

Quick answers to common problems

Citrix® XenDesktop® 7 Cookbook

Over 35 recipes to help you implement a fully featured
XenDesktop® 7 architecture with a rich and powerful
VDI experience

Gaspare A. Silvestri

[PACKT] enterprise
professional expertise distilled

Citrix® XenDesktop® 7 Cookbook

Over 35 recipes to help you implement a fully featured XenDesktop® 7 architecture with a rich and powerful VDI experience

Gaspare A. Silvestri



BIRMINGHAM - MUMBAI

Citrix® XenDesktop® 7 Cookbook

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: January 2013

Second edition: January 2014

Production Reference: 2210114

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

ISBN 978-1-78217-746-3

www.packtpub.com

Cover Image by Aniket Sawant (aniket_sawant_photography@hotmail.com)

Credits

Author

Gaspare A. Silvestri

Project Coordinator

Priyanka Goel

Reviewers

Jack Cobben

Ferdinand Feenstra

Florian Zoller

Proofreader

Sandra Hopper

Indexer

Tejal Soni

Acquisition Editors

Rubal Kaur

Kunal Parikh

Production Coordinators

Melwyn D'sa

Aditi Gajjar Patel

Lead Technical Editor

Amey Varangaonkar

Adonia Jones

Komal Ramchandani

Technical Editors

Pragnesh Bilmoria

Jinesh Kampani

Shruti Rawool

Aman Preet Singh

Cover Work

Melwyn D'sa

Adonia Jones

Copy Editors

Roshni Banerjee

Sarang Chari

Brandt D'Mello

Disclaimer

The statements made and opinions expressed herein belong exclusively to the author and reviewers 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, or 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

Gaspare A. Silvestri is an IT specialist with 10 years of experience in the Information Technology market. Currently, he works as the CTO for an ICT company based in Italy. Being a multicertified IT director, he considers his job as the first of all his passions, with a particular preference for the areas of virtualization and Unix. He is always curious and in search of new IT projects on which to perform research activities. Gaspare has been involved in the design, tuning, and consolidation of physical and virtual infrastructures for important system integration companies based in Italy.

Gaspare is also the author of *Citrix XenDesktop 5.6 Cookbook*, by Packt Publishing.

Thanks to Viola and Manuela—the shining stars of my life.

Thanks to my parents—for the road of life they have given to me.

Thanks to Tiziana and Sergio—for the help they gave me with my shining stars.

Thanks to Roberto—who gave me the opportunity to start working on the Citrix® platforms some years ago.

A special thanks to Steven Wright—a wonderful person who permitted me to use his fantastic software (WrightSMS2 in *Chapter 10, Configuring the XenDesktop® Advanced Logon*).

Thanks to the coffee and Miles Davis—who have been my main fellowships during working hours.

Special thanks to the entire Packt staff and the Technical Reviewers—for the exceptional work they have done with me and for all the work we have done together.

About the Reviewers

Jack Cobben is no stranger to the challenges that enterprises can experience when managing large deployments of Windows systems and Citrix® implementations, with over thirteen years of systems management experience. In his free time, Jack writes for his own blog at www.jackcobben.nl and is active on the Citrix® support forums. He loves to test new software and share the knowledge in any way he can. You can follow him on twitter via @jackcobben. While he works for Citrix®, Citrix® didn't help with, or support, this book in any way or form.

Ferdinand Feenstra, based in the Netherlands, is a Citrix® Certified Architect and a senior specialist for Microsoft environments. He is working in the IT field since 1998, and he has experience in many complex environments with different customers in different functions.

His experience is categorized into building and designing Citrix® environments, implementations and migrations projects, and consultancy projects. Since he began working with Citrix® in 2004, a new world of solutions and the opportunity to work on any device combined with a great user experience came his way. This makes IT more dynamic and easier to adopt for users. You can find his blog at www.CitrixGuru.net or check his tweets on Twitter at @f_feenstra.

This is the fifth review for him. He has already reviewed *Instant EdgeSight for XenApp* by Vaqar Hasan, *XenServer 6.0 Administration Essential Guide* by Daniele Tosatto, *Citrix XenDesktop 5.6 Cookbook* by Gaspare A. Silvestri, and *Implementing Citrix XenServer Quickstarter* by Gohar Ahmed.

Ferdinand works for Imtech ICT Communication Solutions B.V., which is a Citrix® Gold Solution Advisor. With 2,500 IT professionals, Imtech ICT is part of Royal Imtech NV (30,000 employees worldwide). Solutions that Imtech provides range from embedded software for high-tech industrial environments and business software applications to IT infrastructures. Imtech ICT Communication Solutions BV designs and implements large-scale infrastructures, such as virtual desktop environments, secure networks, servers, unified communications, storage, and backup solutions. Among Citrix®, Imtech ICT provides (managed) solutions based on Cisco, HP, VMware, Avaya, Microsoft, and other major market leading vendors. For more information, visit www.imtech.com/nl/ICT.

Florian Zoller works as a senior IT consultant for a consulting company in Germany. He has several years of experience in designing and implementing Citrix® infrastructures. Additionally, he is an expert in automated server- and client-deployment technologies.

www.PacktPub.com

Support files, eBooks, discount offers and more

You might want to visit www.PacktPub.com for support files and downloads related to your book.

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.



<http://PacktLib.PacktPub.com>

Do you need instant solutions to your IT questions? PacktLib is Packt's online digital book library. Here, you can access, read and search across 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 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 nine entirely free books. Simply use your login credentials for immediate access.

Instant Updates on New Packt Books

Get notified! Find out when new books are published by following [@PacktEnterprise](#) on Twitter, or the *Packt Enterprise* Facebook page.

Table of Contents

Preface	1
Chapter 1: XenDesktop® 7 – Upgrading, Installing, and Configuring	5
Introduction	5
Upgrading from XenDesktop® 5.6 to XenDesktop® 7	9
Preparing the SQL Server 2012 database	16
Installing and configuring the Citrix Licensing Services – 11.11.1	19
Installing XenDesktop® 7 components	25
Installing and configuring StoreFront 2.0	30
Installing and configuring Provisioning Services 7	41
Chapter 2: Configuring and Deploying Virtual Machines for XenDesktop®	55
Introduction	55
Configuring the XenDesktop® site	56
Configuring XenDesktop® to interact with Citrix® XenServer®	61
Configuring XenDesktop® to interact with VMware vSphere 5.1	66
Configuring XenDesktop® to interact with Microsoft Hyper-V	73
Chapter 3: Master Image Configuration and Tuning	87
Introduction	87
Configuring and optimizing a desktop OS master image	88
Configuring and optimizing a server OS master image	97
Configuring a target device – PVS architecture	103
Installing and configuring the master image policies	110

Table of Contents

Chapter 4: User Experience – Planning and Configuring	117
Introduction	117
Implementing a profile architecture	118
Installing Virtual Desktop Agent – server OS and desktop OS	126
Installing and configuring HDX Monitor	135
Configuring Citrix Receiver™	143
Chapter 5: Configuring Additional Architectural Components	151
Introduction	151
Configuring the Merchandising Server	152
Configuring the CloudBridge platform	164
Installing and configuring the XenDesktop® Collector	174
Chapter 6: Creating and Configuring a Desktop Environment	181
Introduction	181
Creating and configuring the Machine Catalog	182
Modifying an existing machine catalog	199
Using the new Citrix® Director platform	208
Configuring printers	217
Configuring USB devices	227
Chapter 7: Deploying Applications	233
Introduction	233
Publishing the hosted applications	234
Publishing the Local Access Apps (LAA)	246
Publishing applications using Microsoft App-V	255
Chapter 8: XenDesktop® Tuning and Security	267
Introduction	267
Configuring the XenDesktop® policies	267
Installing and configuring Citrix® NetScaler Gateway 10.1	298
Configuring the XenDesktop® logging	312
Chapter 9: Working with XenDesktop® PowerShell	319
Introduction	319
Retrieving system information – configuration Service cmdlets	320
Managing Active Directory accounts – ADIdentity cmdlets	323
Managing the Citrix® Desktop Controller and its resources – the Broker and AppV cmdlets	328
Administering hosts and machines – the Host and Machine Creation cmdlets	338
Managing additional components – the StoreFront Admin and Logging cmdlets	343

Table of Contents

<u>Chapter 10: Configuring the XenDesktop® Advanced Logon</u>	349
Introduction	349
Implementing the two-factor hardware authentication for XenDesktop® 7	350
Implementing strong authentication for XenDesktop® 7 using the RADIUS platform	362
Implementing the two-factor software authentication for XenDesktop® 7	374
<u>Index</u>	385

Preface

The year 2013 can be considered as the final consecration of the use of mobile devices as working instruments. This means that companies will not only have standard workers linked to their corporate workstations, but also "road warrior" employees who will need to use their personal smartphones or tablets to check corporate resources outside their offices.

In the era of **BYOD (Bring Your Own Device)**, Citrix® has moved a step forward in this market, powering its desktop and application virtualization platforms and integrating the ability to publish virtual and physical desktops with the capability of assigning applications and contents in a secure manner. XenDesktop® 7 is the union of two historical products developed by Citrix®, XenDesktop®, and XenApp®. As usual, it is offered on most of the available operating system platforms on the market.

In this book, we will discuss the evolution of the XenDesktop® platform. We will discuss how the new mobile-oriented features are implemented and optimized, as well as how the separation of personal data from the company working spaces is achieved using a personal device. Discussing the changes in some historical components, such as the final use of the Citrix® StoreFront platform in substitution of the classical Citrix® Web Interface, is also covered in this book.

After reading this book, the readers will be able to understand how to implement a full XenDesktop® 7 architecture, from its core components to the satellites features. This will permit them to realize a stronger user experience with improved security of personal information.

What this book covers

Chapter 1, XenDesktop® 7 – Upgrading, Installing, and Configuring, discusses in detail the way to upgrade XenDesktop® 7 from the XenDesktop® 5.6 Version for both MCS and PVS architectures. Moreover, we will install and configure the main platform components, such as a database (Microsoft SQL Server 2012 platform), StoreFront, and the licensing services.

Chapter 2, Configuring and Deploying Virtual Machines for XenDesktop®, shows the way to interface XenDesktop® with Hypervisor's hosts for Farm and VM base image creation. All the recipes will be based on the latest releases of the supported hypervisors.

Chapter 3, Master Image Configuration and Tuning, focuses on configuration and optimization operations realized on base desktop, server, or physical workstation images for future deployments.

Chapter 4, User Experience – Planning and Configuring, discusses the way to implement the profile management techniques, the virtual desktop agent versions (Server, Desktop, and Remote PC), and how to provide a better user experience for the customers—including the new HDX mobile offer.

Chapter 5, Configuring Additional Architectural Components, discusses implementation and optimization activities for infrastructural satellite components, such as Citrix® Merchandising Server or the CloudBridge platform.

Chapter 6, Creating and Configuring a Desktop Environment, explains administrative tasks for the desktop environment, such as catalog creation, power management, resource allocation, delivery groups, and the integrated EdgeSight features with the new Director platform.

Chapter 7, Deploying Applications, explains in detail a new way to deploy and migrate applications with the integrated XenApp® platform such as Hosted applications, Local Access App, and Microsoft App-V.

Chapter 8, XenDesktop® Tuning and Security, focuses on performing optimization activities to enrich the quality level of the VDI by using the XenDesktop® policies, the Citrix® NetScaler Gateway, and the Desktop Lock feature.

Chapter 9, Working with XenDesktop® PowerShell, is an advanced guide to XenDesktop® PowerShell modules. With these modules, we'll realize high-level configurations by using the command line.

Chapter 10, Configuring the XenDesktop® Advanced Logon, explains the operations to implement a secure and strong authentication for the Citrix® XenDesktop® 7 architecture.

What you need for this book

The software required to perform component installation are:

- ▶ Windows Server 2008 R2 SP1 (Standard, Enterprise, Datacenter editions) or Windows Server 2012 (Standard, Datacenter editions)
- ▶ Microsoft .NET Framework 3.5 SP1 (only for Windows Server 2008 R2) and Microsoft .NET 4.0
- ▶ SQL Server 2008 R2 SP2 (Express, Standard, Enterprise, Datacenter editions) and SQL Server 2012 SP1 (Express, Standard, Enterprise)

- ▶ Microsoft Internet Information Services (at least 7.0 edition)
- ▶ 100 MB of disk space for the Delivery Controller
- ▶ 75 MB of disk space for the Citrix® Studio component
- ▶ 50 MB of disk space for the licensing and director components

Who this book is for

If you are a system administrator or an experienced IT professional who wants to refer to a centralized container of procedures and advanced tasks in XenDesktop, this is the book for you. If you are an IT technician approaching this technology for the first time and you want to integrate a more theoretical, formative process with step-by-step installation and configuration activities, this book will help you. You will need to have experience of the virtualized environment and an understanding of the general concepts of desktop virtualization.

Conventions

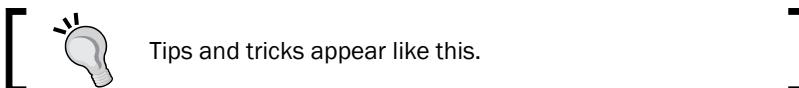
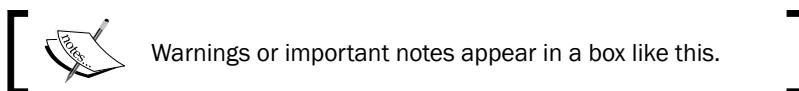
In this book, you will find a number of styles of text that distinguish between the different kinds of information. Here are some examples of these styles, and an explanation of their meaning.

Code words in text, database table names, folder names, filenames, file extensions, pathnames, dummy URLs, user input, and Twitter handles are shown as follows: "To avoid this situation, you have to use the `setspn` command."

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

```
Set-ConfigDBConnection -DBConnection $null  
Set-AcctDBConnection -DBConnection $null  
Set-HypDBConnection -DBConnection $null  
Set-BrokerDBConnection -DBConnection $null
```

New terms and **important words** are shown in bold. Words that you see on the screen, in menus or dialog boxes for example, appear in the text like this: "Accept the **Citrix License Agreement** and click on the **Next** button."



Reader feedback

Feedback from our readers is always welcome. Let us know what you think about this book—what you liked or may have disliked. Reader feedback is important for us to develop titles that you really get the most out of.

To send us general feedback, simply send an e-mail to feedback@packtpub.com, and mention the book title via 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 on 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 would 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 on our website, or added to any list of existing errata, under the Errata section of that title. Any existing errata can be viewed by selecting your title from <http://www.packtpub.com/support>.

Piracy

Piracy of copyright 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

You can contact us at questions@packtpub.com if you are having a problem with any aspect of the book, and we will do our best to address it.

1

XenDesktop® 7 – Upgrading, Installing, and Configuring

In this chapter, we will cover the following recipes:

- ▶ Upgrading from XenDesktop® 5.6 to XenDesktop® 7
- ▶ Preparing the SQL Server 2012 database
- ▶ Installing and configuring the Citrix Licensing Services – 11.11.1
- ▶ Installing XenDesktop® 7 components
- ▶ Installing and configuring StoreFront 2.0
- ▶ Installing and configuring Provisioning Services 7

Introduction

XenDesktop 7 is the new platform realized by Citrix to publish desktop and applications to end users, strongly oriented to the mobile world and the **BYOD (Bring Your Own Device)** way of working. This gives the customer the ability to use their personal devices, with no loss in terms of security and data isolation.

In this chapter, we will discuss the implementation of the **Machine Creation Service (MCS)** and **Provisioning Services (PVS)** architectures. We will discuss about how to upgrade from the XenDesktop Version 5.6 to Version 7 of this platform, including the Provisioning Services 7 component. After this, we will see how to install a XenDesktop 7 infrastructure from scratch, configuring the most important and required components such as the database server, the licensing components, and the new Web access portal for the user's StoreFront 2.0. StoreFront 2.0 is the substitute for the old web interface platform.

The prerequisites to install and configure a full functioning Citrix XenDesktop 7 architecture are given as follows:

- ▶ Operating Systems such as Windows Server 2008 R2 SP1 (Standard Edition, Enterprise Edition, Datacenter) and Windows Server 2012 (Standard Edition, Datacenter) are supported.



For the Citrix Studio and the Virtual Delivery Agent, Windows 8 and Windows 7 (Professional and Enterprise) are also supported as operating systems. With the XenDesktop 7.1 version, which was released at the time of writing this book, Windows 8.1 and Windows Server 2012 R2 operating systems are also supported.

- ▶ Microsoft .NET Framework 3.5 SP1 (Windows Server 2008 R2), Microsoft .NET Framework 4.0.
- ▶ Windows PowerShell 2.0 (included in Windows Server 2008 R2), Windows PowerShell 3.0 (included in Windows Server 2012).
- ▶ At least 100 MB disk space is required for the Delivery Controller, at least 75MB for the Studio platform, at least 50 MB for the Citrix Director, and at least 40 MB for the License Server.
- ▶ At least **Microsoft Internet Information Services (IIS)** 7.0 version is required as the web or application server.

IT professionals or users can choose between two architectural implementations: MCS (which consists of hosted desktops and applications published to users based on given accessibility permissions) and PVS (which consist of a single desktop, or a pool of them, booted over a network and streamed on demand to end users).

In both cases, information is stored in a Citrix database repository, which is based on the Microsoft SQL Server. It's used and populated with data coming from the main architectural components. In this book, we will discuss all of them in detail.



With XenDesktop 7, you can deliver both desktop and server operating system images, virtually or physically, thanks to the union with the XenApp platform.

Configured resources such as virtual desktops can be accessed by end users through a web portal called **StoreFront**, the substitute for the old Citrix Web Interface, that permits publishing of online stores with the applications and the desktops that are published to the end users.

MCS and PVS architectures can be combined and used within the same company for different desktop distribution areas. This is the implementation of the **Citrix Flexcast** technique. It is a methodology which applies different Citrix products and configurations together, based on the requirements of specific company areas or customized architectures for specific teams.



For a number of delivered virtual desktops nearer to or greater than 500, you should always consider using the PVS architecture in order to avoid global performance and maintenance issues.



The main goal of this recipe is to help you understand the differences between the two main kinds of architectures: MCS and PVS. Once you've understood this, you'll be able to better comprehend what to implement and how to implement a consistent and coherent XenDesktop installation.

Starting from the database server and licensing configuration, we'll walk through XenDesktop components, StoreFront, and the complex configuration of provisioning service architecture in this chapter.

The first implementable architecture type is MCS. Its most important part is based on hosted virtual desktops.

How can we choose if MCS is the better solution for us? We've a set of main parameters that will help us decide:

- ▶ MCS is the right solution only if we want to deploy only a virtualized desktop infrastructure, both client and server operating systems.
- ▶ We should choose MCS when the number of deployed desktops is lower than 500.
- ▶ It should be better to use MCS when we need to frequently upgrade base images. Despite the complexity of the operations required with the use of the PVS architecture, it is quite a simple process in terms of operations for the machine creation platforms.



The cons for the MCS configuration are as follows: I/O intensive, more storage per single VM despite the PVS infrastructure, and higher time to update images in the case of an elevated number of desktops.



- ▶ Consider implementing this architecture when you have a shared storage like **NFS (Network File System)** or **SAN(Storage Area Network)**; especially in the second case, it's preferable to have MCS architecture, thanks to its large IOPS capacity.

To implement a pure MCS architecture, you will need the following XenDesktop components:

- ▶ Director
- ▶ Delivery Controller
- ▶ Studio
- ▶ StoreFront
- ▶ Licensing Service



Even if not explicitly specified, you need a Hypervisor platform to create the virtualized resources.



The second kind of XenDesktop infrastructure is **PVS**, a Citrix implementation that is fully based on desktop streaming technology.

PVS is the right choice in the following cases:

- ▶ When you need to provide users with not only hosted desktops, but also streamed workstations.
- ▶ In case of physical machines, PVS is the only available solution.
- ▶ When we have more than one site, with a number of desktops per location between 500 and 2,500 per PVS server.
- ▶ When we don't have a shared storage, or we're in the situation of a low performance data area. In this case, we'll take advantage of the PVS memory caching activity.
- ▶ When we have a lot of users logging on or logging off simultaneously, it is known as an I/O **boot storm** phenomenon. If we choose PVS, we could avoid this problem by bypassing the storage constraints.



The cons for the PVS infrastructure are given as follows: possible network boot storm, and network traffic has to be separated and isolated from the company network traffic to avoid bottlenecks.



To implement PVS instead of MCS, you must configure these components in your architecture:

- ▶ Director
- ▶ Delivery Controller
- ▶ Studio
- ▶ StoreFront
- ▶ Licensing Services
- ▶ Citrix Provisioning Services



You should consider combining MCS and PVS, especially in the cases where your architecture has the right balance of RAM quantity and storage performance. This is what Citrix calls the **Flexcast approach**, a way of combining the different architectures to satisfy all the requirements for a set of different end user topologies.

Upgrading from XenDesktop® 5.6 to XenDesktop® 7

If you have got an already existing and configured XenDesktop 5.6 site, you have the ability to upgrade it to this latest release of the platform. In this recipe, we will discuss in detail all the steps required to perform a fully functioning migration while being careful to lose no production data.



If you are using the XenDesktop Express edition, you cannot upgrade the platform. You have to obtain a valid nonexpress license to proceed with the upgrade process.

Getting ready

You can perform a direct upgrade to XenDesktop 7 from one of the following XenDesktop components versions:

- ▶ Virtual Desktop Agent (5.0 SP1, 5.5, 5.6, 5.6 FP1) to the Virtual Delivery Agents 7
- ▶ Controller (5.0, 5.0 SP1, 5.5, 5.6, 5.6 FP1) to the Delivery Controller 7
- ▶ Director (1.0, 1.1, 2.0, 2.1) to the Citrix Director 7

Before starting the upgrade process, be sure you have considered the following points:

- ▶ In the presence of a single Desktop Controller, this will be unavailable during the upgrading process.
- ▶ Be sure that all the users have been logged off by the involved desktop resources.
- ▶ Be sure that you have backed up the system critical components, such as database and controller platforms.
- ▶ If using the Citrix NetScaler platform, make sure that your running version is compatible with the XenDesktop 7 platform.

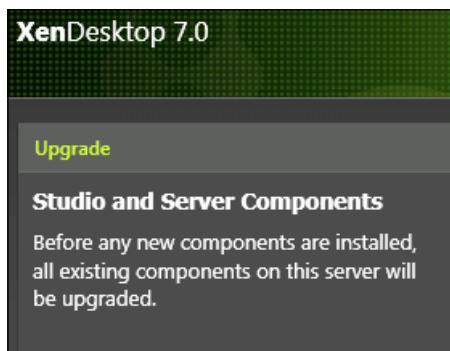
How to do it...

To perform a correct and functioning XenDesktop resources upgrade, you have to execute the following steps in the right order:

1. Connect to your XenDesktop 5.6 License Server machine with the domain and XenDesktop administrative credentials.
2. After downloading the ISO file from your personal Citrix account, burn it or mount it as a virtual CD (if performing the installation with a virtual machine, for example).
3. Double-click on the **AutoSelect** executable file on the installation media.
4. In the XenDesktop 7 welcome screen, click on the **Start** button to proceed.

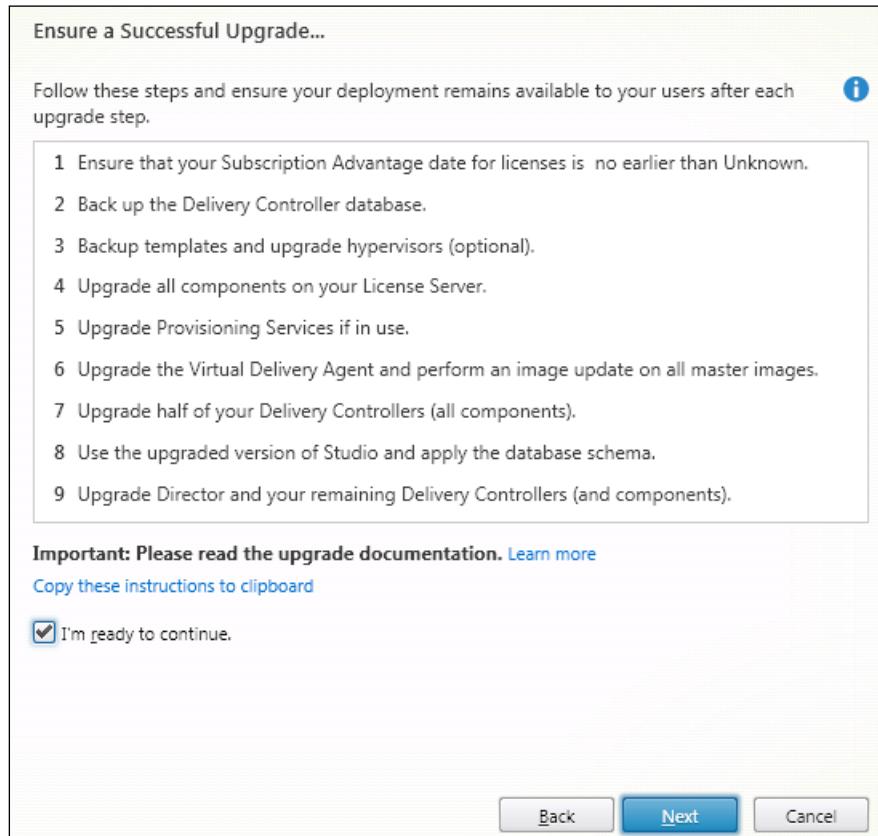


5. In the XenDesktop 7.0 installation menu, click on the **Upgrade | Studio and Server Components** section.



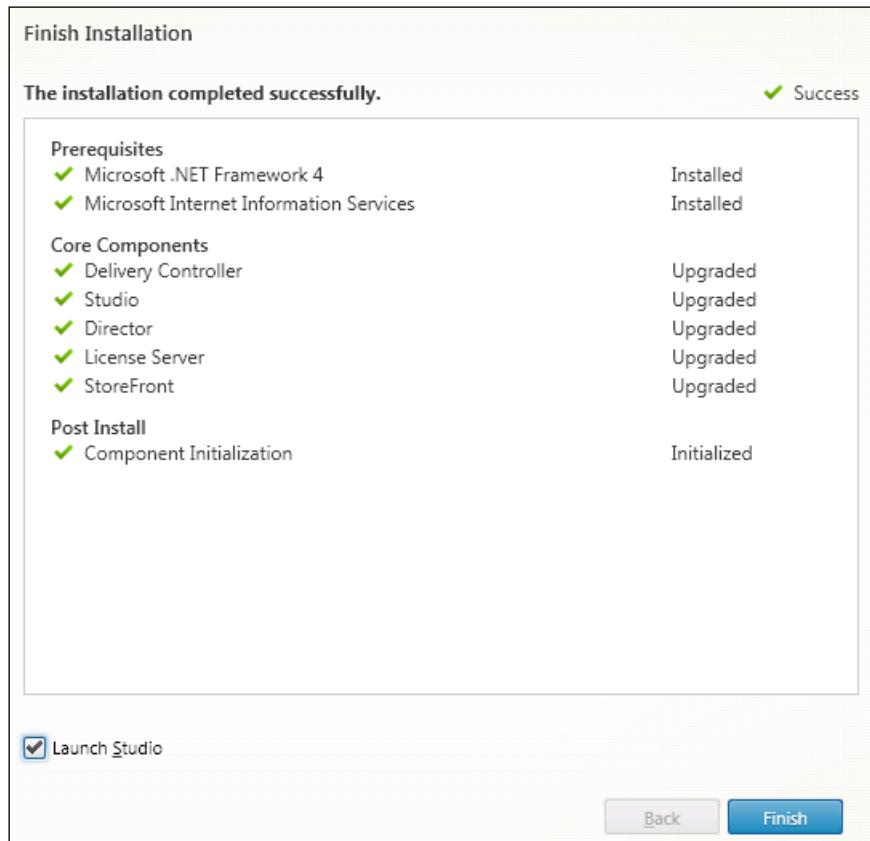
6. Accept the **Software License Agreement** and click on the **Next** button.

7. Carefully read the **Ensure a Successful Upgrade...** tasks list. Then flag the **I'm ready to continue** option and click on **Next**.



8. In the **Firewall** section, let XenDesktop configure the required firewall exceptions by selecting the **Automatically** radio button. Then click on **Next** to continue.
9. In the **Summary** screen, if all the information are correct, click on the **Upgrade** button to proceed.

10. After completing the preceding steps, in case of a positive upgrade you will see a screen as shown in the following screenshot. Flag the **Launch Studio** option and click on the **Finish** button.

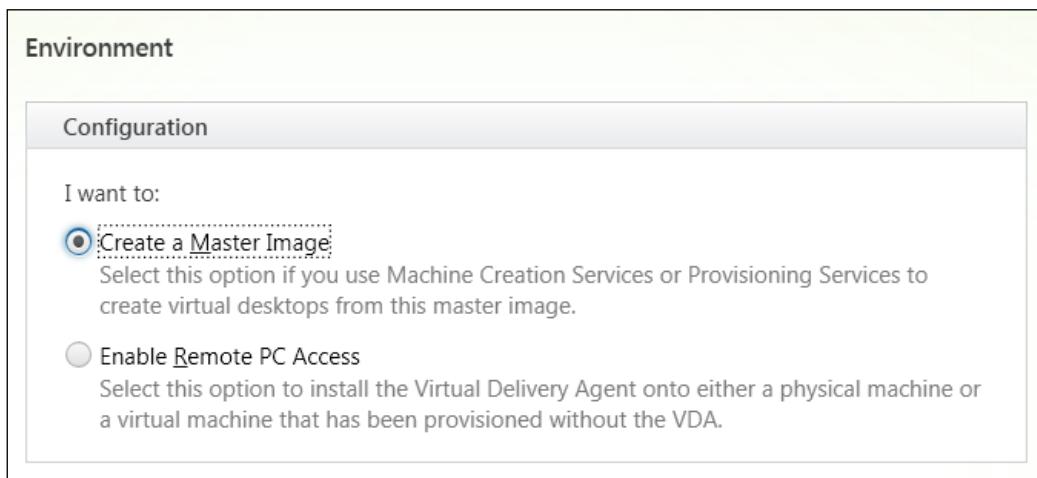


11. After you've started the **Studio** console, you have to upgrade the existing site configured for XenDesktop 5.6 and the relative database. In the **Mandatory upgrade** page, click on the **Start the Site upgrade automatically** option.
12. When required, flag the **I am ready to upgrade** option and click on **Next**.
13. At the end of the procedure (the **Site Upgrade Complete** screen), click on the **Finish** button.
14. In the **Upgrade Successful** section, select the **Finish upgrade and return to the Site overview** option to come back to the **Studio** console.

If you want, you can manually update the database component by running the following PowerShell and SQL scripts in the indicated order within the specified environment:

`DisableServices.ps1`: XenDesktop controller
`UpgradeDatabase.sql`: DB Server with SQL Server Management Studio
`EnableServices.ps1`: XenDesktop controller

15. The last operation is upgrading the VDA component on the instance machines. To perform this, select the **Virtual Delivery Agent for Windows Desktop OS** option from the installation menu.
16. In the **Environment** section, select **Create a Master Image** and click on **Next**. We will discuss the **Remote PC Access** later in this book.



