IP** - the IP or FQDN for the repository
   d. **Target Directory** - this is the directory on the FTP server to which the repository will be written.
   e. **User name** - the user name for the account that vRanger will use to connect to the repository.
   f. **Password** - the password for the user account above.
   g. **Port** - the port that vRanger will use to connect to the FTP server.The default FTP port is 21
   h. **Timeout** - this value determines how long to wait before terminating an idle connection. The default value is 600 seconds
3. Select **Encrypt all backups to this repository** if you wish these backups to be password-protected.
4. Enter a Password for the encrypted repository -- confirm the password by re-entering it.

   Caution If you wish to use the **Encrypt all backups** feature**, make certain to retain** the password you enter in the following steps. There is no back-door or admin-level password. If the password is unknown, the backups will not be usable.
5. Click **OK** -- the connection to the repository is tested and the repository is added to the My Repositories pane and the Repository Information dialog.
6. vRanger will check the configured repository location for existing manifest data to identify existing savepoints. If any are found, you will be prompted to take one of three actions:
   - Import as Read-Only - with this option, all savepoint data will be imported into the vRanger database, but only for restores. You will not be able to backup to this repository.
   - Import -all savepoint data will be imported into the vRanger database. vRanger will be able to use the repository for backups and restores. vRanger requires read and write access to the directory.

- Overwrite - the savepoint data will be retained on the disk, but will not be imported into vRanger. vRanger will ignore the existence of the existing savepoint data and treat the repository as new.

Adding an SFTP Repository

The process for adding an SFTP repository is described below.

To add an SFTP Repository:

1 To add an SFTP repository, navigate to the My Repositories pane. Right-click anywhere in the My Repositories pane. Select **Add--> SFTP.**

1 On the **Add SFTP Repository** dialog, populate the fields below:

a **Repository Name** - a descriptive name for the repository.

b **Description** - a long form description for the repository. This is an optional field.

c **DNS Name or IP** - the IP or FQDN for the repository

d **Target Directory** - this is the directory on the SFTP server to which the repository will be written.

e **User name** - the user name for the account that vRanger will use to connect to the repository.

f **Password** - the password for the user account above.

g **Port** - the port that vRanger will use to connect to the SFTP server.The default SFTP port is 22.

h **Timeout** - this value determines how long to wait before terminating an idle connection.

2 Select **Encrypt all backups to this repository** if you wish these backups to be password-protected.

3 Enter a Password for the encrypted repository -- confirm the password by re-entering it.

Caution If you wish to use the **Encrypt all backups** feature**, make certain to retain** the password you enter in the following steps. There is no back-door or admin-level password. If the password is unknown, the backups will not be usable.

4 Click **OK** -- the connection to the repository is tested and the repository is added to the My Repositories pane and the Repository Information dialog.

5 vRanger will check the configured repository location for existing manifest data to identify existing savepoints. If any are found, you will be prompted to take one of three actions:

- Import as Read-Only - with this option, all savepoint data will be imported into the vRanger database, but only for restores. You will not be able to backup to this repository.
- Import -all savepoint data will be imported into the vRanger database. vRanger will be able to use the repository for backups and restores. vRanger requires read and write access to the directory.
- Overwrite - the savepoint data will be retained on the disk, but will not be imported into vRanger. vRanger will ignore the existence of the existing savepoint data and treat the repository as new.

Adding an NVSD Repository

The process for adding a NetVault SmartDisk (NVSD) repository is described below.

To add an NVSD Repository:

1 To add an NVSD repository, navigate to the My Repositories pane. Right-click anywhere in the My Repositories pane. Select **Add--> NVSD.**

1 On the **Add NVSD Repository** dialog, populate the fields below:

a **Repository Name** - a descriptive name for the repository.

b **Description** - a long form description for the repository. This is an optional field.

c **DNS Name or IP** - the IP or FQDN for the NVSD server.

d **User name/Password** - the credentials for the account that vRanger will use to connect to the repository.

Note If you have enabled WebDav authentication on your NVSD server, then use those credentials here. If you have not enabled WebDav authentication, then no credentials are required. See the *Quest NetVault SmartDisk Administrators Guide* for more information.

e **Target Directory** - this is the directory on the NVSD server to which the repository will be written. You may select an existing NVSD repository (if one exists) from the drop-down, or enter a name for your repository to have it created.

f **Port** - the port that vRanger will use to connect to the NVSD server.The default port is 37453.

g **Timeout** - this value determines how long to wait before terminating an idle connection.

Note Note that encryption is not supported for NVSD repositories.

2 Click **Ok**.

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.

4 vRanger will check the configured repository location for existing manifest data to identify existing savepoints. If any are found, you will be prompted to take one of three actions:

- Import as Read-Only - with this option, all savepoint data will be imported into the vRanger database, but only for restores. You will not be able to backup to this repository.
- Import -all savepoint data will be imported into the vRanger database. vRanger will be able to use the repository for backups and restores. vRanger requires read and write access to the directory.
- Overwrite - the savepoint data will be retained on the disk, but will not be imported into vRanger. vRanger will ignore the existence of the existing savepoint data and treat the repository as new.

Adding an EMC Data Domain Boost (DDB) Repository

The process for adding an EMC Data Domain Boost repository is described below. This procedure assumes the following:

- That you have a properly configured Data Domain appliance that is accessible to the vRanger machine.
- That DD Boost is licensed and enabled on the Data Domain device.
- That you have designated a DD Boost User account.

Note Please consult the Data Domain documentation for information on performing the configurations listed above.

To add an EMC Data Domain Boost Repository:

1. To add a DD Boost repository, navigate to the My Repositories pane. Right-click anywhere in the My Repositories pane. Select **Add--> EMC Data Domain Boost (DDB).**
2. On the **Add EMC Data Domain Boost Repository** dialog, populate the fields below:
   a. **Repository Name** - a descriptive name for the repository.
   b. **Description** - a long form description for the repository. This is an optional field.
   c. **DNS Name or IP** - the IP or FQDN for the Data Domain device.
   d. **User name/Password** - these are the credentials for the account selected as the **DD Boost User** on the Data Domain device.

      Note Please consult the Data Domain documentation for more information on setting a DD Boost user name.
3. **Storage Unit -** this is the Storage Unit configured on the Data Domain device. Select one from the drop-down menu, or enter the name for a new Storage Unit and vRanger will create one for you.Click **OK** -- the connection to the repository is tested and the repository is added to the My Repositories pane and the Repository Information dialog.

