



Community Experience Distilled

Mastering Citrix® XenServer®

Design and implement highly optimized virtualization solutions
using Citrix® XenServer® 6.2

Martez Reed

[PACKT] open source*
PUBLISHING community experience distilled

<http://freepdf-books.com>

Mastering Citrix® XenServer®

Design and implement highly optimized virtualization solutions using Citrix® XenServer® 6.2

Martez Reed

[PACKT] open source 
PUBLISHING community experience distilled

BIRMINGHAM - MUMBAI

Mastering Citrix® XenServer®

Copyright © 2014 Packt Publishing

All rights reserved. No part of this book may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, without the prior written permission of the publisher, except in the case of brief quotations embedded in critical articles or reviews.

Every effort has been made in the preparation of this book to ensure the accuracy of the information presented. However, the information contained in this book is sold without warranty, either express or implied. Neither the author, nor Packt Publishing, and its dealers and distributors will be held liable for any damages caused or alleged to be caused directly or indirectly by this book.

Packt Publishing has endeavored to provide trademark information about all of the companies and products mentioned in this book by the appropriate use of capitals. However, Packt Publishing cannot guarantee the accuracy of this information.

First published: December 2014

Production reference: 1221214

Published by Packt Publishing Ltd.
Livery Place
35 Livery Street
Birmingham B3 2PB, UK.

ISBN 978-1-78328-739-0

www.packtpub.com

Cover image by Duraid Fatouhi (duraidfatouhi@yahoo.com)

Credits

Author

Martez Reed

Project Coordinator

Kinjal Bari

Reviewers

Jon Auman

Prateek Pandey

Matthew Spah

Brian Webb

Proofreaders

Mario Cecere

Ameesha Green

Lucy Rowland

Commissioning Editor

Julian Ursell

Indexers

Mariammal Chettiyar

Tejal Soni

Acquisition Editor

Joanne Fitzpatrick

Graphics

Valentina D'silva

Content Development Editors

Azharuddin Sheikh

Rikshith Shetty

Production Coordinator

Aparna Bhagat

Technical Editor

Mrunal M. Chavan

Cover Work

Aparna Bhagat

Copy Editors

Shambhavi Pai

Rashmi Sawant

Notice

The statements made and opinions expressed herein belong exclusively to the author/s and reviewer/s of this publication, and are not shared by or represent the viewpoint of Citrix Systems®, Inc. This publication does not constitute an endorsement of any product, service or point of view. Citrix® makes no representations, warranties or assurances of any kind, express or implied, as to the completeness, accuracy, reliability, suitability, availability or currency of the content contained in this publication or any material related to this publication. Any reliance you place on such content is strictly at your own risk. In no event shall Citrix®, its agents, officers, employees, licensees or affiliates be liable for any damages whatsoever (including, without limitation, damages for loss of profits, business information, loss of information) arising out of the information or statements contained in the publication, even if Citrix® has been advised of the possibility of such loss or damages.

Citrix®, Citrix Systems®, XenApp®, XenDesktop®, and CloudPortal™ are trademarks of Citrix Systems®, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries.

About the Author

Martez Reed is an IT professional with over 6 years of experience in designing, implementing, and supporting VMware/Citrix® VDI and server virtualization solutions. In addition to focusing on virtualization solutions, he has extensive experience in managing Windows environments as well as developing Puppet modules for automation.

I would like to thank God for giving me the opportunity to write this book and share my knowledge with others. I am truly thankful to my family (Mark Sr., Beverly, Marcia, Marshelle, Marquita, Mark Jr., Mario, Marvin, Marlan, and Marrick) for supporting and encouraging me in this arduous process, and I would also like to thank Tamika for continually pushing me to complete this book. I'd like to thank all those who have supported me in my endeavors and hope to continue sharing my knowledge with others.

About the Reviewers

Jon Auman has been a system administrator for over 15 years, and he is currently focusing on DevOps and WebOps methodologies. He holds certifications in Red Hat, NetApp, Amazon Web Services, and Puppet. He has worked for a number of employers, such as Duke University, Analysts International, and NetApp in the U.S. as well as Mind Candy, MedicAnimal.com, Monitise, and HMRC in the UK. He currently runs his own consultancy DaveOps Ltd., London.

Jon installed his first XenServer® in 2008 and has been automating VMs ever since. His favorite DevOps toolset includes Puppet, Ansible, AWS CLI, and Jenkins.

Prateek Pandey is a system administrator at Pythian Group. He received his BTech degree in Computer Science from Rajasthan Technical University. He has been working as a system administrator in the IT industry for 4 years. His major interests are in cloud computing, virtualization, and Linux administration, and Big Data operations. He is willing to work on new technologies and would like to do some training on OpenStack, CloudStack, and Big Data technologies such as Hadoop.

Matthew Spah is currently working as an infrastructure engineer for Zulily in Seattle, WA, and has worked as an implementation engineer for Coalfire Systems. He has also been a computer information science tutor at Everett Community College. He is on the current advisory board for the Computer Information Science program at Everett Community College.

He always had a strong passion for open source technologies and has spent a majority of his career working with tools and applications in open source. Currently, he is working on a project that documents many of the commands in the XE command stack found in XenServer®. He is continuing with his education by taking certification courses at the University of Washington.

Brian Webb has over 17 years of experience in web, mobile, and software development. With a Bachelor's degree in Business Administration, majoring in Computer Information Systems, he possesses academic knowledge as well as extensive practical experience.

Currently, Brian is working as the CTO for Indatus – a cloud-based communications SaaS company. Previously, he was the owner of Parker Smith Software, a custom development firm building mission-critical applications for startups, small businesses, and the Fortune 500 and government agencies. He's held many positions, including a global software project manager, startup partner, interactive developer, and entrepreneur. He is a frequent attendee at tech meetups in the Louisville area.

In his spare time, Brian writes about IT leadership and development on his blog at brianwebb.org and publishes open source projects, which can be found at brianwebb.org/projects.

www.PacktPub.com

Support files, eBooks, discount offers, and more

For support files and downloads related to your book, please visit www.PacktPub.com.

Did you know that Packt offers eBook versions of every book published, with PDF and ePub files available? You can upgrade to the eBook version at www.PacktPub.com and as a print book customer, you are entitled to a discount on the eBook copy. Get in touch with us at service@packtpub.com for more details.

At www.PacktPub.com, you can also read a collection of free technical articles, sign up for a range of free newsletters and receive exclusive discounts and offers on Packt books and eBooks.



<https://www2.packtpub.com/books/subscription/packtlib>

Do you need instant solutions to your IT questions? PacktLib is Packt's online digital book library. Here, you can search, access, and read Packt's entire library of books.

Why subscribe?

- Fully searchable across every book published by Packt
- Copy and paste, print, and bookmark content
- On demand and accessible via a web browser

Free access for Packt account holders

If you have an account with Packt at www.PacktPub.com, you can use this to access PacktLib today and view 9 entirely free books. Simply use your login credentials for immediate access.

Table of Contents

Preface	1
Chapter 1: Getting Started with XenServer®	7
Citrix® XenServer®	8
Citrix® XenCenter®	8
Features of Citrix® XenServer®	8
What's new in Citrix® XenServer® 6.2	10
Open source	10
New licensing model	10
Improved guest support	10
Retired features	11
Deprecated features	11
Planning and Installing Citrix® XenServer®	11
Selecting the server hardware	11
Meeting the system requirements	12
Installing Citrix® XenServer® 6.2	13
Installation methods	13
Installation source	13
Supplemental packs	14
XenServer® installation	14
Installing and setting up XenCenter®	20
XenCenter® system requirements	20
Installing Citrix® XenCenter®	20
XenServer® PXE installation	21
XenServer® answer file	21
Planning and upgrading Citrix® XenServer®	22
Supported upgrade paths	23
The upgrade checklist	23
Upgrading XenServer®	24

Rolling pool upgrades	26
Summary	26
Chapter 2: Planning and Configuring XenServer® Networking	27
XenServer® networking overview	28
Configuration limits	29
XenServer® network components	29
PIF	30
VIF	30
Network	31
Network types	32
External	32
Bonded	34
Single-server private	38
Cross-server private	40
The management interface	40
The management interface configuration	41
Dedicated IP storage NICs	43
Bonding	46
Active-active bonding	46
Active-passive bonding	48
LACP IP and port hash	50
The LACP source MAC address	52
Virtual Local Area Networks	53
XenServer® VLAN support	53
QoS	56
Jumbo frames	56
Network troubleshooting	58
Emergency Network Reset	59
Summary	59
Chapter 3: Planning and Configuring XenServer® Storage	61
XenServer® storage overview	61
Supported storage protocols	62
XenServer® storage components	62
PBD	63
VDIs	64
The VDI format	64
VBDs	65
SRs	65
ISO library SRs	66
Virtual disk library SRs	70
Disk provisioning	71
The host bus adapter hardware	82
StorageLink technology	83

Managing SRs	83
Detach	83
Detaching an SR (using the GUI)	83
Detaching an SR (using the CLI)	84
Reattach	86
Reattaching an SR (using the GUI)	86
Reattaching an SR (using the CLI)	87
Forget	87
Forgetting an SR (using the GUI)	88
Forgetting an SR (using the CLI)	88
Destroy	89
Repair	89
Repairing an SR	89
Resize	91
The suspend SR	91
The crash dump SR	92
The default SR	92
Changing the default SR (using the GUI)	93
Changing the default SR (using the CLI)	94
Summary	95
Chapter 4: Creating and Managing Virtual Machines	97
VM overview	98
Creating a VM	98
XenServer® Tools	104
Installing XenServer® Tools on Windows VMs	104
Installing XenServer® Tools on Linux VMs	105
Modifying VMs	106
Processor (vCPU)	106
Memory (RAM)	106
The DVD drive	108
Hard disk	108
The network adapter	108
Managing VMs	108
Power states of a VM	109
Copying a VM	110
Copying a VM (using the GUI)	111
Copying a VM (using the CLI)	112
Deleting VMs	112
Deleting a VM (using the GUI)	112
Deleting a VM (using the CLI)	113
VM snapshots	114
Creating a snapshot (using the GUI)	115
Creating a snapshot (using the CLI)	117

VM templates	118
Creating a custom VM template (using the GUI)	118
Creating a custom VM template (using the CLI)	121
vApps	122
Creating a vApp (using the GUI)	122
Creating a vApp (using the CLI)	126
Importing and exporting VMs	128
Operating System Fixup	129
The transfer VM	129
Importing a VM (using the GUI)	129
Importing a VM (using the CLI)	135
Exporting a VM (using the GUI)	135
Manifest	137
OVF package signing	137
Create OVA package	138
Compress OVF files	138
Exporting a VM (using the CLI)	139
Summary	140
Chapter 5: Ensuring Availability	141
Resource pool overview	141
Resource pool requirements	142
The pool master	143
Creating a resource pool (using the GUI)	143
Creating a resource pool (using the CLI)	144
Adding a host to a resource pool (using the GUI)	145
Adding a server to a resource pool (using the CLI)	146
Removing a server from a resource pool	147
Removing a server from a resource pool (using the GUI)	148
Removing a server from a resource pool (using the CLI)	149
XenServer® maintenance mode	150
Placing a server into maintenance mode (using the GUI)	150
Placing a server into maintenance mode (using the CLI)	151
XenMotion®	152
XenMotion® requirements	152
Migrating a VM	153
Storage XenMotion®	156
Storage XenMotion® requirements	156
Migrating a VM	157
Understanding HA	158
The role of heartbeats	158
Server fencing	158
HA capacity planning	159
HA requirements	159

Enabling HA (using the GUI)	160
Enabling HA (using the CLI)	163
VM HA settings	165
The HA restart priority	165
The start order	165
The delay interval	166
Disabling HA (using the GUI)	166
Disabling HA (using the CLI)	167
Summary	168
Chapter 6: Business Continuity	169
<hr/>	
Developing a XenServer® business continuity plan	170
VMs	170
Hosts	171
SRs	171
Backing up and restoring XenServer® VMs	171
Agent-based	171
Agent-based backups	172
Agent-based restores	172
Agent-based backup solutions	172
Hypervisor-based	172
Hypervisor-based backup solutions	173
Backing up and restoring XenServer®	173
The host metadata	173
The control domain	174
Backing up the pool metadata	174
Restoring the pool metadata	174
Backing up the control domain (using the GUI)	175
Backing up the control domain (using the CLI)	176
Restoring the control domain (using the GUI)	177
Restoring the control domain (using the CLI)	180
Restoring a XenServer® deployment	182
XenServer® Disaster Recovery	183
Failover	183
Failback	184
Test failover	184
XenServer® DR requirements	185
Configuring XenServer® DR	185
XenServer® DR test failover	187
XenServer® DR failover	191
XenServer® DR failback	196
Summary	200

Chapter 7: Managing and Monitoring XenServer®	201
XenServer® updates	201
Deploying updates	202
Monitoring XenServer® performance	205
Performance alerts	207
E-mail notifications	209
Configuring e-mail notification settings (using the GUI)	209
Configuring e-mail notification settings (using the CLI)	210
Configuring e-mail notification authentication settings (using the CLI)	211
Simple Network Management Protocol	212
Configuring SNMP	212
XenServer® logging	215
Configuring remote logging (using the GUI)	215
Configuring remote logging (using the CLI)	216
The XenCenter® event log	217
The server status report	217
Generating a server status report (using the GUI)	218
Generating a server status report (using the CLI)	220
The XenCenter® application log	221
Summary	223
Chapter 8: Securing XenServer®	225
Local authentication	225
Changing the root password (using the GUI)	226
Changing the root password (using the CLI)	228
Disabling the root SSH login	228
Active Directory integration	229
Active Directory integration requirements	230
Enabling Active Directory integration (using the GUI)	230
Enabling Active Directory integration (using the CLI)	232
Disabling Active Directory integration (using the GUI)	232
Disabling Active Directory integration (using the CLI)	234
Managing Active Directory accounts	234
Adding Active Directory users/groups (using the GUI)	234
Adding Active Directory users/groups (using the CLI)	235
Removing Active Directory users/groups (using the GUI)	236
Removing Active Directory users/groups (using the CLI)	237
RBAC	238
Roles	238
Managing user roles (using the GUI)	238
Managing user roles (using the CLI)	240

Audit logging	240
Configuring audit logging (using the CLI)	241
Host security	241
XenServer® host firewall	242
VM security	243
Storage security	243
iSCSI CHAP	244
Summary	245
Chapter 9: Extending XenServer®	247
Command-line management	247
PowerShell integration	248
Installing XenServer® PowerShell Snap-in	249
XenServer® SDKs	253
CloudStack integration	253
System requirements	253
Changing the dom0 memory settings	254
Configuring the CloudStack XenServer® Support Package	254
The XenServer® Conversion Manager	257
System requirements	258
Operating systems	258
Importing the XenServer® Conversion Manager virtual appliance	258
Installing the XenServer® Conversion Manager	261
Converting a VMware VM to XenServer®	263
Troubleshooting VM conversion	268
Summary	268
Index	269

Preface

As more and more companies move their workloads from physical hardware to virtualized servers, the decision regarding which hypervisor should be used for the deployment must be made by engineers and administrators. The latest version of the Citrix XenServer® hypervisor has made the deployment of a highly available and scalable virtualization solution simple and extremely affordable.

This book provides administrators with a good mix of the design and system administration knowledge necessary to deploy and maintain an optimized XenServer® deployment.

What this book covers

Chapter 1, Getting Started with XenServer®, covers features that have been added, deprecated, and removed in the latest version of Citrix® XenServer®. We also covered installing and upgrading to the latest version of Citrix® XenServer®.

Chapter 2, Planning and Configuring XenServer® Networking, covers XenServer® networking concepts such as network bonds, jumbo frames, and dedicated IP storage networks.

Chapter 3, Planning and Configuring XenServer® Storage, covers XenServer® storage concepts such as Physical Block Devices (PBDs) and Virtual Disk Images (VDIs) as well as various storage repositories. We also covered how to manage the various types of storage repositories.

Chapter 4, Creating and Managing Virtual Machines, covers the virtual machine life cycle from its creation to deletion. We also covered topics such as VM snapshots, VM power states, vApps, as well as importing and exporting VMs.

Chapter 5, Ensuring Availability, covers XenServer® features for ensuring a highly available environment such as resource pools, XenMotion®, storage XenMotion®, and High Availability (HA).

Chapter 6, Business Continuity, covers restoring a XenServer® deployment following a disaster. The topics covered in this chapter are the methods for backing up and restoring VMs as well as hosts along with using the Citrix® XenServer® Disaster Recovery feature to restore entire sites following a disaster.

Chapter 7, Managing and Monitoring XenServer®, covers managing and monitoring a XenServer® deployment to ensure that the environment is running optimally. We also explained the process of installing system updates, monitoring system performance, configuring alerts, and setting up system logging.

Chapter 8, Securing XenServer®, covers securing a XenServer® deployment through the use of centralized authentication with Active Directory and role-based access control (RBAC). In this chapter, the techniques and methods for securing VMs, XenServer® hosts, and network storage access are explained to help prevent a compromise of the XenServer® deployment.

Chapter 9, Extending XenServer®, covers tools for automating a XenServer® environment to reduce manual administration such as the built-in CLI, Windows PowerShell as well as SDKs provided by Citrix®. It also covers integrating Citrix® XenServer® with Apache CloudStack to build Infrastructure as a Service (IaaS) private clouds. We also explained how to convert VMware VMs to XenServer®.

What you need for this book

You will need computer hardware that meets the minimum requirements for installing Citrix® XenServer® 6.2 as well as a Windows computer for managing the Citrix® XenServer® host.

Who this book is for

If you are an administrator, who is looking to gain a greater understanding of how to design and implement a virtualization solution based on Citrix® XenServer®, then this book is for you. The book will serve as an excellent resource for those who are already familiar with other virtualization platforms such as Microsoft Hyper-V or VMware vSphere.

The book assumes that you have a good working knowledge of servers, networking, and storage technologies.

Conventions

In this book, you will find a number of text styles that distinguish between different kinds of information. Here are some examples of these styles and an explanation of their meaning.

Code words in text, database table names, folder names, filenames, file extensions, pathnames, dummy URLs, user input, and Twitter handles are shown as follows: "The `since` parameter allows you to export only the events that have taken place since a particular point in time."


A block of code is set as follows:


```
<?xml version="1.0"?>
<installation srtype="ext">
<primary-disk>sda</primary-disk>
<guest-disk>sdb</guest-disk>
<keymap>us</keymap>
<root-password>mypassword</root-password>
<source type="url">http://pxehost.example.com/XenServer_</source>
<admin-interface name="eth0" proto="dhcp" />
  <timezone>Europe/London</timezone>
</installation>
```

Any command-line input or output is written as follows:

```
xe host-list
```

New terms and **important words** are shown in bold. Words that you see on the screen, for example, in menus or dialog boxes, appear in the text like this: "Review the summary report and click on **Finish** to complete the failback."

 Warnings or important notes appear in a box like this.

 Tips and tricks appear like this.

Reader feedback

Feedback from our readers is always welcome. Let us know what you think about this book – what you liked or disliked. Reader feedback is important for us as it helps us develop titles that you will really get the most out of.

To send us general feedback, simply e-mail feedback@packtpub.com, and mention the book's title in the subject of your message.

If there is a topic that you have expertise in and you are interested in either writing or contributing to a book, see our author guide at www.packtpub.com/authors.

Customer support

Now that you are the proud owner of a Packt book, we have a number of things to help you to get the most from your purchase.

Errata

Although we have taken every care to ensure the accuracy of our content, mistakes do happen. If you find a mistake in one of our books – maybe a mistake in the text or the code – we would be grateful if you could report this to us. By doing so, you can save other readers from frustration and help us improve subsequent versions of this book. If you find any errata, please report them by visiting <http://www.packtpub.com/submit-errata>, selecting your book, clicking on the **Errata Submission Form** link, and entering the details of your errata. Once your errata are verified, your submission will be accepted and the errata will be uploaded to our website or added to any list of existing errata under the Errata section of that title.

To view the previously submitted errata, go to <https://www.packtpub.com/books/content/support> and enter the name of the book in the search field. The required information will appear under the **Errata** section.

Piracy

Piracy of copyrighted material on the Internet is an ongoing problem across all media. At Packt, we take the protection of our copyright and licenses very seriously. If you come across any illegal copies of our works in any form on the Internet, please provide us with the location address or website name immediately so that we can pursue a remedy.

Please contact us at copyright@packtpub.com with a link to the suspected pirated material.

We appreciate your help in protecting our authors and our ability to bring you valuable content.

Questions

If you have a problem with any aspect of this book, you can contact us at questions@packtpub.com, and we will do our best to address the problem.

1

Getting Started with XenServer®

One of the most important technologies in the information technology field today is virtualization. Virtualization is beginning to span every area of IT, including but not limited to servers, desktops, applications, network, and more. Our primary focus is server virtualization, specifically with Citrix XenServer 6.2. There are three major platforms in the server virtualization market: VMware's vSphere, Microsoft's Hyper-V, and Citrix's XenServer.

In this chapter, we will cover the following topics:

- XenServer's overview
- XenServer's features
- What's new in Citrix XenServer 6.2
- Planning and installing Citrix XenServer
- PXE installation
- XenServer answer files
- Standalone upgrades
- Rolling pool upgrades

Citrix® XenServer®

Citrix XenServer is a type 1 or bare metal hypervisor. A bare metal hypervisor does not require an underlying host operating system. Type 1 hypervisors have direct access to the underlying hardware, which provides improved performance and guest compatibility. Citrix XenServer is based on the open source Xen hypervisor that is widely deployed in various industries and has a proven record of stability and performance.

Citrix® XenCenter®

Citrix XenCenter is a Windows-based application that provides a graphical user interface for managing the Citrix XenServer hosts from a single management interface.

Features of Citrix® XenServer®

The following section covers the features offered by Citrix XenServer:

- **XenMotion/Live VM Migration:** The XenMotion feature allows for running virtual machines to be migrated from one host to another without any downtime. XenMotion relocates the processor and memory instances of the virtual machine from one host to another, while the actual data and settings reside on the shared storage. This feature is pivotal in providing maximum uptime when performing maintenance or upgrades. This feature requires shared storage among the hosts.
- **Storage XenMotion / Live Storage Migration:** The Storage XenMotion feature provides functionality similar to that of XenMotion, but it is used to move a virtual machine's virtual disk from one storage repository to another without powering off the virtual machine.
- **High Availability:** High Availability automatically restarts the virtual machines on another host in the event of a host failure. This feature requires shared storage among the hosts.
- **Resource pools:** Resource pools are a collection of Citrix XenServer hosts grouped together to form a single pool of compute, memory, network, and storage resources that can be managed as a single entity. The resource pool allows the virtual machines to be started on any of the hosts and seamlessly moved between them.
- **Active Directory integration:** Citrix XenServer can be joined to a Windows Active Directory domain to provide centralized authentication for XenServer administrators. This eliminates the need for multiple independent administrator accounts on each XenServer host in a XenServer environment.

- **Role-based access control (RBAC):** RBAC is a feature that takes advantage of the Active Directory integration and allows administrators to define roles that have specific privileges associated with them. This allows administrative permissions to be segregated among different administrators.
- **Open vSwitch:** The default network backend for the Citrix XenServer 6.2 hypervisor is Open vSwitch. Open vSwitch is an open source multilayer virtual switch that brings advanced network functionality to the XenServer platform such as NetFlow, SPAN, OpenFlow, and enhanced **Quality of Service (QoS)**. The Open vSwitch backend is also an integral component of the platform's support of **software-defined networking (SDN)**.
- **Dynamic Memory Control:** Dynamic Memory Control allows XenServer to maximize the physical memory utilization by sharing unused physical memory among the guest virtual machines. If a virtual machine has been allocated 4 GB of memory and is only using 2 GB, the remaining memory can be shared with the other guest virtual machines. This feature provides a mechanism for memory oversubscription.
- **IntelliCache:** IntelliCache is a feature aimed at improving the performance of Citrix XenDesktop virtual desktops. IntelliCache creates a cache on a XenServer local storage repository, and as the virtual desktops perform read operations, the parent VM's virtual disk is copied to the cache. Write operations are also written to the local cache when nonpersistent or shared desktops are used. This mechanism reduces the load on the storage array by retrieving data from a local source for reads instead of the array. This is particularly beneficial when multiple desktops share the same parent image. This feature is only available with Citrix XenDesktop.
- **Disaster Recovery:** The XenServer Disaster Recovery feature provides a mechanism to recover the virtual machines and vApps in the event of the failure of an entire pool or site.
- **Distributed Virtual Switch Controller (DVSC):** DVSC provides centralized management and visibility of the networking in XenServer.
- **Thin provisioning:** Thin provisioning allows for a given amount of disk space to be allocated to virtual machines but only consume the amount that is actually being used by the guest operating system. This feature provides more efficient use of the underlying storage due to the on-demand consumption.

What's new in Citrix® XenServer® 6.2

Citrix has added a number of new and exciting features in the latest version of XenServer:

- Open source
- New licensing model
- Improved guest support

Open source

Starting with Version 6.2, the Citrix XenServer hypervisor is now open sourced, but continues to be managed by Citrix Systems. The move to an open source model was the result of Citrix Systems' desire to further collaborate and integrate the XenServer product with its partners and the open source community.

New licensing model

The licensing model has been changed in Version 6.2, with the free version of the XenServer platform now providing full functionality, the previous advanced, enterprise, and platinum versions have been eliminated. Citrix will offer paid support for the free version of the XenServer hypervisor that will include the ability to install patches/updates using the XenCenter GUI, in addition to Citrix technical support.

Improved guest support

Version 6.2 has added official support for the following guest operating systems:

- Microsoft Windows 8 (full support)
- Microsoft Windows Server 2012
- **SUSE Linux Enterprise Server (SLES) 11 SP2** (32/64 bit)
- **Red Hat Enterprise Linux (RHEL)** (32/64 bit) 5.8, 5.9, 6.3, and 6.4
- **Oracle Enterprise Linux (OEL)** (32/64 bit) 5.8, 5.9, 6.3, and 6.4
- CentOS (32/64 bit) 5.8, 5.9, 6.3, and 6.4
- Debian Wheezy (32/64 bit)
- VSS support for Windows Server 2008 R2 has been improved and reintroduced

Citrix XenServer 6.2 Service Pack 1 adds support for the following operating systems:

- Microsoft Windows 8.1
- Microsoft Windows Server 2012 R2

Retired features

The following features have been removed from Version 6.2 of Citrix XenServer:

- **Workload Balancing (WLB)**
- SCOM integration
- **Virtual Machine Protection Recovery (VMPR)**
- Web Self Service
- XenConvert (this has been replaced by XenServer Conversion Manager)

Deprecated features

The following features will be removed from the future releases of Citrix XenServer. Citrix has reviewed the XenServer market and has determined that there are third-party products that are able to provide the product functionality more effectively:

- Microsoft System Center Virtual Machine Manager SCVMM support
- Integrated StorageLink

Planning and Installing Citrix® XenServer®

Installing Citrix XenServer is generally a simple and straightforward process that can be completed in 10 to 15 minutes. While the actual install is simple, there are several major decisions that need to be made prior to installing Citrix XenServer in order to ensure a successful deployment.

Selecting the server hardware

Typically, the first step is to select the server hardware that will be used. While the thought might be to just pick a server that fits our needs, we should also ensure that the hardware meets the documented system requirements. Checking the hardware against the **Hardware Compatibility List (HCL)** provided by Citrix Systems is advised to ensure that the system qualifies for Citrix support and that the system will properly run Citrix XenServer. The HCL provides a list of server models that have been verified to work with Citrix XenServer.

[ The HCL can be found online at <http://www.citrix.com/xenserver/hcl>.]

Meeting the system requirements

The following sections cover the minimal system requirements for Citrix XenServer 6.2.

Processor requirements

The following list covers the minimum requirements for the processor(s) to install Citrix XenServer 6.2:

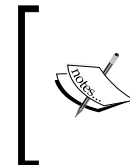
- One or more 64-bit x86 CPU(s), 1.5 GHz minimum, 2 GHz or faster multicore CPU
- To support VMs running on Windows, an Intel VT or AMD-V 64-bit x86-based system with one or more CPU(s) is required
- Virtualization technology needs to be enabled in the BIOS



Virtualization technology is disabled by default on many server platforms and needs to be manually enabled.

Memory requirements

The minimum memory requirement for installing Citrix XenServer 6.2 is 2 GB with a recommendation of 4 GB or more for production workloads.




In addition to the memory usage of the guest virtual machines, the Xen hypervisor on the Control Domain (dom0) consumes the memory resources. The amount of resources consumed by the Control Domain (dom0) is based on the amount of physical memory in the host.

Hard disk requirements

The following are the minimum requirements for the hard disk(s) to install Citrix XenServer 6.2:

- 16 GB of free disk space minimum and 60 GB of free disk space is recommended
- Direct attached storage in the form of SATA, SAS, SCSI, or PATA interfaces are supported

- XenServer can be installed on a LUN presented from a **storage area network (SAN)** via a **host bus adapter (HBA)** in the XenServer host

 A physical HBA is required to boot XenServer from a SAN.

Network card requirements

100 Mbps or a faster NIC is required for installing Citrix XenServer. One or more gigabit NICs is recommended for faster P2V, export/import data transfers, and VM live migrations.

Installing Citrix® XenServer® 6.2

The following sections cover the installation of Citrix XenServer 6.2.

Installation methods

The Citrix XenServer 6.2 installer can be launched via two methods as listed:

- CD/DVD
- PXE or network boot

Installation source

There are several options where the Citrix XenServer installation files can be stored, and depending on the scenario, one would be preferred over another. Typically, the HTTP, FTP, or NFS option would be used when the installer is booted over the network via PXE or when a scripted installation is being performed. The installation sources are as follows:

- Local media (CD/DVD)
- HTTP or FTP
- NFS

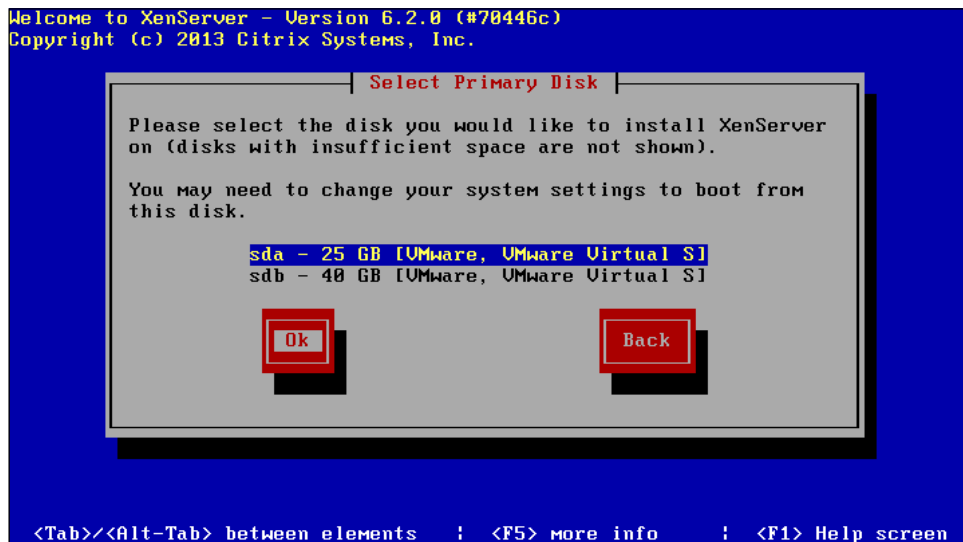
Supplemental packs

Supplemental packs provide additional functionality to the XenServer platform through features such as enhanced hardware monitoring and third-party management software integration. The supplemental packs are typically downloaded from the vendor's website and are installed when prompted during the XenServer installation.

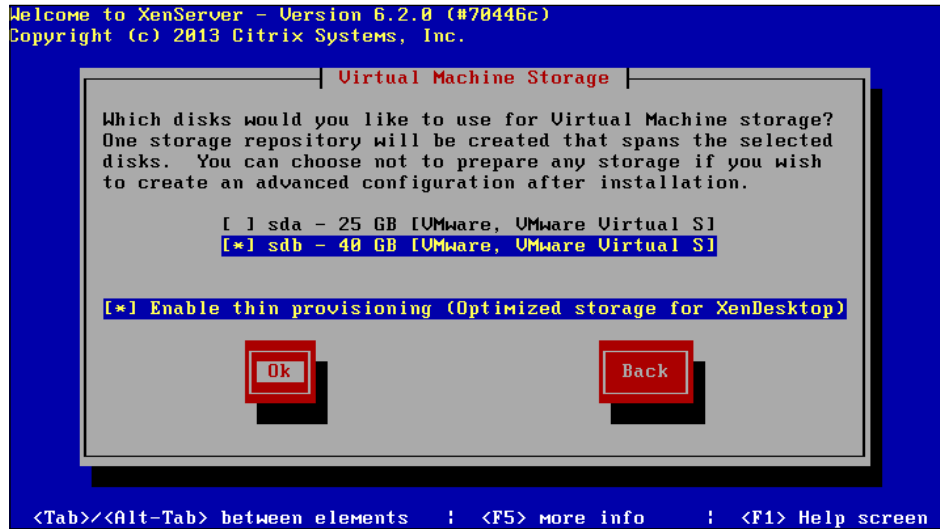
XenServer® installation


The following steps cover installing Citrix XenServer 6.2 from a CD:

1. Boot the server from the Citrix XenServer 6.2 installation media and press *Enter* when prompted to start the Citrix XenServer 6.2 installer.
2. Select the desired key mapping and select **Ok** to proceed.
3. Press *F9* if additional drivers need to be installed or select **Ok** to continue.
4. Accept the EULA.
5. Select the hard drive for the Citrix XenServer installation and choose **Ok** to proceed.

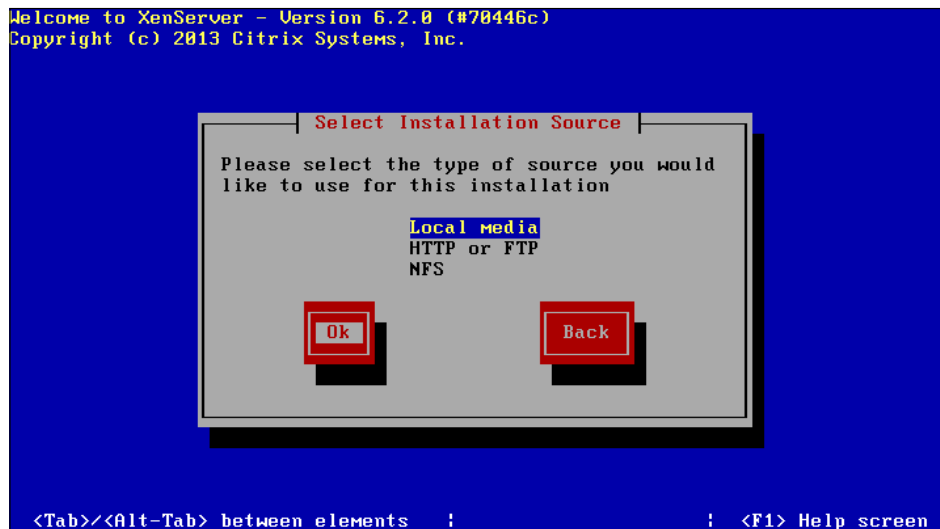


6. Select the hard drive(s) to be used for storing the guest virtual machines and choose **Ok** to continue.

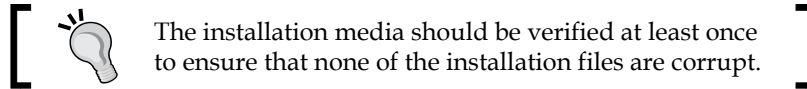


 You need to select the **Enable thin provisioning (Optimized storage for XenDesktop)** option to make use of the IntelliCache feature.

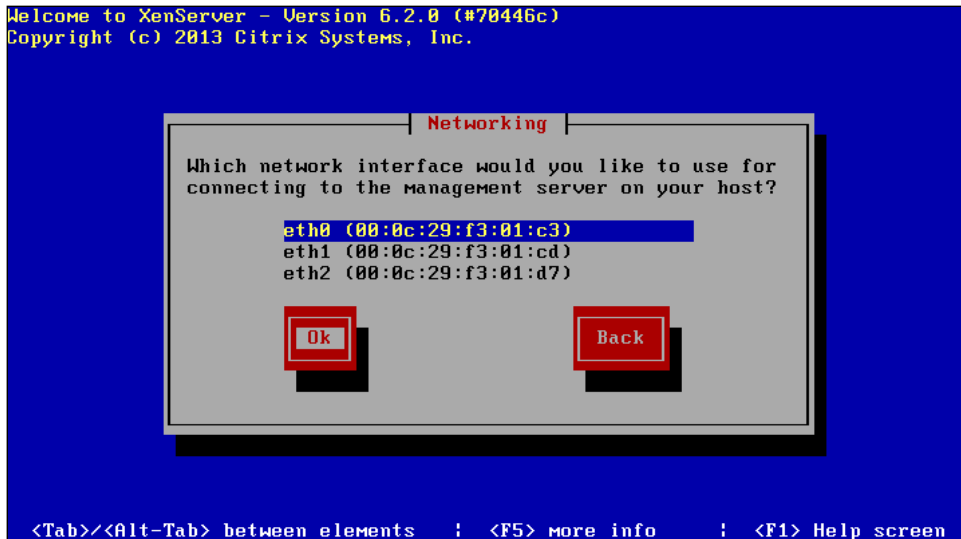
7. Select the installation media source and select **Ok** to continue.



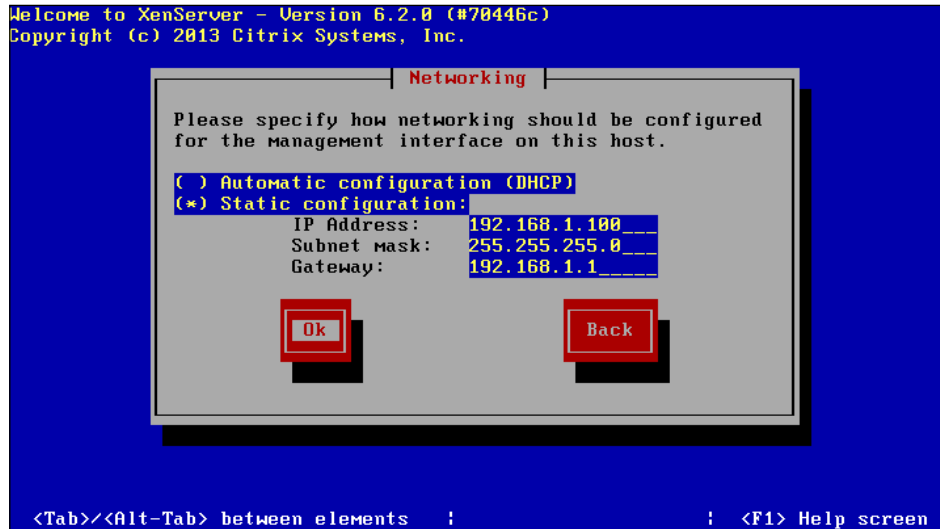
8. Install supplemental packs if necessary and choose **No** to proceed.
9. Select **Verify installation source** and select **Ok** to begin the verification.



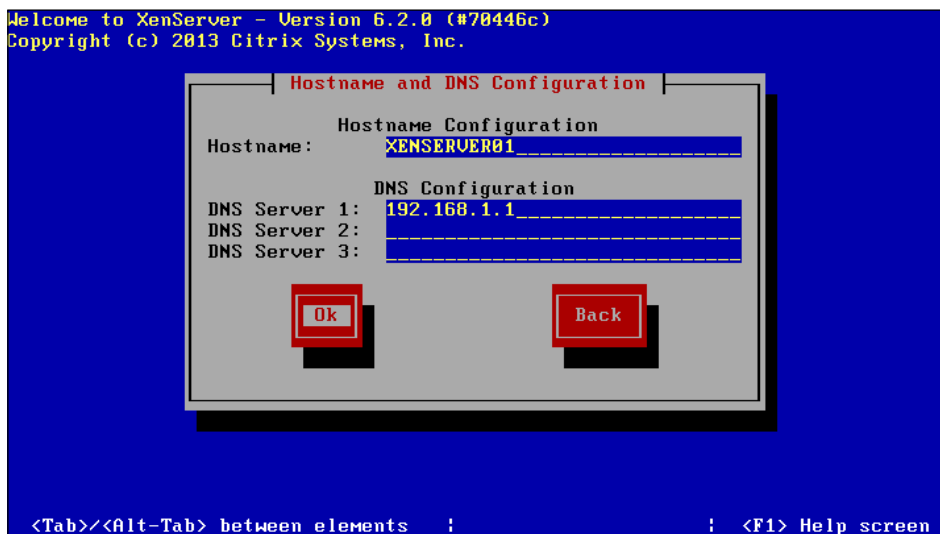
10. Choose **Ok** to continue after the verification has successfully completed.
11. Provide and confirm a password for the root account and select **Ok** to proceed.
12. Select the network interface to be used as the primary management interface and choose **Ok** to continue.



13. Select the **Static configuration** option and provide the requested information. Choose **Ok** to continue.

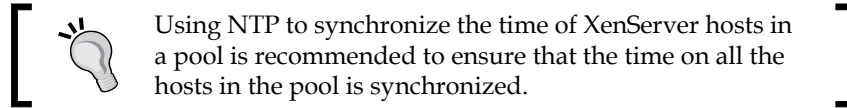


14. Enter the desired hostname and DNS server information. Select **Ok** to proceed.

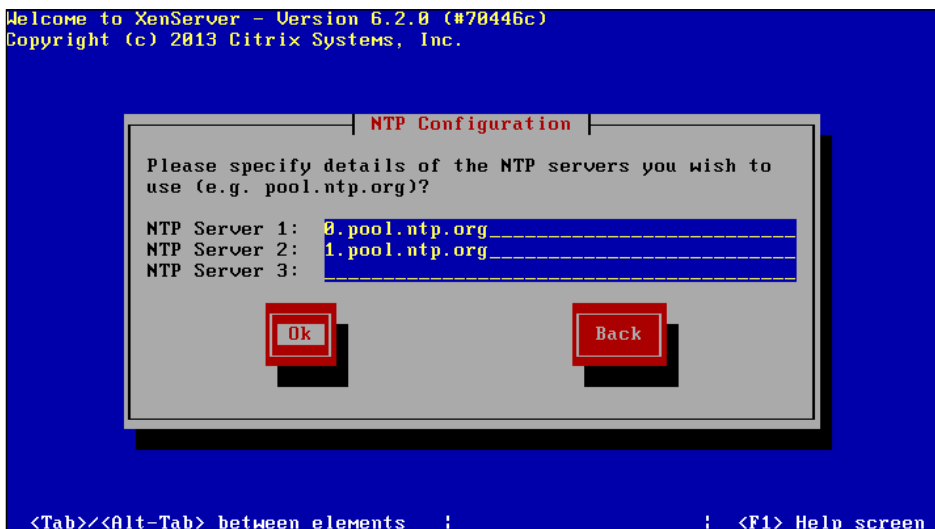


15. Select the appropriate geographical area to configure the time zone and select **Ok** to continue.
16. Select the appropriate city or area to configure the time zone and select **Ok** to proceed.

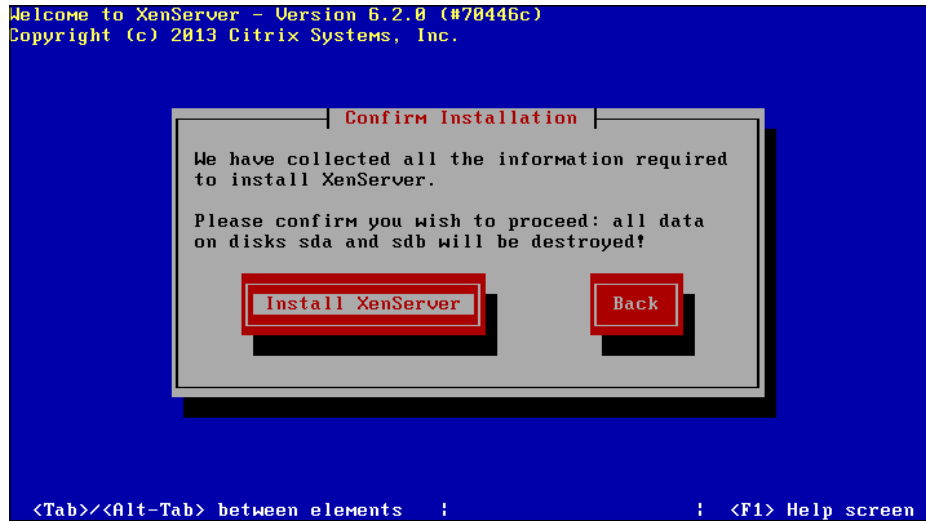
17. Select **Using NTP** or **Manual time entry** for the server to determine the local time and choose **Ok** to continue.



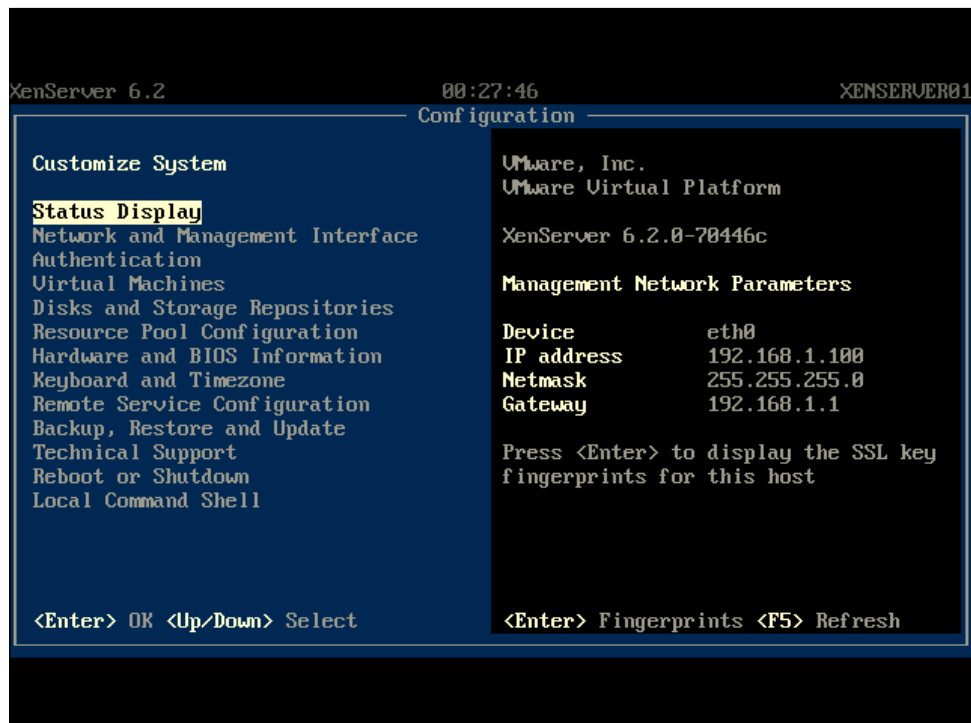
18. Enter the IP address or hostname of the desired NTP server(s) and select **Ok** to proceed.



19. Select **Install XenServer** to start the installation.



20. Click on **Ok** to restart the server after the installation has completed. The following screen should be presented after the reboot:



Installing and setting up XenCenter®

Citrix XenCenter is a Windows-based application that provides a graphical user interface for managing the Citrix XenServer hosts from a single management interface. The installation files can be downloaded from Citrix.com or by entering the IP address of the Citrix XenServer in a web browser and downloading the installer.

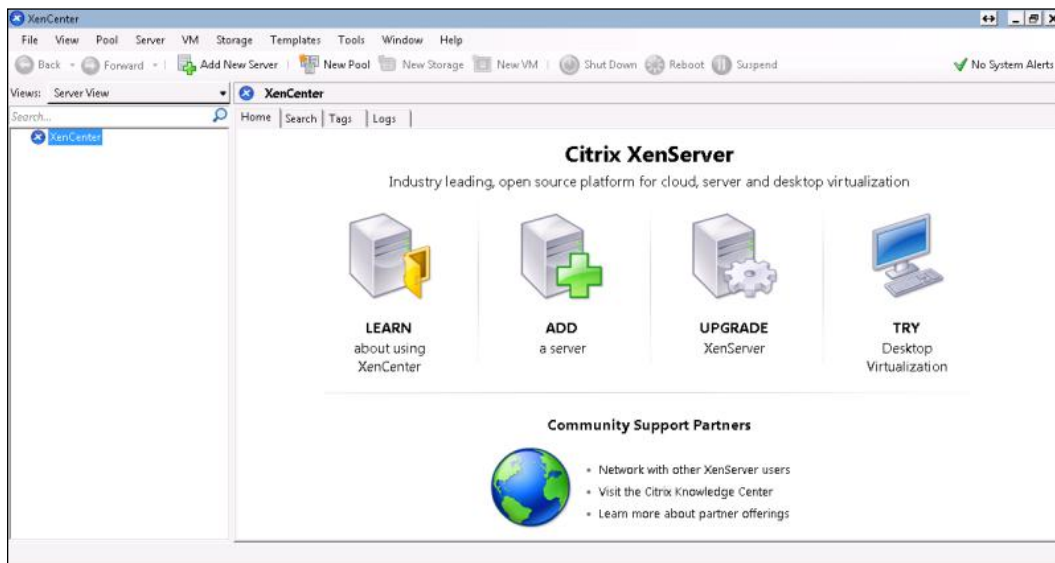
XenCenter® system requirements

The following are the system requirements to install XenCenter:

- **OS:** Windows XP, Vista, 7, 8, 2003, 2008, and 2012
- **CPU:** 750 MHz minimum, 1 GHz or faster is recommended
- **RAM:** 1 GB minimum, 2 GB or more is recommended
- **Disk space:** 100 MB minimum
- **Network:** 100 MB or faster NIC
- **Software:** .NET Framework 3.5 or later

Installing Citrix® XenCenter®

The installation of Citrix XenCenter is a straightforward guided process that simply prompts for basic information such as the location of the installation files and user information:



After Citrix XenCenter has been installed, add the Citrix XenServer host to XenCenter by clicking on the **Add New Server** button and providing the requested credentials.

XenServer® PXE installation

Installing Citrix XenServer is a fairly quick and effortless process when dealing with just a handful of servers, but performing an installation of twenty, forty, or even a hundred with a CD is a recipe for a long day. The PXE installation is a key component in automating XenServer deployments in order to reduce the deployment time and eliminate human errors during the installation. The PXE installation requires the use of a PXE server, which utilizes DHCP and TFTP to facilitate booting the XenServer installer over the network. HTTP, FTP, or NFS are the protocols used to serve the installation source files to the hosts.

XenServer® answer file

The installation of Citrix XenServer can be automated through the use of an answer file, which provides the answers to the prompts during the installation. An answer file is typically used in conjunction with PXE booting the servers to expedite a mass deployment. The answer file is XML based and the administrator specifies the location of the answer file in the XenServer boot options. The answer file can be fetched via FTP, HTTP, or NFS.

The following is an example of a PXE boot menu entry that is used to install a host using an answer file stored on an HTTP server:

```
default xenserver
label xenserver
kernel mboot.c32
append xenserver/xen.gz dom0_max_vcpus=2 dom0_mem=752M com1=115200,8n1
console=com1,vga --- xenserver/vmlinuz xencons=hvc console=hvc0
console=tty0 answerfile=http://Server_Address/answer_file.xml install
--- xenserver/install.img
```

The following is an example of an answer file that provides the minimum answers required to complete an automated installation of XenServer:

```
<?xml version="1.0"?>
<installation srtype="ext">
<primary-disk>sda</primary-disk>
<guest-disk>sdb</guest-disk>
<keymap>us</keymap>
<root-password>mypassword</root-password>
```

```
<source type="url">http://pxehost.example.com/XenServer_/</source>
<admin-interface name="eth0" proto="dhcp" />
  <timezone>Europe/London</timezone>
</installation>
```

The following table explains the options used in the preceding answer file:

Element	Description
Installation srtype	The srtype attribute sets the storage repository type used during the installation
Primary-disk	This determines the location of the control domain
Guest-disk	This sets which disk(s) will be used to store the guest virtual machines
Keymap	The name of the keymap used during the installation
Root-password	This sets the password for the root account
Source type	This defines where the installation files are located
Admin-interface name="eth0" proto="dhcp"	This sets the interface used for the host administration
Timezone	This sets the host time zone



Additional options can be found in the Citrix XenServer installation guide.

Planning and upgrading Citrix® XenServer®

There are several reasons to upgrade to the latest version of Citrix XenServer whether it is for security, new features, or improved stability. Properly planning the upgrade can make the difference between a long weekend and a short one.

Supported upgrade paths


The following table breaks down the upgrade paths that can be taken to upgrade an existing XenServer installation to Version 6.2:

Version	Supported or not
XenServer 6.1.0	Yes
XenServer 6.0.2	Yes
XenServer 6.0	Yes
XenServer 5.6, 5.6 Feature Pack 1, 5.6 Service Pack 2	Yes
XenServer 5.5	No; you must first upgrade to XenServer Version 5.6 and then to version 6.2


The upgrade checklist

Upgrading a XenServer deployment can be a difficult task that involves various moving parts and interdependencies that need to be accounted for, so having a checklist to work with can help make things easier. The following steps will walk you through some of the high-level tasks involved in the upgrade process:

1. Check the release notes for the new version on Citrix's website.

 This may reveal known issues with the version and indicate what features have been added along with the issues resolved from previous versions.

2. Check the server hardware against the HCL for the new version of Citrix XenServer.
3. Check the server hardware vendor's website for new hardware drivers for the new XenServer version.
4. Check whether the currently hosted virtual machines are supported on the new XenServer version.

 This is typically only an issue with support for older operating systems being deprecated in the newer version.

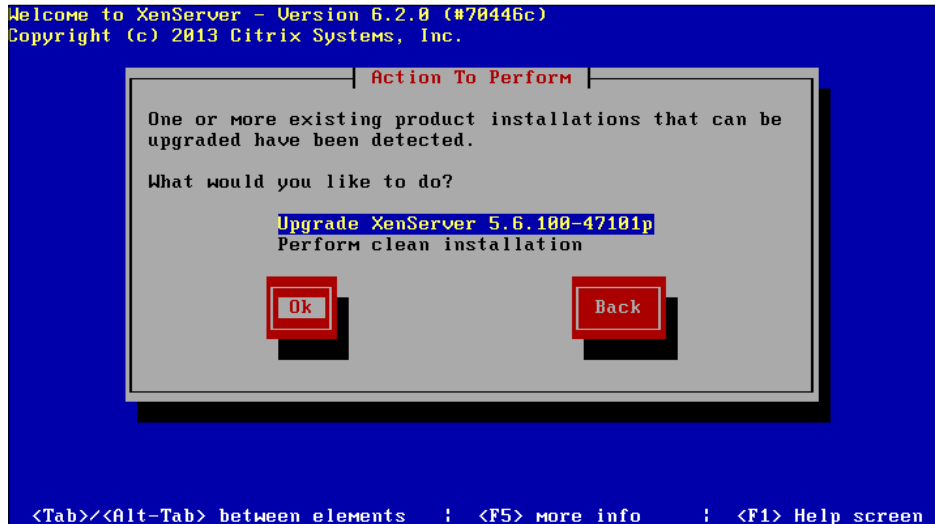
5. Identify and verify dependency support. Dependencies are typically third-party software that integrate with XenServer such as Citrix XenDesktop, CloudStack, OpenStack, and other management software.
6. Attempt an upgrade on test hardware if test hardware is available.
7. Backup the host/pool configuration.
8. Backup the virtual machines.
9. Migrate the virtual machines off the host to be upgraded by placing the host into the maintenance mode. This operation requires multiple Citrix XenServer hosts.
10. Upgrade Citrix XenCenter to the latest version.
11. Upgrade the host to the latest version of Citrix XenServer.
12. Install the latest patches on the upgraded host.
13. Create snapshots of the virtual machines.
14. Migrate a test virtual machine(s) to the upgraded host to test functionality.
15. Migrate noncritical virtual machines to the upgraded host first.
16. Upgrade Citrix xen-tools on the migrated virtual machines to the latest version.
17. Verify that the virtual machines are functioning properly.
18. Remove the snapshots from the virtual machines after a successful verification.
19. Migrate the remaining virtual machines and repeat steps 16 through 18.

Upgrading XenServer®

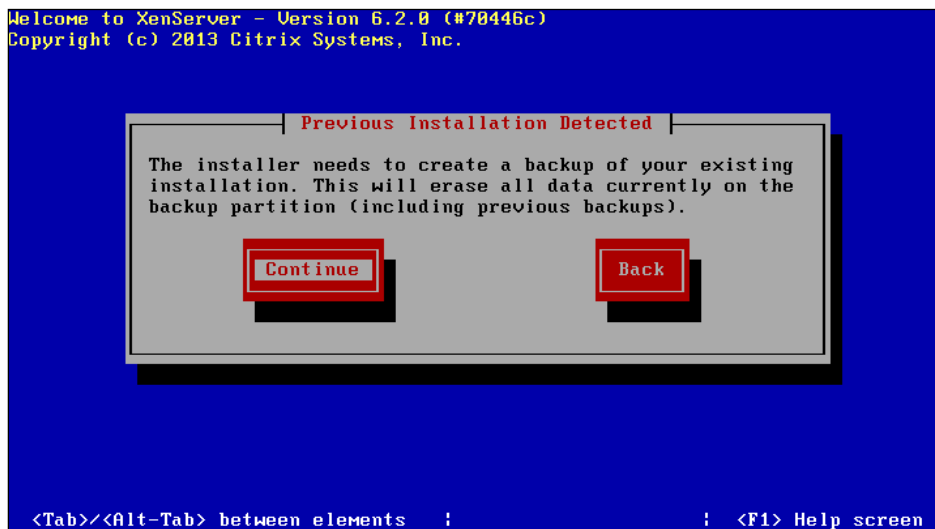
The following steps cover upgrading an existing installation of XenServer to Citrix XenServer 6.2:

1. Boot the server from the Citrix XenServer 6.2 installation media and press *Enter* when prompted to start the Citrix XenServer 6.2 installer.
2. Select the desired key mapping and choose **Ok**.
3. Press *F9* if additional drivers are needed or select **Ok** to continue.
4. Accept the EULA.

5. Select the upgrade option and choose **Ok**. The installer will display the currently installed version on the server.

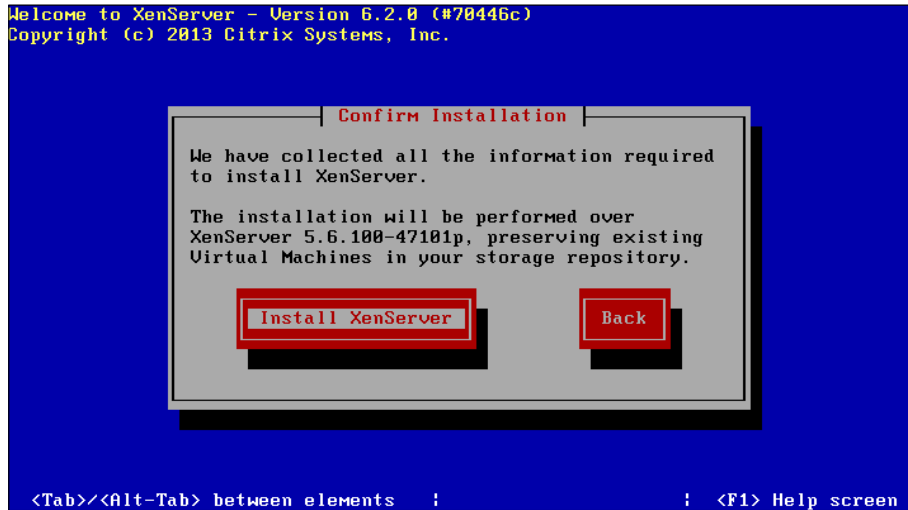


6. Select **Continue** to proceed with the upgrade, as shown in the following screenshot:




7. Select the appropriate installation media location and select **Ok** to continue.
8. Install supplemental packs if necessary.
9. Select **Verify installation source** and select **Ok** to begin the verification.

10. Choose **Ok** to continue after the verification has successfully completed.
11. Select **Install XenServer** to begin the upgrade process.



12. Choose **Ok** to restart the server to complete the upgrade.

[ In the event of an issue with the upgrade, the installation can be rolled back to the previous version if a backup was created.]

Rolling pool upgrades

Rolling pool upgrades allow an environment to be upgraded to the latest version of Citrix XenServer without the need for downtime for the virtual machines. The rolling pool feature is managed within Citrix XenCenter, and provides a guided wizard for migrating the virtual machines from one host to another as the hosts are upgraded. This process continues until the entire pool is upgraded to the latest version of Citrix XenServer.

Summary

In this chapter, we covered an overview of Citrix XenServer along with the features that were available. We also looked at the new features that were added in XenServer 6.2 and then examined installing XenServer as well as performing upgrades of existing installs.

In the next chapter, we will learn about Citrix XenServer networking.

2

Planning and Configuring XenServer[®] Networking

The previous chapter provided us with an overview of XenServer. We got familiar with the new and exciting features of Citrix XenServer 6.2. We learned how to install and upgrade to Citrix XenServer 6.2. Now that we have a firm grip on the installation and upgrade process, let's move on to see what XenServer has to offer with regards to virtual networking features. Citrix XenServer provides a rich feature set and robust scalability in terms of networking.

In this chapter, we will cover the following topics:

- XenServer networking overview
- XenServer network components
- Network types
- A management interface
- A dedicated IP storage
- Network bonding
- QoS and jumbo frames
- VLANs
- Network troubleshooting

XenServer® networking overview

The default network stack in Citrix XenServer 6.2 is Open vSwitch, which replaced the Linux bridge as the default network stack starting from Version 6.0 of Citrix XenServer. Open vSwitch is an open source multilayer virtual switch that provides enhanced functionality in comparison with the Linux bridge network stack. Some of the features provided by Open vSwitch are listed as follows:

- **NetFlow:** NetFlow is a technology originally developed by Cisco Systems that is used to monitor network traffic and provide administrators with visibility into traffic that traverses the network.
- **sFlow:** sFlow is an open standard technology used to monitor network traffic and provide administrators with visibility into traffic that traverses the network.
- **Switched Port Analyzer (SPAN):** SPAN or port mirroring is used to copy or mirror the packets from one port to another on the switch. This is typically used for monitoring purposes.
- **Remote Switched Port Analyzer (RSPAN):** RSPAN provides you with the ability to copy or mirror packets that are sourced from ports on different switches and allows you to have a centralized monitoring device.
- **Quality of Service (QoS):** QoS provides the ability to classify and prioritize traffic based upon certain criteria.
- **Link Aggregation Control Protocol (LACP):** LACP provides the ability to aggregate or combine multiple physical network links into a single logical link in order to provide redundancy as well as additional aggregate bandwidth.
- **OpenFlow support:** OpenFlow allows the abstraction of the control plane from the forwarding plane of virtual switches in the case of Open vSwitch. This functionality provides centralized administration of the vSwitches as well as advanced forwarding capabilities.
- **Generic Routing Encapsulation (GRE):** GRE is an IP encapsulation protocol that is used to tunnel network packets across a virtual point-to-point link.
- **VXLAN:** VXLAN allows the creation of an overlay network or a logical layer 2 network that is established over a layer 3 network.

Configuration limits

Citrix XenServer 6.2 supports up to 16 physical network interfaces per XenServer host, up to four physical network interfaces can be bonded together in a supported configuration, and up to seven virtual network interfaces can be added to a virtual machine.

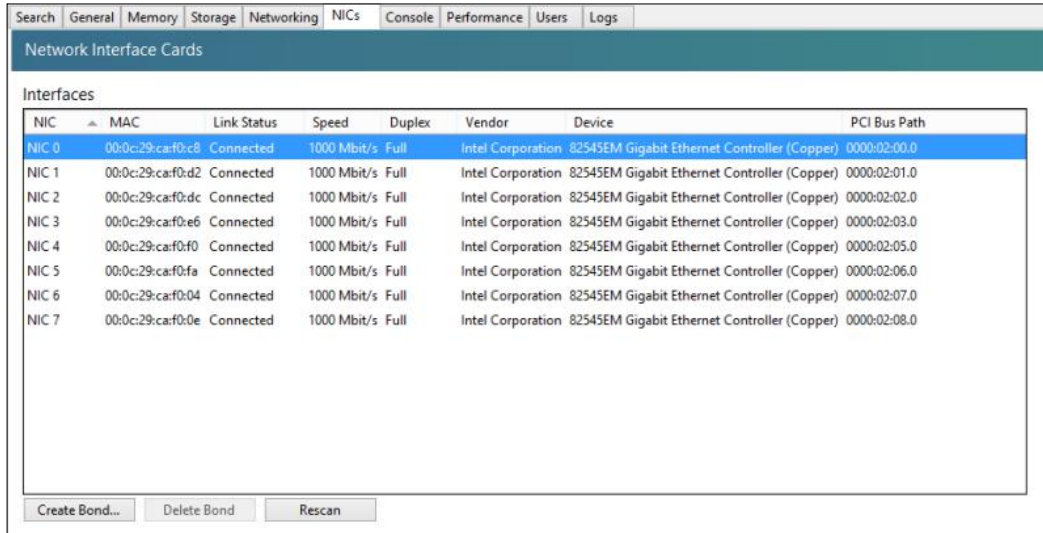
XenServer® network components

The primary Citrix XenServer network components are **virtual interfaces (VIFs)**, networks, and **physical interfaces (PIFs)**, which are simply physical components, which are virtualized. The following diagram displays how each of the pieces fits together to form the virtual network:




PIF

A PIF represents the physical network interface on the XenServer host. PIFs on the XenServer host act as uplink interfaces, providing access to the physical network. These are just like uplink ports on a physical switch that are used to interconnect switches except in this case, one of them is virtual and the other is physical. Have a look at the following screenshot:



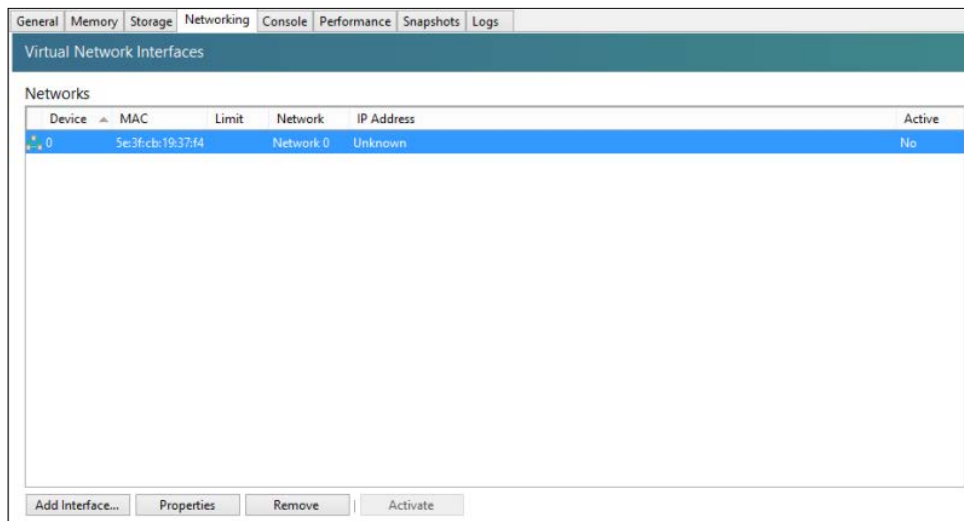
The screenshot shows the 'Network Interface Cards' tab in XenCenter. It displays a table of Network Interface Cards (NICs) with the following columns: NIC, MAC, Link Status, Speed, Duplex, Vendor, Device, and PCI Bus Path. There are seven NICs listed, all with a 'Connected' status and '1000 Mbit/s Full' duplex. The vendor for all is 'Intel Corporation' and the device is '82545EM Gigabit Ethernet Controller (Copper)'. The PCI bus paths range from 0000:02:00.0 to 0000:02:08.0.


NIC	MAC	Link Status	Speed	Duplex	Vendor	Device	PCI Bus Path
NIC 0	00:0c:29:ca:f0:c8	Connected	1000 Mbit/s	Full	Intel Corporation	82545EM Gigabit Ethernet Controller (Copper)	0000:02:00.0
NIC 1	00:0c:29:ca:f0:d2	Connected	1000 Mbit/s	Full	Intel Corporation	82545EM Gigabit Ethernet Controller (Copper)	0000:02:01.0
NIC 2	00:0c:29:ca:f0:dc	Connected	1000 Mbit/s	Full	Intel Corporation	82545EM Gigabit Ethernet Controller (Copper)	0000:02:02.0
NIC 3	00:0c:29:ca:f0:e6	Connected	1000 Mbit/s	Full	Intel Corporation	82545EM Gigabit Ethernet Controller (Copper)	0000:02:03.0
NIC 4	00:0c:29:ca:f0:f0	Connected	1000 Mbit/s	Full	Intel Corporation	82545EM Gigabit Ethernet Controller (Copper)	0000:02:05.0
NIC 5	00:0c:29:ca:f0:fa	Connected	1000 Mbit/s	Full	Intel Corporation	82545EM Gigabit Ethernet Controller (Copper)	0000:02:06.0
NIC 6	00:0c:29:ca:f0:04	Connected	1000 Mbit/s	Full	Intel Corporation	82545EM Gigabit Ethernet Controller (Copper)	0000:02:07.0
NIC 7	00:0c:29:ca:f0:0e	Connected	1000 Mbit/s	Full	Intel Corporation	82545EM Gigabit Ethernet Controller (Copper)	0000:02:08.0

 PIFs can be viewed from the NICs tab under the XenServer host in XenCenter.

VIF

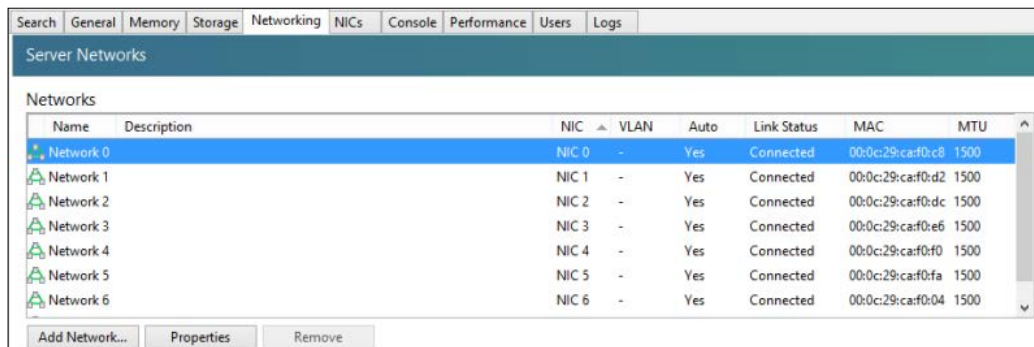
A VIF represents the virtual network interface that is attached to the virtual machine. The VIF connects the virtual machine to the designated network or virtual switch in order to provide connectivity to network resources. A VIF is just like the network card on a physical server that is connected to a switch or in the case of XenServer, a network. Have a look at the following screenshot:




[ VIFs can be viewed from the **Networking** tab after selecting a virtual machine in XenCenter.]

Network

A network represents the virtual switch that the VIFs and PIFs are connected to. VIFs are downstream interfaces connecting the virtual switch to the virtual machines, and PIFs are upstream interfaces connecting the virtual switch to the physical switches. Have a look at the following screenshot:



[ When a virtual machine is created, any network marked as **Auto** will be automatically added to the virtual machine unless it is manually removed.]

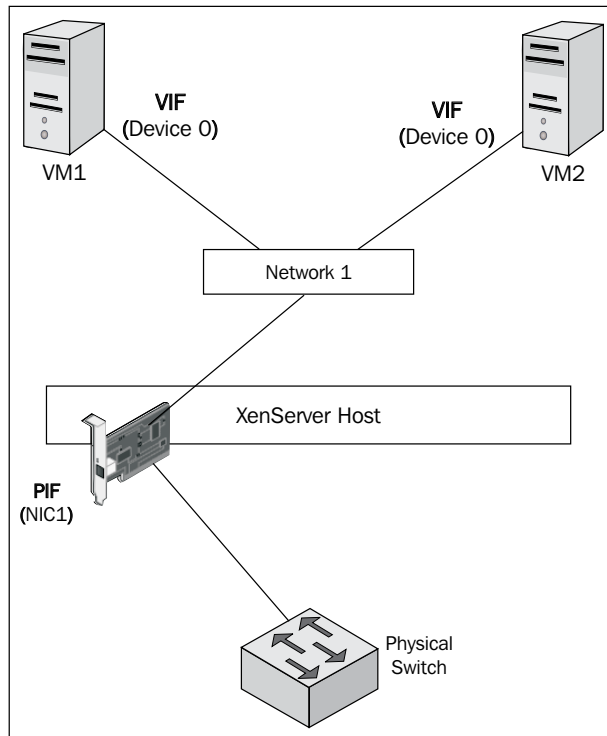
Network types

There are four different network types that can be configured in Citrix XenServer 6.2:

- External
- Bonded
- Single-server private
- Cross-server private

External

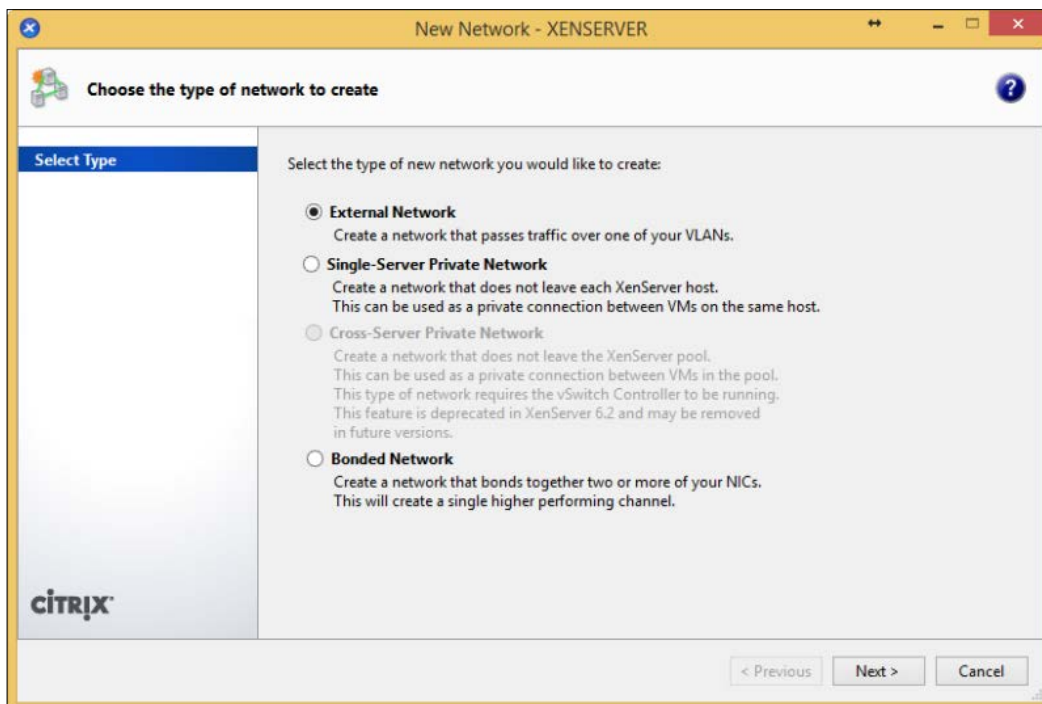
An external network type is used to provide virtual machine's access to a network outside of the XenServer host. The network utilizes a PIF as an uplink to provide access to the network resources. This is shown in the following diagram:



The external network configuration

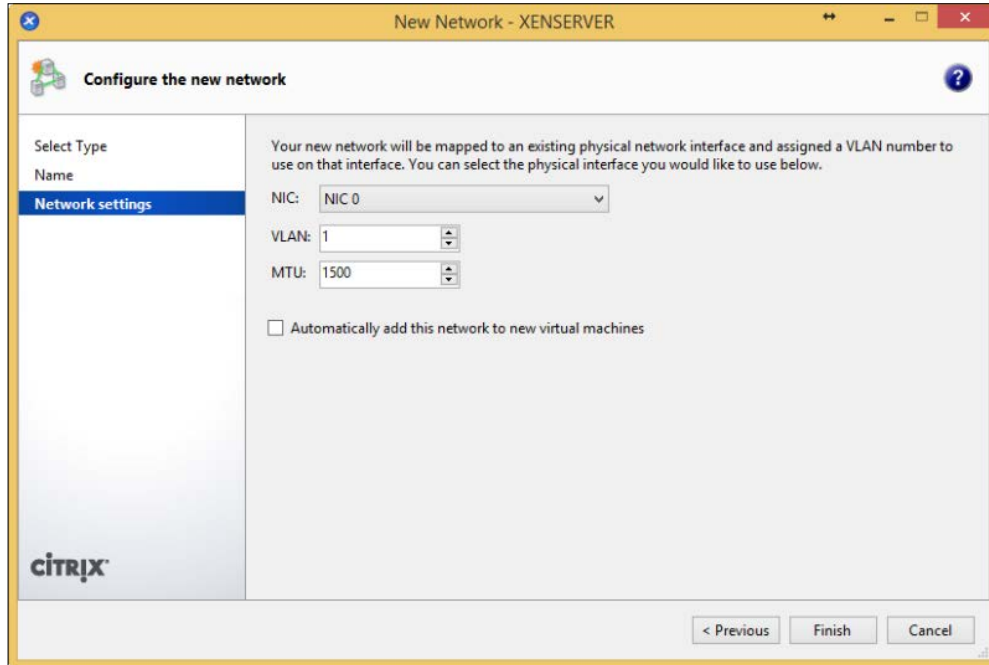
The following steps show you how to configure an external network using the XenCenter GUI:

1. Click on the **Add Network** button under the **Networking** tab of the XenServer host.
2. Select the **External Network** option and click on **Next** to continue.