17. In the **Firewall** screen, configure the firewall rules **Automatically**. Then, click on **Next** to continue.
18. If the information in the **Summary** screen are correct, click on the **Upgrade** button to proceed with the VDA upgrade activities.
19. At the end of the installation procedure, click on the **Finish** button to complete the entire infrastructure upgrade task.

How it works...

The process we have illustrated is known as an in-place upgrade procedure. This is a kind of upgrade procedure based on the evolution of an already installed and running system to a newer version; this is the only way to perform the upgrade from XenDesktop 5.6 to XenDesktop 7.



In the presence of a XenDesktop 4.x architecture, the operation will not be based on an upgrade in-place procedure, but will be in the form of a platform migration.

The steps required to successfully complete the procedure are given as follows:

1. Upgrade the **License Server** platform.
2. Upgrade the **Provisioning Services** platform.



If you want to maintain a hybrid infrastructure with both XenDesktop 5.6 and XenDesktop 7, you don't have to upgrade the **Provisioning Services** to version 7.

3. Upgrade the installed client agents, both for MCS (VDA) and PVS.
4. Upgrade the Controller components.
5. Manually/automatically upgrade the XenDesktop 5.6 database.



Before running the database upgrade, you should consider creating a backup of your data in order to avoid unexpected loss of data.

After verifying all the prerequisites, we have started the XenDesktop 7 installation setup from the resource media. At this point, we have selected the platform installation option by upgrading the existing XenDesktop 5.6 systems. The procedure flow goes on automatically, upgrading all or part of the components installed on the machine on which you are running the procedure. Next, the most important operation in this procedure is upgrading the existing site, including its database. This operation can be performed in two ways: automatically, by using the Citrix Studio GUI and selecting the upgrade site option; or manually, by executing already generated scripts (PowerShell plus SQL) which directly operate on the Citrix services and data repository. These scripts can be generated by choosing the **Manually upgrade this site** option in the Citrix Studio console's **Mandatory upgrade** section.

At the end, you have to upgrade the template image and client's components, such as Virtual Delivery Agent and Citrix Receiver. Also, in this case, the procedure is based on the automatic upgrade allowed by the Citrix XenDesktop setup agent, which detects the presence of an installed agent on the target machine and performs an upgrade operation instead of a normal installation task.

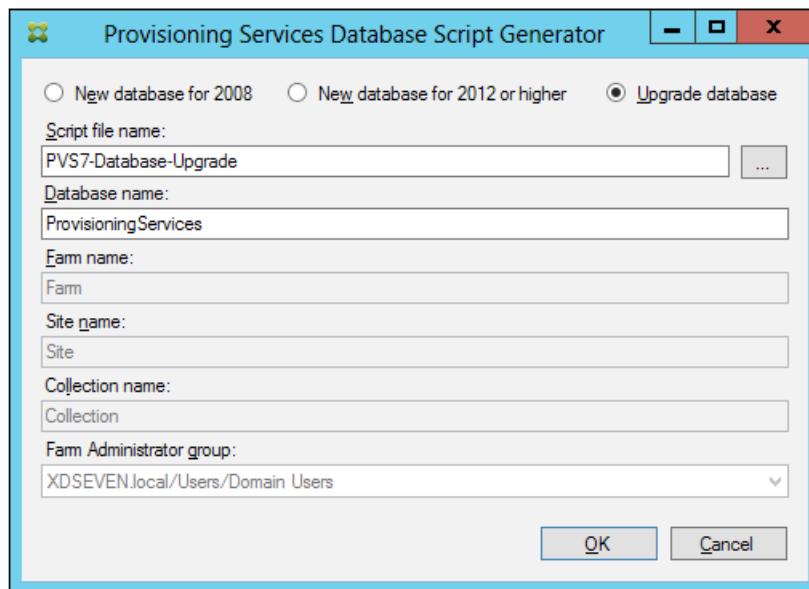
There's more...

In case you decide not to have more XenDesktop 5.6 components within your infrastructures, it is important to upgrade the Provisioning Services component.

Despite the illustrated procedure for the XenDesktop core components, PVS requires you to completely uninstall all the software components on the infrastructural server, and then reinstall them at this latest release. At this point, the only thing you have to do is select the **Join a farm that is already configured** option.

The database upgrade part requires more attention. This can be performed by using the PVS GUI, or by running a specific GUI tool.

This is the `dbscript.exe` utility, which is located under the default installation path (in our case the path is: `C:\Program Files\Citrix\Provisioning Services`). In order to generate an upgrading database script, you have to choose the **Upgrade database** option in the software GUI, then you have to assign a name to the script you're going to generate, and at the end select the PVS database name that you want to upgrade. Now, click on the **OK** button, as shown in the following screenshot. You are now ready to perform the database upgrade task by running the script on the appropriate database server.



See also

- ▶ The *Configuring a target device – PVS architecture* recipe in *Chapter 3, Master Image Configuration and Tuning*

Preparing the SQL Server 2012 database

The evolution of the XenDesktop platform is not only in terms of the Citrix core components, but also for collateral technologies that are used to implement a virtualized architecture. For this reason, we have decided to implement all the latest releases of the software required by XenDesktop 7. This is also the case for the database component that will be installed and configured on the Microsoft SQL Server 2012 edition in this recipe.

Getting ready

Citrix XenDesktop 7 supports the following versions of Microsoft SQL Server:

- ▶ SQL Server 2008 R2 SP2 (Express, Standard, Enterprise, and Datacenter editions)
- ▶ SQL Server 2012 SP1 (Express, Standard, and Enterprise editions)

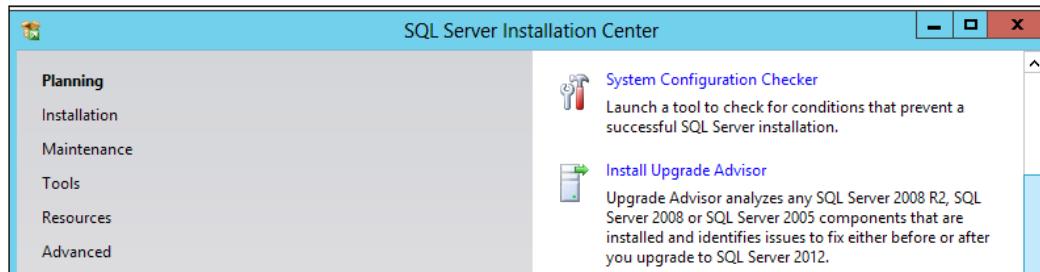
How can we choose the right database version? It depends on what level of performance and availability is needed. For standalone installations (integrated with the XenDesktop Controller server) within a test or POC environment, Express edition should be the right choice. In the case of a huge number of clients and users, if you want to create a clustered database instance, you should implement the non-Express version of SQL Server.

For a separate database installation, we need to perform the common installation operations, as explained in the following section.

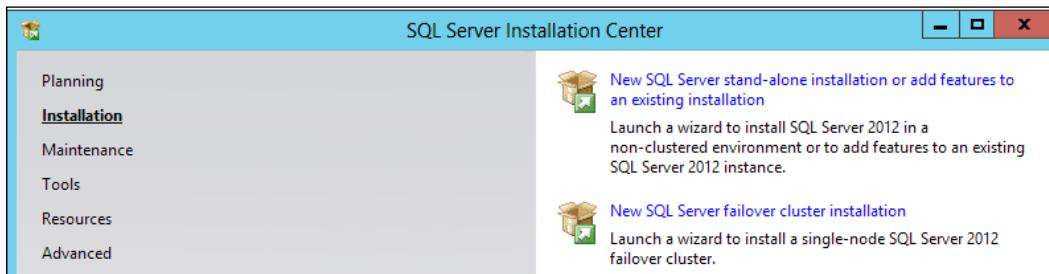
How to do it...

Perform the following steps to generate SQL Server Database, which will be used by XenDesktop:

1. From the SQL Server installation media, launch the executable setup file.
2. If you want, you can launch **System Configuration Checker** from the **Planning** section to perform a pre-installation test and verify that all the requirements are met.



3. Click on the **Installation** tab, which you can see in the left-hand side menu, and select **New SQL Server stand-alone installation or add features to an existing installation**. In this book, we won't execute all the steps required to complete the database installation:



4. If you've got available resources, you can choose to create a new named instance instead of using the default SQL Server instance (MSSQLSERVER).
5. On the database server, create a database on the desired instance (preferably having a dedicated instance for Citrix, as seen previously) with the following parameters:
 1. Create a new database instance on the database server, setting the parameter **Collation sequence** to **Latin1_General_CI_AS_KS**.
 2. Configure the authentication method as only Windows authentication.
 3. Configure the **Permissions** settings, as shown in the following table:

Activity	Server role	Database role
Database creation	dbcreator	
Schema creation	securityadmin	db_owner
Controller addition	securityadmin	db_owner
Controller removal		db_owner
Schema update		db_owner

6. This permission will be granted to the operating system user, who will perform configuration activities through XenDesktop.

[ Using a separate instance is not mandatory, but it is better (more isolation, more security).]

How it works...

We've configured the most common format for the collation sequences (the same used by Citrix) and also restricted the way to log on to the database at Windows authentication because XenDesktop does not support SQL or Mixed mode. For the collation, you are free to use the indicated version. But, the most important thing is that you will choose one that is a member of the *_CI_AS_KS category (collation family is case and accent insensitive, but kanatype sensitive).

You must be careful when increasing the size of database logging. Despite the normal data component (you should expect to have a database size of 250 MB with some thousands of clients), logs could unexpectedly increase in 24 hours in the case of thousands of desktops. Based on the following table for MCS architectures, we'll be able to calculate the database log and data files occupation:

Component	Data/log	Occupation
Registration information	Data	2.9 KB per desktop
Session state	Data	5.1 KB per desktop
Active Directory computer account info	Data	1.8 KB per desktop
MCS machine info	Data	1.94 KB per desktop
Transaction log for idle desktop	Log	62 KB per hour



For a more detailed SQL Server installation, please refer to official Microsoft online documentation at <http://msdn.microsoft.com/en-us/library/ms143219.aspx>.

There's more...

In case it is necessary to redeploy one or more Desktop Delivery Controller servers configured in your VDI infrastructure, the first step is to clean the Citrix XenDesktop-configured database. To perform this task, you have to set all the Citrix components' database connection to null by using the custom Citrix PowerShell and running the following commands:

```
Set-ConfigDBConnection -DBConnection $null
Set-AcctDBConnection -DBConnection $null
Set-HypDBConnection -DBConnection $null
Set-BrokerDBConnection -DBConnection $null
```

Once you've finished these operations, you can proceed with the manual deletion and recreation of the SQL Server database.



Later in this book, we will explain how to use the Citrix PowerShell cmdlets available with XenDesktop 7.



See also

- ▶ The *Retrieving system information – Configuration Service cmdlets* recipe in the Chapter 9, *Working with XenDesktop® PowerShell*

Installing and configuring the Citrix Licensing Services – 11.11.1

The new XenDesktop platform also includes the licensing component. The advantage of this agent is that it allows the customers to naturally convert their existing licenses to the XenDesktop 7 platforms without any additional effort in terms of money and work. In this recipe, we will discuss how to allocate licenses in this latest License Server version.

Citrix permits the users to buy XenDesktop in different versions, as given in the following list:

- ▶ Citrix XenDesktop Express Edition, which is a free edition that allows you to test the platform without any cost and has the ability to publish up to 10 desktops
- ▶ Citrix XenDesktop VDI Edition
- ▶ Citrix XenDesktop Enterprise Edition
- ▶ Citrix XenDesktop Platinum Edition

The choice is based on personal needs. In this book, when we refer to XenDesktop 7, it will be the Platinum Edition. It has the ability to show and implement the full functionality of the platform.

Getting ready

The associated version of the license server for XenDesktop 7 is Version 11.11.1.

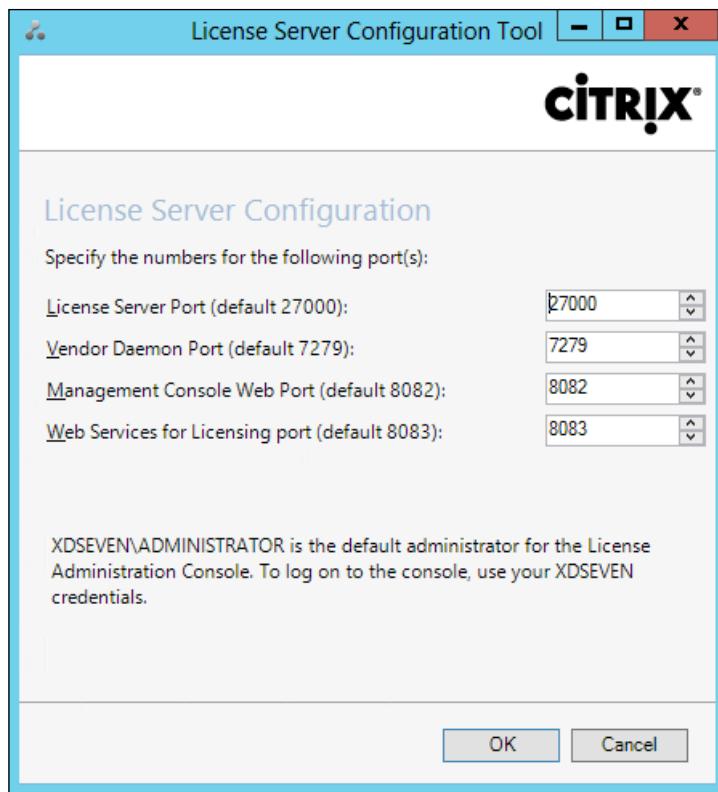
System requirements for the latest version of the License Server are as follows:

- ▶ Windows Server 2008, 2008 R2, or Windows Server 2012 version; alternatively, you can also use Windows 7 and Windows 8 (both 32 or 64 bits)
- ▶ 50 MB for licensing components and 2 GB for user and/or device licenses
- ▶ .NET Framework 3.5
- ▶ A compatible browser

How to do it...

In this section, we are going to perform the operations required for the Citrix license server installation and configuration, based on the Windows Server 2012 operating system platform:

1. After downloading the XenDesktop 7 installation media from your personal Citrix account, run the **CTX_Licensing.msi** installer that is located under the installation media path **x64\Licensing**.
2. Accept the **Citrix License Agreement** and click on the **Next** button.
3. Select a destination folder's path for the program as default; we selected: **C:\Program Files (x86)\Citrix**. Then, click on the **Install** button.
4. Click on the **Finish** button when the license server is successfully installed.
5. On the first configuration screen, you must assign the port numbers for the **License Server Port**, **Vendor Daemon Port**, **Management Console Web Port**, and **Web Services for Licensing port** fields, as shown in the following screenshot. Then, click on the **OK** button.

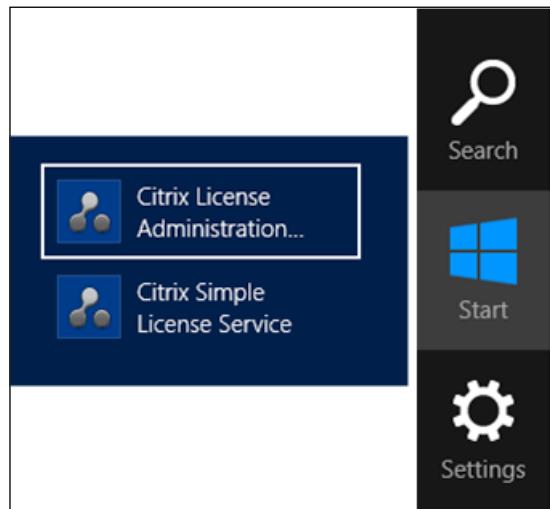


6. You can decide to leave default ports for these three options, or change them. In any case, the ports you decide to use must be opened on the Windows Server's personal firewall.
7. To generate the license file that will be imported to our license server, run a Web browser installed on your client machine, connect to www.citrix.com/MyCitrix, and log in using your credentials.
8. Go to **Activate and Allocate Licenses**.
9. Click on **Allocate licenses**.
10. Insert the **Full Qualified Domain Name (FQDN)** of your license server, and select the number of licenses you want to allocate.
11. Generate the license file by clicking on the **Allocate** button.
12. Now, you'll be able to save the file. When prompted for the location, select the path on which the license manager will read the file with the .lic extension as C:\Program Files (x86)\Citrix\Licensing\MyFiles.

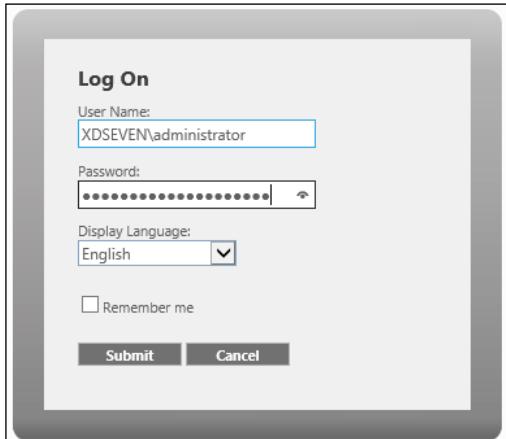


The XenDesktop license server is case sensitive. Be careful when you insert the server FQDN. You've got to respect all uppercase and lowercase characters.

13. To configure the license server, search for the link **Citrix License Administration Console** (using the Windows + C key combination or by clicking on the **Search** icon), and then click on it.

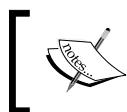


14. You'll see the summary dashboard. Click on the **Administration** button and insert the administrative credentials for your machine (domain or local admin account).



15. After a quick look in the **Summary** tab, click on the **User Configuration** button on the left-hand side menu.
16. Add a new user account to differentiate from the standard administrative machine credentials. We can decide to create this account as **Locally Managed Admin**, **Domain Administrator**, or **Domain Administrator Group**. After these operations, click on **Save**.





You can decide to force the user to change his/her password on next logon by enabling the relative flag, as showed in the earlier picture.



17. Now it's time to configure the alerts. Depending on our needs, we can set up the critical and important alerts. It's preferable to leave them as default settings, and click on **Save** to archive the options.



You should take care of the following licensing alerts: **Out of activatable licenses**, **Out of concurrent license**, and **Concurrent license expired**.



18. In the **Server Configuration** menu, configure the port for the web server (default is **8082**) and session timeout period (default is 30 minutes, but you should try to reduce this value so that you can avoid inactive sessions that are locking unused resources). For security reasons, it's a good practice to enable SSL (port 443) and eventually use a personal certificate for strong authentication (as shown in next screenshot).
19. The available port range on which configuring the License Server is from 27000 to 27009; the default port is 27000.

Server Configuration

Web Server Configuration

Secure Web Server Configuration

Enable HTTPS (Default 443)

*HTTPS Port:

*Certificate File:

*Certificate Key File:

Certificate Chain File:

Redirect non-secure web access to secure web access

License Server Configuration

Logging

User Interface

20. The most important part is at the end—**Vendor Daemon Configuration**. After that the license file has been generated; click on **Import License**, browse for the file location, and upload it by clicking on the **Import License** button.
21. If everything is OK, you'll receive a confirmation message about the success of the loading operation.
22. Click on **Vendor Daemon** (in our case, the default daemon is called **Citrix**) and click on **Reread license file** to make sure that everything's correct.



Never manually edit the license file! If vendor daemon configuration returns an error, probably you have to reallocate licenses and regenerate files, but don't correct it with any text editor.



How it works...

The XenDesktop license file is generated in the personal area on the MyCitrix Web portal. When you generate a .lic file, it must be generated and registered with the FQDN of the license server on which you're going to use the file. This means that if you need to reinstall the server or change its name, you must reallocate the license currently assigned and reassign it to the new server, always referring to its FQDN. The license file must be regenerated and reimporrted, as seen previously.



If using XenDesktop for test purposes, or in the case of a License Server's fault, Citrix gives you a grace period of 30 days.



There's more...

It's also possible to install the License Server from the command line by using the Windows command `msiexec` with the following parameters:

- ▶ `/I`: This is the installation option.
- ▶ `/qn`: This is for a silent installation.
- ▶ `INSTALLDIR`: This is used to specify the path of the installation folder (if not specified, the default one for a 64-bit system is `C:\Program files\Citrix\Licensing`, or `C:\Program files (x86)\Citrix\Licensing` for a 32-bit system).
- ▶ `LICSERVERPORT`: The License Server will listen to this port for connections (default is 27000).
- ▶ `ADMINPASS`: This is the administrative password for the user admin on the licensing console. In the presence of an active directory, you have to use the administrative domain credentials.

- ▶ **VENDORDAEMONPORT:** This is the port of the vendor daemon component (default is 7279).
- ▶ **MNGMTCONSOLEWEBPORT:** This is the administrative license console port (default is 8082).

So, for example, if we would install Licensing in a silent way by using the **LICSERVER** folder on port 27004 and assigning **TestCase01** as the administrative password, the following string needs to be run:

```
msiexec /I ctx_licensing.msi /qn INSTALLDIR=C:\LICSERVER  
LICSERVERPORT=27004 ADMINPASS=TestCase01
```

See also

- ▶ The *Managing the Citrix® Desktop Controller and its resources – Broker and AppV cmdlets* recipe in Chapter 9, *Working with XenDesktop® PowerShell*

Installing XenDesktop® 7 components

After discussing how to upgrade from the older version of XenDesktop and implementing the database and licensing components, it's time to install and configure all the XenDesktop 7 core components from scratch.

Getting ready

In order to install all the necessary components, you need to have domain administrative credentials on the server machine(s) on which you are going to implement your infrastructure.

How to do it...

The following are the steps by which we will perform the installation of the core components of the XenDesktop platform, including the Desktop Delivery Controller:

1. After downloading the ISO file from your personal Citrix account, burn it or mount it as a virtual CD (if performing the installation with a virtual machine, for example).

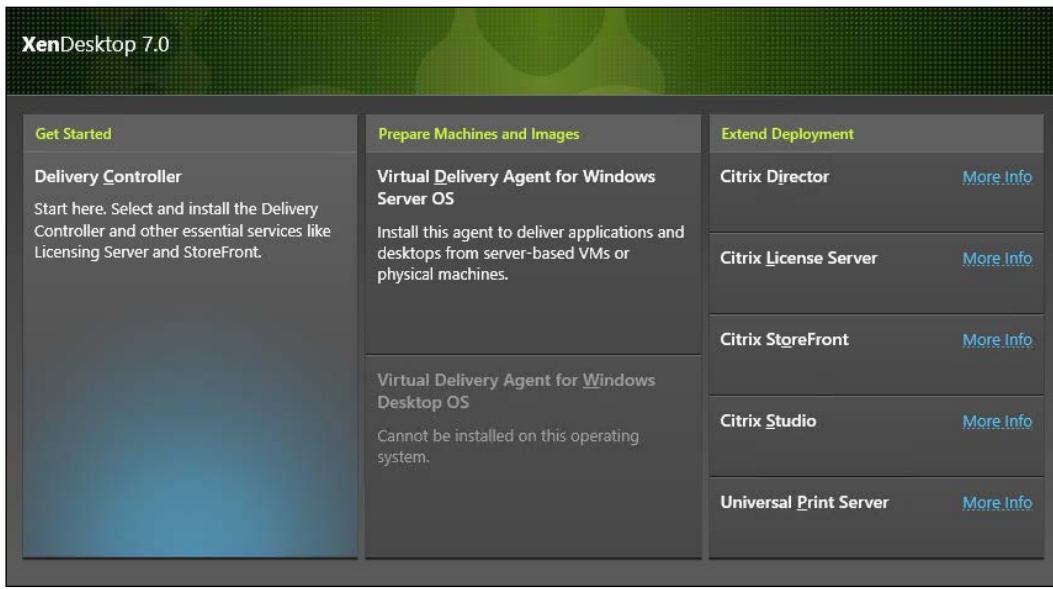


On Windows Server 2012 / Windows 8, you can directly mount the ISO within the operating system by right-clicking it and selecting the **Mount** option.

2. Double-click on the CD-ROM icon or browse the mounted media, and run the **AutoSelect.exe** file. Then, launch the XenDesktop installation by clicking on the **Start** button in the welcome screen, as shown in the following screenshot:

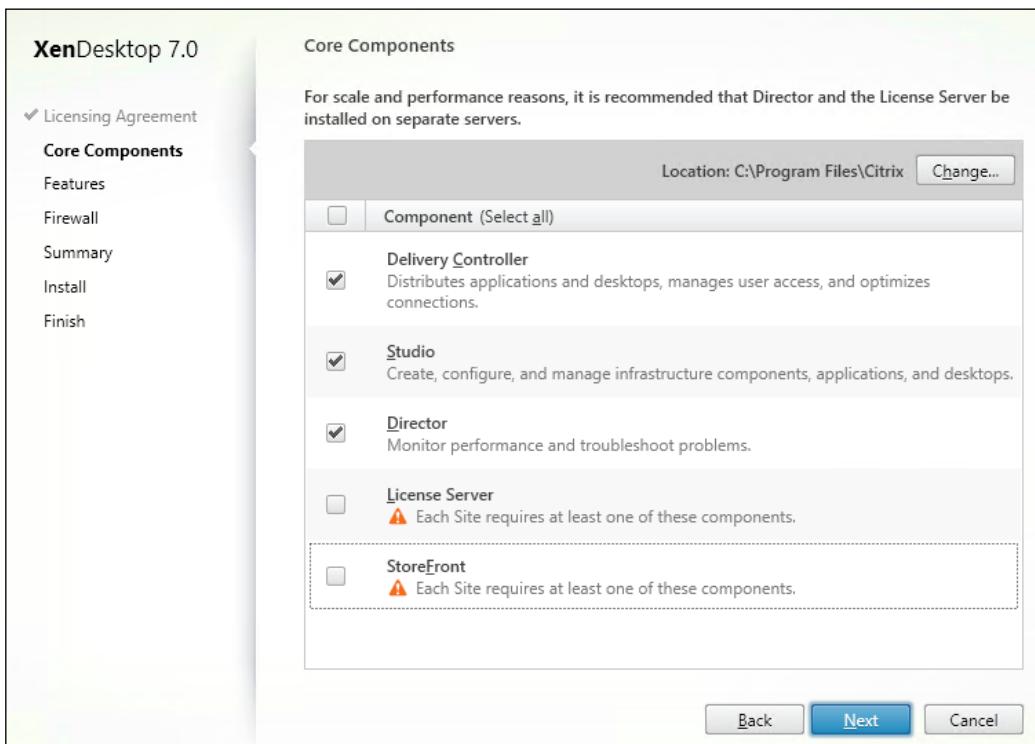


3. In the installation menu screen, click on the **Get Started** section button to proceed with the setup procedure.

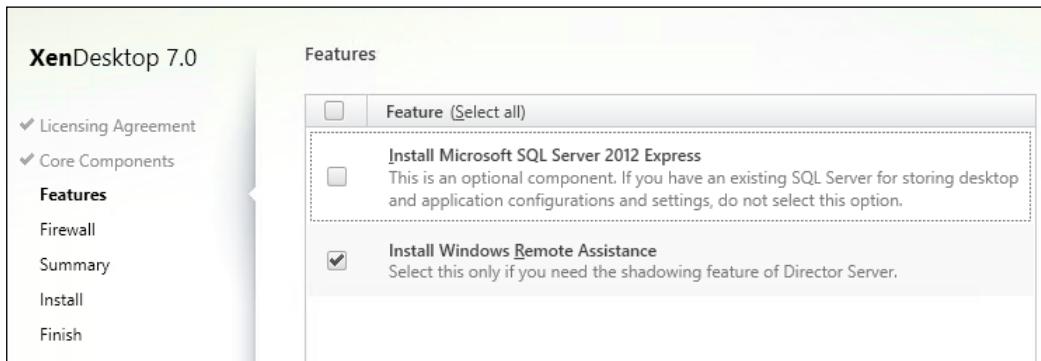


4. After the setup initialization, accept the licensing agreement, then click on the **Next** button.
5. At this point, select the components that we need to install (**Delivery Controller**, **Studio**, and **Director**).
6. It's also possible to change the installation folder by clicking on the **Change** button on the top-right of the screen. If the path is correct, click on the **Next** button to proceed with the installation.

 Don't check both the **License Server** and **StoreFront** options. The first has already been installed on a separate server, and the second will be explained and configured in the next recipe.



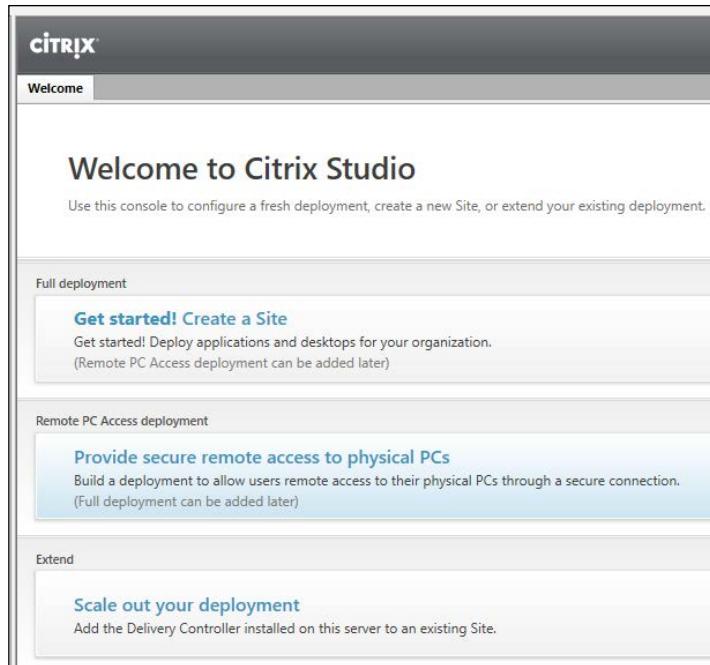
7. In the **Features** screen, you have to select the **Install Windows Remote Assistance** option. In case you do not need to use a full SQL Server version, also select the **Install Microsoft SQL Server 2012 Express** choice option. Click on **Next** to proceed.



8. In the **Firewall** section, you can let XenDesktop automatically open the required network ports on the Windows firewall (**TCP 80/443**), or you can operate on it manually. After this, click on **Next** to continue.

The screenshot shows the 'Firewall' configuration screen. At the top, it says 'The default ports are listed below.' and has a 'Printable version' link. Below this is a table with two columns: 'Delivery Controller' and 'Director'. Under 'Delivery Controller', it lists '80 TCP' and '443 TCP'. Under 'Director', it lists '80, 443 TCP'. At the bottom, there's a section titled 'Configure firewall rules:' with two radio button options: 'Automatically' (selected) and 'Manually'. The 'Automatically' option is described as creating rules in the Windows Firewall even if it's turned off. The 'Manually' option is described as for users not using Windows Firewall or wanting to create rules themselves.

9. You'll be presented with the **Summary** window. If you agree with the summary details, click on the **Install** button to proceed.
10. At the end of installation, leave the **Launch Studio** checkbox checked in order to verify the correct execution of the installed platform:



How it works...