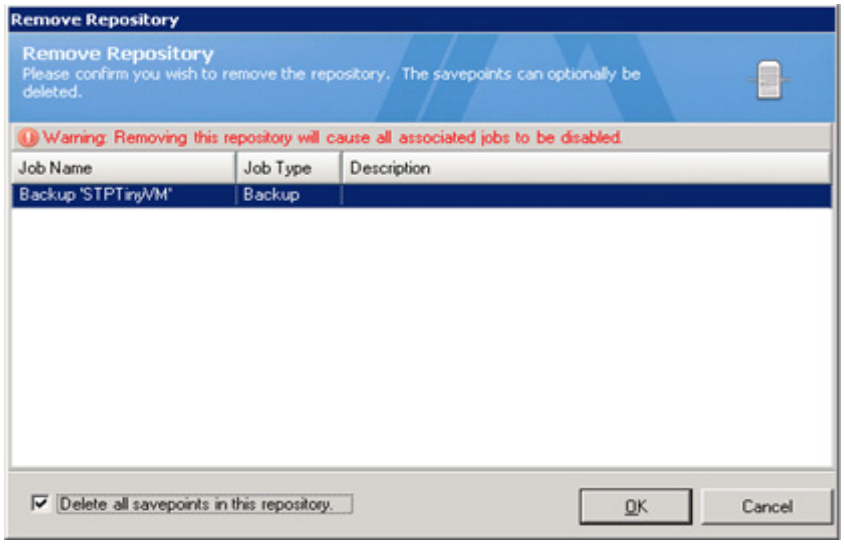
   Note For Data Domain devices running DD OS 5.0, the only characters allowed in storage unit names are alphanumeric characters, “-”, and “_”. For devices running DD OS 5.1, the supported characters are alphanumeric characters and ~!@#$^_+`-={}[],.
4. vRanger will check the configured repository location for existing manifest data to identify existing savepoints. If any are found, you will be prompted to take one of three actions:
   - **Import as Read-Only** - with this option, all savepoint data will be imported into the vRanger database, but only for restores. You will not be able to backup to this repository.
   - **Import** -all savepoint data will be imported into the vRanger database. vRanger will be able to use the repository for backups and restores. vRanger requires read and write access to the directory.
   - **Overwrite** - the savepoint data will be retained on the disk, but will not be imported into vRanger. vRanger will ignore the existence of the existing savepoint data and treat the repository as new.

Removing an EMC Data Domain Boost (DDB) Repository

The process for removing a Data Domain Boost repository is the same as removing any other repository type, except that you also have the option of removing the storage unit used by the repository. There is a hard limit on the number storage units that can be configured on a Data Domain device, which makes removing unused storage units an important maintenance effort.

To remove a DD Boost repository:

1. From the My Repositories view, right-click on the Data Domain Boost repository and select **Remove**.
2. The **Remove Repository** dialogue appears, showing the savepoints in the selected repository.

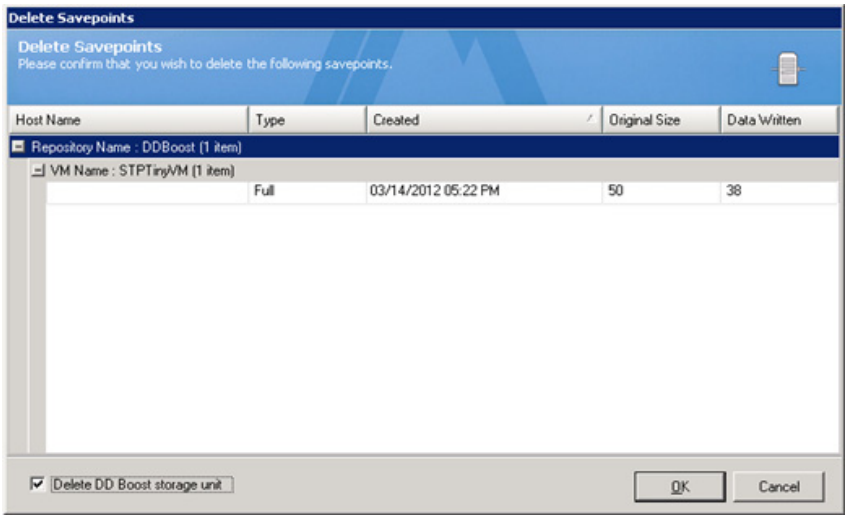


When removing a repository, you have the option of keeping the savepoints on disk or deleting them. In order to remove the storage unit associated with the repository, you will need to remove the savepoints.

3. Select **Delete all savepoints in this repository**. Click **OK**

Caution This will delete the savepoints from the repository disk, not just the vRanger database. Exercise caution when deleting savepoints.

4. The **Delete Savepoints** dialogue appears.



Select **Delete DD Boost storage unit**, and click **OK**. The savepoints will be deleted, along wit the storage unit associated with the repository.

Configuring the Virtual Appliance

This chapter outlines the process of deploying and configuring the vRanger Virtual Appliance.

This chapter contains the following sections:

The vRanger Virtual Appliance 82
Deploying the Virtual Appliance 85
Adding the Virtual Appliance to vRanger 94
Changing Virtual Appliance Configuration 96

The vRanger Virtual Appliance

vRanger uses a virtual appliance for replication to and from ESXi hosts, for file-level recovery (FLR) from Linux machines, and optionally for backups and restores. You may also use the VA on ESX hosts as well to avoid taxing the Service Console resources, which are limited.

Virtual Appliance Overview

The vRanger virtual appliance is a lightweight virtual machine that serves as an operating environment for the components that would normally run in the Service Console. Removing the workload from the Service Console is clearly necessary for ESXi and vSphere 5, but it is advantageous for ESX servers as well. While the Service Console is restricted to a single CPU (CPU 0), with virtual appliances the workload can be spread across the other CPUs available to a host. This provides increased reliability and scalability over operations limited to the Service Console.

The virtual appliance must be deployed to any ESXi host that you will configure for replication (either as a source or a destination). For hosts in a cluster, you may deploy just one VA to the cluster; the VA will be shared among the cluster's other hosts. When deploying a VA to a cluster, you must chose a host in the cluster to which the VA will be associated.

In addition, replication via virtual appliance requires that if a VA is used on one host or cluster in a replication job, then a VA must be used on both the source and destination host or cluster. In other words, virtual appliances, when used for replication, must be used in pairs.

When configuring the virtual appliance, special consideration should be given to the amount of resources (CPU and RAM) allocated to the VA as the number of simultaneous tasks the VA will be able to process is directly tied to available resources. In addition, if you will be performing replication tasks using a virtual appliance, carefully consider an appropriate size for the VA scratch disk. See the section below for more information on scratch disk usage.