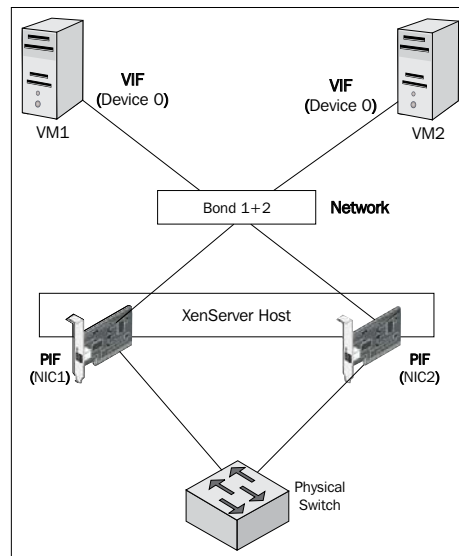
3. Provide a name and description for the new network.

4. Select the desired physical interface, **VLAN**, **MTU**, and check whether the network should be automatically added to the newly created virtual machines. Click on **Finish** to create the new network.



Bonded

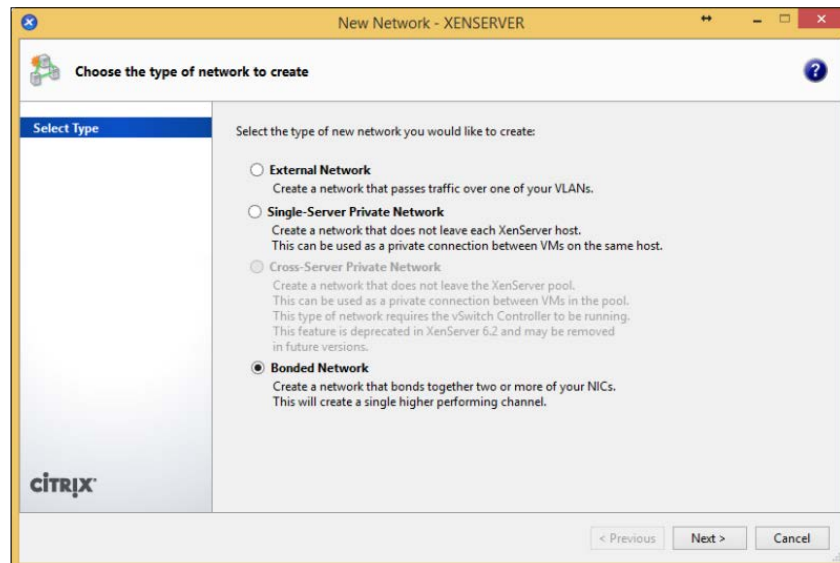
Bonded networks are used to bundle multiple physical network interfaces in order to create a redundant and resilient network uplink for a XenServer virtual network. The bonded network is also primarily used to aggregate the available bandwidth of individual physical interfaces in order to eliminate potential network bottlenecks. Have a look at the following diagram:



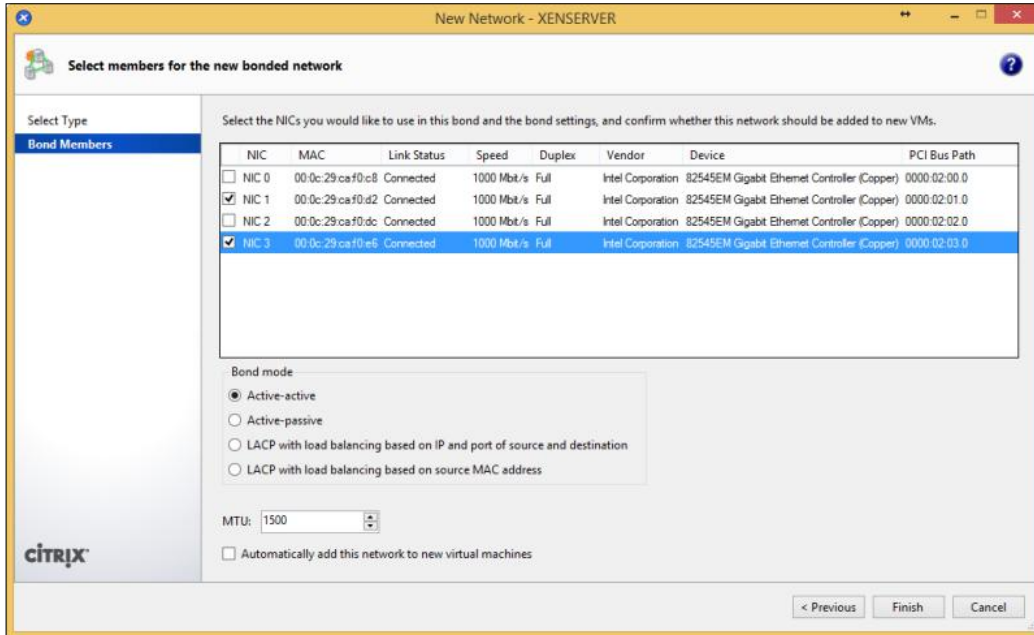
The bonded network configuration


The following steps show how to configure a bonded network using the XenCenter GUI:

1. Click on the **Add Network** button under the **Networking** tab of the XenServer host.
2. Select the **Bonded Network** option and click on **Next** to continue.



3. Select the physical network interfaces for the network bond, choose the desired bond mode, MTU, and check whether the network should be automatically added to the newly created virtual machines.



 A best practice is to use PIFs on different physical network cards to create the network bond. This is done in order to prevent a service disruption due to the failure of a network card.

4. The new bonded network should now appear under the **Networking** tab of the XenServer host, as shown in the following screenshot:

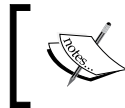
The screenshot shows the XenServer interface with the 'Networking' tab selected. The 'Server Networks' section displays a table of networks:

Name	Description	NIC	VLAN	Auto	Link Status	MAC	MTU
Bond 1+3		Bond 1+3	-	No	Connected	00:0c:29:caf0:d2	1500
Network 0		NIC 0	-	Yes	Connected	00:0c:29:caf0:c8	1500
Network 2		NIC 2	-	Yes	Connected	00:0c:29:caf0:dc	1500

Below the network table are buttons for 'Add Network...', 'Properties', and 'Remove'. The 'IP Address Configuration' section shows a table with the following data:

Server	Interface	Network	NIC	IP Setup	IP Address	Subnet mask	Gateway	DNS
XENSERVER	Management	Network 0	NIC 0	DHCP	192.168.1.39	255.255.255.0		

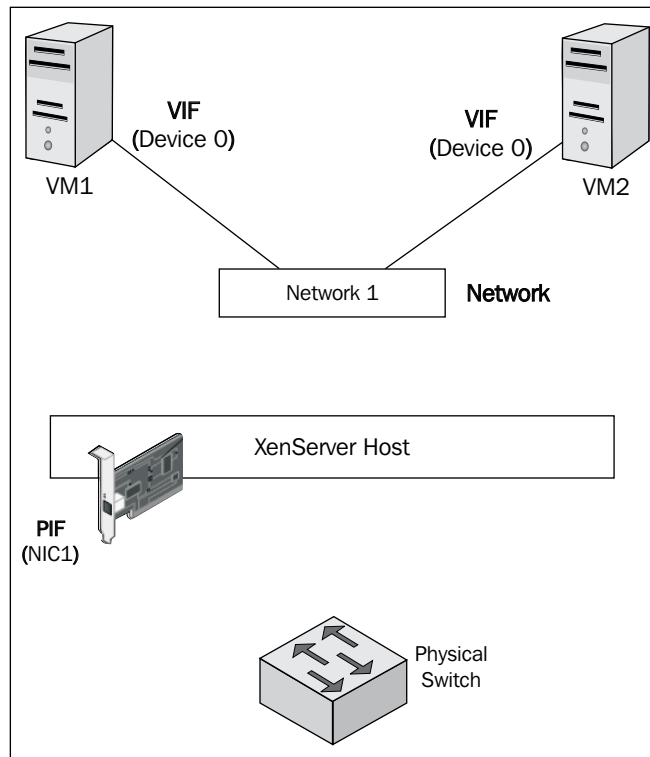
At the bottom of the IP configuration section is a 'Configure...' button.



The bonded network can be renamed after the bond is created, as there is no option to enter a bond name during the creation process.

Single-server private

The single-server private network type is an internal XenServer network that has no physical network interface connected to the virtual switch. The lack of a physical network interface to act as an uplink to the physical network isolates the virtual machines on the virtual network from the rest of the network. This network type is most commonly used for security purposes to control what traffic can reach the isolated virtual machines. In such a scenario, a virtual machine is deployed to act as a router between an isolated virtual network and a virtual network with an associated physical interface. This is shown in the following diagram:

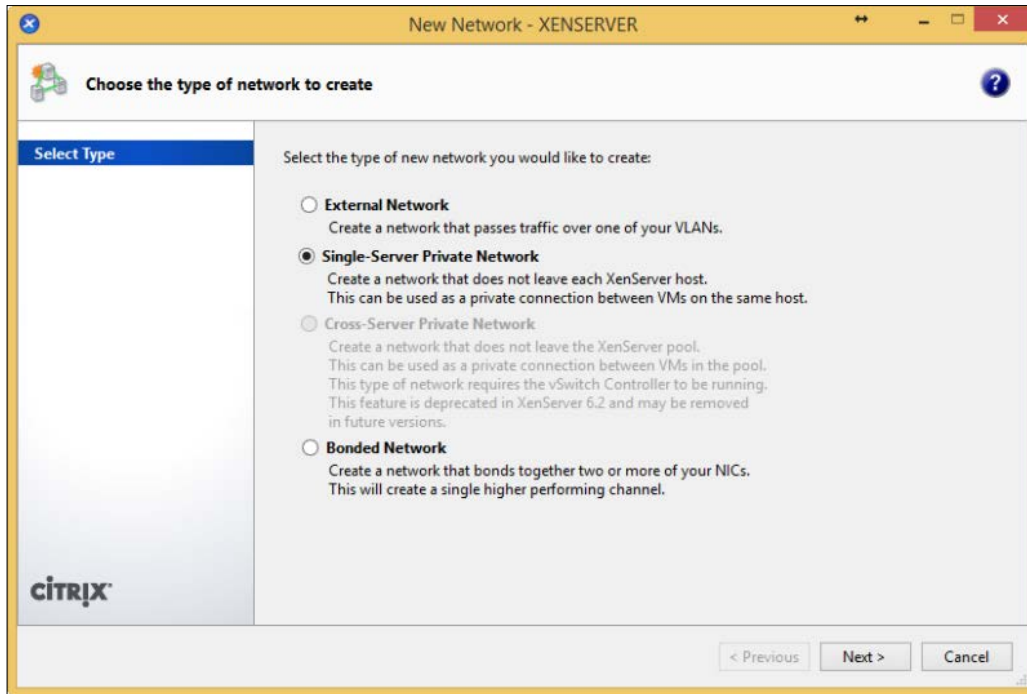


The single-server private network configuration

The following steps show you how to configure a single-server private network using the XenCenter GUI:

1. Click on the **Add Network** button under the **Networking** tab of the XenServer host.

2. Select the **Single-Server Private Network** option and click on **Next** to continue.



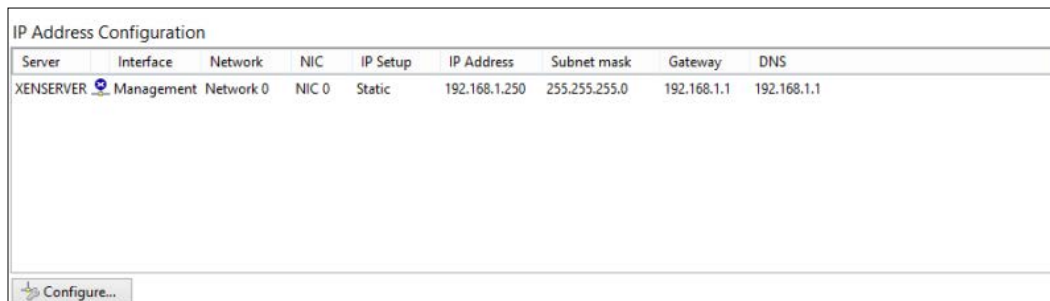
3. Provide a name and description for the new network. Click on **Next** to continue.
4. Check whether the network should be automatically added to new virtual machines and select **Finish** to complete the configuration.

Cross-server private

The cross-server private network type is used to extend the single-server private network across multiple hosts in a XenServer pool. This configuration provides the benefit of being able to use an additional XenServer host to host the virtual machines. The primary management interface for configuring cross-server private networks is the **Distributed Virtual Switch Controller (DVSC)**, which is provided by Citrix as a virtual appliance, so that the Open vSwitches on the XenServer hosts can connect to support the centralized configuration.


The management interface

The XenServer management interface is responsible for the communication between the host and the other components on the network. The management interface is also used for inter-host communication between the hosts in a XenServer pool. The management interface is configured during the installation process in which the physical interface that acts as the management interface is selected along with the desired network providing the addressing information, as shown in the following screenshot:



Server	Interface	Network	NIC	IP Setup	IP Address	Subnet mask	Gateway	DNS
XENSERVEN	Management	Network 0	NIC 0	Static	192.168.1.250	255.255.255.0	192.168.1.1	192.168.1.1

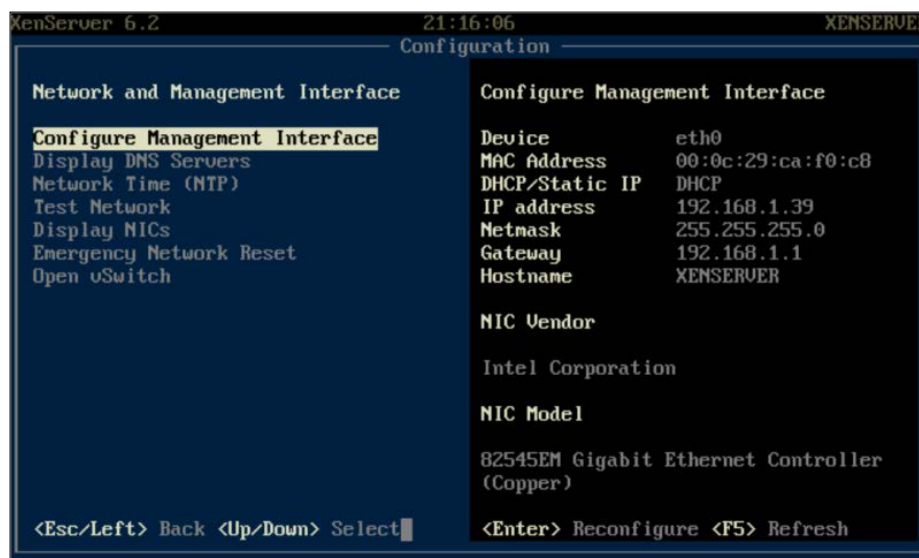
The management interface settings can be found under the **IP Address Configuration** section under the **Networking** tab in XenCenter.

 A host with a bonded management interface cannot join a XenServer pool. The bond must be removed before the host can join the pool.

The management interface configuration

The following steps show you how to reconfigure the management interface from the physical server's console:

1. At the server's physical console, type `xsconsole` to access the management console.
2. Use the arrow keys to select the **Network and Management Interface** option and press *Enter*.
3. Select the **Configure Management Interface** option and press *Enter*.



```
XenServer 6.2                21:16:06                XENSERVER
----- Configuration -----
Network and Management Interface
Configure Management Interface
Display DNS Servers
Network Time (NTP)
Test Network
Display NICs
Emergency Network Reset
Open vSwitch

Device          eth0
MAC Address     00:0c:29:ca:f0:c8
DHCP/Static IP  DHCP
IP address      192.168.1.39
Netmask         255.255.255.0
Gateway         192.168.1.1
Hostname        XENSERVER

NIC Vendor
Intel Corporation

NIC Model
82545EM Gigabit Ethernet Controller
(Copper)

<Esc/Left> Back <Up/Down> Select <Enter> Reconfigure <F5> Refresh
```

4. When prompted, enter the appropriate credentials and press *Enter* to continue.
5. Select the desired physical interface that is to be used as the management interface and press *Enter* to proceed.
6. Select the appropriate IP address assignment method and press *Enter* to continue.

7. Enter the appropriate information for the desired network configuration and press *Enter* until presented with the next screen, as shown in the following screenshot:

```
XenServer 6.2 21:19:39 root@XENSERVER
Configuration
Network and Management Interface  Configure Management Interface
Configure Management Interface
Device eth0
Display DNS Servers MAC Address 00:0c:29:ca:f0:c8
Network Management Interface Configuration
Test Ne Enter static IP address configuration
Display IP Address 192.168.1.250
Emergen Netmask 255.255.255.0
Open uS Gateway 192.168.1.1
Hostname XENSERVER
<Enter> OK <Esc> Cancel
82545EM Gigabit Ethernet Controller (Copper)
<Esc/Left> Back <Up/Down> Select <Enter> Reconfigure <F5> Refresh
```

8. Press *Enter* to apply the entered settings.

```
XenServer 6.2 21:20:48 root@XENSERVER
Configuration
Network and Management Interface  Configure Management Interface
Conf Management Interface Configuration
Disp Press <Enter> to apply the following configuration
Netu Device eth0
Test Name 82545EM Gigabit Ethernet Controller (Copper)
Disp IP Mode Static
Emer IP Address 192.168.1.250
Open Netmask 255.255.255.0
Gateway 192.168.1.1
Hostname XENSERVER
<Enter> OK <Esc> Cancel
82545EM Gigabit Ethernet Controller (Copper)
<Esc/Left> Back <Up/Down> Select <Enter> Reconfigure <F5> Refresh
```



Extreme caution should be taken when modifying the management interface of a host due to the potential impact on other hosts in the XenServer pool. XenCenter's connectivity to the management interface will be lost if the network settings have been changed.

Dedicated IP storage NICs

XenServer supports dedicating physical network interfaces just to carry the IP storage traffic. In many production environments, the storage and production network traffic are segregated to ensure that there is no contention for resources. Given the importance of storage traffic, it is critical to ensure that the network traffic doesn't slow down or disrupt the IP storage traffic. The dedicated storage NIC is a secondary management interface, which is assigned an IP address, that is on a separate subnet other than the primary management interface. The physical network interfaces carrying the storage traffic can be bonded in order to provide improved performance and redundancy.

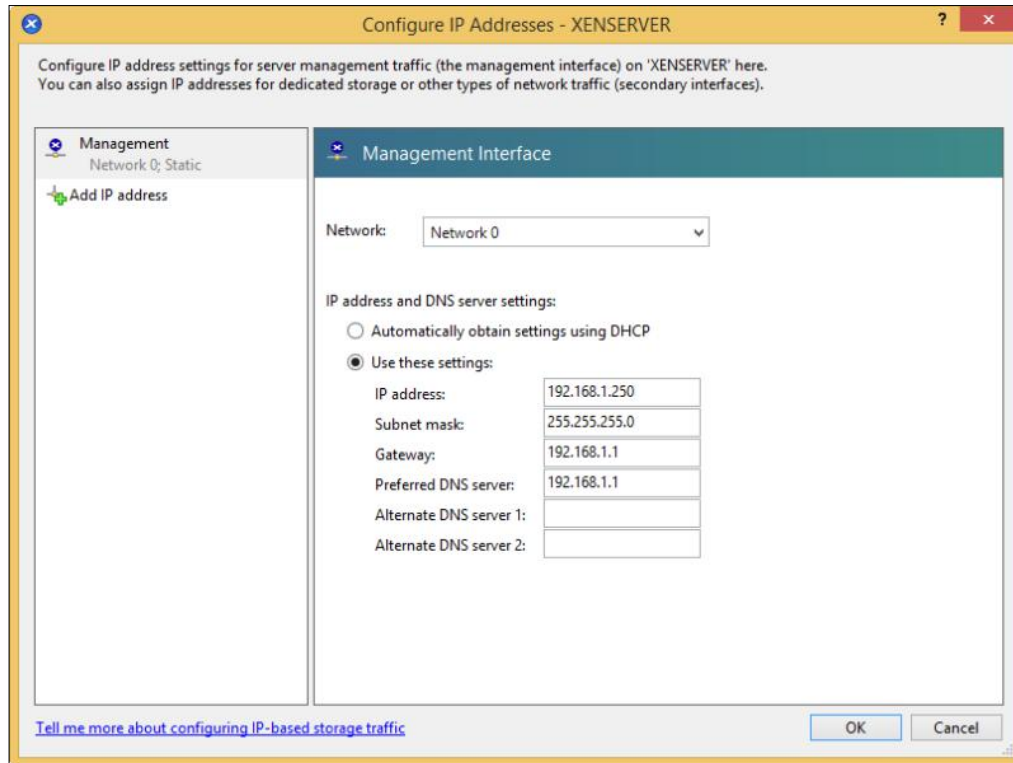


If a network bond is used, it must be created prior to assigning the IP address to one of the physical interfaces.

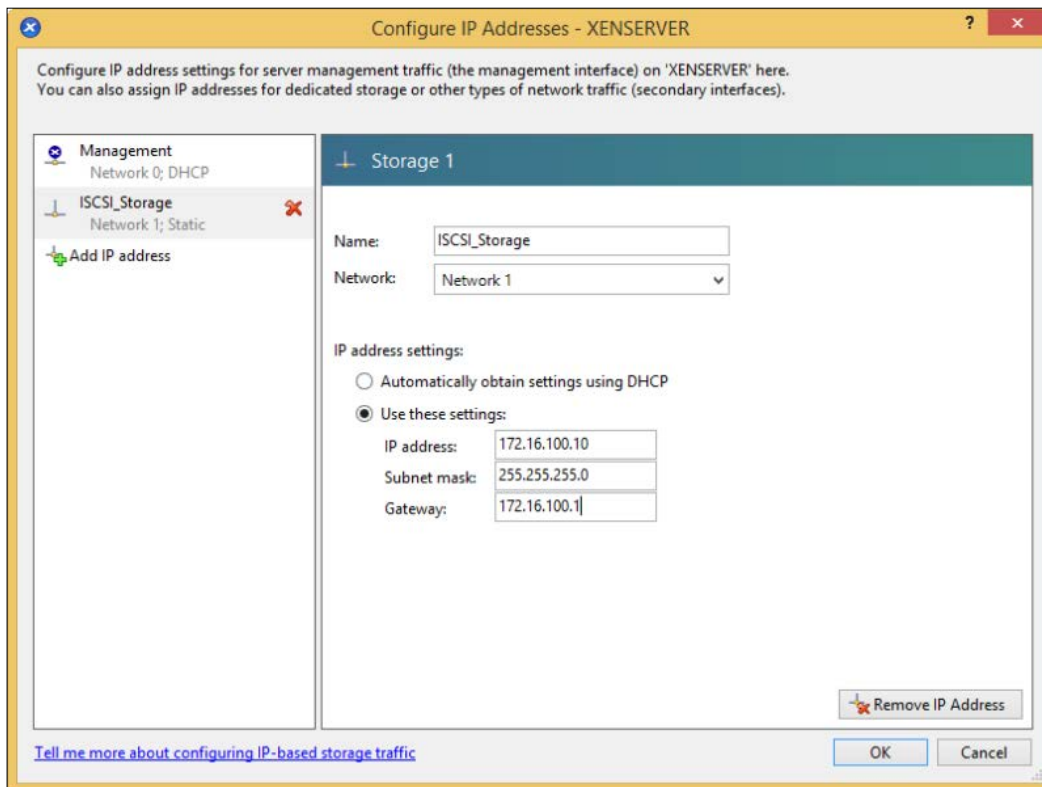
The following steps show how to configure dedicated IP storage NICs:

1. On the **Networking** tab of the XenServer in XenCenter, click on **Configure** under the **IP Address Configuration** section.

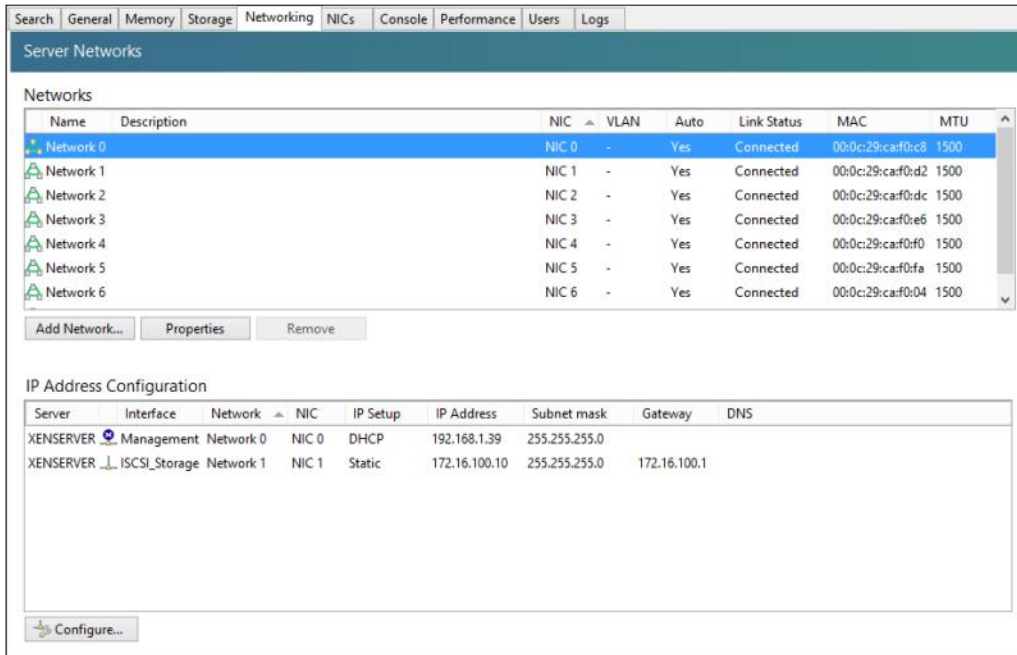
2. Click on **Add IP address** to create a secondary interface.



3. Provide a name for the secondary interface, select the associated network, and configure the network settings. Click on **OK** to apply the settings.



- The new secondary interface should now appear in the **IP Address Configuration** section.



Bonding

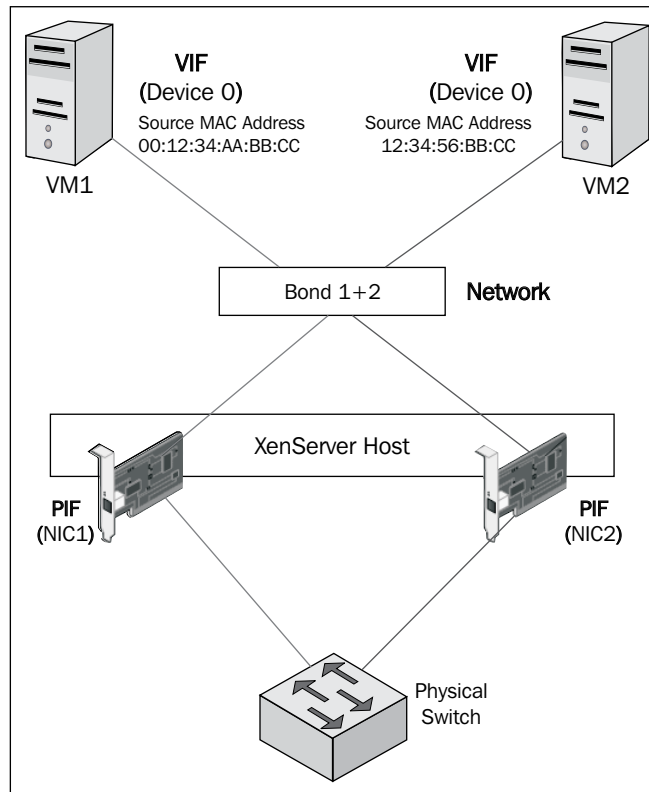
The following sections examine the bonding algorithms that are available in Citrix XenServer 6.2.

Active-active bonding

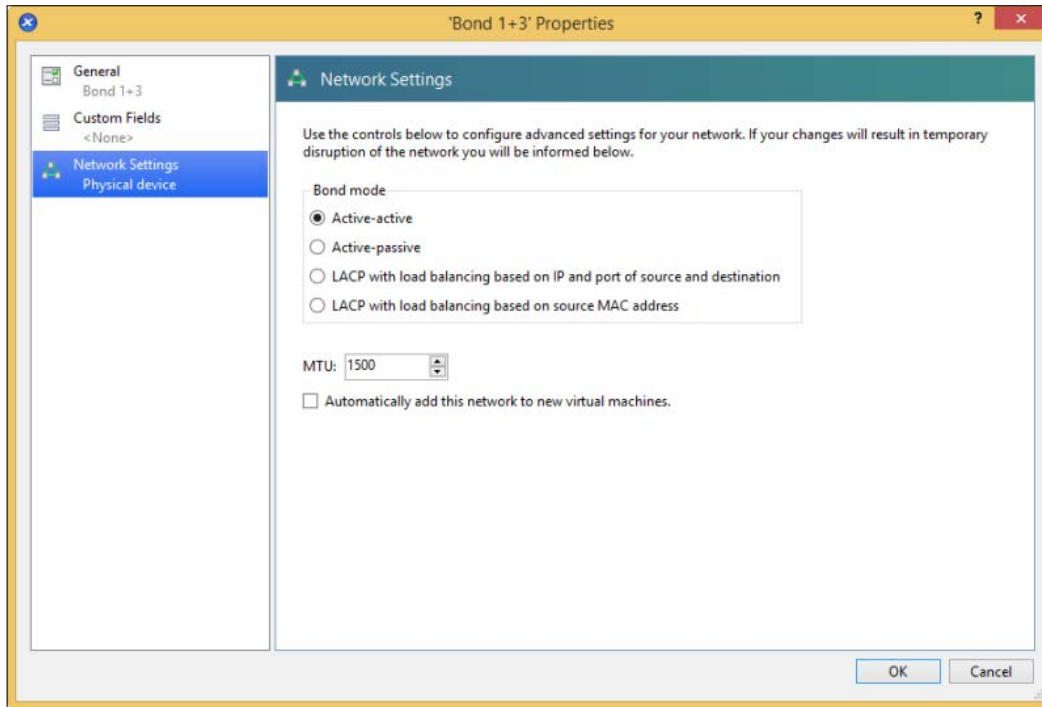
The active-active bonding is the default bond mode of XenServer for both the Linux bridge and vSwitch network backends. The full functionality of the active-active bond mode is only utilized by the virtual machine traffic, which can be load balanced across as many as four physical interfaces. The following are the restrictions for utilizing active-active bonding:

- Management traffic can only use one NIC at a time to pass the traffic
- Storage traffic can only use one NIC at a time to pass the traffic

Active-active bonding utilizes the source MAC address as the basis for load balancing packets. This is why management and storage traffics cannot be load balanced using the active-active bonding algorithm, considering that each one uses only a single MAC address for the network traffic. Active-active bonding dynamically rebalances the traffic at 30-minute intervals based on the amount of traffic each physical interface sends and receives during a given period of time. This is shown in the following diagram:

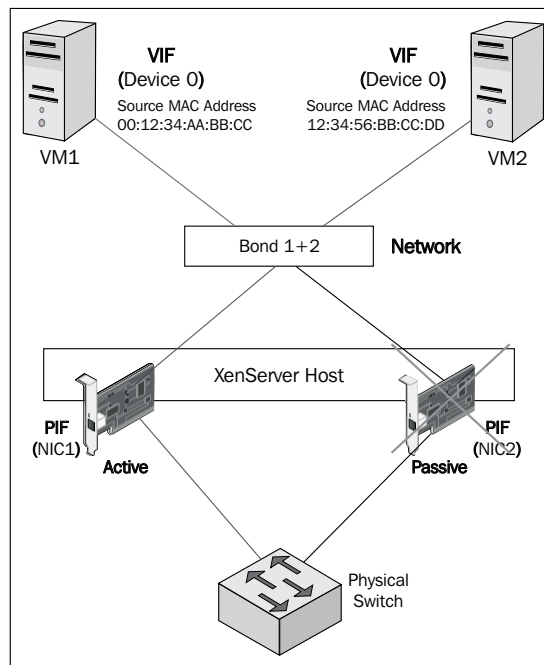


The bonding algorithm can be modified by accessing the **Properties** section of the network under the **Networking** tab in XenCenter, as shown in the following screenshot:

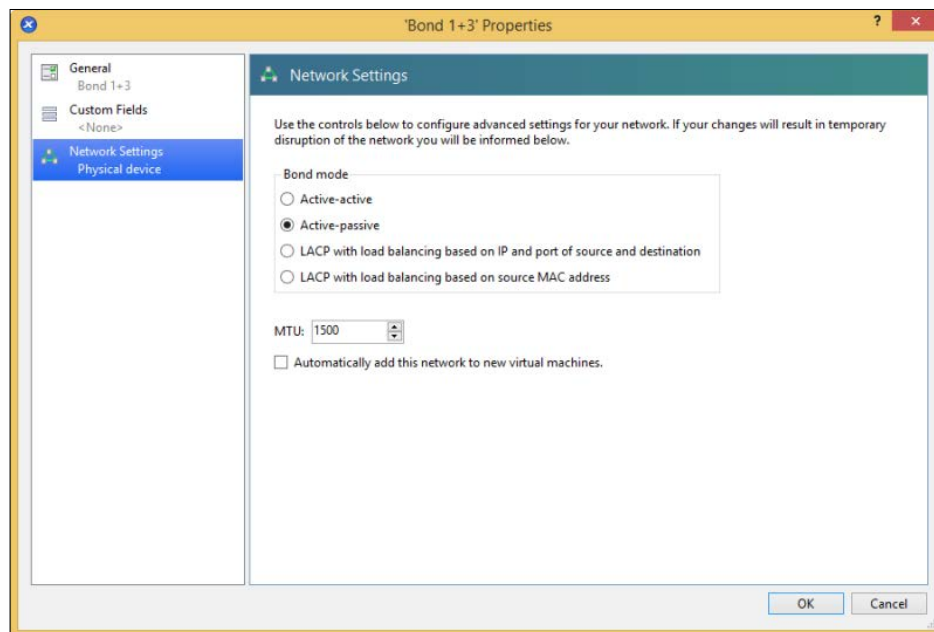


Active-passive bonding

The active-passive bonding only passes traffic over a single physical interface and the other physical interfaces in the bond are in a standby state, becoming active only when the active link fails. This bonding algorithm provides redundancy but does not provide any additional performance functionality, as shown in the following diagram:

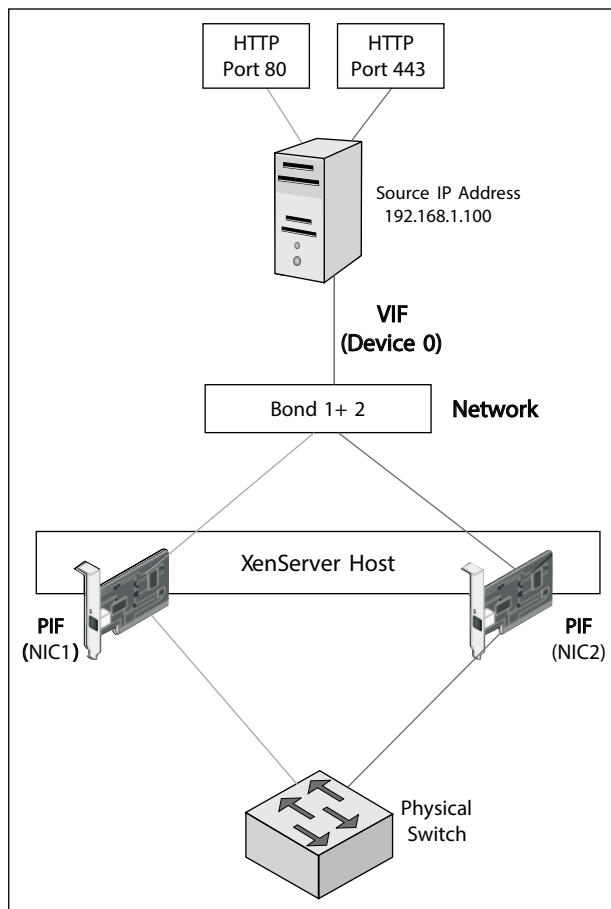


The bonding algorithm can be modified by accessing the **Properties** section of the network under the **Networking** tab in XenCenter:

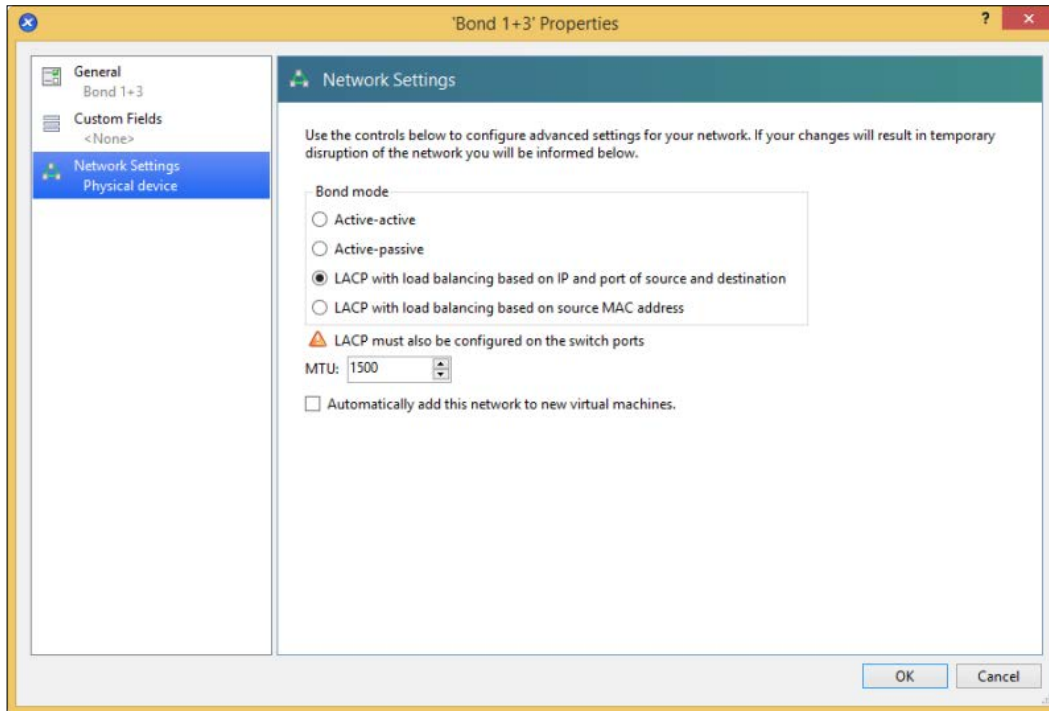


LACP IP and port hash

The IP and port hash algorithm is the default algorithm that is used when **Link Aggregation Control Protocol (LACP)** is enabled. LACP requires OVS on the XenServer host(s) as well as additional configuration on the physical switches, which need to support the 802.3ad (LACP) protocol. The algorithm uses a variation of source and destination IP or port numbers to distribute the network traffic. This allows a more even distribution of traffic given that a single virtual machine can make use of multiple physical interfaces to pass the traffic in comparison to the other bonding algorithms. Have a look at the following diagram:

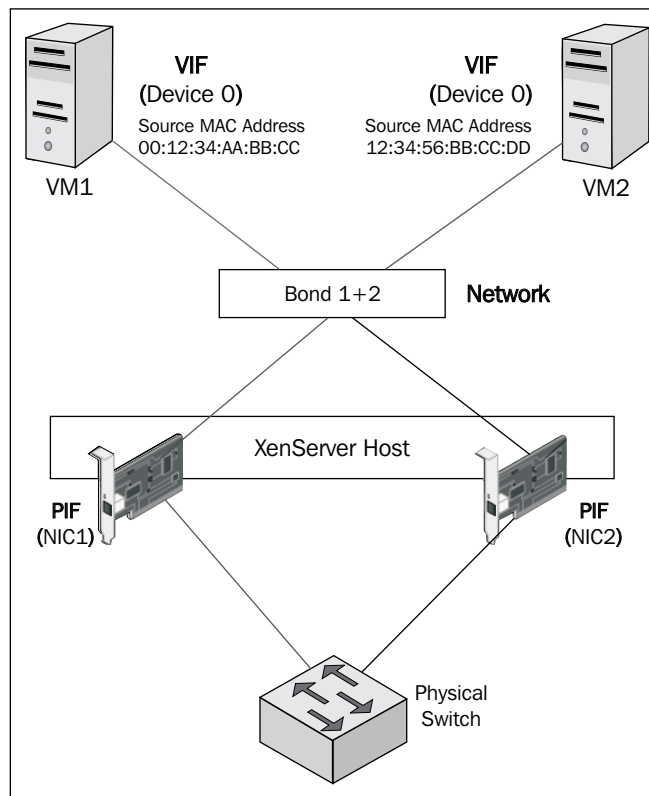


The bonding algorithm can be modified by accessing the **Properties** section of the network under the **Networking** tab in XenCenter, as shown in the following screenshot:

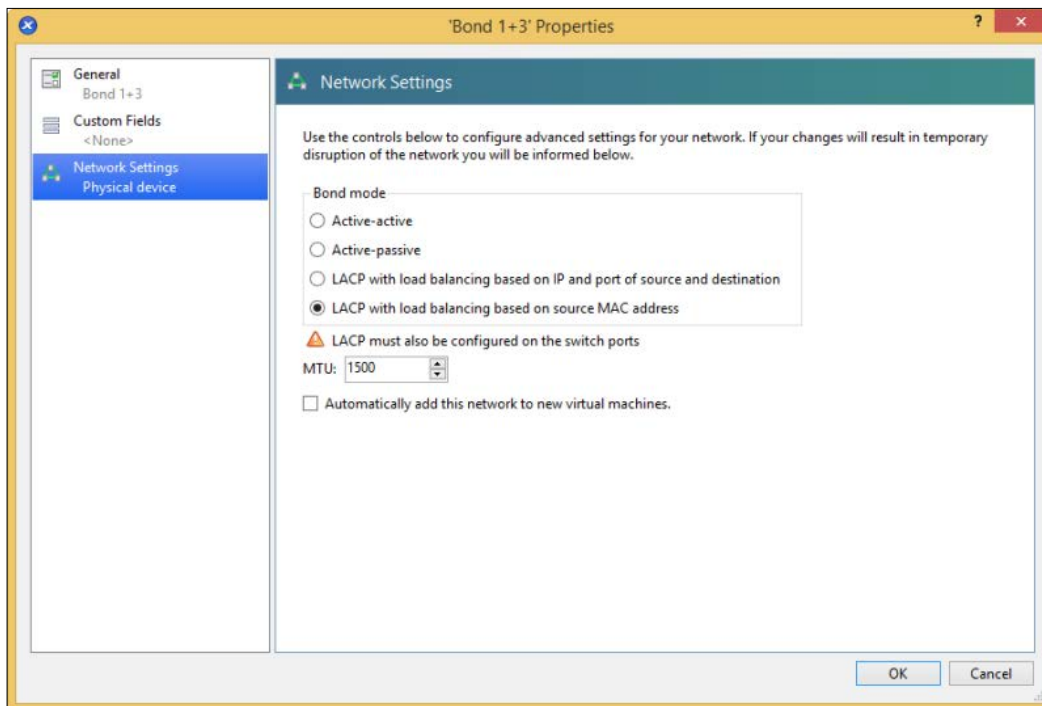


The LACP source MAC address

The source MAC address load balancing algorithm balances traffic based on the MAC address of the virtual machine. As traffic leaves the virtual network, the physical interface used is determined based on the MAC address of the virtual machine and sends the packet out to the designated physical interface. With the source MAC address algorithm, traffic from a single virtual machine is not balanced among the physical interfaces, but the group of virtual machines that are attached to a virtual network are placed each onto a particular physical interface. This method of load balancing would be used when there are multiple virtual machines attached to a virtual network. Have a look at the following diagram:



The bonding algorithm can be modified by accessing the **Properties** section of the network under the **Networking** tab in XenCenter, as shown in the following screenshot:



Virtual Local Area Networks

Virtual Local Area Networks (VLANs) are used to logically partition a physical network for security, performance, or management reasons. Citrix XenServer supports the use of VLANs and can handle the VLAN tagging/untagging process in many scenarios.

XenServer® VLAN support

The following list breaks down XenServer VLAN support based on the traffic type.

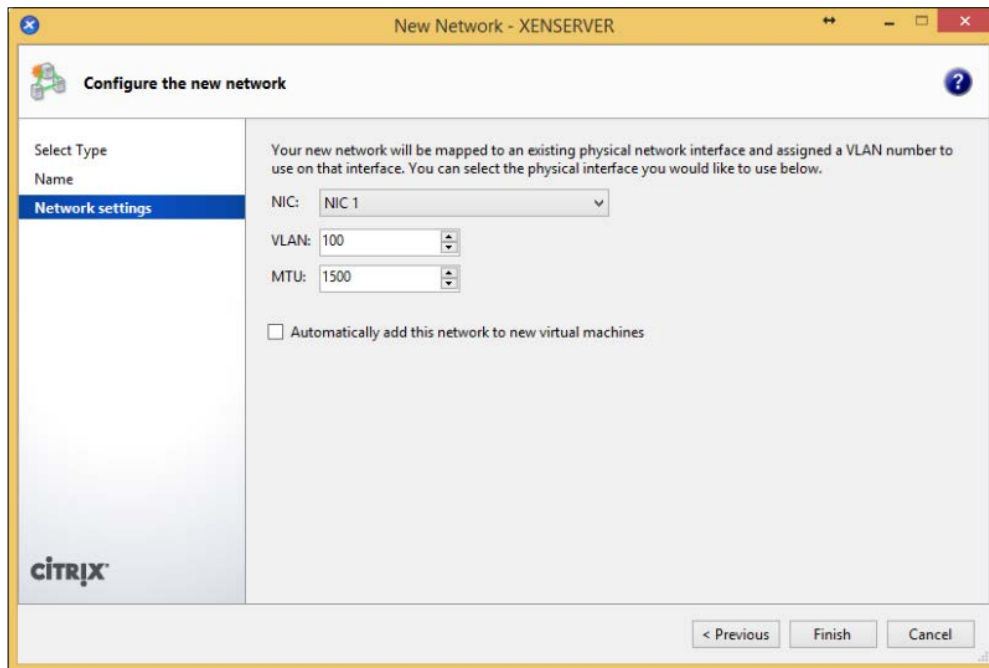
- **Management traffic:** Assigning a VLAN to the management interface is not supported by the management interface. The management interface supports a single access VLAN or the native VLAN that is configured on the physical switch.

- **Dedicated IP storage traffic:** Dedicated storage NICs support both the native VLAN/access mode configuration as well as a trunked port.
- **Virtual machines:** Virtual machines support virtual networks that use both native VLAN/access mode configuration along with the trunked port configuration.

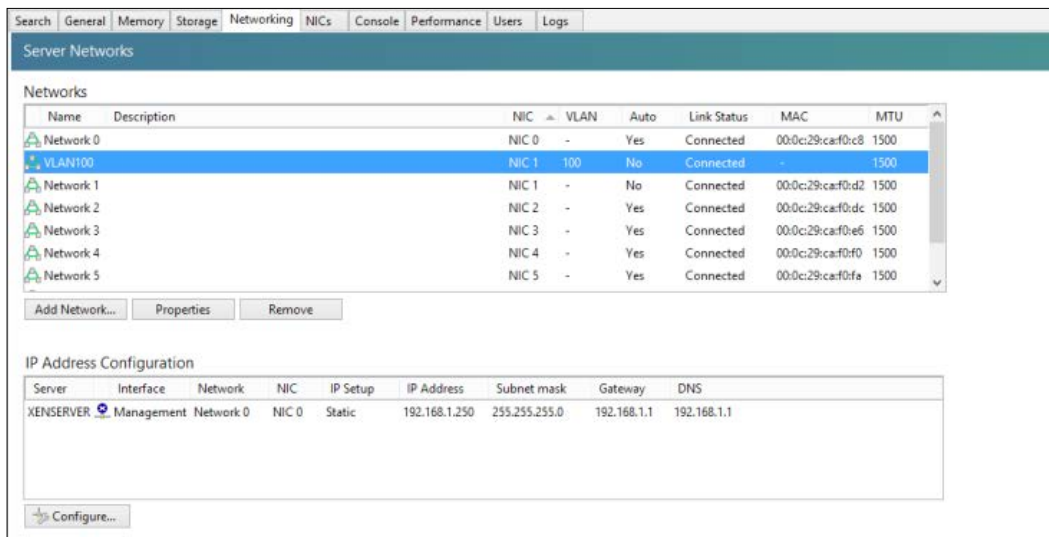
Configuring VLANs

The following steps show you how to configure a VLAN on a XenServer network using the XenCenter GUI:

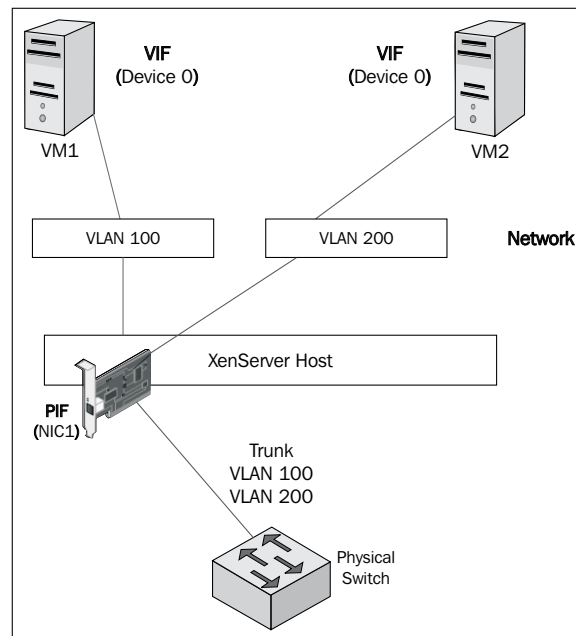
1. Click on the **Add Network** button under the **Networking** tab of the XenServer host.
2. Select the **External Network** option and click on **Next** to continue.
3. Provide a name and description for the new network.
4. Select the desired physical interface, **VLAN**, **MTU**, and check whether the network should be automatically added to the newly created virtual machines. Click on **Finish** to create the new network.



5. The new network should now appear under the **Networking** tab of the XenServer host. The VLAN ID should show under the **VLAN** column.



The following diagram shows the common configuration for XenServer, where the port on the physical switch is a trunk port carrying multiple VLANs and multiple XenServer networks that are created with the corresponding XenServer physical interface for that port. In this scenario, each XenServer network or virtual switch is used to carry traffic for a particular VLAN.



QoS

Citrix XenServer 6.2 supports rate limiting or throttling the egress traffic of a virtual machine. XenServer does not provide any native functionality for limiting the ingress traffic of a virtual machine. QoS can only be configured through the DVSC or from the command line when the Open vSwitch backend is enabled. The following is an example of a possible QoS configuration:

- Enable rate limiting on the VIF of the desired virtual machine:


```
xe vif-param-set uuid=<vif_uuid> qos_algorithm_type=ratelimit
```
- Apply the desired limit in **kilobits (kbps)** to the virtual interface:

```
xe vif-param-set uuid=<vif_uuid> qos_algorithm_params:kbps=100
```

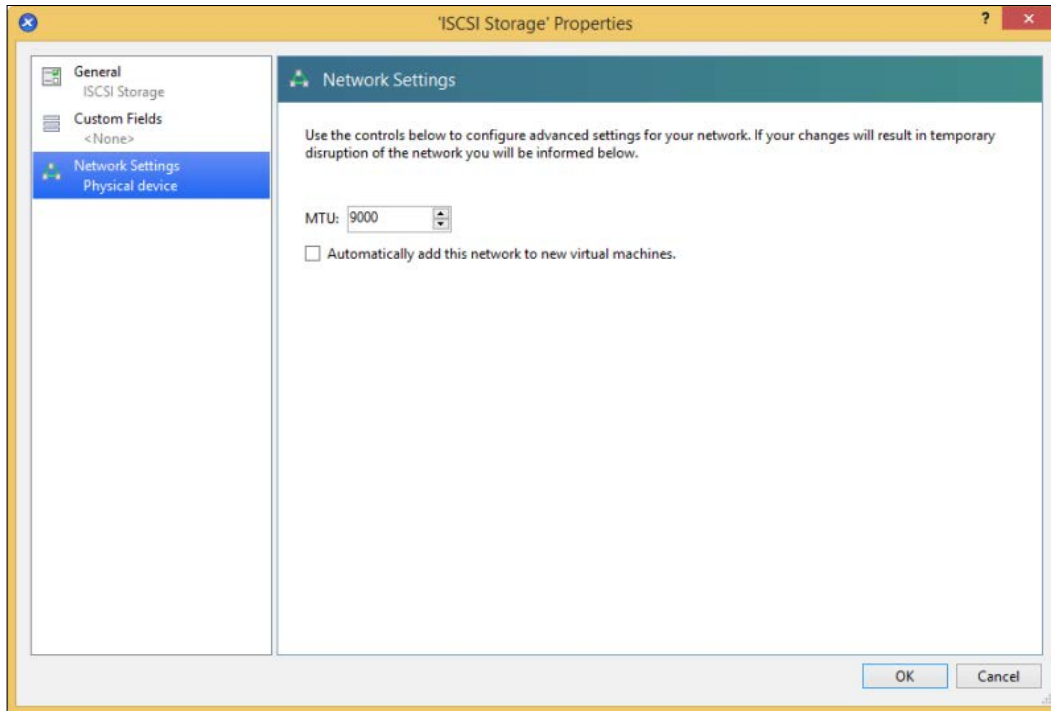
Jumbo frames


In the virtualization space, jumbo frames are commonly used to improve performance for implementations utilizing iSCSI for the storage backend. Jumbo frames are Ethernet frames carrying more than the standard 1,500 bytes of payload data. The configuration of jumbo frames involves modifying the **Maximum Transmission Unit (MTU)** on the network components from the XenServer host to the iSCSI storage target as well as the devices in between. The MTU is generally changed from 1,500 to 9,000 or 9K. Jumbo frames can reduce the CPU utilization by reducing the number of network packets that need to be processed, considering that more data is contained in each packet with jumbo frames. This only applies to packets that are large enough to fill the jumbo frame. The following are the jumbo frame requirements:

- All XenServer hosts in the pool must use vSwitch as the network backend
- Jumbo frames must be supported and configured end to end

[ Jumbo frames are not supported for use on VMs.]

The following screenshot shows how to configure the MTU for a XenServer network:



[ The MTU cannot be changed on a network that has already been assigned an IP address.]

Network troubleshooting

As XenServer is built on top of Linux, there are inherently a number of tools that are available for network troubleshooting purposes. The best place to start troubleshooting is always working up through the OSI model to ensure that a methodical approach is taken. The following is a list of commands and utilities that are useful when troubleshooting:

- The following command lists the physical interfaces on the XenServer host:
`XE PIF-LIST`
- The following command lists the virtual networks on the XenServer host:
`XE NETWORK-LIST`
- The following command lists the virtual interfaces on a virtual machine:
`XE VM-VIF-LIST UUID=VM_UUID`
- The following command lists the virtual interfaces of the VMs on the XenServer host:
`XE VIF-LIST`
- The following command scans the XenServer host for new physical interfaces:
`XE PIF-INTRODUCE`
- The following command displays or can change the settings on the physical interface:
`Ethtool`
- The following command shows the packet analyzer:
`Tcpdump`

Emergency Network Reset

In the event that networking on a XenServer host is no longer functioning properly, the **Emergency Network Reset** feature can be used as a last resort. This feature removes all the configurations for the networking on the XenServer host and should only be used after all the other options have been exhausted. The **Emergency Network Reset** feature is initiated from the `xsconsole` at the server's physical console under the **Network and Management Interface** section, as shown in the following screenshot:

```
XenServer 6.2                21:01:35                root@XENSERVER1
----- Configuration -----
Network and Management Interface
Configure Management Interface
Display DNS Servers
Network Time (NTP)
Test Network
Display NICs
Emergency Network Reset
Open vSwitch

Emergency Network Reset
This command will reboot the host and
reset its network configuration.

As part of this utility all running
VMs will be forcefully shutdown.

Before running this command:
- Shutdown running VMs.
- Disable HA if enabled on the pool.

<Esc/Left> Back <Up/Down> Select | <Enter> Reset Networking
```

Summary

In this chapter, we looked at the components that are a part of XenServer networking as well as XenServer network types. We addressed how to configure XenServer management interfaces, dedicated IP storage, network bonds, jumbo frames, and VLANs. We also covered some helpful commands which can be used when troubleshooting a XenServer networking issue.

In the next chapter, we will learn about Citrix XenServer storage.

3

Planning and Configuring XenServer® Storage

Now that we have configured the networking piece of our XenServer deployment, let's move on to the other integral component of a XenServer deployment, which is XenServer storage. Storage plays a critical role in virtualized solutions and can often be the primary bottleneck for performance and scalability.

In this chapter, we will cover the following topics:

- XenServer storage overview
- XenServer storage components
- Storage repositories
- Managing storage repositories

XenServer® storage overview

Citrix XenServer 6.2 provides administrators with the ability to use various common storage protocols to access storage. In a typical deployment, XenServer will make use of local storage drives, SATA or SAS, to store virtual machines, and a Windows or Linux file server to store ISO images for guest OS installations. In larger deployments that require the use of shared storage, protocols such as NFS, iSCSI, Fibre Channel, and **Fibre Channel over Ethernet (FCoE)** can be used to provide access to centralized storage resources, which allow administrators to take advantage of XenServer features such as High Availability, XenMotion, and Disaster Recovery.

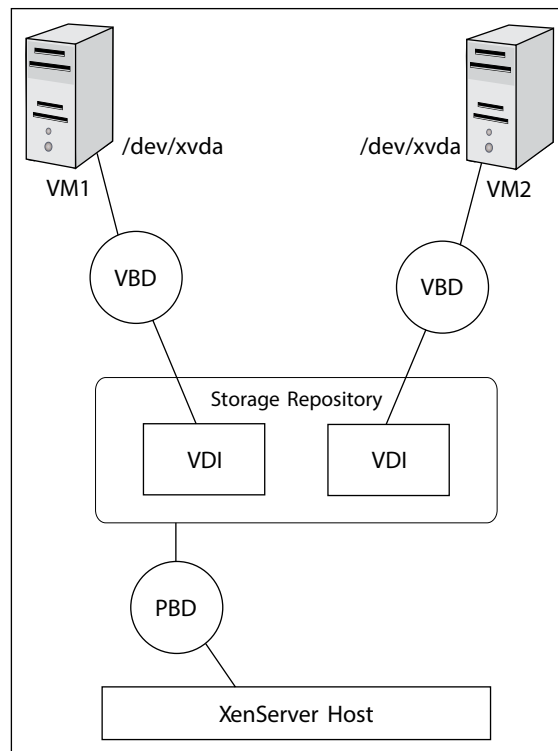
Supported storage protocols

The following protocols are supported in Citrix XenServer 6.2:

- **Network File System (NFSv3):** Citrix XenServer 6.2 supports NFSv3 for both ISO and VM storage. NFS is commonly used on a Linux server to provide file-share access. NFS uses TCP/IP to transmit data and it is recommended to use a link that is a gigabit or larger in size.
- **Fibre Channel:** This is the most common protocol used in storage networks and is known for its low latency as well as speed. Fibre Channel requires a Fibre-Channel-specific host bus adapter for the XenServer; it also requires Fibre Channel switches and a storage array that support Fibre Channel. Fibre Channel installations are often very costly, but Fibre Channel is typically chosen for its robust functionality and performance. It is available in speeds of 1, 2, 4, 8, or 16 gigabit.
- **FCoE:** This provides converged access to resources by allowing a single connection to transport both network and storage connections. FCoE is a newer protocol that offers several advantages, such as reduced cabling, reduced host adapters, and the ability to utilize a majority of the existing network infrastructure. FCoE is available at the speed of 10 gigabit.
- **iSCSI:** This protocol utilizes TCP/IP to transmit SCSI commands and provides the ability to make use of the existing network infrastructure to provide shared storage access. The iSCSI protocol is generally deployed using gigabit Ethernet connections that are commonplace in most computer networks today.
- **Common Internet File System (CIFS):** Citrix XenServer 6.2 supports CIFS only for ISO storage use. The CIFS file protocol is most commonly used by Windows file servers to provide file-share access. Administrators in environments that are primarily Windows based, typically make use of the CIFS protocol to provide XenServer access to ISO files.
- **IDE, SATA, and SAS:** Citrix XenServer 6.2 supports several disk types for local storage use. SAS disks generally provide the best performance and reliability in comparison to IDE and SATA.

XenServer® storage components

The primary Citrix XenServer storage components are **Physical Block Device (PBD)**, **Virtual Disk Images (VDIs)**, **Virtual Block Device (VBD)**, and **Storage Repository (SR)** that provide the layer of abstraction. The following diagram displays how each of the pieces fits together to form the XenServer storage architecture:



PBD

PBDs are connector objects that contain the mapping data of the connection between the XenServer host and storage target, such as an NFS share or an iSCSI **Logical Unit Number (LUN)**. The PBD manages the connection with the local storage subsystem on the XenServer host to provide access to the local storage along with any remote storage the host is connected to. The following screenshot lists the PBD information on a XenServer host:

```

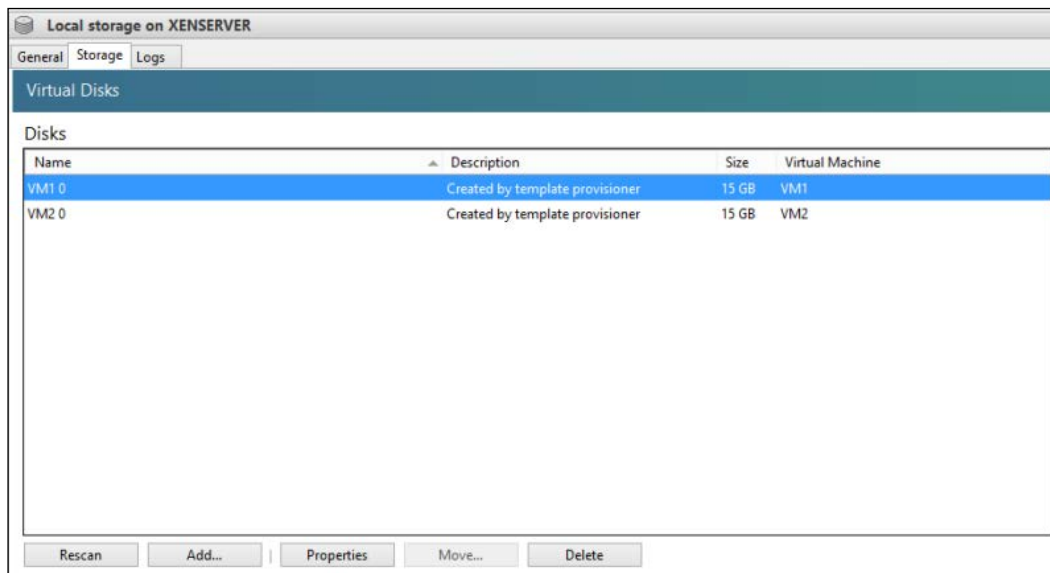
[root@XENSERVER3 ~]# xe pbd-list
uuid ( RO)                : 23205104-8812-05e9-2642-ed25cda2a8bc
  host-uuid ( RO)         : ffa12eeb-d06c-417c-9504-3938f9205a56
  sr-uuid ( RO)           : 9a17db92-a252-15e5-8938-bc408f52790d
  device-config (MRO)     : location: /opt/xensource/packages/iso; legacy_mode: true
  currently-attached ( RO): true

uuid ( RO)                : 389b1d29-3140-5809-7e35-ef5e2e91fc5d
  host-uuid ( RO)         : ffa12eeb-d06c-417c-9504-3938f9205a56
  sr-uuid ( RO)           : 66f9c208-a703-8150-1eae-2ccac3f67c06
  device-config (MRO)     : device: /dev/sdb
  currently-attached ( RO): true
  
```


The `xe pbd-list` command can be run from the XenServer host's console to list the PBDs on the XenServer host. The output also displays the connection state of the PBD to indicate whether it is currently attached or not.

VDIs

VDIs are represented to the virtual machine as a virtual abstraction of a physical hard drive. The virtual disk(s) reside on an SR and can be attached or detached from the virtual machine along with support to be moved from one repository to another. The VDIs on a XenServer host can be viewed from the **Storage** tab of the SR in the XenCenter management console, as shown in the following screenshot:

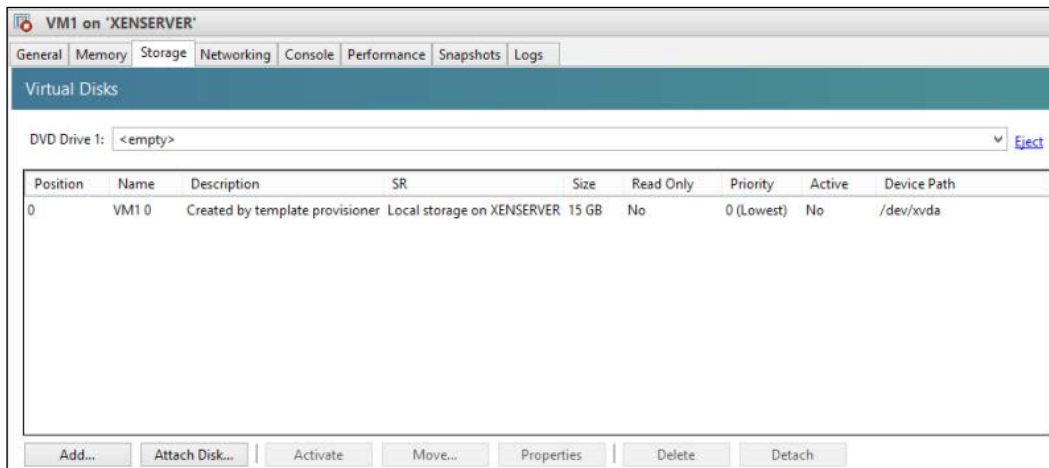


The VDI format

By default, Citrix XenServer utilizes the **Virtual Hard Disk (VHD)** to store virtual machine data. The VHD format is also utilized in Microsoft's Hyper-V product and is the default format used in XenServer. This format supports thin provisioning, which allows the disk to dynamically consume storage space, fast cloning, and snapshotting. Fast cloning is a feature that allows VDIs to be cloned in a matter of seconds, through the use of the **Copy on Write (CoW)** technology. CoW creates a differencing disk for all the changes to the original VDI, and as data is modified, it is written to the differencing disks for the cloned VM instead of the original VDI. Snapshots provide administrators with a point-in-time copy of the VM, which is often used in development or test environments to quickly roll back any changes made to the VM.

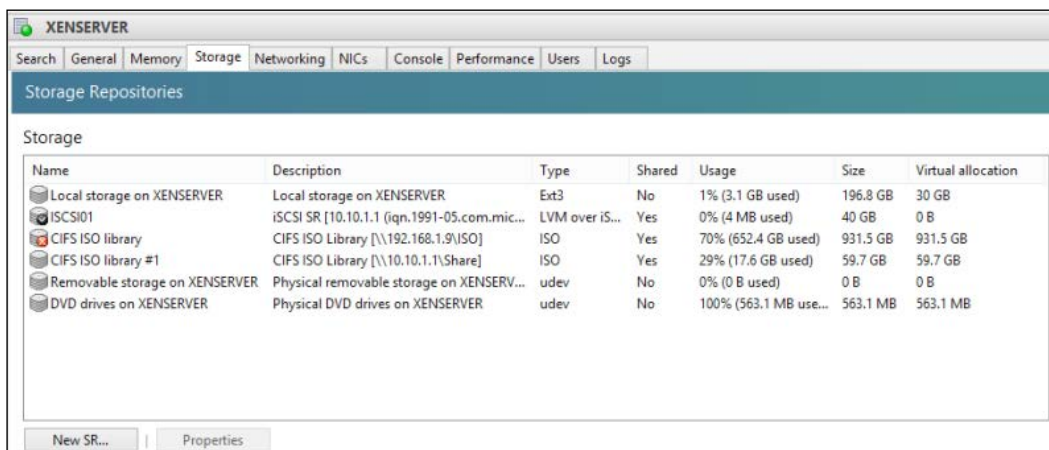
VBDs

VBDs contain the mapping data of the connection between the VDI and the virtual machine. The VBD can also be used to manipulate **Quality of Service (QoS)** and statistics. The following screenshot displays the connection between the VDI and the virtual machine:



SRs


SRs are container objects used to store VDIs for virtual machine VHDs and ISO files. The following screenshot displays the SRs on a XenServer host:



SRs can be found under the **Storage** tab of a XenServer host or pool.

ISO library SRs

ISO library SRs are used to store ISO files that are typically used to install the guest operating system on the XenServer virtual machines. XenServer supports the CIFS and NFS protocols to access ISO files.

 The permissions on the share used for the ISO library are typically set to read-only.

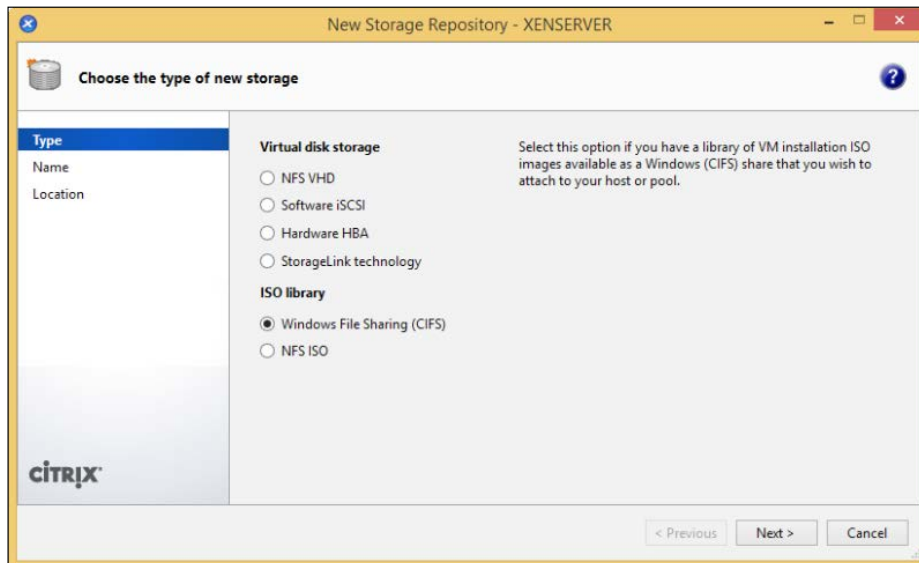
The CIFS ISO library

The CIFS ISO library storage repository utilizes the CIFS file protocol, which is commonly used by Windows file servers. The protocol is a Microsoft-enhanced version of the **Server Message Block (SMB)** protocol. A user account on the target file server is required in order for the XenServer to access the file share. The CIFS ISO library SR is typically only used in an environment with Windows servers, otherwise the NFS protocol is generally used.

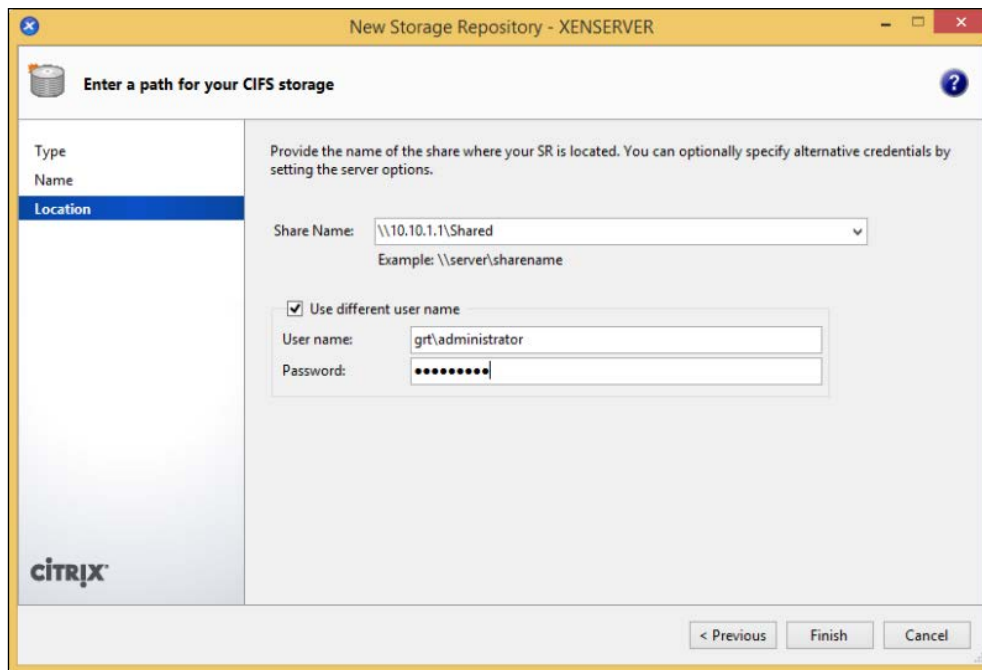
Adding a CIFS ISO library SR (using the GUI)

The following steps cover adding a CIFS ISO library SR on a XenServer host using the XenCenter GUI:

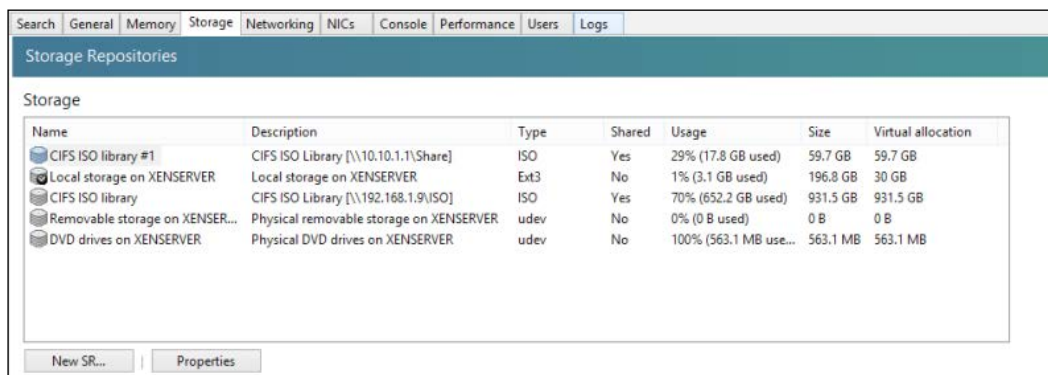
1. Select the desired XenServer host or pool and press the **New Storage** button on the toolbar.
2. Select the **Windows File Sharing (CIFS)** option and press **Next** to continue:



3. Provide a name and description for the storage repository and press **Next** to continue.
4. Enter **Share Name** of the CIFS share, check the **use different user name** box to enter a user account with access to the share, enter the user credentials, and press **Finish** to create the SR:



The newly created SR can be viewed under the **Storage** tab of the XenServer host or pool, as seen in the following screenshot:



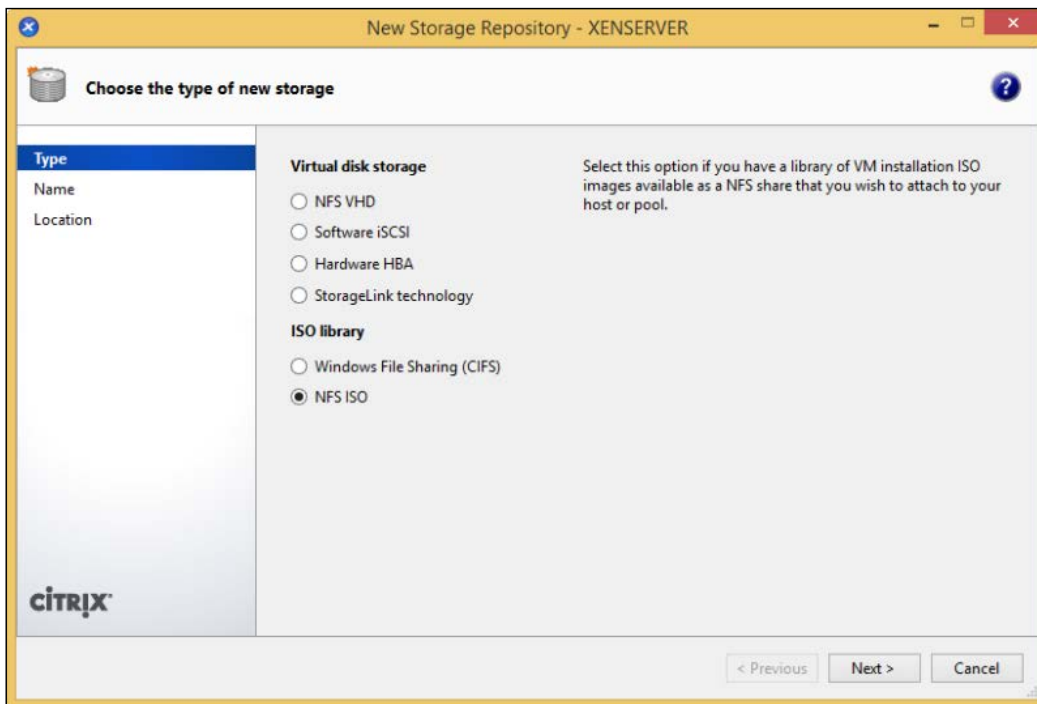
The NFS ISO library

The NFS ISO library SR utilizes the NFS file protocol, which is commonly used by Linux file servers. XenServer uses NFSv3, by default, to connect to the storage target.