XenDesktop 7 can be considered the most complete and advanced version of this software. In fact, it combines the consolidated XenDesktop 5.6 architecture with the XenApp platform, permitting end users to manage all the necessary deployments from a single management point (desktop OS, server OS, physical machines remote access, or published applications).

Users access their resources by using the Citrix Receiver that is installed on the device from which they have established the connection. The Receiver points to the configured store within the StoreFront platform, which can be considered a stronger evolution of the Citrix Web Interface—an infrastructural component that has been deprecated in this release. The delivery of all the resources is managed by the Delivery Controller component, also known as Broker, which regulates the association between the users and their resources. Once this task has been accomplished, the broker stops its intermediary channel activities, and a direct communication is established between the user's physical workstation and the requested desktop or application.

There's more...

With the release of the Citrix XenDesktop 7 platform, the software activation procedure interacts with KMS, thanks to the ability to use a Microsoft KMS Server to release licenses for the operating systems and the Microsoft Office suites installed on the virtual desktops. This permits a better management of the licensing, especially for those environments that are configured in a nonpersistent way, that is, any deployed desktop asks for a license activation code in a unique way, allowing the Microsoft KMS Server to identify any instance as a separate object.



KMS server can be used only with the MCS architecture.

See also

- ▶ The *Configuring a Desktop OS master image* recipe in *Chapter 3, Master Image Configuration and Tuning*

Installing and configuring StoreFront 2.0

The most evident change in XenDesktop 7 is the absence of the Web Interface portal for the users to access their own contents (desktop or applications). This historical component has been now substituted by the StoreFront platform, which with the 2.0 release has been improved to be able to become the final access resource portal. In this recipe we will discuss how to install and configure it, to allow the users to be able to access their published resources.

Getting ready

StoreFront can be installed on both Windows Server 2008 R2 SP2 (Standard, Enterprise and Datacenter editions) and Windows Server 2012 (Standard and Datacenter Editions).

The following ports need to be opened on the firewalls within your network:

- ▶ TCP ports 80 and 443, in order to access the StoreFront Web Portal
- ▶ TCP port 808, which is used to intercommunicate between the StoreFront servers
- ▶ TCP port 8008, which is used by the Citrix Receiver to communicate with the HTML5 portable version

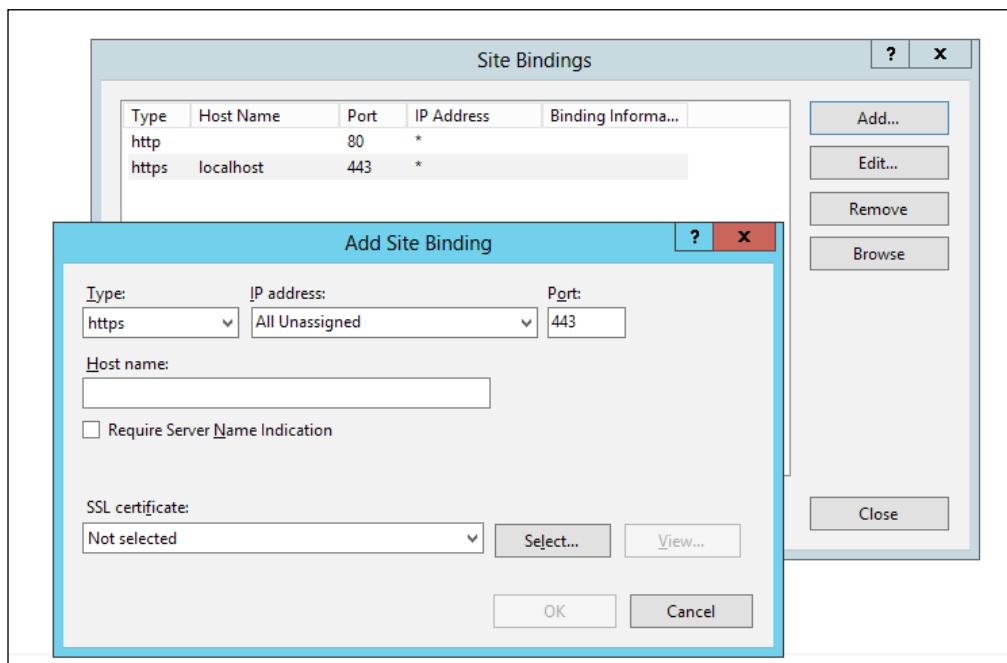
Moreover, you need to configure the IIS role (Web Server) on the Windows Server machine dedicated to StoreFront.



To speed up the StoreFront home page loading and solve the slow loading issue, you can refer to the following Citrix article: <http://support.citrix.com/article/CTX117273>



After this configuration is completed, remember to bind the IIS Web Server address to the HTTPS connection by clicking on the **Bindings** link in the right-hand side menu of the IIS control panel—**Default Web Site** view.



Be sure that you are installing the software on a domain-joined machine within the same forest of XenDesktop components that were installed earlier, and check that the Windows Firewall is up and running. Otherwise, StoreFront won't function.



The Windows Firewall requirement is a StoreFront 2.0 known issue.
This has been fixed in the StoreFront Version 2.1.



How to do it...

The steps required to install and configure the StoreFront 2.0 platform are given as follows:

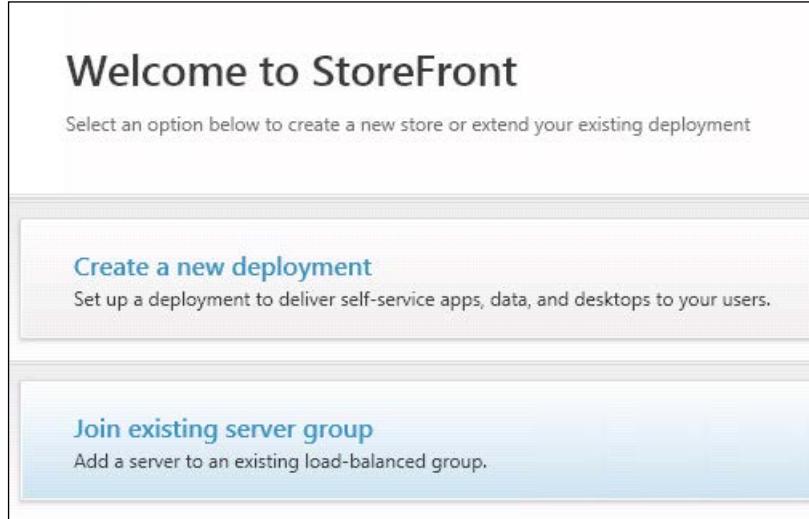
1. After downloading the software from your personal Citrix account, run the CitrixStoreFront-x64.exe installer that is located under the following installation media path: x64\StoreFront.



In the case of a Windows 2008 R2 environment, you will be prompted to install the .NET 3.5.1 framework.



2. Accept the **Citrix StoreFront License Agreement** and click on the **Next** button.
3. Accept to install the missing Web Server IIS components, and click on **Next** to continue.
4. After all the required components have been installed, click on the **Install** button on the **Ready to Install** screen to proceed.
5. After the installation is completed, click on **Finish** to automatically start the StoreFront administration console.
6. After the console has been opened, click on the **Create a new deployment** button in the StoreFront main menu.

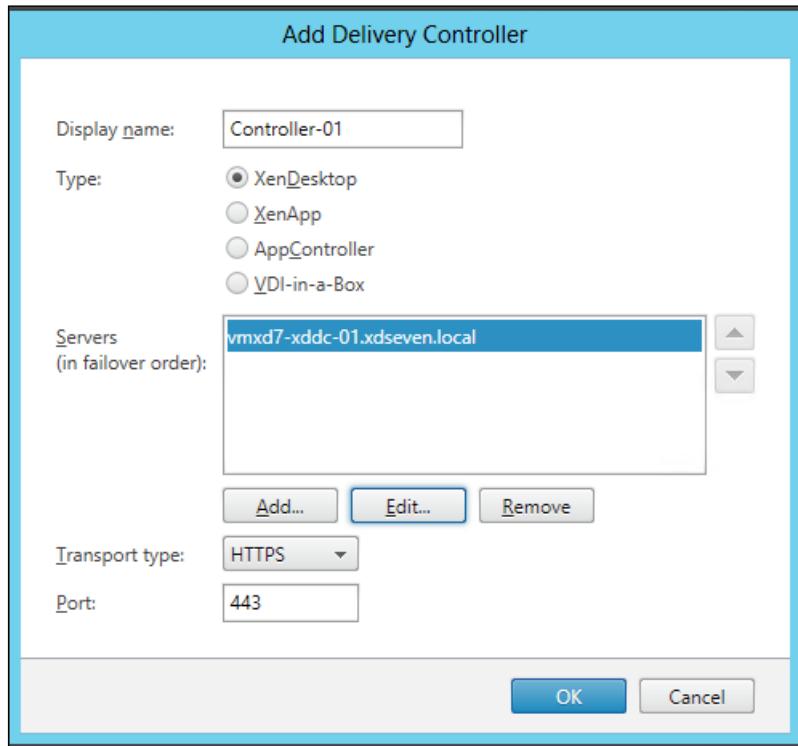


7. In the **Base URL** screen, assign a valid URL at which the StoreFront server will be available to the end users. Then, click on **Next** and wait till the end of the deployment.



8. In the **Store Name** field inside the **Store Name** category, enter a name for the store you are going to create. Then, click on **Next**.
9. In the **Delivery Controllers** section, click on the **Add** button to open the **Delivery Controller** menu.
10. In the **Add Delivery Controller** menu, perform the following configuration steps:
 - ❑ Assign a name to the controller by populating the **Display name** field.
 - ❑ Select the controller type by clicking on the specific radio button option (**XenDesktop**, **XenApp**, **AppController**, or **VDI-in-a-box**).
 - ❑ In the **Servers (in failover order):** field, click on the **Add** button and enter the name of your configured Delivery machine.
 - ❑ Select the relative transport type and port (HTTP/80 or HTTPS/443).
 - ❑ After completion, click on the **OK** button. Then click on **Next** to continue with the procedure.

[ To be able to use the HTTPS connection, you need a valid SSL certificate on the Delivery Controller server.]



11. In the **Remote Access** section, select the option you want to configure (**None**, **No VPN tunnel**, or **Full VPN tunnel**).

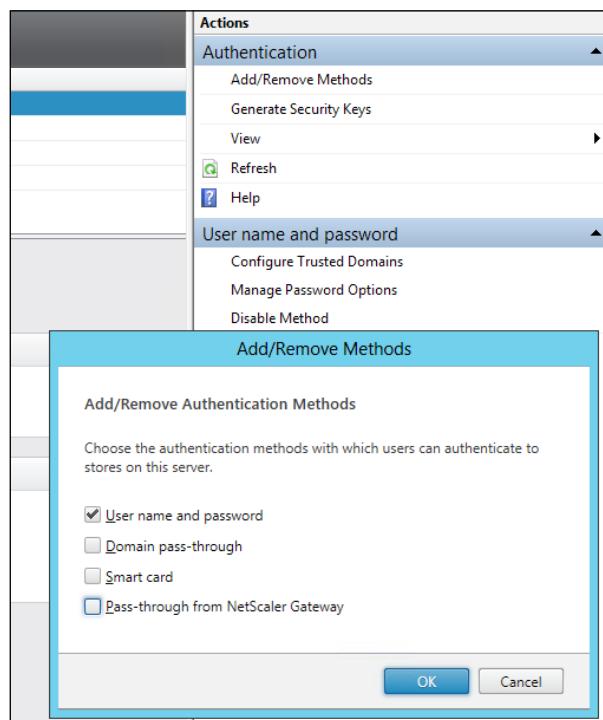
[ In this case, you can select the **None** option. We will configure the secure gateway later in this book.]

12. To complete the configuration process, click on the **Create** button. At the end of the store creation, click on **Finish**.
13. To check the configuration of your StoreFront platform, type the configured address in a compatible browser, in the form of `https://FQDN/Citrix/<storename>`.

[ Before using the web platform, you have to install the Citrix Receiver on the machine from which you want to use the web store.]



14. In the left-side menu, click on the **Server Group** link. In this section, you will have the option to add a server to the configured StoreFront infrastructure (**Add server** link on the right-hand side menu). Also, the default URL to access the platform can be changed (**Change Base URL** link in the right-hand side menu).
15. Click on the **Authentication** link in the left-hand side menu, and configure the following options:
 - **Authentication** section | **Add / Remove Methods**: Select the authentication methods you want to configure for the login on your infrastructure.



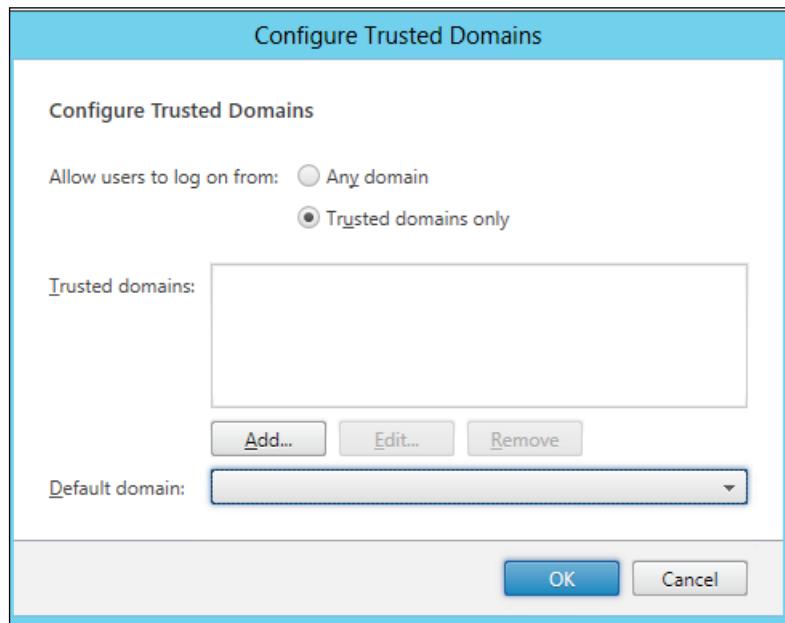


At the end of this book, we will discuss the XenDesktop 7 advanced logon.

- ❑ **Generate Security Keys:** To satisfy the general security practices, you can regenerate the security keys before their expiration date by clicking on the **Generate Keys** button.



- ❑ **User name and password section | Configure Trusted Domains:** With this option, it is possible to restrict the domains from which users can perform the login phase. Click on the **OK** button to complete the configuration.

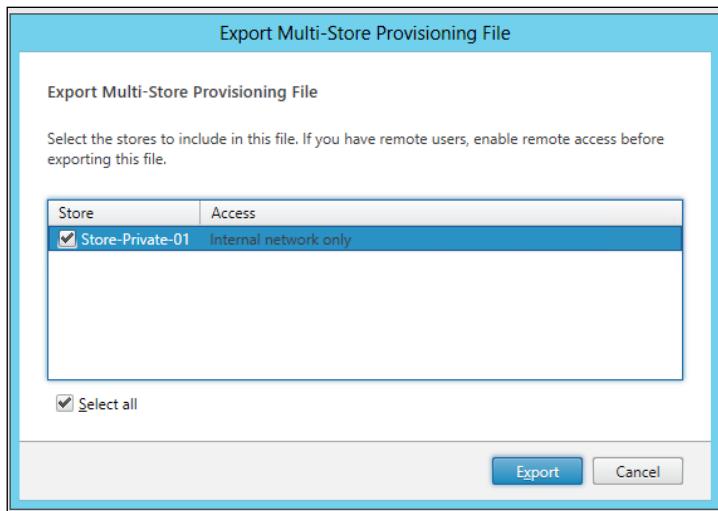


- ❑ **User name and password section | Manage Password Options:** This section permits users to change their password based on the configured option.



16. Click on the **Stores** link in the left-hand side menu, and configure the following options:

- ❑ **Stores section | Create store:** This option permits you to create a new store in the StoreFront infrastructure.
- ❑ **Stores section | Export Multi-Store Provisioning File:** This section permits you to export all the configured stores to the store configuration file to be used by end user devices on which you have installed the Citrix Receiver. The file will be saved with the .cr extension.



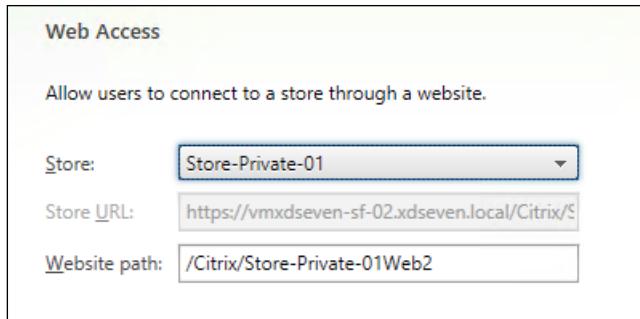
- ❑ **Configured store section | Manage Delivery Controllers:** With this link, you can **Add**, **Edit**, or **Remove** the Delivery Controllers configured within your farm.
- ❑ **Configured store section | Enable Remote Access:** This option is used to configure the external remote access by using a NetScaler Gateway appliance.
- ❑ **Configured store section | Manage Citrix Receiver Updates:** Using this option, you can decide the way you want to manage the Citrix Receiver updates, that is, by using the **Citrix (Citrix.com)** online resource, by using the internal network server used to deploy updates (**Merchandising Server**), or disabling the updates (**Do not check for updates**).
- ❑ **Configured store section | Integrate with Citrix Online:** This option permits you to include the three main Citrix online applications in your configured store.



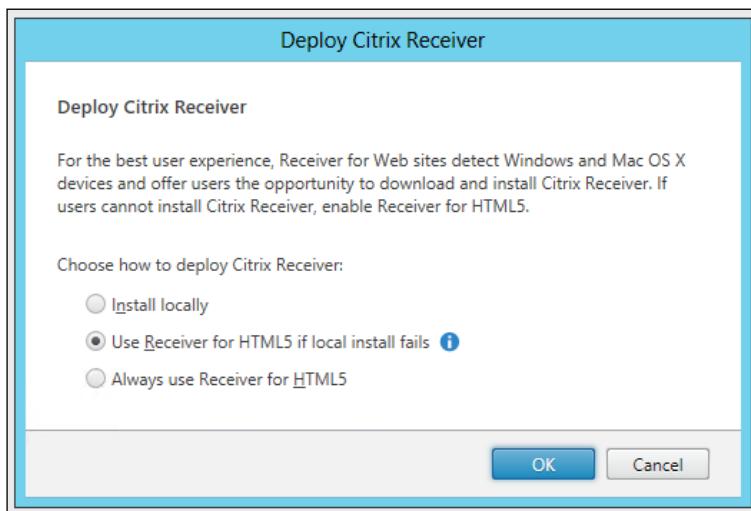
- ❑ **Configured store section | Export Provisioning File:** This option is similar to the multistore export we saw earlier, with the difference that this is related only to the current used store.
- ❑ **Configured store section | Configure Legacy Support:** This option activates the retro compatibility access for old Citrix clients.
- ❑ **Configured store section | Generate Security Keys:** As previously seen, this option permits the regeneration of security access keys before their natural expiration date.
- ❑ **Configured store section | Remove Store:** With this option, customers have the ability to remove configured stores.

17. Click on the **Receiver for Web** link in the left-hand side menu, and configure the following options:

- ❑ **Receiver for Web | Generate Security Keys:** In this section, it's possible to add one or more websites to the StoreFront configured platform.



- ❑ **Configured store section | Add Shortcuts to Websites:** This interesting option permits you to add a StoreFront shortcut to specified websites to provide a quicker access to your published resources.
- ❑ **Configured store section | Change Store:** By clicking on this link, you can change the store to which the configured Web Receiver is assigned.
- ❑ **Configured store section | Deploy Citrix Receiver:** In this section, you can choose how to deploy the Citrix Receiver to end users.



- ❑ **Configured store section | Remove Website:** This option must be used only if you want to remove a configured Receiver Website.



The options **NetScaler Gateway** and **Beacons** will be discussed in *Installing and Configuring Citrix NetScaler Gateway 10.1* recipe in *Chapter 8, XenDesktop Tuning and Security*.



How it works...

StoreFront 2.0 is a new default platform used with XenDesktop to access published resources. It's in the form of a catalog, which is able to deploy resources like desktops and applications from heterogeneous Citrix software (XenDesktop, XenApp, XenMobile, and so on).

StoreFront offers the same login methodologies used by the web interface. Customers can access their contents by using simple authentication, smart card, or smart card pass through. In addition, it's also possible to access the Citrix farm with the pass through from the NetScaler Gateway.

The great step forward in this platform is its new features, which are given as follows:

- ▶ StoreFront no longer needs to use an external database. Now, it can use its local repository for user subscriptions.
- ▶ The high availability has been improved, thanks to Storefront's capacity to replicate its database content among all the StoreFront machines within a configured site.
- ▶ StoreFront gives you choice in the way you want to access the resources, through the use of the Citrix Receiver or by using the new HTML5 web client.



When using the Citrix Receiver to access your StoreFront server, you can use a configured e-mail address to directly access your store. This is the **e-mail-based account discovery** feature.

- ▶ StoreFront is able to apply a sync between all the configured StoreFront servers used by customers to access their resources, this the user permits to not apply it again for application subscription.
- ▶ StoreFront 2.0 allows you to change you changing the password of your Active Directory account used to connect to the store.
- ▶ The Citrix Receiver installed on the end-user workstations can be easily configured by using the exported Store configuration file. Also, in Multi-Store mode, this means that it's possible to export and configure on a client device all the available stores configured in the infrastructure.
- ▶ In a configured store, the Citrix online applications are already available for deployment to the end users (Citrix GoToMeeting, GoToWebinar, and GoToTraining).

StoreFront is a more flexible platform than its predecessor. It is fully oriented to the new Citrix objectives, the mobile world, and the BYOD workers category.

There's more...

Also, in case of the StoreFront installation, users can perform this task using the command line. You have to execute, from a command prompt shell, the same executable file used for the graphical installation (`CitrixStoreFront-x64.exe`). This is followed by one or more of these options:

- ▶ `-silent`: This option executes all the required steps in silently.
- ▶ `-INSTALLDIR`: This option specifies the destination folder on which StoreFront 2.0 will be installed.
- ▶ `-WINDOWS_CLIENT`: This option will make the Citrix Receiver installation files for Windows available on the StoreFront server.
- ▶ `-MAC_CLIENT`: This option will make the Citrix Receiver installation files for Mac available on the StoreFront server.

See also

- ▶ The *Configuring Citrix Receiver™* recipe in *Chapter 4, User experience – Planning and Configuring*

Installing and configuring Provisioning Services 7

As we did earlier in the *Citrix XenDesktop 5.6 Cookbook*, in this book, we have decided to give particular importance to both the possible resource deployment ways: MCS and PVS.

In this recipe, we will explain step-by-step how to install and configure the Provisioning Services 7 platform.

Citrix Provisioning Services 7.0 eliminates the need for external PXE and TFTP platforms, thanks to the empowered **Boot Device Manager** feature.



Thanks to the BDM feature, you can avoid using any IP helper (DHCP relay) within your network, because of the absence of PXE systems, which eliminates the boot problems across different networks.

Getting ready

The Provisioning Services 7 platform can be implemented on the following platforms:

- ▶ **PVS Server**: Operating Systems: Windows Server 2008 and 2008 R2 (Standard, Enterprise, Datacenter editions), Windows Server 2012 (Essential, Standard and Datacenter editions).



For a number of vDisks equal or greater than 250, the minimum RAM requirement for the server machine changes from 2 GB to 4 GB of RAM.



- ▶ **Databases:** Microsoft SQL Server 2008 and 2008 R2 (Express, Standard, Enterprise editions), Microsoft SQL Server 2012 (Express and Standard editions).
- ▶ **Target Devices:** Operating Systems: Windows Server 2008 R2, Windows Server 2012, Windows XP SP2 and SP3, Windows 7 SP1 (Ultimate Edition supported only in Private Image mode) and Windows 8.



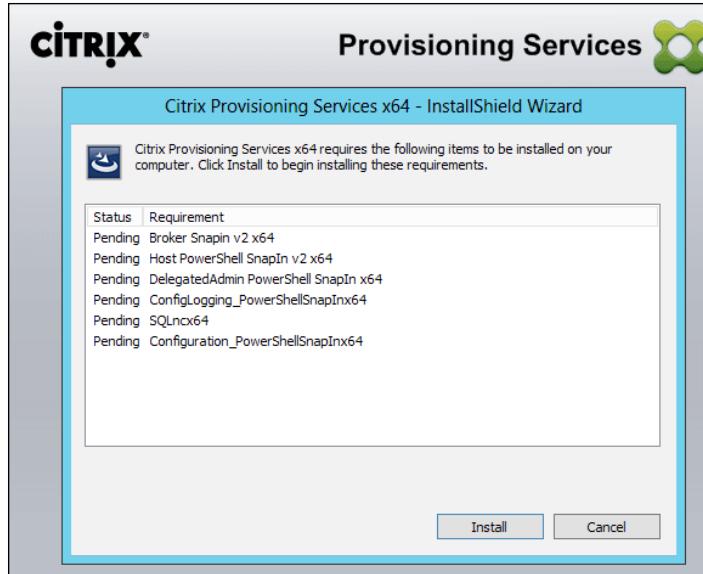
Because of the master images deployed with the latest XenDesktop Virtual Desktop Agent installation, Windows XP is not supported.



How to do it...

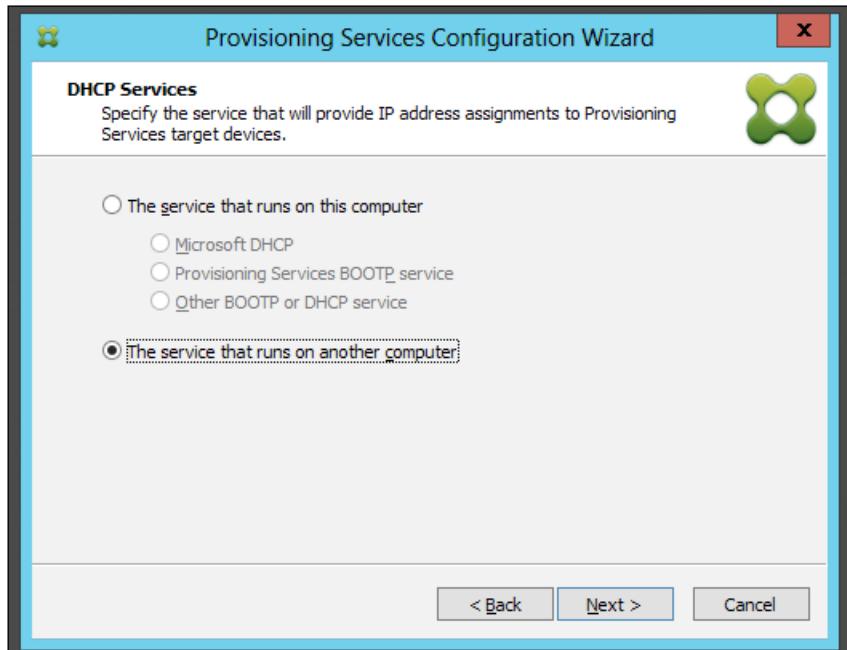
In this recipe, we are going to execute all the steps required to install and configure the Citrix Provisioning Services platform.

1. Download the PVS 7 ISO software from the Citrix website by using your credentials on www.citrix.com/MyCitrix.
2. It's necessary to install .NET Framework 3.5. If it is not present on your PVS server, you can install it from **Windows Server Features**.
3. Run Autorun.exe from the installation media.
4. From the **Provisioning Services** installation screen, select **Server installation**, and then click on **Install Server**.
5. In the missing prerequisites screen, click on **Install** to add all the pending components to the system.



6. In the welcome screen, click on **Next** to proceed.
7. Accept the **Citrix License Agreement**, and click on the **Next** button.
8. Insert valid **User Name** and **Organization** values, choose whether you want to install the application for **Anyone who uses this computer (all users)** or **Only for me (Windows User)**, and then click on **Next**.
9. In the **Destination Folder** screen, accept the proposed installation path (default path is C:\Program Files\Citrix\Provisioning Services\)) or modify it by clicking on the **Change** button. After completion, click on the **Next** button to proceed.
10. In the **Ready to Install the program** screen, click on the **Install** button to start the installation process.
11. After completion, click on the **Finish** button, and then proceed with the configuration operations.
12. In the welcome screen, click on the **Next** button to proceed.

13. In the **DHCP Services** screen, select the **The service that runs on another computer** radio button, and then click on **Next**.



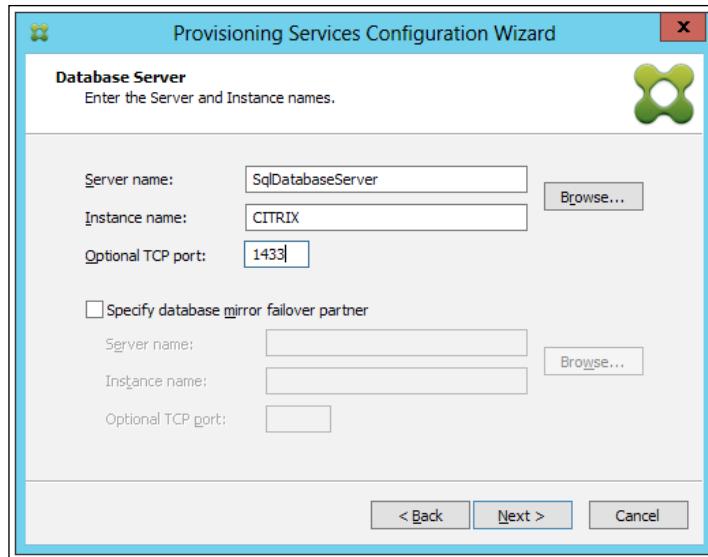
The best choice is to install DHCP server on a machine other than the Provisioning Service server. You should always separate components for better performance and roles isolation.

14. On the **PXE Services** screen, select the first option to configure the PXE component (**The Service that runs on this computer | Provisioning Services PXE service**), and click on **Next** to continue.
15. In the **Farm Configuration** section, select the **Create farm** radio button, and then click on the **Next** button.



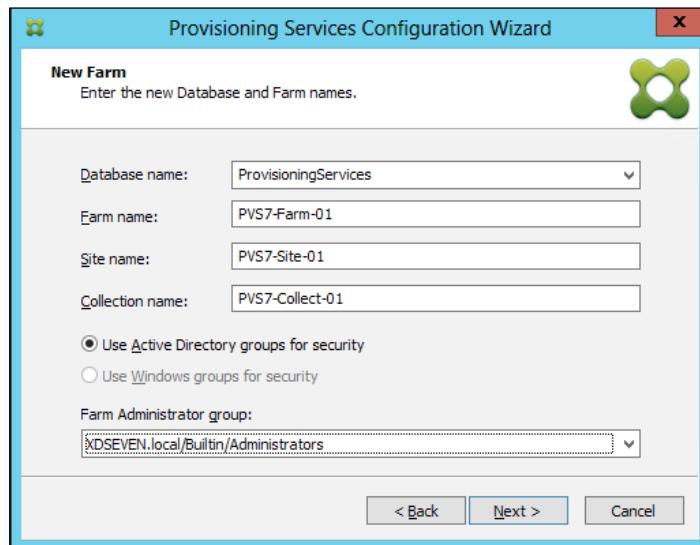
To better convey the differences between the MCS and PVS architectures, we'll always use two different farms to accomplish tasks for both architectures.