The Virtual Appliance Scratch Disk

If you will be performing replication tasks with your virtual appliance, you will need to add a second "scratch" disk to the VA. This scratch disk is used to store two types of files:

- *vzmap* files - block maps (in the form of a *vzmap* file) for the VMs replicated to the destination host. This is block map information, and not actual data blocks. These maps are compared to the source VM during each replication pass to identify the data blocks that have changed since the last replication. The *vzmap* files make differential replication significantly faster as they remove the need to scan the destination VM blocks for comparison with the source VM.
- *vzUndo* files - As data is sent to the destination host (via the VA), blocks in the destination disk are written to the undo file before they are overwritten by the changed data. If replication fails and an undo becomes necessary, then the original destination disk blocks are read from the undo file and written to the destination disk to rollback the failed replication. This is a key function designed to provide resiliency in the face of a network failure; if there

is a network failure during the replication pass, the destination VM is not corrupted by incomplete data.

Once the pass is complete, and all data has been received by the destination VA, the undo file is deleted. At that point, the storage space used by the undo file is returned to the VA for use. Note that undo files are not created during the first pass of a replication job. During the first pass, the entire VM is sent to the destination host, but there is no existing data on the destination VMDKs, and therefore no risk of corruption. Data is streamed directly to the VMDK. You do not need to allocate scratch disk space for this scenario.

While the vzmap files are trivial in size (in the order of a few MBs), the undo file can potentially be as large as the VM itself. While the scratch disk needs to be configured to a size sufficient to handle the data of concurrent replication tasks, making it too large wastes valuable storage space. Use the sections below to guide you in determining the proper size for the scratch disk.

Strategies for Sizing the Scratch Disk

The scratch disk needs to be large enough only to hold the permanent *vzmap* files and the temporary *vzUndo* files, plus a small margin for safety. How large that is depends almost entirely on the amount of changed data you are replicating. The amount of changed data is itself a function of the number of VMs you'll be replicating, their total disk size, replication frequency, and the data change rate per VM. It is important to understand all of this data when sizing the scratch disk.

If you are using one VA for a cluster, remember that you must account for all simultaneous replications for the cluster.

Use Historical Data

If you have previously replicated the source VMs, the most accurate method to properly size the scratch disk (without wasting storage space) is to use historical replication data available in the Replicate Task Reports (in the vRanger My Reports view) for the VMs in question. This report will show the amount of data written during each replication task.

The safest method to size your scratch disk based on historical data is to record the highest amount of data written for each VM that you will replicate at once, and size the disk to accommodate those values.

To avoid filling your scratch disk, Quest Software recommends that you add a small margin (10% or so) to the calculated scratch disk size for safety.

Calculating

If you do not have information on the amount of changed data for each VM, you can estimate the appropriate size of the scratch disk based on the VM size and the number of VMs you will be replicating at once.

A general rule for sizing the scratch disk is to choose a percentage of the total VM size to represent the practical limit of changed data for a given replication pass. Only you can decide what is appropriate for your environment. The numbers below are examples given to illustrate the concept:

Assume that you will have four virtual machines that you wish to replicate to a host or cluster at the same time. These VMs are described in the table below.

VM	V M Size	Change Rate	Change Size
1	100 GB	15%	15 GB
2	100 GB	10%	10 GB
3	100 GB	20%	20 GB
4	60 GB	5%	3 GB

For the VMs above, we would need approximately 48 GB of disk space for the undo files, plus a buffer of approximately 10% (for safety's sake). In our example, an appropriate estimate for the scratch disk size for the VMs above would be approximately 55 GB.

Bear in mind that the estimate exercise should be done for every set of VMs that will be replicated to that host or cluster, with the scratch disk being sized to accommodate the largest value obtained.

Caution If the scratch disk runs out of space, replication tasks will fail with the error "*FATAL cant_write can't write vix".*

Options for a Smaller Scratch Disk

As previously stated, the primary driver for the scratch disk size is the amount of changed data that needs to be replicated. If you need to reduce the storage requirements for your scratch disk, you can:

- reduce the amount of time that passes between replication intervals. More frequent replication passes will contain smaller amounts of changed data.
- reduce the number of VMs that you replicate simultaneously. This will send less data through the scratch disk at any one time, allowing it to be smaller. Remember that the *vzundo* files are deleted after the replication pass completes.
- when provisioning the scratch disk, select the Thin Provisioning option. Thin provisioning helps prevent wasted storage space by not allocating blocks until they are written by the VM.

The Scratch Disk on the Source Host

As the scratch disk is used primarily for staging changes before they are written to disk – activity which occurs on the destination host or cluster– the scratch disk on the source side can be kept fairly small. However, in the event that you need to fail over to the D/R site, the replication job will reverse direction and start replicating changes back to the product site (the original source host or cluster). In order for this to occur, the scratch disk on the source side will need to be re-sized to accommodate the changed data.

Scratch Disk Location

When creating the second disk, make sure you place the disk on a datastore with block sizes large enough to support the expected VMDK. The list below shows the maximum file size available for each block size:

- 1 MB block size – 256 GB maximum file size
- 2 MB block size – 512 GB maximum file size
- 4 MB block size – 1024 GB maximum file size
- 8 MB block size – 2048 GB maximum file size

Note This limitation does not apply to VMFS 5.

Deploying the Virtual Appliance

vRanger uses a virtual appliance for both Linux file-level recovery and for replication to and from VMware ESXi servers. The vRanger virtual appliance is available via the Quest website: http://www.quest.com/landing/?id=5414.

Also available on this landing page are:

- A demonstration video describing the VA configuration process
- A short form of the VA Installation Instructions
- Virtual Appliances for older versions of vRanger

Deploying Multiple Virtual Appliances

The vRanger virtual appliance is required when replicating to or from an ESXi server. In addition, replication via virtual appliance requires that if a VA is used on one host in a replication job, then a VA must be used on both hosts. For example, if you are replicating between an ESXi host and an ESX host, you must have a VA deployed on the ESX host as well.

To streamline the deployment process, Quest recommends that you deploy and configure the virtual appliance once, then save it as a template to be used for additional deployments. The Configuring the Virtual Appliance procedures include an optional step for creating a template from the configured VA.

From this template, you have two options to deploy additional VA instances; a manual process using the VI Client, or a scripted process using PowerCLI. Regardless of which process you choose, if you wish to use a static IP address for the virtual appliances, you will need to configure that manually. Instructions for template deployment and network configuration can be found in the sections below:

- Deploying Multiple VAs From a Template - VI Client

- Deploying Multiple VAs From a Template - PowerCLI

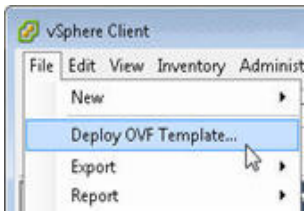
Note The procedures below were capture using VMware vCenter 4.1, update 1. The procedures may differ slightly for previous versions of vCenter. Consult your VMware documentation for the correct procedure for deploying a virtual appliance for your version of vCenter.

To deploy the virtual appliance:

1. Obtain the OVA file for the vRanger virtual appliance. For vRanger 5.4.1, the correct OVA version is 1.6.0.

   Note For the 5.4.1 release of vRanger, this file will be provided directly to customers. Please refer to the *vRanger 5.4.1 Release Notes* for more information.