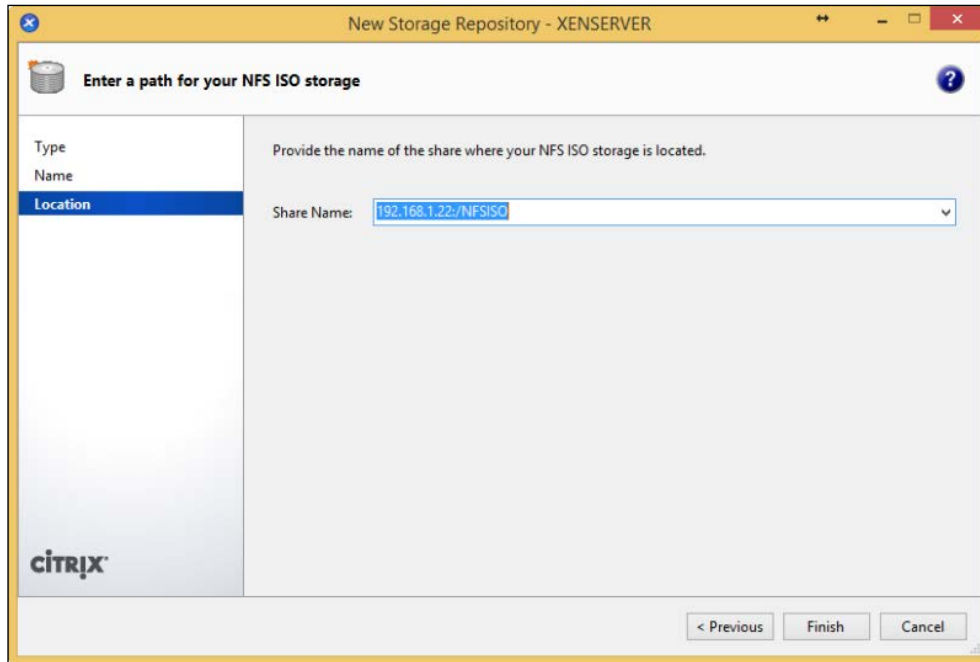
Adding an NFS ISO library SR (using the GUI)

The following steps cover adding an NFS ISO library SR on a XenServer host using the XenCenter GUI:

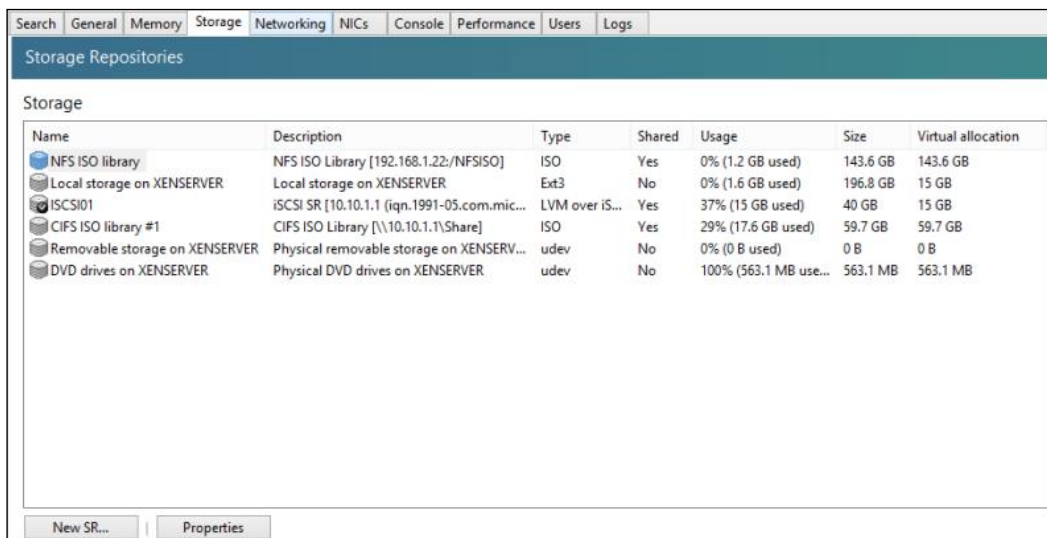
1. Select the desired XenServer host or pool, and press the **New Storage** button on the toolbar.
2. Select the **NFS ISO** option and press **Next** to continue:



- Provide a name and description for the SR and press **Next** to continue. After this, you get the following screen:



- The newly created SR can be viewed under the **Storage** tab of the XenServer host or pool, as shown in the following screenshot:



Adding an NFS ISO library SR (using the CLI)

The following steps cover how to add an NFS ISO library SR on a XenServer host using the `xe` command from the command-line interface:

1. Run the `xe sr-create` command to create an NFS ISO SR:

```
xe sr-create host-uuid=host_uuid content-type=iso type=iso name-label="sr_name" device-config:location=server_name:/share_name
```

2. The following screenshot shows how to add an NFS ISO SR:

```
[root@XENSERVER3 ~]# xe sr-create host-uuid=ffa12eeb-d06c-417c-9504-3938f9205a56 content-type=iso type=iso name-label="NFS_ISO" device-config:location=192.168.1.180:/NFSISO1b4e6f8e-98a0-7a64-c3ba-bd244d87e336
[root@XENSERVER3 ~]#
```

Virtual disk library SRs

Virtual disk library SRs are used to store VDIs. The virtual machine's guest hard disks reside on the SR. The five types of virtual disk storage repositories are listed as follows:

- **Local storage:** This includes locally attached storage, such as SAS, SATA, or SCSI disks, in the XenServer host. Local storage cannot be shared between XenServer hosts.
- **NFS VHD:** Virtual disks are hosted on an NFS share, which supports storage being shared among multiple hosts.
- **Software iSCSI:** Virtual disks are hosted on an iSCSI LUN, which supports storage being shared among multiple hosts.
- **Hardware HBA:** Virtual disks are hosted on a Fibre Channel LUN, which supports storage being shared among multiple hosts.
- **StorageLink technology:** Virtual disks are hosted on storage that supports the StorageLink technology feature.

Disk provisioning

Virtual disks support two types of provisioning, which determines whether the amount of space allocated to the virtual disk is consumed up front or on demand:

- **Thick provisioned:** Thick provisioned disks consume the entire amount of storage allocated to the disk when it is created. The advantage of this type of provisioning is that the space on the SR will never be overallocated, which could lead to running out of space on the SR along with better performance in comparison to a thin provisioned disk. The disadvantage of a thick provisioned disk is that it is typically underutilized and the space not in use cannot be shared with another VM that may need the space.
- **Thin provisioned:** Thin provisioned disks only consume the amount of space on the SR that the VM is actually using. An example is a VM with a 40 GB hard disk, which is only using 20 GB of that space. Only 20 GB is consumed on the SR but it is virtually allocated with 40 GB. The advantage of this type of provisioning is that space can be allocated dynamically to the VMs that are actually using the space on the SR. The drawback of this type of provisioning is the possibility of running out of space on the SR if not properly monitored.

The following table details the type of disk provisioning offered by each type of SR:

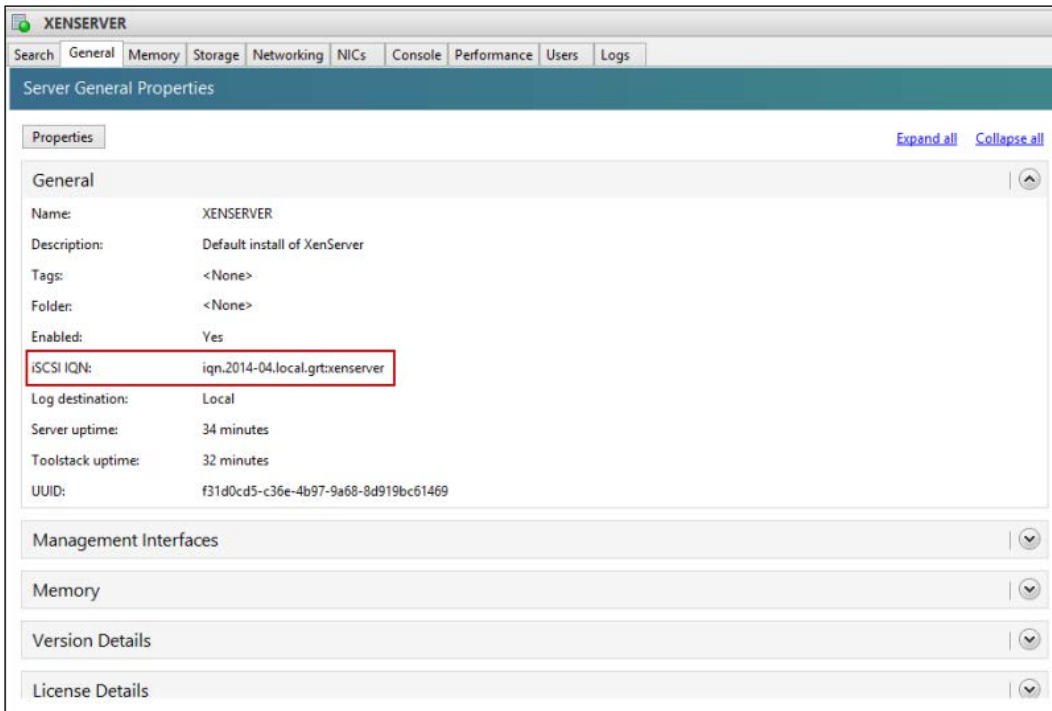
SR type	Storage type	Provisioning
LVM	Local	Thick
LVMoISCSI	iSCSI	Thick
LVMoHBA	Fibre Channel / SAS	Thick
NFS	NFS	Thin
Ext	Local	Thin

The software iSCSI virtual disk SR

The software iSCSI virtual disk storage repository utilizes the block-based iSCSI protocol to communicate with the storage target. VDIs that are hosted on iSCSI storage repositories are thick provisioned.

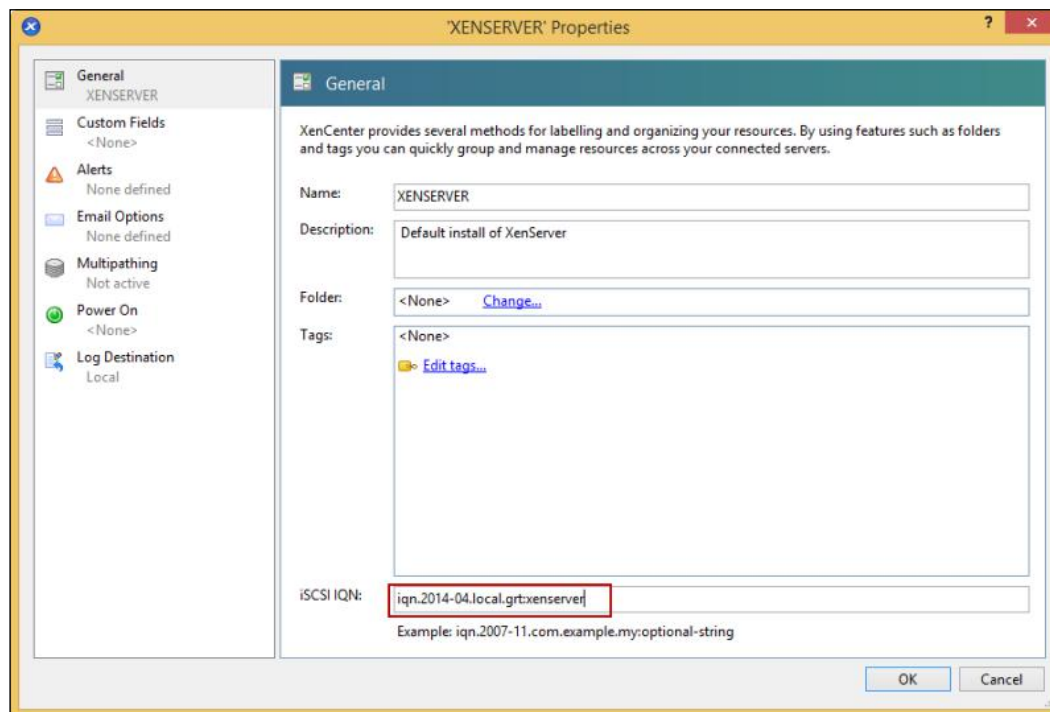
The software iSCSI initiator IQN

Each XenServer requires a unique **iSCSI Qualified Name (IQN)**, which is used while accessing iSCSI storage targets. A sample iSCSI IQN is shown in the following screenshot:



The configured IQN can be found under the **General** tab on the XenServer host.

Consider the following screenshot:



The IQN can be modified by accessing the host properties by pressing the **Properties** button under the **General** tab of the XenServer host. The iSCSI IQN can also be viewed from the command line using the `xe host-param-get` command to view the `iscsi_iqn` parameter for the host:

```
xe host-param-get uuid=host_uuid param-name=other-config param-key=iscsi_iqn
```

The following screenshot displays the iSCSI IQN for the XenServer host:

```
[root@XENSERVER3 ~]# xe host-param-get uuid=1b64f642-2f2e-4ebd-9cea-e009e9041c79 param-name=other-config param-key=iscsi_iqn
iqn.2014-10.com.example:66043589
[root@XENSERVER3 ~]#
```

The `xe host-param-set` command is used to set the iSCSI IQN for a XenServer host:

```
xe host-param-set uuid=host_uuid other-config:iscsi_iqn=new_iscsi_iqn
```

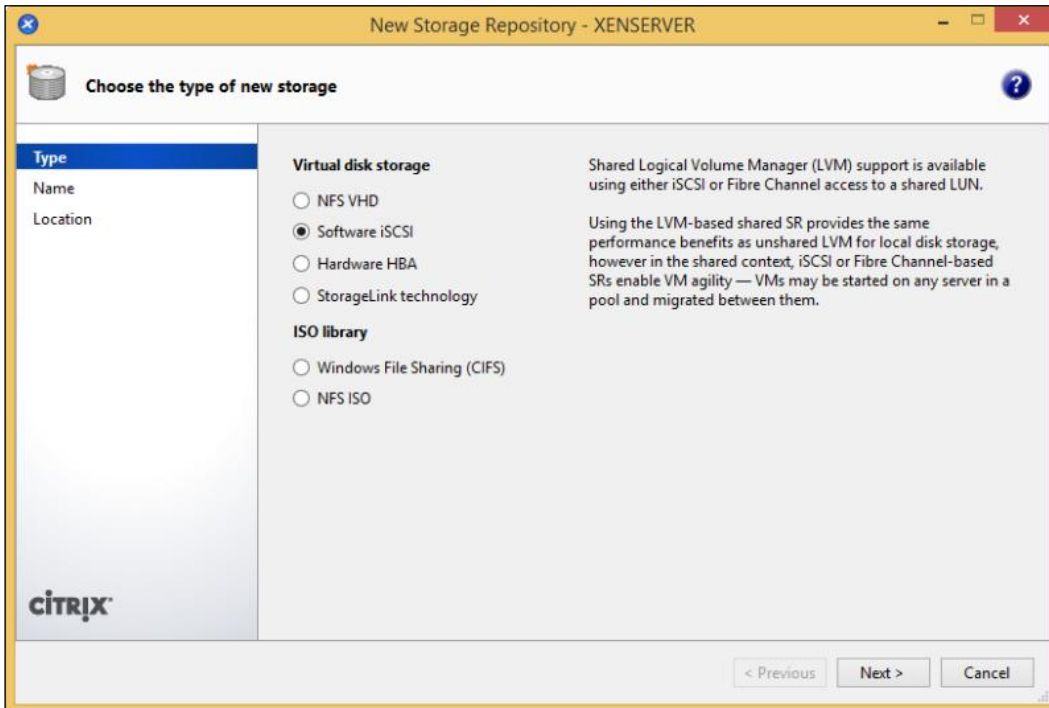
The following screenshot shows how to set the iSCSI IQN for a XenServer host:

```
[root@XENSERVER3 ~]# xe host-param-set uuid=1b64f642-2f2e-4ebd-9cea-e009e9041c79 other-config:iscsi_iqn=iqn.2014-10.local.company:XENSERVER3
[root@XENSERVER3 ~]#
```

Creating a Software iSCSI SR (using the GUI)

The following steps cover how to create a Software iSCSI SR on a XenServer host, using the XenCenter GUI:

1. Select the desired XenServer host or pool and press the **New Storage** button on the toolbar.
2. Select the **Software iSCSI** option and press **Next** to continue:



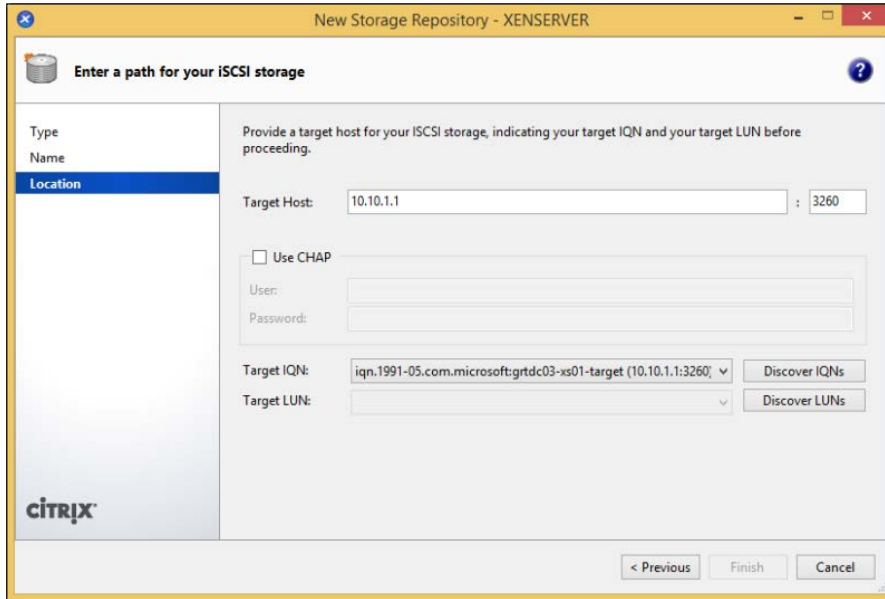
3. Provide a name and description for the SR and press **Next** to continue.
4. Enter the hostname or IP address of the iSCSI storage target into the **Target Host** textbox and the configured TCP port in the box to the right-hand side. Click on the **Discover IQNs** button to query the storage:

The screenshot shows a Citrix wizard window titled "New Storage Repository - XENSERVER". The main heading is "Enter a path for your iSCSI storage". On the left, there is a sidebar with "Type", "Name", and "Location" sections. The "Location" section is selected. The main area contains instructions: "Provide a target host for your iSCSI storage, indicating your target IQN and your target LUN before proceeding." Below this, there are input fields for "Target Host" (containing "10.10.1.1") and a port field (containing "3260"). There is a checkbox for "Use CHAP" which is unchecked. Below that are "User:" and "Password:" fields. At the bottom, there are "Target IQN:" and "Target LUN:" dropdown menus, each with a "Discover" button next to it. The Citrix logo is in the bottom left corner. At the bottom right, there are "< Previous", "Finish", and "Cancel" buttons.

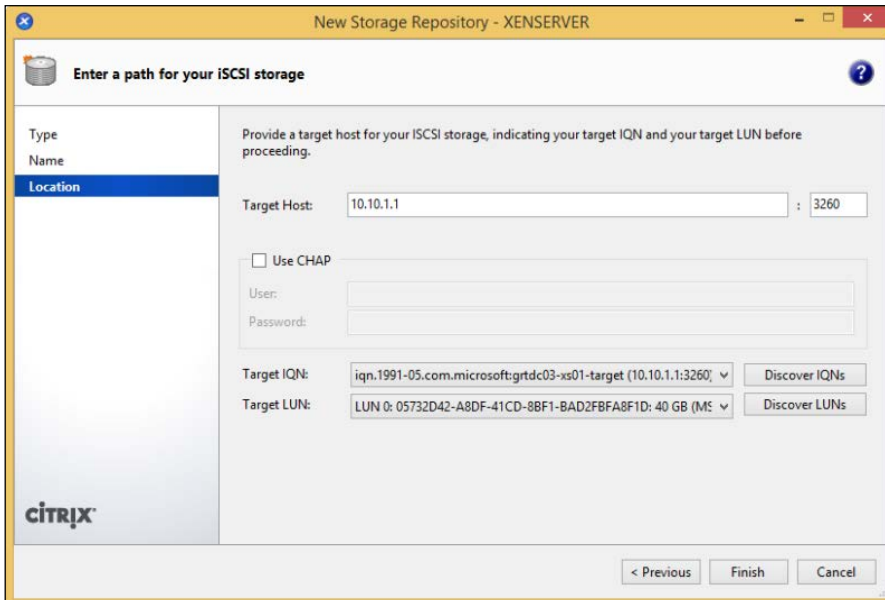



The TCP port is prepopulated with the default iSCSI port number 3260 and should only be changed if another port has been configured on the storage target.

- The available IQNs on the storage target should be presented to the XenServer host. Select the appropriate target IQN and click the **Discover LUNs** button to query the storage for available LUNs:

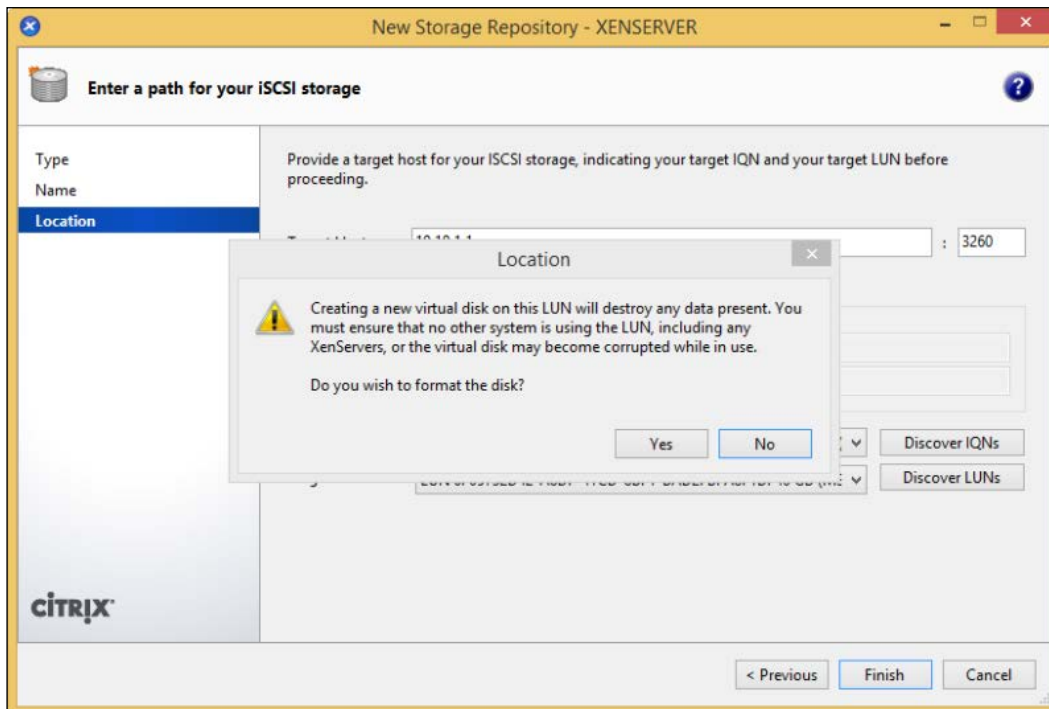



- Press **Finish** to create the SR:



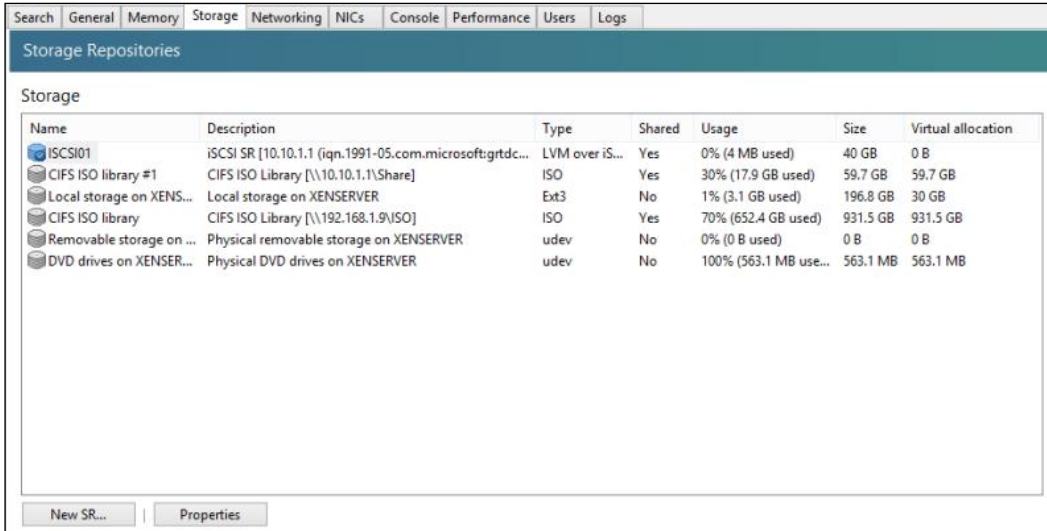
 The XenServer host will only display LUNs that have been granted access to the storage target.

7. Press **Yes** to format the LUN:



 Ensure that there is no existing data on the LUN as new iSCSI SRs require the LUN to be formatted.

8. The newly created SR can be viewed under the **Storage** tab of the XenServer host or pool, as shown in the following screenshot:



Creating a Software iSCSI SR (using the CLI)

The following steps cover how to create a Software iSCSI SR on a XenServer host using the `xe` command from the command-line interface:

1. Run the `xe sr-probe` command to view details of the iSCSI LUN that the SR will use. The `scsiid` value is required during the creation of the iSCSI SR:

```
xe sr-probe type=lvmoiscsi device-config:target=target_ip_address  
device-config:targetIQN=iscsi_target_LUN_IQN
```

The output of this command is shown in the following screenshot:

```
[root@XENSERVER3 ~]# xe sr-probe type=lvmoiscsi device-config:target=
192.168.1.111 device-config:targetIQN=iqn.2014-07.com.citrix: xenstor
age3
Error code: SR_BACKEND_FAILURE_107
Error parameters: , The SCSIid parameter is missing or incorrect, <?x
ml version="1.0" ?>
<iscsi-target>
  <LUN>
    <vendor>
      IET
    </vendor>
    <serial>
      3036181ecce526d26050654d2b7e1a2e
    </serial>
    <LUNid>
      0
    </LUNid>
    <size>
      2147483648
    </size>
    <SCSIid>
      1494554000000000003036181ecce526d26050654d2b7e
1a2e
    </SCSIid>
  </LUN>
</iscsi-target>
```

2. Run the `xe sr-create` command to create the iSCSI SR:

```
xe sr-create content-type=user name-label=sr_name
shared=true device-config:target=target_ip_address device-
config:targetIQN=target_lun_iqn device-config:SCSIid=target_lun_
scsi_id type=lvmoiscsi
```

The following screenshot shows how to create an iSCSI SR on a XenServer host:

```
[root@XENSERVER3 ~]# xe sr-create content-type=user name-label=ISCSI_
SR1 shared=true device-config:target=192.168.1.111 device-config:targ
etIQN=iqn.2014-07.com.citrix: xenstorage3 device-config:SCSIid=1494554
00000000003036181ecce526d26050654d2b7e1a2e type=lvmoiscsi
3a287fc4-1ee9-35de-bb7a-fa227882a00c
[root@XENSERVER3 ~]#
```

3. The `xe sr-list` command can be used to verify that the SR was successfully created:

```
xe sr-list type=lvmoiscsi
```


The following screenshot shows the iSCSI SRs on the XenServer host:

```
[root@XENSERVER3 ~]# xe sr-list type=lvmoiscsi
uuid ( RO)                : 3a287fc4-1ee9-35de-bb7a-fa227882a00c
  name-label ( RW)         : ISCSI_SR1
  name-description ( RW)   :
    host ( RO)             : XENSERVER3
    type ( RO)             : lvmoiscsi
  content-type ( RO)       : user
```

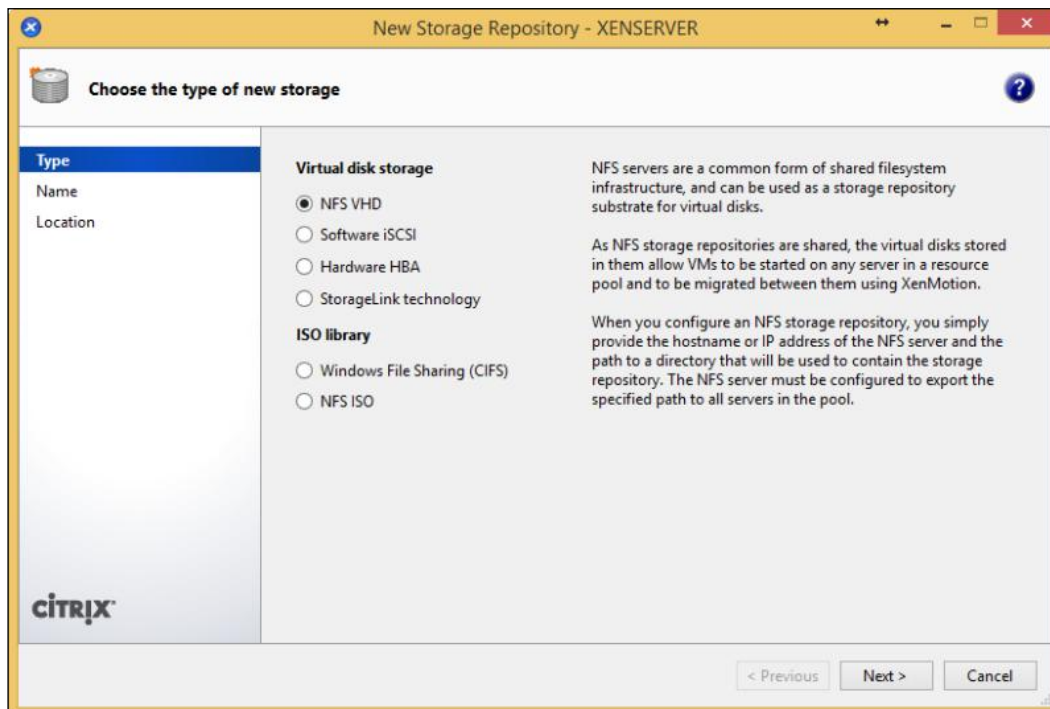
The NFS virtual disk SR

The NFS virtual disk SR utilizes the NFSv3 protocol to connect to an NFS share. NFS SRs are shareable among XenServer hosts and support thin provisioning.

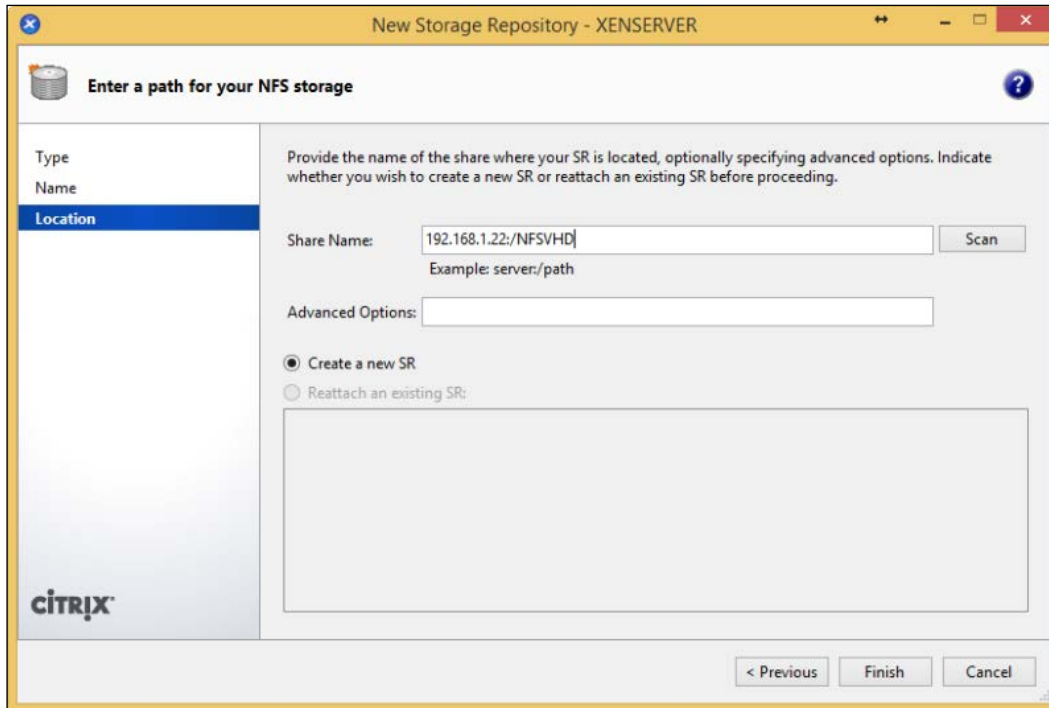
Creating an NFS SR (using the GUI)

The following steps cover how to create an NFS SR using the XenCenter GUI:

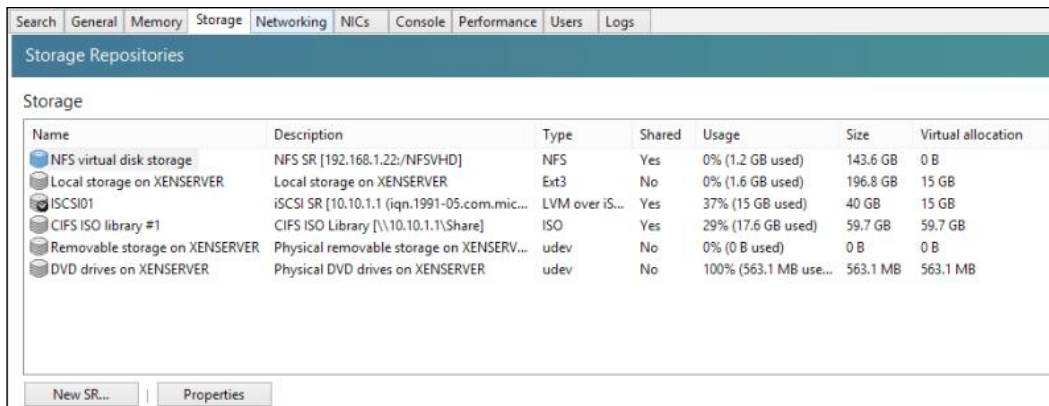
1. Select the desired XenServer host or pool and press the **New Storage** button on the toolbar.
2. Select the **NFS VHD** option and press **Next** to continue:



- Provide a name and description for the SR and press **Next** to continue; you will get the following screen:



- The newly created SR can be viewed under the **Storage** tab of the XenServer host or pool, as shown in the following screenshot:



Creating an NFS SR (using the CLI)

The following steps cover how to create an NFS SR using the `xe` command from the command-line interface:

1. Run the `xe sr-create` command to create an NFS SR:

```
xe sr-create content-type=user name-label=sr_name shared=true
device-config:server=server_ip_address device-config:serverpath=/
nfs_share_path type=nfs
```

The following screenshot shows how to add an NFS share to a XenServer host:

```
[root@XENSERVER3 ~]# xe sr-create content-type=user name-label=nfs_sr
1 shared=true device-config:server=192.168.1.111 device-config:server
path=/NFS_SR type=nfs
5a82b820-0a66-b54d-8fe7-de96103a962b
[root@XENSERVER3 ~]# █
```

2. The `xe sr-list` command can be used to verify that the SR was successfully created:

```
xe sr-list type=nfs
```

The following screenshot shows the iSCSI SRs on the XenServer host:

```
[root@XENSERVER3 ~]# xe sr-list type=nfs
uuid ( RO)          : 5a82b820-0a66-b54d-8fe7-de96103a962b
  name-label ( RW)  : nfs_sr1
  name-description ( RW) :
    host ( RO) : XENSERVER3
    type ( RO) : nfs
    content-type ( RO) : user
```

The host bus adapter hardware

Citrix XenServer supports the use of iSCSI or Fibre Channel **host bus adapters (HBAs)** to access remote storage. While the SR is being created, the XenServer host scans the storage target, utilizing the hardware HBA for any accessible LUNs and the XenServer presents them as SCSI drives.

StorageLink technology

StorageLink or **Integrated StorageLink (iSL)** provides enhanced integration between Citrix XenServer and the storage array. StorageLink is typically used for array-based snapshots, cloning, and provisioning. As of Version 6.2 of XenServer, the StorageLink feature has been deprecated.

Managing SRs

The following section covers managing SRs throughout the life cycle of the XenServer.

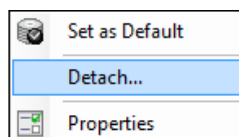
Detach

The detach operation unplugs the PBD connection from the SR. This operation leaves the data on the SR intact but simply removes XenServer's access to the data on the SR.

Detaching an SR (using the GUI)

The following steps cover how to detach an SR from a XenServer host using the XenCenter GUI:

1. Right-click on the desired SR and select **Detach...**:



2. The SR will now display a state of **Detached** under the **General** tab of the SR in the **Status** section, as shown in the following screenshot:



Detaching an SR (using the CLI)

The following steps cover how to detach an SR from a XenServer host, using the `xe` command from the command-line interface:

1. Run the `xe sr-list` command to view the SRs on the XenServer host. The `name-label` value will be used to determine the `uuid` value of the `pbid` entry:

```
xe sr-list shared=true
```

The following screenshot displays the shared SRs on the XenServer host:

```
[root@XENSERVER1 ~]# xe sr-list shared=true
uuid ( RO)                : 99ee1a6b-9edf-812d-2264-0337294ad06a
  name-label ( RW): XenServer Tools
  name-description ( RW): XenServer Tools ISOs
    host ( RO): <shared>
    type ( RO): iso
  content-type ( RO): iso

uuid ( RO)                : 665d9483-9a66-3672-035d-c3efcdb374f1
  name-label ( RW): NFS ISO library
  name-description ( RW): NFS ISO Library [192.168.1.111:/NFSISO]
    host ( RO): <shared>
    type ( RO): iso
  content-type ( RO): iso

uuid ( RO)                : f2b1f237-a8de-045f-aa70-131dbd07ab70
  name-label ( RW): NFS virtual disk storage
  name-description ( RW): NFS SR [192.168.1.111:/NFSVHD]
    host ( RO): <shared>
    type ( RO): nfs
  content-type ( RO):

uuid ( RO)                : 2c32a078-7d20-2268-c8de-441fada239c3
  name-label ( RW): Heartbeat SR1
  name-description ( RW): NFS SR [192.168.1.111:/heartbeat1]
    host ( RO): <shared>
    type ( RO): nfs
  content-type ( RO):
```

2. Run the `xe pbd-list` command to view PBD information for the SR we want to detach. The `name-label` value found in the previous step was used to filter the PBD entries shown. The `uuid` value of the PBD will be used to detach the SR:

```
xe pbd-list sr-name-label=sr_name
```

The following screenshot displays the PBD connection information for the SR:

```
[root@XENSERVER3 ~]# xe pbd-list sr-name-label=nfs_sr1
uuid ( RO)                : 6eed7daa-8b32-5942-5809-b5be9522adb
  host-uuid ( RO)         : 1b64f642-2f2e-4ebd-9cea-e009e9041c79
    sr-uuid ( RO)         : 5a82b820-0a66-b54d-8fe7-de96103a962b
      device-config (MRO) : server: 192.168.1.111; serverpath: /NFS
_SR
  currently-attached ( RO) : true
```

3. Run the `xe pbd-unplug` command to detach the SR. The UUID of the PBD from the previous step was used to identify the correct SR to detach:

```
xe pbd-unplug uuid=pbd_uuid
```

The following screenshot shows how to detach an SR:

```
[root@XENSERVER3 ~]# xe pbd-unplug uuid=6eed7daa-8b32-5942-5809-b5be9522adb
[root@XENSERVER3 ~]#
```

4. The `xe pbd-list` command can be used to verify that the SR has been successfully detached. The `currently-attached` value should be `false` if the SR is detached:

```
xe pbd-list sr-name-label=sr_name
```

The following screenshot displays the PBD connection information for the SR:

```
[root@XENSERVER3 ~]# xe pbd-list sr-name-label=nfs_sr1
uuid ( RO)                : 6eed7daa-8b32-5942-5809-b5be9522adb
  host-uuid ( RO)         : 1b64f642-2f2e-4ebd-9cea-e009e9041c79
    sr-uuid ( RO)         : 5a82b820-0a66-b54d-8fe7-de96103a962b
      device-config (MRO) : server: 192.168.1.111; serverpath: /NFS
_SR
  currently-attached ( RO) : false
```

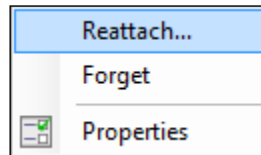
Reattach

The reattach operation plugs the PBD connection to the SR. This operation reconnects the SR on the XenServer host. The process of reattaching the SR requires the administrator to re-enter into the connection information.

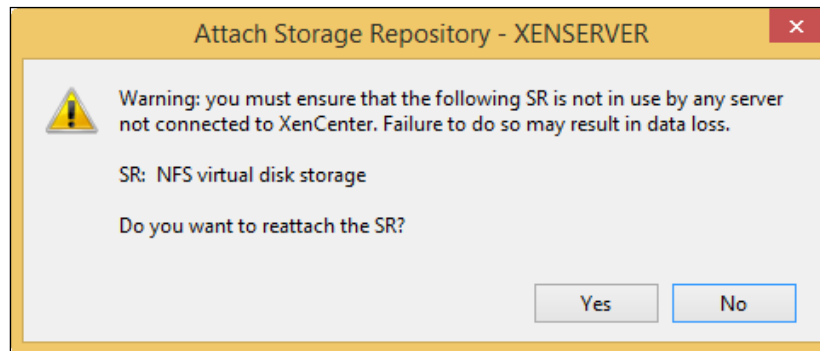
Reattaching an SR (using the GUI)


The following steps cover how to reattach an SR on a XenServer host using the XenCenter GUI:

1. Right-click on the detached SR and select **Reattach...**:



2. Re-enter the connection information for the SR.
3. Press **Finish** to reattach the SR.
4. Press **Yes** to reattach the SR.



[ Ensure that the SR is not attached to any other servers when reattaching the SR to avoid data corruption as a result of multiple hosts accessing the same SR.]

Reattaching an SR (using the CLI)

The following steps cover how to reattach an SR on a XenServer host using the `xe` command from the command-line interface:

1. Run the `xe pbd-list` command to view the PBD information for the SR we want to reattach. The `uuid` value of the PBD will be used to reattach the SR:

```
xe pbd-list sr-name-label=sr_name
```

The following screenshot displays the PBD connection information for the SR:

```
[root@XENSERVER3 ~]# xe pbd-list sr-name-label=nfs_sr1
uuid ( RO)                : 6eed7daa-8b32-5942-5809-b5be9522adbc
  host-uuid ( RO)         : 1b64f642-2f2e-4ebd-9cea-e009e9041c79
  sr-uuid ( RO)           : 5a82b820-0a66-b54d-8fe7-de96103a962b
  device-config (MRO)    : server: 192.168.1.111; serverpath: /NFS
_SR
  currently-attached ( RO) : false
```

2. Run the `xe pbd-plug` command to reattach the SR. The `uuid` value of the PBD from the previous step was used to identify the correct SR to be reattached:

```
xe pbd-plug uuid=pbd_uuid
```

The following screenshot shows how to reattach an SR:

```
[root@XENSERVER3 ~]# xe pbd-plug uuid=6eed7daa-8b32-5942-5809-b5be9522adbc
[root@XENSERVER3 ~]# █
```

Forget

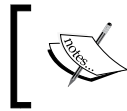
The **Forget** operation removes the PBD connection information from the XenServer host, and unlike the detach operation, the forget operation requires the connection information to be re-entered in the event that the SR needs to be reconnected.

This operation leaves the data on the SR intact but simply removes the connection information used to connect to the PBD. The process of reconnecting the SR requires the administrator to create a new SR that utilizes the connection information from the forgotten storage repository.

Forgetting an SR (using the GUI)

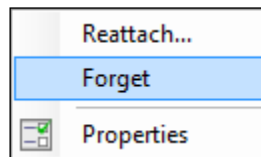
The following steps cover how to forget an SR using the XenCenter GUI.

1. Right-click on the desired SR and select **Detach**.



The **Detach** operation is required before the **Forget** operation can be run on the SR, otherwise, the **Forget** option will not be available.

2. Right-click on the desired SR again and select **Forget...**:



The storage repository will now be removed from the XenServer host.

Forgetting an SR (using the CLI)

The following steps cover how to forget an SR using the `xe` command from the command-line interface:

1. Detach the SR using the `xe pbd-unplug` command discussed earlier in the chapter.
2. Run the `xe sr-list` command to list the information for the SR to forget:

```
xe sr-list name-label=sr_name
```

The following screenshot shows the information for the defined SR:

```
[root@XENSERVER3 ~]# xe sr-list name-label=nfs_sr1
uuid ( RO)                : 5a82b820-0a66-b54d-8fe7-de96103a962b
  name-label ( RW): nfs_sr1
  name-description ( RW):
    host ( RO): <not in database>
    type ( RO): nfs
  content-type ( RO): user
```

- Run the `xe sr-forget` command to forget the SR:


```
xe sr-forget uuid=sr_uuid
```

The following screenshot shows how to forget an SR:

```
[root@XENSERVER3 ~]# xe sr-forget uuid=5a82b820-0a66-b54d-8fe7-de96103a962b
[root@XENSERVER3 ~]#
```

Destroy

The **Destroy** operation deletes the PBD connection information from the XenServer host and deletes the data that resides on the SR. This operation should only be taken when the SR is empty or the data on the SR can be safely deleted.

 This operation cannot be reversed and the data must be restored from backups.

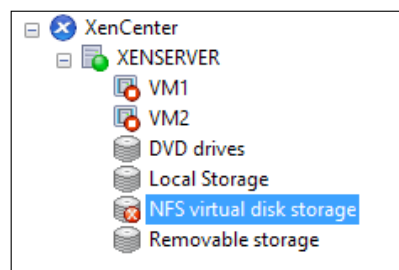
Repair

The **Repair** operation is used to fix a broken SR connection. A repair operation is generally necessary when the XenServer host or pool is unable to communicate with the storage target.

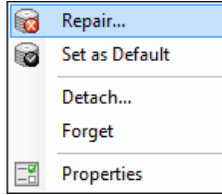
Repairing an SR

The following steps cover how to repair an SR on a XenServer host:

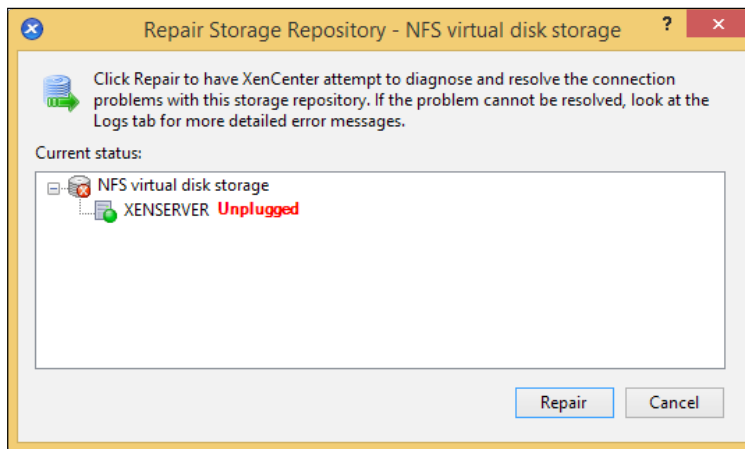
- The SR will have a red circle with a white **x** to indicate that the connection is broken:



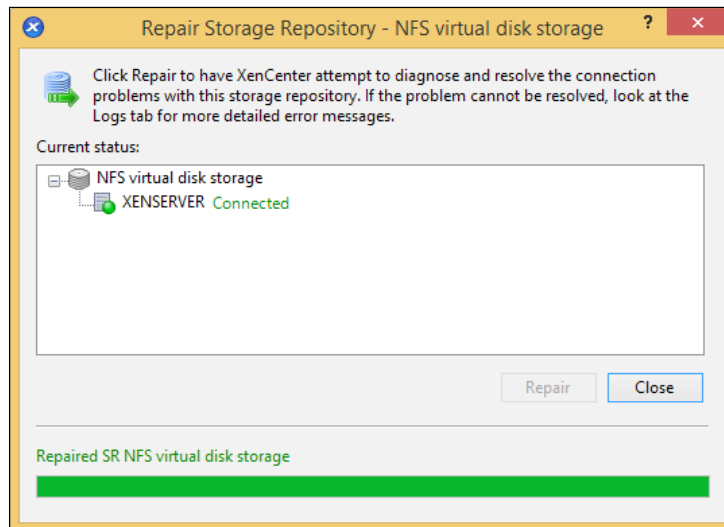
2. Right-click on the desired SR and select **Repair...**:



3. Press the **Repair** button to initiate the repair process:



4. Press **Close** to complete the repair operation:



In the event that the repair operation is unsuccessful, some additional steps need to be taken to restore functionality. Typically, ensuring that the XenServer host can access the storage device is the first troubleshooting step, next is attempting to remove the existing connection, and then, creating a new connection. Restoring the data from backups might be necessary if none of the previous actions were successful.

Resize

The process of resizing an SR varies based on the underlying storage utilized for the storage repository, as listed in the following table:

SR type	Action
EXT3	Unplug the PBD, resize the ext3, and replug the PBD
iSCSI	Unplug the PBD, resize the LUN, and replug the PBD
HBA SRs	Resize the LUN and reboot the XenServer host

The suspend SR

The suspend SR is used to store data for suspended virtual machines. The desired SR to host the suspended virtual machine files can be selected from the `xsconsole`.



The `xsconsole` can be accessed by entering the `xsconsole` command on the physical console or through the XenServer host console in the XenCenter GUI.

```

XenServer 6.2                               19:05:35                               root@XENSERVER
----- Configuration -----
Disks and Storage Repositories
Current Storage Repositories
Create New Storage Repository
Attach Existing Storage Repository
Specify Suspend SR
Specify Crash Dump SR

Specify Suspend SR
This server can be configured to use
a Storage Repository for suspend
images.
The SR named 'Local storage' is
configured as the Suspend Image SR
for this server.

<Esc/Left> Back <Up/Down> Select | <Enter> Specify Suspend SR

```

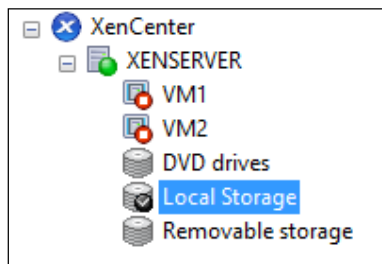
The crash dump SR

The crash dump SR is used to store crash dumps, which contain details regarding the crash event, such as memory dumps or process lists. The desired SR for hosting the crash dump files can be selected from the `xsconsole`, as shown in the following screenshot:



The default SR

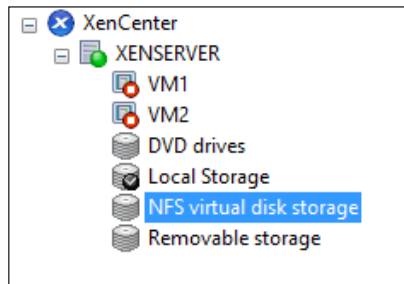
The default SR is used as the default location to place virtual machines that are imported into XenServer. The default SR is denoted by the black circle with the white check mark inside a particular SR in XenCenter, or by using the `xe-pool-param-get` command with the `default-SR` parameter, as shown in the following screenshot:



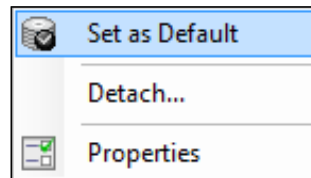
Changing the default SR (using the GUI)

The following steps cover how to change the default SR on a XenServer host using the XenCenter GUI:

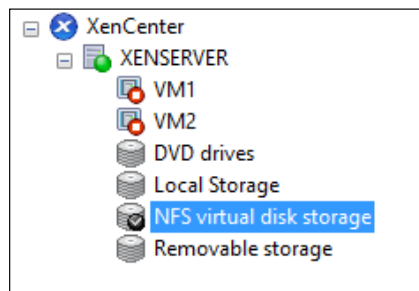
1. Right-click on the desired SR:



2. Select the **Set as Default** option to set the SR as the default SR:



3. A black circle with a white check mark will now appear on the SR:



Changing the default SR (using the CLI)

The following steps cover how to change the default SR on a XenServer host using the CLI:

1. Run the `xe sr-list` command to list the SRs along with the UUID of the SR on the server. The UUID of the SR is required when setting the default SR:

```
xe sr-list
```

The following screenshot shows the SRs on the XenServer host:

```
[root@XENSERVER3 ~]# xe sr-list
uuid ( RO)                : 9a17db92-a252-15e5-8938-bc408f52790d
  name-label ( RW)        : XenServer Tools
  name-description ( RW)  : XenServer Tools ISOs
  host ( RO)              : XENSERVER
  type ( RO)              : iso
  content-type ( RO)     : iso

uuid ( RO)                : f2b1f237-a8de-045f-aa70-131dbd07ab70
  name-label ( RW)        : NFS virtual disk storage
  name-description ( RW)  : NFS SR [192.168.1.180:/NFSVHD]
  host ( RO)              : XENSERVER
  type ( RO)              : nfs
  content-type ( RO)     :

uuid ( RO)                : 83ea35de-5685-c5a4-8bcf-3c5b9e6ab696
  name-label ( RW)        : DVD drives
  name-description ( RW)  : Physical DVD drives
  host ( RO)              : XENSERVER
  type ( RO)              : udev
  content-type ( RO)     : iso

uuid ( RO)                : 66f9c208-a703-8150-1eae-2ccac3f67c06
  name-label ( RW)        : Local Storage
  name-description ( RW)  :
  host ( RO)              : XENSERVER
  type ( RO)              : ext
  content-type ( RO)     : user
```

2. Run the `xe pool-param-set` command to set the default SR for the XenServer pool:

```
xe pool-param-set uuid=pool_uuid default-SR=sr_uuid
```

The following screenshot shows how to set the default SR on a XenServer host:

```
[root@XENSERVER3 ~]# xe pool-param-set uuid=ab83047b-1b90-d597-e596-1
dac249c7ff6 default-SR=f2b1f237-a8de-045f-aa70-131dbd07ab70
[root@XENSERVER3 ~]# █
```

3. The `xe pool-param-get` command can be used to verify the default SR set for the XenServer pool:

```
xe pool-param-get uuid=pool_uuid param-name=default-SR
```

The following screenshot shows the default SR on the XenServer:

```
[root@XENSERVER3 ~]# xe pool-param-get uuid=ab83047b-1b90-d597-e596-1
dac249c7ff6 param-name=default-SR
f2b1f237-a8de-045f-aa70-131dbd07ab70
[root@XENSERVER3 ~]# █
```

Summary

In this chapter, we learned about the components of XenServer storage along with configuring the NFS and CIFS ISO library SRs. In addition to the ISO library SRs, we looked at configuring VHD SRs using NFS and iSCSI protocols. We also examined SR management tasks such as detaching, repairing, forgetting, and destroying.

In the next chapter, we will learn how to create and manage VMs.

4

Creating and Managing Virtual Machines

Now that we have installed Citrix XenServer 6.2, configured networking and storage, we're ready to begin creating and managing **virtual machines (VMs)**. VMs provide several benefits over physical servers, such as being able to move the VM from one host to another to eliminate downtime for hardware maintenance, the ability to dynamically modify the VM's hardware such as memory or hard disk, and the ability to create VM snapshots to take point-in-time captures of the VM state for disaster recovery purposes.

In this chapter, you'll learn the following topics:

- Creating a virtual machine
- Virtual machine hardware
- Managing virtual machines
- Creating and managing **virtual appliances (vApps)**
- Importing and exporting virtual machines

VM overview

A VM is a software container that runs on a host and acts very much like a physical computer. VMs are composed of virtual instances of physical computer hardware such as processors, memory, and hard disks.

XenServer supports VMs that runs in two modes: **hardware-assisted virtualization mode (HVM)** and paravirtualized mode:

- **HVM:** An HVM VM can achieve near-native performance without any modification to the guest operating system. HVM requires host processors that support hardware virtualization such as Intel VT or AMD-V. XenServer uses QEMU to emulate the VM hardware such as the BIOS, disk controllers, and network adapters. Due to the emulation required, HVM guests generally perform slower than paravirtualized guests. To improve the performance of HVM guests, Citrix XenServer Tools are installed to improve guest performance by installing paravirtualized drivers into the guest operating system.
- **Paravirtualized mode:** The guest operating system of a paravirtualized VM is tuned and optimized to run in a virtual environment. Paravirtualized mode does not require that the host's CPUs support virtualization extensions such as Intel VT or AMD-V. Paravirtualized mode requires that the guest has a PV-enabled kernel as well as the PV drivers installed in order to allow the guest to be aware of the hypervisor and can run without emulation. This typically results in better performance and greater flexibility than an HVM guest. Windows guests do not support the use of paravirtualized mode and, by default, Linux templates included with XenServer utilize paravirtualized mode.

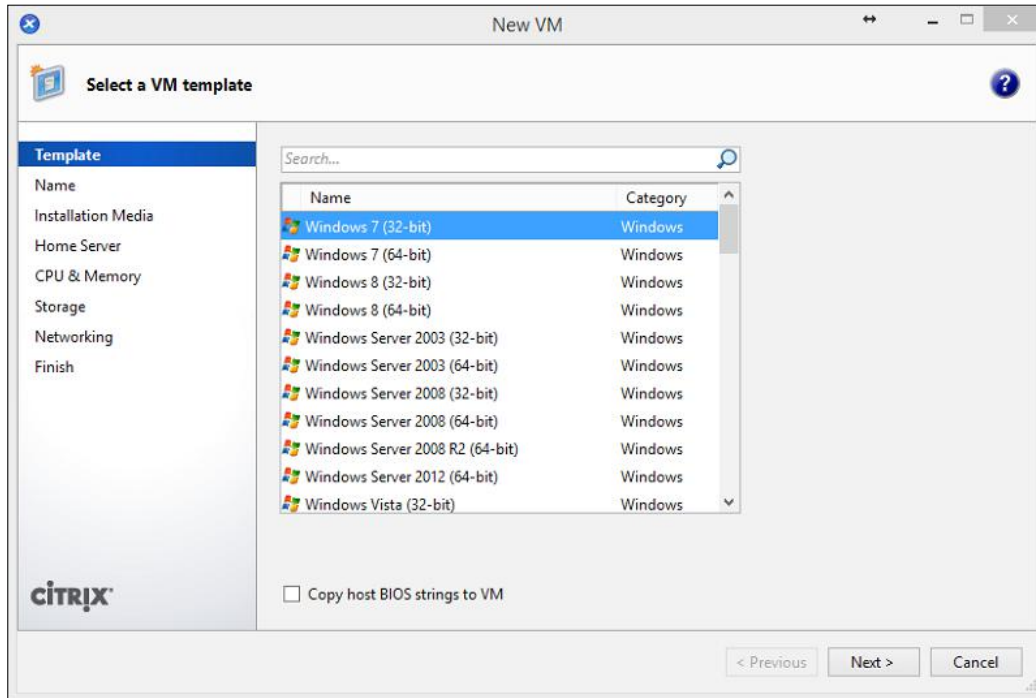
Creating a VM

The following steps cover the process of creating a VM using the **New VM** wizard in the XenCenter GUI:

1. Select the desired XenServer host or pool in Citrix XenCenter and select the **New VM** button on the toolbar to launch the **New VM** wizard.

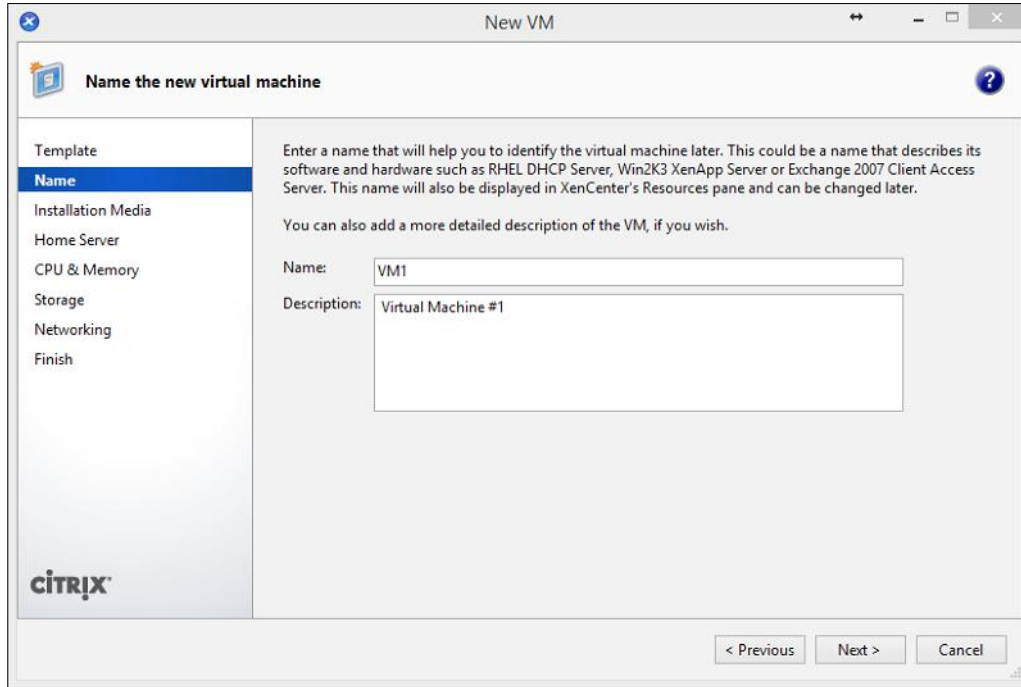


2. Select the template that most closely matches the guest operating system that will be installed as the guest operating system for the VM.



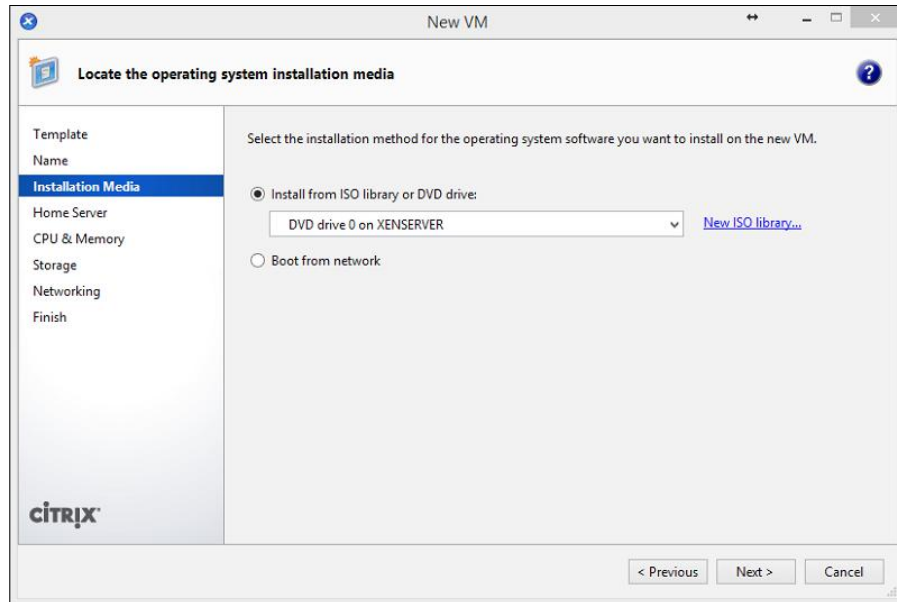
Templates contain the setup information or metadata needed to create a new VM with a specific guest operating system and with the optimum storage, CPU, memory, and virtual network configuration. Custom templates can be created to meet specific deployment needs. Creating custom templates will be discussed later in this chapter.

3. Enter a name and description for the VM in the textboxes provided.

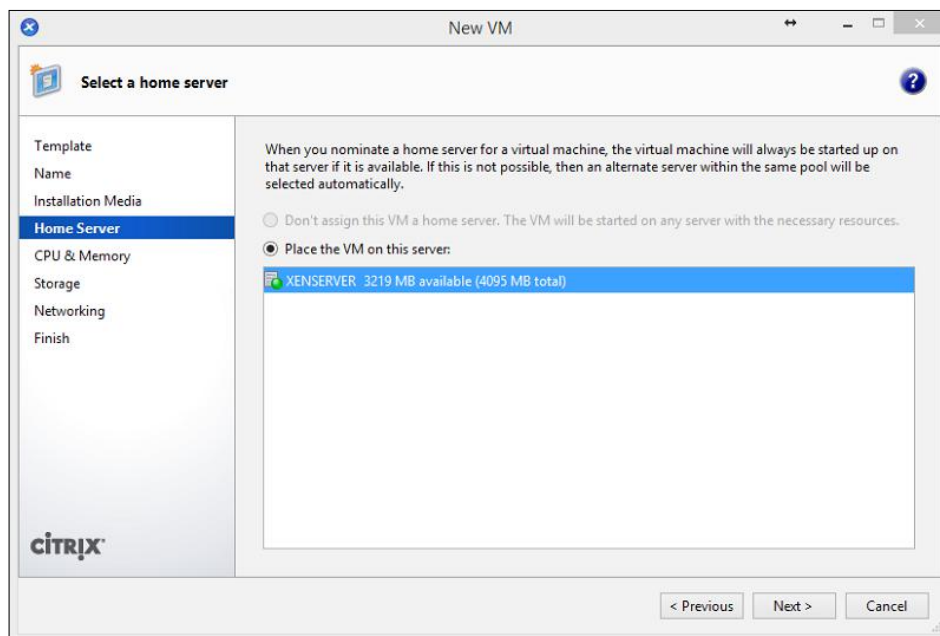


4. Select the appropriate installation method:
 - **Install from ISO library or DVD drive:** This option allows the VM to boot from an `.iso` file on a configured ISO SR or from a physical CD/DVD that is inserted into the CD/DVD drive of the XenServer host
 - **Boot from network:** The VM network or **Preboot eXecution Environment (PXE)** boots and retrieves the necessary files to install the guest operating system from the network

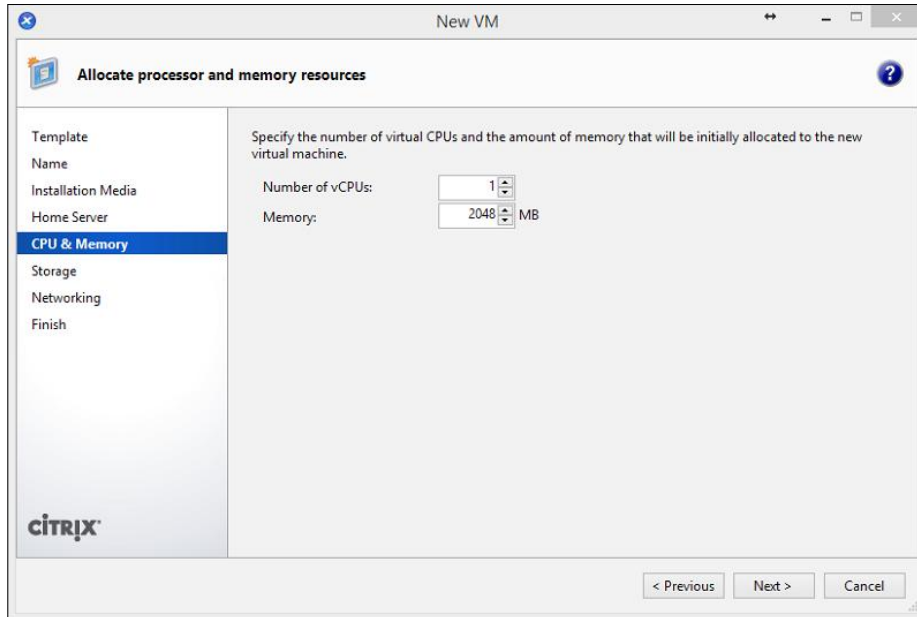
These options are shown in the following screenshot:



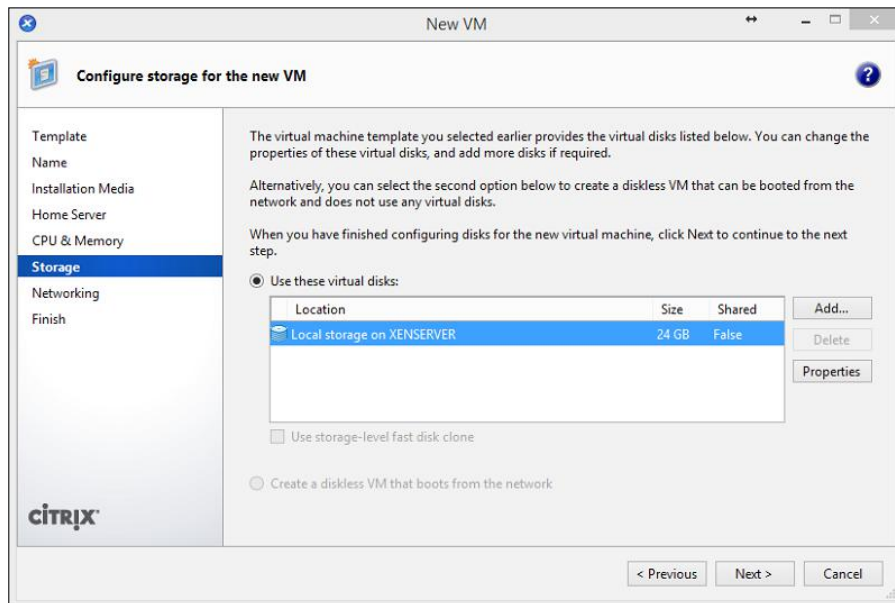
5. Optionally, the VM can be placed onto a particular XenServer host or any server with available resources.



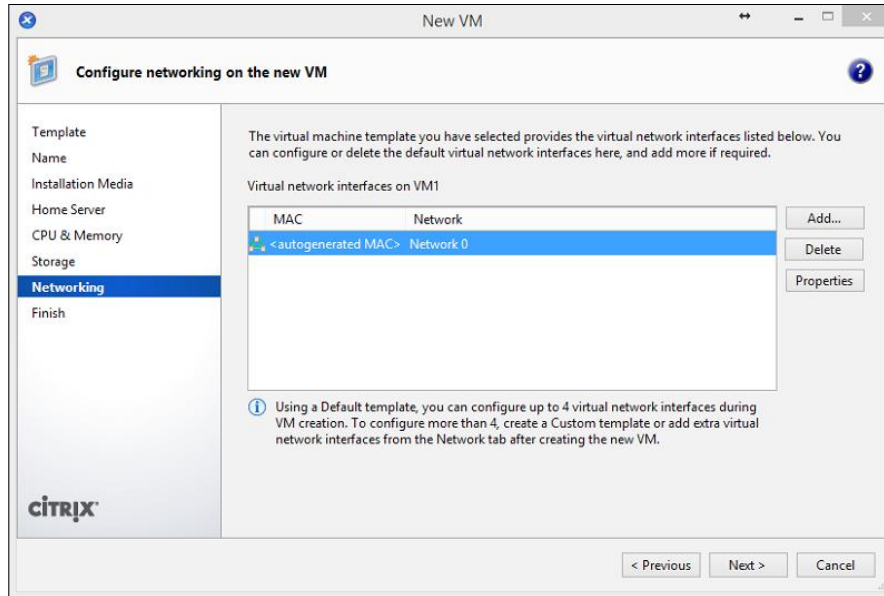
- Specify the number of virtual CPUs and the amount of memory to be allocated to the VM. Click on **Next** to continue.



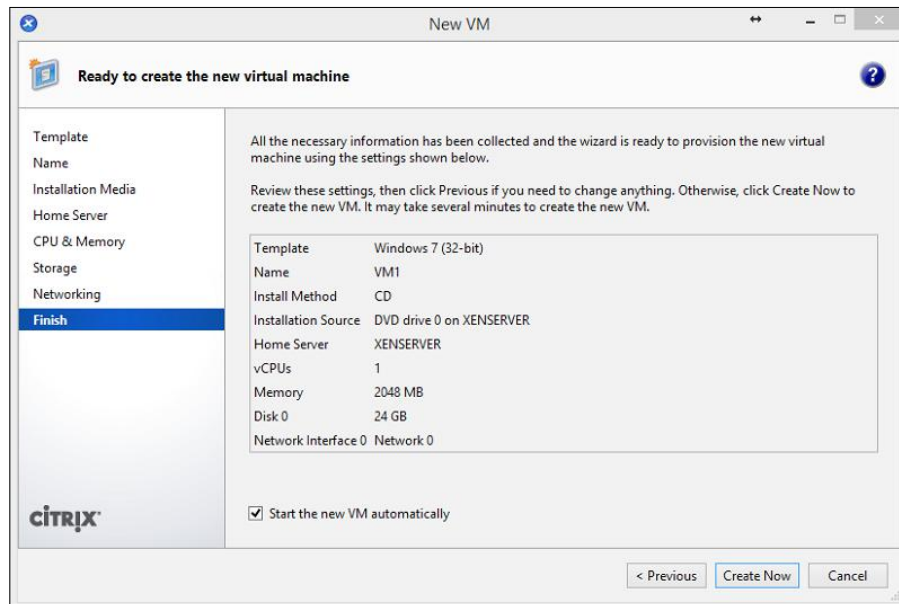
- Configure the virtual disk(s) that will be used for the VM. Click on **Next** to continue.



8. Configure the virtual network interface(s) that will be used for the VM. Click on **Next** to continue.

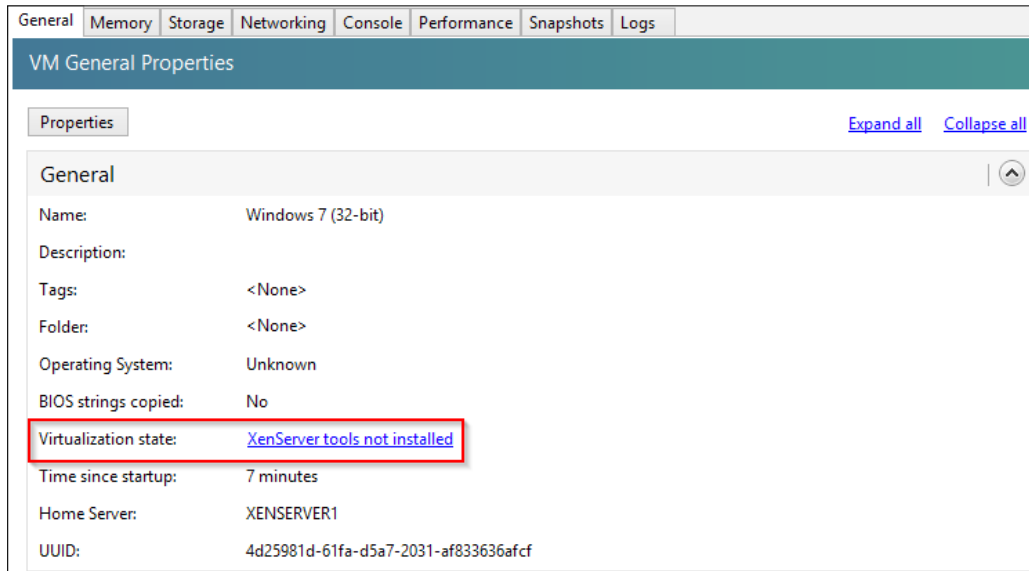


9. Review the selected settings, optionally select the **Start the new VM automatically** checkbox to start the VM immediately after it is created. Click on **Create Now** to create the VM.