16. In the **Database Server** section, populate all the required fields to give the PVS server the ability to connect to the database server. After completion, click on **Next**.



You should always consider separating the database server from the PVS machine. Separating roles will ensure you separation, isolation, and better load balancing and security.

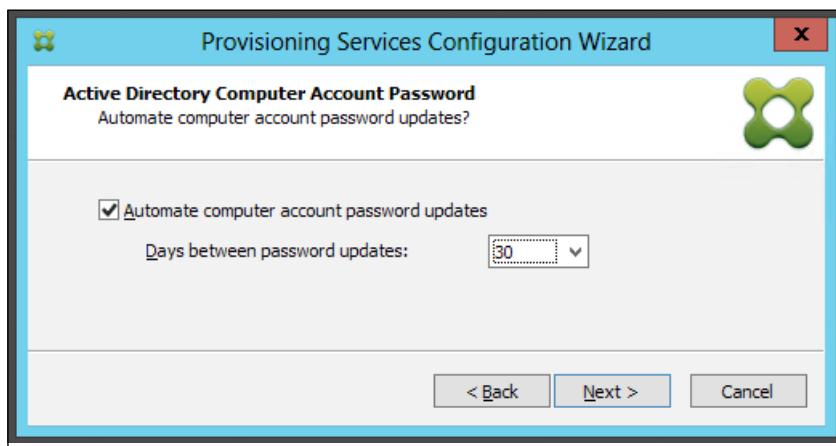
17. In the **New Farm** screen, populate all the required fields, then choose the configured **Active Directory groups for security** radio button. After completion, click on the **Next** button.



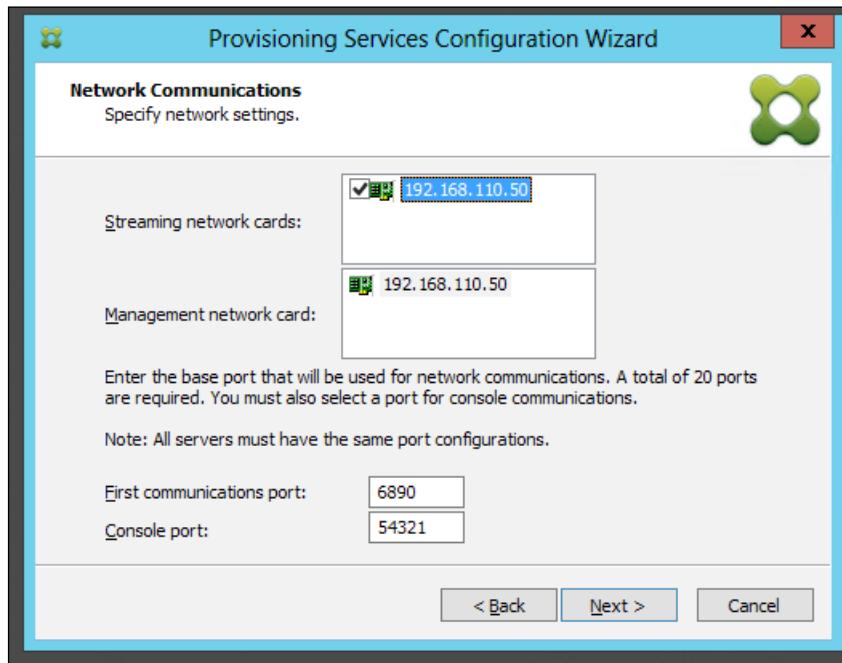
18. In the **New Store** screen, assign a name to the store, select a **Default path**, and click on the **Next** button to continue with the installation process.
19. In the **License Server** section, populate the **License Server name** and **Licenser Server port** fields with the values of an existing Citrix Licensing Server. Then, click on **Next** to proceed.

[ To check and validate the validity of your License Server with the PVS 7 platform, flag the **Validate license server version and communication** option.]

20. In the **User account** screen, specify a valid account for the **Stream and Soap Services**. You can choose between the **Network service account** or **Specified user account**. After configuration, the user should click on the **Next** button.
21. In the **Active Directory Computer Account Password**, you can automate the computer account password updates by enabling this option, configuring the interval in days after which the passwords will be updated. To continue with the **Provisioning Services Configuration Wizard**, click on **Next**.

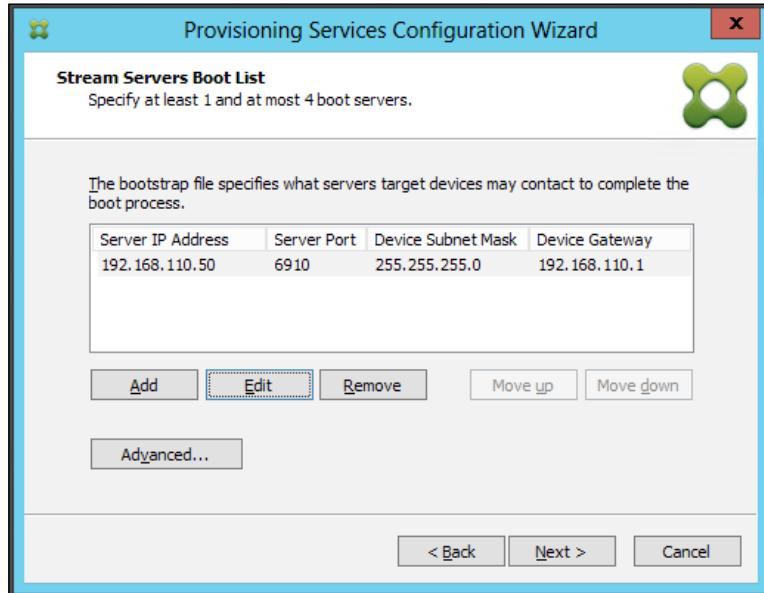


22. The **Network Communications** screen allows users to be able to configure the network components in the PVS console component in terms of streaming NICs and communication ports. Click on **Next** to continue after completed.

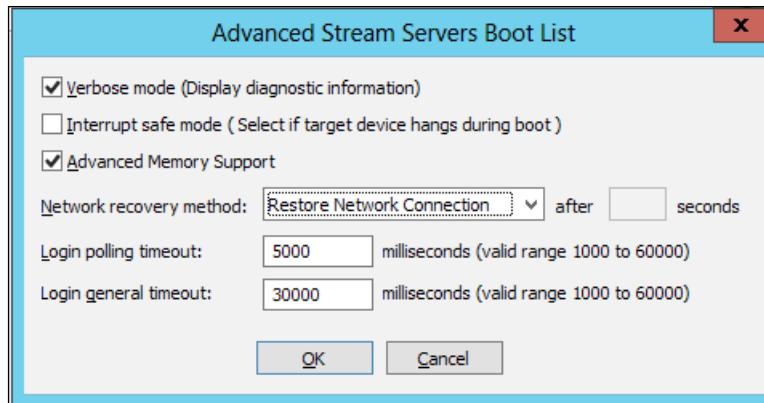


23. In the next screen, flag the **Use the Provisioning Services TFTP Services** to enable the use of the PVS 7 TFTP feature, and browse for a disk path on which the installed resources are located (in our case, the BIN files have been located under C:\\ProgramData\\Citrix\\Provisioning Services\\Tftpboot). Click on the **Next** button to continue.

24. In the **Stream Servers Boot List**, users can configure up to four boot servers, specifying their network configurations.



25. By clicking on the **Advanced...** button, it's possible to configure advanced options such as **Verbose mode** and **Advanced Memory Support**. After completion, click on the **OK** button; and then, click on **Next** to continue.



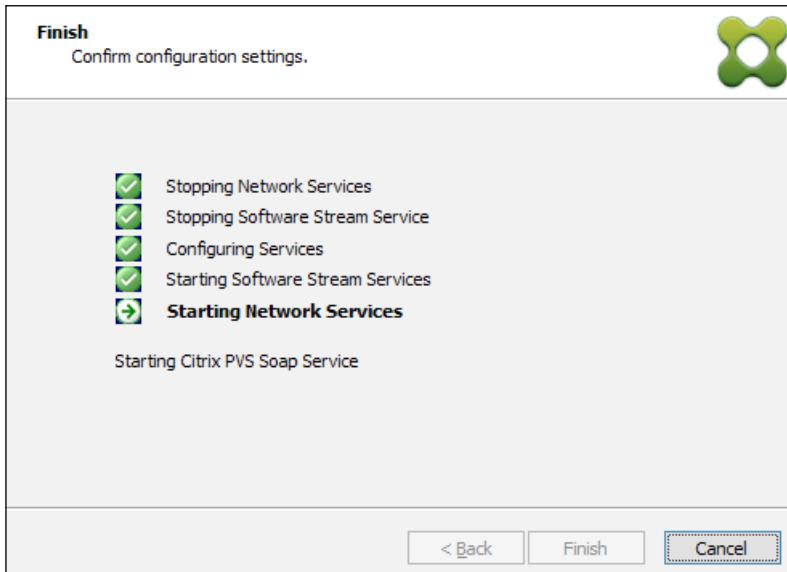


The **Verbose** mode is particular useful when executing a problem analysis. Consider this a PVS debug mode.

26. At the end of this procedure, flag the **Automatically Start Services** option and click on the **Finish** button. Then, click on **Done** after all the configurations have been completed.

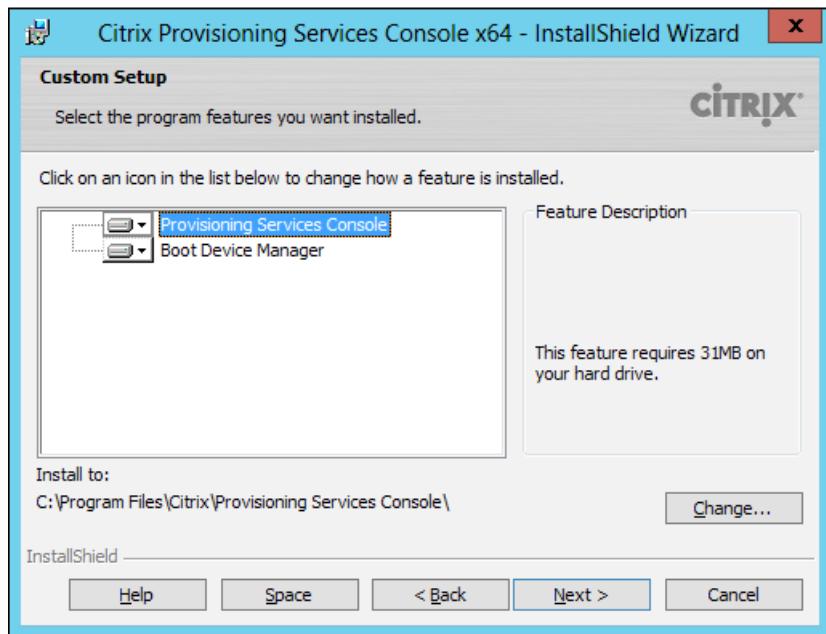


Remember that active Windows Firewall might be a problem for your installation process. You have to open the required ports, or turn it off. The ports are UDP 6890-6909 (Inter-Server communication), TCP 1433 (SQL Server database), TCP 389 (Active Directory communication), UDP 67 (DHCP), UDP 67 and 4011 (PXE Services), UDP 69 (TFTP), UDP 6910 (Target Device logon), UDP 6910-6930 (vDisk Streaming), TCP 54321 and 54322 (SOAP Service).

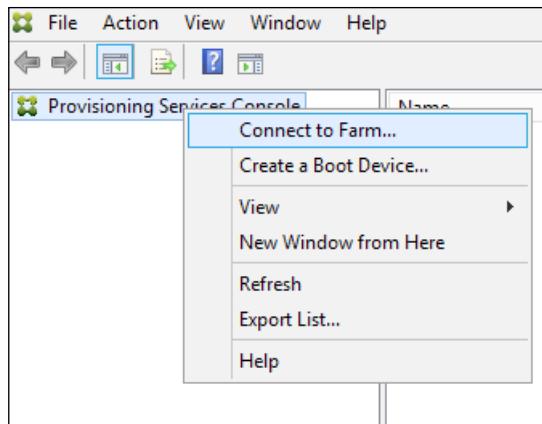


27. On the Installation media menu, select the **Console Installation** link.
28. Click on the **Next** button on the welcome screen, to proceed with the console installation.
29. Accept the **Citrix License Agreement** and click on the **Next** button.
30. In the **Customer Information** section, populate the **User Name** and **Organization** fields with valid data, specifying if the installation is for the entire machine's users (**Anyone who uses this computer**) or only for the current user (**Only for me**). After this choice, click on the **Next** button.

31. Select a valid path in the **Destination Folder** screen, and click on **Next** to continue the installation. To change the default path (C:\Program Files\Citrix\ Provisioning Services Console\), click on the **Change** button and browse for a valid location.
32. In the **Setup Type** screen, select the **Custom** option and click on the **Next** button.
33. In the **Custom Setup** screen, select all the proposed components, maintain the previously chosen path, and click on **Next**.

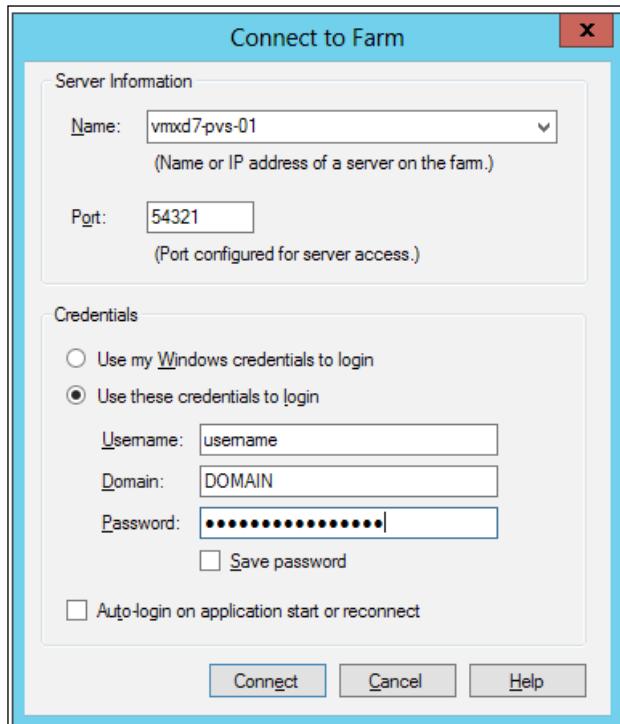


34. In the **Ready to Install the Program** screen, click on **Install** to complete the setup procedure. At the end of this setup, click on the **Finish** button.
35. Click on the **Provisioning Services Console** link from the Windows Server 2012 applications list.
36. The **Provisioning Services Console** will be executed. Right-click on this link in the left-hand side menu and select the **Connect to Farm** option.



Be sure that the **Citrix PVS Soap Server** service is running; otherwise, you won't be able to connect to the PVS configured farm.

37. In the **Connect to Farm** screen, populate all the fields with the correct values and specify a valid domain username. After this, click on the **Connect** button.



38. After verifying the connection parameters, you will be able to use the PVS 7 platform.



In *Chapter 3, Master Image Configuration and Tuning*, we will discuss the creation of the Target Device for the Provisioning Services in the *Configuring a target device – PVS architecture* recipe.

How it works...

PVS is one of the two deployable architecture types for desktop and application deployments. Provisioning Services 7 is the latest release of the software used to implement this kind of architecture.

The structure is quite simple. A server component, which is managed by a PVS console, delivers operating systems images to the end users' devices by creating copies of the virtual disks of an installed operating system called **Master Target Devices** and streaming them through the network from the PVS server memory, every time they're needed by users. This process permits having high elevated network performance, dramatically reducing the impact on storage activities.



You have to give attention to the PVS DB size. In fact, even if it starts with only 20 MB of data, its dimension has a growth of 10 MB. This means that in the case of hundreds or thousands of objects, the database size could become higher than your expectations.

There's more...

Provisioning Services use the Kerberos authentication to allow its components communicate with each other, register the components against the Active Directory through the **Service Principal Name (SPN)**, and permit the Domain Controller to identify the accounts that manage the running services. In the case of registration problems, your PVS service could fail. To avoid this situation, you have to use the `setspn` command in order to give the right permissions to the account that manages the earlier described services (such as the PVS Soap Service) by applying the following syntax:

```
setSpn -a PVSSoap/PVS_Server_FQDN <username_managing_service>
```



At the following MSDN link, you can find more information about the SPN:
[http://msdn.microsoft.com/en-us/library/windows/desktop/ms677949\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms677949(v=vs.85).aspx).

See also

- ▶ The *Creating and configuring the Machine Catalog* recipe in *Chapter 6, Creating and Configuring a Desktop Environment*

2

Configuring and Deploying Virtual Machines for XenDesktop®

In this chapter, we will cover the following recipes:

- ▶ Configuring the XenDesktop® site
- ▶ Configuring XenDesktop® to interact with Citrix® XenServer
- ▶ Configuring XenDesktop® to interact with VMWare vSphere 5.1
- ▶ Configuring XenDesktop® to interact with Microsoft Hyper-V

Introduction

The configuration of the XenDesktop components is the first step to implementing a fully functioning infrastructure. After this, the second, and maybe the most important, step is deploying virtual desktop instances.

To accomplish this task, you need to interface Citrix servers with a hypervisor, a bare-metal operating system, which is able to create, configure, and manage virtual machines. XenDesktop is able to communicate with three important hypervisor systems on the market: Citrix Xenserver, VMware vSphere, and Microsoft Hyper-V. After you've created a template of a virtual machine with a Microsoft desktop or server operating system on board, XenDesktop is able to deploy OS instances to the end users starting from the virtual machine image through the use of different deployment techniques.

The main task of Delivery Controller is starting virtual machines, and assigning them dynamically to end users. At the end of a desktop session, Delivery Controller will send a request to the hypervisor to restart or shutdown the virtual desktop instance.

In this chapter, we're going to implement the communication between hypervisors and Citrix servers.

Configuring the XenDesktop® site

Before any interaction among components, after you've installed Citrix Studio and Citrix Director, you need to configure a Site, which will be the place where you'll configure the hypervisor host.

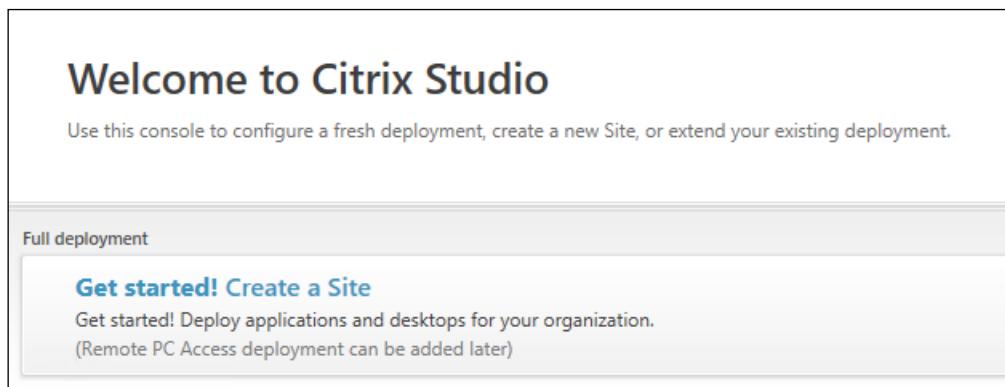
Getting ready

In order to complete all the required steps for this recipe and perform a standard Site Deploy, you need to be assigned the administrator role for all the machines involved in the Site configuration (*Delivery Controller* and the database server).

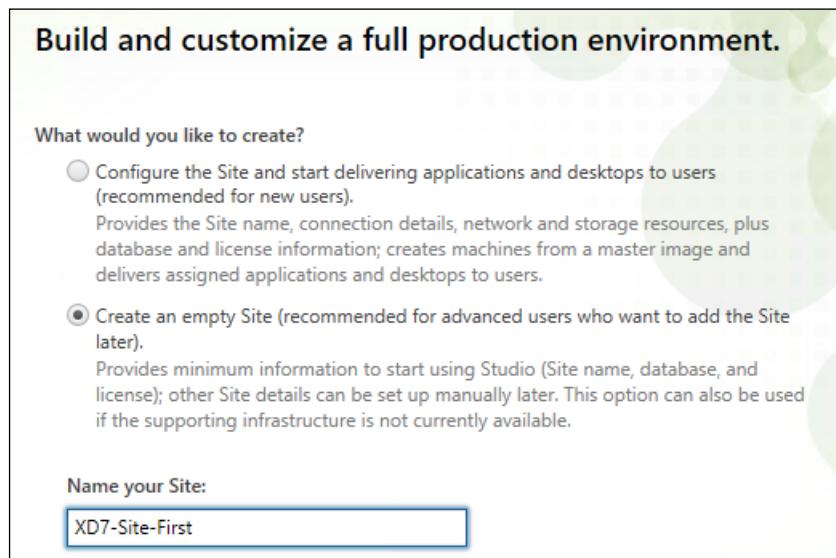
How to do it...

In the following steps, we will describe how to create a site for a XenDesktop 7 infrastructure:

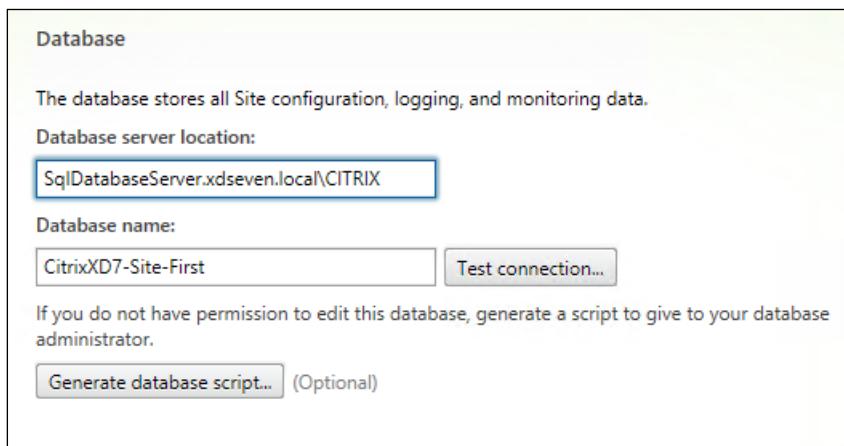
1. Connect to the Citrix Studio by searching for it within the Windows Application list (Windows + C key combination or click on the **Search** icon), and then click on its icon.
2. In the **Welcome to Citrix Studio** screen, click on the **Get Started! Create a Site** option to start the XenDesktop Site creation.



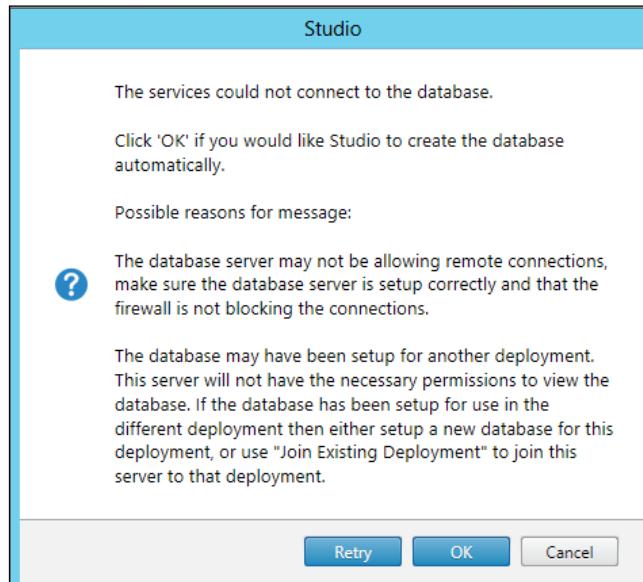
3. In the **Introduction** section, click on the second radio button option to create an empty site; assign a name to it by populating the **Name your Site** field, and click on **Next** to continue.



4. In the **Database** section, populate the **Database server location** field with the hostname of your database server and the Citrix XenDesktop existing instance name in the form of Hostname\InstanceName. Then assign a name to the site database, and click on the **Test** connection button to check that you are able to contact the database machine.



5. When prompted for the automatic database creation, click on the **OK** button to let Studio create the database.



6. As an alternative, if you want, you can create the Citrix database manually by clicking on the **Generate database** script button; you'll get back a set of instructions in the form of two .sql scripts, to generate the database for *standard* or *mirrored* mode.

The screenshot shows a Microsoft Notepad window titled 'Script_For_Database_SqlDatabaseServer.xdseven.local_CITRIX,1434 - Notepad'. The window contains a single text file with the following SQL script content:

```
-- To create a database schema for a Site, use this script: execute on the principal SQL Server database instance
-- 
-- To learn more, visit http://support.citrix.com/article/CTX127359
-- 
-- You can use SQLCMD from the command line to run this script, or you can use SQL Server Management Studio in SQLCMD mode.
-- 
-- Note that you must use a collation which ends with "_CI_AS_KS". In general, it is best to use a collation which ends with "_100_CI_AS_KS".
-- To do so, use this command when creating the database:
-- 
--     create database [CitrixXD7-Site-First] collate Latin1_General_100_CI_AS_KS
--     go
-- 
-- protect against generating tables in the wrong place, if database hasn't been created
use [tempdb];
go

if db_id(N'CitrixXD7-Site-First') is null
begin
    RAISERROR('Database does not exist', 10, 127);
end
go

-- Ensure the database is using a read committed snapshot
declare @groupId uniqueidentifier = null;

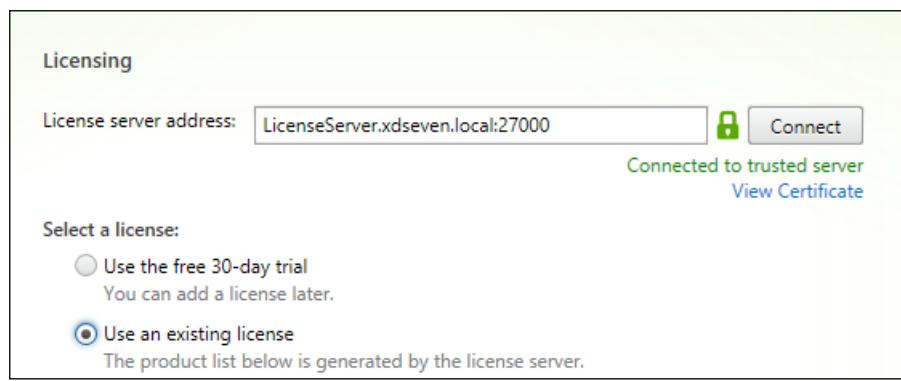
if (serverproperty('IsHadrEnabled') = 1)
begin
```



You can find the two generated scripts at the following default path: C:\Users\<username>\AppData\Local\Temp\1\Create Site-<date>



7. After the database configuration, in the **Licensing** section enter your license server name and the port number, in the form of hostname:port, and click on the **Connect** button. If you already have a configured license file, click on the **Use an existing license** radio button; otherwise, you will have to click on the **Use the free 30-day** trial option, inserting a correct license file later. At the end of these configurations, click on **Next**.

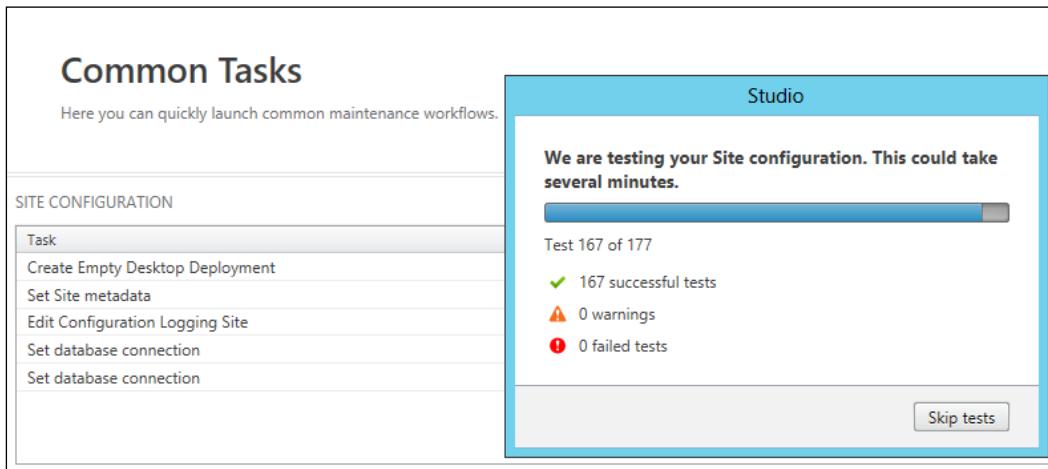


You can verify the validity of your License Server certificate by clicking on the **View Certificate** link—**Connected to trusted server** area.



8. In the **Summary** screen, after you have verified all the configured options, click on the **Finish** button to complete the procedure.

9. After the configuration has been completed, in the Citrix Studio main menu, you will find information about the created Site. If you want, you can check your current implementation by clicking on the **Test Site** button.



How it works...

Configuring a site lets you assemble together all the components previously configured; the main operations to complete during the generic Site configuration procedure are:

- ▶ The connection to the SQL Server instance on which we are creating the XenDesktop database. This task can be accomplished in two ways: first by using the Site configuration wizard (automated operation), and second by generating two database creation scripts and running them within the SQL Server database environment.
- ▶ The connection to the License Server by the use of the Site configuration wizard, you can make a connection to a specified License Server address and port, deciding if using trial (30-days) licenses, or already configured licenses.

If you want, at the end of the procedure, you can check the validity of your configuration by using the **Test Site** button in the Studio Host main menu section.

There's more...

In case you decide to use a database port other than the default SQL Server port value (1433), you will have to insert the connection string in the following form:

`DBSERVER\INSTANCE,SQL_PORT_NUMBER`

For example, in case you have configured the CITRIX instance to listen to on port 1435, the connection string will be the following:

```
SqlDatabaseServer\CITRIX,1435 .
```

See also

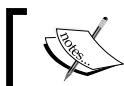
- ▶ The *Administering hosts and machines – the Host and Machine Creation cmdlets* recipe in Chapter 9, *Working with XenDesktop PowerShell®*

Configuring XenDesktop® to interact with Citrix® XenServer

The first and the most common configuration for a XenDesktop site is interfacing it with the Citrix hypervisor, XenServer. The XenServer 6.2.0 release, is related to XenDesktop 7.

Getting ready

The preliminary work required to perform all the operations of this recipe is to install one or more XenServer hosts. To accomplish this task, you need to download the XenServer ISO image file from <http://www.citrix.com/downloads.html>. XenServer is a **bare-metal hypervisor**, a kind of virtualizer, which directly manages the hardware; for this reason, you have to install it as a normal operating system (you need no other operating system installed on the server).



Please refer to the following Citrix document to install the XenServer hypervisor: <http://support.citrix.com/article/CTX137829>.