2. In your vSphere VI Client, click **File**, then **Deploy OVF Template**.



3. In the **Deploy from a file or URL** field, enter the path to the downloaded OVA file. Click **Next**.
4. Continue through the import process, selecting the appropriate host and datastore configuration.

   The OVA import process may take several minutes. When complete, continue to the configuration section below.

Configuring the Virtual Appliance

Before using the virtual appliance, some changes must be made to the default configuration.

Step 1: Change the Default Password

1. From your VI Client, find the VA and power it on.
2. Using the console, login as `root` to the virtual appliance, using the default credentials below:
   - username: root
   - password: vzroot1
3. At the prompt, enter `passwd`. Enter and re-type a new password for the `root` account.

   Caution This is an important security step. Please ensure that you change the default password for the root account.

Step 2: Install VMware Tools

1 From the VI Client, right-click on the virtual appliance. Click **Guest**, then **Install/Upgrade VMware Tools**.

Note This must be done within 5 minutes of powering on or rebooting the virtual appliance. The virtual appliance will automatically install the VMware Tools.



Note No input is necessary for the VMware Tools installation - all prompts will be answered by the installer script.

Step 3: Changing the Hostname

1 Login to the virtual appliance.

2 Using the VI text editor, edit the network configuration file:

```
vi /etc/sysconfig/network
```

Note See Appendix: Using the VI Editor for more information on using the VI editor.

3 Change the hostname to the new value. Save the file.

Step 4: Changing the Network Configuration [Optional]

The virtual appliance is configured by default to use DHCP. You may choose to re-configure network settings to change the hostname, or to use a static IP address.

Note If you will continue using DHCP. Please note that an expired lease or changed address may result in vRanger losing connection with the virtual appliance. MAC Address reservations may be an option utilized for this scenario. If the IP of the virtual appliance changes, you will need to perform an inventory refresh in the vRanger My Inventory view before vRanger can use the virtual appliance(s).

1 Login to the virtual appliance.

2 Using the VI text editor, create a configuration file for eth0:

```
vi /etc/sysconfig/network-devices/ifconfig.eth0/ipv4
```

3 Enter the following text, substituting the appropriate IP address where indicated:

```
ONBOOT=yes
SERVICE=ipv4-static
IP=<static IP of VA>
GATEWAY=<IP of gateway>
PREFIX=<this is the subnet mask - your values may differ>
BROADCAST=<your broadcast IP- the highest IP in the VA's subnet.>
```

4 Save the file.

5 Move the DCHP configuration file to the root directory. This will disable DHCP.

```
mv -v /etc/sysconfig/network-devices/ifconfig.eth0/dhcpcd /root/
```

6 Restart the VM by typing `reboot` at the prompt.

Step 5: Configuring DNS [Optional]

It may be necessary, depending on your environment, to configure the virtual appliance with DNS nameserver information.

1 Login to the virtual appliance.

2 Using the VI text editor, edit the *resolv.conf* file:

```
vi /etc/resolv.conf
```

3 Enter the following text, substituting the appropriate values where indicated:

`search` *<domain1> <domain2> <domain3>*

`nameserver` *<IP address>*

`nameserver` *<IP address>*

4 Save the file.

5 Restart the VM by typing `reboot` at the prompt.

Step 6: Adding Second "Scratch" Disk

The vRanger virtual appliance uses a scratch disk to stage replicated data to an "undo" file, ensuring that the complete transmission is received before writing to the destination VM. In the event of a network (or other) failure, this prevents the replica VM from becoming corrupted.

See Strategies for Sizing the Scratch Disk for guidance on how to select the best size for the scratch disk.

To add the scratch disk:

1 From the VI Client, right-click on the virtual appliance, and select **Edit Settings**.

2 On the Hardware tab, click **Add**.

3 Select **Hard Disk**. Click **Next.**

4 Select **Create a new virtual disk**.

Configure the size for the disk and select your provisioning method. If storage space is a concern, consider selecting the Thin Provision option. This ensures that only the amount of space required is allocated. For more information on thin provisioning, see the VMware KB article *Using thin provisioned disks with virtual machines*. Click **Next**.

5 Leave the **Virtual Device Node** setting as **SCSI**. Click **Next**.

6 Click **Finish**. Click **Ok**.

Caution Do not reboot the virtual appliance. Rebooting the virtual appliance at this point will prevent the VA Utility script from functioning properly.

Step 7: Load VA Utility script

The *vautil_01.02.01.tar.gz* needs to be manually transferred to the VA. This script prepares the scratch disk for replication.

1. Download the *vautil_01.02.01.tar.gz* files
2. Transfer the files to the VA. You may use scp from a Linux machine, or WinSCP from a Windows machine. An example command is shown below:

   ```
   scp vautil_01.02.01.tar.gz root@10.10.10.10:/root/bin/
   ```

3. Login to the VA and extract the utility scripts.

   ```
   tar zxvf vautil_01.02.01.tar.gz
   ```

4. Using the cd command, change the working directory into the extracted directory.

   ```
   cd /root/bin/vautil_01.02.01
   ```

5. Run the following command:

   ```
   /root/bin/vautil_01.02.01/scratch_scsi.sh -a
   ```

   The command, when successful, will display the following output:

   ```
   ADDED:  <device_added's_name> (Example:  ADDED:  sdb)
   ```

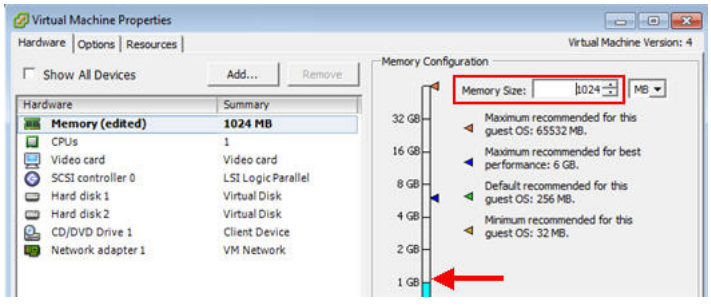
   Note Note that if you added more than one new disk, you will see more than one device name added. (Example: ADDED: sdb sdc)

Step 7: Resource Configuration

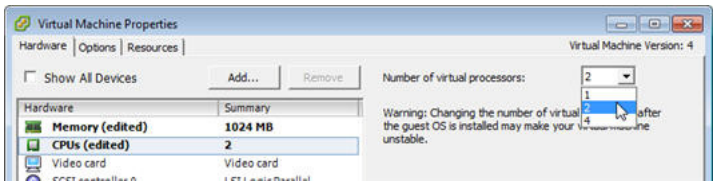
The VA is configured by default with 1 vCPU and 512 MB of RAM. This is sufficient to allow 2 concurrent tasks per VA. If you will need to run more than 2 tasks concurrently, increase the resources allocated to the VA.