XenServer® Tools

XenServer Tools or xs-tools provide a management agent and high-performance drivers to enhance the disk and network performance for VMs. The tools also provide support for XenServer features such as cleanly rebooting, shutting down, and suspending a VM, VM migration, and VM performance data in XenCenter. The following screenshot shows the virtualization state:



Installing XenServer® Tools on Windows VMs

The following steps cover the process of installing XenServer Tools onto a Windows VM.

1. Right-click on the VM and click on **Install XenServer Tools**.
2. Log into the VM and double-click on the CD drive in the VM to launch the installer.
3. Follow the on-screen instructions and reboot the VM when prompted.

Installing XenServer® Tools on Linux VMs

The following steps cover the process of installing XenServer Tools onto a Linux VM.

1. Right-click on the VM and click on **Install XenServer Tools**.
2. Log into the VM as the root user from the XenServer console of the VM or via SSH and mount the image into the VM with the following command:

```
mount /dev/xvdd /mnt
```



The path to the DVD device might be different if there are multiple devices connected to the VM. Block devices are passed through as PV devices on paravirtualized Linux guests. XenServer does not attempt to emulate SCSI or IDE, but instead provides a more suitable interface in the virtual environment in the form of xvd devices.

3. Run the following command to install XenServer Tools on the VM:

```
/mnt/Linux/install.sh
```

4. Restart the VM to complete the installation.

The screenshot shows the 'VM General Properties' window in XenServer. The 'General' tab is selected, and the 'Virtualization state' field is highlighted with a red box, indicating that the VM is in an 'Optimized (version 6.2 installed)' state. Other fields include Name (Windows 7 (32-bit)), Description, Tags (<None>), Folder (<None>), Operating System (Windows 7 Home Premium), BIOS strings copied (No), Time since startup (21 minutes), Home Server (XENSERVER1), and UUID (4d25981d-61fa-d5a7-2031-af833636afcf).

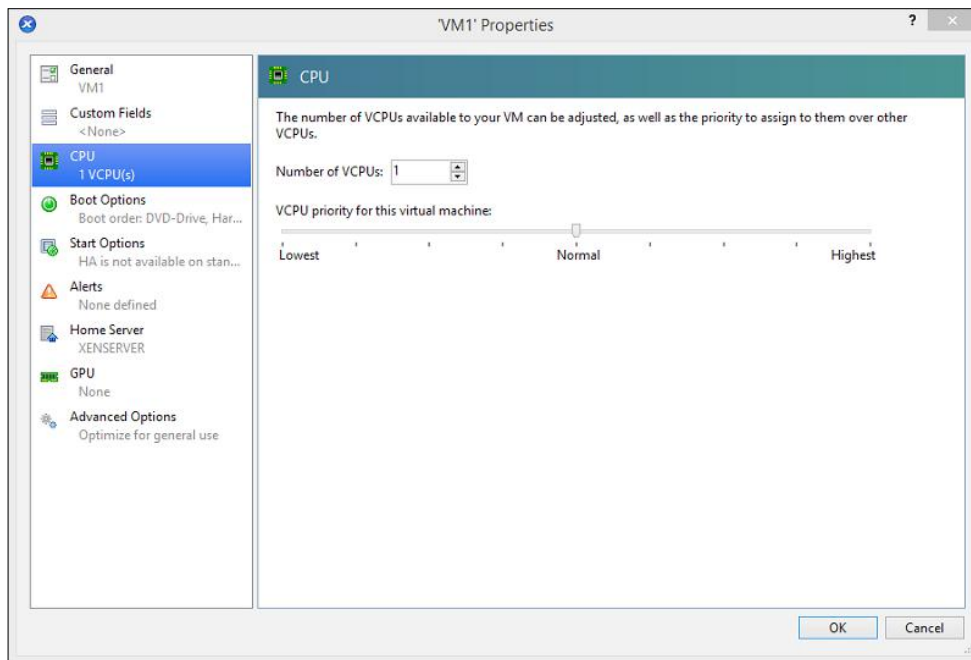
Property	Value
Name	Windows 7 (32-bit)
Description	
Tags	<None>
Folder	<None>
Operating System	Windows 7 Home Premium
BIOS strings copied	No
Virtualization state	Optimized (version 6.2 installed)
Time since startup	21 minutes
Home Server	XENSERVER1
UUID	4d25981d-61fa-d5a7-2031-af833636afcf

Modifying VMs

A VM can be modified after it has been created to accommodate the need for increasing the memory or adding a hard disk to the VM.

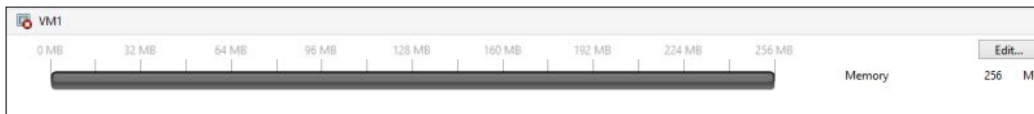
Processor (vCPU)

Citrix XenServer 6.2 supports up to 16 vCPUs per VM. The number of vCPUs available is contingent upon the number of processor cores in the XenServer host. The processor settings of a VM can be modified in the **Properties** section of the VM, as shown in the following screenshot:

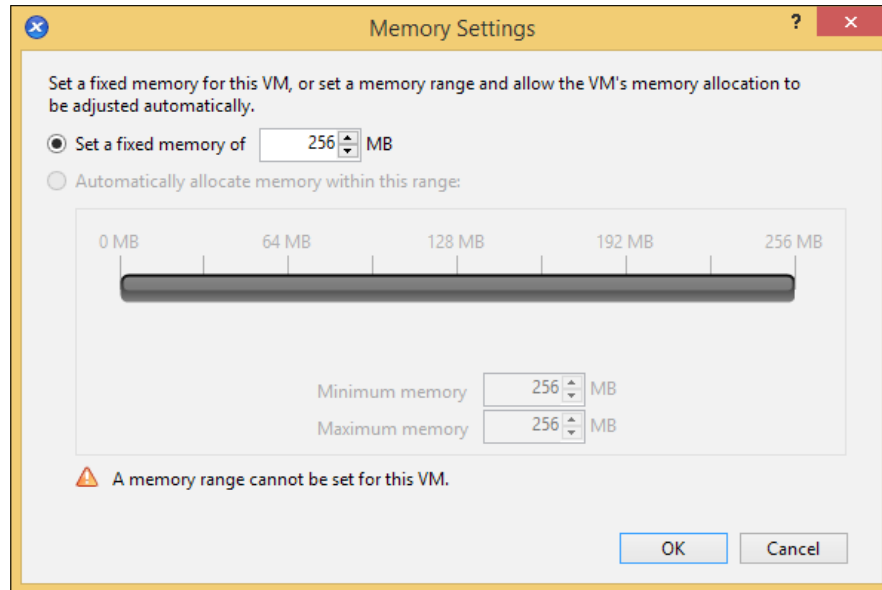


Memory (RAM)

Citrix XenServer 6.2 supports up to 128 GB of RAM in a single VM. The maximum amount of RAM available is contingent upon the amount of RAM in the XenServer host. The memory settings of a VM can be modified under the **Memory** tab of the VM, as shown in the following screenshot:



Clicking on the **Edit** button allows for memory settings to be set:



Dynamic Memory Control

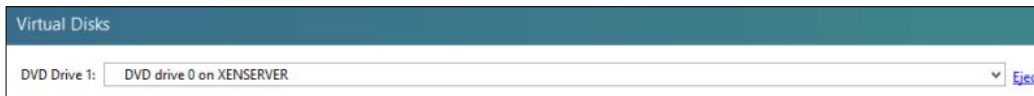
XenServer **Dynamic Memory Control (DMC)** is a feature that allows a XenServer host to dynamically allocate memory to VMs based on the need and configured memory minimums and maximums, it's also known as memory ballooning. This feature enables the host to efficiently share a pool of memory among VMs that allows memory overcommit or overprovisioning, which maximizes the amount of memory in the host.

The two settings for dynamic memory control are as follows:

- **The dynamic memory range:** The dynamic memory range is the minimum and maximum amount of memory that the XenServer host guarantees to the VM. The dynamic memory range allows a VM's memory to be added or removed without the need to reboot the VM.
- **The static memory range:** The static memory range is the hard memory limit that cannot be modified without restarting the VM. The static minimum level is the minimum amount of memory required to support the guest operating system and the static maximum level is the maximum amount of memory that the guest operating system can utilize without requiring a restart of the VM in order to change the memory. The dynamic memory range falls within the static memory range and allows the VM's memory to be dynamically allocated.

The DVD drive

The DVD drive on the VM emulates a physical DVD drive and appears like a physical DVD drive to the VM. The following screenshot shows the virtual DVD drive on a VM:



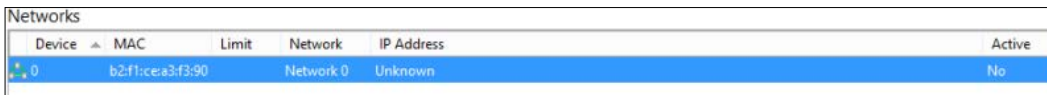
Hard disk

Citrix XenServer 6.2 supports up to 16 hard disks per VM and a maximum size of 2,044 GB per virtual disk.

Position	Name	Description	SR	Size	Read Only	Priority	Active	Device Path
0	VM1 0	Local storage on XENSERVER		1 GB	No	0 (Lowest)	No	<unknown>

The network adapter

Citrix XenServer 6.2 supports up to seven network adapters per VM. The network adapters of a VM can be modified under the **Networking** tab of the VM.

A screenshot of the 'Networks' configuration window. It shows a table with columns: Device, MAC, Limit, Network, IP Address, and Active. There is one row for '0' with MAC 'b2:f1:ce:a3:f3:90', Network 'Network 0', IP Address 'Unknown', and Active 'No'.

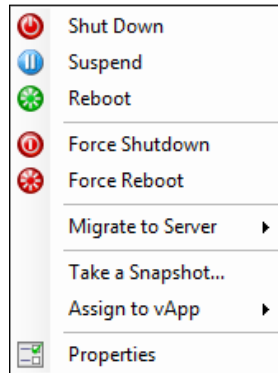
Device	MAC	Limit	Network	IP Address	Active
0	b2:f1:ce:a3:f3:90		Network 0	Unknown	No

Managing VMs

The following section covers VM operations such as power management, snapshots, and cloning or copying.

Power states of a VM

The available VM power operations are covered in this section. The following screenshot shows you some of the power operations that can be performed on a VM:



The various power operations are as follows:

- **Start:** This powers on the VM, the equivalent of pressing the power button to turn on a machine. The `xe vm-start` command can be used to start the VM from the command line.
- **Reboot:** This performs a graceful restart of the VM. The `xe vm-reboot` command can be used to restart the VM from the command line.
- **Force Reboot:** This performs a nongraceful restart of the VM and does not allow the system to properly stop applications and services running on the VM. The `xe vm-reboot` command with the `force=true` parameter can be used to forcefully reboot the VM from the command line.
- **Shut Down:** This performs a graceful shutdown of the VM allowing the system to properly shutdown running applications and services. The `xe vm-shutdown` command can be used to shut down the VM from the command line.
- **Force Shutdown:** This performs a hard shutdown and is the equivalent of unplugging a physical server. A forced shutdown should only be performed when a soft shutdown is not an available option. The `xe vm-shutdown` command with the `force=true` parameter can be used to forcefully shutdown the VM from the command line.

- **Suspend:** The **Suspend** option captures the current system state to the suspend SR and allows the VM to resume from that particular state. The `xe vm-suspend` command can be used to suspend the VM from the command line.
- **Resume:** The **Resume** option allows the VM to continue from the state that it was in, when the VM was suspended. The `xe vm-resume` command can be used to resume the VM from the command line.
- **Pause:** The **Pause** option captures the current system state of memory and allows the VM to resume from that particular state. The `xe vm-pause` command is used to pause a VM and can only be performed from the command line.
- **Unpause:** The **Unpause** option allows the VM to continue from the state that it was in, when the VM was suspended. The `xe vm-unpause` command is used to unpause a VM and can only be performed from the command line.

Copying a VM

Copying a VM creates a duplicate of an existing VM within the XenServer environment. There are two types of VM copying supported by XenServer 6.2:

- **Full copy:** Full copy makes a complete copy of the VM's disks. The full copy operation takes longer to complete than the fast clone operation, but creates a copy of the VM that is independent of the original VM.
- **Fast clone:** Fast clone or copy-on-write speeds up the cloning process by utilizing the original VM's hard disk in order to perform read operations and copies the data to a separate differencing disk, when a write operation needs to be performed. Copy-on-write is designed to save disk space and allow fast clones, but can slightly slow down normal disk performance.

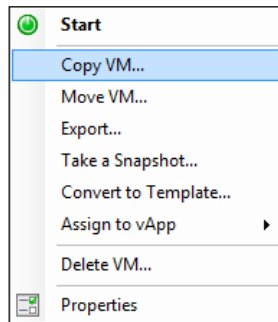



When using fast clones, the hard disk of the original VM is required by all of the VM's clones, as the original hard disk is used for read operations.

Copying a VM (using the GUI)

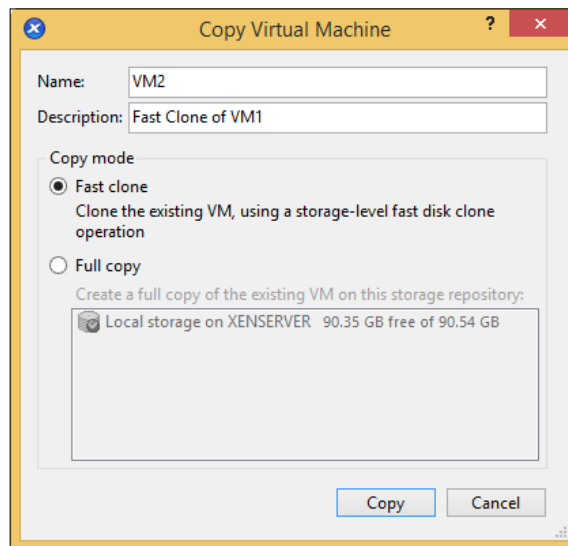
The following steps cover the process of copying an existing VM using the XenCenter GUI:

1. Right-click on the VM and click on **Copy VM...**



 The VM must be powered off to perform a copy operation.

2. Enter a name and description for the VM clone, select the appropriate copy mode, and click on **Copy** to begin the copy operation.



Copying a VM (using the CLI)

The following steps cover the process of copying an existing VM using the `xe` command from the command-line interface:

1. Run the `xe vm-copy` command to copy the VM:
`xe vm-copy vm=original_vm_name new-name-label=new_vm_name`
2. The following screenshot shows you how to copy a VM:

```
[root@XENSERVER1 ~]# xe vm-copy vm=VM1 new-name-label=VM2
ae1251b9-2b37-f22b-1bc9-1ce6dc16266d
[root@XENSERVER1 ~]#
```

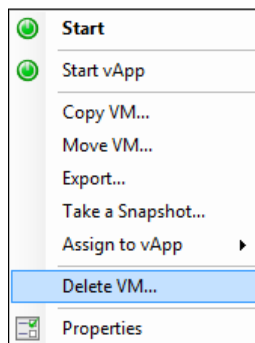
Deleting VMs

Decommissioning a server is typically one of the last steps in the life cycle of a server and in a physical environment, it generally entails powering off the hardware and disposing of it or repurposing it. The decommissioning process in a virtual environment usually involves deleting the VM to free up resources for other VMs in the environment. Deleting the VM removes VM configuration information or metadata as well as the associated virtual disks.

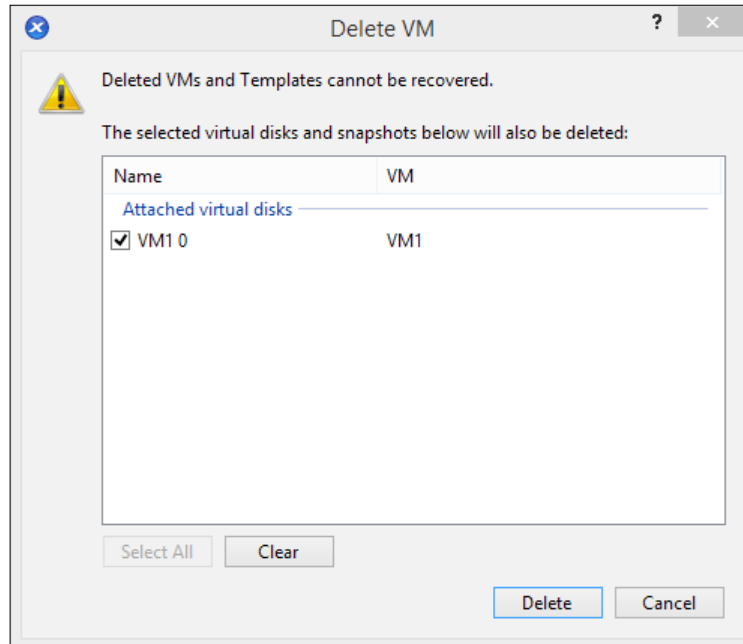
Deleting a VM (using the GUI)


The following steps cover the process of deleting a VM using the XenCenter GUI:

1. Shut down the VM.
2. Right-click on the VM and click on **Delete VM...**



3. Check whether to remove any associated virtual disks and snapshots along with the VM's configuration information. Click on **Delete** to delete the VM.




 The VM deletion process cannot be reversed and it is important that VM backups are properly maintained.

Deleting a VM (using the CLI)

The following steps cover deleting a VM using the `xe` command from the command-line interface:

1. Shut down the VM.

 A VM can be forcefully shutdown using the `xe vm-shutdown` command with the `force=true` parameter.

2. Run the `xe vm-list` command to retrieve the UUID value of the VM:
`xe vm-list name-label=vm_name --minimal`

The following screenshot shows you how to retrieve the UUID value of a VM:

```
[root@XENSERVER1 ~]# xe vm-list name-label=VM2 --minimal
ae1251b9-2b37-f22b-1bc9-1ce6dc16266d
[root@XENSERVER1 ~]#
```

3. Run the `xe vm-destroy` command to delete the VM:
`xe vm-destroy uuid=vm_uuid`

The following screenshot shows you how to delete a VM:

```
[root@XENSERVER1 ~]# xe vm-destroy uuid=ae1251b9-2b37-f22b-
-1bc9-1ce6dc16266d
[root@XENSERVER1 ~]#
```

VM snapshots

A VM snapshot is a point-in-time checkpoint of a VM. The snapshot provides a mechanism to revert the VM to the exact state that it was in, when the snapshot was created. Snapshots are used in a variety of scenarios, but they are most commonly used as a rollback option, when performing software or system upgrades.

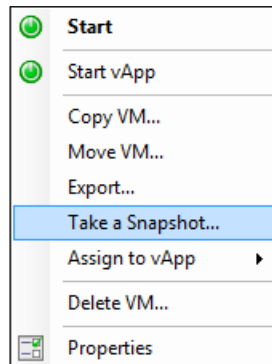
The following are the types of snapshots available in Citrix XenServer 6.2:

- **Disk-only snapshots:** Disk-only snapshots store a VM's configuration information and virtual disks. This type of snapshot can be performed on VMs with any guest operating system.
- **Quiesced snapshots:** Quiesced snapshots are a feature available on Windows guest operating systems that provide application-consistent point-in-time snapshots by utilizing the Windows Volume Shadow Copy Service. XenServer Tools must be installed in the VM to utilize disk and memory snapshots.
- **Disk and memory snapshots:** Disk and memory snapshots save the VM's memory state along with the VM's configuration information and virtual disks. XenServer Tools must be installed in the VM to utilize disk and memory snapshots.

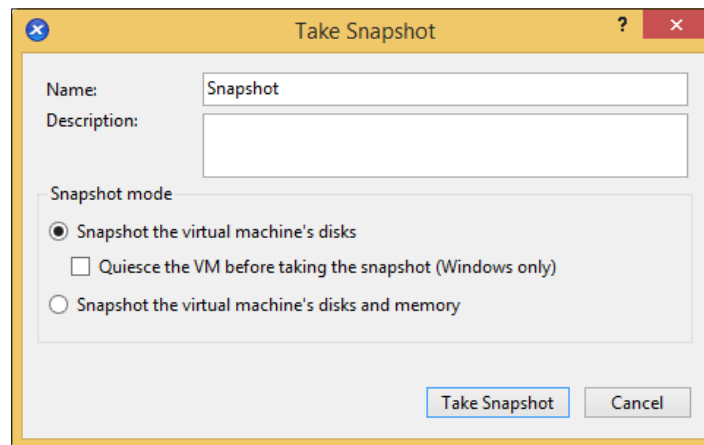
Creating a snapshot (using the GUI)

The following steps cover the process of creating a VM snapshot using the XenCenter GUI:

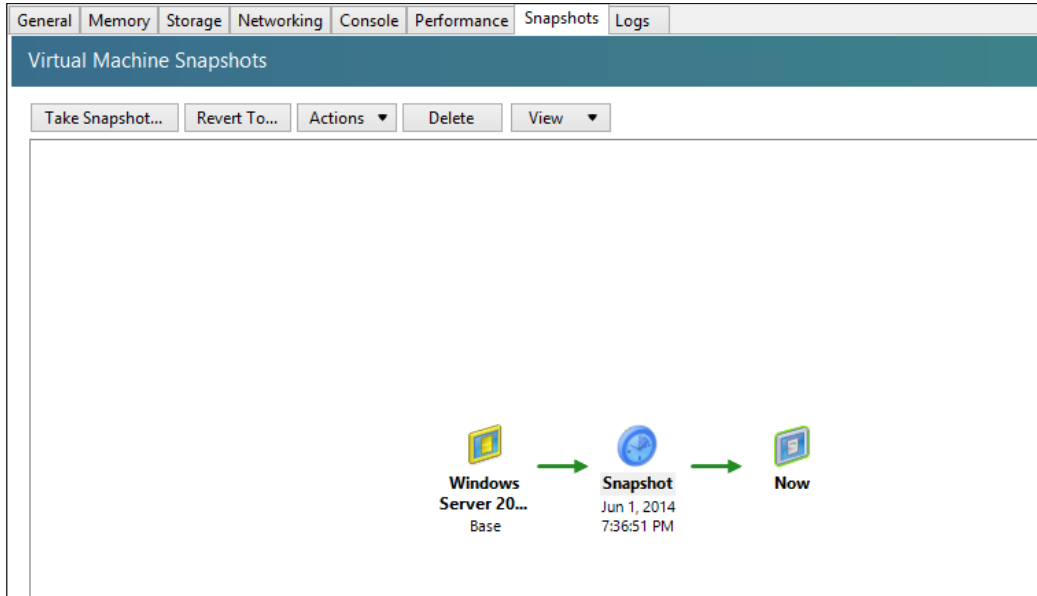
1. Right-click on the VM and click on **Take a Snapshot...**



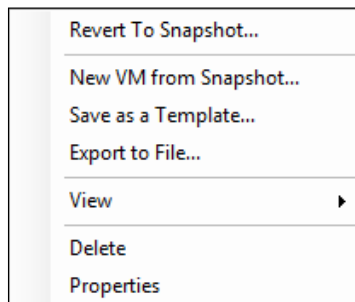
2. Enter a name and description for the snapshot. Select the appropriate snapshot mode and click on **Take Snapshot** to begin capturing the snapshot.



3. The following screenshot shows the snapshot that was created:



There are several actions that can be performed on a snapshot. Right-clicking on a snapshot displays the following menu:



The menu is explained as follows:

- **Revert To Snapshot...:** The **Revert To Snapshot...** option restores the VM to the point-in-time when the snapshot was taken and removes any changes made since the snapshot was taken
- **New VM from Snapshot...:** The **New VM from Snapshot...** option creates a new VM from the point-in-time state of the original VM

- **Save as a Template...:** The **Save as a Template...** option copies the snapshot and converts the copy of the snapshot to a template
- **Export to File...:** The **Export to File...** option exports the snapshot in the XVA format, which can be used for exporting VMs for backup purposes
- **Delete:** The **Delete** option removes the snapshot(s) and commits all the changes made after the snapshot was taken

Creating a snapshot (using the CLI)

The following steps cover the process of creating a VM snapshot using the `xe` command from the command-line interface:

1. Run the `xe vm-snapshot` command to create a snapshot of the VM:

```
xe vm-snapshot vm=vm_name new-name-label=snapshot_name
```

The following screenshot shows you how to create a snapshot of a VM:

```
[root@XENSERVER1 ~]# xe vm-snapshot vm=VM1 new-name-label="Snapshot1"
905c1587-0d0a-0490-996b-fe73def95305
[root@XENSERVER1 ~]#
```

2. The `xe snapshot-list` command can be used to view the snapshots present on a VM here:

Run the `xe vm-list` command to view the UUID value of the VM:

```
xe vm-list name-label=vm_name --minimal
```

The following screenshot shows you how to retrieve the UUID value of a VM:

```
[root@XENSERVER1 ~]# xe vm-list name-label=VM1 --minimal
662c0a86-f3a3-e384-8d93-3c3f62bfaac5
[root@XENSERVER1 ~]#
```

3. Run the `xe snapshot-list` command to view the snapshots on the VM. The UUID value of the VM is used to list the snapshots on the designated VM:

```
xe snapshot-list snapshot-of=vm_uuid
```

The following screenshot shows you the snapshots present on the VM:

```
[root@XENSERVER1 ~]# xe snapshot-list snapshot-of=662c0a86-f3a3-e384-8d93-3c3f62bfaac5
uuid ( RO)                : 905c1587-0d0a-0490-996b-fe73def95305
name-label ( RW)         : Snapshot1
name-description ( RW) :
```

VM templates

XenServer comes with several built-in templates for various operating systems but also provides the ability to create custom templates to allow administrators to deploy VMs based on templates that are created by the administrator. A template is a VM encapsulated into a file that contains the defined configuration settings for the processors, memory, disks, and networking. Templates are commonly used to rapidly deploy new VMs with the desired configuration settings that are defined in the template, which ensures consistent VM provisioning. Templates are generally utilized to provision VMs from a base configuration in order to reduce the time required to configure new VMs and differs from cloning or copying existing VMs, which are commonly used to create an exact replica of this VM for testing purposes.

Creating a custom VM template (using the GUI)

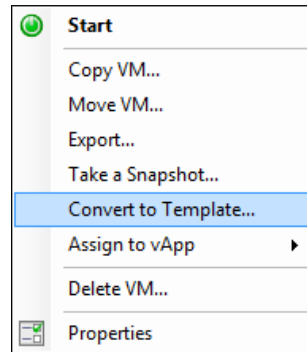
The following steps cover the process of creating a VM template using the XenCenter GUI:

1. Shut down the VM.

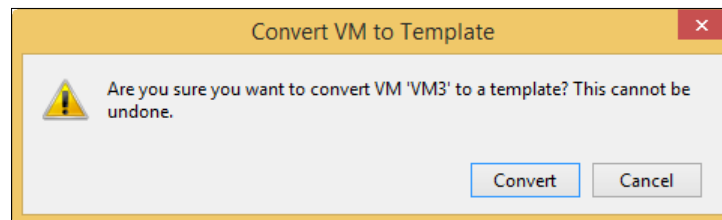



A powered on VM cannot be converted to a template. A template can be created from a VM snapshot to avoid powering off a VM.

2. Right-click on the VM and click on **Convert to Template...**



3. Click on **Convert** to convert the VM to a template. Once a VM has been converted to a template, the process cannot be reversed from within Citrix XenCenter.

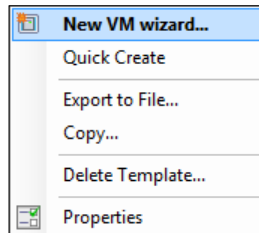


[ Ensure that all the desired changes have been made to the VM before you convert it to a template.]

The new template has been created and can now be used to provision new VMs, which utilize the same settings as the template. The new template appears under the XenServer host in XenCenter, as shown in the following screenshot:

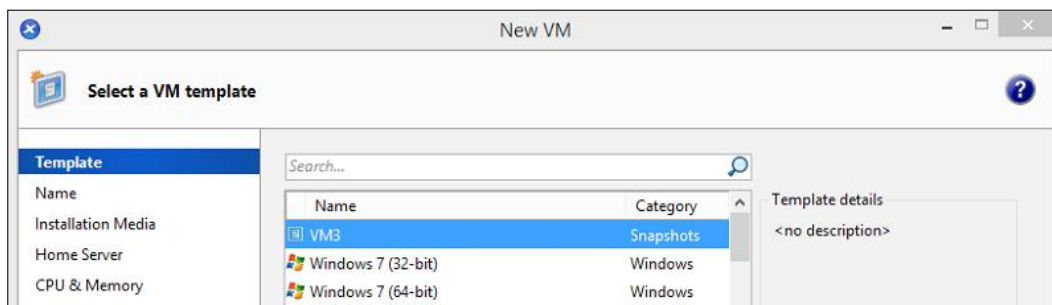


After the VM has been converted to a template, we can now use the template to create new VMs. The following screenshot displays the options available for creating a new VM from a template:




The following options are available for creating a new VM from a template:

- **New VM wizard...:** The **New VM wizard...** option launches the wizard to create a new VM but utilizes the selected template, by default. The following screenshot shows the VM that is converted to a template, as the option is selected, by default:



- **Quick Create:** The **Quick Create** option creates a VM based upon the template selected without the option to change any settings before the VM is created.

[ The **Quick Create** option is best suited for situations in which rapid provisioning is desired. This eliminates the need to create a new VM using the VM wizard.]

Creating a custom VM template (using the CLI)

The following steps cover the process of creating a custom VM template using the `xe` command from the command-line interface:

1. Run the `xe vm-list` command to view the UUID value of the VM to convert to a template:

```
xe vm-list name-label=vm_name
```

The following screenshot shows you how to view the UUID value of a VM:

```
[root@XENSERVER1 ~]# xe vm-list name-label=VM2
uuid ( RO)           : 03d786f1-c6b6-3750-19e9-7d36399c788c
name-label ( RW)    : VM2
power-state ( RO)   : halted
```

2. Run the `xe vm-param-set` command to convert the VM into a template:

```
xe vm-param-set uuid=vm_uuid is-a-template=true
```

The following screenshot shows you the VM being converted to a template:

```
[root@XENSERVER1 ~]# xe vm-param-set uuid=03d786f1-c6b6-3750-19e9-7d36399c788c is-a-template=true
[root@XENSERVER1 ~]#
```

3. The `xe template-list` command can be used to verify that the VM has been converted to a template, as shown in the following screenshot:

```
[root@XENSERVER1 ~]# xe template-list name-label=VM2
uuid ( RO)           : 03d786f1-c6b6-3750-19e9-7d36399c788c
name-label ( RW)    : VM2
name-description ( RW) :
```

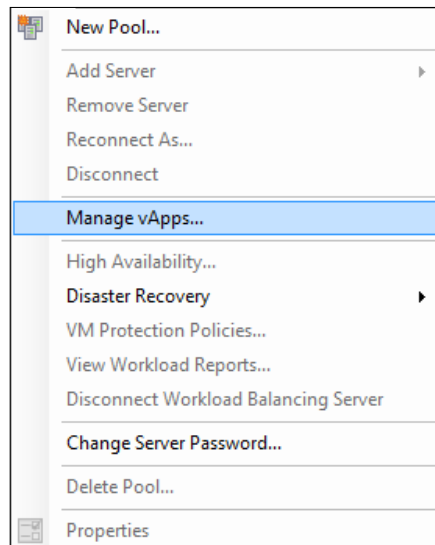
vApps

A vApp is a logical group of one or more related VMs, which can be managed as a single object. vApps are commonly used to manage multi-tier applications such as a three-tier web, middleware, and database stack for a website. The vApp allows the stack to be managed like a single VM for operations such as starting and shutting down the stack. vApps also allow start orders and delay intervals to be defined for the VMs in the vApp. Start orders define the order in which VMs within the vApp are started, and delay intervals define the amount of time between the startup of the VMs. In a three-tier web, middleware, and database stack, the start order is defined to startup the VMs in a particular order first by bringing up the database VM, then the middleware VM, and finally, the web VM. In addition to the start order, it is often required that the database VM is active prior to the other VMs requesting any data from the database and so the delay interval is used to ensure that the database VM has enough time to boot before the other VMs are brought up. vApps can reside on different hosts in a pool.

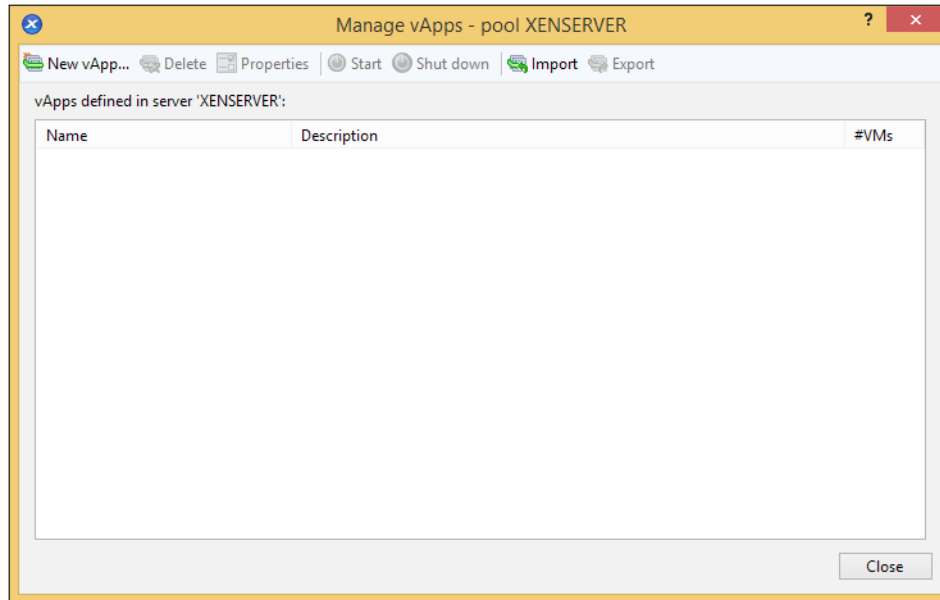
Creating a vApp (using the GUI)

The following steps cover the process of creating a vApp using the XenCenter GUI:

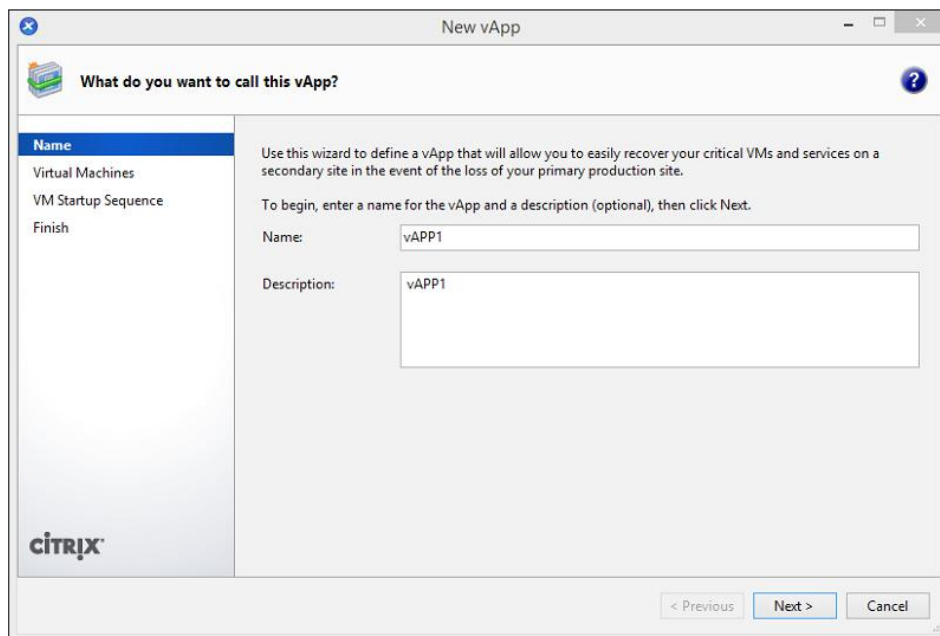
1. From the **Pool** menu, select **Manage vApps...** to launch the **Manage vApps** dialog box.



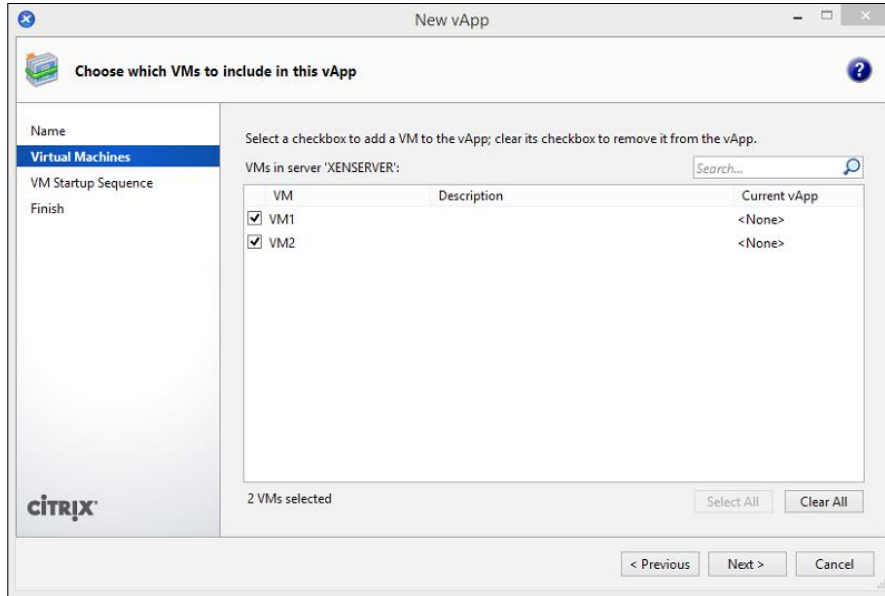
2. Click on **New vApp...**, at the top-left corner of the **Manage vApps** dialog box, to launch the **New vApp...** wizard.



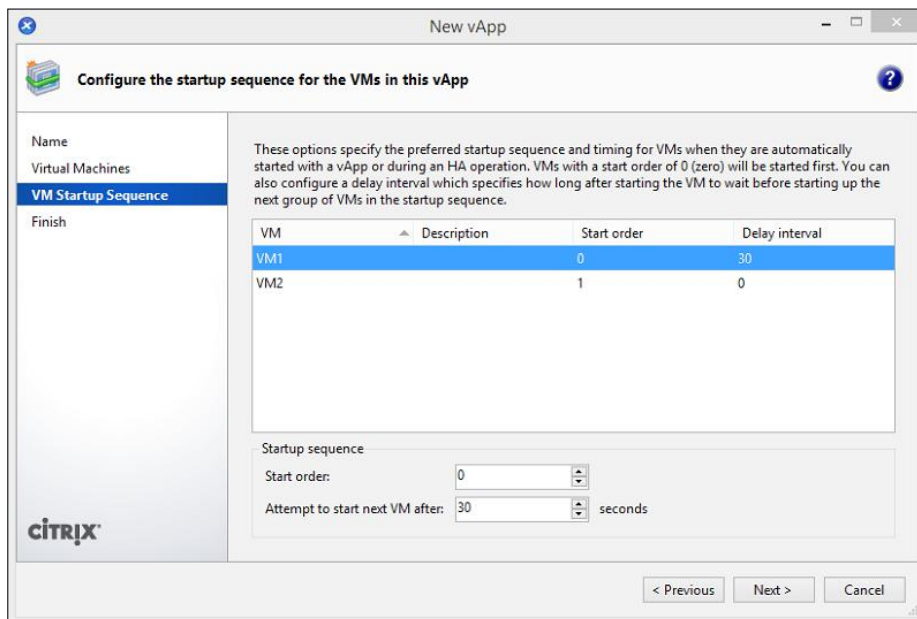
3. Enter the name of the new vApp and a description, and then click on **Next**.



4. Select which VMs to include in the vApp and click on **Next** to continue.



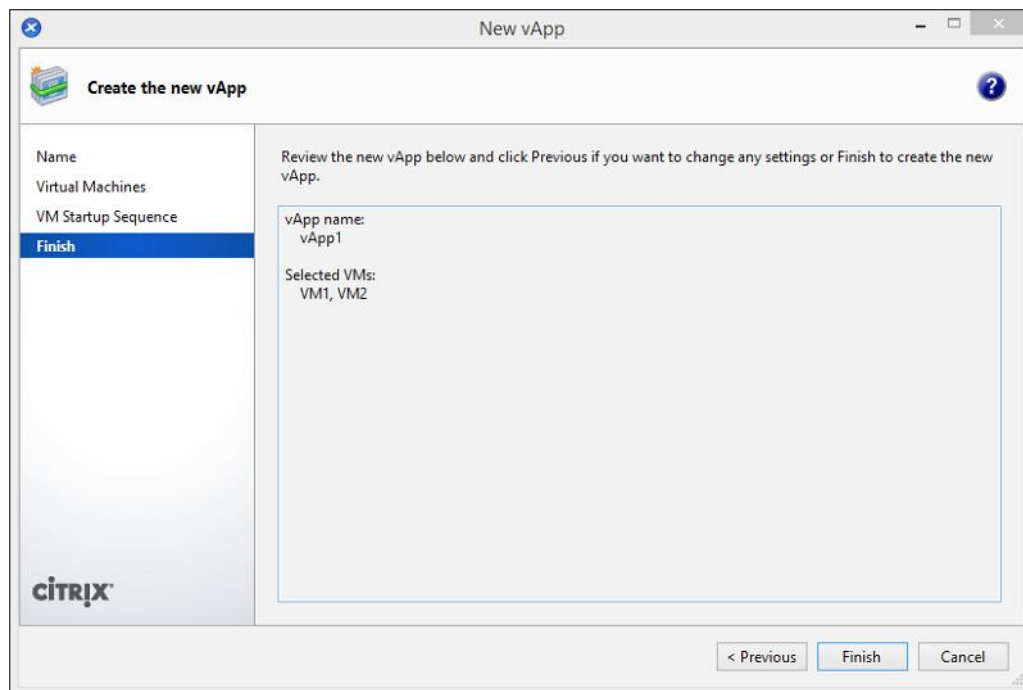
5. Configure the start order and delay interval for each of the VMs in the vApp, and then click on **Next**.



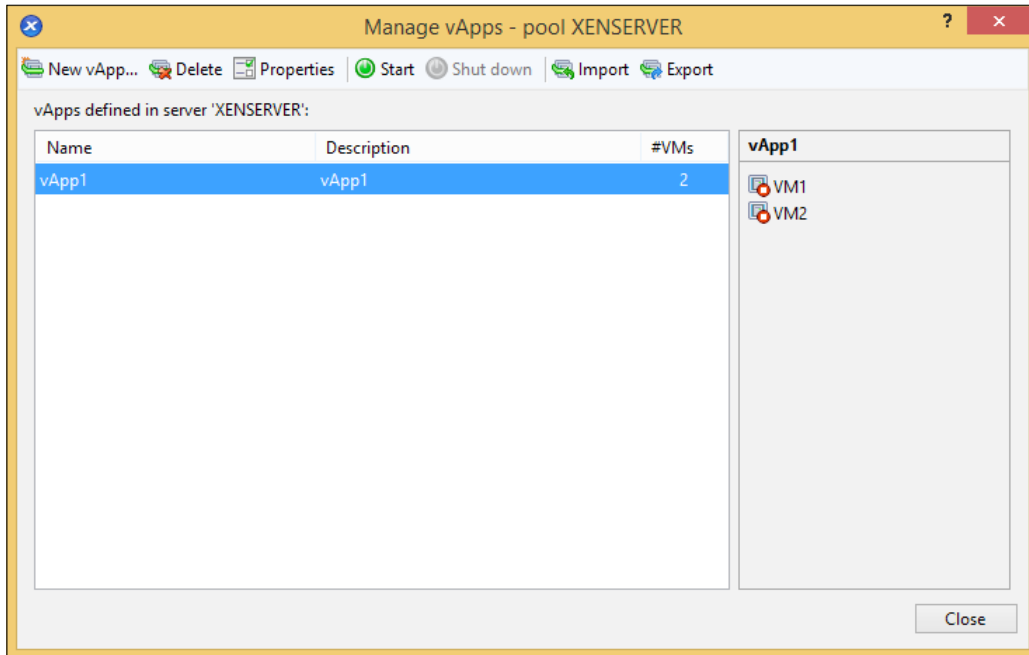
The start order and delay interval are explained as follows:

- **Start order:** This is used to determine the order in which the VMs within the vApp are started in relation to one another. VMs with a lower number are started before VMs with a higher number.
- **Delay interval:** This specifies the amount of time to wait prior to powering on the next VM in the start order.

6. Review the settings selected and click on **Finish** to create the vApp.



7. The following screenshot displays the vApp that we just created in the previous step.



Creating a vApp (using the CLI)

The following steps cover the process of creating a vApp using the `xe` command from the command-line interface:

1. Run the `xe appliance-create` command to create the vApp. The UUID value of the vApp is required when adding a VM to the vApp and is outputted following the execution of the command:

```
xe appliance-create name-label=vapp_name
```

The following screenshot shows you how to create the vApp:

```
[root@XENSERVER1 ~]# xe appliance-create name-label=vApp1  
1b56af45-0903-323b-c041-9c4e7c5b0cc0  
[root@XENSERVER1 ~]#
```

2. Run the `xe vm-list` command to retrieve the UUID value of the machine(s) to be added to the vApp:

```
xe vm-list name-label=vm_name
```

The following screenshot shows you how to view the UUID value of a VM:

```
[root@XENSESERVER1 ~]# xe vm-list name-label=VM1
uuid ( RO)           : 662c0a86-f3a3-e384-8d93-3c3f62bfaac
5
    name-label ( RW) : VM1
    power-state ( RO) : halted
```

3. Run the `xe vm-param-set` command to add the VM(s) to the vApp:

```
xe vm-param-set uuid=vm_uuid appliance=vapp_uuid
```

The following screenshot shows you the VM being added to the vApp:

```
[root@XENSESERVER1 ~]# xe vm-param-set uuid=662c0a86-f3a3-e3
84-8d93-3c3f62bfaac5 appliance=1b56af45-0903-323b-c041-9c4
e7c5b0cc0
```

4. The `xe appliance-list` command can be used to verify that the VM has been added to the vApp, as shown in the following screenshot:

```
[root@XENSESERVER1 ~]# xe appliance-list
uuid ( RO)           : 1b56af45-0903-323b-c041-9c4e
7c5b0cc0
    name-label ( RW) : vAppl
    name-description ( RW) :
        VMs (SRO) : 662c0a86-f3a3-e384-8d93-3c3f
62bfaac5
    allowed-operations (SRO) : start
    current-operations (SRO) :
```


Importing and exporting VMs

Citrix XenServer supports the ability to import VMs along with exporting them. Imported VMs can be VMs that were previously exported from Citrix XenServer or from another virtualization platform such as VMware vSphere or Microsoft Hyper-V. Importing VMs is often done to migrate a VM from one XenServer deployment to another or to utilize a prebuilt appliance typically provided by a third-party vendor. Many of the same reasons apply as to why we would want to export a VM. Exporting a VM can be used to create a backup of the VM to ensure that the VM can be restored in the event of a disaster or can be used for testing a VM in a development environment. Citrix XenServer supports four formats for importing and exporting VMs, the formats are listed as follows:

- **Open Virtualization Format (OVF):** The OVF format is an open standard for packaging and distributing a virtual appliance consisting of one or more VMs. The OVF format provides support for portability of the VM between hypervisors such as Hyper-V and ESXi as well as securing the VM from tampering and including a license agreement. The file extension for the OVF format is `.ovf`.
- **Open Virtual Appliance (OVA):** The OVA format is an OVF encapsulated into a single file. The OVA format offers the same benefits as that of the OVF format, but additionally it encapsulates the VM or vApp into a single file. While the OVA format makes the distribution easier, the import and export process takes longer to complete than the OVF format. The file extension for the OVA format is `.ova`.
- **XVA:** The XVA format is a XenServer-specific format for packaging a single VM into a single file. The XVA format is used between XenServer hosts and when importing and exporting using the CLI. The file extension for the XVA format is `.xva`.
- **XVA Version 1:** The XVA Version 1 format is the format originally used for packaging a VM as a single archive for Xen-based hypervisors. The file extension for the XVA Version 1 format is `ova.xml`.



A VM exported from a XenServer host to a XenServer host with a different CPU type might not run properly.

Operating System Fixup

Operating System Fixup is a XenServer feature that aims to ensure that VMs created on other virtualization platforms will function properly when imported into Citrix XenServer. During the fixup process, the VM automatically boots to an ISO image that performs the repair operations on the VM and then shuts down the VM. The repair operation makes driver changes and disables any VM integration tools for virtualization platforms other than XenServer.

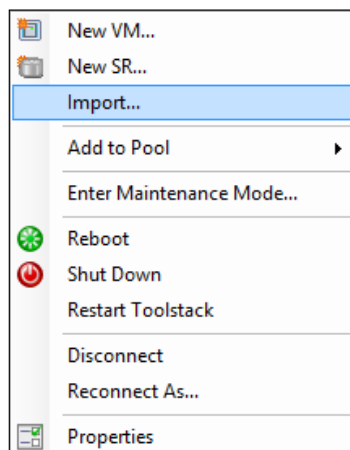
The transfer VM

The transfer VM is a built-in VM that is used to transfer the disk image data between the disk image location and the XenServer SR during the import or export operations. The default transfer protocol used by the transfer VM is iSCSI and requires an iSCSI initiator on the XenServer host. The RawVDI transfer protocol can be used instead of iSCSI to transfer data.

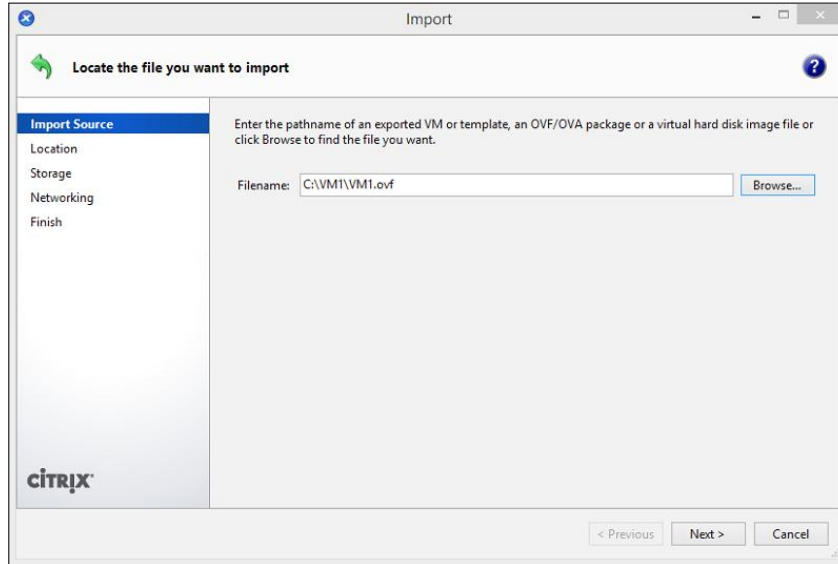
Importing a VM (using the GUI)

The following steps cover the process of importing a previously exported VM in the OVF format using the XenCenter GUI.

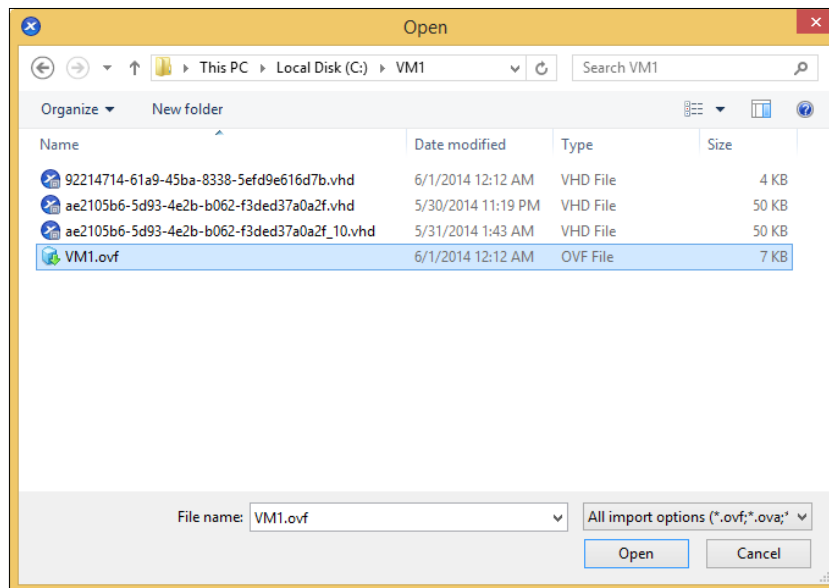
1. Right-click on the desired pool or server to host the VM and click on **Import...** to launch the **Import** wizard.



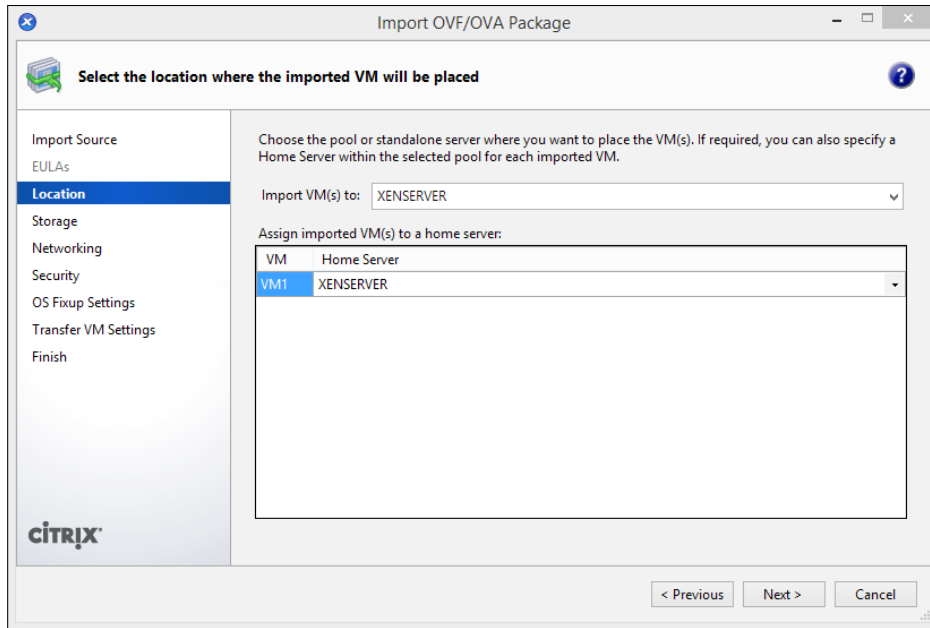
2. Click on **Browse...** to locate the `.ovf` file to be imported, then click on **Next** to continue.



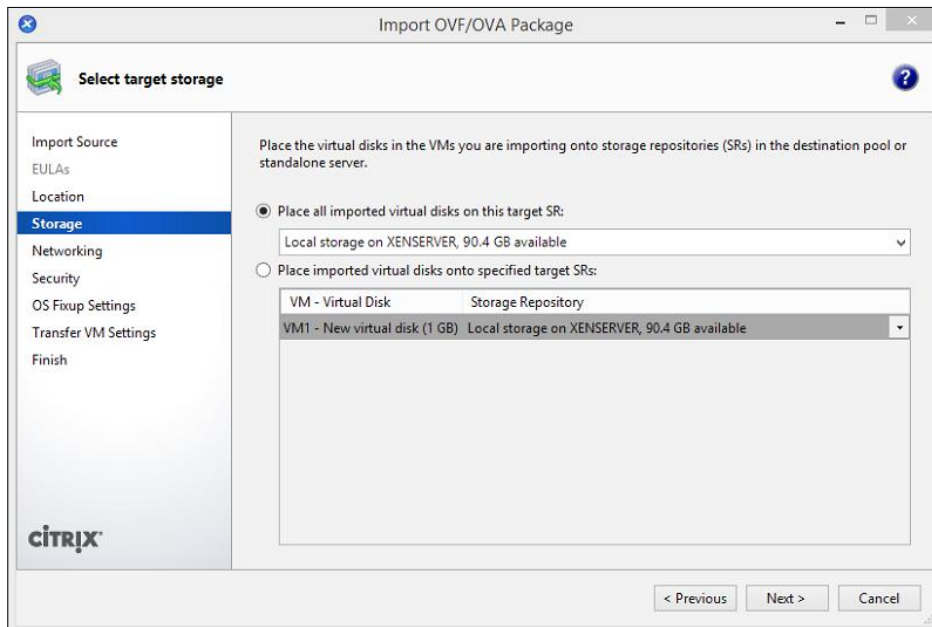
The following screenshot shows you the files that make up an OVF VM export:



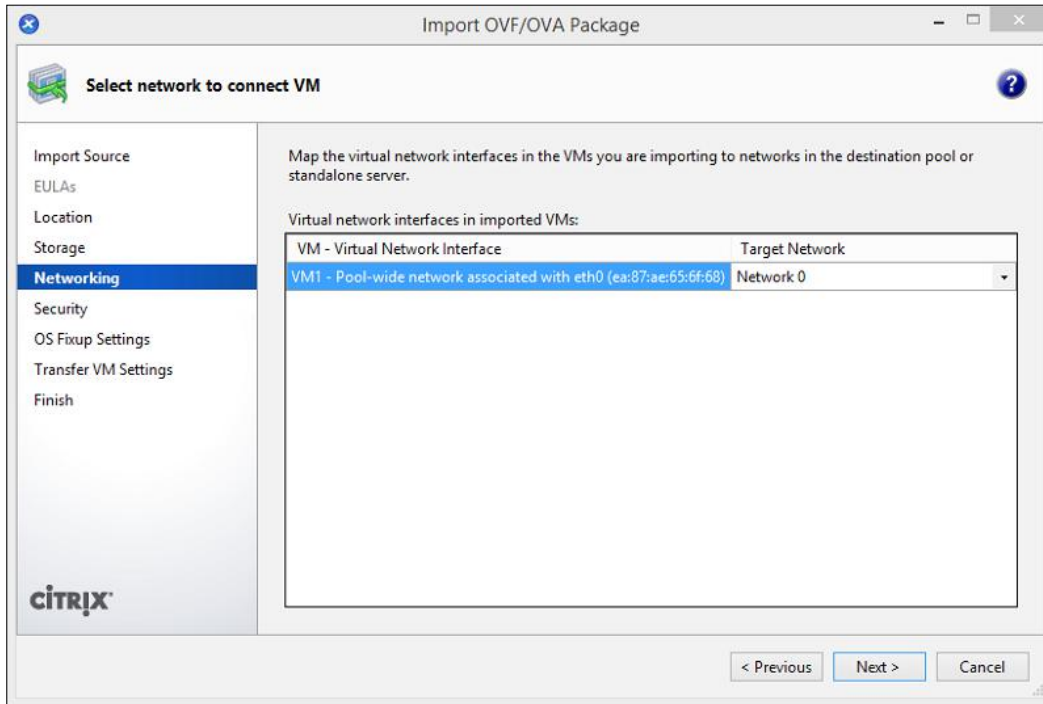
3. Select the pool or server that will host the VM. Click on **Next** to continue.



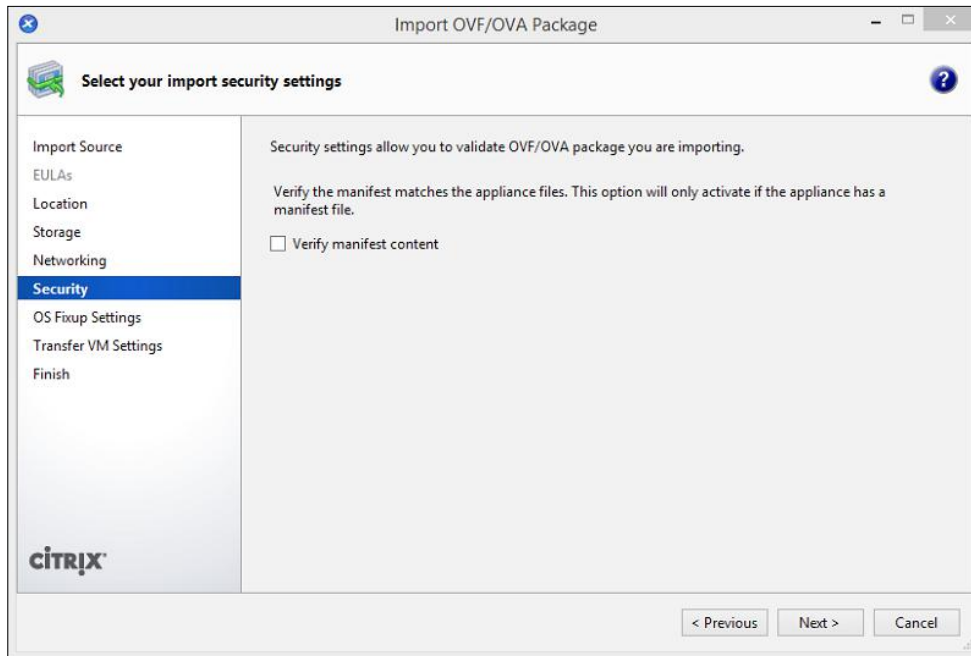
4. Select the SR where the VM will be stored. Click on **Next** to continue.



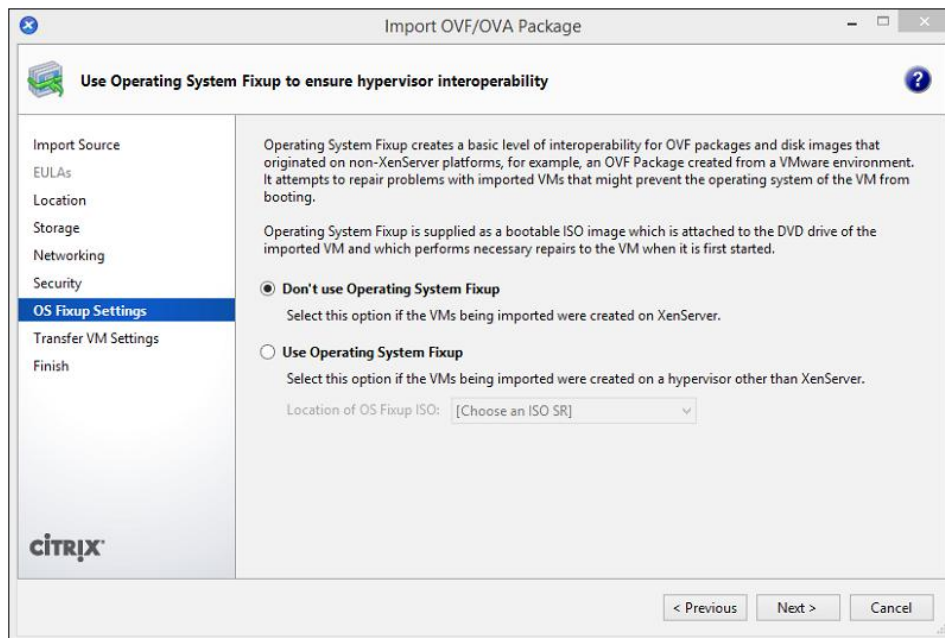
5. Select the network for the VM's network interface(s). Click on **Next** to continue.



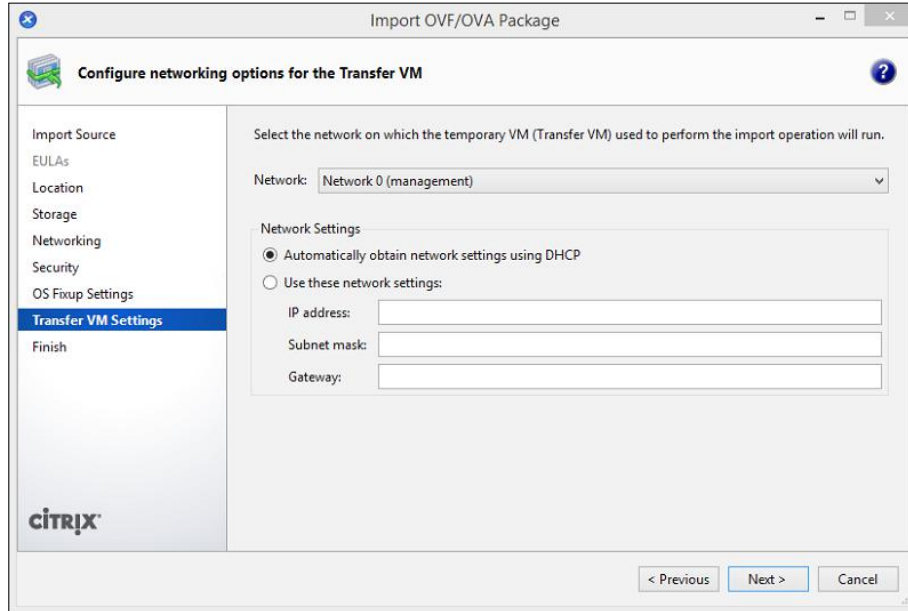
6. Optionally, select **Verify manifest content** in order to verify that the manifest matches the exported VM files. Click on **Next** to continue.



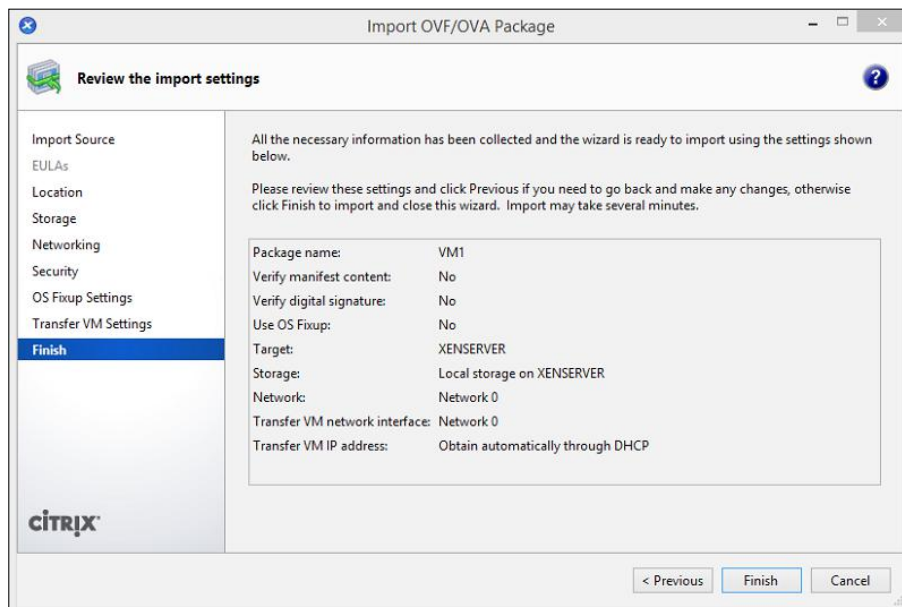
7. Select whether to use the Operating System Fixup feature and click **Next** to continue.



- Configure the appropriate network settings for the transfer VM during the VM import process and click on **Next** to continue.



- Review the settings selected and click on **Finish** to begin the import process.



Importing a VM (using the CLI)

The following steps cover the process of importing a previously exported VM in the .xva format using the `xe` command from the command-line interface:

1. Run the `xe vm-import` command to import the VM to the XenServer host:

```
xe vm-import -s host_ip_address -u username -pw password vm=vm_name filename=filepath_and_filename
```

The following screenshot shows you how to import a VM:

```
c:\Program Files\Citrix\XenCenter>xe vm-import -s 192.168.1.251 -u root -pw password vm="Windows 7" filename=C:\XenServerBackups\Windows7Backup.xva
662c0a86-f3a3-e384-8d93-3c3f62bfaac5
```

2. Run the `xe vm-list` command to verify that the VM has been imported successfully:

```
xe vm-list -s host_ip_address -u username -pw password name-label=vm_name
```

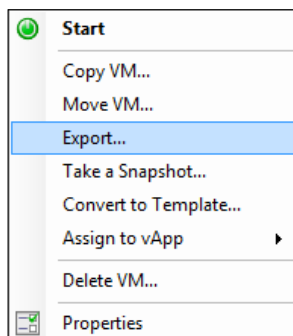
The following screenshot shows you the imported VM:

```
c:\Program Files\Citrix\XenCenter>xe vm-list -s 192.168.1.251 -u root -pw password name-label="Windows 7"
uuid ( RO): 662c0a86-f3a3-e384-8d93-3c3f62bfaac5
name-label ( RW): Windows 7
power-state ( RO): halted
```

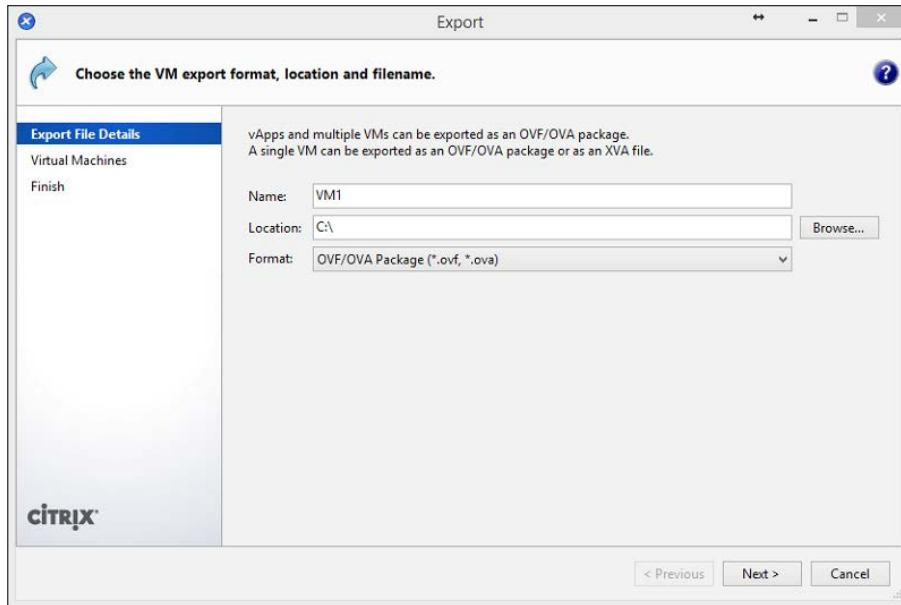
Exporting a VM (using the GUI)

The following steps cover the process of exporting a VM in the OVF format using the XenCenter GUI:

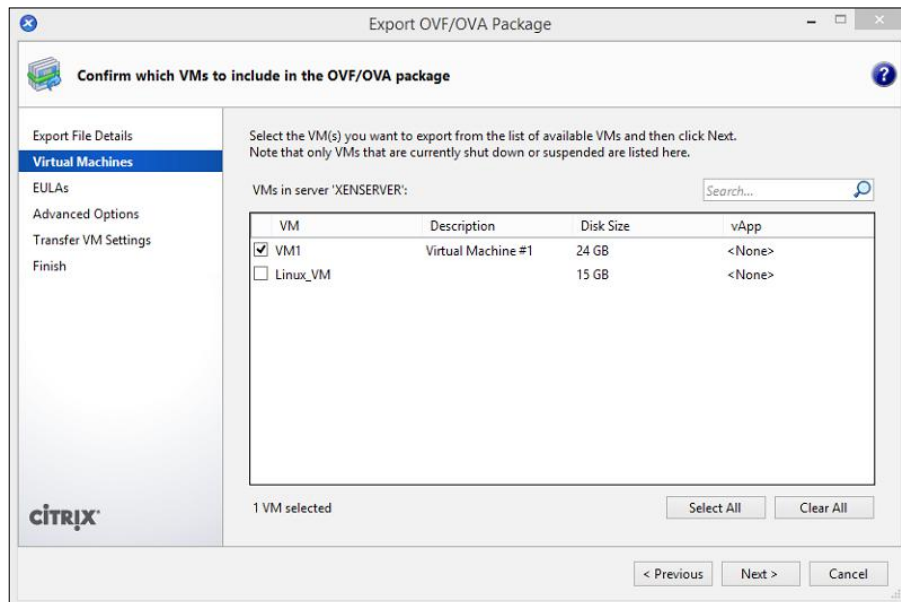
1. Select the pool or server containing the VM, right-click on the VM and click on **Export...**



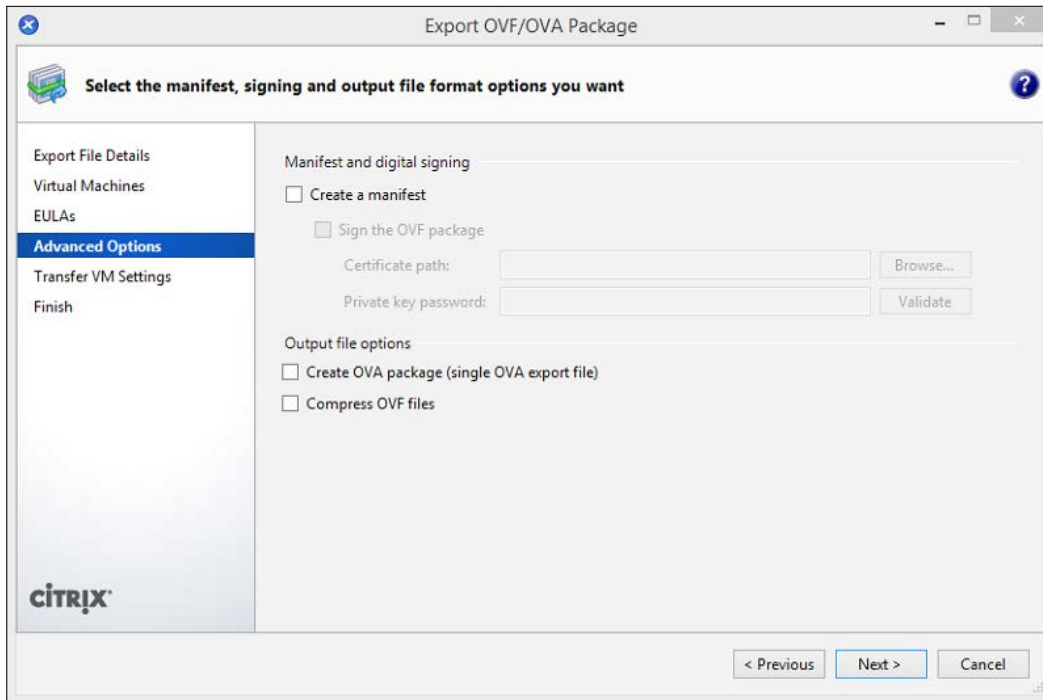
2. Enter the name that will be used for the exported file, specify the folder where the files will be saved, and select **OVF/OVA Package (*.ovf, *.ova)** from the **Format** list and then click on **Next**:



3. Select the VMs to be exported and click on **Next** to continue.



4. Optionally, you can add an **End User License Agreement (EULA)** into the textbox provided. Click on **Next** to continue.
5. Select the appropriate options and click on **Next** to continue.



Manifest

The **Create a manifest** option creates an inventory or a list of the other files in a package and is used to ensure that the files originally included when the package was created are the same files present when the package arrives. XenServer makes use of checksum file to ensure the integrity of the files.

OVF package signing

The **Sign the OVF package** option is used to verify the package creator's identity by using the certificate's public key in order to validate the digital signature. Package signing adds an additional layer of security as it can be used to ensure that the OVF package has been provided by a trusted provider.