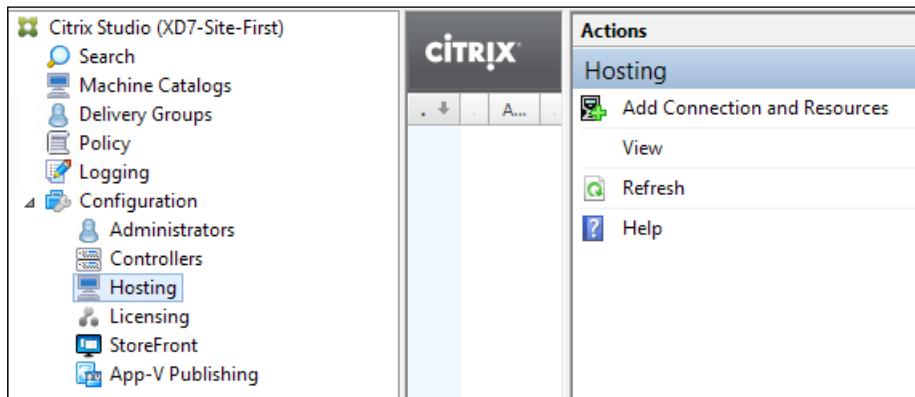


How to do it...

In this section, we will perform the operations required to configure XenDesktop to use the Citrix XenServer hypervisor:

1. Connect to the Citrix Studio by searching for it within the Windows Application list (Windows + C key combination or by clicking on the **Search** icon), and then click on its icon.

2. On the left-hand side menu, expand the **Configuration** section, and select the **Hosting** link. Then click on the **Add Connection and Resources** link on the right-hand side menu.



In the **Connection** section, select **Citrix XenServer** from the **Host type** drop-down menu. In the **Address** field, input the FQDN of the XenServer host (in the form of `http://FQDN`), insert **Username** and **Password** in the respective fields, and give a name to the connection (**Connection name** input text). In the **Create Virtual machine using:** subsection, select the **Studio tools (Machine Creation Services)** radio button, and after completion, click on **Next** to continue.

The screenshot shows the 'Connection' configuration dialog. It includes fields for 'Host type' (set to 'Citrix XenServer®'), 'Address' ('http://xenserver.xdseven.local'), 'Username' ('username'), 'Password' (redacted), and 'Connection name' ('XenServer-Host'). Below these fields is a note: 'The name displayed in Studio. Choose a name that will help administrators identify the Host type and deployment address.' Under 'Create virtual machine using:', there are two radio buttons: 'Studio tools (Machine Creation Services)' (selected) and 'Other tools'. At the bottom are 'Back', 'Next', and 'Cancel' buttons.



You should always add the FQDN and the IP address in the host file of your Desktop Controller machine to avoid unexpected resolution name problems.

1. In the **Host** section on the **Resources** screen, choose a configured network (depending on your XenServer host configuration, you could have one or more available networks) on which you are assigning the generated virtual desktop instances, and then click on the **Next** button.
2. In the **Storage** section, flag the available storage on which to create virtual machines, and select the desired radio button for personal vDisk location (**Use same storage for virtual machines and personal vDisk Normal paragraph style. use different storage for personal vDisk**); these are options that only refer to the Desktop OS instances. To continue, click on the **Next** button.



Separating the storage for the Personal vDisk will improve the global performances and make easier the backup procedure for the user data disk.

The screenshot shows the 'Storage' configuration dialog box. At the top, it says 'Storage' and 'Select one or more storage devices for the new virtual machines:'. Below this is a table with a single row: 'Name' and 'Local storage on nv-xs-62' with a checked checkbox. Underneath the table, there is a section titled 'Personal vDisk storage (Desktop OS only):' with a 'Learn more' link. It contains two radio buttons: 'Use same storage for virtual machines and Personal vDisk' (unchecked) and 'Use different storage for Personal vDisk' (checked). Below these buttons is a button labeled 'Select different storage...' with '(1 resource selected)' next to it. At the bottom of the dialog are three buttons: 'Back', 'Next' (highlighted in blue), and 'Cancel'.



If there is available available storage, you should consider separating the operating system disk area from the personal vDisk storage. Separating these areas could make it easier to locate user disk zones, especially for backup operations or troubleshooting activities.

3. In the **Summary** screen, after you've verified all the information, assign a name to the XenServer connection in the space provided for the **Resource Name** field, and click on **Finish** to complete the procedure.
4. In the main menu of the **Hosting** section, we can now find the configured connection to the XenServer host.

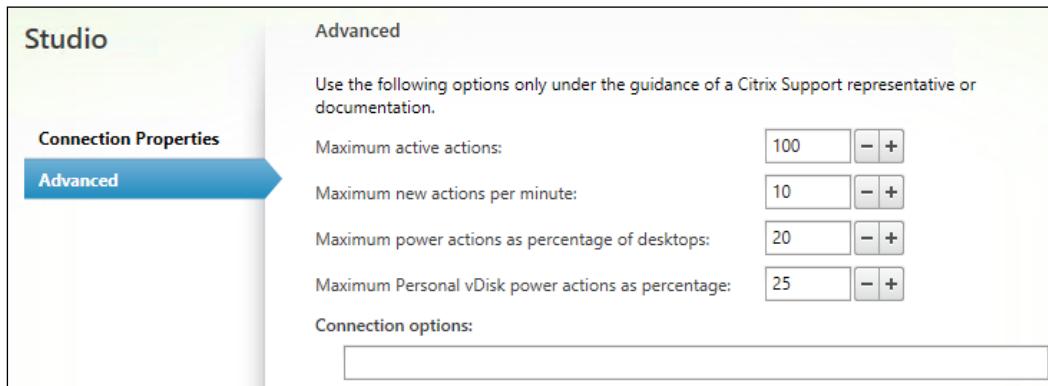
Name	Type	Address	State
XenServer-Host	Citrix XenServer®	http://xenserver.xdseven.local	Enabled
XS-602-Host			

5. If necessary, there is the possibility of changing the connection parameters by selecting the **Edit Connection** link on the right-hand side menu.
6. In the **Connection Properties** section, we can modify the credentials to access the XenServer host (**Host address**, **username**, and **password** fields) by clicking on the **Edit settings...** button, or we can add one or more HA hosts by clicking on the **Edit HA servers...** button.

The screenshot shows the 'Connection Properties' dialog box. On the left, there's a sidebar with tabs for 'Connection Properties' (which is selected and highlighted in blue) and 'Advanced'. The main area displays connection details:

Host address:	http://xenserver.xdseven.local
Username:	root
Password:	*****
Edit settings...	
High availability (HA) servers:	1 servers
Edit HA servers...	

- Upon selecting the **Advanced** section, administrators get the capability to configure the following options: **Maximum active actions**, **Maximum new actions per minute**, **Maximum power actions as percentage of desktops**, and **Maximum Personal vDisk power action as percentage**. On finishing, click on **OK** to complete the configuration.



To perform any modification activity on the host and the connection, you must put them in *Maintenance mode*.

How it works...

XenServer is the hypervisor included in the Citrix Virtualization platform; starting from this discussed version (6.0.2), XenServer is again an open source virtualization platform, with the choice of providing technical and commercial support to be followed up by the Citrix professional team.

XenServer is the best integrated hypervisor with the Citrix VDI platform, which is also thanks to the cooperation between the XenDesktop and the XenServer teams. The way in which XenDesktop interfaces with XenServer is simpler than that of the other hypervisors: in fact, Desktop Controller directly contacts the server without any intermediate server console. One of the advantages of using this hypervisor is the capability to use the XenServer information caching feature also known as **IntelliCache**. The IntelliCache technique drastically reduces the read and write activities of your storage.



The XenServer IntelliCache feature has to be enabled during the installation procedure of this hypervisor.

There's more...

In the presence of tens of hundreds of virtual machines, the XenServer hypervisor could have performance issues in terms of lack of physical resources for Dom0, the most privileged domain in a XenServer installation, which is the only domain that is able to directly interface with the hardware or start non-privileged domains, for instance. To solve this problem, it should be necessary to assign more physical resources to Dom0. This operation can be performed by connecting to the desired XenServer machine using the XenCenter console or through the SSH connection, then editing the /boot/extlinux.conf file, modifying every occurrence of the dom0_mem parameter, and then assigning it the desired value in MB; you should consider using the advised value from Citrix, setting the parameter in the following way: dom0_mem=2940M. The default memory value assigned to Dom0 is 752 megabytes.

To apply the memory changes, you have to restart the XenServer node.

After the reboot operations, run the following commands from XenServer CLI in order to let XenServer understand how to use all the newly assigned memory size:

```
. /etc/xensource-inventory

staticmax=`xe vm-param-get uuid=$CONTROL_DOMAIN_UUID param-name=memory-
static-max` 

echo staticmax=$staticmax

xe vm-param-set uuid=$CONTROL_DOMAIN_UUID memory-dynamic-max=$staticmax

xe vm-memory-target-set uuid=$CONTROL_DOMAIN_UUID target=$staticmax
```

See also

- ▶ The *Configuring the CloudBridge platform* recipe in *Chapter 5, Configuring Additional Architectural Components*

Configuring XenDesktop® to interact with VMware vSphere 5.1

Citrix XenDesktop offers compatibility not only for Citrix proprietary platforms, but it also supports the most important virtualization architectures on the market. VMWare is currently the virtualization solution that better permits you to manage the resource over commitment and assignment for your virtual environments.

Getting ready

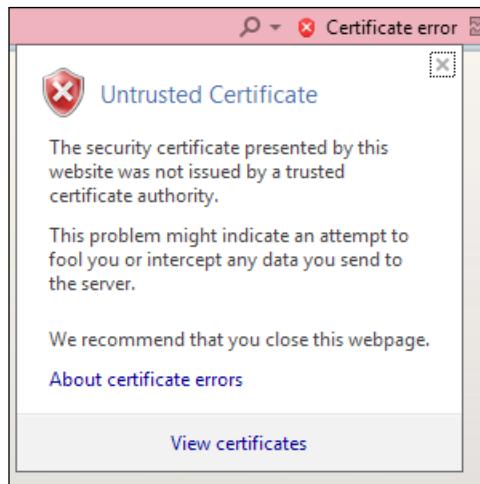
To ensure that all the activities in this chapter will be fully executed, it's required that you have an already-functioning VMware vSphere environment made up of at least two ESXi servers and a Windows server on which to install the VMware Virtual Center software.

After this, the step you've to perform is to import the *VMware Virtual Center certificate* on XenDesktop server to allow Desktop Studio to connect with the SSL connection to *Virtual Center SDK*.

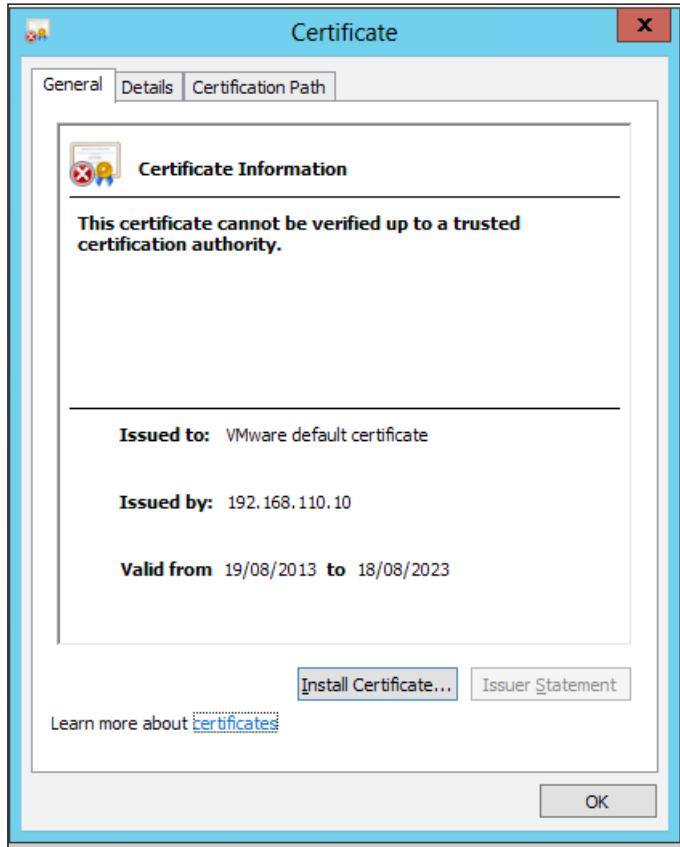
How to do it...

You have to execute the following procedures in order to activate the communication between the XenDesktop Controller machine and the VMware vSphere infrastructure:

1. Launch your chosen Web browser, and insert the hostname of the Virtual Center server in the address bar using the https connection. When prompted for security risk, accept to continue with the site navigation.
2. On the certificate status bar, click on the **Status** error, and select the **View certificates** link (VMware Virtual Center certificate is currently untrusted for XenDesktop).

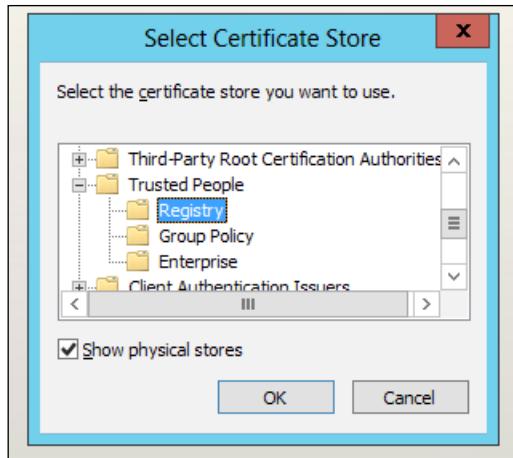


3. After the certificate presentation, click on the **Install Certificate...** button to proceed.

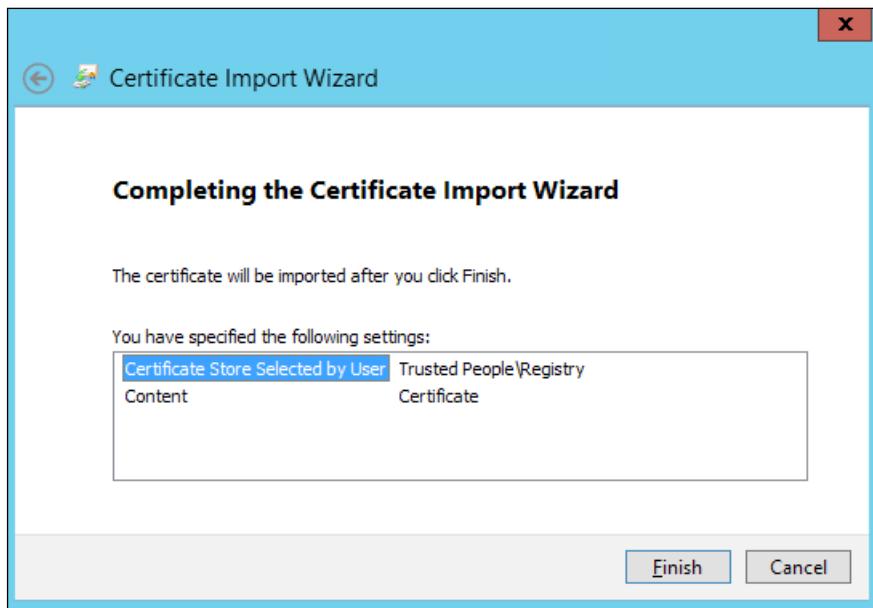


Be sure that the hostname associated with the certificate matches the assigned name to the Virtual Center server. In the case of mismatching, XenDesktop won't be able to connect with VMware. To avoid this, you could consider adding a record to the local file hosts of the XenDesktop server to match the IP address and hostname in the certificate.

4. On the **Welcome to the Certificate Import Wizard** page, select the **Local Machine** radio button as **Store Location**, and then click on **Next**.
5. In the **Certificate Store** section, select the **Place all certificates in the following store** option, and then click on the **Browse** button to specify the location in which you are installing the certificate.
6. Enable the **Show physical stores** option by flagging it, and then select the **Trusted People | Registry** subsection. After you are done, click on the **OK** button, and then click on **Next** to continue.



7. To complete the certificate import activities click on **Finish**.



8. To verify that the certificate import was successful, you must reconnect to the SSL Virtual Center address (`https://FQDN`). If you receive no more prompts about unsecure connections (as previously seen), the import has been successfully completed.



This procedure must be performed for Delivery Controller and the Provisioning Services server, depending on what kind of architecture you've implemented.

9. Connect to the Citrix Studio console; expand the **Configuration** section in the left-hand side menu; select the **Hosting** link; and click on the **Add Connection and Resources** link on the right-hand side menu.
10. In the **Connection** section, select **VMware vSphere** from the **Host type** drop-down menu. In the **Address** field, input the SSL address of the VMware SDK in the form of `https://VirtualCenterFQDN/sdk`; then insert the **Username** and **Password** in the respective fields; and give a name to the connection (**Connection name** input text). In the **Create Virtual machine using:** subsection, select the **Studio tools (Machine Creation Services)** radio button, and after completing, click on **Next** to continue.

Connection

Host type: VMware vSphere®

Address: https://vmxd7-vc-01.xdseven.local/sdk

Username: administrator

Password: [REDACTED]

Connection name: XD7-VMware-01

The name displayed in Studio. Choose a name that will help administrators identify the Host type and deployment address.

Create virtual machine using:

Studio tools (Machine Creation Services)

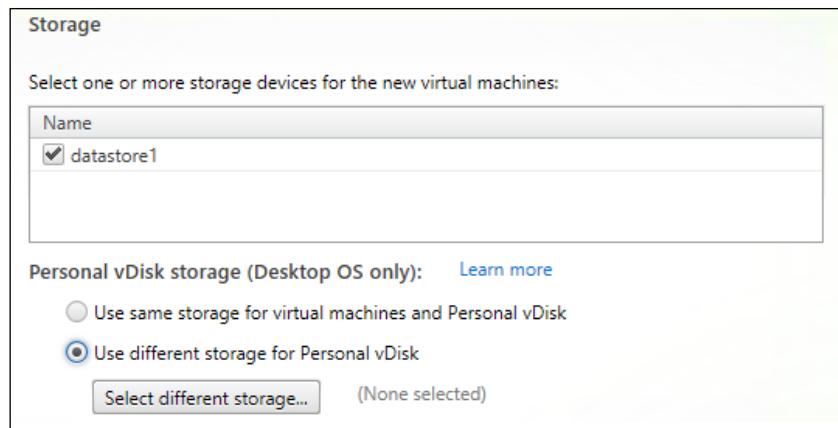
Other tools



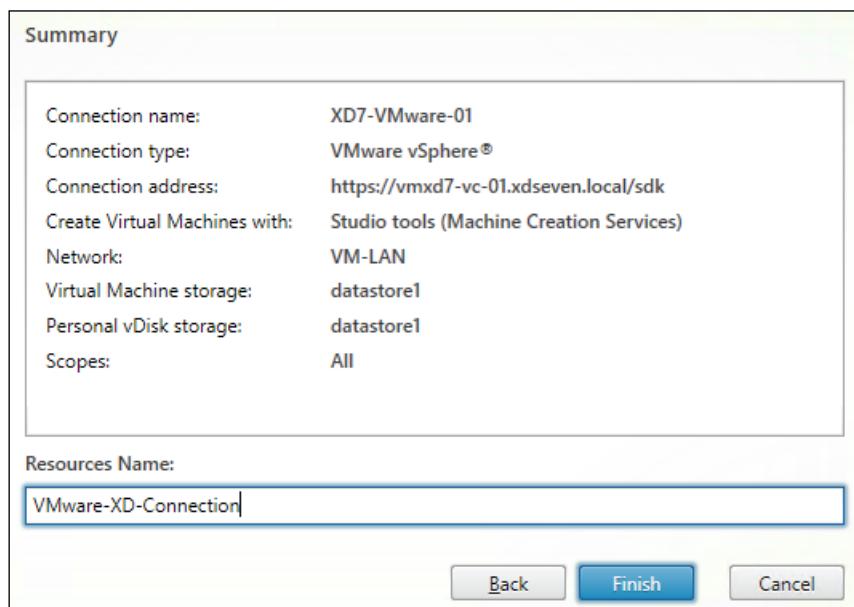
The specified username and password for the connection must be valid domain credentials with elevated privileges within the Virtual Center. Please refer to the following Citrix document to configure the right user permissions:

<http://support.citrix.com/proddocs/topic/xendesktop-7/cds-vmware-rho.html>

11. On the **Cluster** screen, click on the **Browse** button to select a vSphere **Cluster** on which to deploy virtual machines. After this operation, select a **Network** from the presented list on which you are deploying the virtual machine instances. Click on **Next** to continue with the wizard.
12. In the **Storage** section select the storage (VMware datastore as local or shared) for your virtual machine's system disks, and then decide whether to select a separate datastore for personal vDisks (recommended). After this, click on **Next** to continue.



13. In the **Summary** screen, after checking all the listed configured options, assign a name to the VMware connection, and click on the **Finish** button.

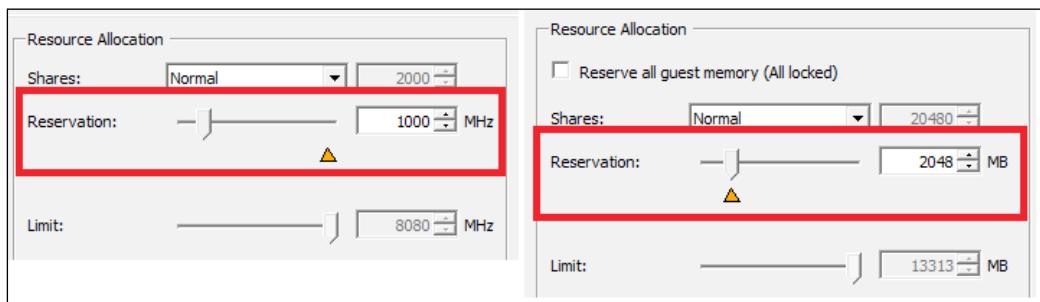


How it works...

XenDesktop and VMWare Virtual Center communication can be realized through two kinds of channels: *http* and *https*. The second is obviously more secure, and this communication is also advised by Citrix. So, to be able to communicate in HTTP over SSL, you need to import your Virtual Center certificate. For these components, VMware best practices say that you should create your own certificate from a personal certification authority. Anyway, communication could be established by using and importing the default self-signed VMware certificate. Once this import has been completed, the only thing remaining is to connect to the VMware API by its published SDK. The use of VMware Virtual Center is not only necessary, it is also a way to implement an architecture that is centrally managed and tuned by a controlling platform, such as the VMware vSphere Virtual Center platform.

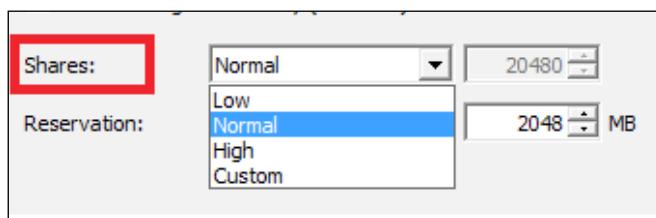
There's more...

The use of VMware vSphere as a hypervisor platform gives you the ability to reserve a set of particular resources to the deployed machine instances. By right-clicking on the desired machine and selecting the **Edit Settings** option, you can reserve vCPU and virtual RAM to the edited virtual machine.



You should apply these parameters to the Master Image template, replicating in this way the configurations to the deployed desktops.

In the case of equal access priority to the hypervisor resources, you can use another parameter that permits giving to the XenDesktop deployed instances higher priority in the resource queue.



The previous screenshot is the **Shares** section in the **Resources** tab, configurable as **Low**, **Normal**, **High** and **Custom**. A higher number means prior access to the resources.

See also

- ▶ The *Creating and configuring the Machine Catalog* recipe in Chapter 6, *Creating and Configuring a Desktop Environment*

Configuring XenDesktop® to interact with Microsoft Hyper-V

In the last few years, collaboration between Citrix and Microsoft has grown so much that they now share application virtualization and a deployment market. Respecting this partnership, it's possible to deploy virtual desktops for Citrix with Hyper-V, the Microsoft hypervisor.

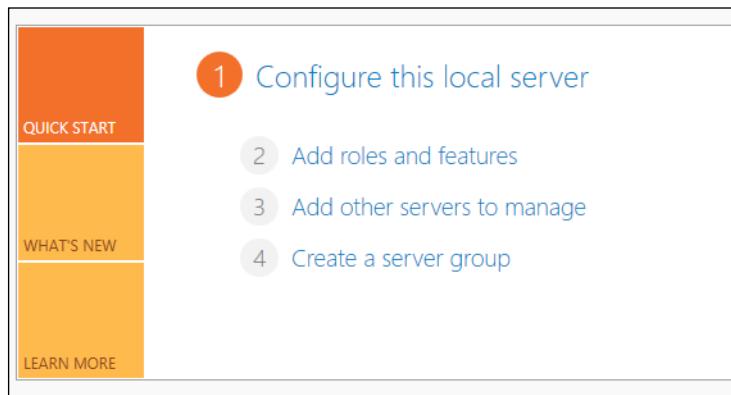
Getting ready

To be able to use virtual machines with Windows Server 2012, first of all we need to install and configure the hypervisor server role. After this, in order to allow Desktop Controller to interact with the Hyper-V server, it's necessary to install the Microsoft **System Center Virtual Machine Manager** release 2012 SP1 (**SCVMM 2012 SP1**).

How to do it...

In this section we will configure the Microsoft Hyper-V 3.0 system and the XenDesktop installation for them to be able to communicate with each other:

1. On a clean Windows Server 2012 installation, with no other roles installed, on the **Server Manager** dashboard, click on the **Add roles and features** link.





A clean installation is required to install the Hyper-V hypervisor role.

2. After clicking on **Next** on the **Before You Begin** section, select the **Role-based or feature-based installation** option, and then click on the **Next** button.

Role-based or feature-based installation
Configure a single server by adding roles, role services, and features.

Remote Desktop Services installation
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

3. In the **Server Selection** screen, choose the **Select a server from the server pool** option; highlight the server name on which you're currently installing the Hyper-V role; and click on the **Next** button.

Select a server or a virtual hard disk on which to install roles and features.

Select a server from the server pool
 Select a virtual hard disk

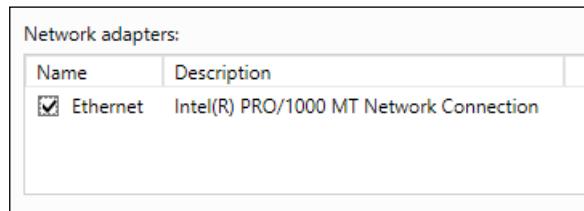
Server Pool

Name	IP Address	Operating System
WIN-37FKPD58HPV	192.168.198.128	Microsoft Windows Server 2012 Datacenter

4. Select the **Hyper-V** role in the **Server Roles** section, and when prompted to install the additional features, click on the **Add Features** button to accept. After this, click on the **Next** button three times to continue.

<input type="checkbox"/> DNS Server
<input type="checkbox"/> Fax Server
► <input checked="" type="checkbox"/> File And Storage Services (Installed)
<input checked="" type="checkbox"/> Hyper-V
<input type="checkbox"/> Network Policy and Access Services
<input type="checkbox"/> Print and Document Services
<input type="checkbox"/> Remote Access
<input type="checkbox"/> Remote Desktop Services

5. In the **Virtual Switches** section, select a network card to be used by Hyper-V to create the virtual switch for the virtual machine connections, and then click on the **Next** button.



6. In the **Migration** section, flag the Live-Migration feature option, and select one of the available authentication methods (**CredSSP** or **Kerberos**). After completion, click on **Next**.



Kerberos is a more secure authentication method. On the other hand, it could be harder to implement, despite the CredSSP configuration.



Hyper-V can be configured to send and receive live migrations of virtual machines on this server. Configuring Hyper-V now enables any available network on this server to be used for live migrations. If you want to dedicate specific networks for live migration, use Hyper-V settings after you install the role.

Allow this server to send and receive live migrations of virtual machines

Authentication protocol

Select the protocol you want to use to authenticate live migrations.

Use Credential Security Support Provider (CredSSP)

This protocol is less secure than Kerberos, but does not require you to set up constrained delegation. To perform a live migration, you must be logged on to the source server.

Use Kerberos

This protocol is more secure but requires you to set up constrained delegation in your environment to perform tasks such as live migration when managing this server remotely.



If your Hyper-V server is to be a part of a Microsoft clustered environment, you don't have to enable the live migration option. This will be performed after the cluster configuration.

7. In the **Default Stores** section, select available paths on which to allocate the virtual machine disks, and the virtual machine configuration files. After completion, click on the **Next** button.

Hyper-V uses default locations to store virtual hard disk files and virtual machine configuration files, unless you specify different locations when you create the files. You can change these default locations now, or you can change them later by modifying Hyper-V settings.

Default location for virtual hard disk files:

C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks

Default location for virtual machine configuration files:

C:\ProgramData\Microsoft\Windows\Hyper-V

8. If the information in the **Confirmation** section is correct, flag the **Restart the destination server automatically if required** option, and click on **Install** to complete the role installation.

To install the following roles, role services, or features on selected server, click **Install**.

Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click **Previous** to clear their check boxes.

Hyper-V
 Remote Server Administration Tools
 Role Administration Tools
 Hyper-V Management Tools
 Hyper-V Module for Windows PowerShell
 Hyper-V GUI Management Tools

9. After completing the Windows Server Hyper-V role configuration, download the SCVMM 2012 SP1 software from the Microsoft portal at this link: <http://technet.microsoft.com/en-us/systemcenter/cc137824.aspx>.



For performance reasons, you have to install the SCVMM server on a machine other than XenDesktop Controller; instead, the SCVMM console must be installed on any configured Delivery Controller.

10. On a server other than Delivery Controller, run the SCVMM setup by extracting the download archive or by mounting the related ISO, and then launch `setup.exe` from the destination folder.
11. On the main screen, click on the **Install** link in the **Virtual Machine Manager** section.



Before the SCVMM installation, be sure you've installed and configured IIS Web Server and **Windows Assessment and Deployment Kit (ADK)** for Windows 8 (available at <http://www.microsoft.com/en-us/download/confirmation.aspx?id=30652>).