Note If you observe consistent high CPU and Memory utilization on the virtual appliance, consider adding more resources ensure uninterrupted performance.

1. From the VI Client, right-click the virtual appliance and select **Edit Settings**.
2. In the Virtual Machine Properties dialog, select **Memory**. Move the slider, or use the up arrow in the **Memory Size** field to adjust the allocated memory.



3. In the Virtual Machine Properties dialog, select **CPU.** Select the desired number of vCPUs from the drop-down.



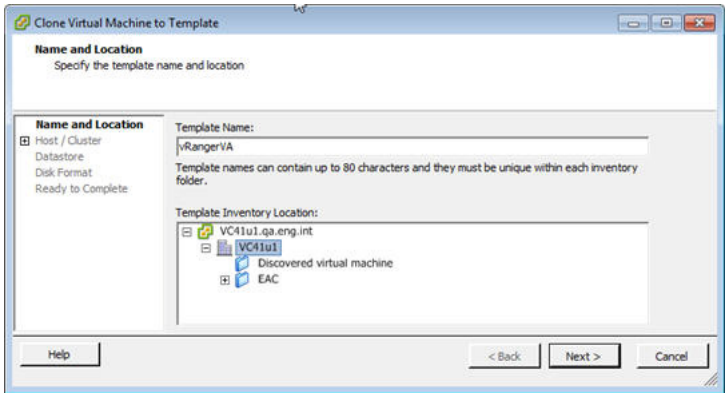
4 Click **Ok** to save the configuration changes.

Step 9: Creating a Template (Optional)

If you need to deploy the vRanger virtual appliance to multiple hosts, it may be helpful to create a virtual machine template from the configured virtual appliance.

1 From the VI Client, right-click the configured virtual appliance and select **Template>Clone to Template**.

2 Enter the template name and select a location. Click **Next**.



3 Select the host or cluster on which the template is to be stored. Click **Next**.

4 Select the datastore in which the template is to be stored. Click **Next**.

5 On the Disk Format dialog, select **Same format as source**. Click **Next**.

6 Review the configurations and click **Finish**.

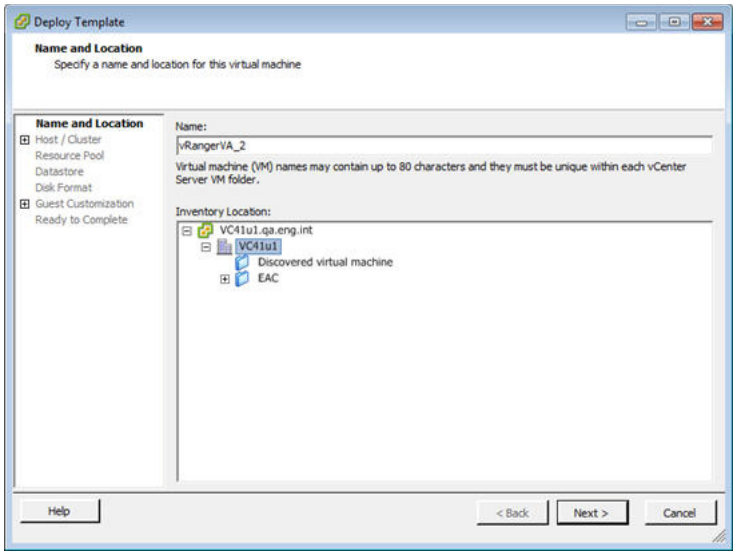
Deploying Multiple VAs From a Template - VI Client

Unless you have only one ESXi host, you will need to deploy multiple instances of the vRanger virtual appliance. You may deploy additional instances either by using the VI client (as documented below), or via a PowerCLI script as documented in Deploying Multiple VAs From a Template - PowerCLI

Note If you wish to use a static IP address, or need to configure DNS information, that must be done manually for each deployed instance - see Configuring the Virtual Appliance for instructions.

To deploy an instance of the vRanger virtual appliance from the template created in Step 7: Resource Configuration, follow the procedures below.

1. In the VI Client, find the template you created previously. To view templates, click **View>Inventory>VMs and Templates**.
2. Right-click on the template, and select **Deploy Virtual Machine from this Template**.
3. In the **Name and Location** dialog, enter a name for the VA, and select the appropriate inventory location. Click **Next**.



4. In the **Host/Cluster** dialog, select the host on which the VA is to be run. Click Next.

   Note You will need to deploy an instance of the vRanger VA to every ESXi host used as a replication source or destination.

5. Select the datastore in which the VA files will be stored. Click **Next**.
6. In the **Disk Format** dialog, select **Same format as source**. Click **Next.**
7. In the **Guest Customization** dialog, select **Do not customize**. Click **Next**.
8. Review the selections. Click **Finish**.
9. Repeat steps 1-8 as needed for other hosts as needed.

Note After the virtual appliances have been deployed, refer to "Configuring the Virtual Appliance" on page 86 for instructions on how to configure IP and DNS information.

Deploying Multiple VAs From a Template - PowerCLI

Using vSphere PowerCLI and a pre-configured CSV file, you can automate the deployment of the vRanger virtual appliance to multiple hosts. This method requires the initial deployment using DHCP, although you can change the networking options for the virtual appliance after deployment using the instructions in Configuring the Virtual Appliance.

The high level steps required for this process are:

- Using the VI Client, create a Customization Specification

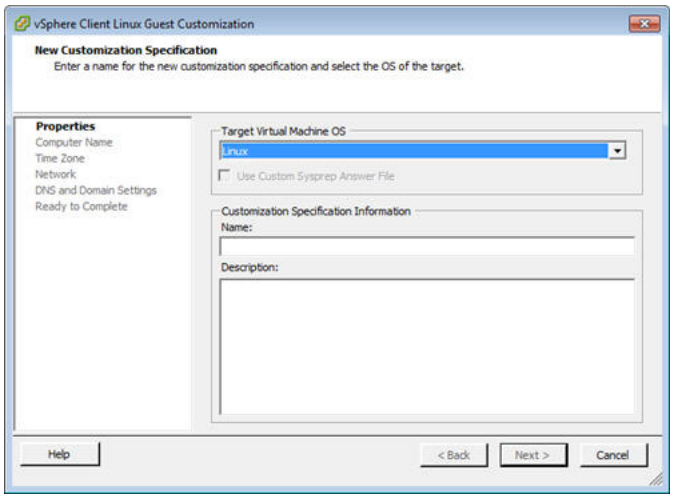
- Populate a CSV with VM, Host, and Datastore information
- Execute the PowerCLI Script

Step 1: Customization Specification

The Customization Specification provides basic configuration information used in creating the VMs.