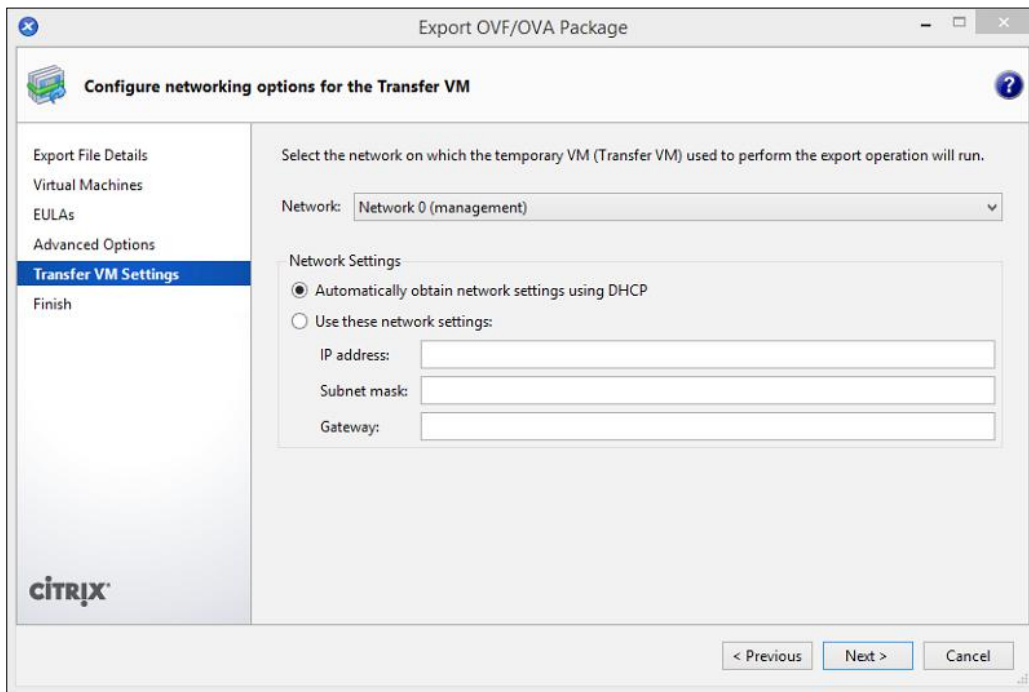
Create OVA package

The **Create OVA package (single OVA export file)** option packages the VM into a single file.

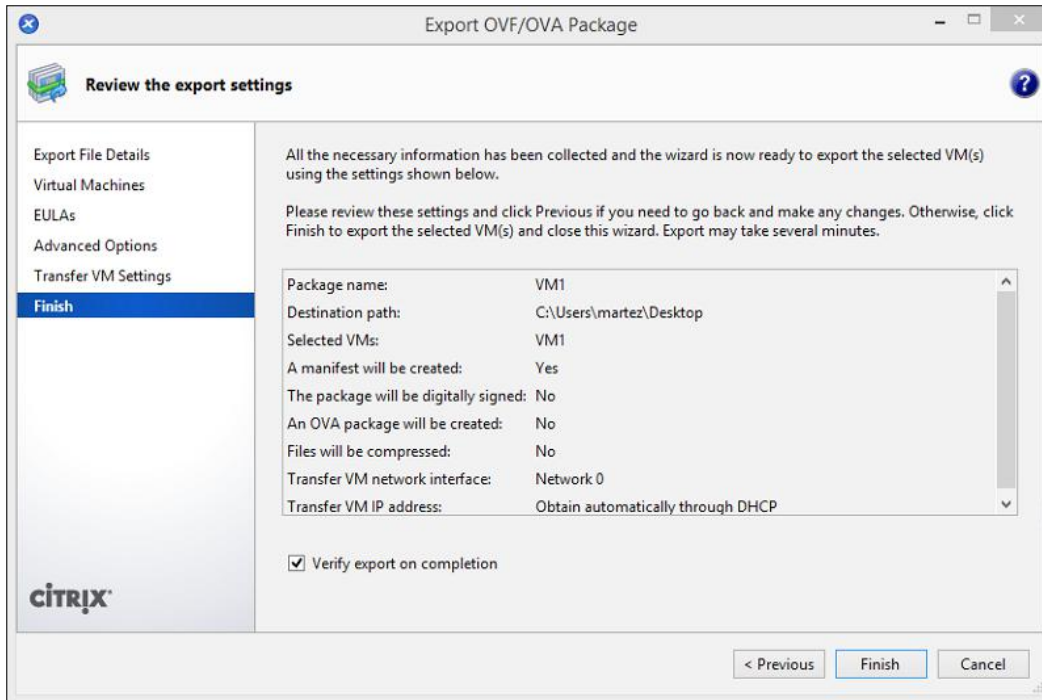
Compress OVF files

The **Compress OVF files** option ensures that the virtual hard disk images only consume the amount of space that is actually used. This means that if a VM uses only 5 GB of hard disk space but is provisioned for 15 GB, the final VM export will consume only the 5 GB that is used. The following steps cover exporting a VM:

1. Configure the appropriate network settings for the transfer VM during the VM export process and click on **Next** to continue.



- Review the settings selected, optionally select the **Verify export on completion** checkbox to verify that the VM exports successfully, and click on **Finish** to begin the export process.



Exporting a VM (using the CLI)

The following steps cover the process of exporting a VM in the XVA format using the `xe` command from the command-line interface. The command line only supports exporting VMs in the `.xva` format.

- Run the `xe vm-list` command to view the VMs on the XenServer host. The VM name will be used during the export process:

```
xe vm-list -s host_ip_address -u username -pw password
```

The following screenshot shows you how to display the VMs on a XenServer host from the command line of a Windows management station with XenCenter installed:

```
c:\Program Files\Citrix\XenCenter>xe vm-list -s 192.168.1.251 -u root -pw password
uid ( R0) : 6247ed81-4b26-8a23-3e92-ad0c991c3098
name-label ( RW): Windows 7
power-state ( R0): halted

uid ( R0) : 4552f445-5d43-4f21-9c00-c50a11c5c717
name-label ( RW): Control domain on host: XENSERVER1
power-state ( R0): running

uid ( R0) : 3e26434b-0691-4313-854b-79be33c2ba3c
name-label ( RW): Control domain on host: XENSERVER2
power-state ( R0): running

uid ( R0) : 4d25981d-61fa-d5a7-2031-af833636afcf
name-label ( RW): Windows 7 (32-bit)
power-state ( R0): running
```

2. Run the `xe vm-export` command to export the VM:

```
xe vm-export -s host_ip_address -u username -pw password vm="vm_name" filename=file_path_and_file_name
```

The following screenshot shows you how to export a VM from the command line of a Windows management station with XenCenter installed. The `.xva` file was exported to a local directory on the Windows management station.

```
c:\Program Files\Citrix\XenCenter>xe vm-export -s 192.168.1.251 -u root -pw password vm="Windows 7" filename=C:\XenServerBackups\Win7Backup.xva
Export succeeded
```

Summary

In this chapter, we covered creating VMs along with VM hardware such as vCPUs, memory, hard disks, and networking. We looked at VM management operations such as VM power states, copying VMs, and deleting VMs. We examined VM snapshots and have seen how they can be used to provide a rollback option for disaster recovery or development environments. We looked at creating custom VM templates to speed up the VM provisioning process and ensure a consistent deployment. We also covered creating vApps and the benefits of using vApps with multi-tier application stacks to manage them as a single logical unit. We examined importing and exporting VMs, which allow us to migrate VMs from other virtualization platforms as well as use VM exports for backing up or distributing VMs. In the next chapter, we will focus on ensuring the availability of the XenServer environment.

5

Ensuring Availability

A primary goal for all IT departments is to ensure that systems are highly available and that users or customers can access the resources they need. Citrix XenServer offers a number of features that help reduce downtime for the hosted virtual machines. The **High Availability (HA)** feature reduces downtime by automatically restarting VMs from a failed server onto an active server.

In this chapter, we'll learn about the following topics:

- Resource pools
- XenMotion
- Storage XenMotion
- HA

Resource pool overview

A resource pool allows multiple XenServer servers to be managed as a single entity. This functionality allows compute and memory resources to be aggregated along with ensuring a consistent configuration across hosts in the pool. In addition to the aggregation of resources, resource pools allow the dynamic migration of VMs between servers as well as the ability to restart a VM on another server in the event of server failure. Citrix XenServer 6.2 supports up to 16 hosts in a resource pool. There are two types of resource pools, both of which are explained as follows:

- **Homogeneous resource pools:** A homogeneous resource pool is composed of servers that contain processors made by the same vendor such as Intel or AMD, the same processor model, and the same processor features or extensions.

- **Heterogeneous resource pools:** A heterogeneous resource pool is composed of servers that contain processors made by the same vendor such as Intel or AMD. Unlike a homogeneous resource pool, the processors in a heterogeneous resource pool are different models and have different features. To accommodate the difference in features, a process known as **CPU masking** is used to hide the features on the newer processors to ensure that all of the servers in the pool use a common set of CPU features. This feature is provided by the Intel VT FlexMigration and AMD-V Extended Migration technologies. This means that the CPU in the resource pool with the least feature set is used as the baseline that all the other CPUs in the resource pool have to match to. When possible, servers should be grouped into homogenous pools in order to avoid degrading the feature set of the pool.

Resource pool requirements

The following list covers the requirements for creating a new resource pool as well as joining a new server to an existing resource pool:

- The CPUs of the server joining the pool must be the same (in terms of vendor) as the CPUs on servers already in the pool.
- A host cannot be a member of another resource pool.
- No existing shared storage can be configured.
- There are no running or suspended VMs on the joining hosts.
- There are no active operations on the VMs, such as a shutdown or export operation.
- Hosts in the pool must be running the same version XenServer in addition to the same patch level.
- The system time on pool members must be synchronized with the pool master.
- Management interfaces cannot be bonded when the pool is being created. In addition, any hosts joining an existing pool cannot have a bonded management interface.
- The management interface must use a static IP address.

The pool master

When a resource pool is created, a pool master is selected during the configuration process. The pool master is a server in the pool that acts as the single management interface for all of the other hosts or members in the pool. The pool master is responsible for forwarding all commands to the pool members, ensuring a consistent configuration across the pool. This provides a simplified configuration so that when a change is made on the pool master, such as adding a new network, that change is replicated to all of the member servers in the pool.

In the event of a failure of the pool master, the pool will not be manageable until one of the pool members is promoted to the pool master or the pool master is brought back online. Each of the pool members contains all the necessary information to become a pool master. Automatic re-election of the pool master will only take place if HA is enabled. If HA is not enabled, a new pool master must be manually elected from the command line using the `xe pool-designate-new-master` command.

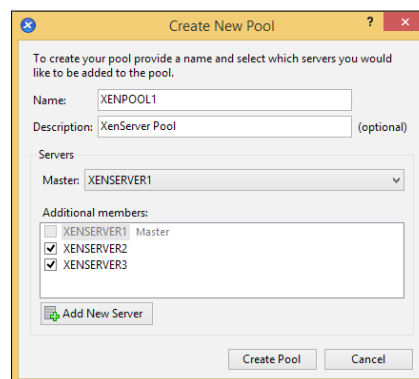
Creating a resource pool (using the GUI)

The following steps cover the process of creating a resource pool using the XenCenter GUI:

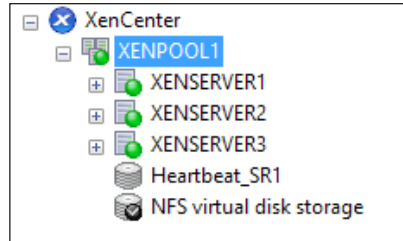
1. Press the **New Pool** button on the toolbar in XenCenter to launch the **Create New Pool** dialog box.



2. Provide a name and an optional description for the resource pool. Designate any server in the pool to become the pool master by selecting the server from the **Master** drop-down menu, select the member servers, and click on **Create Pool** to create the resource pool.



3. The following screenshot displays the pool that we just created:



Creating a resource pool (using the CLI)

The following steps cover the process of creating a resource pool using the `xe` command from the command-line interface:

1. Run the `xe pool-join` command on any server that will be a part of the resource pool. The `master-address` value is the address of the host that will be designated as the pool master:

```
xe pool-join master-address=poolmaster_address master-  
username=poolmaster_username master-password=poolmaster_password
```

The following screenshot shows you how to create a resource pool:

```
[root@XENSERVR2 ~]# xe pool-join master-address=192.168.1.251 master-  
-username=root master-password=password  
Host agent will restart and attempt to join pool in 10.000 seconds...  
[root@XENSERVR2 ~]#
```

2. The `xe pool-list` command can be used to view the information about the newly created resource pool. The command can be run from any host in the resource pool:

```
xe pool-list
```

The following screenshot shows you the information about the created resource pool:

```
[root@XENSERVR2 ~]# xe pool-list  
uuid ( RO) : 9a52fd4f-c12d-7b8d-d75a-d8bfcdded29ed  
name-label ( RW) :  
name-description ( RW) :  
master ( RO) : e5965f49-4482-4cf0-a53d-b6d4f0f6fb24  
default-SR ( RW) : 95999a85-c92a-9034-69ec-b11ce466a910
```

- The resource pool, by default, uses the name of the pool master as the name of the resource pool and it should be changed to avoid any confusion with the host itself. The `xe pool-param-set` command can be used to change the name of the resource pool:

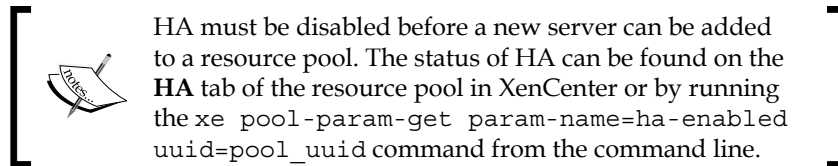
```
xe pool-param-set name-label="pool_name" uuid=pool_uuid
```

The following screenshot shows you how to change the name of a resource pool:

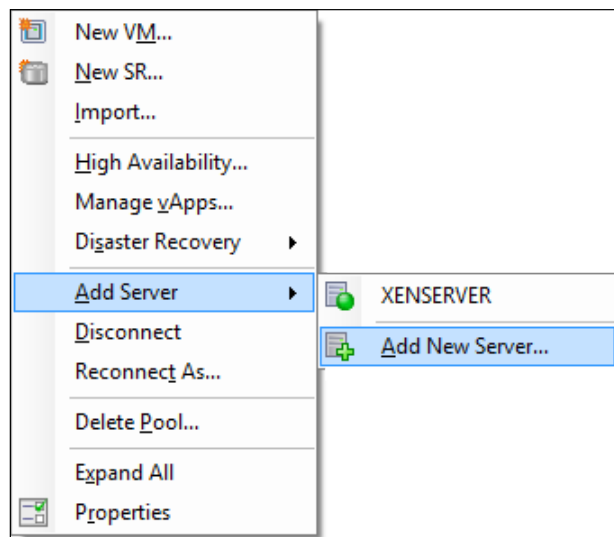
```
[root@XENSERVER2 ~]# xe pool-param-set name-label="XENPOOL1" uuid=9a52fd4f-c12d-7b8d-d75a-d8bfcdded29ed
[root@XENSERVER2 ~]#
```

Adding a host to a resource pool (using the GUI)

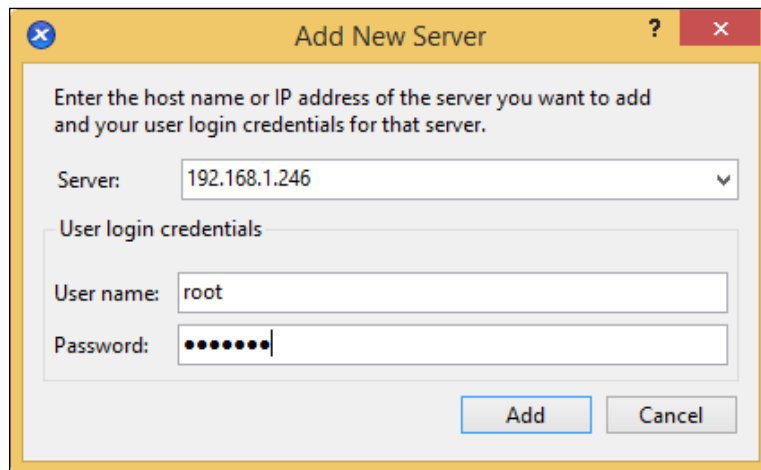
The following steps cover the process of adding a server to a resource pool using the XenCenter GUI.



- Right-click on the desired resource pool. Under the **Add Server** option, select **Add New Server...** to open the **Add New Server** dialog box.



2. Enter the IP address and user credentials for the new server and then click on **Add** to add the server to the resource pool.



After a few seconds, the new server will be added to the existing resource pool.

Adding a server to a resource pool (using the CLI)

The following command covers how to add a server to an existing resource pool using the `xe` command from the command-line interface:

```
xe pool-join master-address=poolmaster_address master-username=poolmaster_username master-password=poolmaster_password
```

The following screenshot shows you how to create a resource pool:

```
[root@XENSERVER3 ~]# xe pool-join master-address=192.168.1.251 master-username=root master-password=password
Host agent will restart and attempt to join pool in 10.000 seconds...
[root@XENSERVER3 ~]#
```

To verify that the server has been successfully added to the resource pool, the `xe host-list` command can be used to view the servers that are a part of the resource pool:

```
xe host-list
```

The following screenshot shows the servers in the resource pool:

```
[root@XENSERVER3 ~]# xe host-list
uuid ( RO)                : 1b64f642-2f2e-4ebd-9cea-e009e9041c79
  name-label ( RW): XENSERVER3
  name-description ( RW): Default install of XenServer

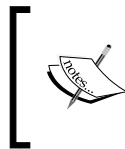
uuid ( RO)                : e5965f49-4482-4cf0-a53d-b6d4f0f6fb24
  name-label ( RW): XENSERVER1
  name-description ( RW): Default install of XenServer

uuid ( RO)                : 1c26efc2-2152-4710-98bf-3ab5e598e7c5
  name-label ( RW): XENSERVER2
  name-description ( RW): Default install of XenServer

[root@XENSERVER3 ~]# █
```

Removing a server from a resource pool

There might be several reasons why a host needs to be removed from a pool such as an issue with updates, networking, or the need to rebuild the host on the new hardware.

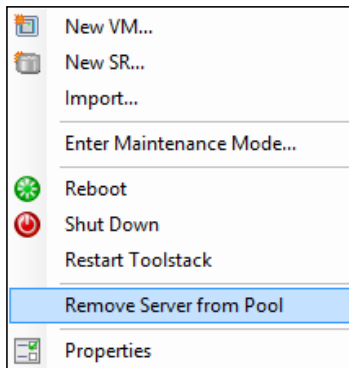


Removing a host from a resource pool will reinitialize and restart the server into a state that resembles a new XenServer installation. Any data on the local storage repositories will be wiped out.

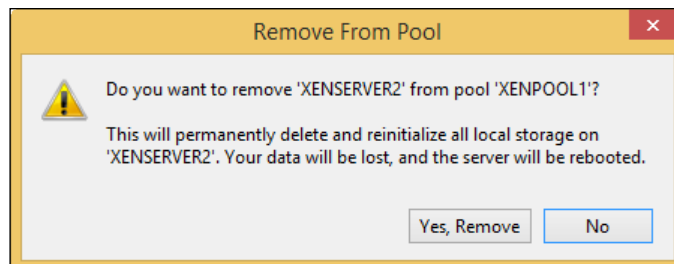
Removing a server from a resource pool (using the GUI)

The following steps cover removing a server from a resource pool using the XenCenter GUI:

1. Right-click on the server that will be removed from the pool and select **Remove Server from Pool**.



2. Click on **Yes, Remove** to confirm that the server will be removed from the pool.



Removing a server from a resource pool (using the CLI)

The following steps cover removing a server from a resource pool using the `xe` command from the command-line interface:

1. Run the `xe host-list` command to view the UUID of the servers in the resource pool. The UUID is used in order to identify the server when running the removal command:

```
xe host-list
```

The following screenshot shows you the servers in the resource pool:

```
[root@XENSERVER3 ~]# xe host-list
uuid ( RO)                : 1b64f642-2f2e-4ebd-9cea-e009e9041c79
  name-label ( RW): XENSERVER3
  name-description ( RW): Default install of XenServer

uuid ( RO)                : e5965f49-4482-4cf0-a53d-b6d4f0f6fb24
  name-label ( RW): XENSERVER1
  name-description ( RW): Default install of XenServer

uuid ( RO)                : 1c26efc2-2152-4710-98bf-3ab5e598e7c5
  name-label ( RW): XENSERVER2
  name-description ( RW): Default install of XenServer

[root@XENSERVER3 ~]#
```

2. Run the `xe pool-eject` command to remove the designated server from the resource pool. Type `yes` and press *Enter* when prompted to acknowledge the local SR reinitialization message. The server will restart after the operation has been completed.

```
xe pool-eject host-uuid=host_uuid
```

The following screenshot shows you how to remove a server from a resource pool:

```
[root@XENSERVER3 ~]# xe pool-eject host-uuid=1b64f642-2f2e-4ebd-9cea-
e009e9041c79
WARNING: Ejecting a host from the pool will reinitialise that host's
local SRs.
WARNING: Any data contained with the local SRs will be lost.
The following VDI objects will be destroyed:
VDI: 48732ee6-4889-430c-9a12-98870b091388 (SCSI 2:0:0:0)
Type 'yes' to continue
yes
Specified host will attempt to restart as a master of a new pool in 1
0.000 seconds...
[root@XENSERVER3 ~]#
```

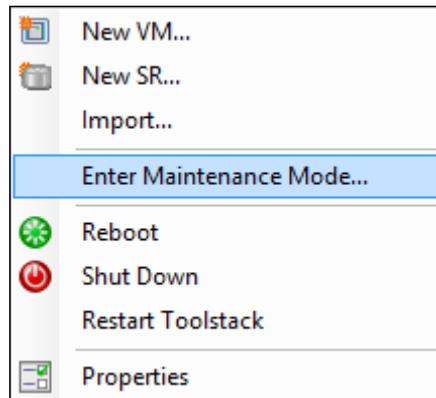
XenServer® maintenance mode

Maintenance mode provides a mechanism in order to perform maintenance operations on a server such as updates or independent configuration changes. Any running or suspended VMs on the server that are placed into maintenance mode are migrated to other servers in the pool. The following section covers placing a server into maintenance mode.

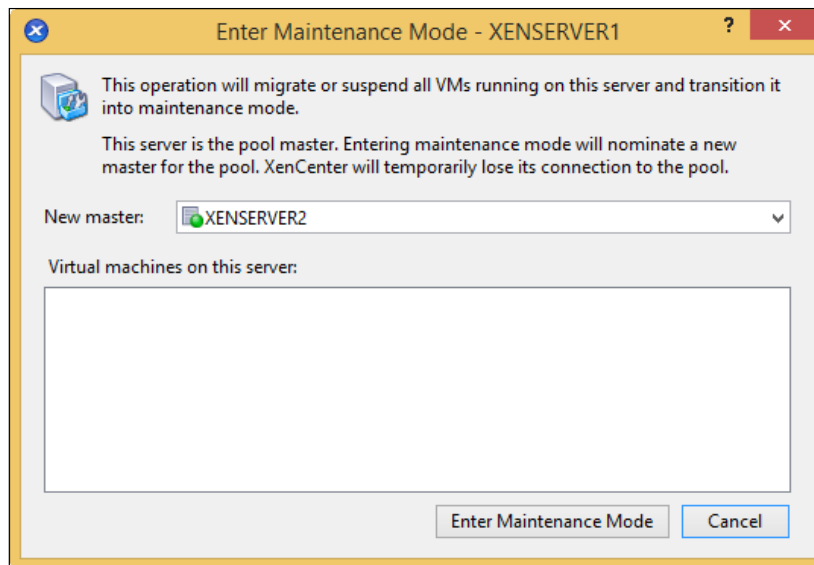
Placing a server into maintenance mode (using the GUI)

The following steps cover placing a server into maintenance mode using the XenCenter GUI:

1. Right-click on the desired server and select **Enter Maintenance Mode...**



2. If the server is the pool master, designate a new pool master and press **Enter Maintenance Mode** to place the server into maintenance mode. If the server is not the pool master, the option to select a new master is not presented.



Placing a server into maintenance mode (using the CLI)

The following steps cover placing a server into maintenance mode using the `xe` command from the command-line interface:

1. Run the `xe host-disable` command to place the server into maintenance mode:

```
xe host-disable host=servername
```

The following screenshot shows you how to place the host into maintenance mode:

```
[root@XENSER1 ~]# xe host-disable host=XENSER1
[root@XENSER1 ~]#
```

2. Run the `xe host-evacuate` command to migrate any running VMs off the server:

```
xe host-evacuate host="hostname"
```


The following screenshot shows you how to migrate all running VMs off the server:

```
[root@XENSERVER1 ~]# xe host-evacuate host=XENSERVER1
[root@XENSERVER1 ~]# █
```

3. To verify that the server has been successfully placed into maintenance mode, the `xe host-list` command can be run:

```
xe host-list enabled=false
```

The following screenshot can be used to view the servers in the resource pool that are in maintenance mode:

```
[root@XENSERVER1 ~]# xe host-list enabled=false
uuid ( RO)                : e5965f49-4482-4cf0-a53d-b6d4f0f6fb24
  name-label ( RW)       : XENSERVER1
  name-description ( RW) : Default install of XenServer

[root@XENSERVER1 ~]# █
```


XenMotion®

XenMotion is a feature that allows VMs to migrate from one server to another without any downtime. This functionality can be used when performing maintenance on a particular server that needs to be taken offline in order to perform a hardware replacement or even replacing a server.

XenMotion® requirements

The following list covers the requirements for performing a live migration operation on a VM:

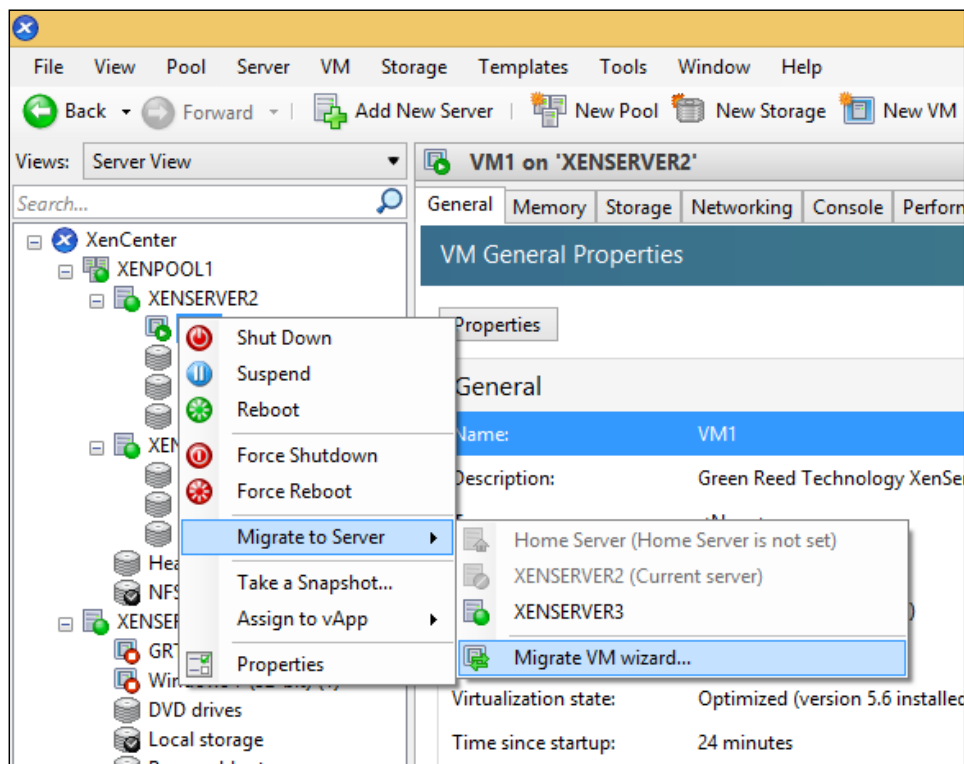
- XenMotion requires that the VMs are hosted on shared storage
- VMs can only be moved between servers in the same resource pool
- XenServer Tools must be installed on the migrating VM
- The DVD drive on the VM should be empty
- There must be enough free memory on the target server to support the migrating VM

 The target server must be the same or a newer version of XenServer. A VM that has migrated to a host running a newer version of XenServer cannot be migrated back to the older host.

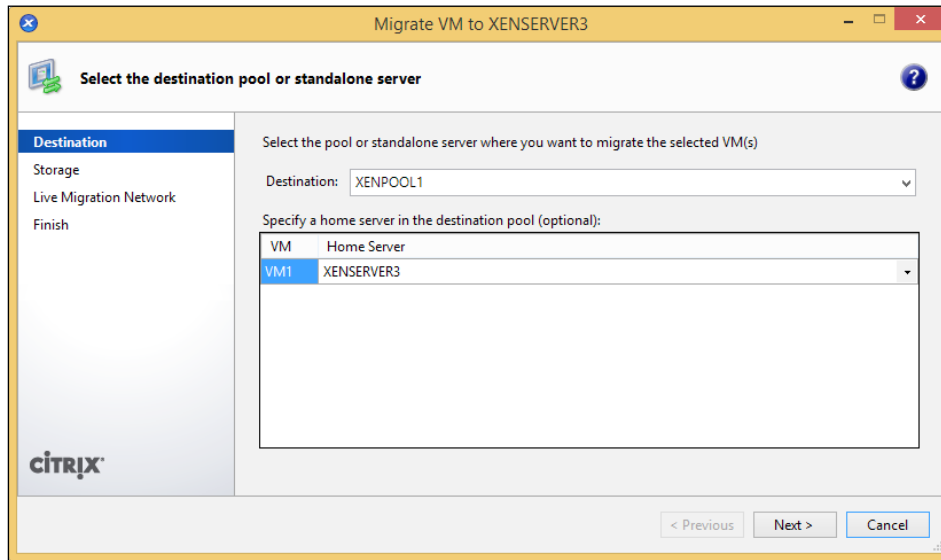
Migrating a VM

The following steps cover migrating a VM from one host to another:

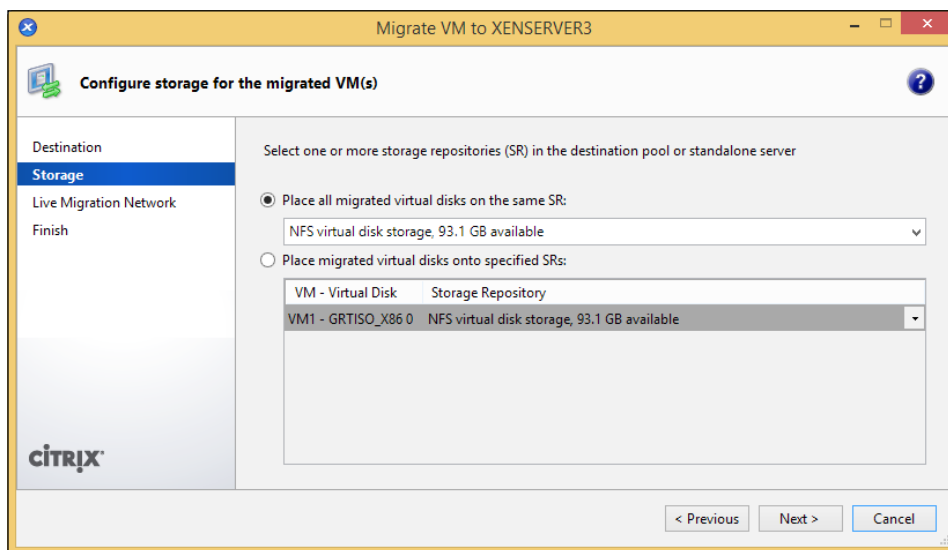
1. Right-click on the desired VM. Under the **Migrate to Server** option, select **Migrate VM wizard...** to launch the **Migrate VM wizard** screen.



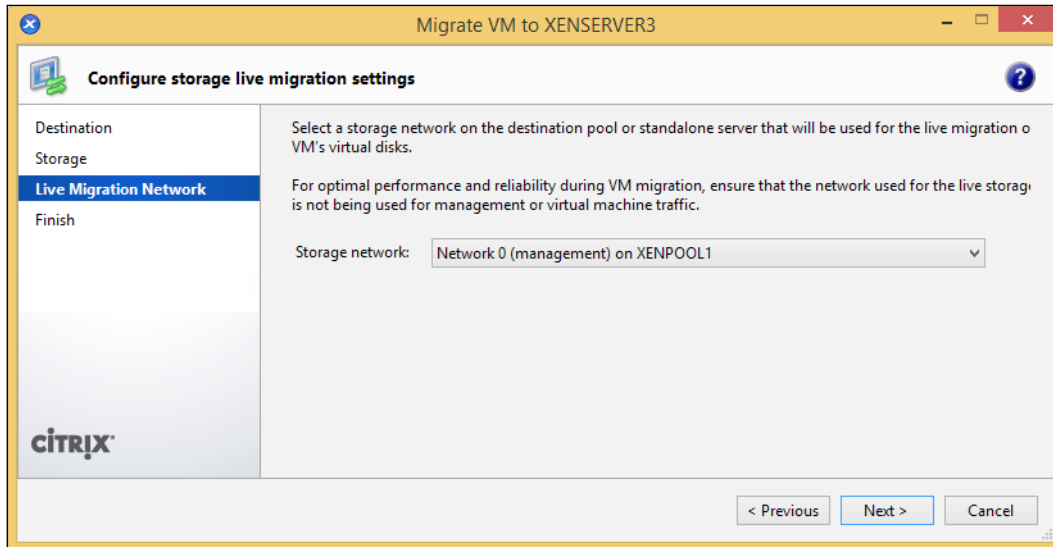
2. Select the target host or the resource pool from the **Destination** drop-down menu. Optionally, define a home server for the VM from the **Home Server** drop-down menu. The home server determines the server that the VM will attempt to start on when resources are available on that server. Click on **Next** to continue.



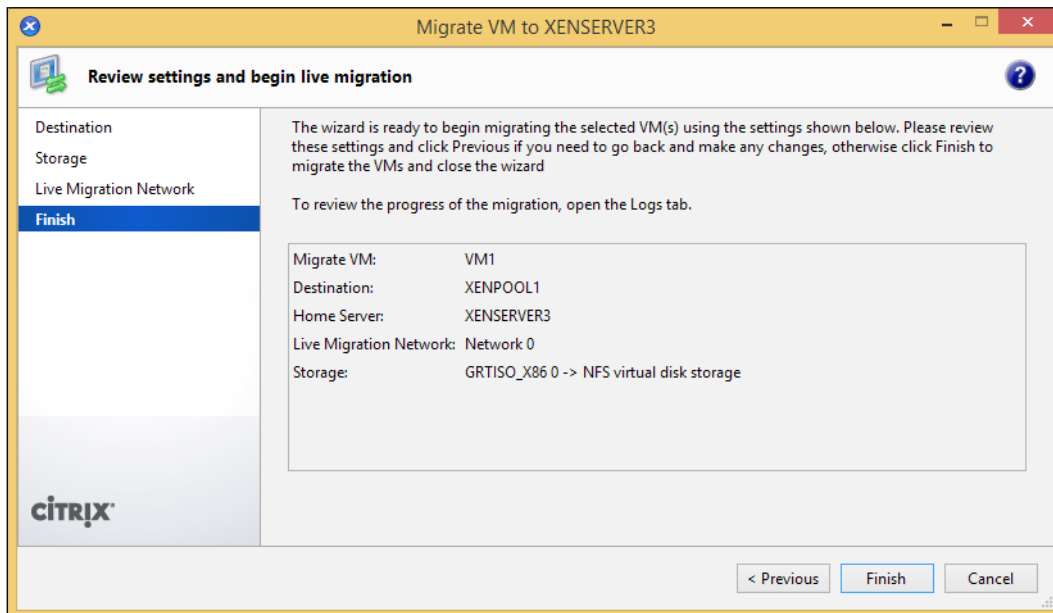
3. Optionally, select a new SR to migrate the VM's VDIs to, otherwise click on **Next** to continue.



- Select the network that is used to migrate the VM's VDI's if a storage migration was configured. Click on **Next** to continue.



- Review the migration settings, and then click on **Finish** to accept the settings and begin migrating the VM.



If a storage migration was not configured, then the migration of the VM from one host to another should take a few minutes to complete.

Storage XenMotion®

Storage XenMotion is a feature that allows a virtual machine's VDIs to migrate from one SR to another, while the VM is powered on. This functionality can be used to perform upgrades to storage arrays or even migrate storage arrays without VM downtime.

Citrix XenServer 6.2 provides you with the ability to live migrate a VM including its VDIs from a local SR to a shared SR as well as from one server to another without the need for shared storage.

Storage XenMotion® requirements

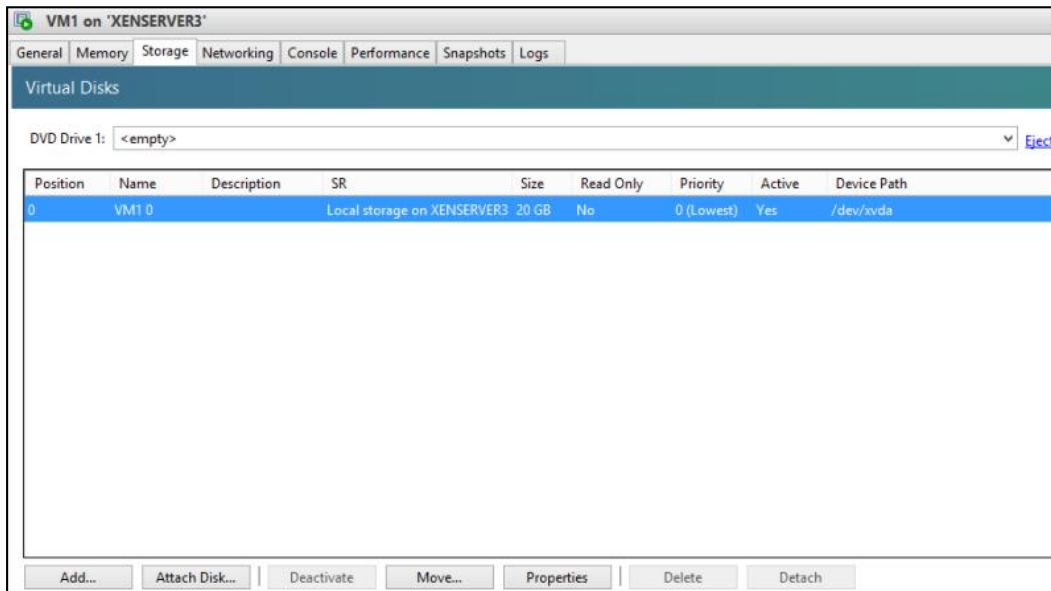
The following list covers the requirements for performing a live storage migration or storage XenMotion operation on a VM:

- The migrating VM must have XenServer Tools installed
- If the CPUs on the source and target server are different, then the CPU on the target must support all the features of the source server
- The migrating VM can have no more than one snapshot
- The migrating VM can have no more than six attached VDIs
- The target SR must have enough free space to accommodate the migrating VMs
- There must be enough free memory on the target server to support the migrating VMs
- The target server must have the same version of XenServer or later as the source server

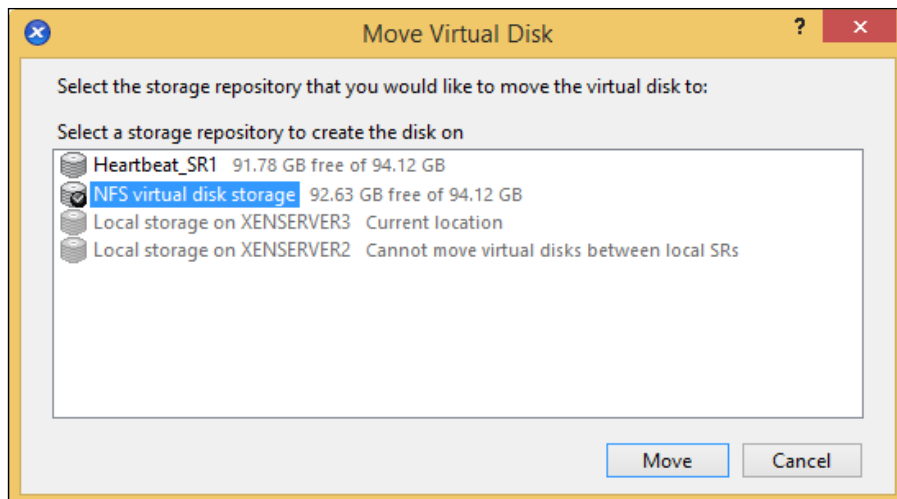
Migrating a VM

The following steps cover migrating/moving a VM's VDI from one SR to another:

1. Under the **Storage** tab of the VM in XenCenter, select the VDI to migrate and click on **Move** at the bottom of the screen.



2. Select the SR to move the VDI to and click on **Move** to begin the migration process.



The time taken to migrate the VDI will vary based upon the network speed of the management interface, the size of the VDI, and the speed of the storage. Storage XenMotion can be a very useful tool when performing upgrades and general cleanup of the XenServer environment.

Understanding HA

HA allows VMs to automatically restart on another host in the resource pool in the event of a host failure. This functionality ensures that the amount of downtime for a VM is limited to just the amount of time it takes to restart the VM on another host. The recommended minimum amount of servers in a HA-enabled deployment is three, this allows us to maximize the availability of our deployment.

The role of heartbeats

Heartbeats are used by the resource pool to determine whether a host is alive or reachable. Citrix XenServer uses two mechanisms for heartbeats, both are covered as follows:

- **Network heartbeats:** The management network of the XenServer hosts in the resource pool is used to facilitate the network heartbeat communication. Bonding the management interface is highly recommended to ensure that HA does not mark a host as offline due to a link failure. It is also a best practice to bond the management interface to ensure that the host can be managed for operations such as XenMotion.
- **Storage heartbeats:** A heartbeat SR is an iSCSI, Fibre Channel, or NFS SR used by the hosts in a HA-enabled resource pool in order to determine host availability. The hosts in the HA-enabled resource pool periodically write to the heartbeat SR as keep-alive mechanism. The LUN used for the heartbeat SR only needs to be 356 Mb or larger. Configuring dynamic multipathing for the SR that is used as the heartbeat SR is recommended to ensure availability.

Server fencing

Server fencing, sometimes referred to as host fencing, is a HA mechanism that is used to protect the cluster in the event that a host is determined to be unreachable. The host is powered off and restarted to prevent the host from writing to the shared storage and potentially corrupting data.

The following conditions will prevent a host from self-fencing:

- The network becomes partitioned where groups of servers can only communicate with the servers in their group. Servers that are in the group with the majority continue running while the smaller group of servers self-fences. If the groups are of equal numbers, then only one group will self-fence, this is why we recommend you to use an odd number of servers in the HA deployment.
- In the event that the storage heartbeats fail but the network heartbeats remain active, the hosts ensure network reachability with one another. If the hosts are able to reach one another, then none of the hosts self-fence based on the assumption that something just happened to the storage heartbeats.

HA capacity planning

XenServer creates a dynamic HA plan when HA is enabled. This plan is used to ensure that there is enough capacity on the remaining host in the pool to run all the VMs that are designated to be protected in the event of a server failure. There are two settings that can be defined by administrators; both of them are covered as follows:

- **The maximum failure capacity:** The maximum failure capacity setting defines the maximum number of hosts that can fail before resources in the pool become insufficient to support all the protected VMs
- **The server failure limit:** The server failure limit setting defines the number of host failures that are allowed in the pool

HA requirements

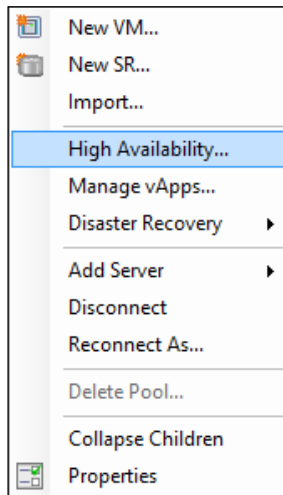
The following list covers the requirements for enabling HA on a resource pool:

- A shared storage SR is required to support the protected virtual machines
- An iSCSI, Fibre Channel, or NFS SR of 356 MB or greater is required for the heartbeat SR
- The virtual machine's network must be a pool-wide network
- The protected virtual machine must not be connected to a local DVD drive

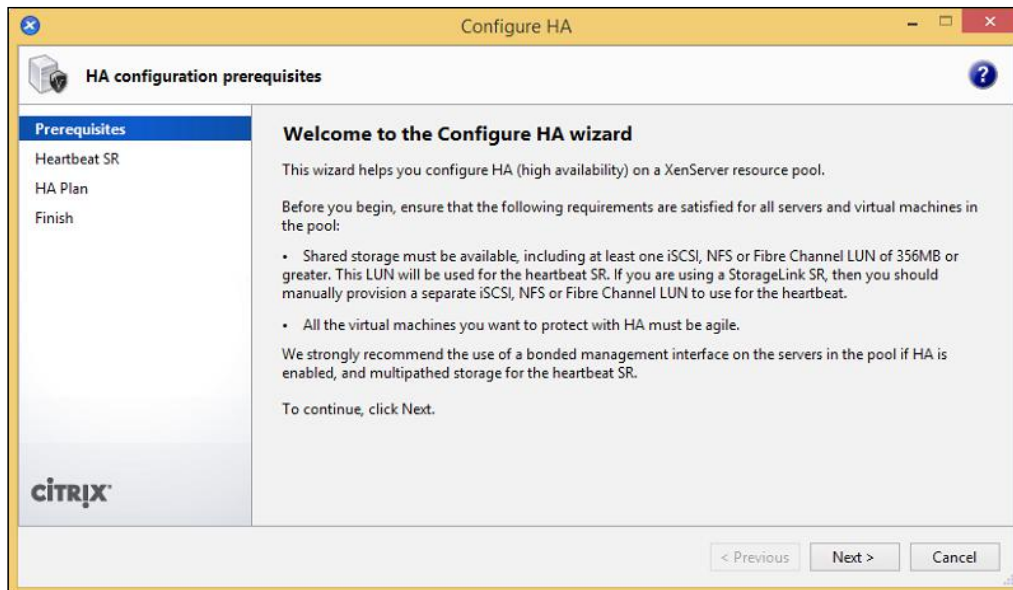
Enabling HA (using the GUI)

The following steps cover enabling HA on a resource pool using the XenCenter GUI:

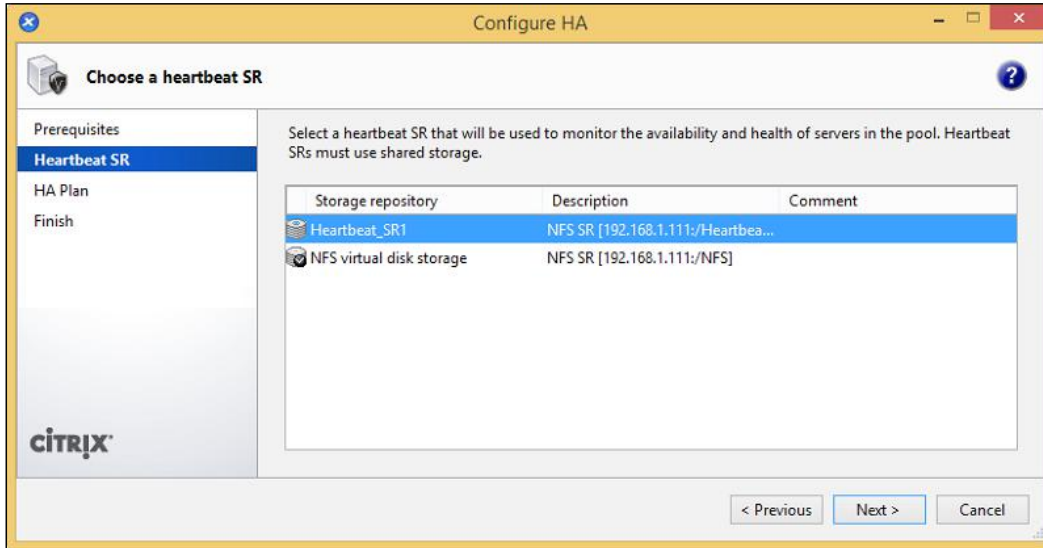
1. Right-click on the desired resource pool and select **High Availability...** to launch the HA wizard.



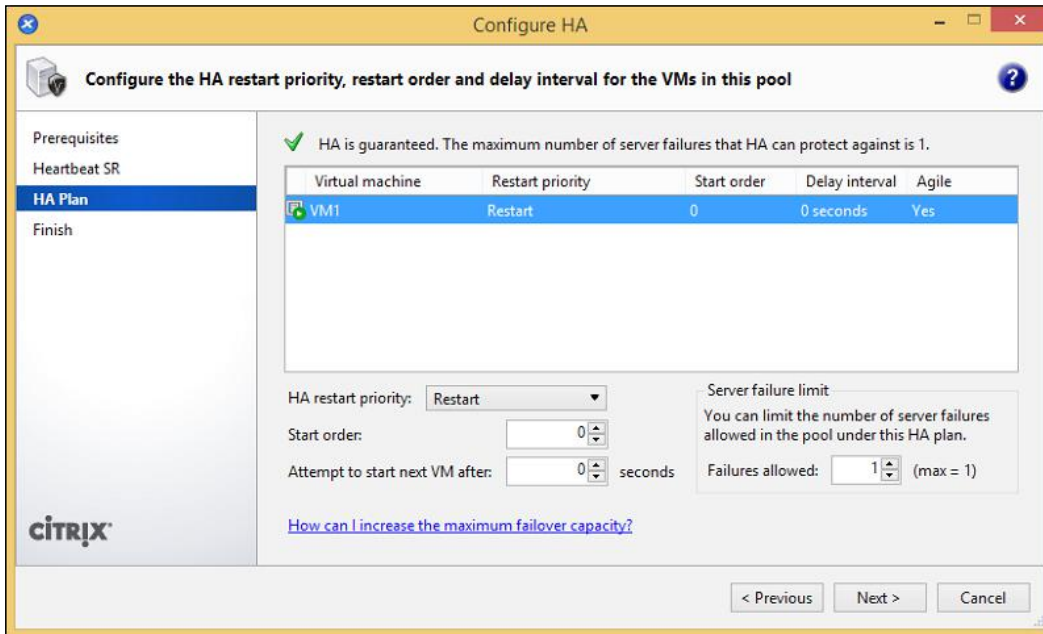
2. Click on **Next** on the first page of the HA wizard to scan the pool for a SR that can be used as the heartbeat SR.



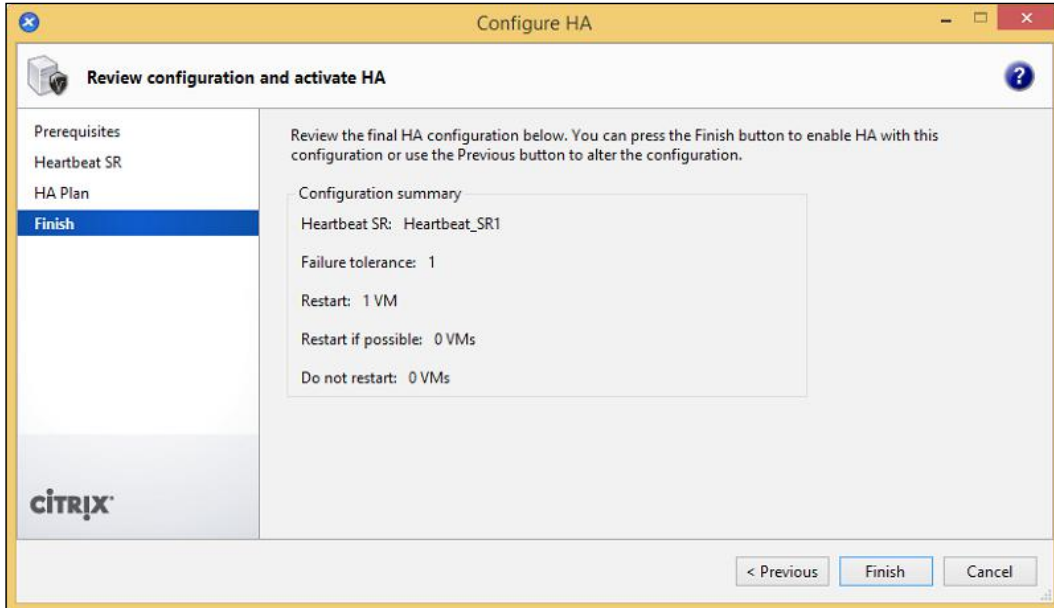
3. Select a SR to use as the heartbeat SR and click on **Next** to continue.



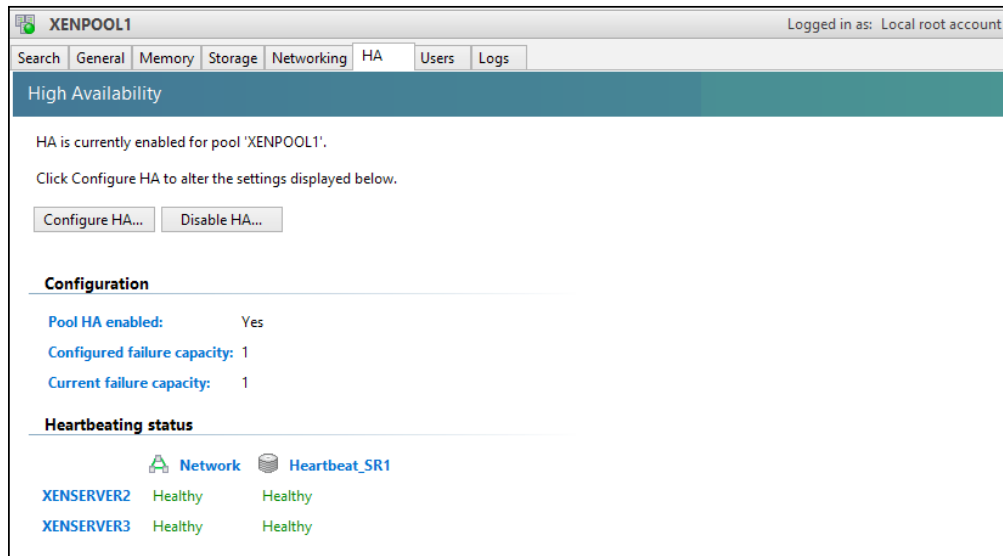
4. Configure the desired setting for the VM startup options and the server failure limit. Click on **Next** to continue.



5. Review the HA settings, then click on **Finish** to accept the settings and enable HA.



HA has now been enabled on the resource pool. We can now verify that HA has been enabled by looking at the **HA** tab of the resource pool, as shown in the following screenshot:



Enabling HA (using the CLI)

The following steps cover enabling HA on a resource pool using the XenCenter GUI:

1. Run the `xe sr-list` command to view the UUID of the SRs in the resource pool. The UUID of the SR that will be used for the storage heartbeat is required when running the HA `enable` command. Appending `shared=true` limits the output to only SRs that are shared, as only the shared SRs are supported for the heartbeat SR:

```
xe sr-list shared=true
```

The following screenshot displays the UUIDs for all the shared SRs in the resource pool:

```
[root@XENSERVER1 ~]# xe sr-list shared=true
uuid ( RO)                : 99eela6b-9edf-812d-2264-0337294ad06a
  name-label ( RW)         : XenServer Tools
  name-description ( RW)   : XenServer Tools ISOs
    host ( RO)             : <shared>
    type ( RO)             : iso
    content-type ( RO)     : iso

uuid ( RO)                : f2b1f237-a8de-045f-aa70-131dbd07ab70
  name-label ( RW)         : NFS virtual disk storage
  name-description ( RW)   : NFS SR [192.168.1.111:/NFSVHD]
    host ( RO)             : <shared>
    type ( RO)             : nfs
    content-type ( RO)     :

uuid ( RO)                : 2c32a078-7d20-2268-c8de-441fada239c3
  name-label ( RW)         : Heartbeat_SR1
  name-description ( RW)   : NFS SR [192.168.1.111:/heartbeat1]
    host ( RO)             : <shared>
    type ( RO)             : nfs
    content-type ( RO)     :

[root@XENSERVER1 ~]# █
```

2. Run the `xe pool-ha-enable heartbeat-sr-uuids=heartbeat_sr_uuids`

The following screenshot displays enabling HA on the resource pool using the UUID of one of the SRs from the previous step:

```
[root@XENSERVER1 ~]# xe pool-ha-enable heartbeat-sr-uuids=2c32a078-7d20-2268-c8de-441fada239c3
[root@XENSERVER1 ~]# █
```

3. Run the `xe pool-param-set ha-host-failures-to-tolerate` command to configure the server failure limit for the resource pool:

```
xe pool-param-set ha-host-failures-to-tolerate=1 uuid=pool_uuid
```

The following screenshot displays the configuration of the resource pool to tolerate the failure of one server:

```
[root@XENSERVER1 ~]# xe pool-param-set ha-host-failures-to-tolerate=1
uuid=9a52fd4f-c12d-7b8d-d75a-d8bfcdded29ed
[root@XENSERVER1 ~]# █
```

4. To verify that HA has been successfully enabled, the `xepool-param-get` command can be used to determine the HA status of the resource pool:

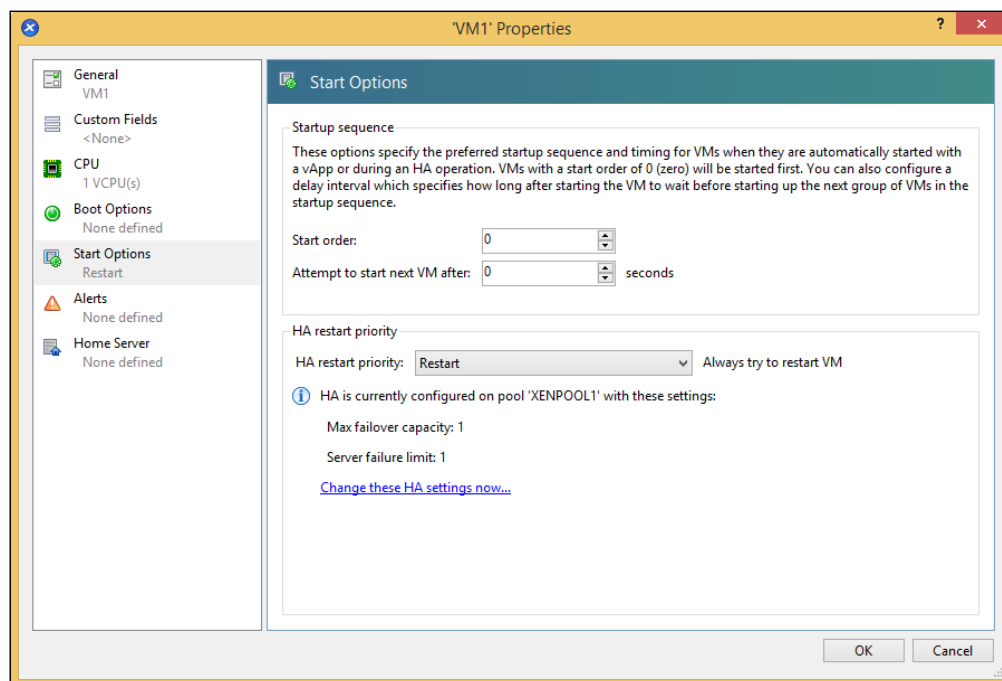
```
xe pool-param-get param-name=ha-enabled uuid=pool_uuid
```

The following screenshot shows the status of HA on the resource pool. The result of `false` indicates that HA has been disabled on the resource pool.

```
[root@XENSERVER1 ~]# xe pool-param-get param-name=ha-enabled uuid=9a52fd4f-c12d-7b8d-d75a-d8bfcdded29ed
true
[root@XENSERVER1 ~]# █
```

VM HA settings

The settings for HA on a per-VM level can be configured under the **Start Options** section of the VM's properties, as shown in the following screenshot:



The HA restart priority

The HA restart priority is used to define the order of precedence used when there is contention for capacity on the remaining hosts in the resource pool. The three HA restart priorities available on XenServer are as follows:

- **Restart:** The VM will restart if there is capacity available on the remaining hosts in the resource pool
- **Restart if possible:** The VM will only restart on another host if there is capacity available after VMs with a higher priority have been restarted
- **Do not restart:** The VM will not restart after a host failure

The start order

The start order determines the order in which VMs are booted after a host failure. This functionality allows VMs that provide services to other VMs such as a database server to be started first.

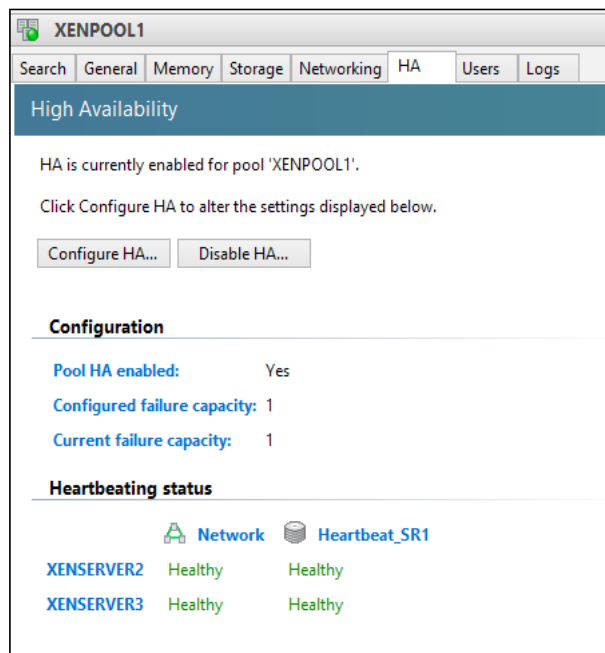
The delay interval

The delay interval determines how long to wait before starting the next set of VMs after the selected VM starts. This setting can be used to ensure that services that are composed of multiple servers are staggered in such a manner that the required servers have time to completely boot. In the case of a Microsoft Windows environment, it may be starting the domain controllers and network services such as DHCP and DNS first, and then starting the database and application servers after the domain controllers have had enough time to finish booting.

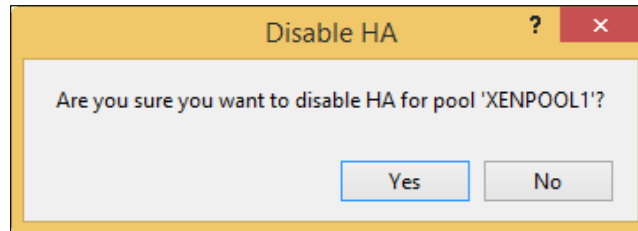
Disabling HA (using the GUI)

HA might need to be disabled when performing maintenance operations such as updates or upgrades. The following steps cover disabling HA on a resource pool using the XenCenter GUI:

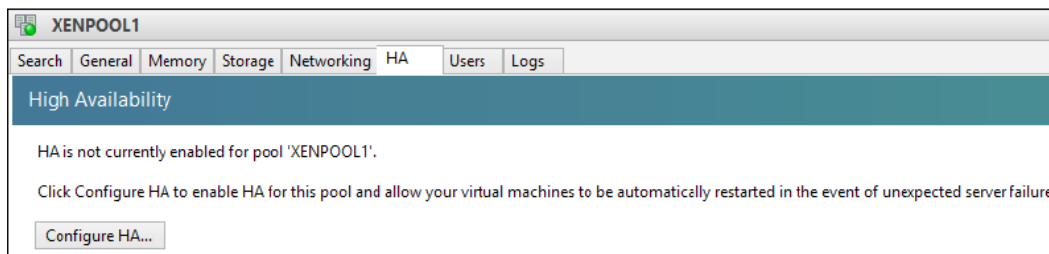
1. Click on **Disable HA...** on the **HA** tab of the resource pool to disable HA.



- Click on **Yes** on the **Disable HA** dialog box to disable HA.



- We can now verify that HA has been disabled by looking at the **HA** tab of the resource pool, as shown in the following screenshot:



Disabling HA (using the CLI)

The following steps cover disabling HA on a resource pool using the `xe` command from the command line:

- Run the `xe pool-ha-disable` command to disable HA on the resource pool:
`xe pool-ha-disable`

The following screenshot shows you how to disable HA on a resource pool:

```
[root@XENSERVER1 ~]# xe pool-ha-disable
[root@XENSERVER1 ~]#
```


2. To verify that HA has been successfully disabled, the `xe pool-param-get` command can be used to determine the HA status of the resource pool:

```
xe pool-param-get param-name=ha-enabled uuid=pool_uuid
```

The following screenshot shows you the status of HA on the resource pool. The result of `false` indicates that HA has been disabled on the resource pool.

```
[root@XENSERVER1 ~]# xe pool-param-get param-name=ha-enabled uuid=9a52fd4f-c12d-7b8d-d75a-d8bfcdded29ed
false
[root@XENSERVER1 ~]# █
```

Summary

In this chapter, we covered creating and managing resource pools to provide availability as well as centralized configuration. We learned about XenMotion and storage XenMotion for migrating VMs along with their VDIs eliminate the need to take hosts offline to perform maintenance. We also covered HA and the benefits that it provides by automatically restarting VMs in the event of a host failure to reduce downtime. Now that we have learned how to ensure the availability of a XenServer deployment, in the next chapter, we will look at restoring the XenServer environment in the event of a disaster.

6

Business Continuity

According to Murphy's Law, what can go wrong will go wrong. This highlights the need to put measures into place to ensure that when something does go wrong, we have a plan or a guide for how to get things up and running again. A primary concern for companies, large and small, is how to quickly bring their computer systems back online following a disaster. In the previous chapter, we looked at features such as resource pools and HA that provide resiliency and allow the environment to cope with the failure of multiple servers. As a part of effective continuity planning, we need to address the possibility of failures at the VM level or even a disaster that destroys the entire site. Most solutions used for restoring an entire site are either incredibly complex or are extremely expensive, and many companies elect to gamble that a failure will never take place. XenServer Disaster Recovery is a built-in feature that provides an easy-to-use mechanism for site recovery, which we'll look at in this chapter.

In this chapter, we'll learn about the following topics:

- Developing a XenServer business continuity plan
- XenServer VM backup and restore
- XenServer host backup and restore
- XenServer Disaster Recovery

Developing a XenServer® business continuity plan

The business continuity plan outlines the components of the environment that need to be restored in the event of a disaster. One of the key aspects in developing a successful business continuity plan is to identify the possible points of failure and draft the plan to address those areas. We'll take a look at some of the possible failures that can occur in our XenServer environment in order to begin developing a plan for how best to protect our environment:

- Guest operating system corruption
- XenServer host upgrade failure
- Storage repository failure
- Accidental VM deletion
- Storage repository misconfiguration
- Server hardware failure

The failures listed here range from storage hardware failures to misconfiguration by an administrator. All of these can create a service outage and warrant the need to perform a restoration operation. The following components of the XenServer environment should be a part of the business continuity plan to ensure that the environment can be successfully restored.

VMs

VMs are the primary aspect of the environment that we need to ensure is backed up and can be restored. The actual methods for backing up the VMs will be covered later in the chapter, but we'll take a look at the components now:

- **Metadata:** The VM metadata contains information about the VM settings such as vCPU configuration, memory settings, and VDI configuration. The VM metadata needs to be backed up in order to fully restore the VM even if the VDI is available on the SR.
- **VDI:** The VDI(s) contain the actual data of the VMs and need to be backed up regularly.

Hosts

We covered HA in a previous chapter that shielded us from catastrophic failure in the event of a single or even multiple host failure. We'll consider what happens in a standalone host deployment where HA is not an option, or when the entire pool fails due to an entire site failure. The two primary components of the XenServer host installation that need to be accommodated as a part of the backup plan are the pool/host metadata and the control domain:

- **The pool/host metadata:** The pool/host metadata contains the information about the configuration of the host and is used to restore the host to the state prior to the failure
- **The control domain:** This is the actual XenServer installation

SRs

Considering that SRs hold all of our data, we need to ensure that we have implemented the measures to restore them in the event of a failure, there are a number of features typically offered in midtier and above storage arrays such as storage-level replication to sync data between arrays and snapshots to create point-in-time copies of LUN volumes.

Backing up and restoring XenServer® VMs

There are two primary methods for VM backup management in a virtualized environment. The first is agent-based and the second is hypervisor-based or agentless, both of which are covered in the following sections.

Agent-based

Agent-based VM backups utilize an agent that is installed on the VM just like an agent installed on a physical machine. Using an agent-based solution can provide a number of advantages such as providing administration consistency in environments, where agents are already used to back up physical servers or allow a single solution to be used in environments with hypervisors from various vendors. A big drawback of an agent-based solution is the need to install and maintain an agent in the guest operating system.

Agent-based backups

The following steps provide a high-level overview of the process of configuring agent-based backups in a virtualized environment. The specific steps required vary between backup software vendors, and it is assumed that the administrator has the knowledge of how to manage the backup solution:

1. Install the backup agent in the guest operating system provided by the software vendor.
2. The backup agent will communicate with the backup server.
3. Schedule the backup of the operating system in the backup solution management interface.

Agent-based restores

The following steps provide a high-level overview of the process of restoring a guest operating system from agent-based backups in a virtualized environment:

1. Mount the disc image provided by the vendor for restoring an operating system into the VMs DVD drive.
2. Boot the VM to the restore the media and proceed with the restoration process according to the vendor's documentation.

Agent-based backup solutions

The following list contains a number of agent-based backup products that are available:

- **Symantec Backup Exec:** Backup Exec is a commercial backup solution provided by Symantec with agents available for Windows, Linux, and MAC. (<http://www.symantec.com/products/data-backup-software>)
- **Acronis Backup Advanced:** Acronis Backup is a commercial backup solution provided by Acronis that is aimed at medium-scale to large-scale businesses. Agents are available for Windows Server, Linux, and Windows desktops. (<http://www.acronis.com/en-us/business/backup-advanced/>)

Hypervisor-based

Hypervisor-based or agentless VM backups typically utilize the **snapshot functionality** in the hypervisor to capture a consistent image of the VM for backup purposes. Since the backup solution interacts directly with the hypervisor, this eliminates the need for installing an agent on the VM to back up the VM. A proxy server is used to manage the backups along with interacting with the hypervisors.

Hypervisor-based backup solutions

The following list contains a number of agentless backup products that are available:

- **Acronis Backup Advanced for Citrix XenServer:** Acronis' Backup Advanced for Citrix XenServer is a commercial hypervisor-based backup solution that offers deduplication, centralized reporting, and management as well as P2V and V2P functionalities (<http://www.acronis.com/en-us/business/backup-advanced/citrix/>)
- **Unitrends Virtual Backup:** Unitrends Virtual Backup is a commercial hypervisor-based backup solution available in three editions: Essential, Professional, and Enterprise (<http://www.unitrends.com/products/data-protection-virtual-appliances/unitrends-virtual-backup>)
- **Quadric Software Alike:** Quadric Software's Alike is a commercial hypervisor-based backup solution available in three editions: Free, Standard, and DR (<https://www.quadricsoftware.com/>)
- **SEP software sesam:** SEP's sesam is a commercial hypervisor-based backup solution that integrates with XenCenter, provides encryption as well as P2V and V2P functionalities (<http://www.sep.de/products/virtual-machine-backup/citrix-xenserver/>)

Apart from the two methods that were discussed, XenServer supports exporting VMs as well as snapshots, which provide a rudimentary mechanism for backing up VMs in the event of a failure. Snapshots are an excellent tool for providing a rollback mechanism following a major change to a VM such as a software upgrade or installation. While these methods are effective, they are typically very difficult to manage, they lack advanced features offered in third-party solutions, and generally don't scale well.

Backing up and restoring XenServer®


The following sections covers the two methods for backing up and restoring a failed XenServer host.

The host metadata

The host metadata holds information about the configuration of the XenServer host/pool such as host, network, and storage configuration. Simply backing up the host metadata is considered best practice, as the actual XenServer installation should remain unmodified. After performing a clean installation of XenServer, the host metadata can be restored to perform the host configuration and bring the host to the state of the backup.

The control domain

The control domain is the actual installation of XenServer and generally should remain unmodified. Since the control domain should remain unmodified, the recommended method for restoring a host is to perform a clean installation and simply restore the host metadata from a backup.

 There are scenarios where a custom third-party software is installed on XenServer to provide additional functionality such as hardware monitoring, which would warrant the desire to back up the control domain.

Backing up the pool metadata


The following section covers backing up the pool metadata on a XenServer server.

The following command creates a backup file of the pool metadata. Backups of the data should be maintained on the storage that does not reside on the server or pool to be backed up. The pool metadata can only be backed up using the command-line interface.

```
xe pool-dump-database file-name="Backup_File"
```

The following screenshot shows the process of backing up the pool metadata of a server:

```
[root@XENSERVER3 ~]# xe pool-dump-database file-name=XENSERVER3_BACKUP01
[root@XENSERVER3 ~]# ls
support.tar.bz2 XENSERVER3_BACKUP01
[root@XENSERVER3 ~]#
```

 No output is displayed after the command is completed. The `ls` command can be used to view the newly created backup file.

Restoring the pool metadata

The `pool restore dry-run` command is used to check whether the target host has the appropriate number of appropriately named NICs to complete the restore process:

```
xe pool-restore-database file-name="Backup_File" dry-run=true
```

The following screenshot shows a dry-run backup of a pool metadata restore:

```
[root@XENSERVER3 ~]# xe pool-restore-database file-name=XENSERVER3_BACKUP01 dry-run=true
Dry-run backup restore successful
[root@XENSERVER3 ~]# █
```

The normal `pool metadata restore` command will restore the XenServer host to the state of the backup, and will automatically reboot the host to complete the restore process. The operation must use the `--force` switch, otherwise an error message is displayed, the restore operation will make the server the pool master and all the member servers will be forgotten:

```
xe pool-restore-database file-name="Backup_File" --force
```

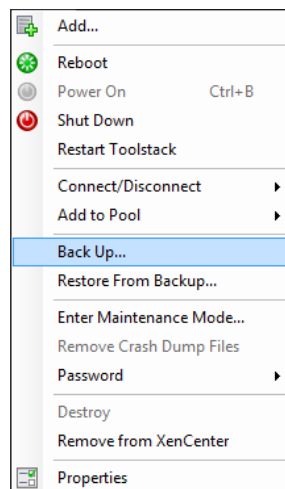
The following screenshot shows the process of restoring pool metadata to a server:

```
[root@XENSERVER3 ~]# xe pool-restore-database file-name=XENSERVER3_BACKUP01 --force
Host will reboot with restored database in 30.000 seconds...
[root@XENSERVER3 ~]# █
```

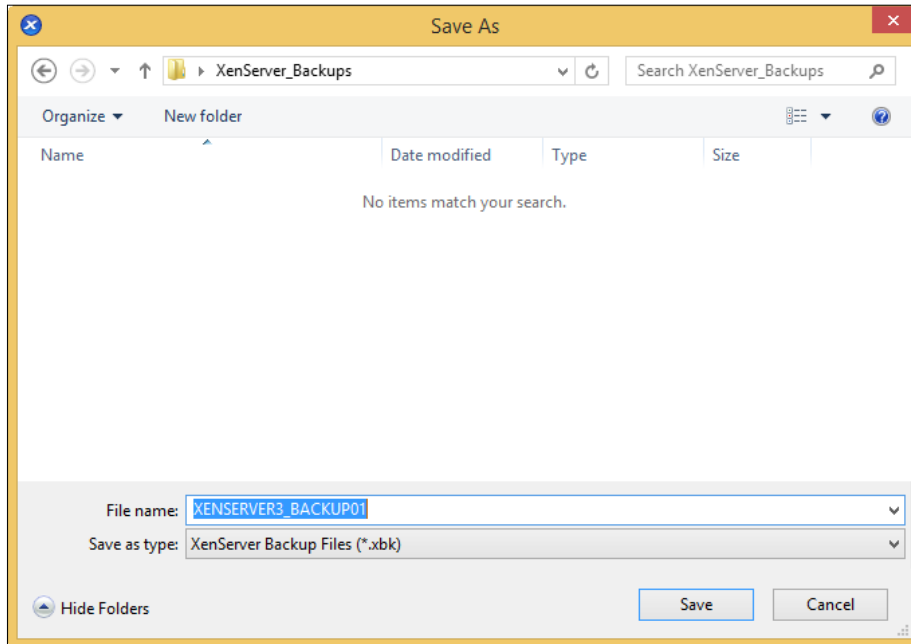
Backing up the control domain (using the GUI)

The following steps cover backing up the control domain of a XenServer host using the XenCenter GUI:

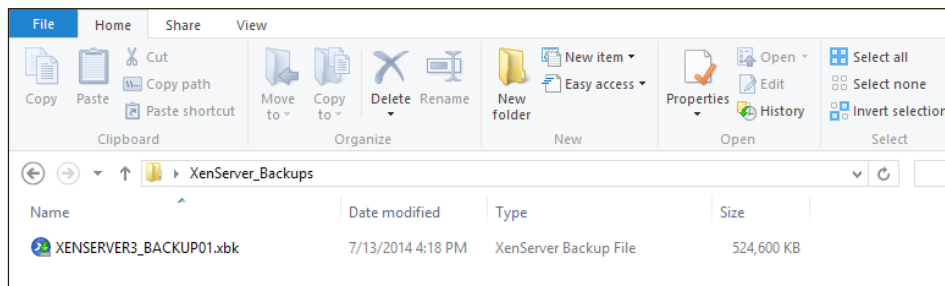
1. Select the desired server or pool and select the **Back Up...** option from the **Server** menu, as shown in the following screenshot:



2. Select a location to save the XenServer backup file, provide a name for the file, and click on **Save** to start the backup process.