12. In the **Select features to install** list, select **VMM Management Server**, and then click on **Next**. The **VMM Console** component will be automatically selected as shown in the following screenshot:



13. Enter the relevant data in the **Name, Organization, and Product Key** fields, and then click on **Next**.



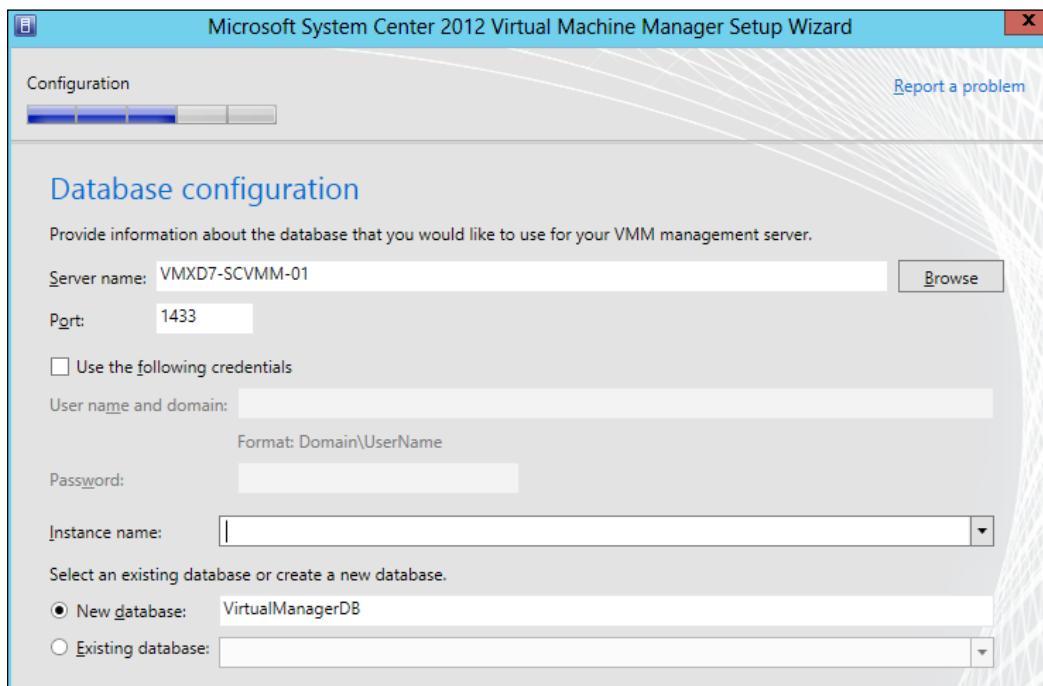
You can also insert your license number after the installation procedure.

14. Accept the License agreement (flag **I've read, understood and agree with the terms of license agreement**), and click on **Next**.
15. Check the appropriate radio button depending on whether you want to participate in the Microsoft collaboration program or not, and click on **Next** to continue.
16. In the Microsoft Update section, select the desired radio button (**On (recommended)** or **Off**), and then click on **Next** to continue.

17. Select the **Installation location** by typing it in the **Location** field, and proceed by clicking on **Next**.



18. After passing the prerequisites check, you must specify the database location (**Server name** and **Port**), Windows administrative credentials (check the **Use the following credentials** checkbox), **Instance name and Database name**, choosing between **New database** creation or **Existing database** utilization.



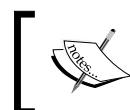


SCVMM 2012 SP1 does not support the SQL Server Express edition!



19. Select whether you are using a **Local system account** or a **Domain account** (service type), and decide if you want to save the encryption keys in Active Directory by flagging the specific option; in this case you also have to specify on which Active Directory machine object you are archiving the keys. To proceed click on the **Next** button.

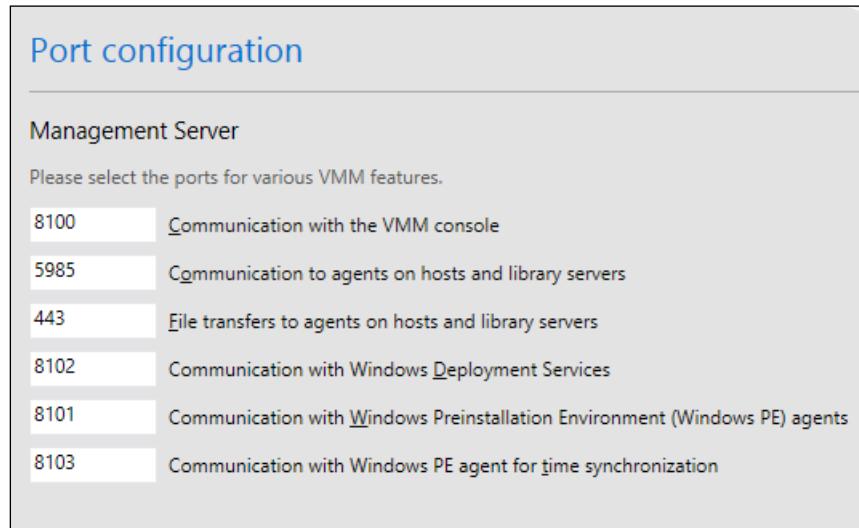
The screenshot shows the 'Configure service account and distributed key management' dialog box. It has two main sections: 'Virtual Machine Manager Service Account' and 'Distributed Key Management'. In the 'Virtual Machine Manager Service Account' section, there is a note about selecting a service account type (Local System or Domain) and a note about storing encryption keys in Active Directory. The 'Domain account' radio button is selected. In the 'Distributed Key Management' section, there is a note about storing keys in Active Directory and a checkbox for 'Store my keys in Active Directory'. A link 'How do I configure distributed key management?' is at the bottom.



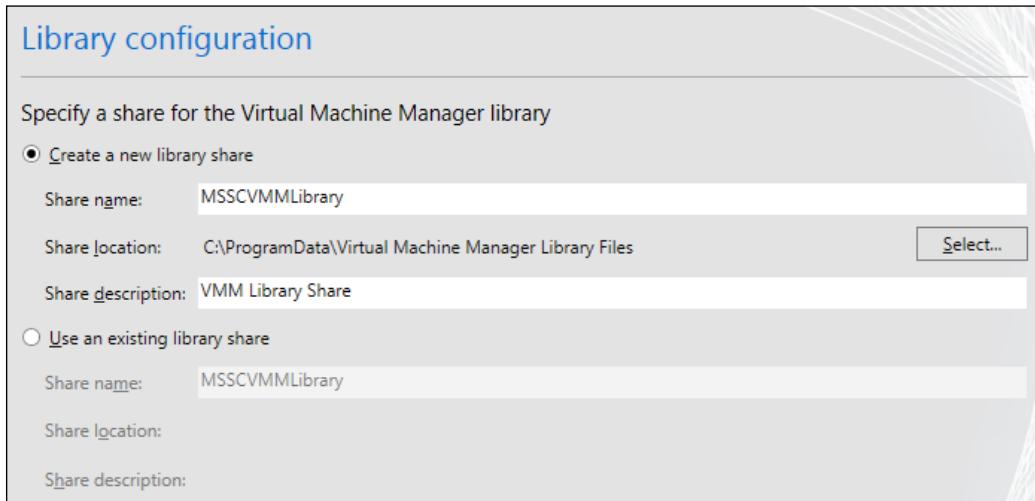
When possible, always consider using Domain accounts in order to have a centralized profile instead of a local and replicated account.



20. Configure the ports for server communication as done in the following screenshot, and then click on **Next**:



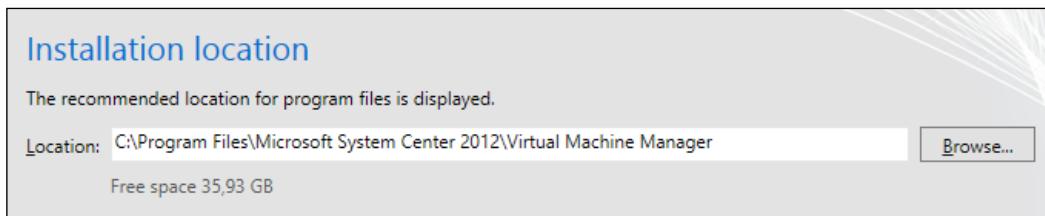
21. On the next screen, you can choose to create a new VMM library (**Create a new library share**, including **Share location** and **Share description**), or use an existing one (**Use an existing library share**) by selecting the second radio button. Click on the **Next** button to continue.



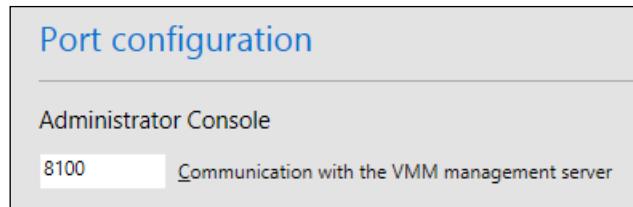
22. If the summary information is **OK**, click on the **Install** button to complete the procedure.
23. Once the server components' installation is terminated, you need to install the *Management Console* on all the Delivery Controller machines within your infrastructure. Repeat the launching setup procedure seen for Server components, and only then flag the **VMM Console** component.
24. After accepting the License Agreement, click on **Next** to proceed; on the next screen, you'll be informed that you have automatically joined the Microsoft collaboration program. Click on the **Next** button to continue.
25. Click on the **On** radio button to activate updates, and then click on **Next**.



26. Select the installation **Location** by populating the **Location** field as seen earlier, and click on **Next**.



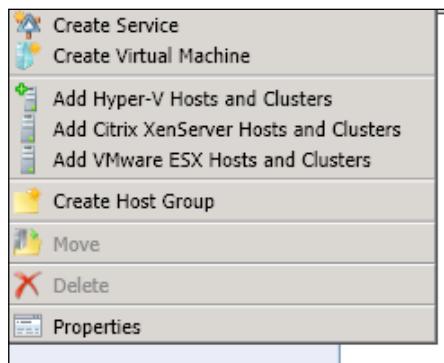
27. Select a port on which to configure the console (**Communication with the VMM management server**, default port 8100), and click on **Next** to proceed.



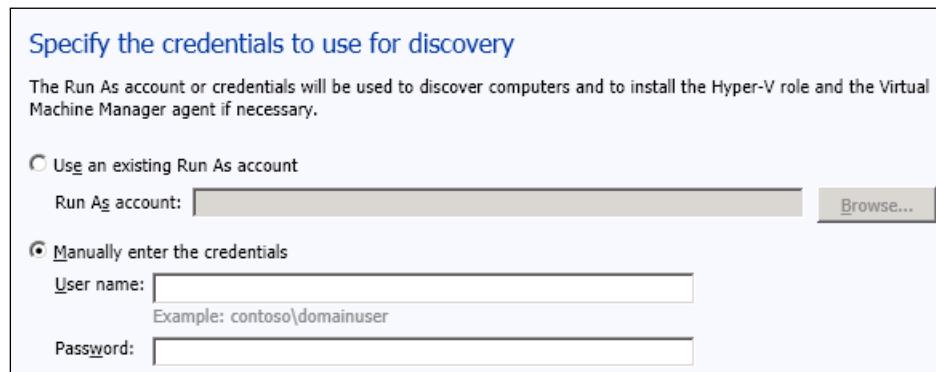
28. If the information on the **Installation** summary is correct, click on **Install** to complete this procedure.
29. After setup has been completed, click on **Close** and leave **Open the VMM console when this wizard closes** checked.
30. At the logon screen, insert **Server name** and port (in the form of hostname:port) for the SCVMM Server, and specify credential access. You can choose **Use current Microsoft Windows session identity** or select **Specify credentials**. Click on **Connect** to proceed with the login.



31. Once logged in, right-click on **All Hosts** on the left-hand side menu, and select **Add Hyper-V Hosts and Clusters**.

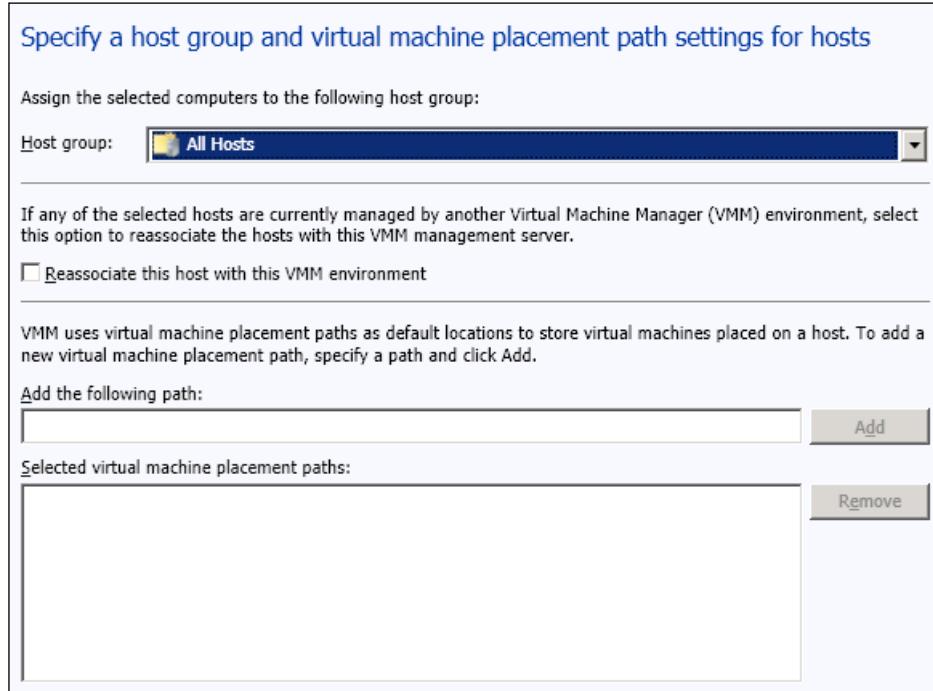


32. Select a Hyper-V host location from one of the following, and click on **Next**:
- Windows Server computers in a trusted Active Directory domain**
 - Windows Server computer in an untrusted Active Directory domain**
 - Windows Server computers in a perimeter network**
 - Physical computer to be provisioned as virtual machine hosts**
33. Insert the **User name** and **Password** (**Use an existing Run As account** or **Manually enter the credentials** checkbox) to run resource discovery for Hyper-V, and then click on **Next**.



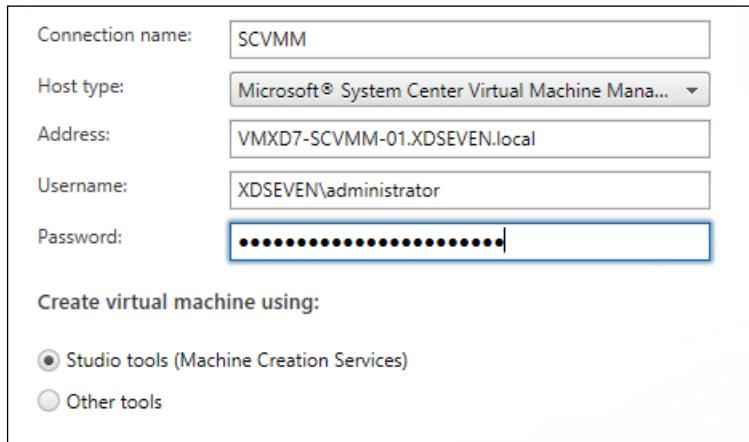
34. Specify a discovery scope (**Specify Windows Server computers by names** or **Specify an Active Directory query to search for Windows Server computers**) to reduce the range on which it performs the host's searches.
35. After you've received query results, flag the desired host(s), and proceed by clicking on **Next**.

36. Select a **Host group** on which to attach the selected Hyper-V server; if you want, you can also check the option **Reassociate this host with this VMM environment**. After this, specify a location on which to store virtual machines, and click on **Next** to proceed.



37. If the configuration information is compliant with your environment parameters, click on **Finish** to complete the procedure.
38. As previously done for XenServer and vSphere, run Citrix Studio, and select the **Hosting** link from the Configuration section.
39. On the right-hand side menu, click on **Add Connection and Resources**

40. In the **Connection** section, select **Microsoft System Center Virtual Machine Manager** from the **Host type** drop-down menu in the **Address** field; input the FQDN of the Microsoft console host; insert **Username** and **Password** in the respective fields; and give a name to the connection (**Connection name** input text). In the **Create Virtual machine using:** subsection, select the **Studio tools (Machine Creation Services)** radio button, and after that is completed, click on **Next** to continue.

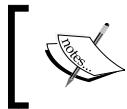


41. Select your Hyper-V configured resource from the list, assign it a name by populating the **Enter a name for the Resources** field, flag the desired network virtual switch from the list, and click on **Next**.
42. In the App-V Publishing section, skip any configuration for the moment. We will discuss App-V later in this book. Click on **Next** to continue.
43. Select the storage on which to archive the virtual machine; it's also possible to separate the VM's operating system storage from personal vDisk storage. After completing this, click on **Next**.
44. In the **Summary** screen, after you have verified all the configured options, click on the **Finish** button to complete the procedure.

How it works...

Citrix XenDesktop 7 is able to communicate with Microsoft Hyper-V servers only using Microsoft SCVMM. In this recipe, we have discussed how to install and configure the 2012 SP1 version, the release associated with the Windows Server 2012 edition.

Being more specific, it uses the *SDK* platform offered by Microsoft System Center; for this reason, we've previously installed the VMM console (the *SDK* is included in it) on Delivery Controller. This is an interaction similar to that used for VMWare vSphere. So, you can consider System Center as similar to VMWare Virtual Center, by which, system engineers can centrally manage all configured Hyper-V hosts in a server farm.



SCVMM is able to manage not only Hyper-V hosts, but also hypervisors from different vendors. So, you can also consider using it to centrally manage the Citrix XenServer and VMware vSphere machines.



See also

- ▶ The *Publishing applications using Microsoft App-V* recipe in Chapter 7, *Deploying Applications*

3

Master Image Configuration and Tuning

In this chapter, we will cover the following recipes:

- ▶ Configuring and optimizing a desktop OS master image
- ▶ Configuring and optimizing a server OS master image
- ▶ Configuring a target device – PVS architecture
- ▶ Installing and configuring the master image policies

Introduction

In *Chapter 1, XenDesktop® 7 – Upgrading, Installing, and Configuring*, and *Chapter 2, Configuring and Deploying Virtual Machines for XenDesktop®*, we installed and configured important **Virtual Desktop Infrastructure (VDI)** components such as database servers, XenDesktop components, and Hypervisor servers for virtual machine creation and provisioning. Now it's time to put aside this class of elements for a while and concentrate our activities on desktop client components.

End users will interact only with Windows desktop machines and not with the architectural components shown earlier. So, you have to be careful about the configuration process for virtual desktops in terms of building a desktop image, optimization, and tuning.

Most of your activities on clients will be based on policy usage and optimization in order to obtain high-level user experience without compromising on agility, performance, and security.

Configuring and optimizing a desktop OS master image

The first important task will be the configuration and the optimization of the Windows desktop OS operating systems, which will be used as a master image, in order to deploy the desktop instances. The latest version of the Microsoft operating systems offer a lot of graphical enhancements useful to better appreciate their potential and usability. In a complex VDI architecture, we need to be careful about both of these aspects as shown in the previous recipe. Consider that this customization process can vary depending on the configured environment. Anyway, the steps implemented in this section can be generally applied without specific issues.

Getting ready

This recipe involves only the Windows client machine. In order to be able to carry out all modifications to the services, the graphical appearance, and the system configuration, you need to use domain or local administrative credentials for Windows 7 and Windows 8 OS versions. An installed virtual machine with a Windows 7 or Windows 8 operating system is required in order to apply the described settings.



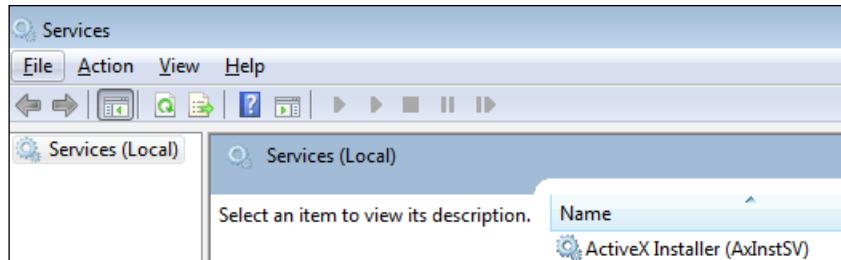
Refer to *Chapter 2, Configuring and Deploying Virtual Machines for XenDesktop®*, to learn about how XenDesktop chooses the right virtualization platform for your specific needs.

How to do it...

The modification activities of the desktop optimization policies involve only the Windows client machine and the domain to which it has been joined. So, you will need domain administrative credentials in order to be able to modify the necessary policies and to force their application on the involved clients. The following are the optimization processes for Windows 7 and Windows 8.

For the Windows 7 master image configuration, the process is as follows:

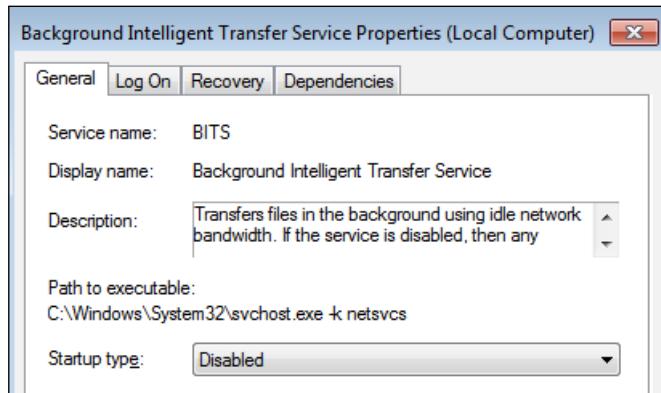
1. Log in to your Windows 7 base image template with administrative credentials.
2. Click on **Start** and type the `services.msc` command. The Windows **Services** snap-in will be opened, as shown in the following screenshot:



3. From the services list, search for this service: **Background Intelligent Transfer Service**.

Application Layer Gateway Service	Manual
Application Management	Manual
Background Intelligent Transfer Service	Started
Base Filtering Engine	Started

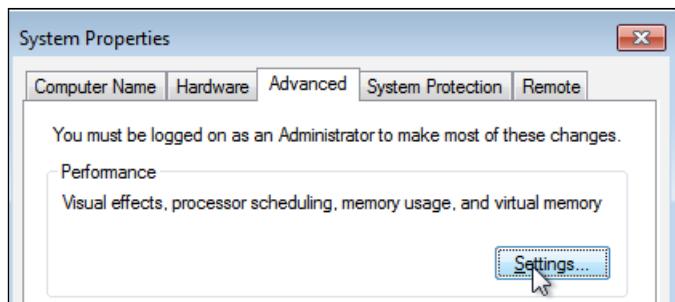
4. Right-click on the name of the service, and select **Properties** from the menu that comes up.
5. From the **Startup type** drop-down list, select **Disabled** as the default state as shown in the following screenshot. Click on **Stop** if the service is running and then click on **OK** to exit from this area:



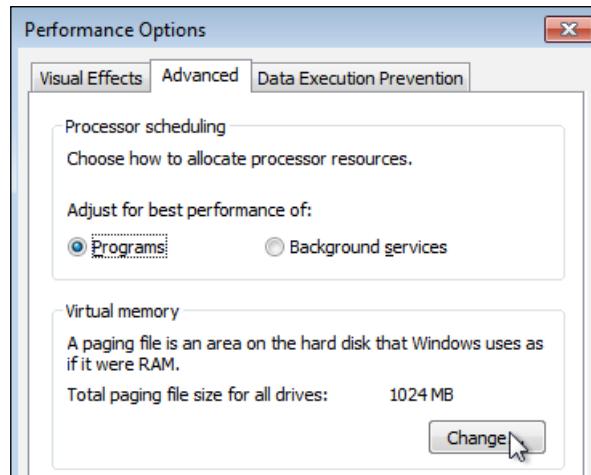
6. Repeat steps 4 and 5 to disable the following services:
 - Desktop Windows Manager Session Manager**
 - HomeGroup Listener**
 - HomeGroup Provider**
 - Windows Search**

- ❑ **Security Center**
- ❑ **Superfetch**
- ❑ **Windows Defender**
- ❑ **Windows Media Player Network Sharing Service**

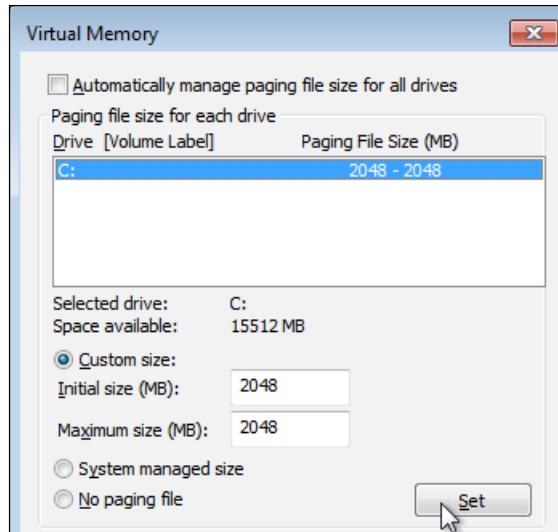
7. Click on **Start** and run the cmd command to open a prompt shell. Then, run the following command—required to disable Windows's animation at boot time—in order to achieve faster machine startup:
`bcdedit /set bootux disabled`
8. Navigate to **Start | Control Panel** and click on the **System** icon. Then, select **Advanced system settings** from the left-hand side menu.
9. Select the **Advanced** tab and click on the **Settings** button in the **Performance** area.



10. Select the **Advanced** tab and click on **Change** in the **Virtual memory** area, as shown in the following screenshot:



11. Uncheck the **Automatically manage paging file size for all drives** option. Then, select the **Custom size** radio button and enter the same value in both textboxes.
12. After entering the values, click on **Set** and then on **OK**, as shown in the following screenshot:



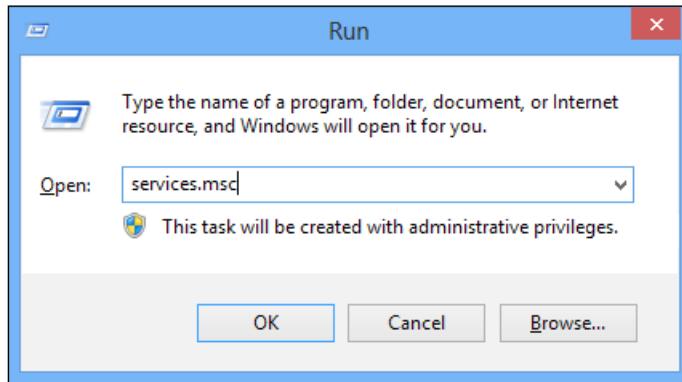
[ It's common to assign a value twice that of the machine memory to the swap memory area (for example, for 1 GB of RAM you'd assign a 2 GB swap size).]

13. After the amount of swap has been modified, you need to restart your machine for the changes to come into effect.

For the Windows 8 master image configuration, the process is as follows:

1. Log in to your Windows 8 master image with administrative credentials.

2. Hit the Windows + R keys simultaneously and type the `services.msc` command. Then click on **OK**, as shown in the following screenshot:



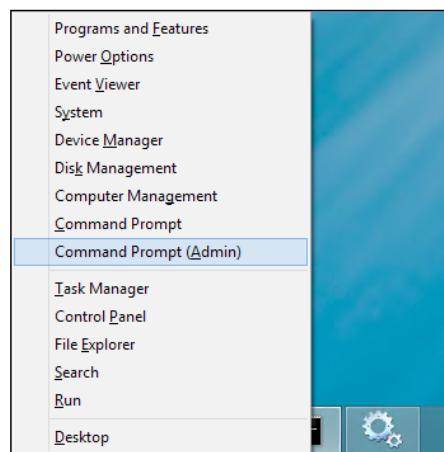
3. In the Windows **Services** snap-in, search, and disable the following services:
 - Application Layer Gateway Service**
 - Background Intelligent Transfer Service (BITS)**
 - BitLocker Drive Encryption Service**
 - Block Level Backup Engine Service**
 - Bluetooth Support Service**
 - Computer Browser**
 - Device Association Service**
 - Device Setup Manager**
 - Diagnostic Policy Service**
 - Diagnostic Service Host**
 - Diagnostic System Host**
 - Family Safety**
 - Function Discovery Resource Publication**
 - Internet Connection Sharing (ICS)**
 - Microsoft iSCSI Initiator Service**
 - Microsoft Software Shadow Copy Provider**
 - Optimize Drives**
 - Secure Socket Tunneling Protocol Service**
 - SSDP Discovery**
 - Superfetch**
 - Telephony**
 - Windows Backup**

- Windows Color System**
- Windows Connect Now – Config Registrar**
- Windows Error Reporting Service**
- Windows Media Player Network Sharing Service**
- WLAN AutoConfig**
- WWAN AutoConfig**

Name	Description	Status	Startup Type
ActiveX Installer (AxInstSV)	Provides User Acco...	Running	Manual
Application Experience	Processes applicati...	Running	Manual (Trigger Start)
Application Identity	Determines and ver...	Running	Manual (Trigger Start)
Application Information	Facilitates the runni...	Running	Manual
Application Layer Gateway Service	Provides support fo...	Disabled	Disabled
Application Management	Processes installati...	Running	Manual
Background Intelligent Transfer Service	Transfers files in th...	Disabled	Disabled
Background Tasks Infrastructure Service	Windows infrastruc...	Running	Automatic
Base Filtering Engine	The Base Filtering E...	Running	Automatic
BitLocker Drive Encryption Service	BDESVC hosts the B...	Disabled	Disabled
Block Level Backup Engine Service	The WBENGINE ser...	Disabled	Disabled
Bluetooth Support Service	The Bluetooth servi...	Disabled	Disabled
BranchCache	This service caches ...	Disabled	Disabled

[ To activate touch features (RemoteFX Multi-Touch), you have to install the Windows 8 Enterprise edition.]

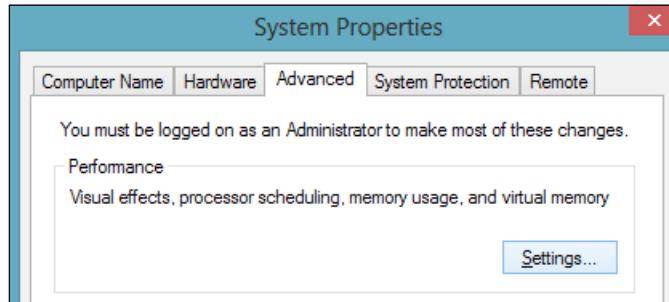
4. After completing the configuration of the services components, hit the Windows + X keys, and then select the **Command Prompt (Admin)** option, as shown in the following screenshot:



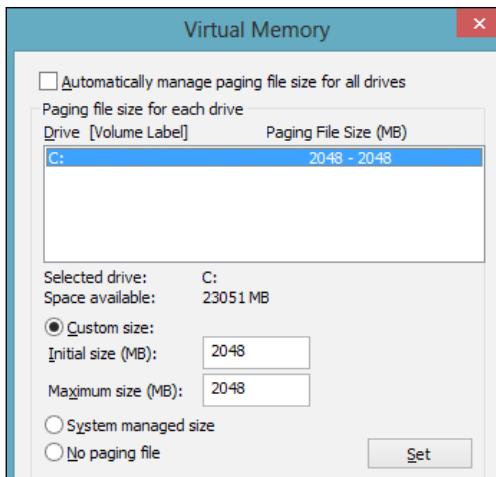
5. At the shell prompt, run the commands indicated in the following lines; these will be used to customize the Windows 8 boot experience, in order to disable the Windows 8 boot screen, the Windows 8 boot logo, and the Windows 8 boot messages, respectively:

```
bcdedit /set {globalsettings} custom:16000069 true  
bcdedit /set {globalsettings} custom:16000067 true  
bcdedit /set {globalsettings} custom:16000068 true
```

6. To apply the boot configuration changes, you have to restart your Windows 8 machine.
7. After the reboot has been completed, press the Windows + X keys and select the **System** option. Then click on the **Advanced system settings** link on the right-hand side of the **System** screen.
8. On the **System Properties** screen, click on the **Settings** button; in the **Performance** subsection, click on the **Advanced** tab, as shown in the following screenshot:



9. On the **Performance Options** screen, select the **Advanced** tab and click on the **Change** button in the **Virtual Memory** subsection.
10. As seen earlier for Windows 7, we have to fix the minimum and maximum quantity of swap with a fixed and equal value here as well. To do this, uncheck the **Automatically manage paging file size** option for all drives, select the **Custom size** radio button, and enter the desired swap value (**Initial size** and **Maximum size**). After that, click on **Set** as shown in the following screenshot, and then on the **OK** button:



11. In order to apply the modified swap parameters, you need to reboot the master image.



Even though we have discussed the Windows 7 configuration, we will only generate catalogs with the Windows 8 version of the operating system in this book.