1 From the VI Client, click V**iew>Management>Customization Specifications Manager**. Click **New**.

The **New Customization Specification Wizard** appears:



2 In the **Target Virtual Machine OS** field, select Linux. Enter a name for the customization specification. Click **Next**.

Note You will need the customization specification name for the deployment script. In the sample script below, the name *vRangerVA* is used.

3 On the Computer Name dialog, select **Use the virtual machine name**. Enter a domain name for the VM. Click **Next**.

Note The VM name will be configured from the CSV file.

4 Select an **Area** and **Location** for the VA's time zone. Click **Next**.

5 On the **Network** dialog, select **Typical Settings**. Click **Next**.

6 Enter a **Primary DNS** server and **DNS Search Path**. Click Next.

Note Due to compatibility issues between the VA OS and VMware Tools, this information will **not** be populated to the deployed VA. The wizard requires at least one DNS server entered before you can continue.

7 Review your configurations and click **Finish**.

Step 2: Populating a CSV

The information required for deploying additional virtual appliances will come from a CSV file imported by the PowerCLI script.

1 Create a CSV file with the headings below:

- VM
- Datastore
- VMhost
- Template

Note It is easiest to create a CSV file in a spreadsheet program such as Microsoft Excel. Once you save the file as a CSV however, only open the file using Notepad.

2 Populate the rows below the headers with the appropriate information:

- VM - this is the name of the VA that will be deployed
- Datastore - the datastore to which the VA will be deployed
- Host - the Host on which the VA will run.
- Template - the name of the template created in Step 7: Resource Configuration.

3 Save the file as a CSV. For best results, open the file using Notepad (or similar) to verify formatting. In the sample script below, this file is named *VADeploy.csv*

Step 3: Executing the PowerCLI Script

The commands below are entered using vSphere PowerCLI.

1 Enter the command below to connect PowerCLI to your vCenter. Substitute the correct values for your environment.

```
Connect-VIServer <vCenter> -User <username>-Password <password>
```

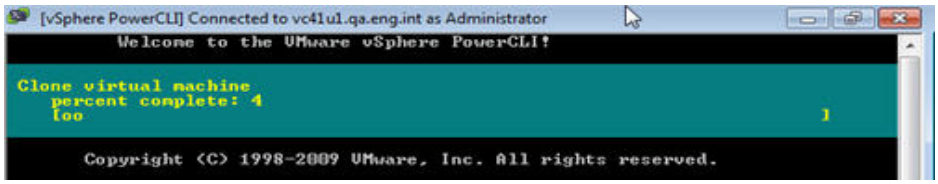
2 Enter the following commands to deploy your virtual appliances:

```
Import-Csv VADeploy.csv | %{
Get-OSCustomizationSpec vRangerVA | Get-OSCustomizationNicMapping | Set-
OSCustomizationNicMapping -IpMode UseDHCP
New-VM -Vmhost $_.VMhost -name $_.VM -Template $_.Template -Datastore
$_.Datastore -OSCustomizationSpec vRangerVA
}
```

The example above uses information that will vary based on your environment, as highlighted in red and italics.

- VADeploy.csv - the name of your CSV file.
- vRangerVA - the name of your Customization Specification.

A status bar indicates deployment progress:



Disabling DRS for the vRanger Appliance

If the vRanger appliance is configured on hosts that are part of a DRS enabled cluster, the VA(s) may be migrated to a different host due to DRS/HA activity. This will cause replication failures as the virtual appliance is no longer in the expected location (as configured in vRanger). To prevent this disruption, it is important to disable DRS for the vRanger virtual appliances.

1. In your VI client, find the cluster(s) containing the vRanger virtual appliances.
2. Right-click on the cluster, and select **Edit Settings**.
3. In the Cluster Settings dialog, select **Virtual Machine Options.**
4. Search for or find the vRanger virtual appliances. Right-click on each virtual appliance, and select **manual**.
5. Click **Ok**.

Adding the Virtual Appliance to vRanger

Once the virtual appliance(s) are configured, you will need to add them to the vRanger Virtual Appliances inventory.

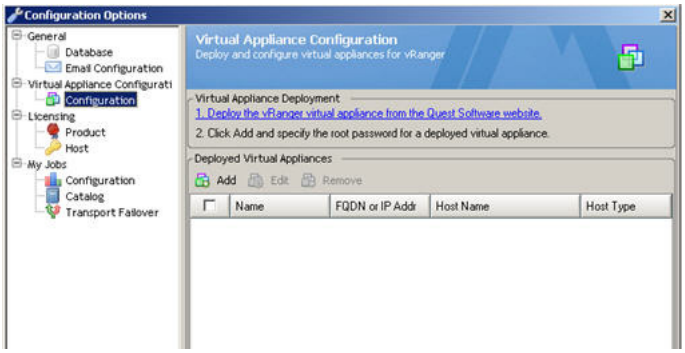
You may add one or more virtual appliances to vRanger during the **Startup Wizard** displayed when vRanger is first launched.

You may also launch the **Startup Wizard** at any point from the Tools menu, or use the **Tools>Options** to launch the **Configuration Options** dialog.

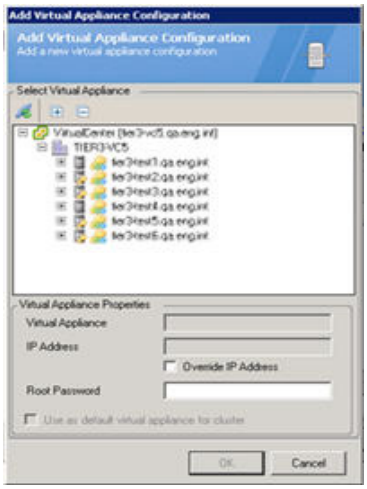
To add a virtual appliance to vRanger:

1. From the vRanger UI, select the **My Inventory** view, and click the refresh icon  to refresh the inventory.

1. From the **Configuration Options** dialog, select **Virtual Appliances**.



2. Click **Add**. The **Add virtual appliance configuration** dialog appears, showing the vCenter inventory tree.



3 Browse the inventory tree, and select the desired virtual appliance.

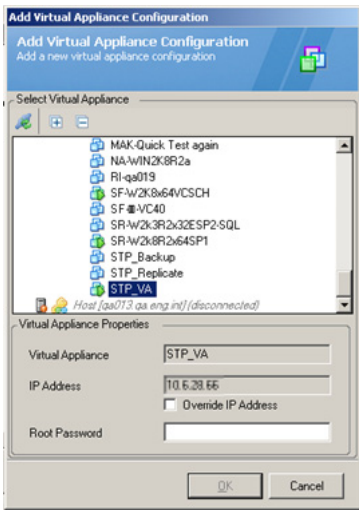
4 By default, vRanger will connect to the vRanger virtual appliance using the first IP address reported by the vSphere API. This IP will be displayed in the IP Address field. If you have only one NIC configured on the virtual appliance, continue to the next step.

or

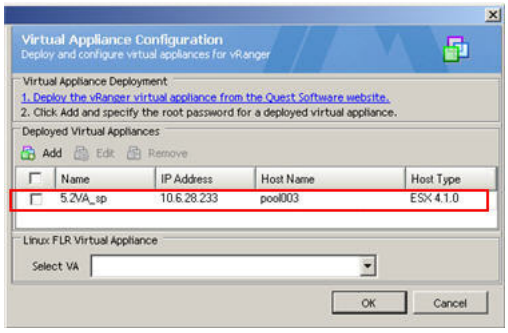
If you have more than one NIC configured on the virtual appliance, you may not want vRanger to connect to the first NIC. Using the **Override IP Address** field, you can configure vRanger with the IP address for the NIC to which vRanger should connect.