3. The following screenshot displays the saved backup file from the control domain backup:




Backing up the control domain (using the CLI)

The same steps can be performed using the XE command from the CLI:

```
xe host-backup host="XENSER_HOST" file-name="File_backup"
```

The following screenshot shows the process of creating a backup of the control domain:

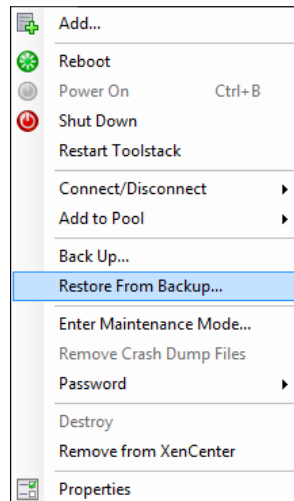
```
[root@XENSERVER3 ~]# xe host-backup host=XENSERVER3 file-name=XENSERVER3_CONTROL_BACKUP01
[root@XENSERVER3 ~]# ls
support.tar.bz2 XENSERVER3_BACKUP01 XENSERVER3_CONTROL_BACKUP01
[root@XENSERVER3 ~]#
```

 The backup of the control domain should be saved somewhere other than the root partition in order to avoid filling up the root partition along with avoiding a single point of failure.

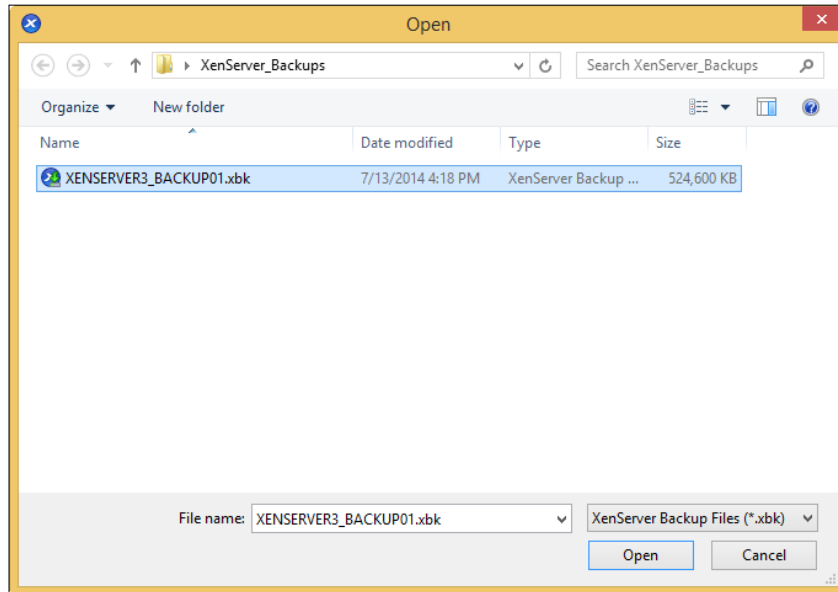
Restoring the control domain (using the GUI)

The following steps cover restoring the control domain of a XenServer host using the XenCenter GUI:

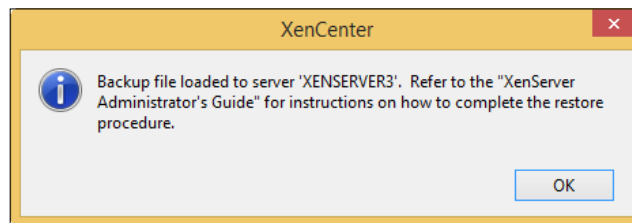
1. Select the desired server or pool and select the **Restore From Backup...** option under the **Server** menu.




2. Select the desired backup file and click on **Open** to load the backup file onto the XenServer host.



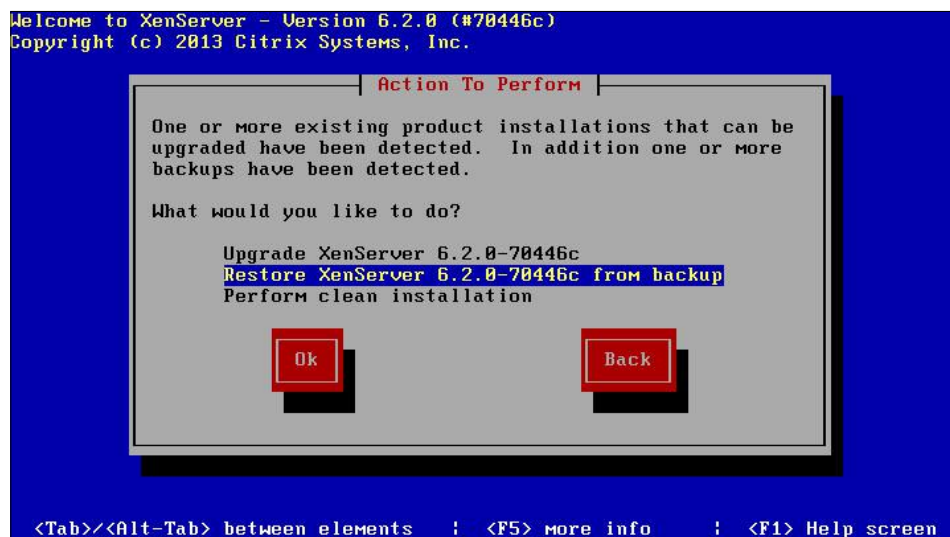
3. Once the backup file has been loaded onto the XenServer host, click on the **OK** button to proceed.



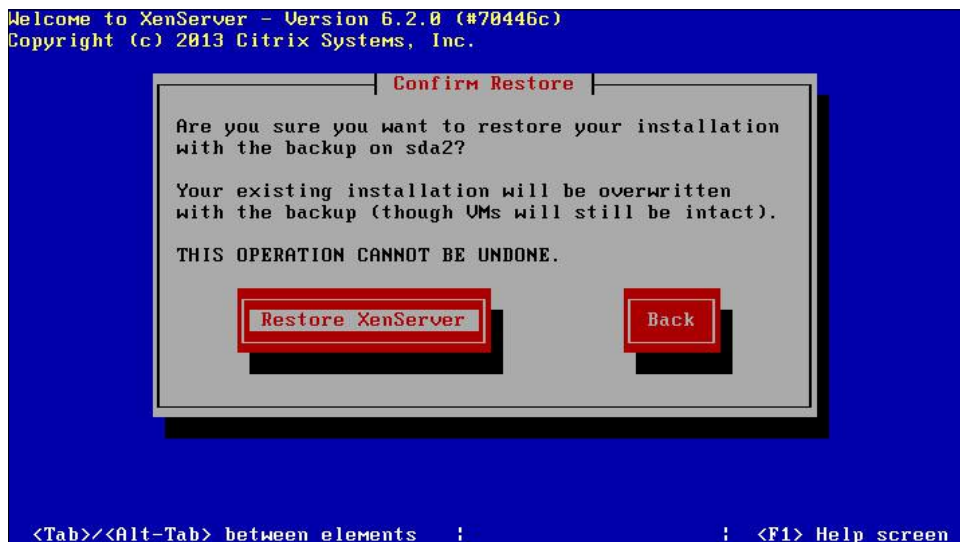
[ The host must be restarted and booted from the Citrix XenServer 6.2 installation media to complete the restore process.]

4. Boot the server from the Citrix XenServer 6.2 installation media and press *Enter* when prompted to start the Citrix XenServer 6.2 installer.
5. Select the desired key mapping and select **Ok** to proceed.

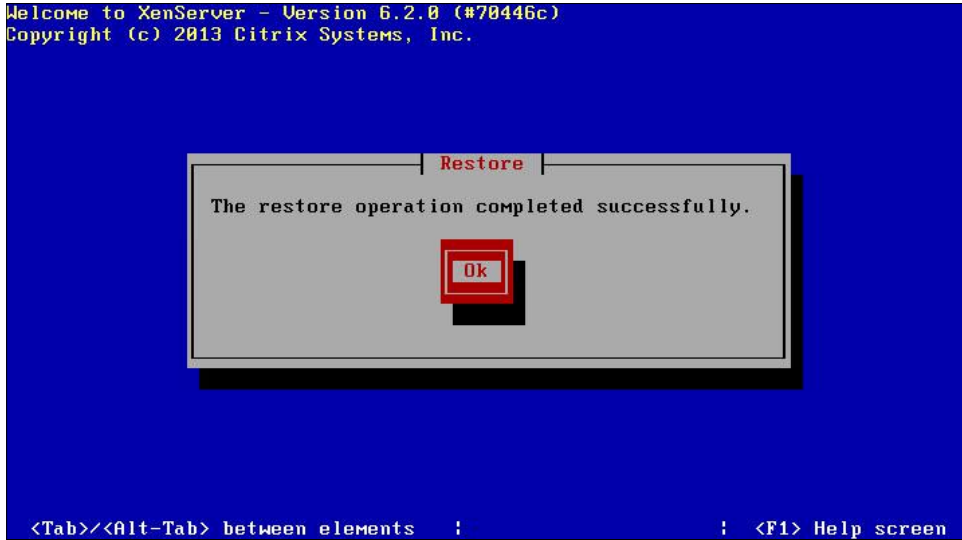
6. Press *F9* if additional drivers need to be installed or select **Ok** to continue.
7. Accept the EULA.
8. Select the **Restore XenServer from backup** option and press *Enter* to continue.



9. Select **Restore XenServer** and press *Enter* to begin the control domain restore process.



10. After the restore process has completed, press *Enter* to restart the server:



The XenServer host will restart to the state of the control domain backup.

Restoring the control domain (using the CLI)


The same steps can be performed using the XE command from the CLI:

1. Run the following command from the XenServer command line to load the control domain:

```
xe host-restore host="Xenserver_host" file-name="File_backup"
```

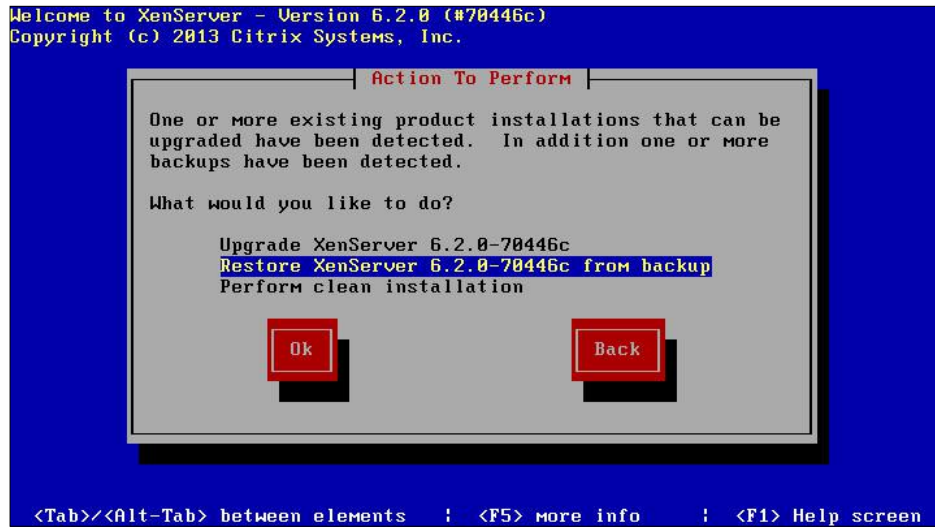
This is also depicted in the following screenshot:

```
[root@XENSER3 ~]# xe host-restore host=XENSER3 file-name=XENSER3_CONTROL_BACKUP01
[root@XENSER3 ~]#
```

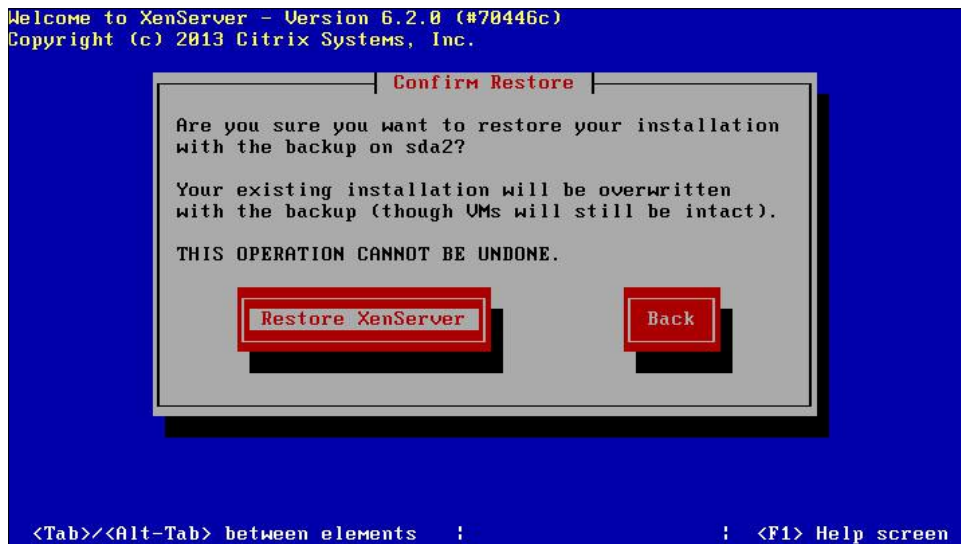
 The command will not display any output when it has completed successfully.

2. Restart the server and boot from the Citrix XenServer 6.2 installation media. Press *Enter* when prompted to start the Citrix XenServer 6.2 installer.
3. Select the desired key mapping and select **Ok** to proceed.
4. Press *F9* if additional drivers need to be installed or select **Ok** to continue.

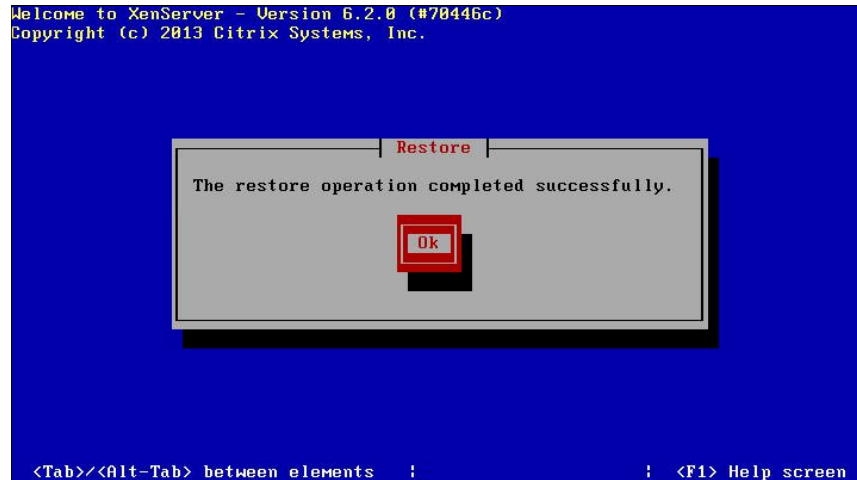
5. Accept the EULA.
6. Select the **Restore XenServer from backup** option and press *Enter* to continue.



7. Select **Restore XenServer** and press *Enter* to begin the control domain restore process.



8. After the restore process has completed, press *Enter* to restart the server.



Restoring a XenServer® deployment

Now that we have looked at backing up and restoring the individual components in a XenServer deployment, we'll take a look at developing a plan for restoring all the components of the deployment and how they all fit together. The following steps apply to the failure of the entire pool. If there are remaining servers in a resource pool, a new pool master can simply be elected.

1. Install Citrix XenServer 6.2 on the server that will be the pool master.
2. Restore the pool metadata backup onto the server to restore the pool configuration by running the `xe pool-restore-database` command on the pool master.
3. Remove the entries of the old pool members by running the `xe host-forget` command on the pool master.
4. Install Citrix XenServer 6.2 on any additional servers and join them to the resource pool.
5. Restore VMs from backup in the event that there is an issue with the resource pool's SRs.

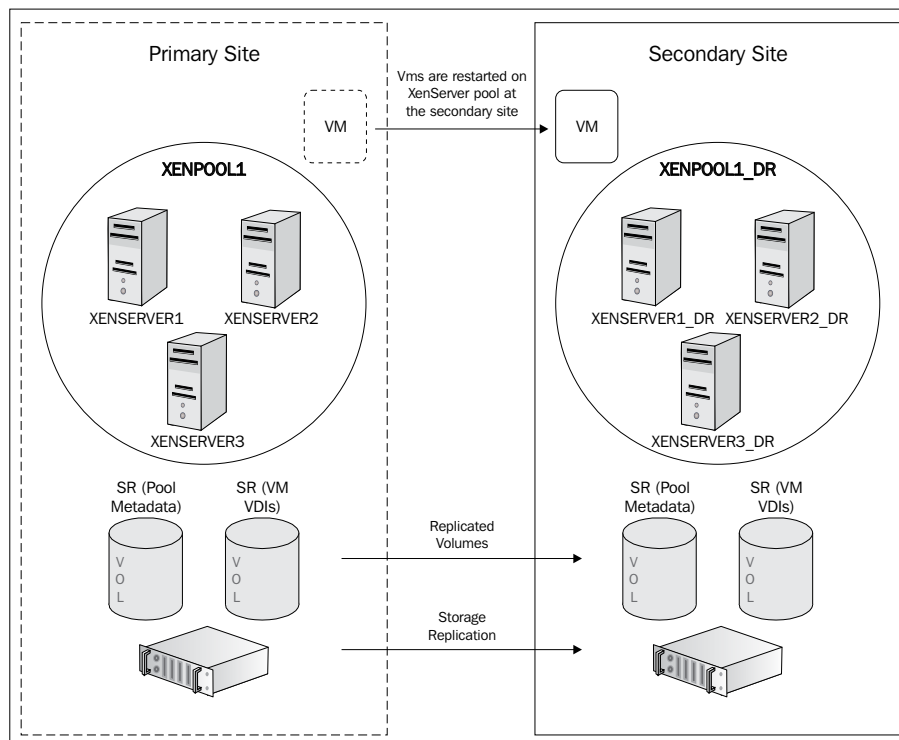
The steps listed here cover restoring a XenServer deployment if there is a failure of the entire pool using methods that were previously discussed in the chapter. While the process discussed utilizes several manual methods, XenServer provides the disaster recovery feature for automating the site recovery process in the event of a site failure, which is ideal for large XenServer deployments.

XenServer® Disaster Recovery

XenServer **Disaster Recover (DR)** is a feature that acts as a recovery mechanism in the event of a XenServer pool or site failure. The DR feature simplifies the process of failing over to a DR site and eventually failing back after the primary site has been brought back online. This feature utilizes the replicated SRs that contain the pool metadata and the VDIs of the protected VMs to restore VMs in the secondary site. After a disaster, the VMs and vApps are restored using the replicated SRs in the secondary site. The feature is built into XenServer and provides reduced administration for recovering an entire site in the event of a disaster.

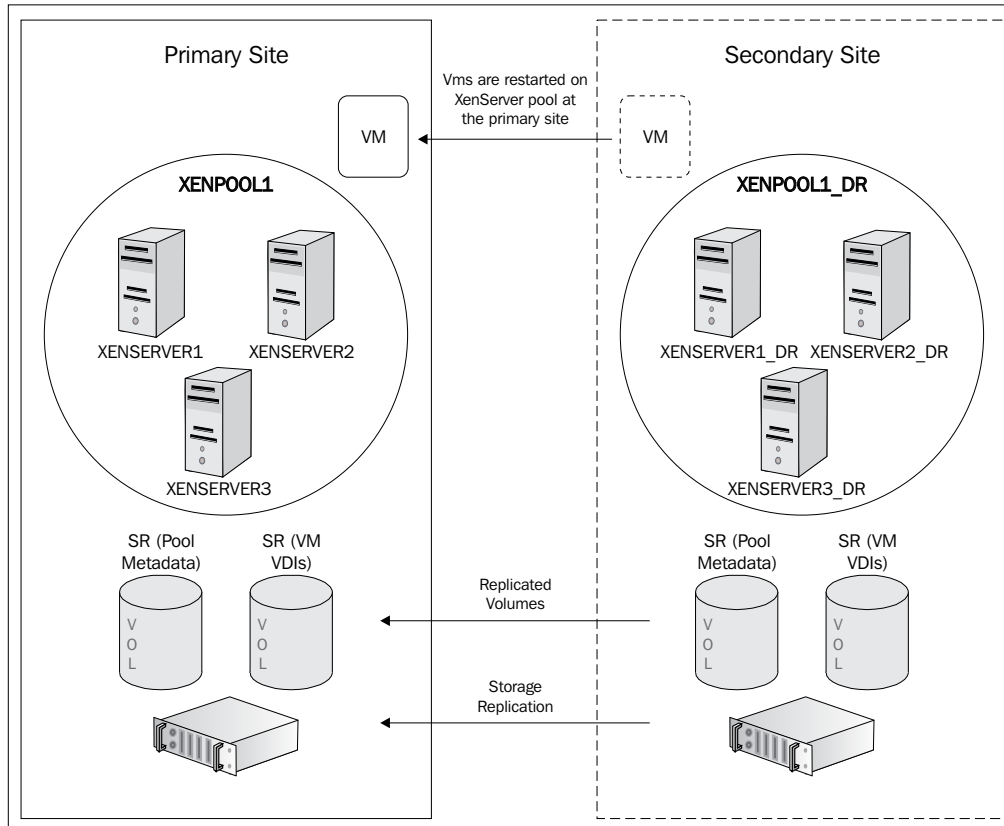
Failover

The failover feature allows VMs and vApps from a failed pool to be recovered on a secondary pool, which is typically in a secondary or DR location. The pool metadata and the VM VDIs are hosted on an SR that is replicated from the primary pool to the secondary pool in order to allow the VMs to be brought at the DR site in the event of a pool failure at the primary site. This is seen in the following diagram, which displays the primary and secondary sites along with the storage-level replication that handles the replication of the XenServer SRs from the primary to the secondary site:



Failback

After the primary site has been restored, XenServer DR can be used to migrate the VMs and vApps to the primary site. In this scenario, the SRs at the secondary site are replicated back to the SRs at the primary site to ensure that the changes that were made while the secondary site was active are available when the primary site is brought back online. This is shown in the following diagram:



Test failover

The test failover option is used to perform a test so that the VMs and vApps can be recovered from the replicated storage to a pool at the secondary site without actually starting the VMs. This feature is critical to any disaster recovery plan as regular testing is a part of any successful plan. The testing process helps you identify any issues with the VMs, SRs, or storage replication that could create an issue during the actual failover process.

XenServer® DR requirements

The following list outlines the requirements for utilizing the XenServer DR feature:

- The SR used must be an iSCSI or Fibre Channel shared SR
- The XenServer version and patch level must be the same at both the primary and secondary sites
- The underlying SRs must be replicated using the storage-level replication



The DR feature does not manage any storage array functionality and replication/mirroring must be configured on the storage array. There are a number of storage vendors that provide the storage mirroring or snapshotting functionality that can be enabled in the vendor's management software. This functionality is often an add-on that must be purchased separately.

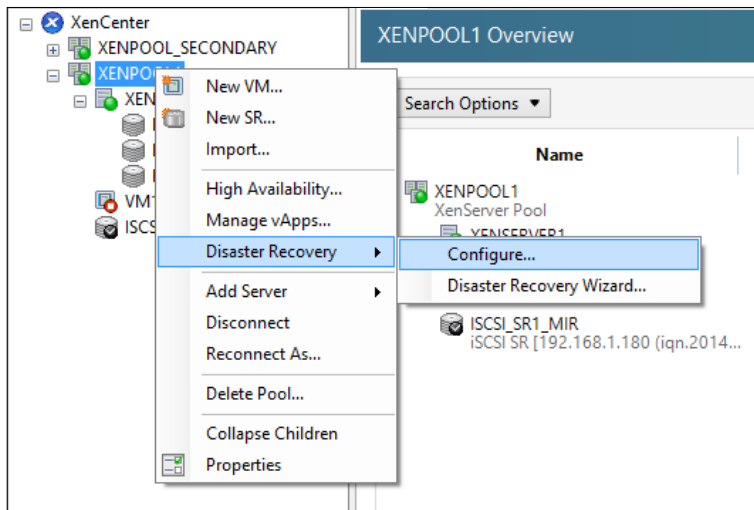
- In order to perform a failback operation, the SRs at the secondary or DR site must be able to replicate data back to the primary site

Configuring XenServer® DR

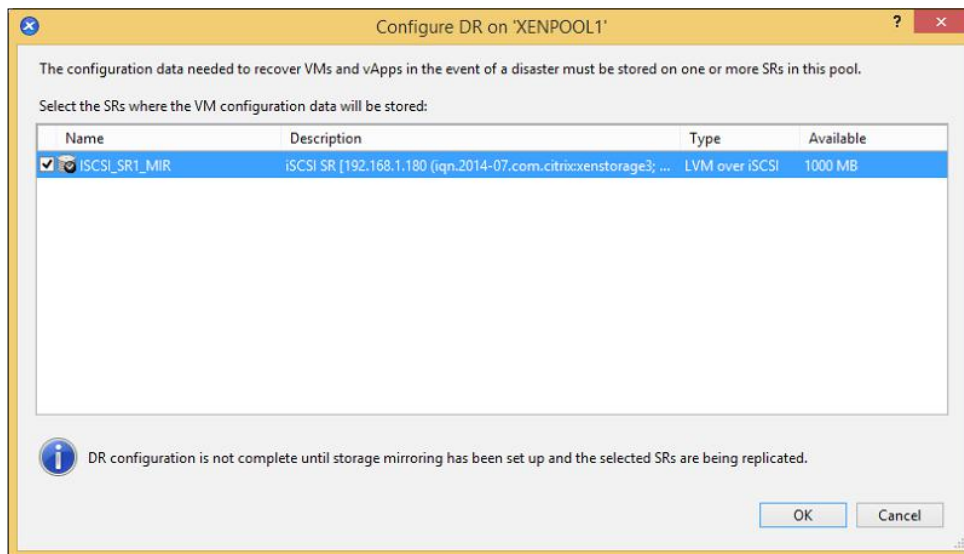
The DR feature requires two XenServer resource pools, a primary and a secondary, with reachability to each other across the management network in order to perform the failover and failback operations. Each pool should be connected to a SR on their respective storage array that is mirrored between the two sites. In the case of the initial configuration, the SR from the primary site should be set to replicate to the secondary site. Following a disaster, the replication should be broken between the primary and secondary SRs in order to avoid any data corruption. The SR from the secondary site should then be configured to replicate data to the primary site before a failback operation is performed.

The following steps cover configuring XenServer DR and selecting the SRs that are used to store the pool metadata:

1. Right-click on the desired resource pool and from the **Disaster Recovery** option, select **Configure...** to open the **Configure DR** dialog box.



2. Select the SRs that will be used for DR and click on **OK** to complete the DR configuration.



- The following screenshot shows the metadata added to the SRs that is used for DR. The metadata can be found under the **Storage** tab of the SR selected during the configure DR process.

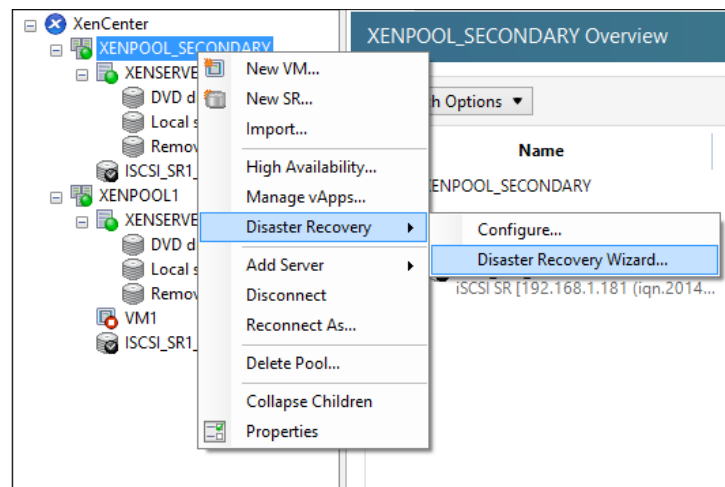


Name	Description	Size	Virtual Machine
Metadata for DR	Used for disaster recovery	256 MB	Control domain on host XENSERVER1
VM1 0		1 GB	VM1

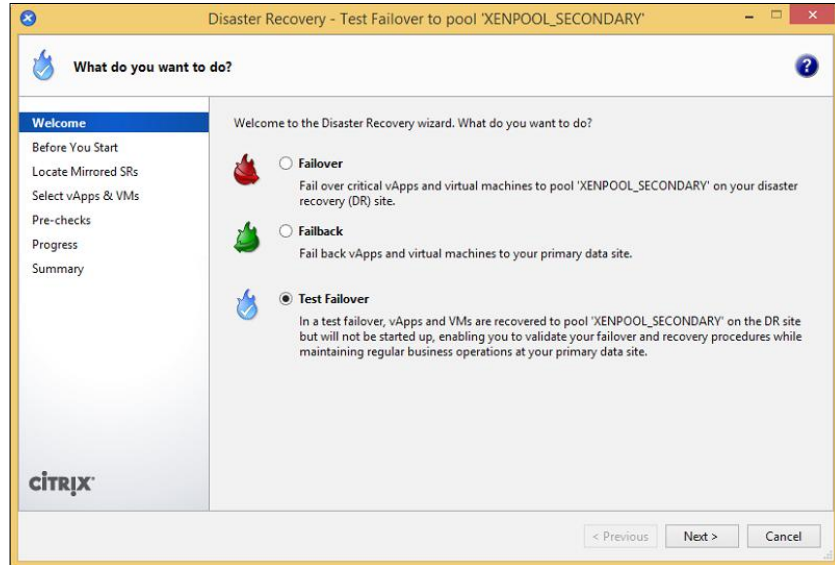
XenServer® DR test failover

The following steps cover testing XenServer DR failover to ensure that the feature is functioning properly:

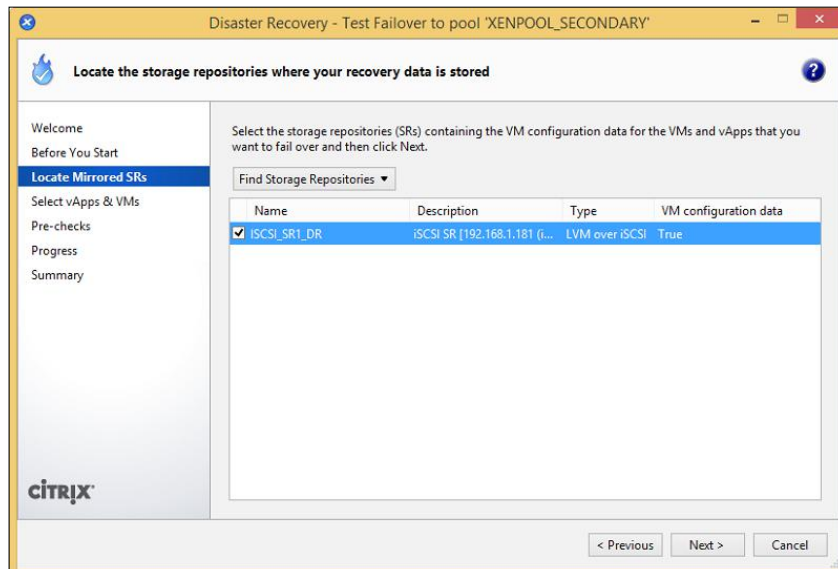
- Right-click on the secondary/DR pool and from the **Disaster Recovery** option, select **Disaster Recovery Wizard...** to launch the **Disaster Recovery** wizard.



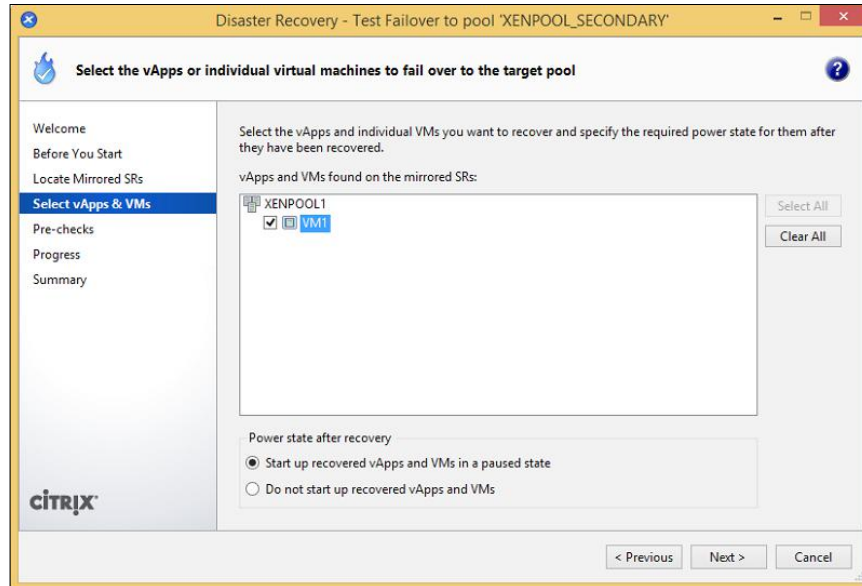
2. Select the **Test Failover** option and click on **Next** to continue.



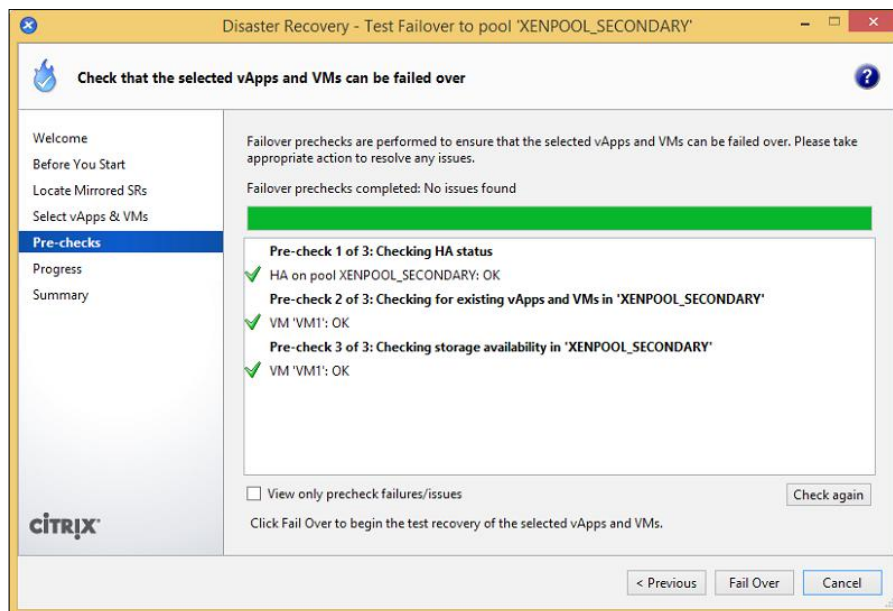
3. Click on **Next** to continue after reading the information on the **Before You Start** page.
4. Select the SR containing the pool metadata for the VMs and vApps that are being recovered. Click on **Next** to continue.



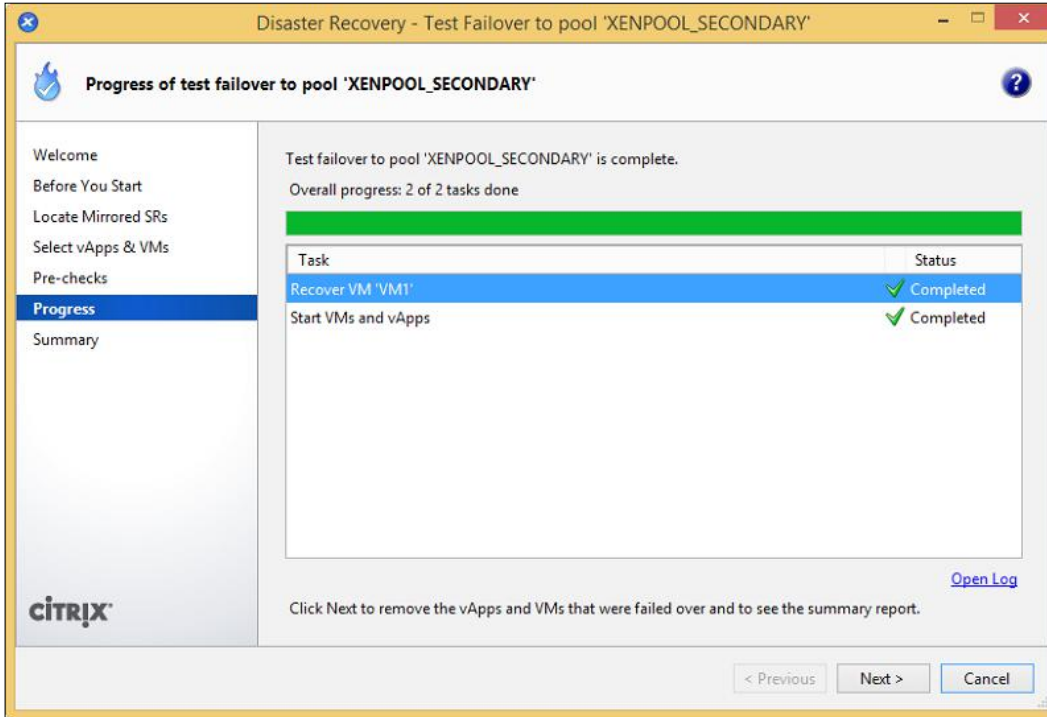
- Select the VMs or vApps to failover and select whether or not to start them after they are recovered. Click on **Next** to continue.



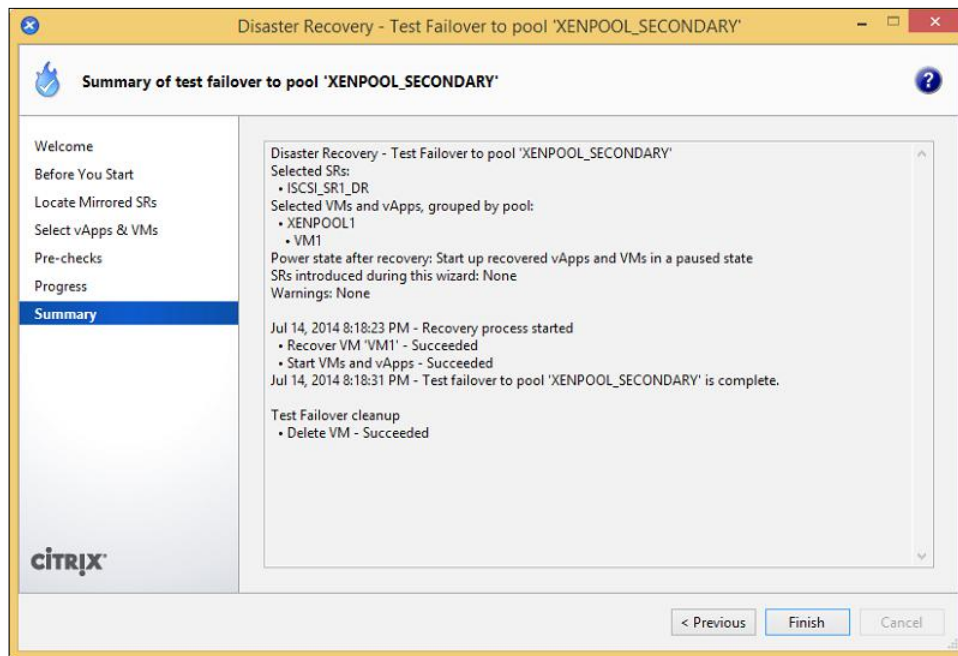
- The wizard performs a number of prechecks to ensure that the failover operation can be performed successfully. Click on **Fail Over** to begin the failover process.



7. Review the status of the failover process and click on **Next** to proceed to the **Summary** page.



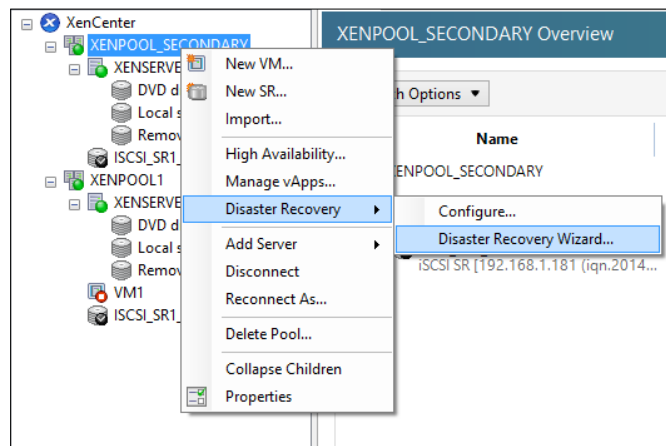
8. Review the summary report and click on **Finish** to complete the test failover.



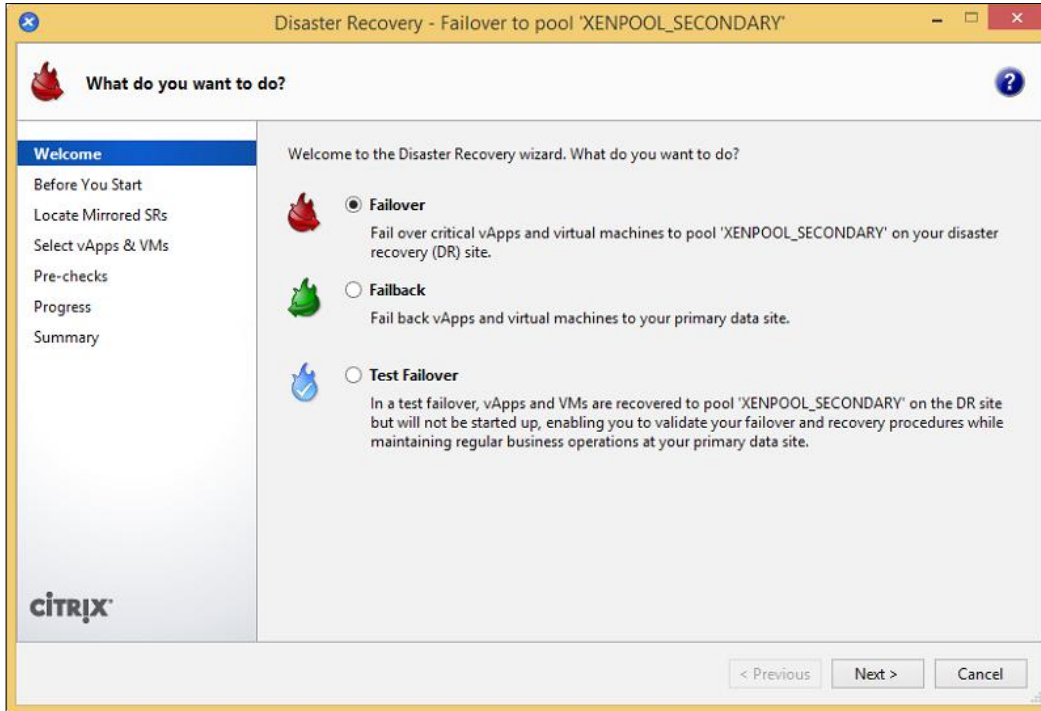
XenServer® DR failover

The following steps cover performing a XenServer DR failover to recover VMs and vApps due to a pool failure:

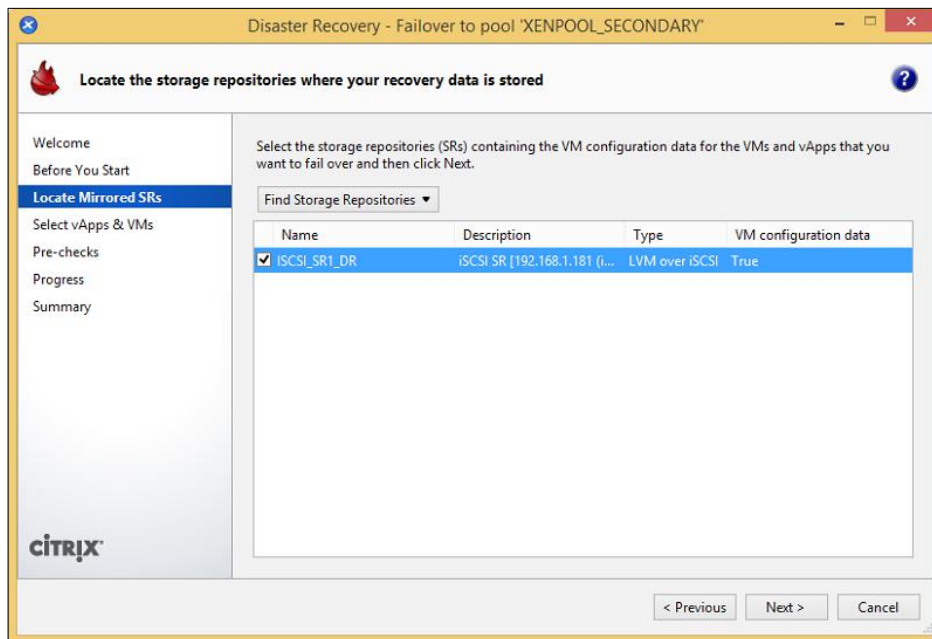
1. Right-click on the secondary/DR pool and from the **Disaster Recovery** option, select **Disaster Recovery Wizard...** to launch the **Disaster Recovery** wizard.



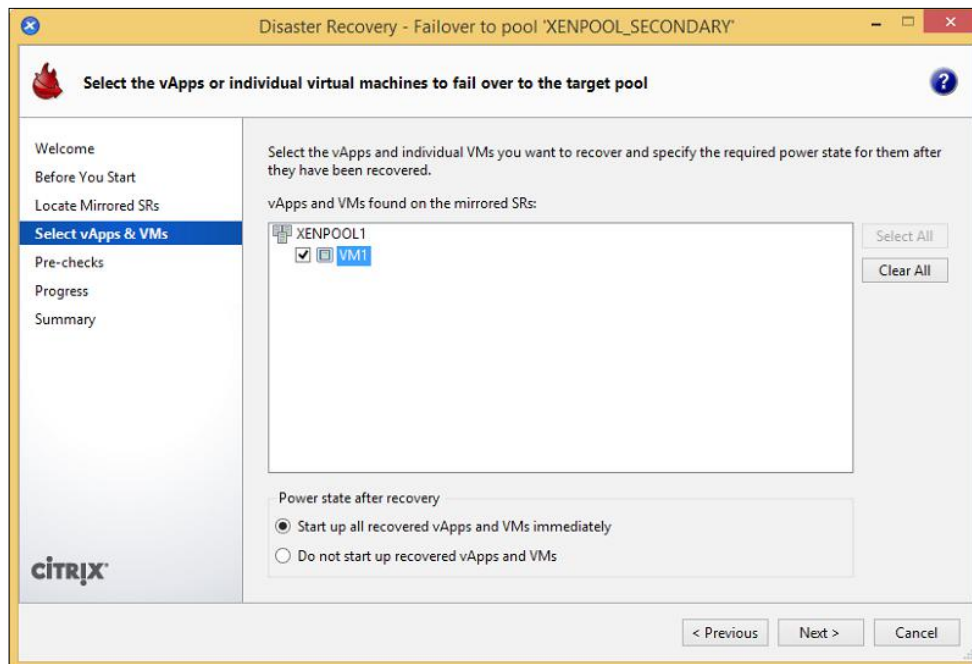
2. Select the **Failover** option and click on **Next** to continue.



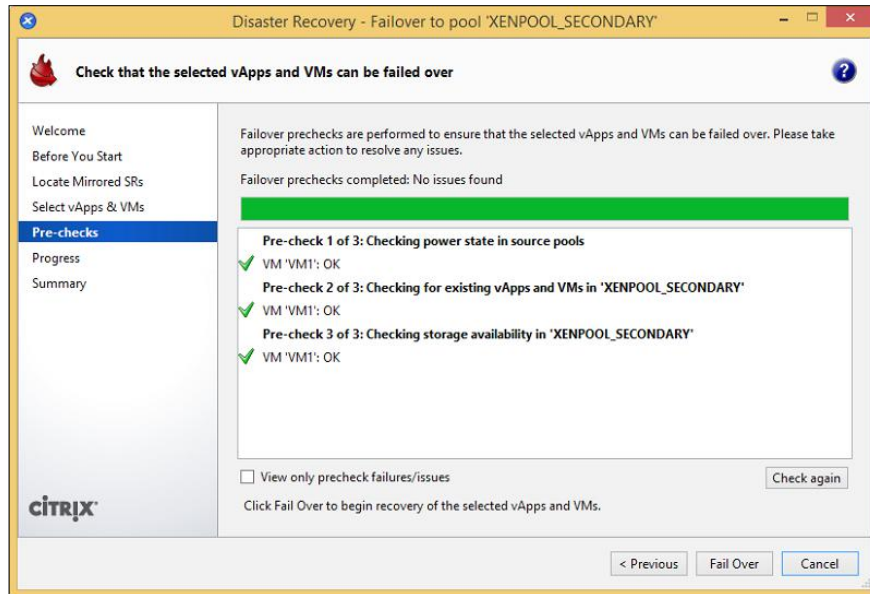
3. Click on **Next** to continue after reading the information on the **Before You Start** page.
4. Select the SR containing the pool metadata for the VMs and vApps that are being recovered. Click on **Next** to continue.



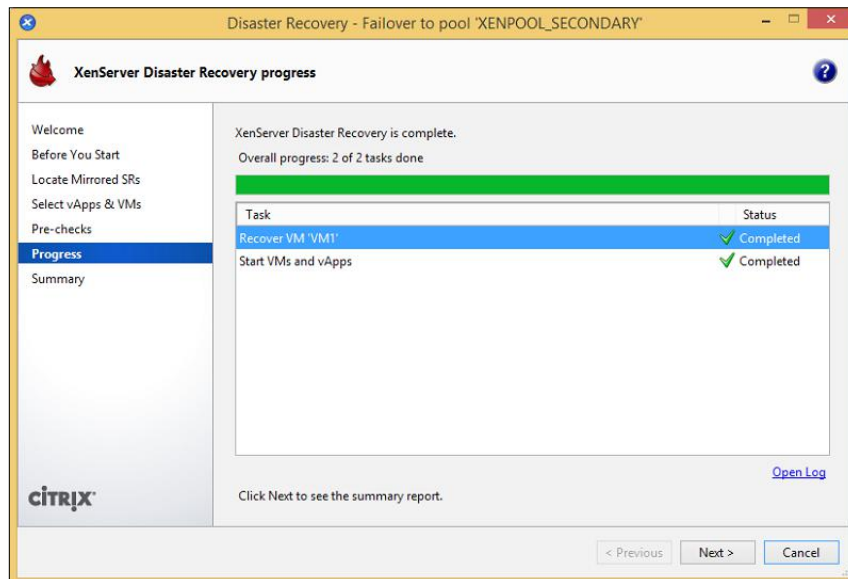
5. Select the VMs or vApps to failover and select whether or not to start them up after they are recovered. Click on **Next** to continue.



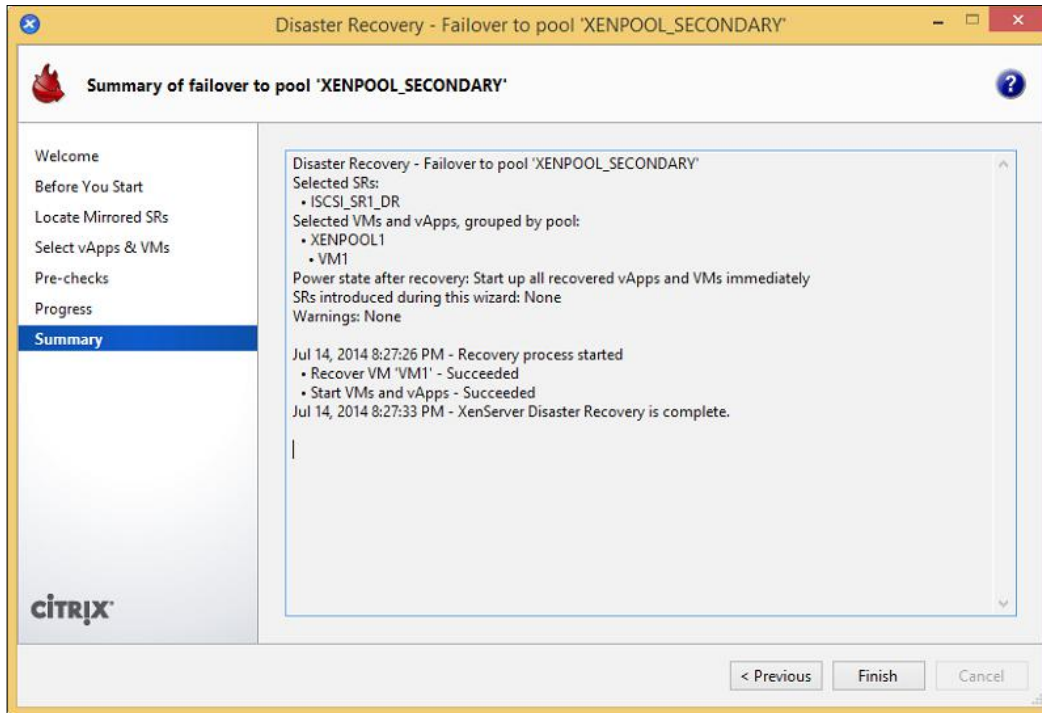
- The wizard performs a number of prechecks to ensure that the failover operation can be performed successfully. Click on **Fail Over** to begin the failover process.



- Review the status of the failover process and click on **Next** to proceed to the **Summary** page.



8. Review the summary report and click on **Finish** to complete the failover.



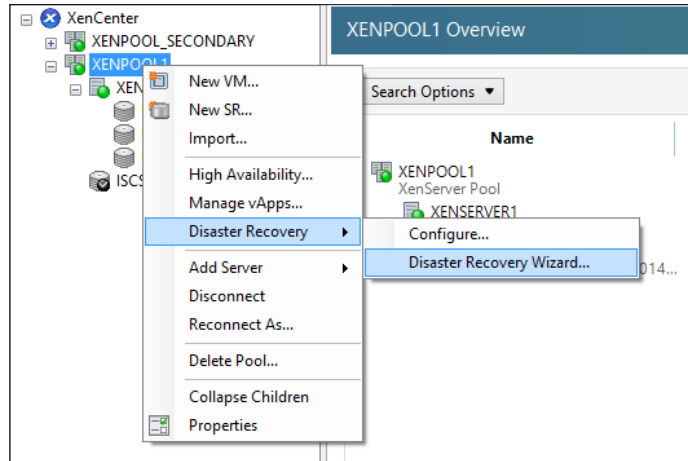
After a successful failover, DR needs to be configured on the secondary site to facilitate the XenServer DR failback feature.

The VMs and vApps that were selected should now appear in the secondary pool.

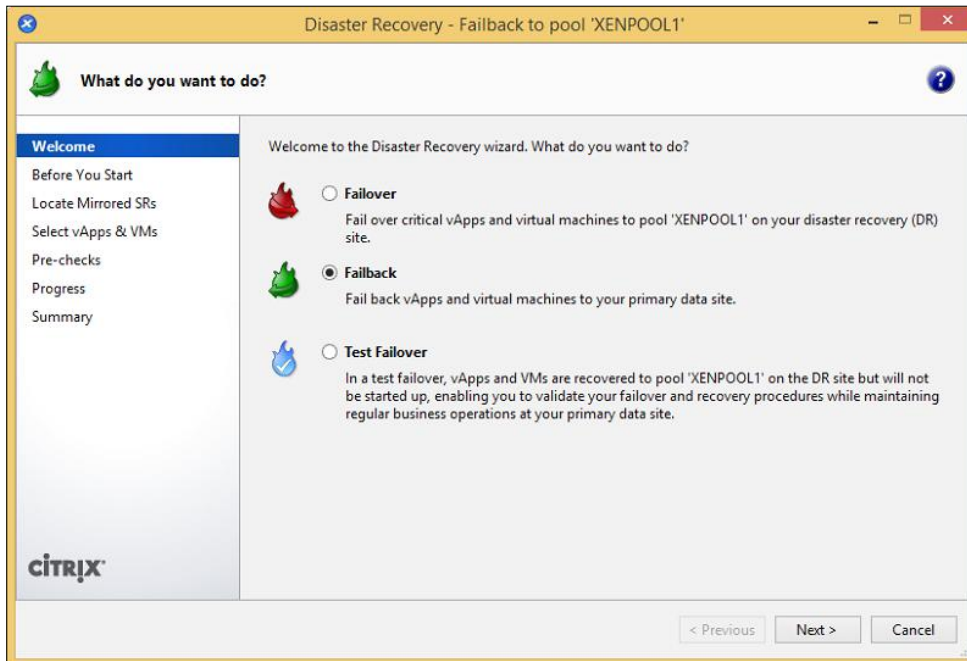
XenServer® DR failback

The following steps cover performing a XenServer DR failback to restore VMs and vApps to the primary site:

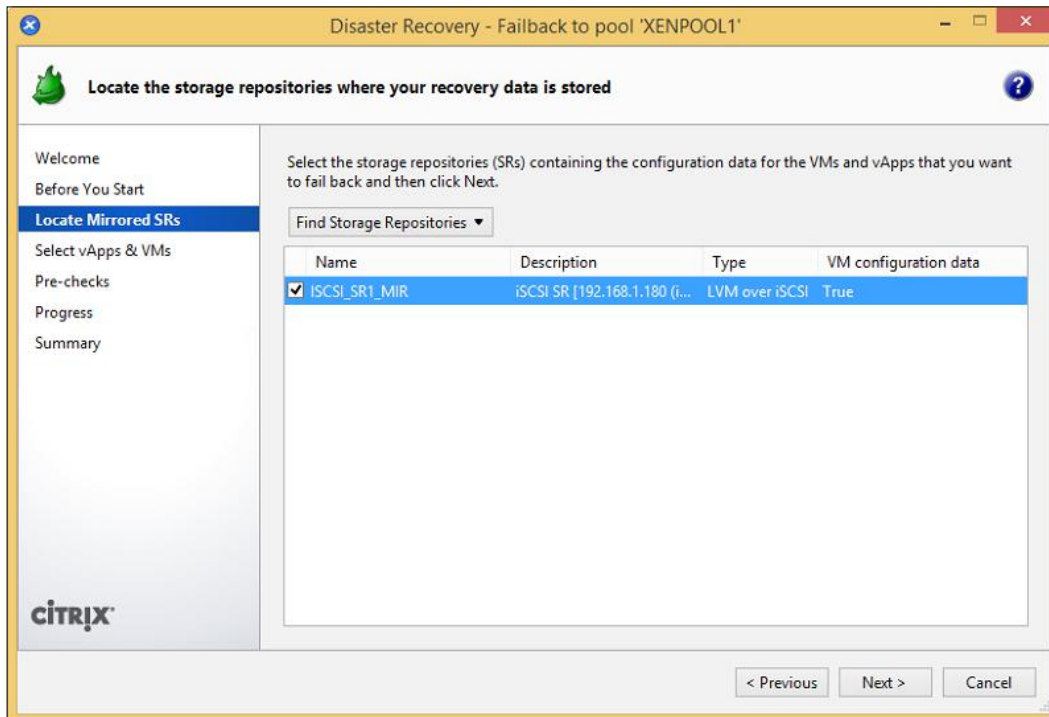
1. Right-click on the primary pool and from the **Disaster Recovery** option, select **Disaster Recovery Wizard...** to launch the **Disaster Recovery** wizard.



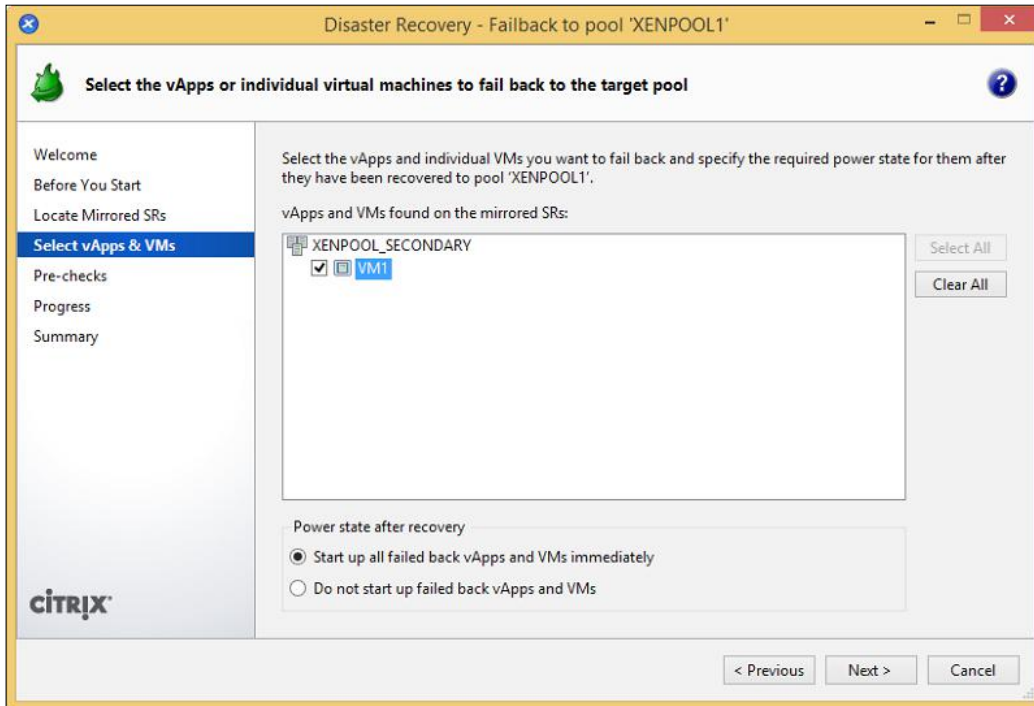
2. Select the **Failback** option and click on **Next** to continue.



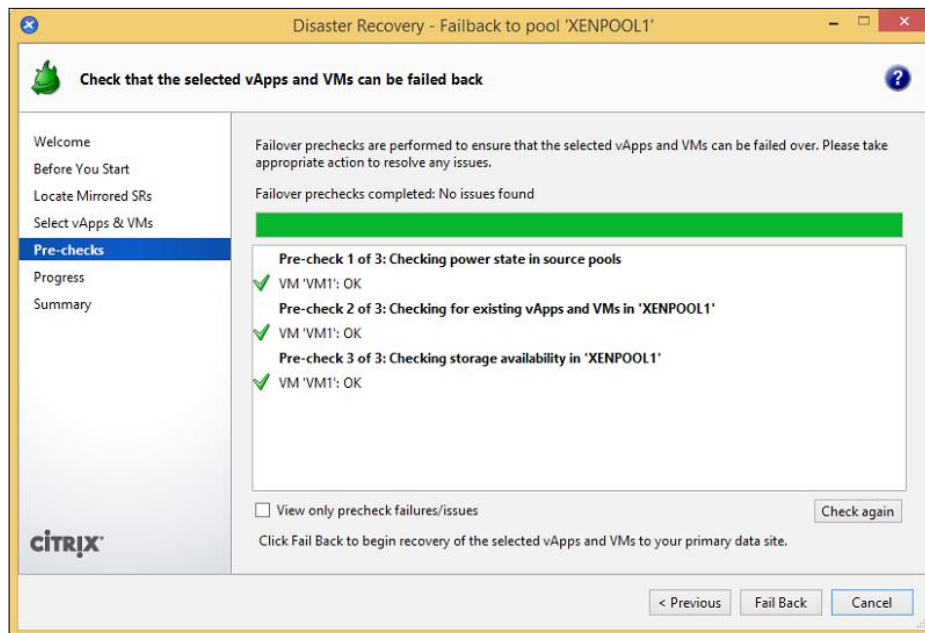
3. Click on **Next** to continue after reading the information on the **Before You Start** page.
4. Select the SR containing the pool metadata for the VMs and vApps that are being recovered. Click on **Next** to continue.



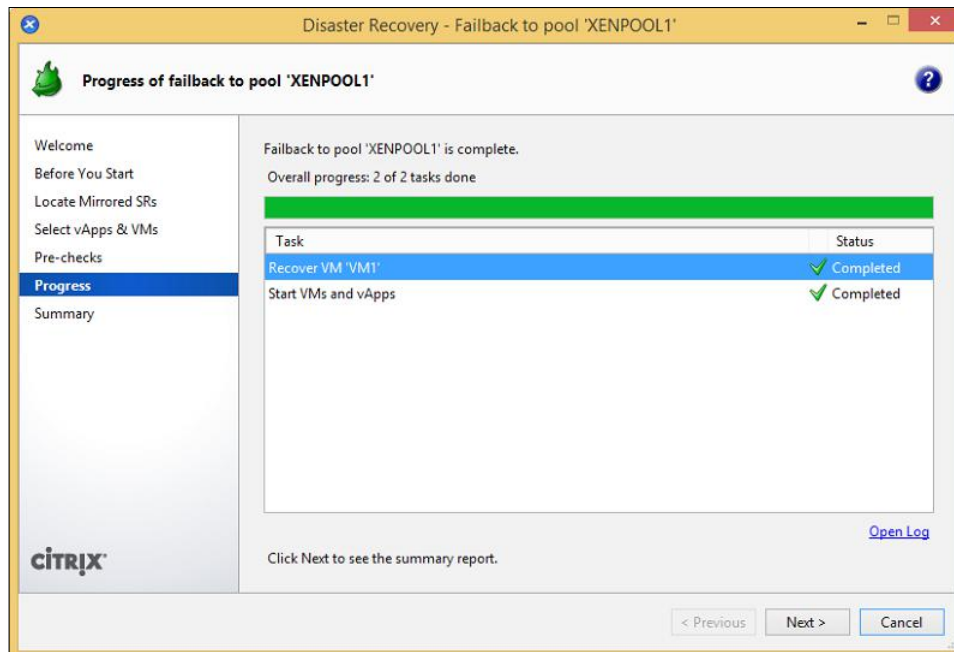
5. Select the VMs or vApps to failback and select whether or not to start them up after they are recovered. Click on **Next** to continue.



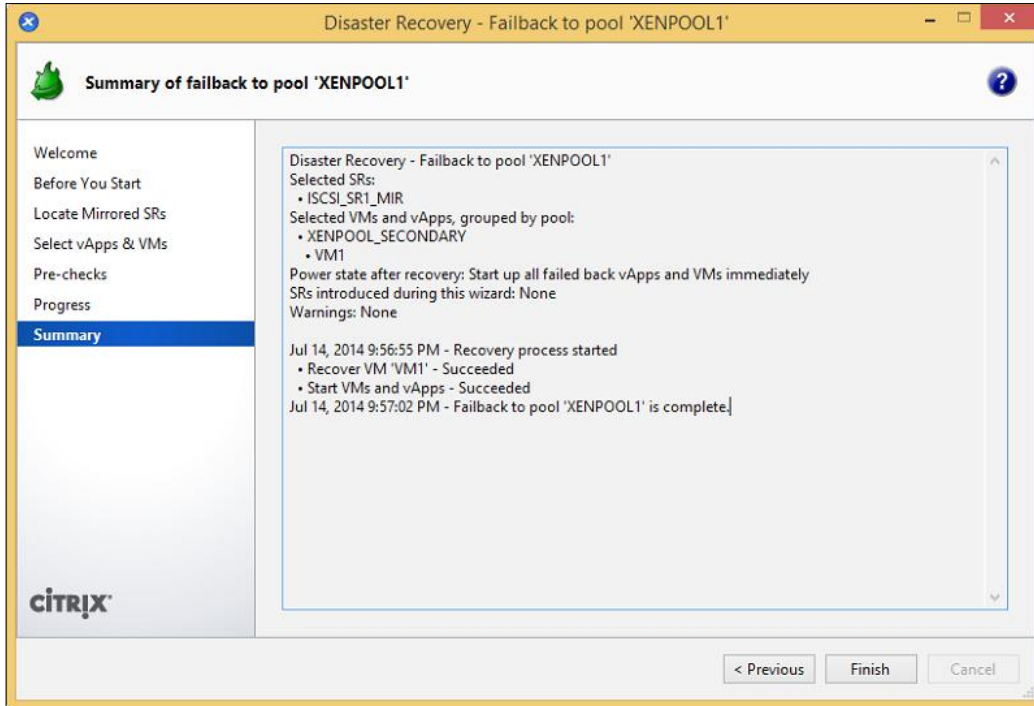
6. The wizard performs a number of prechecks to ensure that the failback operation can be performed successfully. Click on **Fail Back** to begin the failback process.



- Review the status of the failback process and click on **Next** to proceed to the **Summary** page.



8. Review the summary report and click on **Finish** to complete the failback.



Summary

In this chapter, we have looked at some of the major components to address when developing a plan for how to handle failures in our XenServer environment. The development of a plan to restore the environment following a disaster helps you keep calm and level-headed during the disaster, as there is a plan in place. Without a handy plan, administrators often panic and are prone to making mistakes when restoring the environment. We have also looked at backing up and restoring VMs as well as XenServer hosts. Maintaining a current backup of the VMs in the environment is critical to restoring business services following a disaster and provides administrators with the peace of mind that if there is a problem with the VM, it can be restored. We also covered XenServer DR and the benefits it provides by allowing VMs to be recovered in the event of a pool or site failure. The DR feature simplifies the site recovery process for the administrators and provides functionality to perform regular test failovers to ensure that the failover works in the event of a disaster. Now that we have learned how to restore a XenServer deployment in the event of a disaster, in the next chapter, we will take a look at managing and monitoring XenServer.

7

Managing and Monitoring XenServer®

A key aspect of any successful virtualization deployment is the ability to update and monitor the environment to ensure that it is performing optimally, as well as the ability to address any issues that arise in a timely manner. We have covered installing and configuring our XenServer deployment, we will now shift our focus to patching our XenServer environment to maintain system integrity, along with monitoring system performance to ensure that it is operating optimally. XenServer provides several tools that will help us in performing these essential maintenance tasks, such as performance alerts that can be used to notify administrators if certain performance thresholds are reached, as well as support for centralized logging to correlate logs in order to aid in performing root cause analysis in the event of an issue.

In this chapter, you'll learn the following topics:

- XenServer updates
- Monitoring XenServer performance
- Configuring alerts
- XenServer logging

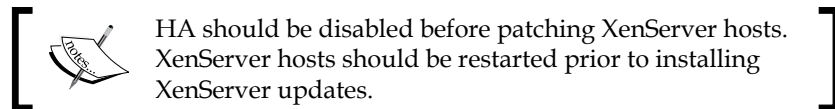
XenServer® updates

Patching is an essential component of maintaining any computer system. Typically, updates or patches are broken down into three categories: feature updates, hotfixes, and security updates. Feature updates are provided to add additional functionality to the product, hotfixes repair a broken feature, and security updates fix identified vulnerabilities.

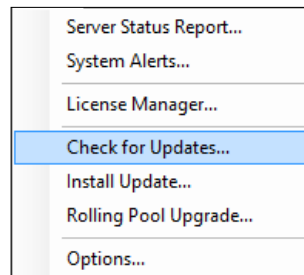
A major change in Version 6.2 of Citrix XenServer is the change in how updates can be deployed for XenServer hosts that are not licensed for Citrix support. If a host is not licensed for Citrix support, then the host can only be patched using the command line.

Deploying updates

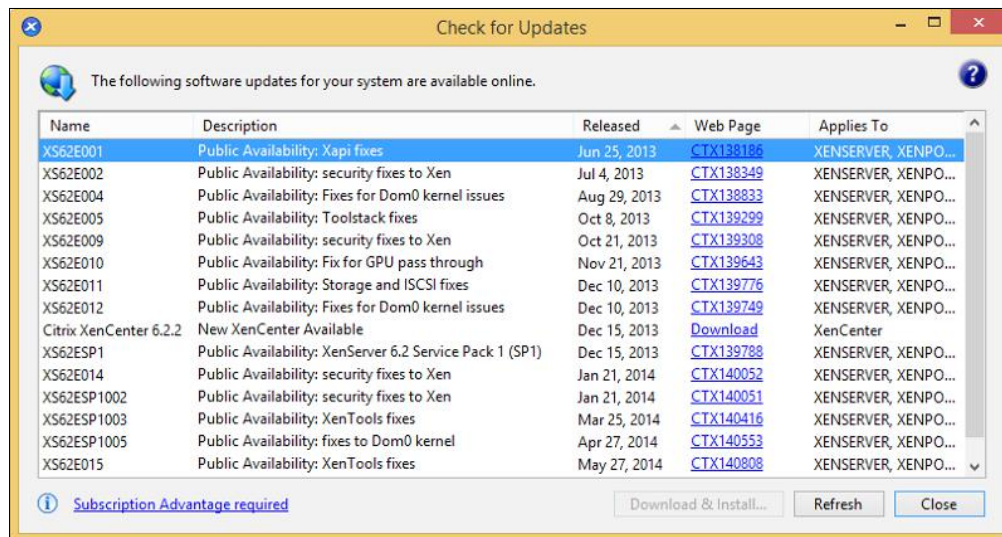
The following steps cover deploying XenServer updates using the `xe` command from the command-line interface of the Windows management station with XenCenter installed.



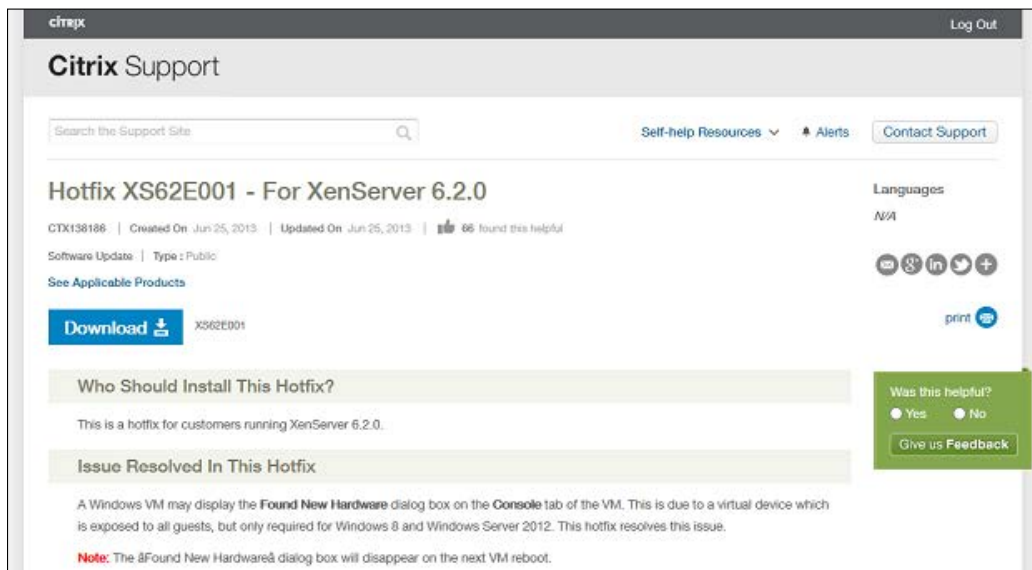
1. Select the **Check for Updates...** option from the **Tools** menu in XenCenter.



2. Click on the blue link under the **Web Page** column to go to the download page for a specific update.



3. Click on the **Download** button on the update page to download the update to the local system. After the download has completed, extract the contents of the .zip file.





4. From the system with XenCenter installed, open a command prompt. Run the following command from the XenCenter directory to upload the update to the XenServer host/pool.

```
xe patch-upload -s XenServer_Hostname -u username -pw user_
password file-name=local_path_of_update
```

The following screenshot shows you how to upload an update to a XenServer host:

```
c:\Program Files (x86)\Citrix\XenCenter>xe patch-upload -s 192.168.1.246 -u root
-pw password file-name=C:\XS62E001\XS62E001.xsupdat
dedcc0dd-d8f3-4f76-90ca-92697c7a44f0
```

 Make a note of the UUID of the patch, as it will be used in the subsequent command. 