How it works...

To reduce the usual overtime needed by Windows 7 and Windows 8 machines to boot and start up all services, we've disabled some of them that are not necessary for regular operating system usage in a VDI configuration.

In order to optimize the operating system, we have performed the following configurations:

- ▶ We have disabled the animation presented at boot time (with a time reduction of approximately 20 percent)
- ▶ We have reduced the impact on the network by disabling BITS. Background Intelligent Transfer Services (BITS) is used to automatically download programs or information with software such as Windows Update or Windows Live.
- ▶ We have reduced the impact on the virtual machine CPU and memory usage by disabling services such as Desktop Window Manager Session Manager and the Desktop Window Manager (DWM) service, which manages the Windows Aero graphical user interface).



Disabling Aero will dramatically improve the performance, but on the other hand, the user experience quality could be lower than the expected levels.

- ▶ For CPU/RAM resources, we have also reduced the service's impact on the system by disabling indexing (Windows Search, not required in a nonpersistent VDI environment), system protection (Security Center and Windows Defender substituted by system protection software that is better integrated with VDI and that we're going to explain in this book), and unnecessary multimedia components (Windows Media Player Network Sharing Center).



Disabling the Windows Search service could have an impact on specific indexing functions, for instance, in the case of the Microsoft Outlook e-mail client.

- ▶ The last-performed operation is the assignment of a single value (for both minimum and maximum size parameters) for the swap area memory size.



For both the operating systems, you could consider disabling the operating system's long-term performance optimizer (the Superfetch service) discussed earlier, in the case of nonpersistent machine deployments. Disabling this service is particularly useful in the case of SSD disks in terms of disk space and faster boot time (no more prefetch files will load during the startup phase).

For the Windows 8 environment, we have also specified infrastructural services, which are unnecessary for VDI deployments, such as Bluetooth, iSCSI, and Telephony component initiator (you won't use them on a virtual machine), or troubleshooting components, which could cause loss of meaning within a VDI infrastructure configured with nonpersistent machines (such as Diagnostic Policy Service or Diagnostic Service / System Host).



Disable the Windows Search (Indexing) service only in the case of nonpersistent Virtual Desktops; in any other case, you should keep it active to avoid general content search issues.

As a general plan, you should use desktop OS machines when users require a particular customization of their work environment in terms of installed software and/or personal data, with the management of resources by IT staff in the form of heterogeneous pools (persistent, nonpersistent, and so on).

There's more...

To improve the responsiveness of your Windows machines, you could also apply the following operating system configurations:

- ▶ Reduce the event log size and retention to the minimum in terms of the number of days for which events are retained and the number and types of events logged
- ▶ Remove all unnecessary scheduled system tasks
- ▶ Install and configure an antivirus platform compatible with a VDI architecture



A useful guide to configuring the antivirus exclusions correctly can be found at <http://blogs.citrix.com/2013/09/22/citrix-consolidated-list-of-antivirus-exclusions/>.



See also

- ▶ The *Administering hosts and machines – the Host and Machine Creation cmdlets* recipe in Chapter 9, *Working with XenDesktop® PowerShell*

Configuring and optimizing a server OS master image

XenDesktop 7 includes the ability not only to publish standard desktop operating systems but also to deploy desktops of the server edition of the Microsoft operating system. In this chapter, we will discuss the best practices to apply to obtain better user experience.

Getting ready

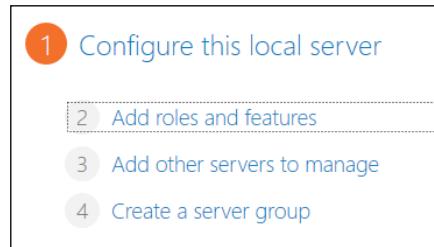
In order to complete all the required steps for this recipe, you need to connect to the Windows Server 2012 machine with administrative credentials to be able to install and configure all the necessary features.

How to do it...

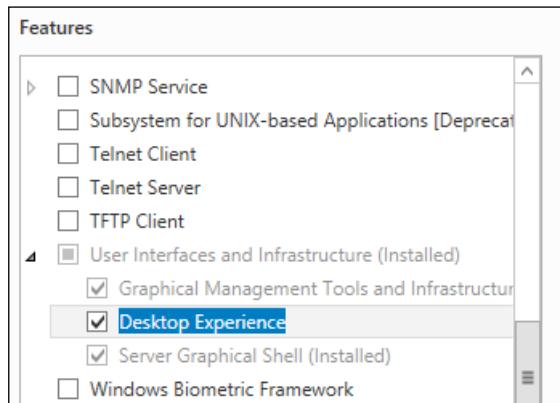
In the following steps, we will describe how to improve the graphical and user experience for a Windows Server 2012 operating system in order to deploy desktops of server operating systems later in this book:

1. Connect to the selected Windows Server 2012 machine with domain administrative credentials.
2. Start the **Server Manager** utility if it has not automatically been started.

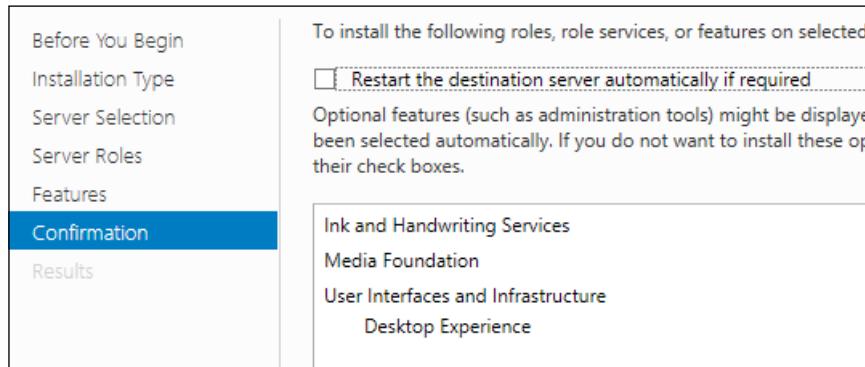
3. In the **Configure this local server** section, click on the **Add roles and features** link as shown in the following screenshot:



4. On the **Add Roles and Features Wizard** screen, click on the **Next** button to continue.
5. On the **Installation Type** menu, select the **Role-based or feature-based installation** option and click on **Next** to continue.
6. In the **Server Selection** menu, check the **Select a server from the server pool** radio button, select the machine on which you're configuring the user experience, and then click on **Next** to proceed.
7. On the **Server Roles** screen, click on the **Next** button without selecting any option to skip role configuration.
8. In the **Features** section, expand the **User Interfaces and Infrastructure** voice and check the **Desktop Experience** option. When prompted for additional required components, click on the **Add Features** button and then click on **Next**.



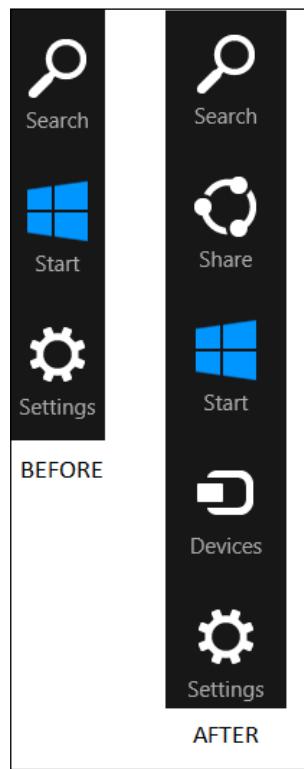
9. In the **Confirmation** box, click on the **Install** button to complete the activation procedure as shown in the following screenshot:



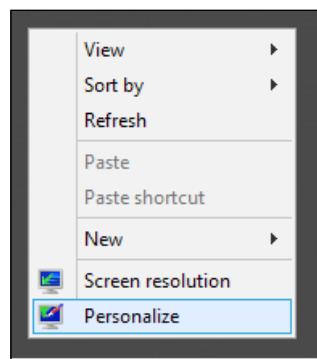
10. After that, click on the **Close** button and reboot the Windows Server 2012 machine.
11. Reconnect with the same domain administrative credentials. You will know that the features have been enabled when you see a Windows 8-like start menu as the first screen.



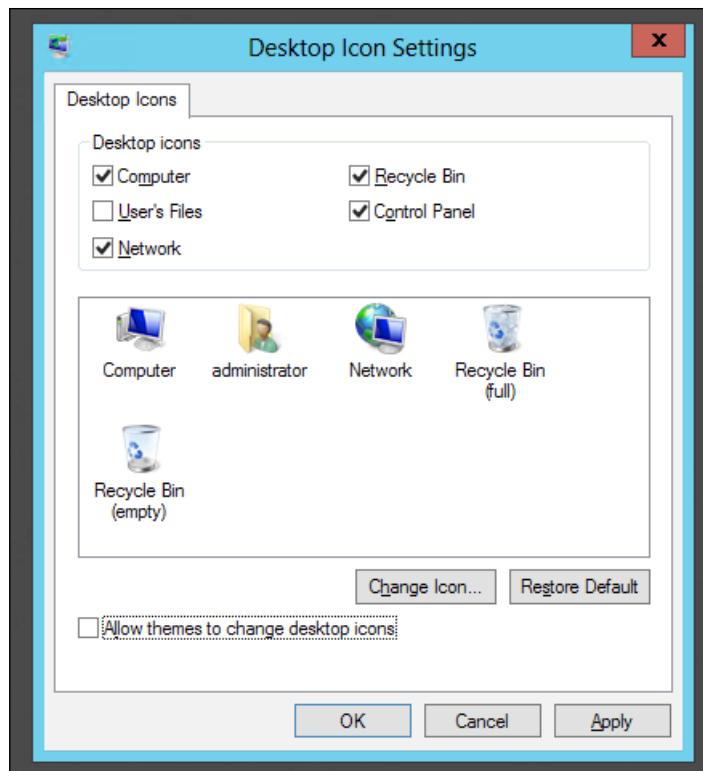
12. By using the Windows + C key combination, it's also possible to view the newly installed features as shown in the following screenshot:



13. From the Start menu, click on the **Desktop** icon. Once you have been moved to the desktop view, right-click on it, and select the **Personalize** option, as shown in the following screenshot:

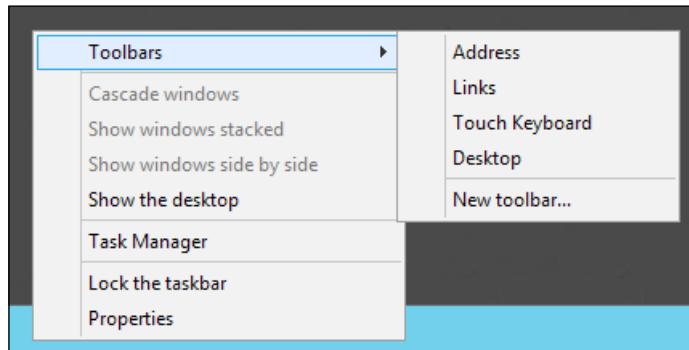


14. On the **Personalization** menu, click on the **Change desktop icons** link on the left-hand side menu.
15. On the **Desktop Icon Settings** screen, enable the desired icons and uncheck the **Allow themes to change desktop icons** checkbox. Then, click on the **Apply** button first and click on **OK**, as shown in the following screenshot:



You should avoid using desktop background images for a server operating system. The purpose of this recipe is to create the right balance between the graphical experience and desktop performance.

16. On the **Desktop** view, right-click on the Windows **Taskbar** and select the **Toolbars** option. Click on one or more options that you want to enable on the bar.



[The **Touch Keyboard** option could be particularly useful when using the Windows Server 2012 desktop on a tablet or a smartphone.]

How it works...

The configuration of a Windows Server operating system version for VDI purposes is slightly different than normal Windows Desktop platforms. In fact, the most important thing to understand is that a system administrator has to maintain the right balance between the graphical experience for end users and the performance required by the operating system to perform its normal activities. Starting with this point of view, the use case to which we apply the deployment of a server operating system should include one or all of the following points:

- ▶ The deployed machines will be allocated per session based on a mechanism by which the first user that requires a desktop is served.
- ▶ The deployed machines are standard and noncustomizable. This means that users can't install applications but have to use only the proposed environment.



This hint can be also applied to the previously discussed desktop OS environments.

- ▶ The VDI environment has been designed to assign and maintain only the required instances with a one-to-many association (one server desktop, many users).

In this recipe, we have performed the installation and configuration of the native user experience feature in Windows Server 2012—Desktop Experience. As a result, it's now possible to use features which you could find, by default, in desktop operating systems versions, such as the Windows bar seen in one of the previous screenshots or system tools such as Windows Media Player, desktop themes (which should be used with care to avoid performance issues arising from high-resolution graphics), video for Windows, or Sound Recorder.

See also

- ▶ The *Configuring the XenDesktop® policies* recipe in *Chapter 8, XenDesktop® Tuning and Security*

Configuring a target device – PVS architecture

After describing the process of the basic configuration of a master image, desktop, or server, it's time to pass from the MCS architecture configuration type to the **Provisioning Services (PVS)** previously discussed in this book. In this recipe, we will explain how to configure an operating system target device, which will be used later in this book to deploy machine catalogs for the Provisioning Services offer.

Getting ready

The main required step for this recipe is installing a Windows 8 virtual machine, which will be used as the master image for the deployment of the virtual desktop instances within a XenDesktop PVS configuration.



You can refer at the following Microsoft link for the Windows 8 installation procedure: <http://technet.microsoft.com/en-us/windows/hh974336.aspx>.

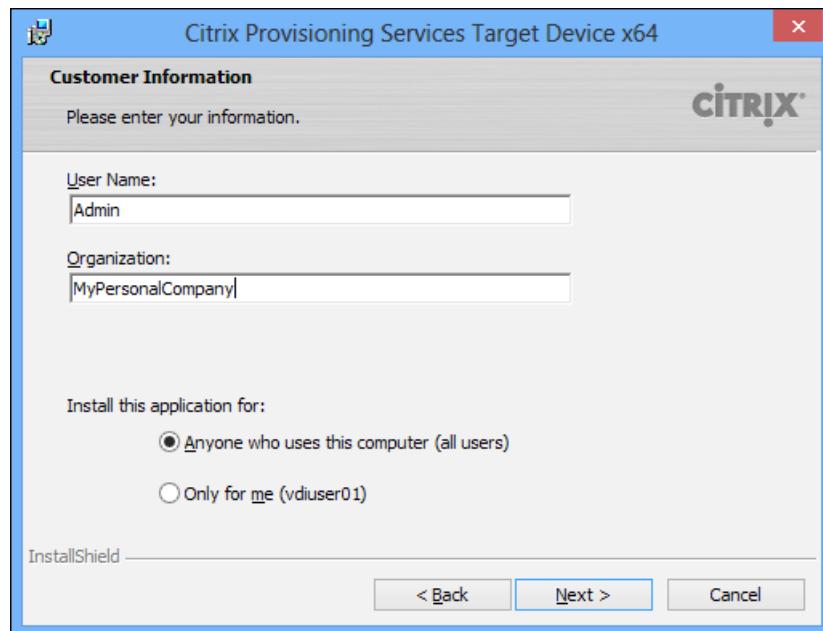


How to do it...

In the following steps, we will describe how to configure a Windows 8 machine as a target device for the PVS architecture:

1. After downloading the ISO file from your personal Citrix account, mount the Provisioning Services 7.0 ISO by right-clicking on it and selecting the **Mount** option. Perform this task on the machine that will be used as the target device.
2. Connect to the Windows virtual machine by using domain administrative credentials.
3. Browse the mounted PVS 7.0 CD-ROM, and then double-click on the autorun.exe executable file.

4. On the **Citrix Provisioning Services** menu, select the **Target Device Installation** option by clicking on it. On the new selection menu, click again on the **Target Device Installation** link.
5. On the **Welcome** screen, click on **Next** to continue.
6. In the license agreement section, accept the terms and click on the **Next** button.
7. Populate the **Customer Information** section with the required information. After that, click on **Next** to proceed, as follows:



8. On the **Destination Folder** screen, select a valid path on which you will be installing the agent and then click on the **Next** button.
9. In the **Ready to Install the Program** section, click on **Install** to start with the installation process.
10. After the installation has been completed, leave the **Launch Imaging Wizard** checkbox enabled and click on the **Finish** button.
11. After clicking on **Next** on the **Welcome** screen, populate the required fields to connect your target machine to the PVS server. After that, click on **Next** to continue.

Connect to Farm

Enter the name or address of a server in the farm to connect to.

Server information

Server:

Port:

Credentials

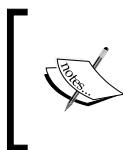
Use my Windows credentials

Use these credentials

User name:

Password:

Domain:



Please refer to the *Installing and configuring Provisioning Services 7* recipe in *Chapter 1, XenDesktop® 7 – Upgrading, Installing, and Configuring*, for the Citrix Provisioning Services installation steps.

12. In the **Select New or Existing vDisk** section, select the **Create new vDisk** option and click on the **Next** button.
13. On the **New vDisk** screen, assign a name to the vDisk, associate it with a configured store, and select **vDisk type (Fixed or Dynamic)**. In the case of a dynamic disk, you can also choose the correct **vDisk block size** as per your needs (**2 MB** or **16 MB**). After that, click on **Next**.

vDisk name:

Store:

Accessible by server: VMXD7-PVS-01

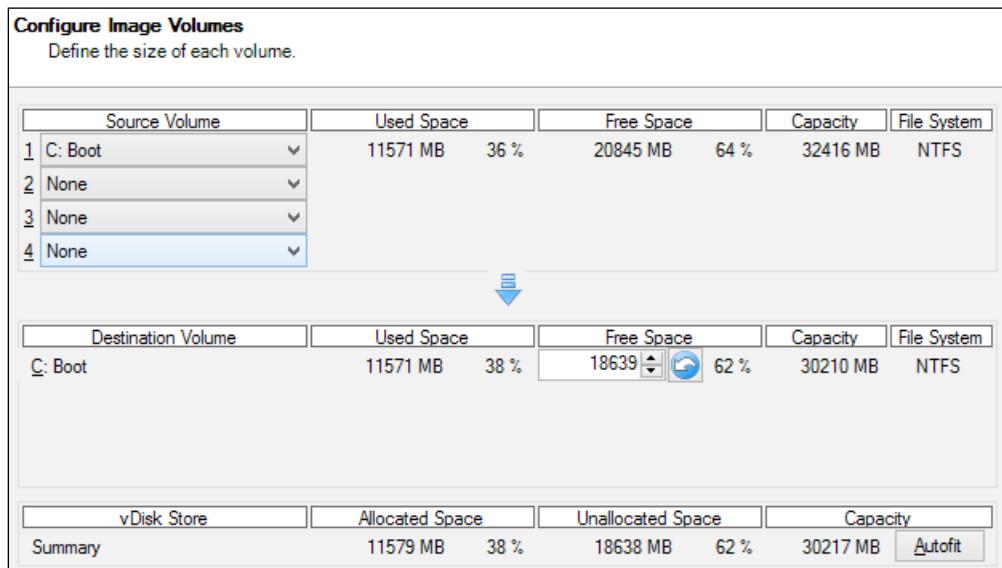
vDisk type:

vDisk block size:

14. Select what kind of license activation mode you want to enable (**Multiple Activation Key (MAK)**, **Key Management Services (KMS)**), or **None**, and then click on the **Next** button.

[ With the latest release of the PVS, in the presence of valid KMS licenses, you should always consider using the KMS server to activate and manage your Windows licenses.]

15. In the **Configure Image Volumes** section, you have to configure the dimension of the disk image size, which must be at least the minimum original disk dimension. After completing this step, click on **Next**, as shown in the following screenshot:



16. In the **Add Target Device** section, configure the following fields:

- Target device name:** The name of the target device
- MAC:** The MAC address of the network card (from the presented drop-down list)
- Collection:** The configured collection to which a device is assigned

17. After that, click on **Next**, as shown in the following screenshot:

The screenshot shows the 'Target device name' field set to 'XD7-W8-T01'. A note below it states: 'Note: The target device name cannot be the same Active Directory name of this machine.' The 'MAC' field is set to 'Ethernet 00-0C-29-E8-0C-01'. The 'Collection' dropdown is set to 'Collection00'. At the bottom, it says 'In the Site00 site of server: VMXD7-PVS-01'.



Refer to the *Installing and configuring Provisioning Services 7* recipe in Chapter 1, *XenDesktop 7 – Upgrading, Installing, and Configuring*, for more information about the Provisioning Services platform installation.

18. On the **Summary of Farm Changes** screen, if all the information is correct, click on the **Finish** button to complete device configuration.

The screenshot shows the summary of changes. It lists the creation of a new vDisk named 'TD-Vdisk-0' with a store 'Store0000', type 'Dynamic', size '30217', VHD block size '16 MB', Microsoft Volume Licensing 'Multiple Activation Key (MAK)', and volume 'C: 11571 MB used, 18638 MB free, 30209 MB capacity, NTFS system'. It also lists adding the machine to the farm with device name 'XD7-W8-T01', MAC '00-0C-29-E8-0C-01', and collection 'Collection00'. At the bottom is a blue button labeled 'Optimize for Provisioning Services'.

19. After clicking on the **Optimize for Provisioning Services** button, you can enable or disable with a checkbox the following features, used to optimize the PVS device:

- Disable Offline Files**
- Disable DefragBootOptimizationFunction**
- Disable Last Access TimeStamp**
- Reduce DedicatedDumpFile DumpFileSize to 2MB**
- Disable Move to Recycle Bin**
- Reduce IE Temp File**
- Disable Machine Account Password Changes**
- Disable windows Defender**
- Disable ScheduledDefrag**
- Disable ProgramDataUpdater**
- Disable Windows AutoUpdate**
- Disable Background Layout Service**
- Disable Hibernate**
- Disable Indexing Service**
- Reduce Event Log Size to 64k**
- Disable Clear Page File at Shutdown**
- Disable Windows SuperFetch**
- Disable Windows Search**
- Disable System Restore**
- Run NGen ExecuteQueuedItems (new Window)**

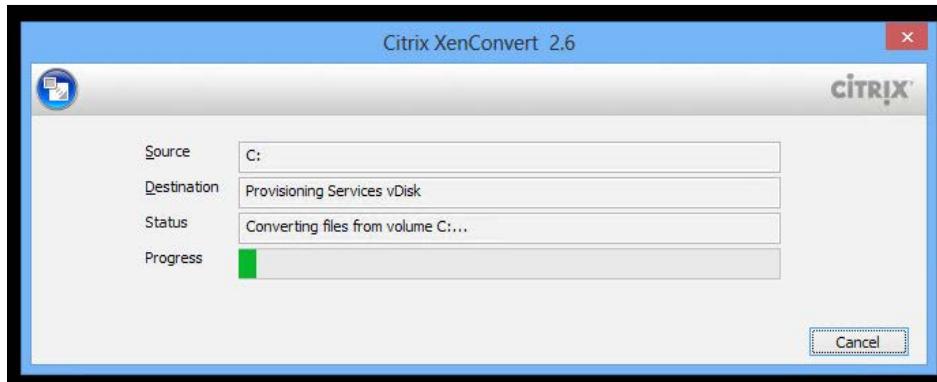
20. At the end of the operation of vDisk creation, reboot the Windows target machine and configure its BIOS to boot from the network.



During the network boot process, the virtual machine will connect to the PVS server. So, the XenConvert utility will be able to make a virtual machine copy and transfer it to the PVS server.



21. After the machine has been properly booted from the network—after the logon phase—you will find the **Citrix XenConvert** screen as shown in the following screenshot:



22. To check that all the target device configurations have been executed properly, connect to the PVS farm and check the existence of the earlier created vDisk in the **vDisk Pool** section.

Name	Store	Connections	Size	Mode
TD-Vdisk-0	Store0000	1	30.217 MB	Private

[ The available **Mode** for vDisks are **Standard** (vDisk shared among all the involved target devices) and **Private** (vDisk assigned and dedicated to a single specific target device).]

23. After the conversion has been completed, the target device will be available for use to deploy desktop instances by the PVS server and the desktop studio.

[ It's always possible to revert the virtual machine BIOS to boot from disk and not from the Provisioning Services vDisk over the network.]

How it works...

The procedure seen and explained in this recipe is about the generation of the master target device; this is the device that points to the master image template operating systems (in our case, Windows 8) from which the vDisk has been built. This component is the data container, which will be streamed to the configured target devices within a configured PVS farm. The device needs to be associated with a predefined PVS store and collection, and it is necessary to specify the MAC address (for network identification) and the kind of vDisk that has to be deployed (fixed or dynamic, which will be explained in the next section). The BIOS of the configured device must support network boot.

There's more...

As discussed earlier in this recipe, when creating a vDisk, we have the ability to choose between two kinds of disk formats: fixed disks and dynamic disks. The first type pre-allocates all the assigned disk space, while dynamic allocation populates disk files during data writing activities (if you're familiar with virtualization concepts, it's the same as thick and thin disk allocation). The following may help you to understand how to choose between fixed and dynamic disk:

- ▶ Because of the nature of fixed disks (full space preallocation), a fixed disk could be a waste of storage space.
- ▶ PVS uses memory caching mechanisms that reduce disk I/O activities. For this reason, dynamic allocation should be the right choice because of the huge reduction in storage reading activities. The only interfacing with disk components is given by writing operations. Also, in this case, after configuring the PVS vDisk image in read-only mode, we'll have almost no more storage activities, except for the write-cache operations. On the other hand, to have a responsive system, this infrastructure needs to be supported by 64-bit systems, the right memory sizing (for a PVS server, you should have a quantity of RAM between 8 GB and 32 GB), and a block-level storage device (SAN or iSCSI and not a network share repository on NAS).

 The write cache is a cache area on which the already written data is stored instead of being rewritten on the base vDisk. The write cache area can be a local PVS server hard disk, a specific remote server, or the PVS server's RAM cache. More information can be found at <http://support.citrix.com/proddocs/topic/provisioning-60/pvs-technology-overview-write-cache-intro.html>.

Using a fixed disk is a standard way to operate, which at the moment won't offer the advantages that a memory cache along with dynamic disk mode could give IT departments (in terms of performance and cost saving).

See also

- ▶ The *Administering hosts and machines – the Host and Machine Creation cmdlets* recipe in Chapter 9, *Working with XenDesktop® PowerShell*

Installing and configuring the master image policies

After you've completed installation procedures for the profile management client, it's time to configure the policies to apply to the domain-joined machines for the MCS/PVS architectures.

Getting ready

To configure the specific domain policies for the VDI environment, you need to have domain administrative permissions, and you also have to be able to propagate them to the client; these policies will be used as the master image template. You have to create a specific OU containing the involved VDI resources and apply this custom configuration only to the OU containing these machines.

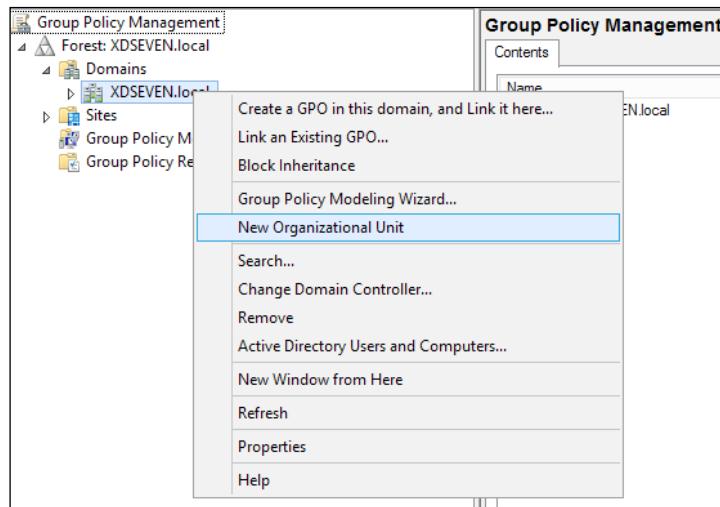
How to do it...

The following steps help us to configure the policies at the domain level:

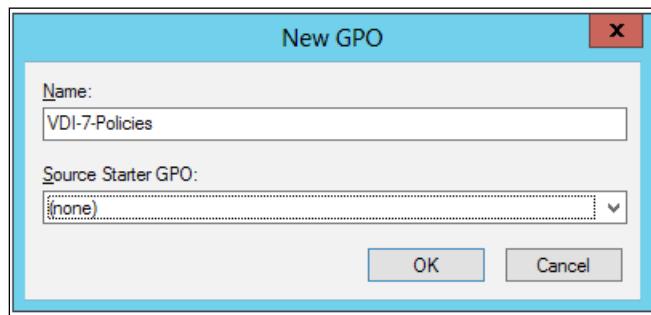
1. Log in to your domain controller server(s), and in order to find and use the template containing the Citrix policies to import, mount the Citrix XenDesktop 7 ISO image by right-clicking on it and selecting the **Mount** option.

[ As an alternative, you can install the Group Policy Management console on any Windows Server 2012 domain machine to manage the domain policies.]