For example, if you have two NICs configured on the virtual appliance, and want vRanger to connect to the second NIC, simply select **Override IP Address**. The **IP Address** field will become enabled. Enter the IP for the second NIC in the IP Address field.

5 Enter the root password for the virtual appliance, and click **OK**.



The virtual appliance will appear in the Deployed Virtual Appliances section:



6 In the Linux FLR Virtual Appliance section, select a deployed virtual appliance to use for Linux file-level recovery.

Changing Virtual Appliance Configuration

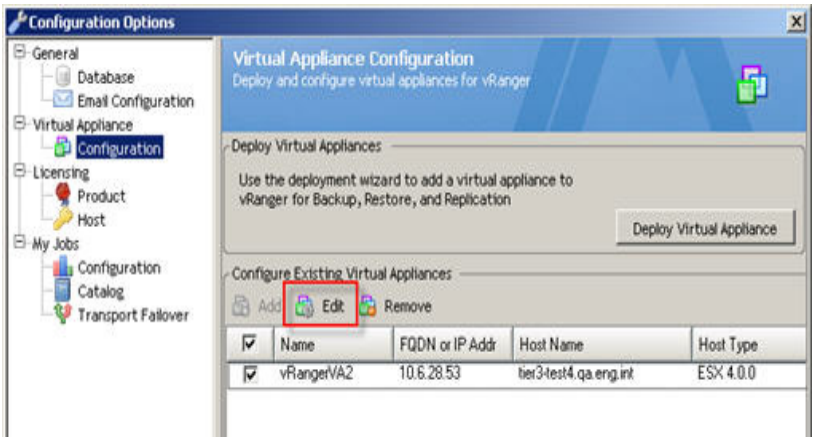
After a virtual appliance is deployed, you may change its configuration from the vRanger interface. If you need to add additional NICs or configure the VA with a static IP address, you will need to do that by logging into the virtual appliance.

Caution Reconfiguring the virtual appliance may cause it to be power cycled, possibly affecting configured jobs. You will be prompted with the jobs configured for the virtual appliance, please review these carefully to avoid service interruption.

1 From the My Inventory view, right-click on the virtual appliance you want to change, and click **Virtual Appliance Configuration**.

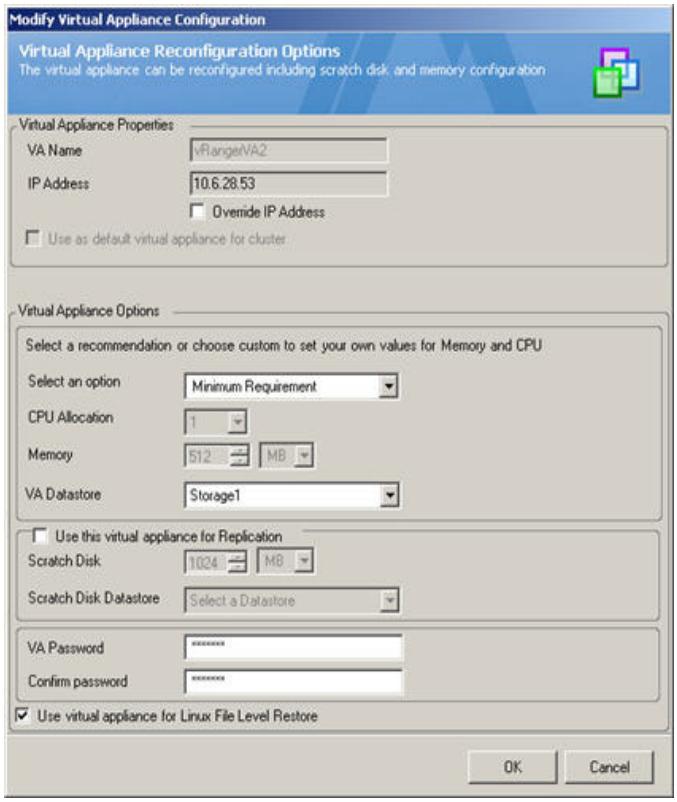
or

From the vRanger toolbar, click **Tools>Options**, then select **Virtual Appliance**. Select the virtual appliance to edit, and click **Edit**.



2 The **Modify Virtual Appliance** dialogue appears.

Click **Ok**.



1 In the Virtual Appliance Properties section, confirm the VA Name. Edit as required.

2 By default, vRanger will connect to the vRanger virtual appliance using the first IP address reported by the vSphere API. This IP will be displayed in the IP Address field. If you have only one NIC configured on the virtual appliance, continue to the next step.

   or

   If you have more than one NIC configured on the virtual appliance, you may not want vRanger to connect to the first NIC. Using the **Override IP Address** field, you can configure vRanger with the IP address for the NIC to which vRanger should connect.

   For example, if you have two NICs configured on the virtual appliance, and want vRanger to connect to the second NIC, simply select **Override IP Address**. The **IP Address** field will become enabled. Enter the IP for the second NIC in the IP Address field.

   Note See Disabling DRS for the vRanger Appliance for manual network configuration procedures.

3 In the **Virtual Appliance Option** section, change the resources allocated to the virtual appliance as needed. You may select one of two preconfigured options, or configure a custom setting.

   - **Minimum Requirement** - this setting allocates 1 CPU and 512 MB of RAM. This is usually sufficient for 2 concurrent tasks per VA.
   - **Quest Recommended** - this setting allocates 2 CPUs and 1 GB of RAM. This is sufficient for 4 concurrent tasks per VA.

- **Custom Setting** - select this value to configure the VA with higher resources for more concurrent tasks per VA.

4 To change the datastore for the VA's primary disk, select the new datastore in the **VA Datastore** field,.

5 **DO NOT** create or modify the VA Scratch Disk from this dialogue.

Caution Rebooting the VA will cause a reboot after the VA configuration change, which will prevent the VA Utility script from functioning properly.