5. Run the following command to apply the patch to the XenServer host/pool:

```
xe -s XenServer_Hostname -u username -pw user_password patch-pool-
apply uuid=patch_uuid
```

The following screenshot shows you how to install an update on a XenServer host:

```
c:\Program Files (x86)\Citrix\XenCenter>xe -s 192.168.1.246 -u root -pw password
patch-pool-apply uuid=dedcc0dd-d8f3-4f76-90ca-92697c7a44f0
c:\Program Files (x86)\Citrix\XenCenter>_
```

6. Run the following command to check whether the patch has been applied to the XenServer host/pool:

```
xe patch-list -s XenServer_Hostname -u username -pw user_password
name-label=update_name
```

The following screenshot shows you how to install an update on a XenServer host:

```
c:\Program Files (x86)\Citrix\XenCenter>xe patch-list -s 192.168.1.246 -u root -
pw password name-label=XS62E001
uuid ( R0)      : dedcc0dd-d8f3-4f76-90ca-92697c7a44f0
name-label ( R0) : XS62E001
name-description ( R0) : Public Availability: Xapi fixes
size ( R0) : 6625641
hosts (SR0) : 537c74a5-b328-4885-9f3b-00a15da30bab, 41ce84a6-d
0a1-4688-a05f-3f023e1ebddc
after-apply-guidance (SR0) : restartXAPI
c:\Program Files (x86)\Citrix\XenCenter>_
```

7. Run the following command to place the host into maintenance mode:

```
xe host-disable -s XenServer_Hostname -u username -pw user_
password host=XenServer_Hostname
```

The following screenshot shows you how to place a XenServer host into maintenance mode:

```
c:\Program Files (x86)\Citrix\XenCenter>xe host-disable -s 192.168.1.246 -u root
-pw password host=XENSER2
c:\Program Files (x86)\Citrix\XenCenter>
```

8. Run the following command to evacuate any running virtual machines on the XenServer host before rebooting the host:

```
xe host-evacuate -s XenServer_Hostname -u username -pw user_
password host=XenServer_Hostname
```

The following screenshot shows you how to evacuate any running VMs on the XenServer host:

```
c:\Program Files (x86)\Citrix\XenCenter>xe host-evacuate -s 192.168.1.246 -u root
-pw password host=XENSER2
c:\Program Files (x86)\Citrix\XenCenter>
```

9. Run the following command to reboot the XenServer host after the virtual machines have been migrated to the other host in the pool:

```
xe host-reboot -s XenServer_Hostname -u username -pw user_password
host=XenServer_Hostname
```

The following screenshot shows you how to reboot the XenServer host after the updates have been applied:

```
c:\Program Files (x86)\Citrix\XenCenter>xe host-reboot -s 192.168.1.246 -u root
-pw password host=XENSER2
c:\Program Files (x86)\Citrix\XenCenter>
```

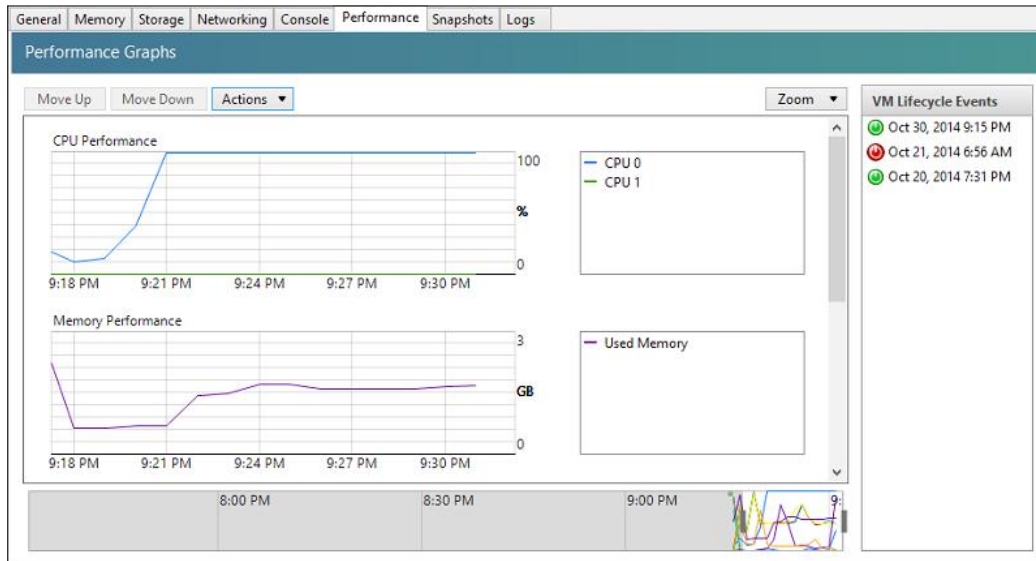
Monitoring XenServer® performance

Being able to effectively analyze the system performance is a critical aspect of ensuring that systems continually perform as expected. XenServer provides a number of tools to assess the system performance both in real time as well as historically.

The following screenshot displays the real-time performance metrics for the entire pool as well as the VMs that are running on the pool. This view provides a good overview of the pool performance along with the resources that are being consumed by individual VMs. Complete performance data for VMs requires the installation of XenServer Tools on the VM. This view can be found under the **Search** tab of the XenServer pool.

Name	CPU Usage	Used Memory	Disks (avg / max KBs)	Network (avg / max KBs)	Address	Uptime
XENPOOL1 XenServer Pool	-	-	-	-	-	-
XENSERVER3 Default install of XenServer	1% of 4 CPUs	879 of 6144 MB	-	1/2	192.168.1.246	3 hours 53 minutes
XENSERVER2 Default install of XenServer	1% of 4 CPUs	2919 of 4096 MB	-	2/2	192.168.1.249	16 minutes
Windows 7	1% of 2 CPUs	603 of 2048 MB	72/145	0/0	fe80::383d:3ec3...	2 minutes
VM1	-	-	-	-	-	-
ISCSI_SR1_MIR ISCSI SR [T92.168.1.180 (i...	-	-	-	-	192.168.1.180	-

The following screenshot displays more granular performance metrics for a XenServer host that can be used to analyze the system performance over a longer period of time, up to 1 year. The graphs can be modified to include additional performance metrics. This view can be found under the **Performance** tab of XenServer:

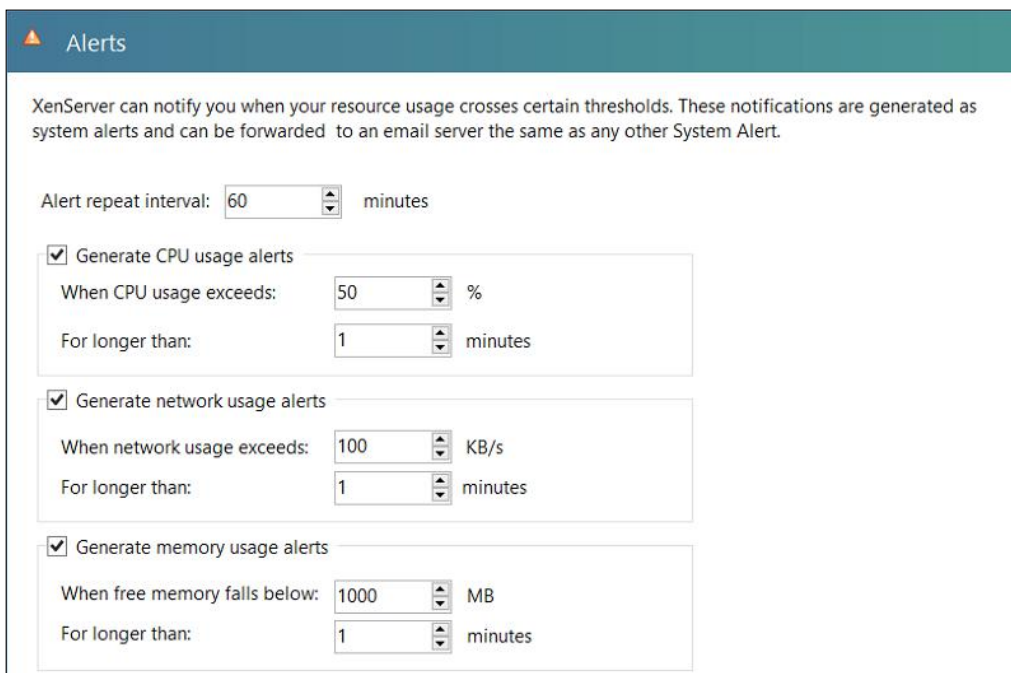


Performance alerts

Performance alerts can be configured to generate system alerts, when defined thresholds are reached for objects such as XenServer hosts, VMs, and SRs. These alerts can provide valuable insight when addressing performance issues or even aid in making adjustments before the performance issues impact users.

The alerts can be configured within the properties of the hosts, VMs, and SRs under the **Alerts** section.

The following screenshot displays the basic alerts available for XenServer hosts:



The screenshot shows the 'Alerts' configuration window for XenServer. It features a teal header with an orange triangle icon and the title 'Alerts'. Below the header, a paragraph explains that XenServer can notify users when resource usage crosses certain thresholds, and these notifications are generated as system alerts that can be forwarded to an email server. The configuration options are as follows:

- Alert repeat interval:** 60 minutes
- Generate CPU usage alerts**
 - When CPU usage exceeds: 50 %
 - For longer than: 1 minutes
- Generate network usage alerts**
 - When network usage exceeds: 100 KB/s
 - For longer than: 1 minutes
- Generate memory usage alerts**
 - When free memory falls below: 1000 MB
 - For longer than: 1 minutes

The following screenshot displays the basic alerts available for SRs:

Alerts

XenServer can notify you when your resource usage crosses certain thresholds. These notifications are generated as system alerts and can be forwarded to an email server the same as any other System Alert.

Alert repeat interval: 60 minutes

Generate storage throughput alerts

When SR throughput for any host exceeds: 1000 KB/s

For longer than: 1 minutes

The following screenshot displays the basic alerts available for VMs:

Alerts

XenServer can notify you when your resource usage crosses certain thresholds. These notifications are generated as system alerts and can be forwarded to an email server the same as any other System Alert.

Alert repeat interval: 60 minutes

Generate CPU usage alerts

When CPU usage exceeds: 50 %

For longer than: 1 minutes

Generate network usage alerts

When network usage exceeds: 100 KB/s

For longer than: 1 minutes

Generate disk usage alerts

When disk usage exceeds: 1000 KB/s

For longer than: 1 minutes

Additional metrics can be used to create advanced alerts by utilizing the command line. Additional information can be found in the *Citrix XenServer 6.2.0 Administrator's Guide*.

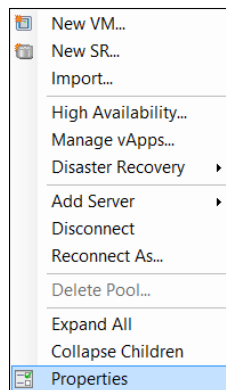
E-mail notifications

XenServer supports sending e-mail notifications for system alerts such as update notifications and performance alerts. This helps us ensure that we are constantly aware of what is happening in our environment. The following sections cover configuring XenServer to use an SMTP server for sending the e-mail notifications from both the XenCenter GUI and the CLI.

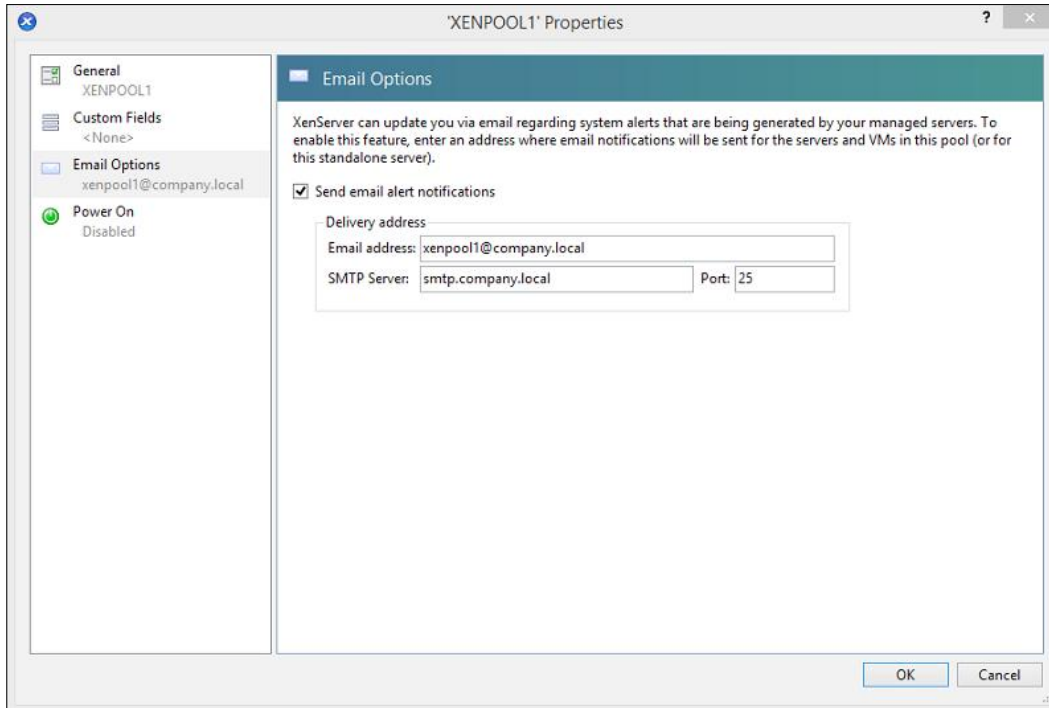
Configuring e-mail notification settings (using the GUI)

The following steps cover configuring e-mail settings for sending e-mail notifications of system alerts using the XenCenter interface:

1. Right-click the desired server/pool and select the **Properties** option.



2. Select the **Email Options** section to configure settings for e-mail notifications. Check the **Send email alert notifications** checkbox to enable e-mail notifications. In the **Email address** textbox, enter the sender's e-mail address that XenServer will send e-mails to. Enter the SMTP server hostname or IP address in the **SMTP Server** textbox and provide the server port number in the **Port** textbox. Click on the **OK** button to save the changes.



Configuring e-mail notification settings (using the CLI)

The following steps cover configuring settings for sending system e-mail notifications of system alerts via the command line using the XE command:

1. The following command is used to configure the sender's address used by the XenServer host when sending e-mail notifications:

```
xe pool-param-set uuid=pool_uuid other-config:mail-destination=source_address
```

The following screenshot shows you how to configure the sender's SMTP address for e-mail notifications on a XenServer host:

```
[root@XENSERVER1 ~]# xe pool-param-set uuid=e3559531-b9b6-0812-00c7-3a60fb12dd12
other-config:mail-destination=xenpool1@company.local
[root@XENSERVER1 ~]# █
```

2. The following command is used to set the SMTP server information:

```
xe pool-param-set uuid=pool_uuid other-config:ssmtp-mailhub=smtp_
server:smtp_port
```

The following screenshot shows you how to configure the SMTP server and port for e-mail notifications on a XenServer host:

```
[root@XENSERVER1 ~]# xe pool-param-set uuid=e3559531-b9b6-0812-00c7-3a60fb12dd12
other-config:ssmtp-mailhub=smtp.company.local:25
[root@XENSERVER1 ~]# █
```

Configuring e-mail notification authentication settings (using the CLI)

The following steps cover configuring the basic e-mail server settings and allows you to provide a username and password if required by the e-mail system:

1. Create the `mail-alarm.conf` configuration file, which is used for e-mail settings, by running the following command:

```
nano /etc/mail-alarm.conf
```

The following screenshot shows you how to configure the basic e-mail settings:

```
[root@XENSERVER etc]# nano /etc/mail-alarm.conf █
```

2. Enter the username for the `authUser` property, the password for the `authPass` property, and the SMTP server name and port number for the `mailhub` property. The `root` property should be left as the default of `postmaster`. After the desired information has been entered, press `Ctrl + X` to save the file and press `Y` on the keyboard to confirm it.

```
GNU nano 1.3.12 File: /etc/mail-alarm.conf
root=postmaster
authUser=Xenserver
authPass=P@$w0rd!
mailhub=SMTP.company.local:25
```

Simple Network Management Protocol

Simple Network Management Protocol (SNMP) is another tool available on Citrix XenServer that can be used to monitor the health of the XenServer host. SNMP allows performance metrics to be polled from **Network Management Software (NMS)** so that it can be used in order to provide a complete performance view across the entire environment.

Configuring SNMP

The following steps cover configuring SNMP on a XenServer host using the command line:

1. Run the following command to modify the `iptables` configuration file:

```
nano /etc/sysconfig/iptables
```

The following screenshot shows you how to launch the nano text editor to modify the `iptables` configuration file:

```
[root@XENSERVER1 ~]# nano /etc/sysconfig/iptables
```

2. Add the following line to the `iptables` configuration file to permit SNMP access to the host from the designated management station:

```
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp -s SNMP_
MANAGEMENTN_STATION_IP_ADDRESS --dport 161 -j ACCEPT
```

The following screenshot shows you how to add an entry to the `iptables` configuration file on a XenServer host to allow SNMP access from only the designated SNMP management station:

```

GNU nano 1.3.12      File: /etc/sysconfig/iptables      Modified
# Firewall configuration written by system-config-securitylevel
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -p icmp --icmp-type any -j ACCEPT
-A RH-Firewall-1-INPUT -p 50 -j ACCEPT
-A RH-Firewall-1-INPUT -p 51 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp --dport 5353 -d 224.0.0.251 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp -m udp --dport 631 -j ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m tcp --dport 631 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp -m udp --dport 67 --in-interface xenapi -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 694 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 443 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp -s 192.168.1.180 --dport 161 -j ACCEPT
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT

```

- Run the following command to restart the `iptables` service, in order to apply the firewall changes made in step 2:

```
Service iptables restart
```

The following screenshot shows you how to restart the `iptables` service on the XenServer host:

```

[root@XENSERVER1 ~]# service iptables restart
Flushing firewall rules:          [ OK ]
Setting chains to policy ACCEPT: filter [ OK ]
Unloading iptables modules:      [ OK ]
Applying iptables firewall rules: [ OK ]
[root@XENSERVER1 ~]#

```

- Run the following command to edit the SNMP configuration file:

```
nano /etc/snmp/snmpd.conf
```

The following screenshot shows you how to launch the nano text editor in order to modify the `snmpd.conf` configuration file:

```
[root@XENSERVER1 ~]# nano /etc/snmp/snmpd.conf
```

5. Modify the `community` string in the `snmpd.conf` configuration file to the desired community string. Press `Ctrl + X` on the keyboard and then `Y` to save the configuration file.

```
GNU nano 1.3.12 File: /etc/snmp/snmpd.conf
#####
# Access Control
#####

# As shipped, the snmpd demon will only respond to queries on the
# system mib group until this file is replaced or modified for
# security purposes.

###
# First, map the community name "public" into a "security name"

#      sec.name      source      community
com2sec notConfigUser default secretcommunity
```

6. Run the following command to configure the `snmpd` service to automatically start when the host boots up:

```
chkconfig snmpd on
```

The following screenshot shows you how to configure the XenServer host to automatically start the SNMP service on boot:

```
[root@XENSERVER1 ~]# chkconfig snmpd on
[root@XENSERVER1 ~]#
```

7. Run the following command to restart the `snmpd` service:

```
service snmpd restart
```

The following screenshot shows you how to restart the SNMP service on the XenServer host:

```
[root@XENSERVER1 ~]# service snmpd restart
Stopping snmpd: [ FAILED ]
Starting snmpd: [ OK ]
[root@XENSERVER1 ~]#
```



Stopping the `snmpd` service failed because the service has not yet begun. The `restart` command should be run to accommodate for any host in which the `snmpd` service might have already been started.

XenServer® logging

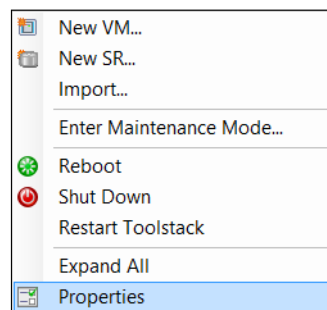
A very good place to start when experiencing issues with a XenServer host is looking at the system logs to get a better idea of what the system is doing. Syslog provides us with a built-in mechanism for logging system events and is commonly used by Linux administrators and network engineers to ensure system health. In environments where there are only a couple of hosts, setting up a central syslog might not be a high priority, but when managing tens or hundreds of XenServer hosts, having a centralized location for logging is imperative to monitor system health.

The local system logs can be found in the `/var/log/messages` file in the event that a remote syslog location is not configured or there is an issue with remote logging.

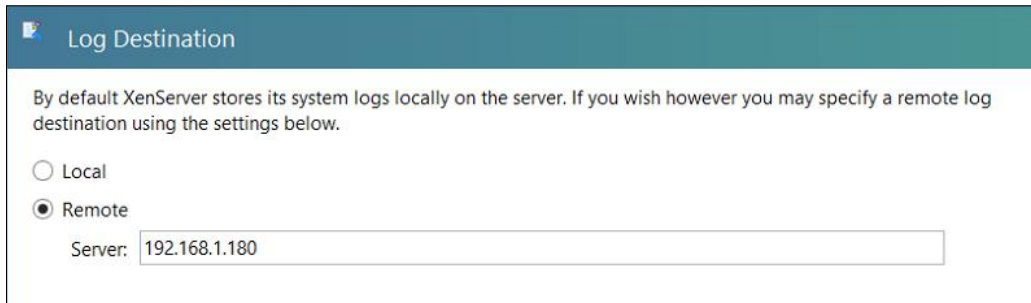
Configuring remote logging (using the GUI)

The following steps cover configuring a XenServer host in order to log to a remote syslog server from within the XenCenter GUI:

1. Right-click on the desired server and select the **Properties** option.



2. Click on the **Log Destination** tab in the **Properties** dialog box, select the **Remote** option, and enter the hostname or IP address of the syslog server. Click on **OK** to save the changes.



Configuring remote logging (using the CLI)

The following set of commands cover configuring a XenServer host to log to a remote syslog server from the command line using the XE command:

1. The following command is used to set the remote server that is used for logging:

```
xe host-param-set uuid=XenServer_UUID logging:syslog_  
destination=syslog_server
```

The following screenshot shows you how to configure the syslog destination on a XenServer host:

```
[root@XENSERVER1 ~]# xe host-param-set uuid=537c74a5-b328-4885-9f3b-00a15da30bab  
logging:syslog_destination=192.168.1.180  
[root@XENSERVER1 ~]# █
```

2. The following command must be run to commit the changes:

```
xe host-syslog-reconfigure host-uuid=XenServer_UUID
```

The following screenshot shows you how to commit the syslog destination on a XenServer host:

```
[root@XENSERVER1 ~]# xe host-syslog-reconfigure host-uuid=537c74a5-b328-4885-9f3b-00a15da30bab  
[root@XENSERVER1 ~]# █
```

- The changes can be verified by running the following command:

```
xe host-param-get uuid=XenServer_UUID param-name=logging
```

The following screenshot shows you how to retrieve the syslog destination configured on a XenServer host:

```
[root@XENSERVER1 ~]# xe host-param-get uuid=537c74a5-b328-4885-9f3b-00a15da30bab
param-name=logging
syslog_destination: 192.168.1.180
[root@XENSERVER1 ~]# █
```

The XenCenter® event log

The XenCenter event log can be used to track the recent operations performed in XenCenter or even the status of the pending operations. The following screenshot displays the event log, which can be found in the **Logs** tab of any object in XenCenter:

Event	Time
<p>Repairing SR NFS virtual disk storage</p> <p>Details: Repaired SR NFS virtual disk storage</p> <p>Time: 00:00:02</p>	Jul 26, 2014 10:47:30 PM
<p>Repairing SR NFS virtual disk storage</p> <p>Error: Unable to detect an NFS service on this target.</p> <p>Time: 00:00:01</p>	Jul 26, 2014 10:22:17 PM
<p>Connected to 192.168.1.248</p> <p>Details: Connection to 192.168.1.248 successful.</p>	Jul 26, 2014 10:08:10 PM

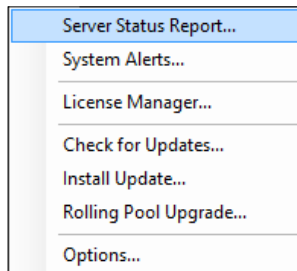
The server status report

XenServer server status reports provide detailed information regarding the configuration of the XenServer host(s) for which the report is generated. Information such as XenServer logs, system services, hardware details, and disk configuration are provided in the report that can be very useful when troubleshooting an issue with a XenServer host.

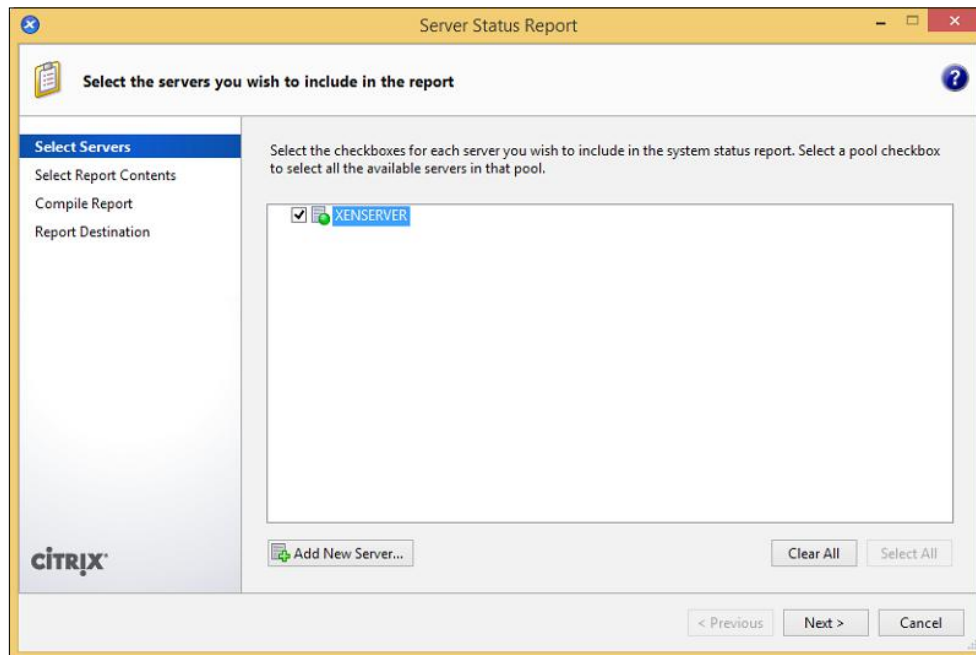
Generating a server status report (using the GUI)

The following steps cover generating a server status report through the XenCenter GUI:

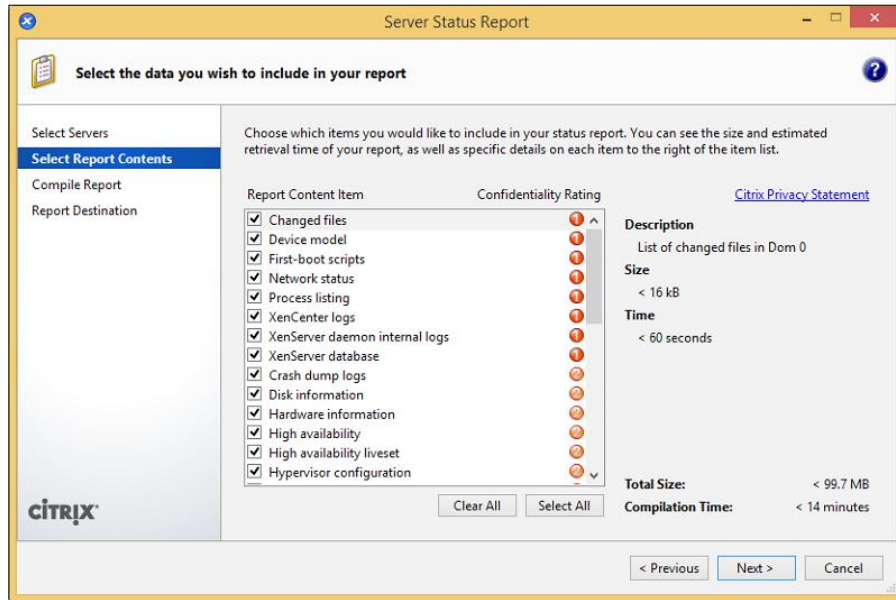
1. Select the **Server Status Report...** option from the **Tools** menu in XenCenter.



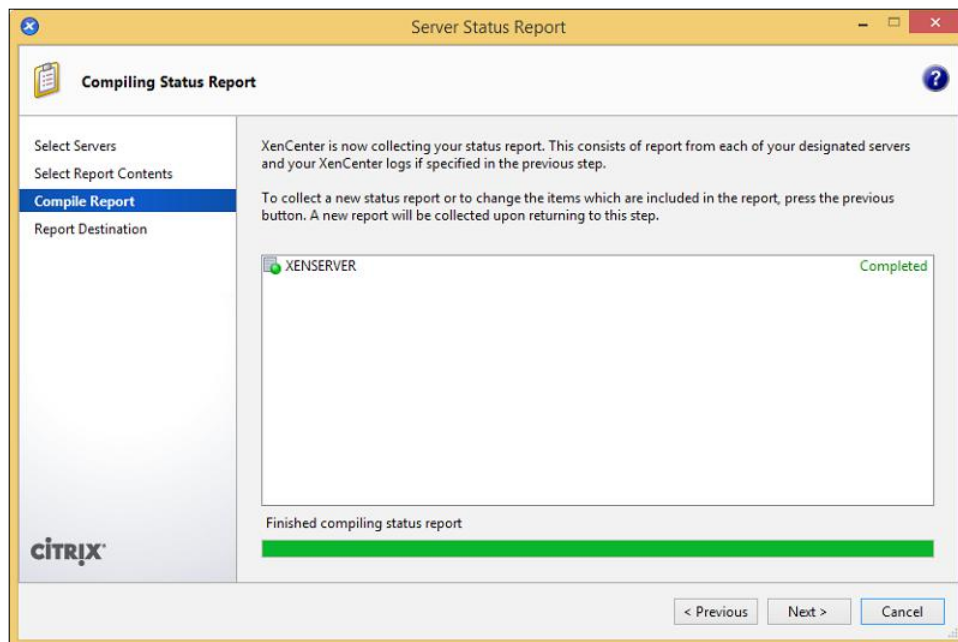
2. Select the XenServer host for which the report will be generated. Click on **Next** to continue.



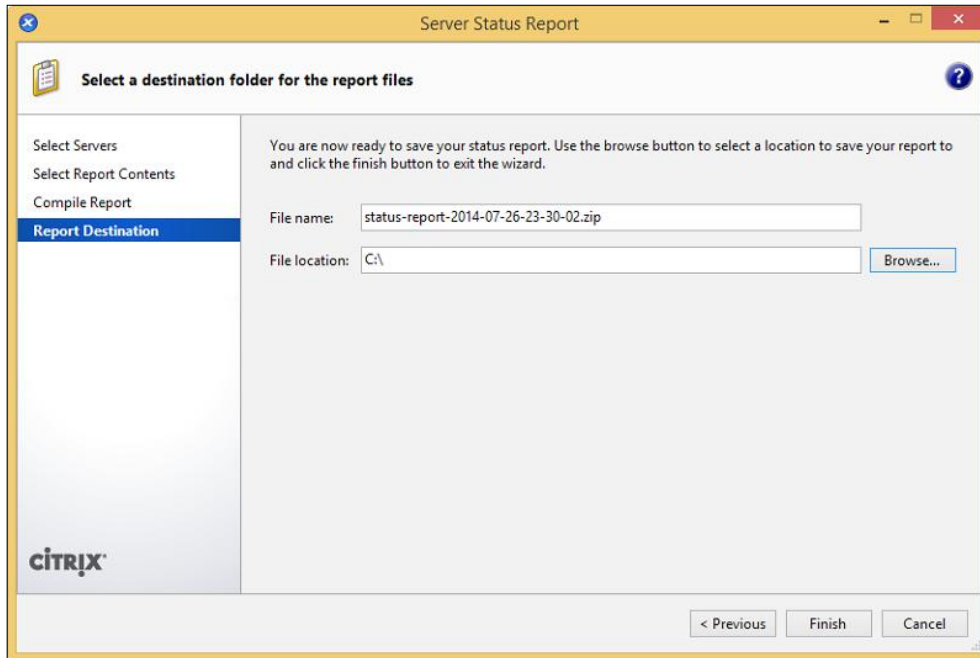
3. Select the information to include the status report in the server. Click on **Next** to continue.



4. Click on **Next** to continue after the report has finished compiling.



5. Provide a filename for the server status report and the location on the local system to save the report. Click on **Finish** to save the report.



Generating a server status report (using the CLI)

The following command covers generating a XenServer status report using the `xe` command from the command-line interface:

```
xen-bugtool --yestoall
```

The following screenshot shows you how to generate a status report on a XenServer host:

```
[root@XENSERVER1 ~]# xen-bugtool --yestoall
Warning: '--yestoall' argument provided, will not prompt for individual files.

This application will collate the Xen dmesg output, details of the hardware configuration of your machine, information about the build of Xen that you are using, plus, if you allow it, various logs.

The collated information will be saved as a .tar.bz2 for archiving or sending to a Technical Support Representative.

The logs may contain private information, and if you are at all worried about that, you should exit now, or you should explicitly exclude those logs from the archive.

[10/30/14 16:25:07 CDT] Running commands to collect data
[10/30/14 16:25:08 CDT] Creating output file
Writing tarball /var/opt/xen/bug-report/bug-report-20141030162508.tar.bz2 successful.
[root@XENSERVER1 ~]#
```

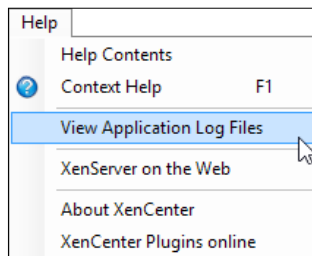
The XenCenter® application log

The XenCenter application log can be used to view all the operations performed in XenCenter as well as any errors that occurred when using XenCenter. The logfile only contains information about XenCenter sessions on the local system. The XenCenter logfile can be found in the user's profile folder at the following path:

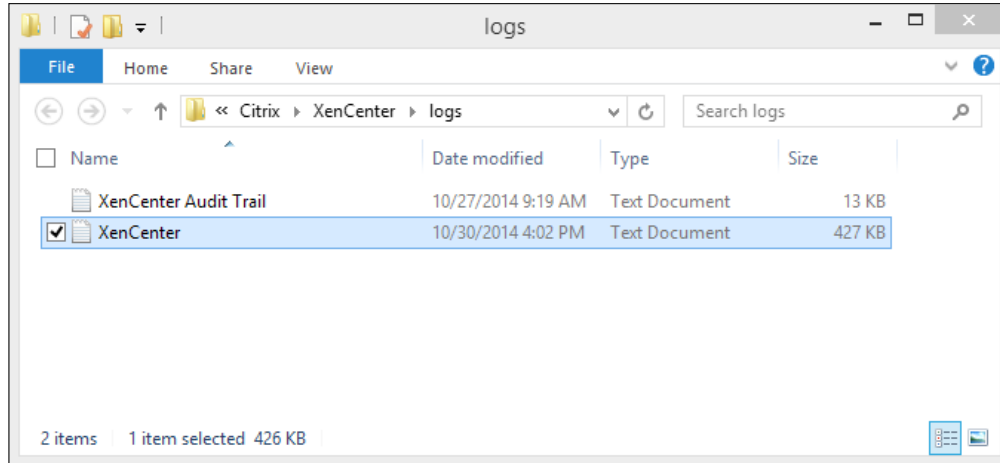
```
%userprofile%\AppData\Roaming\Citrix\XenCenter\logs\XenCenter.log
```

The following steps cover how to access the XenCenter application logfile:

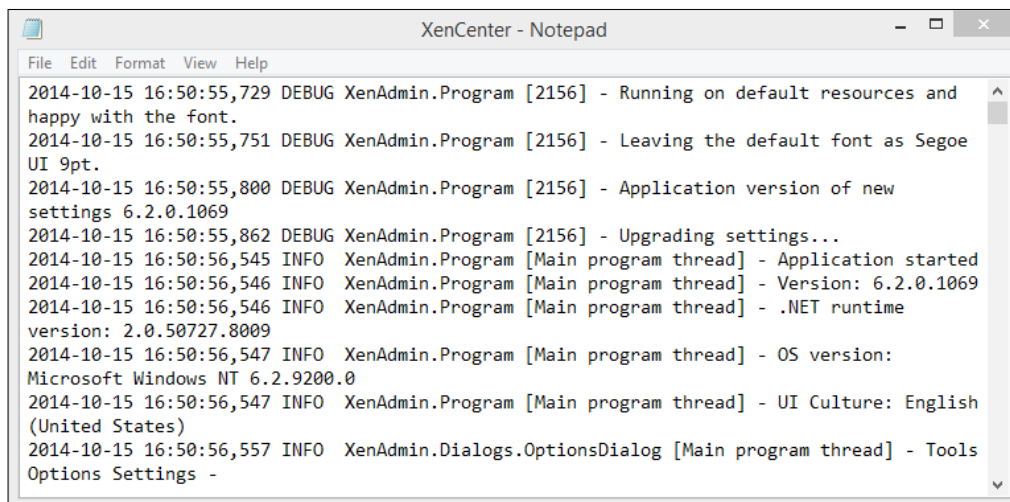
1. Select **View Application Log Files** from the **Help** menu in XenCenter to open the XenCenter logfile directory on your local system.



2. Open the **XenCenter** logfile to view the log information.



The following screenshot displays the information found in the **XenCenter** logfile:



Summary

In this chapter, we covered patching XenServer hosts to maintain system performance and security. We also examined XenServer system performance metrics that can be used to identify any performance issues that can cause problems. In addition to examining the performance metrics, we looked at configuring alerts to trigger when the performance metrics reached a defined threshold. As part of configuring the performance alerts, we went through configuring e-mail notifications so that administrators would be e-mailed when a performance alert is triggered. We took a look at the log information from both XenServer as well as XenCenter, which is used in identifying any issues and preventing problems before they become major issues.

In the next chapter, we'll take a look at extending our XenServer deployment to take advantage of automation and integration functionality in XenServer.

8

Securing XenServer®

Securing our XenServer environment is of paramount importance, given the ease with which hackers are able to expose vulnerabilities in computer systems today. With the complexity and tight integration of virtualized solutions, it is imperative that we address the major elements when securing our XenServer environment. XenServer is built on Linux, which is known for its security in comparison with other operating systems, but additional consideration should be taken when securing a XenServer deployment. Virtualization security requires considering every aspect of the deployment such as the server, networking, storage, and the VMs, as each component could potentially be compromised. The shared-resource architecture of virtualized deployments requires extra care to be given to security, as a breach could result in the compromise of multiple VMs hosted on the XenServer host.

In this chapter, you'll learn about the following topics:

- Local authentication
- Active Directory integration
- **Role-based access control (RBAC)**
- Host security
- VM security
- Storage security

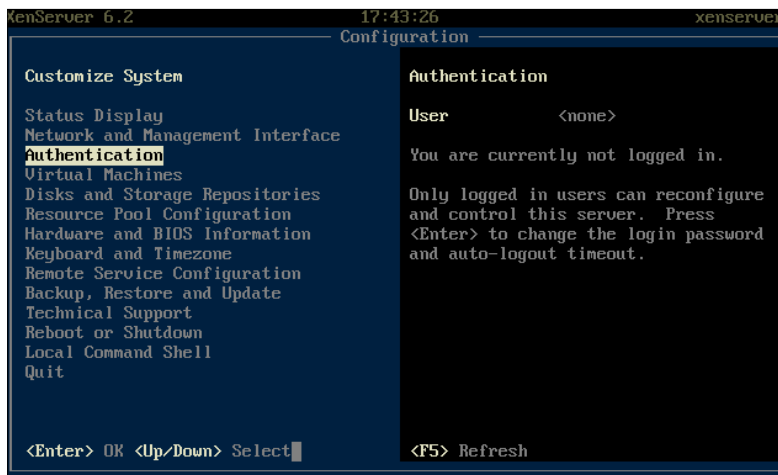
Local authentication

During the installation of XenServer, we entered a password for the root account that is used to manage our XenServer hosts. The root account is granted all the privileges on a XenServer host, by default. This account is local to the individual XenServer host and is authenticated by the host.

Changing the root password (using the GUI)

The following steps cover changing the password for the root account on a XenServer host using the graphical xsconsole utility:

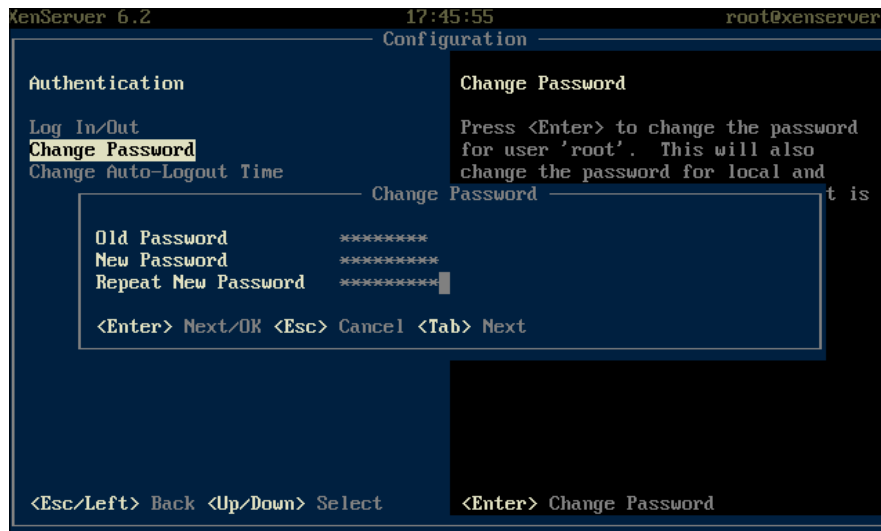
1. Enter the xsconsole command in the console under the **Console** tab on the XenServer host to launch the management console.
2. Select the **Authentication** option and press *Enter* to continue.



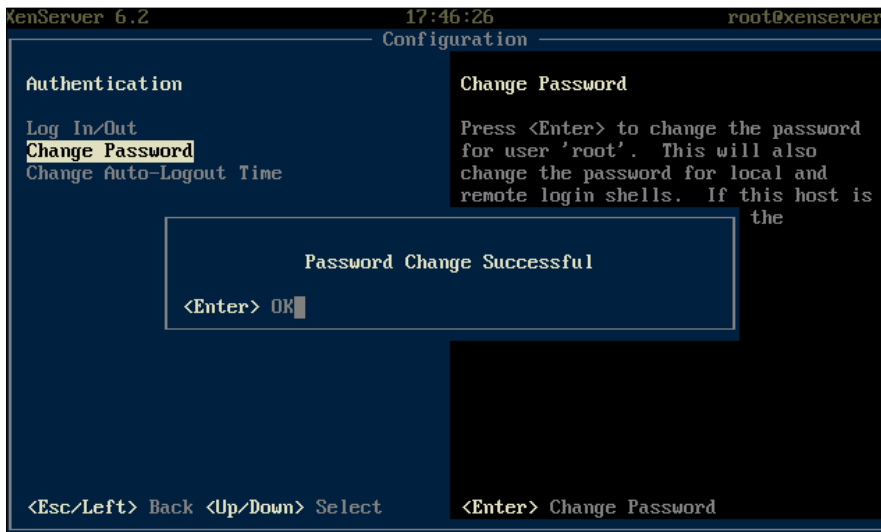
3. Select the **Change Password** option and press *Enter* to continue.



4. Enter the current password for the root account to perform the password change operation.
5. Enter the current password for the root account and then enter the new password twice in the subsequent fields. Press *Enter* to submit the password change.



6. Press *Enter* to acknowledge that the password change operation has been completed.



Changing the root password (using the CLI)

The following command can be used to change the password of the root account from the command line using the built-in `passwd` command:

```
passwd root
```

This is shown in the following screenshot:

```
[root@xenserver1 ~]# passwd root
Changing password for user root.
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
[root@xenserver1 ~]# █
```

Disabling the root SSH login

By default, XenServer uses the root account for server administration and SSH access by the root account is enabled by default. Based on security best practices, SSH access via the root account should be disabled to protect access to the system and a separate account should be used to access the system remotely. The following steps disable the root SSH login:

1. Run the following command to launch the nano text editor to modify the SSH configuration file:

```
nano /etc/ssh/sshd_config
```

The following screenshot shows you how to launch the nano text editor:

```
[root@XENSER3 ~]# nano /etc/ssh/sshd_config █
```

2. Uncomment the **PermitRootLogin** line and change the value from `yes` to `no` to disable the root access via SSH:

```

GNU nano 1.3.12      File: /etc/ssh/sshd_config      Modified
#LogLevel INFO
# Authentication:
#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6

#RSAAuthentication yes
#PubkeyAuthentication yes
#AuthorizedKeysFile      .ssh/authorized_keys

# For this to work you will also need host keys in /etc/ssh/ssh_known$
#RhostsRSAAuthentication no
# similar for protocol version 2
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# RhostsRSAAuthentication and HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

^G Get Help ^O WriteOut ^R Read File ^Y Prev Pag ^K Cut Text ^C Cur Pos
^X Exit     ^J Justify  ^W Where Is ^V Next Pag ^U UnCut Te ^T To Spell

```

3. Run the following command to restart the SSH service to apply the changes to the configuration file:

```
/etc/init.d/sshd restart
```

The following screenshot shows you how to restart the SSH service:

```

[root@XENSERVER3 ~]# /etc/init.d/sshd restart
Stopping sshd:                                     [ OK ]
Starting sshd:                                     [ OK ]
[root@XENSERVER3 ~]#

```

Active Directory integration

Citrix XenServer can be integrated with Microsoft Active Directory to provide centralized authentication in order to reduce administration overhead in environments with multiple XenServer hosts. It also provides greater security by eliminating the use of a shared root password among the administrators as well as individual named administrator logins for auditing purposes.

Active Directory integration requirements

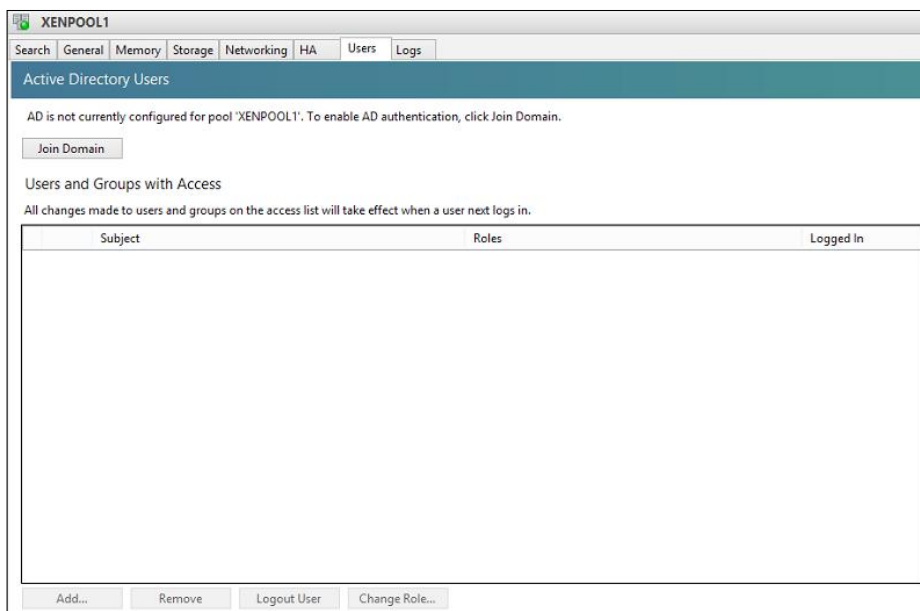
The following list covers the requirements for enabling Active Directory integration on a XenServer pool/host:

- Ensure that the XenServer host can resolve the domain name
- Domain controllers must be 2003 or later
- An Active Directory user account with rights to add computers to the domain must be used
- The time on the XenServer host must be synchronized with the domain controllers in the domain
- XenServer does not support a mixed authentication pool in which some hosts are configured for Active Directory integration and others are not

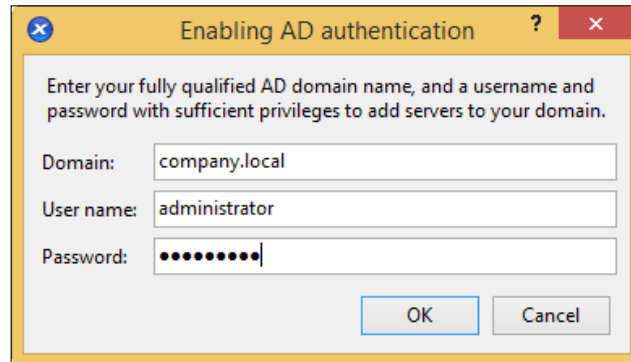
Enabling Active Directory integration (using the GUI)

The following steps cover enabling Active Directory integration on a XenServer pool/host using the XenCenter GUI:

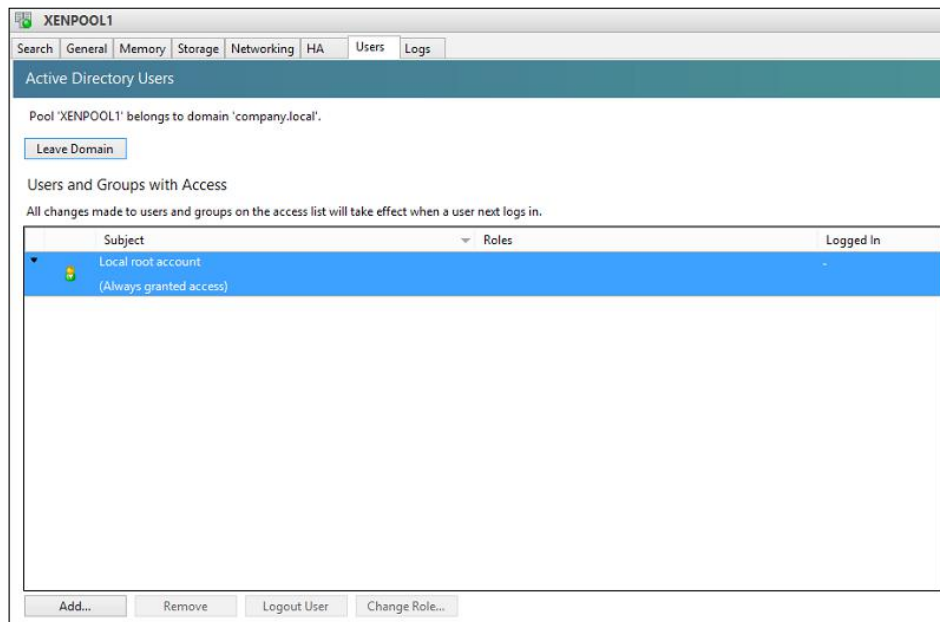
1. Click on the **Join Domain** button under the **Users** tab of the XenServer pool/host.



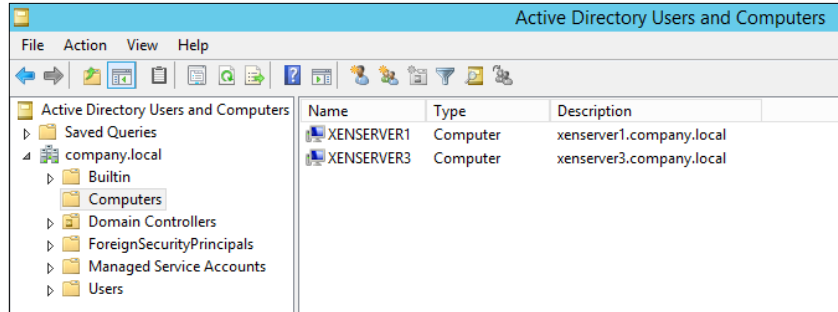
2. Enter the domain name of the Active Directory domain along with the username and password of a user with the privileges to add the computer accounts. Click on the **OK** button to enable Active Directory integration.



3. Active Directory integration can be verified by looking at the **Users** tab of the XenServer pool/host. As seen in the following screenshot, this will indicate that the respective pool belongs to the Active Directory domain that was configured in the previous section:



4. An Active Directory computer account is created for the XenServer hosts that have joined the Active Directory domain. The following screenshot displays the computer accounts created in Active Directory and they can be viewed from the **Active Directory Users and Computers** management console.



Enabling Active Directory integration (using the CLI)

The following command covers enabling Active Directory integration on a XenServer pool/host from the command line using the XE command:

```
xe pool-enable-external-auth auth-type=AD service-name=domain_name  
config:user=username config:pass=user_password
```

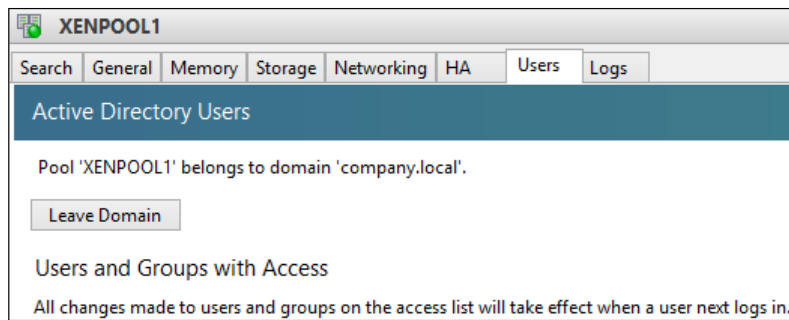
The following screenshot displays enabling Active Directory integration on the XenServer host:

```
[root@xenserver1 ~]# xe pool-enable-external-auth auth-type=AD service-name=company.local  
config:user=xenserver config:pass=password  
[root@xenserver1 ~]#
```

Disabling Active Directory integration (using the GUI)

The following steps cover disabling Active Directory integration on a XenServer pool/host from an Active Directory domain using the XenCenter GUI:

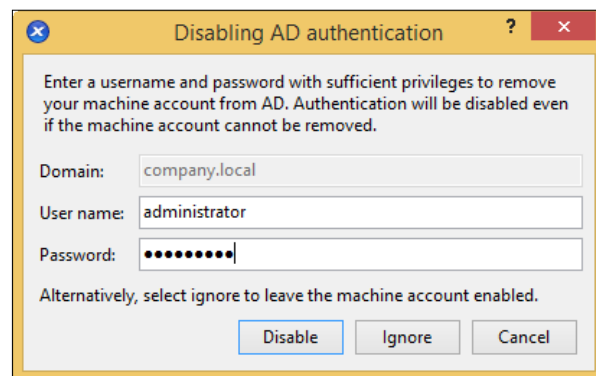
1. Click on the **Leave Domain** button under the **Users** tab of the XenServer pool/host, which is to be removed from the domain.



2. Click on the **Yes** button to confirm that the hosts in the pool will be removed from the Active Directory domain.



3. Enter the username and password of an account with Active Directory privileges to disable the computer accounts and click on the **Disable** button to disable the computer accounts for the XenServer hosts. If disabling of the computer accounts is not required, simply click on the **Ignore** button to continue without disabling the computer accounts.



Disabling Active Directory integration (using the CLI)

The following command disables Active Directory integration on a XenServer pool/host from the command line using the XE command:

```
xe pool-disable-external-auth
```

The following screenshot shows you how to disable the Active Directory integration on the XenServer host:

```
[root@xenserver1 ~]# xe pool-disable-external-auth
[root@xenserver1 ~]# █
```

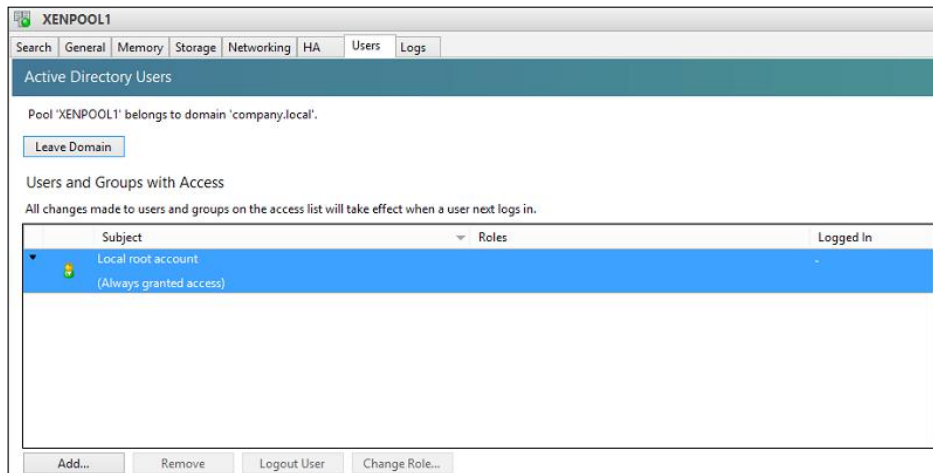
Managing Active Directory accounts

The following sections cover managing the user/group accounts on the XenServer pool/hosts.

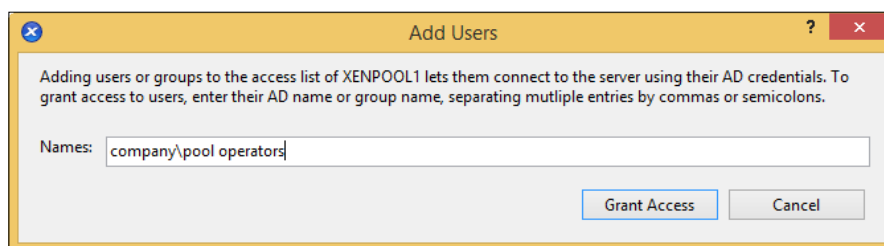
Adding Active Directory users/groups (using the GUI)

The following steps cover adding a new user or group from the Active Directory domain to the XenServer pool/server using the XenCenter GUI:

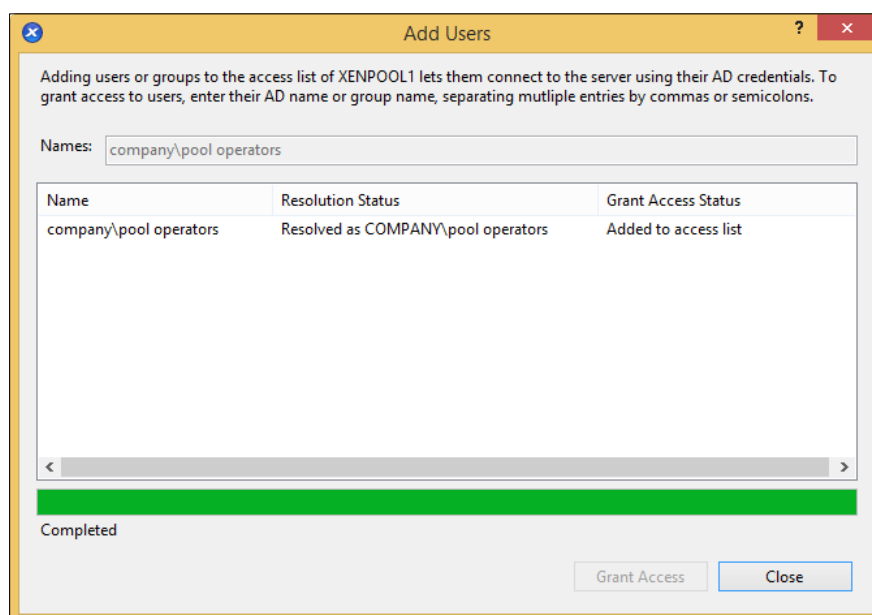
1. Click on the **Add ...** button under the **Users** tab of the desired XenServer pool/host.



- Enter the name of the user or group to be added to the XenServer pool/host. Click on the **Grant Access** button to add the user.



- Click on the **Close** button after the user has been added to close the **Add Users** dialog box.




Adding Active Directory users/groups (using the CLI)

The following steps cover adding a new user or group from the Active Directory domain to the XenServer pool using the XE command from the command line:

```
xe subject-add subject-name=domain\username
```

The following screenshot shows you the addition of an Active Directory group called `pool operators` to the XenServer host:

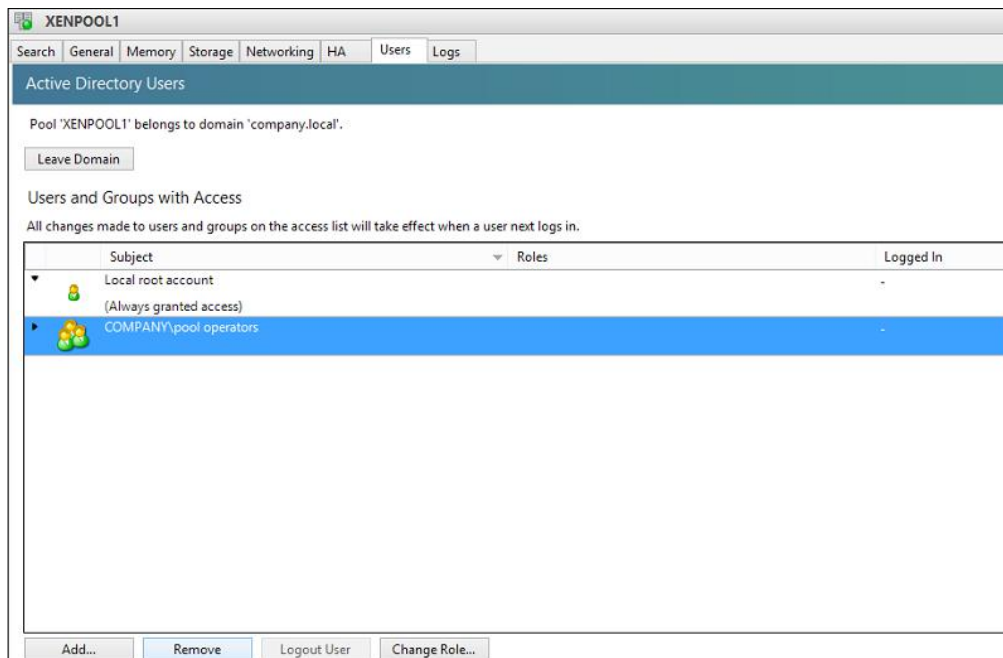
```
[root@xenserver1 ~]# xe subject-add subject-name="company\pool operators"
9b05384c-31b6-2fd3-a7c4-c7cf374cb19b
[root@xenserver1 ~]# █
```

 If there is a space in the username or group name, then the domain name and the account name should be enclosed in double quotation marks.

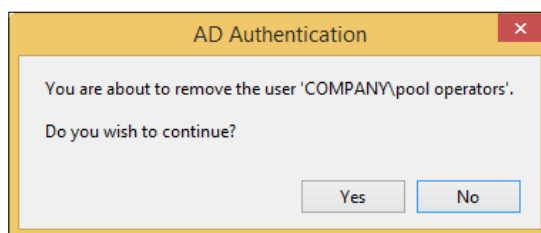
Removing Active Directory users/groups (using the GUI)

The following steps cover removing a user or group in the Active Directory domain from the XenServer pool/host using the XenCenter GUI.

1. Select the user or group from the **Users** tab on the XenServer host/pool and click on the **Remove** button under the **Users and Groups with Access** section.



- Click on **Yes** to confirm that the user/group should be removed from the XenServer pool/host.



Removing Active Directory users/groups (using the CLI)

The following steps cover removing a user or group in the Active Directory domain from the XenServer pool/host from the command line using the XE command:

- The following command is used to list the subjects present on the XenServer pool/host, which we'll use to determine the UUID or unique identifier of the actual subject/object that we'll use with the remove operation:

```
xe subject-list
```

The following screenshot shows you the subjects on the XenServer host/pool:

```
[root@xenserver1 ~]# xe subject-list
uuid ( RO)                : d3ed4122-41fd-49bb-ee50-fd4de1eae673
subject-identifier ( RO)  : S-1-5-21-1660949473-1421435605-34430364-1108
other-config (MRO): subject-name: COMPANY\pool operators; subject-gid: 1098384468; subject-sid: S-1-5-21-1660949473-1421435605-34430364-1108; subject-is-group: true
roles (SRO):
```

- The following command removes the subject object from the XenServer host/pool:

```
xe subject-remove subject-uuid=domain\username
```

The following screenshot shows you how to remove the user account from the XenServer host/pool:

```
[root@xenserver1 ~]# xe subject-remove subject-uuid=d3ed4122-41fd-49bb-ee50-fd4de1eae673
[root@xenserver1 ~]#
```


RBAC

Citrix XenServer supports RBAC, which allows administrators to segregate the administrative duties among several administrators, which allows compliance with a least privilege administrative security model. RBAC requires that the pool/host is Active Directory integrated in order to support adding additional accounts to the XenServer pool/host. XenServer offers six defined roles, each with a specific set of permissions to administer the host.

Roles

The following list covers the six roles that can be added to user or group accounts in order to manage the XenServer environment:

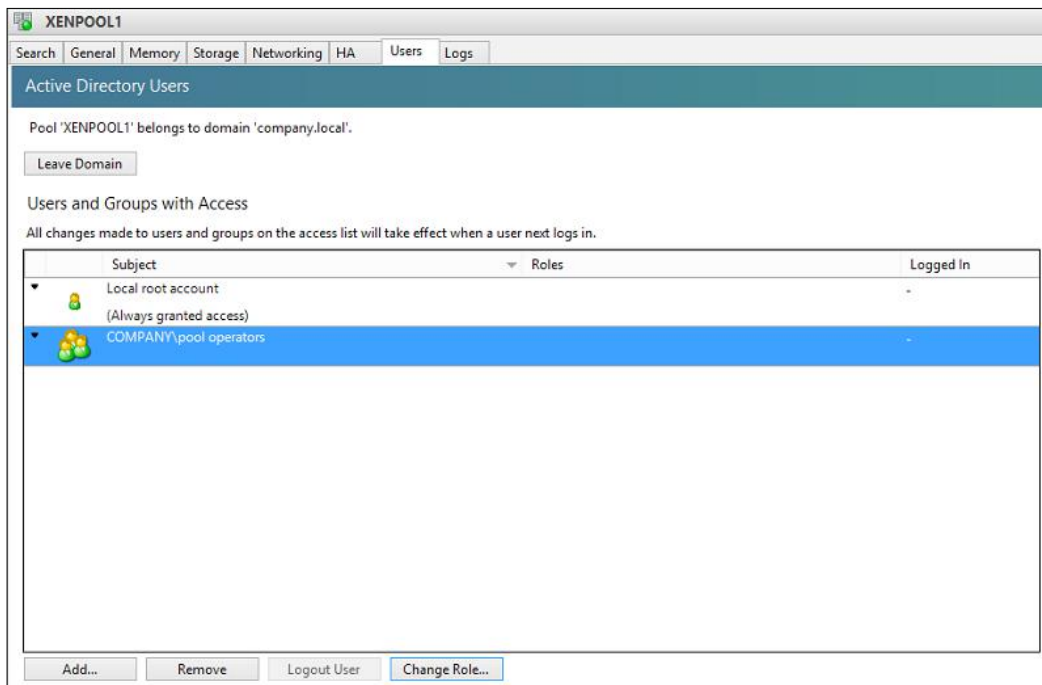
- **Pool Admin:** The Pool Admin account provides unrestricted access to the XenServer pool/host
- **Pool Operator:** The Pool Operator role provides unrestricted access to manage the XenServer pool/host with the exception of user management
- **VM Power Admin:** The VM Power Admin role provides the ability to manage the life cycle of a VM from creation to deletion and everything in between
- **VM Admin:** The VM Admin role provides the ability to manage VMs with the exception of migrating them and taking snapshots
- **VM Operator:** The VM Operator role provides the ability to perform power management operations on a VM such as power on and off
- **Read Only:** The Read Only role provides the ability to view the environment, but doesn't allow any changes to be made

 XenServer only supports the six predefined roles and additional administrator defined roles cannot be created.

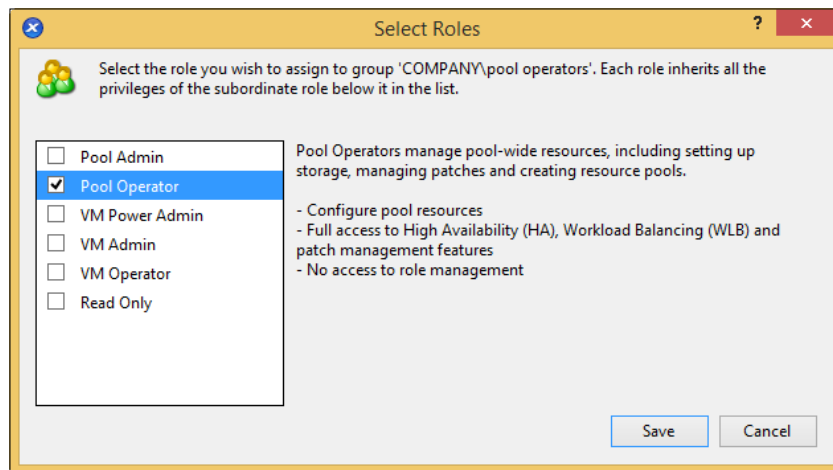
Managing user roles (using the GUI)

The following steps cover modifying an Active Directory user's or a group's XenServer role using the XenCenter GUI:

1. Click on the **Change Role...** button under the **Users** tab of the XenServer pool/host to launch the **Select Roles** dialog box.



2. Select the checkbox next to the desired role(s) for the user or group and click on the **Save** button to grant the permissions.



- The following screenshot displays the XenServer roles that a user has been assigned. This view can be found under the **Users** tab of the XenServer host/pool.

Subject	Roles	Logged In
Local root account (Always granted access)		-
COMPANY\pool operators	Pool Operator	-

Managing user roles (using the CLI)

The following commands cover modifying an Active Directory user or group's XenServer role from the command line using the XE command:

The following command adds a specified role to a user or a group:

```
xe subject-role-add uuid=user_uuid role-name="role_name"
```

The following screenshot shows you the addition of the user account to the pool operator role:

```
[root@xenserver1 ~]# xe subject-role-add uuid=28bb8893-4f69-8ee4-72e8-5502c514a411
role-name=pool-operator
[root@xenserver1 ~]#
```

The following command removes a specified role from a user or group:

```
xe subject-role-remove uuid=user_uuid role-name="role_name"
```

The following screenshot shows the removal of the user account from the pool operator role:

```
[root@xenserver1 ~]# xe subject-role-remove uuid=28bb8893-4f69-8ee4-72e8-5502c514a411
role-name=pool-operator
[root@xenserver1 ~]#
```

Audit logging

An integral component of any security plan is to constantly monitor any activities within the environment. Specifically, logging the actions taken by administrators of the environment ensures that any changes that are made to the configuration of the XenServer are tracked and can be audited at a later point in time. XenServer audit logs can only be exported using the command line.

Configuring audit logging (using the CLI)

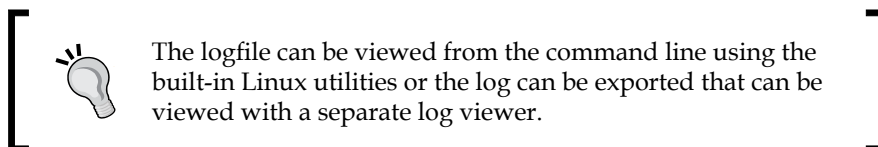
The following command can be used to export the audit log of the XenServer pool/host:

```
xe audit-log-get since=<timestamp> filename=<output filename>
```

The following screenshot shows you how to export an audit log:

```
[root@xenserver1 ~]# xe audit-log-get filename=auditlog.log
audit-log-get into file auditlog.log succeeded
[root@xenserver1 ~]#
```

The `since` parameter allows you to export only the events that have taken place since a particular point in time.



Host security

There are a number of basic steps that can be taken in order to reduce the security exposure of our XenServer hosts. XenServer is built on Linux and our primary concern is to secure the XenServer control domain in order to prevent a malicious or unauthorized user from accessing the management components of the XenServer. If the control domain is compromised, the malicious user will be able to gain access to the management functionality of XenServer and can cause severe damage to the environment. The following list touches on a number of simple guidelines that can be helpful in securing our XenServer environment:

- Avoid installing additional software unless necessary
- Ensure that any additional services that were started are stopped when they no longer needed
- Limit the machines that have SSH access to the system
- Limit the user accounts with SSH access to the system
- Disable root SSH login access to the system
- Change the root password every 90 days or in compliance with the password policy for the overall environment

- Ensure that the root password is a strong password including lowercase letters, capital letters, numbers, and special characters
- The management interface should be placed onto a separate and secure management network in order to prevent unauthorized access to the system

XenServer® host firewall

XenServer utilizes the `iptables` firewall that is built into the Linux operating system to manage what network traffic is allowed in and out of the XenServer host. The firewall should remain unmodified unless there is a specific reason to modify it; and if a modification is required, it should be limited to just the traffic that needs to be allowed to pass. Limiting the number of open ports on the firewall is best practice for security, as it reduces the possible attack surface.

The following command can be used to view the current settings of the `iptables` firewall on a XenServer host from the command line:

```
iptables -nL
```

The following screenshot displays the firewall rules on the server:

```
[root@xenserver1 ~]# iptables -nL
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
ACCEPT    47  --  0.0.0.0/0             0.0.0.0/0
RH-Firewall-1-INPUT  all  --  0.0.0.0/0             0.0.0.0/0

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination
RH-Firewall-1-INPUT  all  --  0.0.0.0/0             0.0.0.0/0

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination

Chain L (0 references)
target     prot opt source                destination

Chain RH-Firewall-1-INPUT (2 references)
target     prot opt source                destination
ACCEPT    all  --  0.0.0.0/0             0.0.0.0/0
ACCEPT    icmp --  0.0.0.0/0             0.0.0.0/0             icmp type 255
ACCEPT    esp  --  0.0.0.0/0             0.0.0.0/0
ACCEPT    ah   --  0.0.0.0/0             0.0.0.0/0
ACCEPT    udp  --  0.0.0.0/0             224.0.0.251           udp dpt:5353
ACCEPT    udp  --  0.0.0.0/0             0.0.0.0/0             udp dpt:631
ACCEPT    tcp  --  0.0.0.0/0             0.0.0.0/0             tcp dpt:631
ACCEPT    udp  --  0.0.0.0/0             0.0.0.0/0             udp dpt:67
ACCEPT    all  --  0.0.0.0/0             0.0.0.0/0             state RELATED,ESTABLISHED
ACCEPT    udp  --  0.0.0.0/0             0.0.0.0/0             state NEW udp dpt:694
ACCEPT    tcp  --  0.0.0.0/0             0.0.0.0/0             state NEW tcp dpt:22
ACCEPT    tcp  --  0.0.0.0/0             0.0.0.0/0             state NEW tcp dpt:80
ACCEPT    tcp  --  0.0.0.0/0             0.0.0.0/0             state NEW tcp dpt:443
ACCEPT    udp  --  192.168.1.180         0.0.0.0/0             state NEW udp dpt:161
REJECT    all  --  0.0.0.0/0             0.0.0.0/0             reject-with icmp-host-prohibited
[root@xenserver1 ~]#
```

VM security

The virtual machines running on the XenServer host are critically important to the overall security of any virtualized environment. There are a number of technical solutions to protect the servers and desktops in a physical environment that might not work as well in a virtualized environment. Antivirus is a key component that translates differently into a virtualized environment and can have a more severe impact on things such as system performance, which are as follows:

- **Agent-based:** Antivirus commonly deployed to physical machines is agent-based. This means that a software client is deployed to the machine, which is typically managed by a server that controls the policies and software components. The client typically performs on-demand as well as scheduled scans in order to ensure that the machine is free of viruses. The scanning process creates I/O on the hard disk as it goes through while checking every file for potential viruses. While this process might slow down the system slightly, it usually doesn't create serious problems. When this solution is moved to a virtualized environment, the I/O that is created by each virtual machine can collectively bring the environment to a standstill, considering that many of the VMs will be in contention for the same storage I/O, unlike on separate physical servers.
- **Virtualization-optimized:** Antivirus solutions that have been optimized for virtualization generally eliminate the storage I/O impact on the environment by offloading the actual virus scanning process to a dedicated pool of virus scanner servers. This ensures that the virtual machines are protected by an agent-based antivirus but this avoids creating excessive storage I/O that can reduce the performance of the XenServer environment.

Storage security

Several technical solutions can be implemented to protect the storage that is used by the XenServer pools or hosts in our environment:

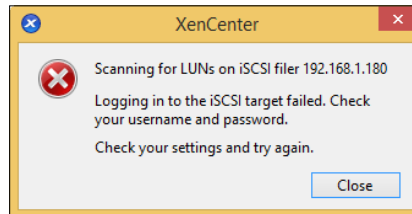
- iSCSI traffic can and should be placed onto a separate VLAN for security reasons and performance reasons as well. If possible, a separate networking infrastructure can be used to further isolate the iSCSI traffic.
- iSCSI traffic can be encrypted using IPsec in order to avoid any data being deciphered if captured.
- Zoning should be used in Fibre Channel implementations to not only protect data integrity, but to limit the data access.

- NFS shares should be restricted to only the hosts that require access to the share.
- **iSCSI Challenge-Handshake Authentication Protocol (CHAP)** can be used to provide a form of authentication in order to ensure that only the hosts that are supposed to can access the data.