See the following sections for more information:

- For information on creating the Scratch Disk, see Step 6: Adding Second "Scratch" Disk.
- For information on running the VA Utility script, see Step 7: Load VA Utility script.
- For information on resizing the scratch disk, see Increasing The VA Scratch Disk Size.

6 If desired, enter a new password for the virtual appliance.

7 If you wish to perform file-level recovery from backups of Linux virtual machines, you will need to configure a VA to use for Linux FLR. Select **Use virtual appliance for Linux File Level Restore**.

If you select this option for a different VM in the future, then that VM will be used for Linux FLR.

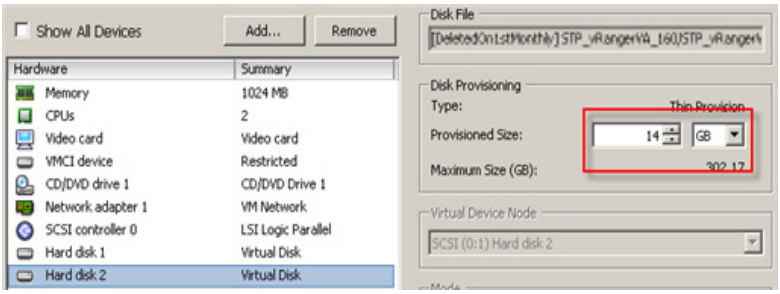
Increasing The VA Scratch Disk Size

If you increase the size of the scratch disk, you must re-run the VA utility script to take advantage of the new storage space.

To increase the VA scratch disk size:

1 In the VI Client, right-click the virtual appliance and select **Edit Settings**.

2 Select the scratch disk (usually Hard Disk 2), and configure the desired size.



3 Click OK and wait for the configuration change to take place.

Caution Do not reboot the virtual appliance

4 Login to the VA, or connect via a terminal application.

5 Using the cd command, change the working directory into the extracted directory.

```
cd /root/bin/vautil_01.02.01
```

6 Run the following command:

```
/root/bin/vautil_01.02.01/scratch_scsi.sh -g
```

The command, when successful, will display the following output:

```
RESIZED:  ${devX} ${devX_new_size_in_bytes}
```

7 Reboot the virtual appliance.

Disabling DRS for the vRanger Appliance

If the vRanger appliance is configured on hosts that are part of a DRS enabled cluster, the VA(s) may be migrated to a different host due to DRS/HA activity. This will cause replication failures as the virtual appliance is no longer in the expected location (as configured in vRanger). To prevent this disruption, it is important to disable DRS for the vRanger virtual appliances.

1 In your VI client, find the cluster(s) containing the vRanger virtual appliances.

2 Right-click on the cluster, and select **Edit Settings**.

3 In the Cluster Settings dialog, select **Virtual Machine Options.**

Search for or find the vRanger virtual appliances. Right-click on each virtual appliance, and select **manual**.

Appendix: Using the VI Editor

This information is a summary of VI functionality, intended to satisfy the basic needs of a user new to VI that just wants to edit the required files for the vRanger virtual appliance configuration. Much more information can be found freely on the internet by searching for “vi editor commands”.

Note	Linux commands and file names are case sensitive.

VI Editor Overview

VI is a modal text editor commonly used in Linux and Unix environments. VI operates in either *insert mode* (where keystrokes are entered as part of the document) or *command mode* (where keystrokes are interpreted as commands). The dual modes of VI allow users to perform both text editing and command operations without removing their hands from the keyboards home row. The VI editor starts in command mode.

Starting VI

When starting the VI editor, you may create a new file or open an existing file.

- The command `vi` without any file name will open a new file. You will need to name and save the file when editing is complete.
- The command `vi` followed by an existing file name will open that file for editing.

Changing Modes

Files are opened by the VI editor in command mode, which means that input from the keyboard will be treated as VI commands rather than text. Before editing the file, you must change the VI editor to insert mode. The most commands to get into insert mode are listed below. You may also use any of the insertion commands listed in “Inserting Text” on page 102.

Command	Description

a	enter insert mode; the characters typed will be inserted after the current cursor position.
Esc	switches back to command mode

Editing Commands

The sections below contain basic information about navigating the file and editing the text within.

Moving the Cursor

Moving the cursor around a file using the VI editor can be a challenge to those not familiar with the commands. Use the commands below as a quick reference.

Command	Description
h	moves the cursor one space to the left
j	moves the cursor one line down
k	moves the cursor one line up
l	moves the cursor one space to the right
$	moves the cursor to the end of the current line
^	moves the cursor to the beginning of the current line
Enter	moves the cursor to the beginning of the first word on the next line
G	moves the cursor to the end of the file
:*n*	moves the cursor to line *n*
w	moves the cursor to the beginning of the next word
e	moves the cursor to the end of the next word
b	moves the cursor to the beginning of the previous word

Inserting Text

Use the commands below to insert text into the open file.

Command	Description
a	append text starting right of cursor
A	append at the end of the current line
i	insert text starting left of cursor
I	insert text at beginning of the current line
o	open line below cursor, then enter insert mode
O	open line above cursor, then enter insert mode

Deleting Text

Use the commands below to delete text from the file.

Command	Description
x	delete single character
dw	delete word
dd	delete line
s	delete character, remain in insert mode
cw	delete word, remain in insert mode
cc	delete line, remain in insert mode
u	undo last change
U	undo all changes to current line

Saving Your Changes

VI will not automatically save your changes. To save your changes, or leave the file without saving changes, use the appropriate command below:

Command	Description

:w	writes the changes to disk
:zz	writes the changes to disk and quits VI
:q!	quits without saving changes.

Index

A

About
vRanger 7

C

cataloging
filtering 73
installing the catalog manager 47
configuration
options 71
with Startup Wizard 52
without Startup Wizard 62
credentials
host 56
vCenter 54

D

database 17
sizing the catalog database 18

E

ESXi
root 56

I

installation
catalog manager 47
database 17
in a vm 12
on new SQL Express 35
on SQL server 41
options 11

L

license changes 27
licensing
changes in vRanger 27
during an upgrade 27
licensing levels 10
single license limitation 11
trial license 11
Linux FLR Configuration 70

R

repository
cifs 58
DD Boost 77
FTP 75
NFS 74
NVSD 77
SFTP 76
root
with ESXi 56

S

Startup Wizard
add repositories 58
email notification 60
select a license 53
support 8

T

technical support 8

V

vCenter
required permissions 21
VI
using the VI editor 100
virtual appliance
adding to vRanger 94
changing scratch disk size 98
deploying mutltiple instances 85
disabling DRS 94, 99
required configurations 86
sizing the scratch disk 83
upgrading 31
VA utility script 89
vRanger
installation
database 17

on new SQL Express 35
on SQL server 41
options 11
license changes 27
upgrading
from vRanger 27
from vReplicator 32
the virtual appliance 31