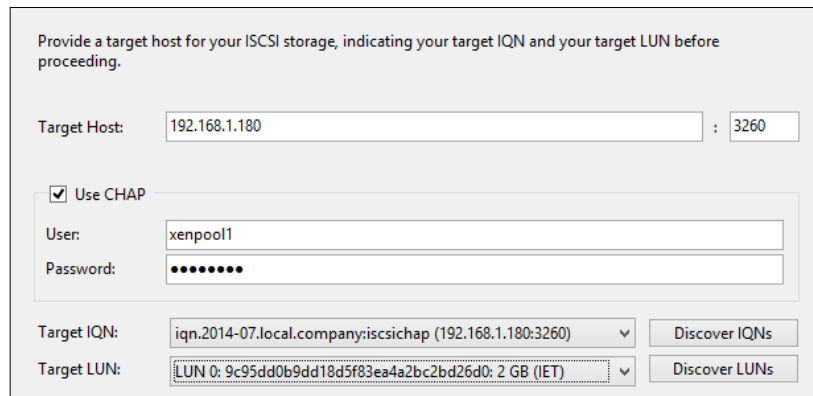
iSCSI CHAP

iSCSI CHAP provides a mechanism for the XenServer host to be authenticated against the storage target or specific storage LUN. This helps increase security by avoiding the possibility of a host accessing storage that it shouldn't have access to. iSCSI CHAP uses a username and password that is configured on the storage target or on both the initiator and target in the case of mutual authentication. XenServer supports one-way authentication in which the storage target authenticates the host.

The following screenshot displays the error message that is presented when a host attempts to access an iSCSI target without the correct credentials:



The following screenshot displays configuring a SR to use CHAP authentication with a username and password, which is defined on the storage target:



Summary

In this chapter, we have covered integrating XenServer with Microsoft Active Directory to provide centralized authentication in order to improve security through the use of named accounts for system administration. We also learned about RBAC and how we can assign users or groups to specific roles to segregate the administration tasks. We went through examples of how to add and remove Active Directory users and groups to the XenServer pool and assigning these accounts to XenServer roles as well. We also looked at several aspects of securing the XenServer host along with VM and storage security to protect the environment from potential threats. Now that we've taken a look at securing our XenServer deployment, we will look at extending our XenServer deployment in order to integrate it with other products in the next chapter.

9

Extending XenServer®

In the previous chapters, we looked at the aspects of managing our Citrix XenServer hosts and how to take advantage of the features that are available within XenServer. A major area for any virtualization solution is how well it is able to integrate with third-party products in order to enhance the capabilities of the overall solution. Citrix XenServer offers a robust ecosystem for integration with third-party products based upon its open source Xen hypervisor roots as well as its tight integration with Citrix's other products such as XenDesktop and CloudPlatform.

In this chapter, we'll cover the following topics:

- Command-line management
- Windows PowerShell integration
- XenServer SDKs
- Apache CloudStack integration
- VMware to Citrix XenServer conversions

Command-line management

Citrix XenServer provides a command-line interface for managing hosts in the XenServer environment without the need for a graphical interface. The command line also provides an excellent mechanism for automating XenServer management and configuration tasks. The following command lines are available:

- **The host command line:** The command line on a host can be accessed from either the **Console** tab of the XenServer host in Citrix XenCenter or from the physical console of the server
- **The SSH command line:** The command line can be accessed remotely via SSH as SSH is enabled, by default, on Citrix XenServer host

- **The XE command:** The XE command can be run from the command line of any machine that has Citrix XenCenter installed on it as well as the XenServer host itself

The following directories contain the XE command that is installed along with Citrix XenCenter:

- **32 bit:** C:\Program Files\Citrix\XenCenter
- **64 bit:** C:\Program Files (x86)\Citrix\XenCenter

 The working directory of the command prompt needs to be changed to one of the directories mentioned in order to properly execute the `xe` command.

The following command displays how to use the `xe` command on a remote host to perform administration tasks:

```
xe -s Server_Name -u admin_user -pw admin_password vm-list
```

The following screenshot shows how to list the VMs on a XenServer host using the `xe` command:

```
c:\Program Files (x86)\Citrix\XenCenter>xe -s 192.168.1.246 -u root -pw password
vm-list
uuid ( R0)           : bdd989d3-e5a6-4237-924d-a55185cb491d
  name-label ( RW): Control domain on host: xenserver1
  power-state ( R0): running

c:\Program Files (x86)\Citrix\XenCenter>_
```

The `xe help` command is a very useful command that can be used to view information on any of the available commands.

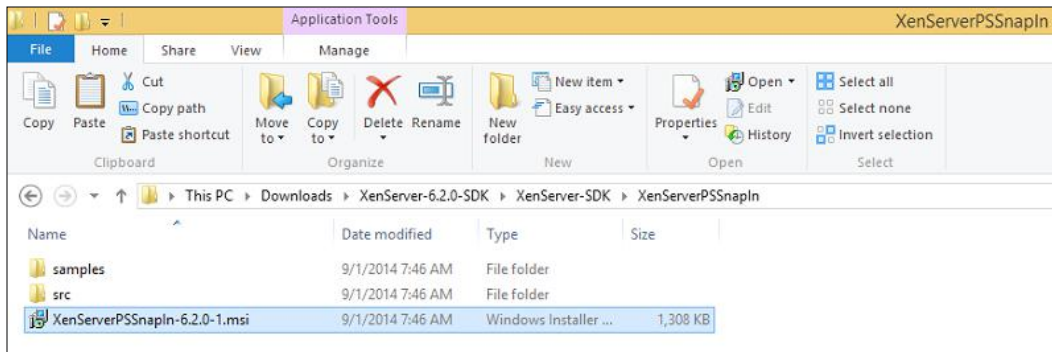
PowerShell integration

Windows PowerShell has become an essential tool for many Windows administrators, as more and more operations across Windows platforms can only be performed utilizing Windows PowerShell. Windows PowerShell provides a robust set of features that can be used to reduce the overall administration effort. An extensive collection of XenServer PowerShell cmdlets are available through the installation of the XenServer PowerShell Snap-in for the Windows platform. A number of example scripts can be found at the Citrix website (<http://blogs.citrix.com/2014/09/10/scripting-automating-vm-operations-on-xenserver-using-powershell/>).

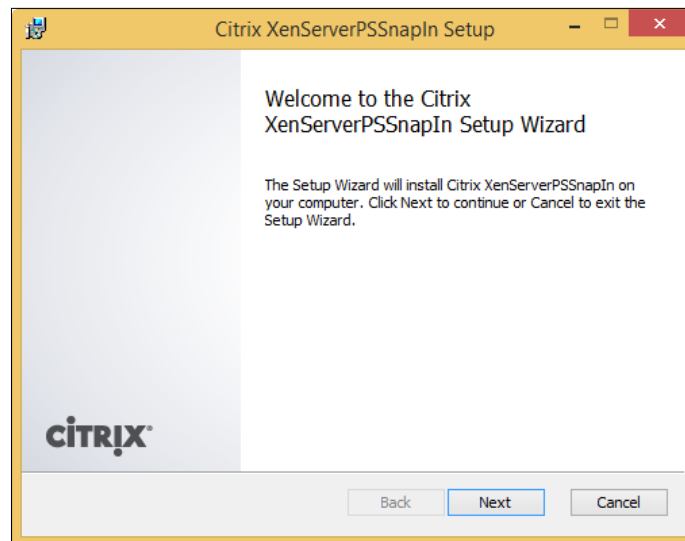
Installing XenServer® PowerShell Snap-in

The following steps cover installing the XenServer PowerShell Snap-in:

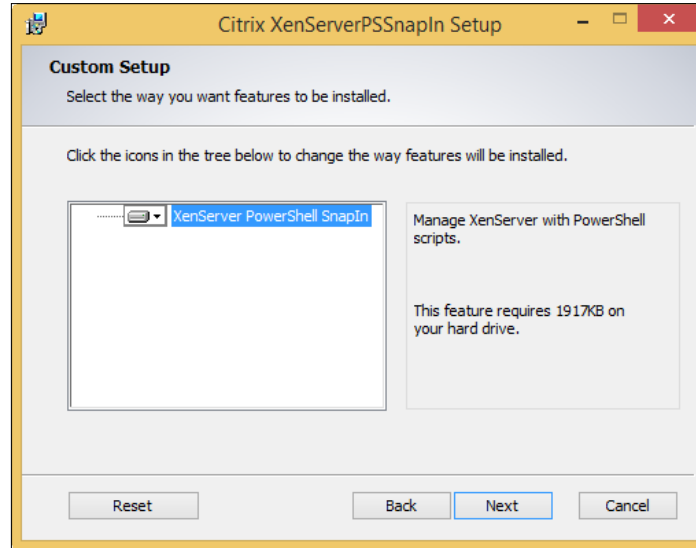
1. Download the XenServer 6.2 **Software Development Kit (SDK)** from <http://xenserver.org/open-source-virtualization-download.html>.
2. Unzip the SDK zip file and double-click on the XenServerPSSnapIn-6.2.0-1.msi MSI file to start the XenServer PowerShell Snap-in installation:



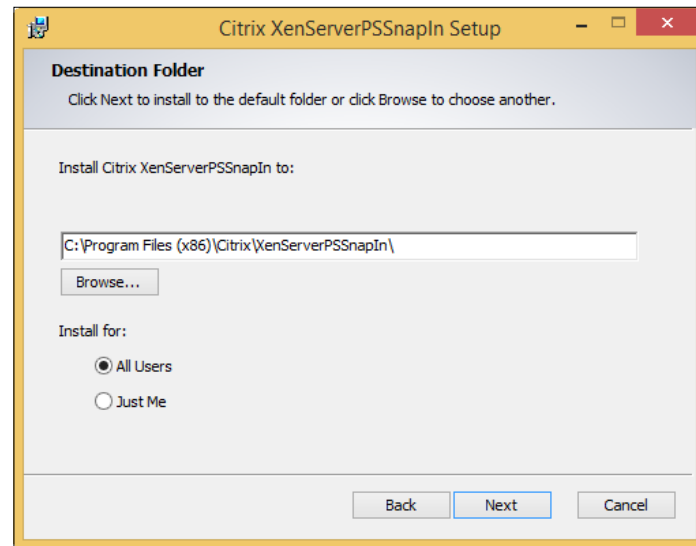
3. Click on **Next** to begin the XenServer PowerShell Snap-in installer:



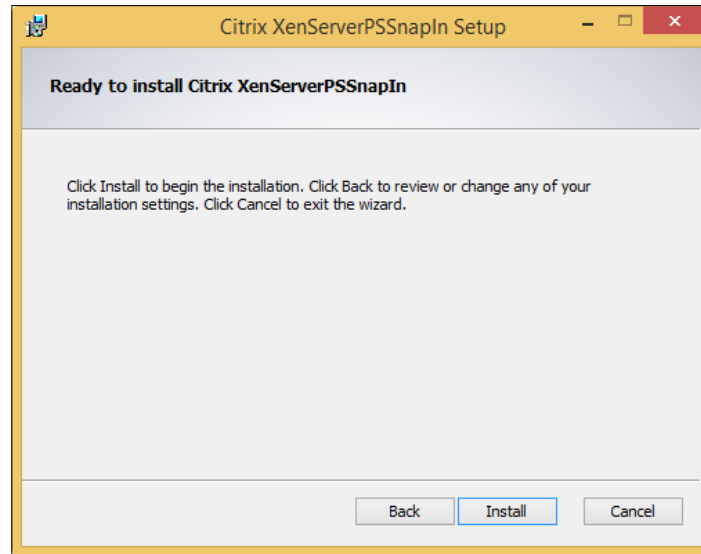
4. Click on **Next** to accept the installed features and proceed:



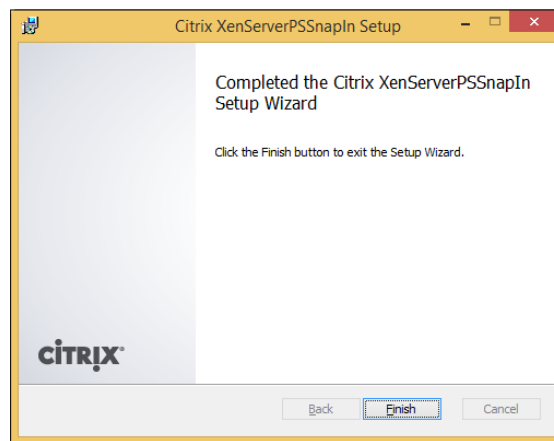
5. Select the installation location on the local system and check whether the installation will be available to all the users on the system or just the current user. Click on **Next** to proceed:



- Click on **Install** to begin the installation process:



- Click on **Finish** to complete the installation:



The following command covers connecting to a XenServer host using the XenServer PowerShell Snap-in:

```
Connect-XenServer -Server Server_Name -username user -password password
```

The following screenshot displays how to connect to a XenServer host using the Citrix XenServer PowerShell Snap-in:

```
PS C:\Program Files (x86)\Citrix\XenServerPSSnapIn> Connect-XenServer -Server 192.168.1.246 -username root -password pas
sword
New Security Certificate
The certificate fingerprint of the server you have connected to is :
35:A2:CD:33:D6:07:6C:F9:77:DE:AC:2B:37:D4:60:D6:C4:20:07:9A
The certificate on this server is not trusted.
Do you wish to continue?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): y
PS C:\Program Files (x86)\Citrix\XenServerPSSnapIn>
```

The following command can be used to list all of the available XenServer PowerShell commands:

```
get-command -module xenserverpssnapin
```

The following screenshot displays how to view all of the XenServer PowerShell commands:

```
PS C:\Program Files (x86)\Citrix\XenServerPSSnapIn> get-command -module xenserverpssnapin
CommandType      Name                                     ModuleName
-----
Cmdlet           Add-XenBond                            XenServerPSSnapIn
Cmdlet           Add-XenConsole                         XenServerPSSnapIn
Cmdlet           Add-XenCrashdump                       XenServerPSSnapIn
Cmdlet           Add-XenGPUGroup                        XenServerPSSnapIn
Cmdlet           Add-XenHost                            XenServerPSSnapIn
Cmdlet           Add-XenHostCpu                         XenServerPSSnapIn
Cmdlet           Add-XenHostCrashdump                  XenServerPSSnapIn
Cmdlet           Add-XenHostMetrics                    XenServerPSSnapIn
Cmdlet           Add-XenHostPatch                      XenServerPSSnapIn
Cmdlet           Add-XenNetwork                        XenServerPSSnapIn
Cmdlet           Add-XenPBD                             XenServerPSSnapIn
Cmdlet           Add-XenPCI                             XenServerPSSnapIn
Cmdlet           Add-XenPGPU                            XenServerPSSnapIn
Cmdlet           Add-XenPIF                             XenServerPSSnapIn
Cmdlet           Add-XenPIFMetrics                     XenServerPSSnapIn
Cmdlet           Add-XenPool                            XenServerPSSnapIn
Cmdlet           Add-XenPoolPatch                      XenServerPSSnapIn
Cmdlet           Add-XenSecret                          XenServerPSSnapIn
Cmdlet           Add-XenSM                              XenServerPSSnapIn
Cmdlet           Add-XenSR                              XenServerPSSnapIn
Cmdlet           Add-XenSubject                         XenServerPSSnapIn
Cmdlet           Add-XenTask                            XenServerPSSnapIn
Cmdlet           Add-XenTunnel                          XenServerPSSnapIn
Cmdlet           Add-XenUser                            XenServerPSSnapIn
Cmdlet           Add-XenVBD                             XenServerPSSnapIn
Cmdlet           Add-XenVBDMetrics                     XenServerPSSnapIn
Cmdlet           Add-XenVDI                             XenServerPSSnapIn
Cmdlet           Add-XenVGPU                            XenServerPSSnapIn
Cmdlet           Add-XenVIF                             XenServerPSSnapIn
Cmdlet           Add-XenVIFMetrics                     XenServerPSSnapIn
Cmdlet           Add-XenVLAN                            XenServerPSSnapIn
Cmdlet           Add-XenVM                              XenServerPSSnapIn
Cmdlet           Add-XenVMGuestMetrics                 XenServerPSSnapIn
Cmdlet           Add-XenVMetrics                       XenServerPSSnapIn
Cmdlet           Add-XenVMPP                            XenServerPSSnapIn
Cmdlet           Connect-XenServer                      XenServerPSSnapIn
Cmdlet           ConvertTo-XenRef                       XenServerPSSnapIn
Cmdlet           Disconnect-XenServer                  XenServerPSSnapIn
Cmdlet           Get-XenAuth                            XenServerPSSnapIn
```

XenServer® SDKs

SDKs provide developers a way to develop applications that integrate with XenServer and provide additional functionality. Citrix provides several language bindings for accessing the API presented by XenServer. C, C#, Java, Python, and PowerShell are the language bindings currently available for interacting with XenServer. The SDKs can be downloaded from <http://downloadns.citrix.com.edgesuite.net/akdlm/7289/XenServer-6.2.0-SDK.zip>.

CloudStack integration

Apache CloudStack (<http://cloudstack.apache.org/>) is an open source **Infrastructure as a Service (IaaS)** platform that allows organizations to create public or private clouds. CloudStack provides a highly available and scalable public/private cloud solution that allows administrators to provision virtual machines similar to public cloud offerings such as Amazon EC2, IBM Cloud, and Windows Azure. Apache CloudStack supports various hypervisors from VMware ESXi to KVM and of course, it also supports Citrix XenServer. The CloudStack project was donated by Citrix to the Apache Software Foundation.

System requirements

The following are the system requirements:

- The processor must support HVM
- The hypervisor must be fully patched
- All hosts in the cluster must have the same processors
- 4 GB of memory
- A minimum 1 NIC
- Statically assigned IP address
- No running virtual machines during the CloudStack deployment
- The username and password on all the XenServer hosts must match those configured in CloudStack
- The time across all hosts in the cluster must be synchronized

Changing the dom0 memory settings

The following steps cover changing the memory settings for the dom0 virtual machine. CloudStack best practices stipulate that the memory for the XenServer dom0 virtual machine should be changed from the default 752 megabytes to 2940 megabytes.

1. Connect to the XenServer host via SSH, XenServer console, or the local physical console.
2. Run the following command to change the dom0 memory settings:

```
/opt/xensource/libexec/xen-cmdline --set-xen  
dom0_mem=2940M,max:2940M
```

The following screenshot shows you how to change the dom0 memory settings on a XenServer host:

```
[root@XENSERVER2 ~]# /opt/xensource/libexec/xen-cmdline --set-xen dom0_mem=2940M,max:2940M  
[root@XENSERVER2 ~]# █
```

3. Reboot the XenServer host.

The following command can be used to verify that the change was made successfully:

```
free
```

The following screenshot shows you the modified memory settings for dom0 on the XenServer host:

```
[root@XENSERVER2 ~]# free  
              total        used        free      shared    buffers     cached  
Mem:           3002760       364560      2638200           0         5720      136764  
-/+ buffers/cache:      222076      2780684  
Swap:          524280           0         524280  
[root@XENSERVER2 ~]# █
```

Configuring the CloudStack XenServer® Support Package

In order to enable security groups, elastic load balancing, and elastic IP on XenServer, the **CloudStack XenServer Support Package (CSP)** must be configured. The CSP is preinstalled on Citrix XenServer 6.1 and later.

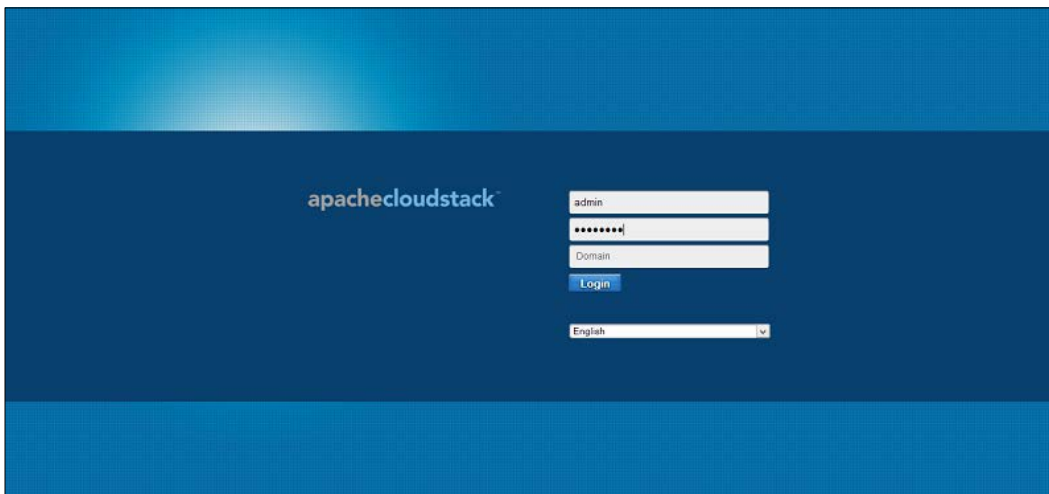
Perform the following steps to configure the CSP:

1. Run the `xe-switch-network-backend` command to change the network backend from OVS to bridge:
`xe-switch-network-backend bridge`
2. Modify the `/etc/sysctl.conf` configuration file with the following settings:
`net.bridge.bridge-nf-call-iptables = 1`
`net.bridge.bridge-nf-call-ip6tables = 0`
`net.bridge.bridge-nf-call-arptables = 1`
3. Run the `sysctl` command to commit the settings:
`sysctl -p /etc/sysctl.conf`

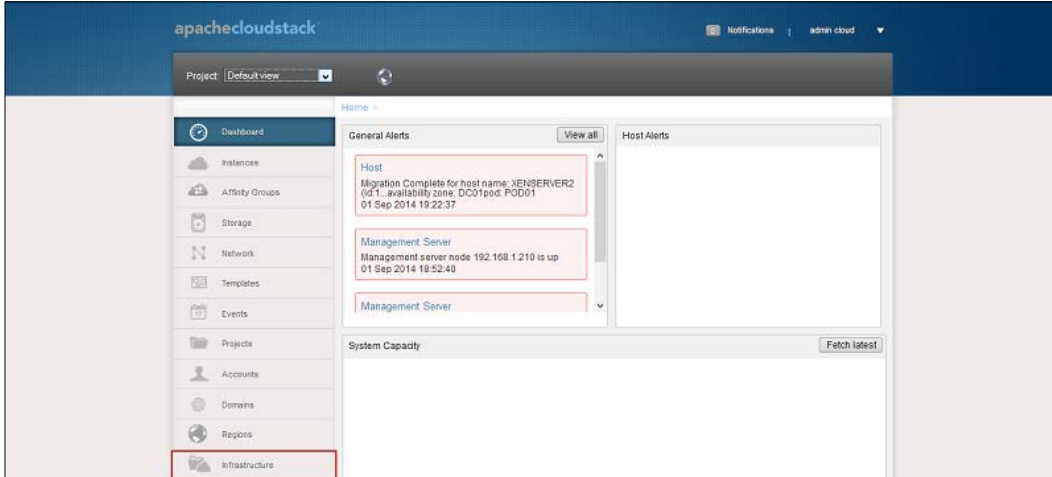
Adding a host

The following steps cover adding a XenServer host to a CloudStack deployment:

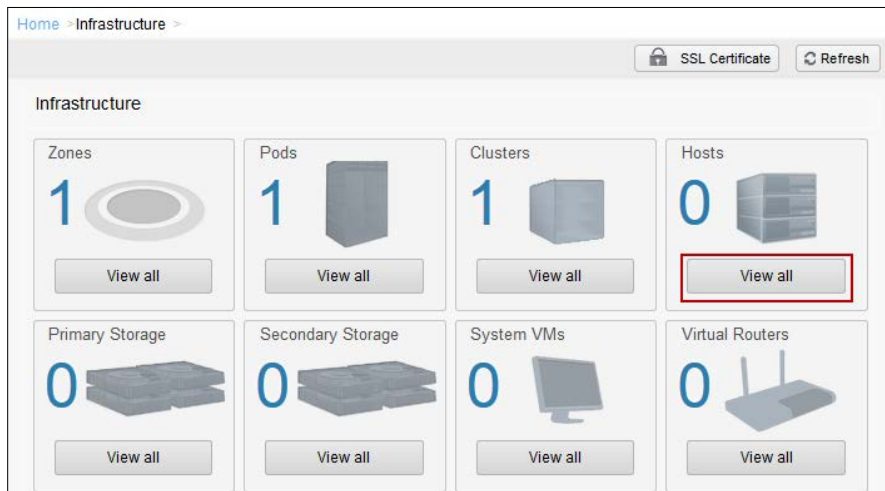
1. Log in to the CloudStack web interface:



2. Select **Infrastructure** from the menu:



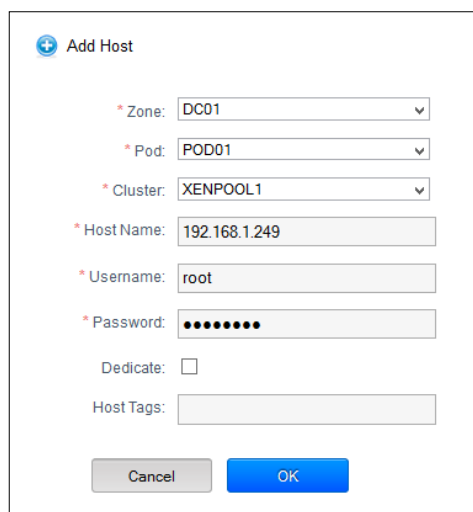
3. Select **View all** from the **Hosts** section:



4. Click on the **Add Host** button:



5. Select the appropriate zone, pod, and cluster for the host being added. Enter the hostname or IP address along with the user credentials for the XenServer into the fields provided and click on **OK** to add the host:



The screenshot shows a dialog box titled "Add Host" with a plus icon in a blue circle. It contains the following fields and controls:

- * Zone: DC01 (dropdown menu)
- * Pod: POD01 (dropdown menu)
- * Cluster: XENPOOL1 (dropdown menu)
- * Host Name: 192.168.1.249 (text input)
- * Username: root (text input)
- * Password: [masked with dots] (password input)
- Dedicate: (checkbox)
- Host Tags: (empty text input)
- Buttons: Cancel (grey), OK (blue)

The XenServer® Conversion Manager

The XenServer Conversion Manager utility provides a mechanism to convert VMware ESXi virtual machines and allows them to be imported into Citrix XenServer. This allows the hardware to be converted to Citrix XenServer without a lot of hassle or the need for an expensive third-party product to handle the **virtual to virtual (V2V)** conversion process. The XenServer Conversion Manager is composed of two components: the XenServer Conversion Manager console and the XenServer Conversion Manager virtual appliance. Both the components are covered in this section and can be downloaded from <http://www.citrix.com/downloads/xenserver/tools/conversion.html#ctx-dl-eula>.

- **The XenServer Conversion Manager console:** The XenServer Conversion Manager console is a Windows-based application that provides a graphical interface for managing the virtual machine conversions.
- **The XenServer Conversion Manager virtual appliance:** The XenServer Conversion Manager virtual appliance is a virtual machine that is responsible for copying the VMware VMs into the XenServer format and importing them into the XenServer host. The virtual appliance is imported into the XenServer host that will host the converted virtual machines.

System requirements

The following list covers the requirements for installing the XenServer Conversion Manager Console.

- Microsoft .NET Framework 4.0
- 4 MB of available hard disk space

 The current version of the XenServer Conversion Manager console is 1.0.0.629. 

Operating systems

The following list covers the operating systems supported to run the XenServer Conversion Manager console:

- Microsoft Windows 7
- Microsoft Windows Server 2008
- Microsoft Windows Server 2008 R2

Importing the XenServer® Conversion Manager virtual appliance

The following steps cover configuring the XenServer Conversion Manager virtual appliance:

1. Import the XenServer Conversion Manager virtual appliance into the XenServer host and power on the virtual appliance.

2. Access the console of the virtual appliance from within XenCenter. Type *yes* and press *Enter* to accept the EULA:

```
Citrix XenServer Conversion Manager Virtual Appliance -
End User License Agreement

-----

CITRIX(R) LICENSE AGREEMENT

Use of this component is subject to the Citrix license covering the
Citrix product(s) with which you will be using this component. This
component is only licensed for use with such Citrix product(s).

CTX_code: EP_R_A32490

-----

Accept the terms in License Agreement? (yes/no): yes
```

3. Enter a new password for the root user and confirm the new password by entering it again. Press *Enter* to accept the new password:

```
Citrix XenServer Conversion Manager Virtual Appliance

Welcome to the Virtual Appliance configuration wizard.

Choose a root password for this virtual machine. This password
will only be used for appliance configuration or maintenance.

Changing password for user root.
New UNIX password:
Retype new UNIX password:
```

4. Enter a hostname to be used for the virtual appliance and press *Enter* to continue:

```
Citrix XenServer Conversion Manager Virtual Appliance

Answer the following questions to configure networking:

Choose a short hostname for this virtual machine.

Specify a hostname: XCMUAPP
```

5. Enter a domain suffix for the virtual appliance and press *Enter* to continue:

```
Citrix XenServer Conversion Manager Virtual Appliance
Answer the following questions to configure networking:
Choose a short hostname for this virtual machine.
Specify a hostname: XCMVAPP
Enter the domain suffix for this machine. e.g. mydomain.com: company.local
```

6. Choose whether to use DHCP for address assignment or manually enter the network settings by entering *Y* or *N* accordingly. Press *Enter* to continue:

```
Citrix XenServer Conversion Manager Virtual Appliance
Answer the following questions to configure networking:
Choose a short hostname for this virtual machine.
Specify a hostname: XCMVAPP
Enter the domain suffix for this machine. e.g. mydomain.com: company.local
Do you want to use DHCP to configure the network settings? (y/n):
```

7. Verify that the entered settings are correct, press *Y* or *N* accordingly and then, press *Enter* to complete the setup:

```
Citrix XenServer Conversion Manager Virtual Appliance
Confirm your network settings:
Hostname: XCMVAPP
Domain name: company.local
DHCP: Yes
Are these settings correct? (y/n):
```

- After the setup has completed, the appliance will present a login prompt:

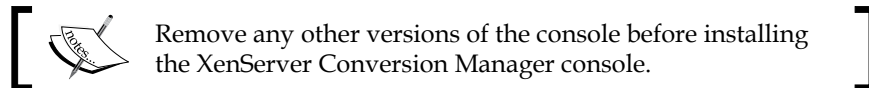
```
Citrix XenServer Conversion Manager Virtual Appliance
Citrix XenServer Conversion Manager Virtual Appliance configuration is complete.
Starting conusvc.exe [ OK ]
Starting monit: monit: generated unique Monit id 57c446c8464c3e4202a62ae8746b3a6
7 and stored to '/var/monit/id'
Starting monit daemon
Monit start delay set -- pause for 240s
[ OK ]
The Citrix XenServer Conversion Manager Service is running at 192.168.1.15
[ OK ]

Citrix XenServer Conversion Manager Virtual Appliance v1.0.0-633
XCMUAPP login: █
```

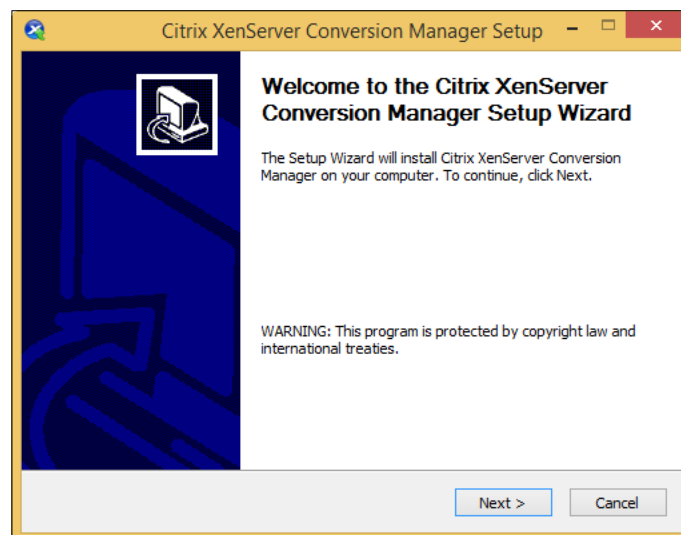
Installing the XenServer® Conversion Manager

The following steps cover installing the XenServer Conversion Manager:

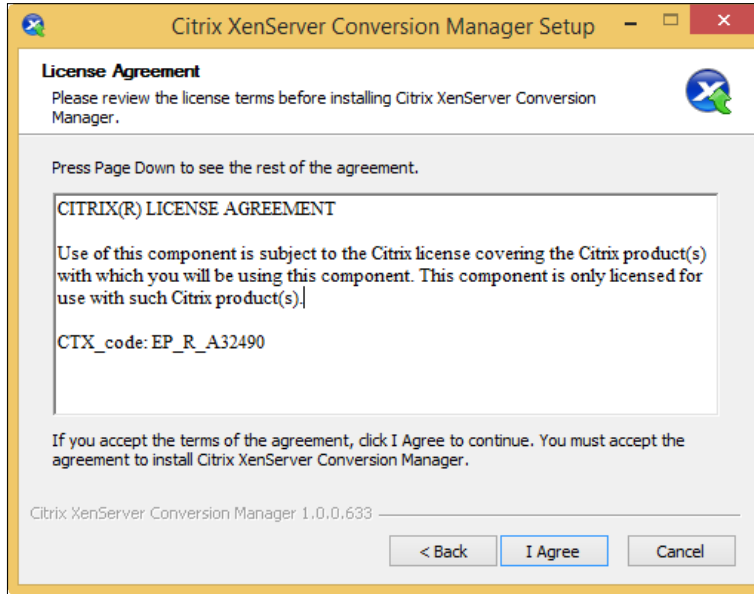
- Double-click on the XenServer Conversion Manager executable to launch the installer.



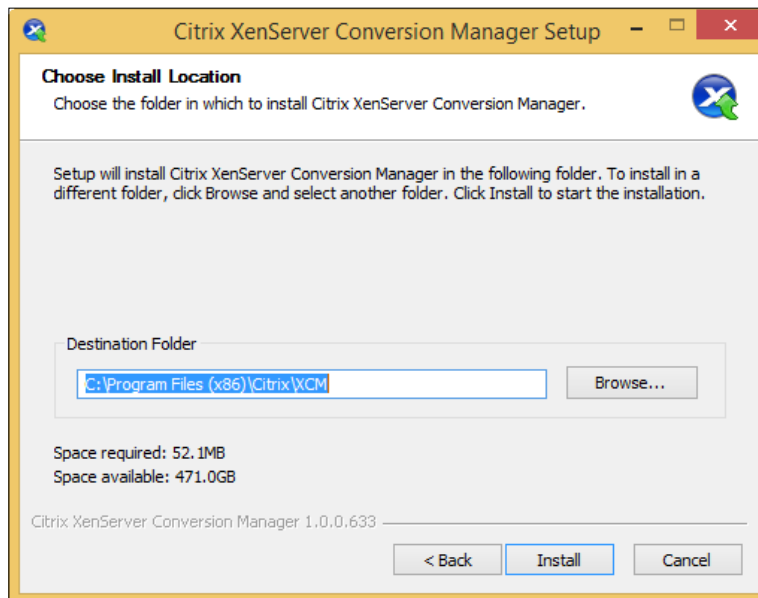
- Click on **Next** to start the installation for XenServer Conversion Manager:



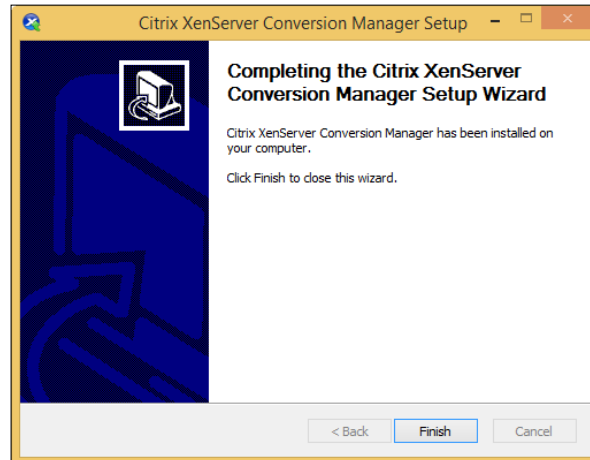
3. Click on **I Agree** to accept the EULA and proceed:



4. Select the installation location on the local system and click on **Install** to proceed:



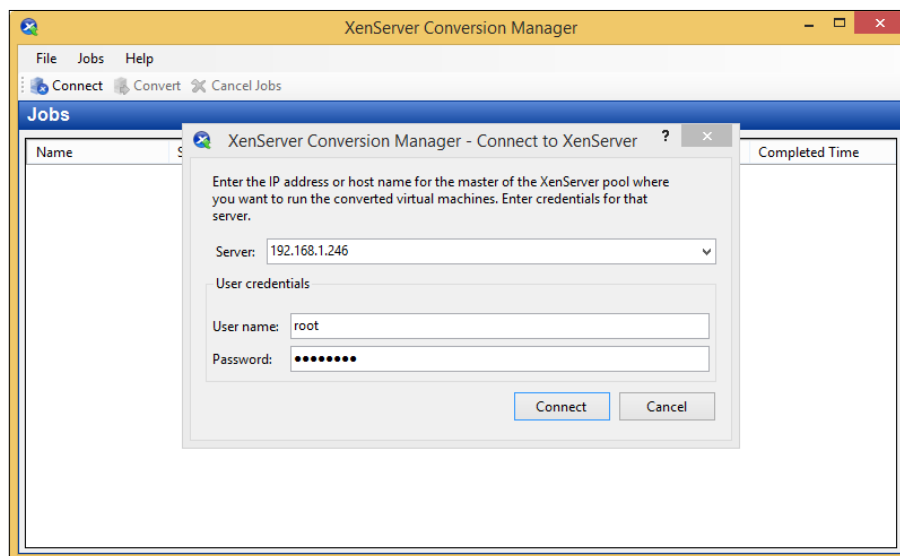
- Click on **Finish** to complete the installation of the XenServer Conversion Manager:



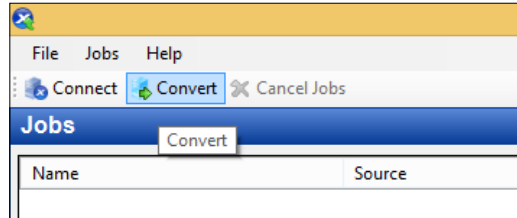
Converting a VMware VM to XenServer®

The following steps cover converting a virtual machine hosted on VMware ESXi to Citrix XenServer:

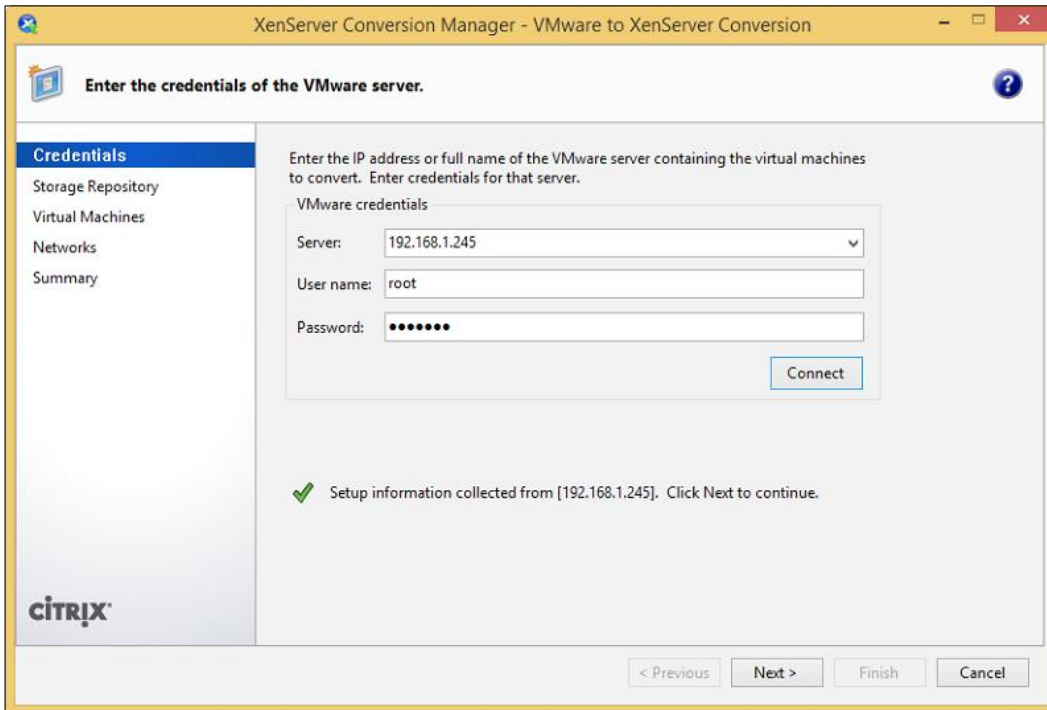
- Enter the hostname or IP address for the XenServer host along with the user credentials to access the server. Click on **Connect** to establish a connection with the XenServer host:



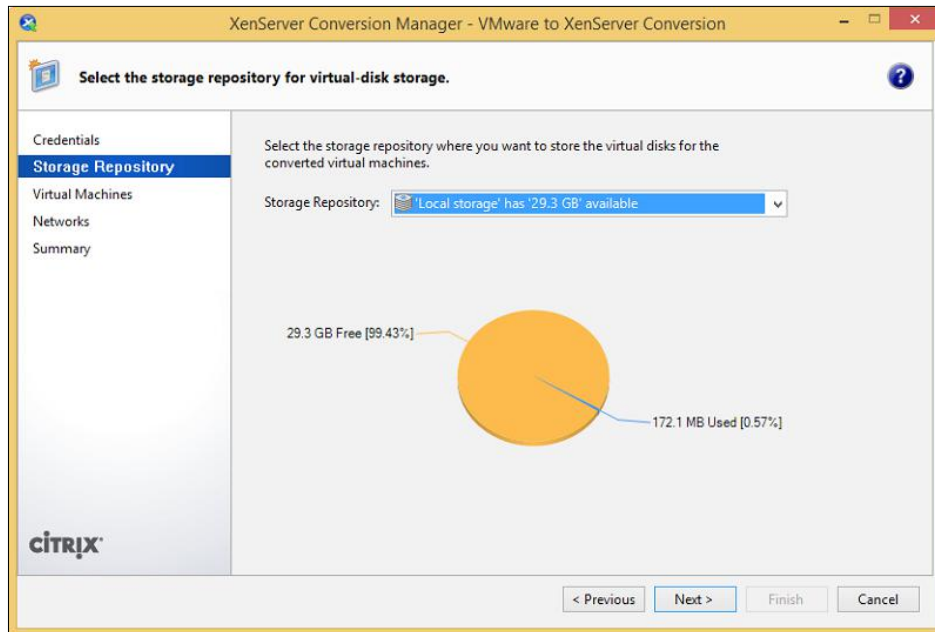
2. Click on **Convert** on the toolbar at the top of the XenServer Conversion Manager:



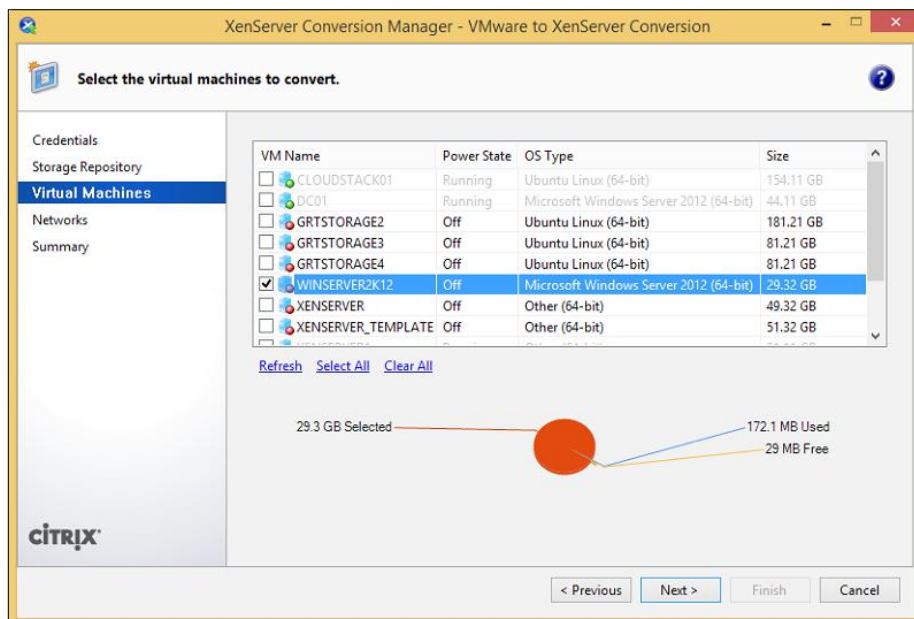
3. Enter the hostname or IP address for the VMware server along with the user credentials to access the server. Click on **Connect** to establish a connection with the VMware server. After the connection has been established, click on **Next** to continue:



- Select the storage repository to import the converted virtual machine onto.
Click on **Next** to continue:

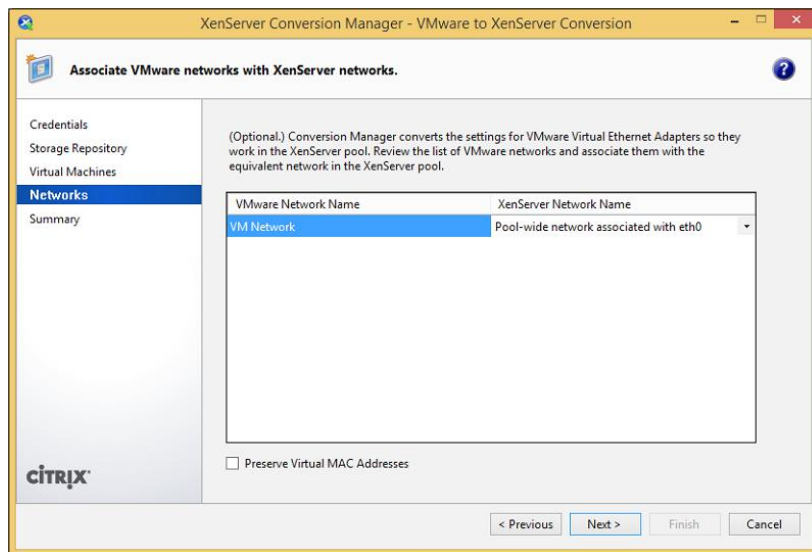


- Select the virtual machine(s) to convert and click on **Next** to continue:

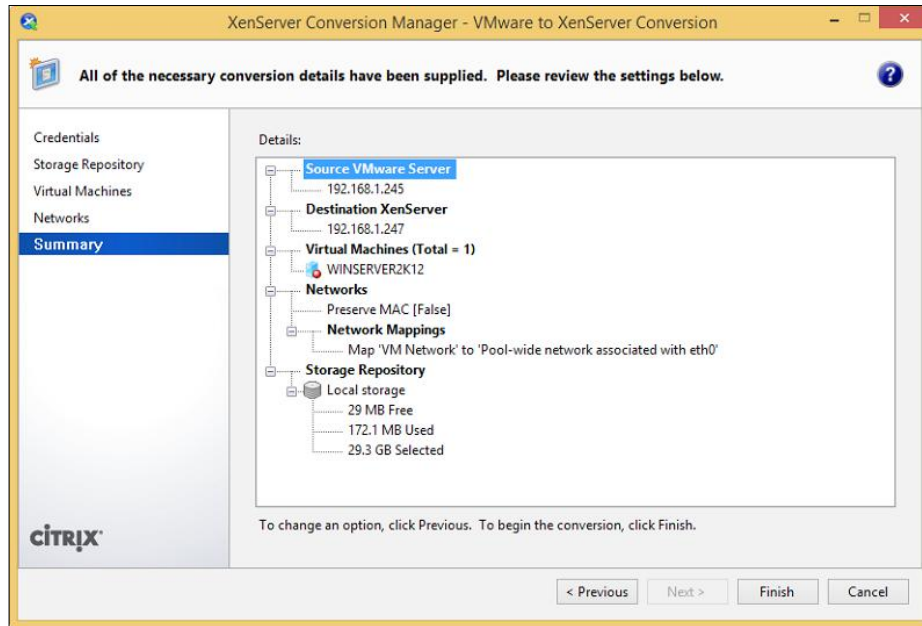


6. Select the network on the XenServer host used for the converted virtual machine. Optionally, check the **Preserve Virtual MAC Addresses** checkbox to keep the MAC address of the virtual machine after the conversion process. Click on **Next** to proceed.

The **Preserve Virtual MAC Addresses** option is advantageous when any networking component or application uses the MAC address of the virtual machine as a key identifier. This would typically be for security purposes in order to isolate the traffic and guarantee the integrity of security boundaries.

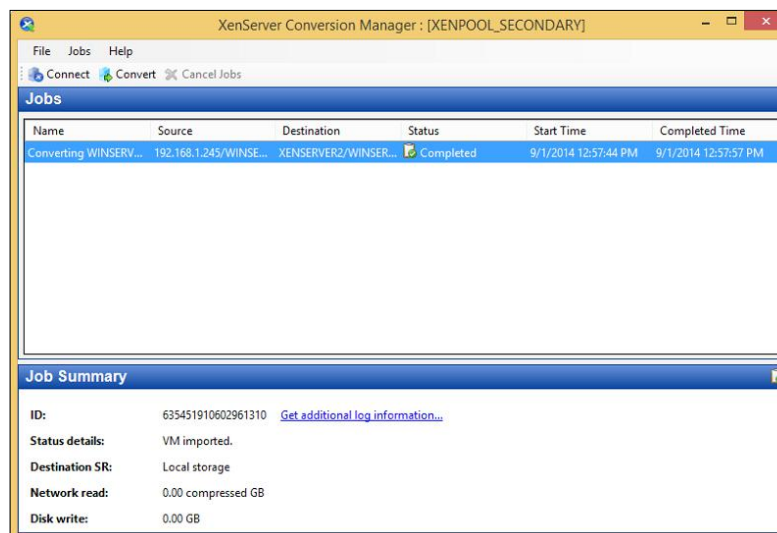


7. Click on **Finish** to start the conversion process:



8. Power on the VM following the successful conversion of the VM and install Citrix XenServer Tools onto the VM.

The following screenshot displays the status of previous and current conversion jobs:



Troubleshooting VM conversion

The XenServer Conversion Manager provides administrators with a robust tool to convert VMs from various platforms. While the tool provides a streamlined and easy process to convert VMs, there might be instances in which the conversion process does not complete successfully and troubleshooting needs to be performed. The following list contains some of the common errors:

- **Blue screen with Windows stop code 0x0000007B:** This error is caused when the conversion process is unable to properly convert a device critical to booting the Windows operating system. The conversion logs should be saved and provided to Citrix technical support to resolve the issue.
- **Windows product activation:** This error is caused by the conversion process as Windows might think that a hardware change has been made and prompt for reactivation. The issue can be resolved by reactivating Windows.
- **Unable to boot VMware SCSI disk:** This error is caused when a VMware VM is converted with a SCSI and an IDE hard disk, the conversion process assigns the IDE hard disk a lower device number than the SCSI disk. The issue can be resolved by rearranging the position of the disk so that the VM boots from the disk with the operating system.

Summary

In this chapter, we covered performing management tasks using the command line along with Windows PowerShell. We examined XenServer integration with the CloudStack IaaS platform, which is used in both public and private cloud solutions. We also looked at converting virtual machines from VMware ESXi to Citrix XenServer using XenServer Conversion Manager.

Index

A

- Acronis Backup Advanced**
 - about 172
 - URL 172
- active-active bonding**
 - about 46
 - specifications 46, 47
- Active Directory accounts**
 - managing 234
- Active Directory integration**
 - about 8, 229
 - disabling, CLI used 234
 - disabling, GUI used 232, 233
 - enabling, CLI used 232
 - enabling, GUI used 230, 231
 - requisites 230
- Active Directory users/groups**
 - adding, CLI used 235
 - adding, GUI used 234, 235
 - removing, CLI used 237
 - removing, GUI used 236, 237
- active-passive bonding 48, 49**
- agent-based backup solutions**
 - Acronis Backup Advanced 172
 - Symantec Backup Exec 172
- agent-based VM backups**
 - about 171
 - agent-based backups 172
 - agent-based backup solutions 172
 - agent-based restores 172
- antivirus 243**
- audit logging**
 - about 240
 - configuring, CLI used 241

B

- basic alerts, for SRs 208**
- basic alerts, for VMs 208**
- basic alerts, for XenServer® hosts 207**
- bonded network**
 - about 34
 - configuring 35-37
- bonding**
 - about 46
 - active-active bonding 46, 47
 - active-passive bonding 48, 49
 - LACP IP and port hash 50, 51
 - LACP source MAC address 52

C

- CIFS 62**
- CIFS ISO library 66**
- CIFS ISO library SR**
 - adding, on XenServer® host 66, 67
- Citrix® XenServer®**
 - installing 11
 - overview 8
 - planning 11, 22
 - supported upgrade paths 23
 - upgrade checklist 23, 24
 - upgrading 22-26
- Citrix® XenServer® 6.2**
 - about 10
 - configurations limits 29
 - network types 32
 - supported storage protocols 62
- Citrix® XenServer® 6.2, features**
 - deprecated features 11
 - improved guest support 10

- new licensing model 10
- open sourced 10
- retired features 11
- Citrix® XenServer® 6.2 installation**
 - from CD 14-19
 - methods 13
 - source 13
 - supplemental packs 14
- Citrix® XenServer®, features**
 - Active Directory integration 8
 - Disaster Recovery 9
 - DVSC 9
 - Dynamic Memory Control 9
 - HA 8
 - IntelliCache 9
 - Open vSwitch 9
 - RBAC 9
 - resource pools 8
 - Storage XenMotion/Live Storage Migration 8
 - XenMotion/Live VM Migration 8
- Citrix® XenServer® installation**
 - server hardware, selecting 11
- Citrix® XenServer® installation, prerequisites 12**
 - hard disk 12
 - memory 12
 - network card 13
 - processor 12
- CLI**
 - server, adding to resource pool 146, 147
 - server, removing from resource pool 149
 - used, for adding Active Directory users/groups 235
 - used, for adding NFS ISO library SR 70
 - used, for backing up control domain 176, 177
 - used, for configuring audit logging 241
 - used, for configuring e-mail notification authentication settings 211
 - used, for configuring e-mail notification settings 210, 211
 - used, for configuring remote logging 216, 217
 - used, for copying VM 112
 - used, for creating NFS SR 82
 - used, for creating resource pool 144
 - used, for creating Software iSCSI SR 78-80
 - used, for creating vApps 126, 127
 - used, for creating VM snapshot 117
 - used, for creating VM templates 121
 - used, for deleting VMs 113, 114
 - used, for detaching SR 84, 85
 - used, for disabling Active Directory integration 234
 - used, for disabling HA 167, 168
 - used, for enabling Active Directory integration 232
 - used, for enabling HA 163, 164
 - used, for exporting VMs 139, 140
 - used, for forgetting SR 88
 - used, for importing VMs 135
 - used, for managing user roles 240
 - used, for modifying default SR 94, 95
 - used, for modifying root password 228
 - used, for reattaching SR 87
 - used, for removing Active Directory users/groups 237
 - used, for restoring control domain 180-182
- CloudStack**
 - about 253
 - URL 253
- CloudStack deployment**
 - XenServer® host, adding to 255-257
- CloudStack integration**
 - about 253
 - system requisites 253
- CloudStack XenServer® Support Package**
 - configuring 254
- command line management**
 - about 247
 - host command line 247
 - SSH command line 247
 - XE command 248
- Common Internet File System. See CIFS**
- components, for backing up VMs**
 - metadata 170
 - VDIs 170
- components, XenServer® host installation**
 - control domain 171
 - pool/host metadata 171

components, XenServer® networking

network 31, 32

PIF 30

VIF 30, 31

configurations limits, Citrix®

XenServer® 6.2 29

control domain

about 171, 174

backing up, CLI used 176, 177

backing up, GUI used 175, 176

restoring, CLI used 180-182

restoring, GUI used 177-180

Copy on Write (CoW) 64

CPU masking 142

crash dump SR 92

cross-server private network 40

D

dedicated IP storage NICs

about 43

configuring 43-46

default SR

about 92

modifying, CLI used 94, 95

modifying, GUI used 93

Destroy operation 89

detach operation 83

directories, XE command

32 bit 248

64 bit 248

Disaster Recovery 9

disk and memory snapshots 114

disk-only snapshots 114

disk provisioning, SRs

about 71

NFS virtual disk SR 80

software iSCSI initiator IQN 72, 73

software iSCSI virtual disk SR 71

thick provisioned 71

thin provisioned 71

Distributed Virtual Switch

Controller. *See* DVSC

DMC

about 9, 107

dynamic memory range 107

static memory range 107

dom0 memory settings

modifying 254

DVD drive 108

DVSC 9, 40

Dynamic Memory Control. *See* DMC

dynamic memory range, DMC 107

E

e-mail notification authentication settings

configuring, CLI used 211

e-mail notification settings

configuring, CLI used 210, 211

configuring, GUI used 209, 210

Emergency Network Reset feature 59

End User License Agreement (EULA) 137

external network

about 32

configuring 33

F

failback option, XenServer® Disaster Recovery 184

failover feature, XenServer® Disaster Recovery 183

fast clone 110

Fibre Channel 62

Fibre Channel over Ethernet (FCoE) 61, 62

Forget operation 87

full copy 110

G

Generic Routing Encapsulation (GRE) 28

GUI

CIFS ISO library SR, adding on

XenServer® host 66, 67

host, adding to resource pool 145, 146

server, removing from resource pool 148

used, for adding Active Directory

users/groups 234, 235

used, for adding NFS ISO library SR 68, 69

used, for backing up control

domain 175, 176

used, for configuring e-mail notification

settings 209, 210

- used, for configuring remote logging 215, 216
- used, for copying VM 111
- used, for creating NFS SR 80, 81
- used, for creating resource pool 143, 144
- used, for creating Software iSCSI SR 74-78
- used, for creating vApps 122-126
- used, for creating VM snapshot 115, 116
- used, for creating VM templates 118-120
- used, for deleting VMs 112, 113
- used, for detaching SR 83
- used, for disabling Active Directory integration 232, 233
- used, for disabling HA 166, 167
- used, for enabling Active Directory integration 230, 231
- used, for enabling HA 160-162
- used, for exporting VMs 135-137
- used, for forgetting SR 88
- used, for importing VMs 129-134
- used, for managing user roles 238-240
- used, for modifying default SR 93
- used, for modifying root password 226, 227
- used, for reattaching SR 86
- used, for removing Active Directory users/groups 236, 237
- used, for restoring control domain 177-180
- VLAN, configuring on XenServer® network 54, 55

H

HA

- about 8, 141, 158
- disabling, CLI used 167, 168
- disabling, GUI used 166, 167
- enabling, CLI used 163, 164
- enabling, GUI used 160-162
- requisites 159

HA capacity planning

- about 159
- maximum failure capacity 159
- server failure limit 159

hard disk 108

hardware-assisted virtualization mode. *See* HVM

Hardware Compatibility List. *See* HCL

hardware HBA 70

HA restart priority 165

HCL

- about 11
- URL 11

heartbeats

- about 158
- network heartbeats 158
- storage heartbeats 158

heterogeneous resource pool 142

High Availability. *See* HA

homogeneous resource pool 141

host bus adapter (HBA) 13, 82

host command line 247

host metadata 173

hosts

- about 171
- adding, to resource pool 145, 146

host security 241

HVM 98

hypervisor-based backup solutions

- Acronis Backup Advanced for Citrix® XenServer® 173
- Quadric Software Alike 173
- SEP software sesam 173
- Unitrends Virtual Backup 173

I

IDE 62

Infrastructure as a Service (IaaS) 253

installation, Citrix® XenServer® 11

installation, XenCenter® 20

installation, XenServer® Conversion Manager 261-263

installation, XenServer® PowerShell Snap-in 249-252

installation, XenServer® Tools

- on Linux VMs 105
- on Windows VMs 104

Integrated StorageLink (iSL) 83

IntelliCache 9

iSCSI 62

iSCSI Challenge-Handshake Authentication Protocol (iSCSI CHAP) 244

iSCSI Qualified Name (IQN) 72

ISO library SRs

about 66

CIFS ISO library 66

NFS ISO library 68

J

jumbo frames, QoS

about 56

requisites 56

K

kilobits (kbps) 56

L

LACP 28, 50

LACP IP and port hash 50, 51

LACP source MAC address 52

licensing model, Citrix® XenServer® 6.2 10

Link Aggregation Control

Protocol. *See* LACP

Linux VMs

XenServer® Tools, installing 105

local authentication

about 225

root password, modifying CLI used 228

root password, modifying GUI

used 226, 227

root SSH login, disabling 228, 229

local storage 70

Logical Unit Number (LUN) 63

M

management interface

about 40

configuring 41, 42

Maximum Transmission Unit (MTU) 56

memory ballooning 107

memory (RAM)

about 106

DMC 107

methods, for backing XenServer® VM

about 171

agent-based 171

hypervisor-based 172

modification, VM

DVD drive 108

hard disk 108

memory (RAM) 106

network adapter 108

processor (vCPU) 106

N

NetFlow 28

network 31

network adapter 108

Network File System (NFSv3) 62

network heartbeats 158

Network Management Software (NMS) 212

network troubleshooting, QoS

about 58

Emergency Network Reset 59

network types, Citrix® XenServer® 6.2

bonded 34

cross-server private 40

external 32

single-server private 38

NFS ISO library SR

about 68

adding, CLI used 70

adding, GUI used 68, 69

NFS SR

creating, CLI used 82

creating, GUI used 80, 81

NFS VHD 70

NFS virtual disk SR 80

O

OpenFlow 28

Open Virtual Appliance. *See* OVA

Open Virtualization Format. *See* OVF

Open vSwitch 9

Operating System Fixup 129

Oracle Enterprise Linux (OEL) 10

OVA 128
OVF 128
OVF package
 Compress OVF files option 138, 139
 Create OVA package option 138
 signing 137

P

paravirtualized mode 98
patching 201
performance alerts 207
Physical Block Device (PBD) 63
physical interface (PIF) 30
Pool Admin account 238
pool/host metadata 171
pool master 143
pool metadata
 backing up 174
 restoring 174, 175
pool metadata restore command 175
Pool Operator role 238
pool restore dry-run command 174
power operations, VM
 Force Reboot 109
 Force Shutdown 109
 Pause 110
 performing 109, 110
 Reboot 109
 Resume 110
 Shut Down 109
 Start 109
 Suspend 110
 Unpause 110
PowerShell integration 248
Preserve Virtual MAC Addresses
 option 266
processor (vCPU) 106

Q

QoS
 about 9, 28, 56, 65
 jumbo frames 56
 network troubleshooting 58

QoS configuration
 example 56
Quadric Software Alike
 URL 173
Quality of Service. *See* **QoS**
quiesced snapshots 114

R

RBAC 9, 225, 238
Read Only role 238
reattach operation 86
Red Hat Enterprise Linux (RHEL) 10
remote logging
 configuring, CLI used 216, 217
 configuring, GUI used 215, 216
Remote Switched Port
 Analyzer. *See* **RSPAN**
Repair operation 89
resource pool
 about 141
 creating, CLI used 144
 creating, GUI used 143, 144
 heterogeneous resource pool 142
 homogeneous resource pool 141
 host, adding to 145, 146
 pool master 143
 requisites 142
 server, adding to 146, 147
 server, removing from 147
role-based access control. *See* **RBAC**
roles, XenServer® environment
 Pool Admin 238
 Pool Operator 238
 Read Only 238
 VM Admin 238
 VM Operator 238
 VM Power Admin 238
rolling pool upgrades 26
root password
 modifying, CLI used 228
 modifying, GUI used 226, 227
root SSH login
 disabling 228, 229
RSPAN 28

S

SAS 62

SATA 62

SEP software sesam

URL 173

server

adding, to resource pool 146, 147

removing, from resource pool 147

removing from resource pool, with CLI 149

removing from resource pool,

with GUI 148

server fencing, HA 158

Server Message Block (SMB) protocol 66

server status report, XenCenter® event log

about 217

generating, CLI used 220

generating, GUI used 218-220

sFlow 28

Simple Network Management Protocol. See

SNMP

single-server private network

about 38

configuring 38, 39

snapshot functionality 172

snapshots, VM

about 114

creating, CLI used 117

creating, GUI used 115, 116

disk and memory snapshots 114

disk-only snapshots 114

quiesced snapshots 114

vApps 122

VM templates 118

SNMP

about 212

configuring 212-214

software-defined networking (SDN) 9

software iSCSI 70

software iSCSI initiator IQN 72, 73

Software iSCSI SR

creating, CLI used 78-80

creating, GUI used 74-78

software iSCSI virtual disk SR 71

SPAN 28

SRs

about 65, 171

crash dump SR 92

default SR 92

Destroy operation 89

detach operation 83

detaching, CLI used 84, 85

detaching, GUI used 83

disk provisioning 71

Forget operation 87

forgetting, CLI used 88

forgetting, GUI used 88

host bus adapter hardware 82

ISO library SRs 66

managing 83

reattach operation 86

reattaching, CLI used 87

reattaching, GUI used 86

Repair operation 89

repairing, from XenServer® host 89-91

resizing 91

StorageLink Technology 83

suspend SR 91

virtual disk library SRs 70

SSH command line 247

static memory range, DMC 107

storage area network (SAN) 13

storage components, XenServer®

PBD 63

SRs 65

VBDs 65

VDIs 64

storage heartbeats 158

StorageLink technology 70

storage security 243, 244

Storage XenMotion®

about 156

requisites 156

VM, migrating 157, 158

supported storage protocols,

Citrix® XenServer® 6.2

CIFS 62

FCoE 62

- Fibre Channel 62
- IDE 62
- iSCSI 62
- Network File System (NFSv3) 62
- SAS 62
- SATA 62
- SUSE Linux Enterprise Server (SLES) 10**
- suspend SR 91**
- Switched Port Analyzer.** *See* SPAN
- Symantec Backup Exec**
 - about 172
 - URL 172
- system requisites, CloudStack integration**
 - about 253
 - CloudStack XenServer® Support Package configuration 254
 - dom0 memory settings, modifying 254
- system requisites, XenServer® Conversion Manager**
 - about 258
 - operating systems 258

T

- test failover option, XenServer® Disaster Recovery 184**
- thick provisioned disks 71**
- thin provisioned disks 71**
- traffic types, XenServer® VLAN**
 - dedicated IP storage traffic 54
 - management traffic 53
 - virtual machines 54
- transfer VM 129**

U

- Unitrends Virtual Backup**
 - URL 173
- user roles**
 - managing, CLI used 240
 - managing, GUI used 238-240

V

- VBDs 65**
- VDIs**
 - about 64, 170
 - format 64

- VIF 30, 31**
- virtual appliances (vApps)**
 - about 97, 122
 - creating, CLI used 126, 127
 - creating, GUI used 122-126
 - delay interval 125
 - start order 125
- Virtual Block Devices.** *See* VBDs
- Virtual Disk Images.** *See* VDIs
- virtual disk library SRs**
 - about 70
 - hardware HBA 70
 - local storage 70
 - NFS VHD 70
 - software iSCSI 70
 - StorageLink technology 70
- Virtual Hard Disk (VHD) 64**
- virtual interface.** *See* VIF
- virtualization 7**
- Virtual Machine Protection Recovery (VMPR) 11**
- virtual machine.** *See* VM
- virtual to virtual (V2V) 257**
- VLAN**
 - configuring, on XenServer® network 54, 55
- VM**
 - about 97, 170
 - copying 110
 - creating 98-103
 - deleting 112
 - deleting, CLI used 113, 114
 - deleting, GUI used 112, 113
 - exporting 128
 - exporting, CLI used 139, 140
 - exporting, GUI used 135-137
 - exporting, with Create a manifest option 137
 - importing 128
 - importing, CLI used 135
 - importing, GUI used 129-134
 - managing 108
 - modifying 106
 - overview 98
 - power operations, performing 109, 110
 - XenServer® Tools 104

- VM Admin role** 238
- VM conversion**
 - errors 268
 - troubleshooting 268
- VM, copying**
 - CLI, using 112
 - fast clone 110
 - full copy 110
 - GUI, using 111
- VM HA settings**
 - about 165
 - delay interval 166
 - HA restart priority 165
 - start order 165
- VM metadata** 170
- VM, modes**
 - HVM 98
 - paravirtualized mode 98
- VM Operator role** 238
- VM Power Admin role** 238
- VM security**
 - about 243
 - agent-based 243
 - virtualization-optimized 243
- VM templates**
 - about 118
 - creating, CLI used 121
 - creating, GUI used 118-120
- VMware VM**
 - converting, to XenServer® 263-267
- VXLAN** 28

W

- Windows VMs**
 - XenServer® Tools, installing 104
- Workload Balancing (WLB)** 11

X

- xe appliance-create command** 126
- xe appliance-list command** 127
- xe help command** 248
- xe host-forget command** 182

- xe host-list command** 149, 152
- xe host-param-get command** 73
- xe host-param-set command** 73
- XenCenter®**
 - about 20
 - installing 20
 - system requisites 20
- XenCenter® application log**
 - about 221
 - accessing 221, 222
- XenCenter® event log**
 - about 217
 - server status report 217
 - server status report, generating
 - with CLI 220
 - server status report, generating
 - with GUI 218-220
- XenMotion®**
 - about 152
 - requisites 152
 - VM, migrating 153-155
- XenServer®**
 - backing up 173
 - restoring 173
 - storage components 62
 - VMware VM, converting to 263-267
- XenServer® 6.2 Software Development Kit (SDK)**
 - URL, for downloading 249
- XenServer® answer file** 21, 22
- XenServer® answer file, elements**
 - Admin-interface name="eth0"
 - proto="dhcp" 22
 - Guest-disk 22
 - Installation srtype 22
 - Keymap 22
 - Primary-disk 22
 - Root-password 22
 - Source type 22
 - Timezone 22
- XenServer® business continuity plan**
 - developing 170
- XenServer® Conversion Manager**
 - about 257
 - installing 261-263

- system requisites 258
- URL, for downloading 257
- XenServer® Conversion Manager**
 - console 257
- XenServer® Conversion Manager virtual appliance**
 - configuring 258-261
- XenServer® deployment**
 - restoring 182
- XenServer® DR**
 - about 183
 - configuring 185-187
 - failback option 184
 - failover feature 183
 - requisites 185
 - test failover option 184
- XenServer® DR failback**
 - performing 196-200
- XenServer® DR failover**
 - performing 191-195
- XenServer® DR test failover 187-190**
- XenServer® environment**
 - guidelines, for host security 241, 242
- XenServer® host**
 - adding, to CloudStack deployment 255-257
 - SR, repairing from 89-91
- XenServer® host firewall 242**
- XenServer® logging**
 - about 215
 - remote logging, configuring
 - with CLI 216, 217
 - remote logging, configuring
 - with GUI 215, 216
- XenServer® maintenance mode**
 - about 150
 - server, placing into maintenance mode
 - with CLI 151, 152
 - server, placing into maintenance mode
 - with GUI 150
- XenServer® networking**
 - components 29-32
 - overview 28
- XenServer® performance**
 - monitoring 205
- XenServer® PowerShell Snap-in**
 - installing 249-252
- XenServer® PXE installation 21**
- XenServer® SDKs**
 - about 253
 - URL, for downloading 253
- XenServer® storage**
 - overview 61
- XenServer® Tools**
 - about 104
 - installing, on Linux VMs 105
 - installing, on Windows VMs 104
- XenServer® updates**
 - about 201
 - deploying 202-205
- xe pbd-list command 85, 87**
- xe pbd-plug command 87**
- xe pbd-unplug command 85, 88**
- xe pool-designate-new-master command 143**
- xe pool-eject command 149**
- xe pool-ha-disable command 167**
- xe pool-ha-enable command 164**
- xe pool-join command 144**
- xe pool-list command 144**
- xe pool-param-get command 164, 168**
- xe pool-param-set command 94, 145**
- xe pool-restore-database command 182**
- xe snapshot-list command 118**
- xe sr-create command 70, 82**
- xe sr-forget command 89**
- xe sr-list command 79, 82, 84, 88, 94**
- xe sr-probe command 78**
- xe template-list command 121**
- xe vm-copy command 112**
- xe vm-destroy command 114**
- xe vm-export command 140**
- xe vm-import command 135**
- xe vm-list command 114, 121, 127, 135, 139**
- xe vm-param-set command 121, 127**
- xe vm-pause command 110**
- xe vm-reboot command 109**
- xe vm-resume command 110**
- xe vm-shutdown command 109, 113**

xe vm-snapshot command 117
xe vm-start command 109
xe vm-suspend command 110
xe vm-unpause command 110
xsconsole command 91
XVA 128
XVA Version 1 128



Thank you for buying Mastering Citrix® XenServer®

About Packt Publishing

Packt, pronounced 'packed', published its first book, *Mastering phpMyAdmin for Effective MySQL Management*, in April 2004, and subsequently continued to specialize in publishing highly focused books on specific technologies and solutions.

Our books and publications share the experiences of your fellow IT professionals in adapting and customizing today's systems, applications, and frameworks. Our solution-based books give you the knowledge and power to customize the software and technologies you're using to get the job done. Packt books are more specific and less general than the IT books you have seen in the past. Our unique business model allows us to bring you more focused information, giving you more of what you need to know, and less of what you don't.

Packt is a modern yet unique publishing company that focuses on producing quality, cutting-edge books for communities of developers, administrators, and newbies alike. For more information, please visit our website at www.packtpub.com.

About Packt Open Source

In 2010, Packt launched two new brands, Packt Open Source and Packt Enterprise, in order to continue its focus on specialization. This book is part of the Packt Open Source brand, home to books published on software built around open source licenses, and offering information to anybody from advanced developers to budding web designers. The Open Source brand also runs Packt's Open Source Royalty Scheme, by which Packt gives a royalty to each open source project about whose software a book is sold.

Writing for Packt

We welcome all inquiries from people who are interested in authoring. Book proposals should be sent to author@packtpub.com. If your book idea is still at an early stage and you would like to discuss it first before writing a formal book proposal, then please contact us; one of our commissioning editors will get in touch with you.

We're not just looking for published authors; if you have strong technical skills but no writing experience, our experienced editors can help you develop a writing career, or simply get some additional reward for your expertise.



Citrix® XenDesktop® 7 Cookbook

ISBN: 978-1-78217-746-3 Paperback: 410 pages

Over 35 recipes to help you implement a fully featured XenDesktop® 7 architecture with a rich and powerful VDI experience

1. Implement the XenDesktop 7 architecture and its satellite components.
2. Learn how to publish desktops and applications to the end user devices, optimizing their performance and increasing the general security.
3. Designed in a manner that will allow you to progress gradually from one chapter to another or to implement a single component only referring to the specific topic.



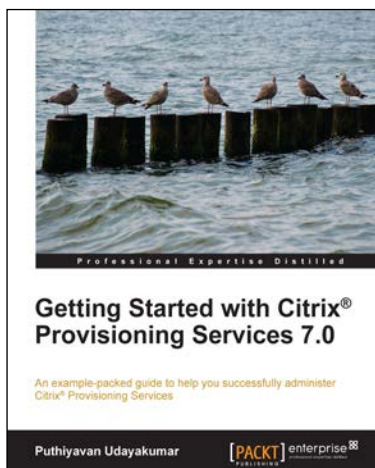
Citrix® XenApp® 6.5 Expert Cookbook

ISBN: 978-1-84968-522-1 Paperback: 420 pages

Over 125 recipes that enable you to configure, administer, and troubleshoot a XenApp® infrastructure for effective application virtualization

1. Create installation scripts for Citrix XenApp, License Servers, Web Interface, and StoreFront.
2. Use PowerShell scripts to configure and administer the XenApp's infrastructure components.
3. Discover Citrix and community written tools to maintain a Citrix XenApp infrastructure.

Please check www.PacktPub.com for information on our titles



Getting Started with Citrix® Provisioning Services 7.0

ISBN: 978-1-78217-670-1 Paperback: 134 pages

An example-packed guide to help you successfully administer Citrix® Provisioning Services

1. Install and configure Citrix Provisioning Services quickly and efficiently.
2. Master the architecture of Citrix Provisioning Services.
3. Successfully manage and operate Citrix Provisioning Services.



Citrix® XenMobile™ Mobile Device Management

ISBN: 978-1-78217-214-7 Paperback: 112 pages

Gain an insight into the industry's best and most secure Enterprise Mobility Management solution

1. Deploy and manage the complete XenMobile solution.
2. Learn how to customize and troubleshoot your XenMobile apps.
3. Step-by-step instructions with relevant screenshots for better understanding.

Please check www.PacktPub.com for information on our titles