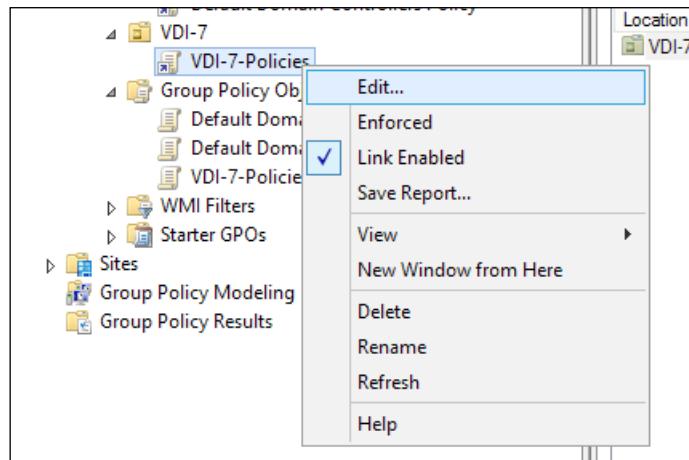
2. Hit the Windows + X keys, select the **Run** option, and run the following command to launch the Group Policy Management console:
`gpedit.msc`
3. Expand the **Forest** and **Domain** trees, right-click on the domain name of your organization, and select **New Organizational Unit** to create a container that includes the MCS/PVS Windows desktop machines:



4. When prompted for the OU name, populate the required **Name** field and click on the **OK** button.
5. Right-click on the created organizational unit, select **Create a GPO in this domain**, and link it here. In this way, we have started linking the Citrix policies to Active Directory.
6. In the **New GPO** screen, assign a name to the policy, select **(none)** in the **Source Starter GPO** drop-down list, and click on **OK**, as shown in the following screenshot:

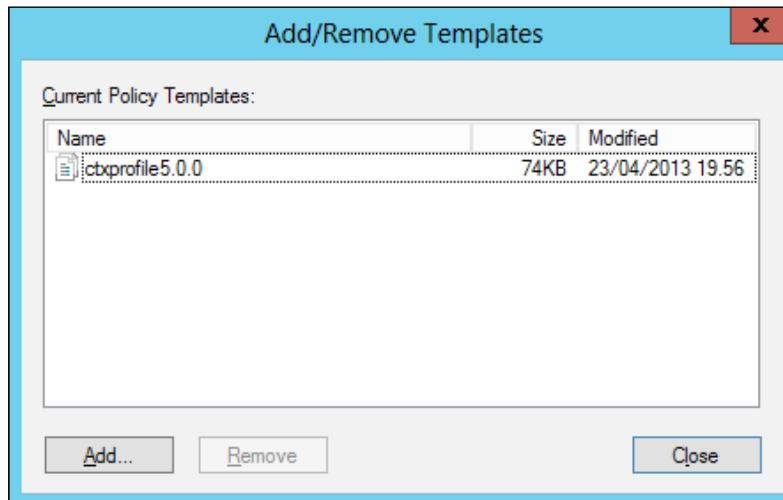


7. After creating the GPO, right-click on it and select the **Edit** option from the menu, as shown in the following screenshot:

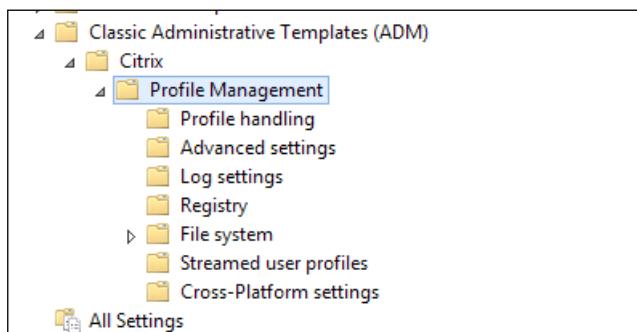


8. On the newly opened screen, navigate to **Computer Configuration | Policies**, and right-click on **Administrative Templates**. From the menu, select the **Add/Remove Templates** link.

9. On the new screen, click on the **Add** button, and then browse the installation media for the Citrix Profile Management policy template (path <cdrom>:\x64\ProfileManagement\ADM_Templates). Select the template based on your OS installation language, searching for the .adm file. Once done, click on the **Close** button.



10. Navigate to **Computer Configuration | Administrative Templates | Classic Administrative Templates (ADM) | Citrix | Profile Management**. Within this level, you can find all the configurable options for the imported Citrix policies.



In the next chapter, we will configure these imported policies in the Citrix Profile Management section.

11. Come back to the higher level of the VDI-created domain policy and configure the listed domain policies as follows:

- ❑ Navigate to **Computer Configuration | Policies | Administrative Templates | Windows Components | Windows Update**. Set the **Configure Automatic Updates** policy to the **Disabled** state and then click on **OK**.
- ❑ Navigate to **Computer Configuration | Policies | Administrative Templates | System | System Restore** and set **Turn off System Restore** to **Enabled**. After this, click on **OK**.
- ❑ Navigate to **User Configuration | Policies | Administrative Templates | Control Panel | Personalization** and enable the screensaver by setting the **Enable Screen Saver** policy to **Enabled**. After this, click on **OK** to continue.
- ❑ In the same section, set **Prevent changing screen saver** to **Enabled** and **Password protect screen saver** to **Enabled**; assign a numeric value in seconds to the **Screen saver timeout** policy after setting it to **Enabled**.



These configurations have been applied in order to standardize the master images used to deploy desktop instances.



12. After completing the configuration, log on to your Windows desktop master image and run the following command on a shell prompt in order to force the policy update application:

```
gpupdate /force
```

Have a look at the following screenshot:

The screenshot shows an "Administrator: Command Prompt" window. The command `gpupdate /force` is entered, followed by the output: "Updating policy..." and "Computer Policy update has completed successfully. User Policy update has completed successfully." The prompt then returns to `C:\Windows\system32>`.

```
Administrator: Command Prompt
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Windows\system32>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

C:\Windows\system32>
```

How it works...

Policies loaded in this recipe work as normal Active Directory policies. For this reason, you have to configure them by modifying their default configuration (the default state is not configured) to the enabled or disabled states. These are the Citrix Profile Management policies. In this section, we have performed only the installation process; the configuration will be executed in the next chapter when we discuss the configuration process of the profile management policies in detail.

The second step of the configuration process has been about the Windows Active Directory policies due to the necessity to standardize, as much as possible, the Windows image template to deploy to end users. For this reason, we've disabled Windows Update on the first applied policy; the required updates will be propagated only once to the base image, and the entire set of assigned desktops will be updated every time they are generated from the source machine. A security plus to this policy is given by using a WSUS server, a centralized Windows Update server manager. This is the only point of contact to the public network, which covers the update propagation tasks in your **Local Area Network (LAN)**.

Moreover, we've also blocked screensaver customization and system restore points; the user will be subjected to a predefined configuration, in most cases optimized as per the company's requirements.

See also

- ▶ The *Implementing a profile architecture* recipe in Chapter 4, User Experience – Planning and Configuring

4

User Experience – Planning and Configuring

In this chapter, we will cover the following recipes:

- ▶ Implementing a profile architecture
- ▶ Installing Virtual Desktop Agent – server OS and desktop OS
- ▶ Installing and configuring HDX Monitor
- ▶ Configuring Citrix Receiver™

Introduction

In *Chapter 3, Master Image Configuration and Tuning*, we discussed how to optimize the virtual desktop component in order to optimize and standardize the operating system base image, which we're going to deploy in future activities.

Now it's time to configure the components that are nearest to the user's perspective, such as advanced profile techniques, plugin installations, and appearance configuration settings. These configurations will be more oriented towards tuning and optimizing user experience instead of the operations oriented to the installation and configuration of the desktop template as explained in the previous chapter.

This was formerly known as user experience, the way in which an end user notices no difference between the use of a standard physical desktop and a virtual desktop deployed by the **Virtual Desktop Infrastructure (VDI)** architecture.

Implementing a profile architecture

When you've decided to implement the VDI architecture for your company, you need to take care of the location where you will be storing all the users' data, such as documents, projects, and mailbox file data.

So, an important step is deciding what kind of profile architecture you will be implementing for your organization. With XenDesktop 7, you have the capability to choose from among three kinds of profiles: profiles managed by the **Citrix Profile Management** 5.0 Version, **Microsoft Roaming Profiles**, and the Citrix solution known as **Personal vDisk**, a feature introduced in the XenDesktop 5.6 release.

Getting ready

To properly implement any kind of profile architecture, you need to have domain administrative credentials to be able to operate on the AD user objects. Moreover, it's also necessary to have an assigned centralized storage (network share and/or SAN) to implement the roaming profile technique or the Citrix Personal vDisk technology.

How to do it...

In the following steps we will explain the ways to implement and configure the earlier described profile management technologies.

Using Citrix Profile Management 5.0

The following steps help us to implement profile architecture by using Citrix Profile Management:

1. Log in to your Windows 8 master image with administrative credentials.
2. Mount the Citrix XenDesktop 7 ISO by right-clicking on it and select the **Mount** option. Then, browse the media support for the Citrix Profile Management folder (DVDDrive:\x64\ProfileManagement), and then double-click on the profilemgt_64.msi setup file.
3. On the **Welcome** screen, click on the **Next** button to proceed with the installation.
4. Accept the end-user license agreement by flagging the agreement option, and then click on **Next**.
5. In the **Destination Folder** section, select a valid path on which you will be installing Citrix Profile Management, and then click on the **Next** button.
6. On the **Ready to install** screen, click on the **Install** button to complete the setup.
7. Click on the **Finish** button when the setup has been completed.

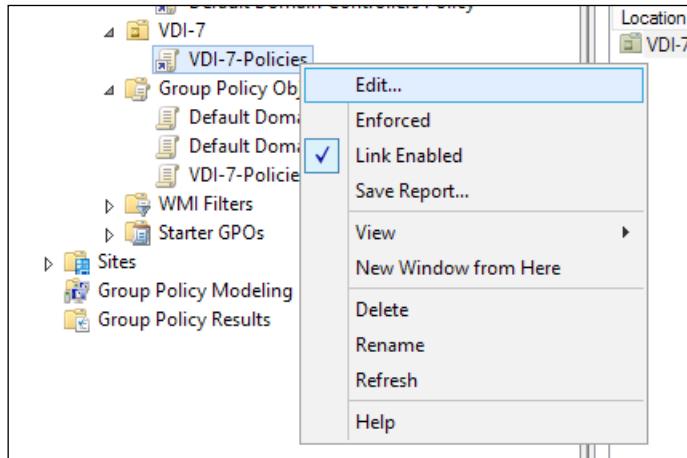


In order to complete the installation procedure, you need to restart your Windows client machine.

8. After the machine has been rebooted, press the Windows + X key combination, select the **Run** link, and type the `services.msc` command.
9. In the list of running Windows services, check whether Citrix Profile Management is running or not.

Certificate Propagation	Copies user ...	Running	Manual
Citrix Profile Management	Manages us... The CNG ke...	Running	Automatic
CNG Key Isolation			Manual (Trig...

10. Connect to your Windows Domain Controller machine; then use the Windows + X key combination; select the Run option; and insert the `gpmc.msc` command to execute Group Policy Management Console.
11. Expand the Forest and Domain trees; then search for the VDI group policy created in the previous chapter; right-click on it; and select the **Edit** option from the menu, as shown in the following screenshot:



12. Navigate to **Computer Configuration | Administrative Templates | Classic Administrative Templates (ADM) | Citrix | Profile Management**, and enable the following Citrix Profile Management policies:

- ❑ In the **Profile management** section:
 - Enable profile management**
 - Path to user store**

Active write back

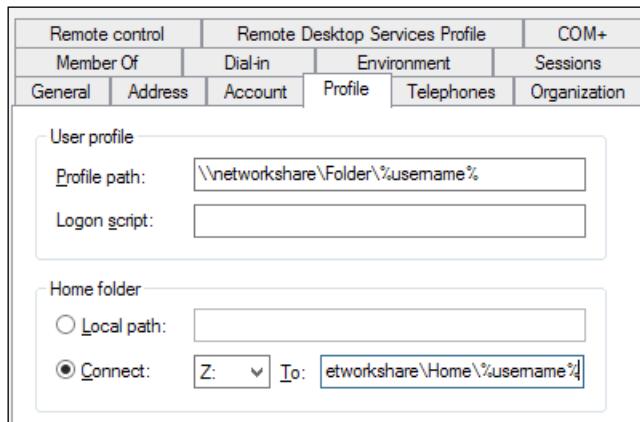
Offline profile support

- ❑ In the **Profile handling** section:
Local profile conflict handling
- ❑ In the **Advanced settings** section:
Number of retries when accessing locked files
- ❑ In the **Log settings** section:
Log settings

Using roaming profiles

The following steps help us to implement the profile architecture by using roaming profiles:

1. Right-click on the created (or already existing) user profile, and then select the Properties option.
2. Select the **Profile** tab, and insert a valid network path (for example, a network share governed by a file server) on which both the user profile and the user home folder are stored. Click on the **Apply** button, and then click on **OK** to complete the procedure, as shown in the following screenshot:

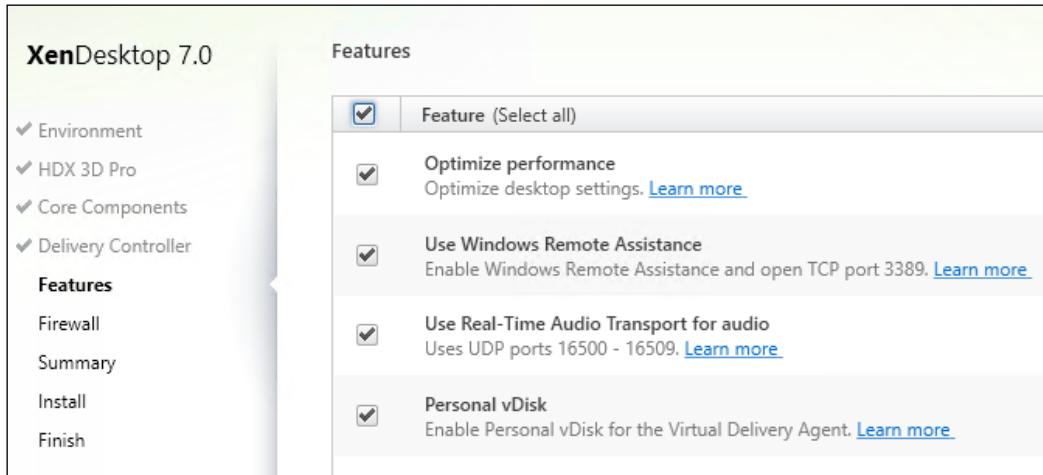


[ For both the explained profiles (Citrix Profile / Microsoft Roaming Profile), you should configure a centralized repository share for allocating the user profiles. Consider using the Microsoft Windows file server role for these purposes.]

Using Personal vDisk

The following step helps us to implement the profile architecture by using Personal vDisk:

1. In the Citrix Virtual Desktop Agent installation, when you arrive at step number five, you have to enable the **Personal vDisk** option in order to be able to deploy the desired number of Virtual Desktop instances with the additional feature of having a virtual disk assigned to every user.



In the next recipe, *Installing Virtual Desktop Agent – server OS and desktop OS*, we'll discuss the full agent installation procedure.

How it works...

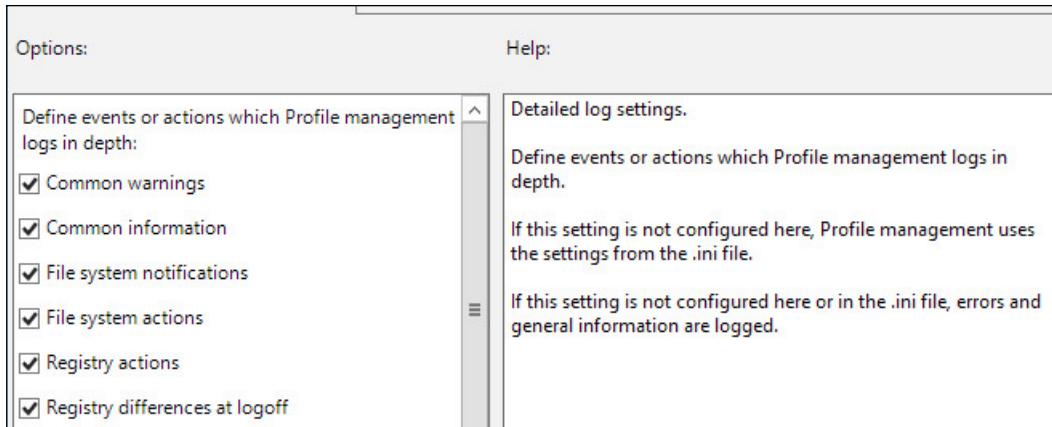
The user profile is the location where all the user data is usually stored. The first and most common profile is the local profile. With this option, you will have a copy of your user profile for every device from which you will start a user session. This technique is usable only when you have deployed static and persistent virtual desktops (this will be explained in detail later in this book). In this case, you will not lose your profile data when executing a logoff (persistent deployment) session, and with the static machine assignment, you can also avoid the profile's duplication on different devices because you will have a one-to-one association between the user and the assigned machine.

The second way to deploy a profile technique is using Citrix Profile Management—the release associated with XenDesktop 7 is 5.0. In this recipe we have configured (enabled) a set of domain policies, which will be applied to the deployed desktop instances with the profile management on board in the following ways:

- ▶ In the **Profile management** section:
 - **Enable profile management**
Enabling this policy will activate the processing of the logon and logoff phases by Citrix Profile Manager.
 - **Path to user store**
You must enable this policy to be able to specify the centralized folder on the file server on which you store the profiles. By enabling this policy, you have to specify the right network path.
 - **Active write back**
By enabling this policy, the synchronization between the desktop and the user store (only for user data and not for registry keys) will be performed during an active session before the logoff action.
 - **Offline profile support**
Enabling this policy will permit users that are also working offline without any kind of network connection.
- ▶ In the **Profile handling** section:
 - **Local profile conflict handling**
In order to respect default Profile Management concepts (the only profiles used are domain profiles), you should configure this policy to delete a local profile in order to substitute any nondomain resources with the information stored on Central Profile Manager.
- ▶ In the **Advanced settings** section:
 - **Number of retries when accessing locked files**
This policy has a default value of five retries when accessing locked files.
After being enabled, you can reuse this parameter.
- ▶ In the **Log settings** section:
 - **Enable logging**
With this, only errors will be logged; if you want to activate the debug mode to log activities in the verbose mode, you can choose to enable the policy.

- **Log Settings**

Enable this policy, and select what you want to log, in a more detailed way, selecting options shown in the following screenshot:



- **Maximum size of the log file**

The default value for the log file size is 1 MB. Define a preferred value in bytes after which the current log will be rotated in a .bak file and a new active log file will be generated.

- **Path to log file**

Specify this location, if possible using a centralized location as performed for the user profile store.

- ▶ In the **Registry** section:

- **Exclusion list:** Depending on your requirements, you can specify a set of registry keys to exclude during synchronization activities. So, any change made to these values will be discarded and not sent to the user profile store.
- **Inclusion list:** If you specify keys in this policy, they will be synchronized during the logoff phase.

- ▶ In the **Filesystem** section:

- **Exclusion list | Files**

Specify the files that must not be saved after a user performs a logoff operation.

- **Exclusion list | Directories**

Specify the folders that must not be saved after a user performs a logoff operation.

- ▶ In the **Streamed user profiles** section:

- **Profile streaming**

With this policy enabled, profile synchronization activates caching on the local computer only when file and folders are accessed; for registry keys, sync is in real time.

The latest release of the Citrix Profile Management has been improved with the help of the following features:

- ▶ Instead of assigning a temporary profile to the users in the case of multiple active sessions for the same user, the profile management now forces the user to log off, notifying it by a system pop-up message
- ▶ Citrix Profile Management is now able to automatically configure its main options based on analysis of the configured environment
- ▶ Within a configured Citrix Profile Management infrastructure, you now have the ability to integrate the use of the Citrix ShareFile platform



You can find more information on the Citrix ShareFile platform available at <http://www.citrix.com/products/sharefile/overview.html>.



As an alternative, we have the Windows roaming profile; this solution is similar to the Citrix User Profile Manager seen earlier, but with fewer features because of the fact that the Microsoft solution has been developed in the past. So we can consider the Citrix product an evolution of this technique. It's based on a centralized store on a network share on which you archive all the user data. This is a way to solve the problem of duplicated information caused by a local profile.

Finally, we have the Citrix Personal vDisk. This is a secondary virtual disk created by the Hypervisor chosen for your infrastructure and assigned to every deployed desktop machine instance associated to only one user. So, in this case we'll have a one-to-one association between the user and its Personal vDisk. Citrix PvD is made up of two components—a hidden volume identified with the V: drive letter, which is a sort of catalog of the applications installed by the user and a visible volume identified with the default P: drive letter on which users can archive their personal data. The last solution permits you to have a huge reduction of storage occupation, giving more flexibility to the users about the applications' installations and data modifications without impacting the operating system volume.

The following table is useful to compare the pros and cons of every profile method, with a set of real-world application cases:

Profile technology	Pros	Cons	Use cases
Local profile	Faster than centralized profiles.	Data duplication with multiple desktops.	Persistent virtual desktops, physical desktops.
Citrix Profile Management	Centralized profile location, no duplicated data, efficient solution to the last write wins issue (only changed file system's objects are overwritten).	An alternative to the Roaming Profiles only in the case of a low number of users.	Persistent virtual desktops and physical desktops.
Roaming profile	Centralized profile location, no duplicated data.	Slower than local profiles. Last write wins problems (overwrite of files or settings managed and modified by two or more applications simultaneously).	Nonpersistent (pooled) virtual desktops.
Personal vDisk	Virtualization of the user profile space, no reason to use centralized profiles to maintain user customization.	Backup and restore are a little bit more difficult than in other technologies and are performed at the Hypervisor level.	Nonpersistent (pooled) virtual desktops.

There's more...

The Personal vDisk drive letters can be modified, but they follow two different procedures: for the user data visible drive (defaults to P:), you can modify the assigned letter in the creation phase using Desktop Studio, and for the V: hidden drive, you have to modify a registry key on the template virtual machine. The key is located under the `HKEY_LOCAL_MACHINE\Software\Citrix\personal_vDisk\Config` section of your Windows machine registry, and its name is **VHDMountPoint**. The only operation to perform is to edit the value of the registry voice, specifying the drive letter that you want to assign.



Remember that you must perform the V: hidden drive letter modification before creating the Personal vDisk inventory and before generating any machine catalog from Desktop Controller.

See also

- ▶ *Creating and configuring the machine catalog recipe in Chapter 6, Creating and Configuring a Desktop Environment*

Installing Virtual Desktop Agent – server OS and desktop OS

After you've chosen the method to implement the profile technology, it's time to allow your Windows master image to communicate with your XenDesktop infrastructure. You can accomplish this task by installing Virtual Desktop Agent. In this latest release of the Citrix platform, VDA has been redeployed in three different versions: desktop operating systems, server operating systems, and Remote PC, a way to link an existing physical or virtual machine to your XenDesktop infrastructure.

Getting ready

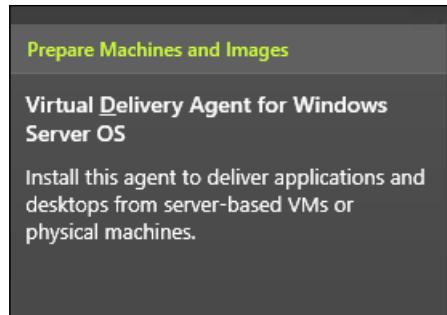
You need to install and configure the described software with domain administrative credentials within both the desktop and server operating systems.

How to do it...

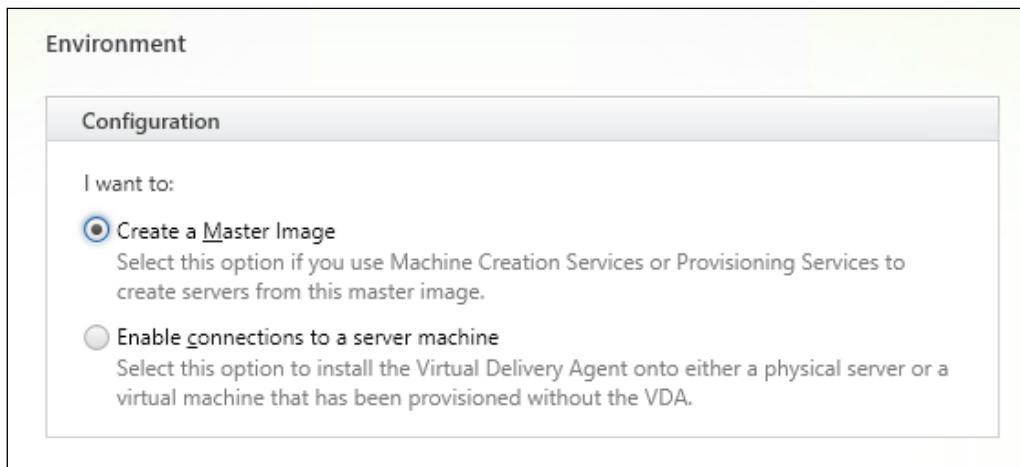
In the following section, we are going to explain the way to install and configure the three different types of Citrix Virtual Desktop Agents.

Installing VDA for a server OS machine

1. Connect to the server OS master image with domain administrative credentials.
2. Mount the Citrix XenDesktop 7.0 ISO on the server OS machine by right-clicking on it and selecting the **Mount** option.
3. Browse the mounted Citrix XenDesktop 7.0 DVD-ROM, and double-click on the `AutoSelect.exe` executable file.
4. On the **Welcome** screen, click on the **Start** button to continue.
5. On the XenDesktop 7.0 menu, click on the **Virtual Delivery Agent for Windows Server OS** link, in the **Prepare Machines and Images** section.

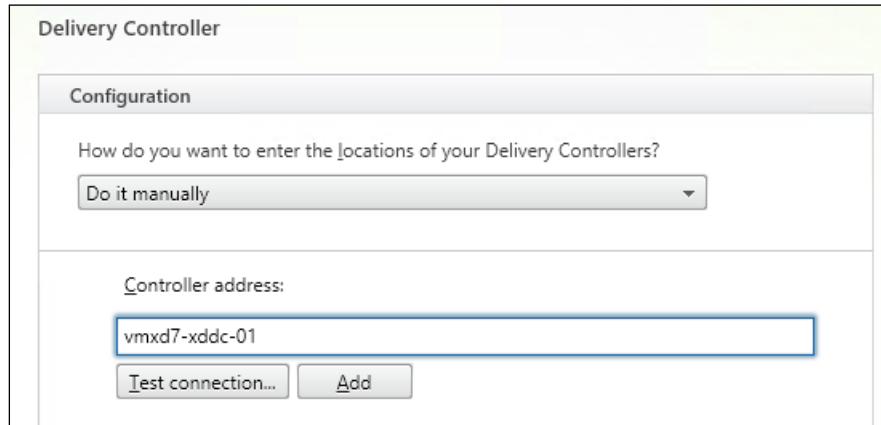


6. In the **Environment** section, select **Create a master image** if you want to create a master image for the VDI architecture (MCS/PVS). Or enable a direct connection to a physical or virtual server. After completing this step, click on **Next**.



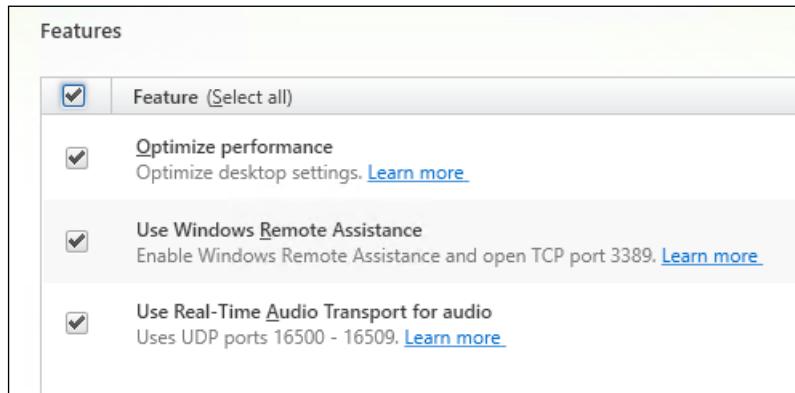
7. In the **Core Components** section, select a valid location to install the agent; then flag the Citrix Receiver component; and click on the **Next** button.

8. In the **Delivery Controller** section, select **Do it manually** from the drop-down list in order to manually configure Delivery Controller; type a valid controller FQDN; and click on the **Add** button, as shown in the following screenshot. To continue with the installation, click on **Next**.



[ To verify that you have entered a valid address, click on the **Test connection...** button.]

9. In the **Features** section flag, choose the optimization options that you want to enable, and then click on **Next** to continue, as shown in the following screenshot:



10. In the **Firewall** section, select the correct radio button to open the required firewall ports automatically if you're using the Windows Firewall, or manually if you've got a firewall other than that on board. After completing this action, click on the **Next** button as shown in the following screenshot:

Firewall

The default ports are listed below. [Printable version](#)

Controller Communications	Remote Assistance	Real Time Audio
80 TCP	3389 TCP	16500 - 16509 UDP
1494 TCP		
2598 TCP		
8008 TCP		

Configure firewall rules:

Automatically
Select this option to automatically create the rules in the Windows Firewall. The rules will be created even if the Windows Firewall is turned off.

Manually
Select this option if you are not using Windows Firewall or if you want to create the rules yourself.

11. If the options in the Summary screen are correct, click on the **Install** button to complete the installation procedure.



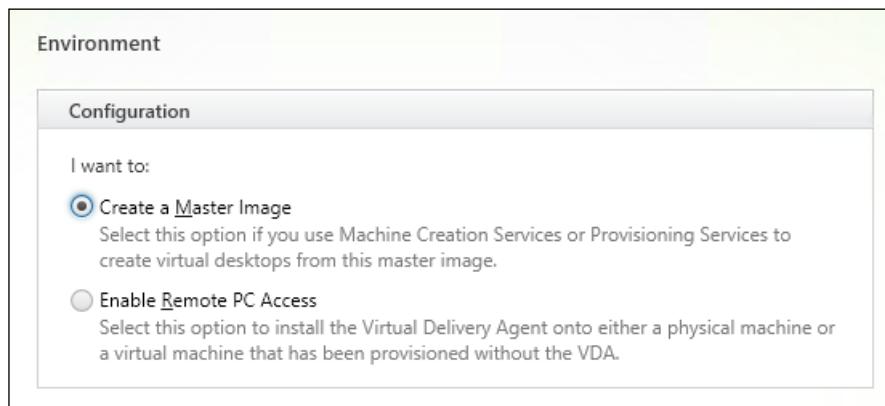
In order to complete the procedure, you'll need to restart the server OS machine several times.

Installing VDA for a desktop OS machine

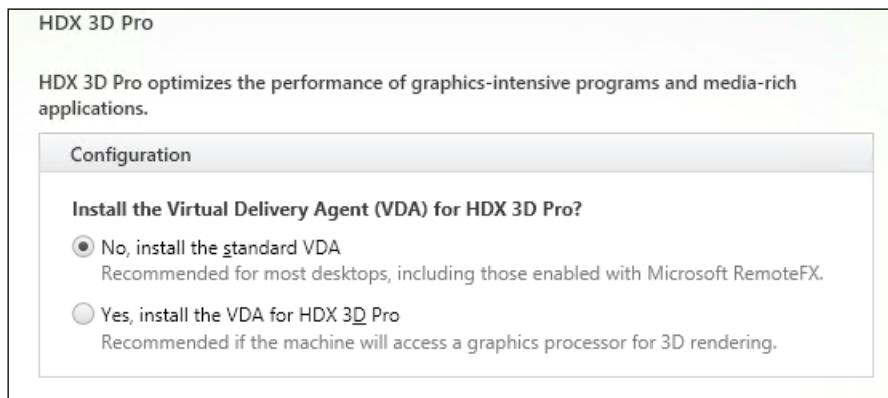
1. Connect to the desktop OS master image with domain administrative credentials.
2. Mount or burn the Citrix XenDesktop 7.0 ISO on the desktop OS machine.
3. Browse the mounted Citrix XenDesktop 7.0 DVD-ROM, and double-click on the AutoSelect.exe executable file.
4. On the **Welcome** screen, click on the **Start** button to continue.
5. On the XenDesktop 7.0 menu, click on the **Virtual Delivery Agent for Windows Desktop OS** link in the **Prepare Machines and Images** section as shown in the following screenshot:



6. In the **Environment** section, select **Create a Master Image** if you want to create a master image for the VDI architecture (MCS/PVS), or select Enable Remote PC Access to enable access to a physical or virtual desktop machine. After completing this action, click on **Next**.



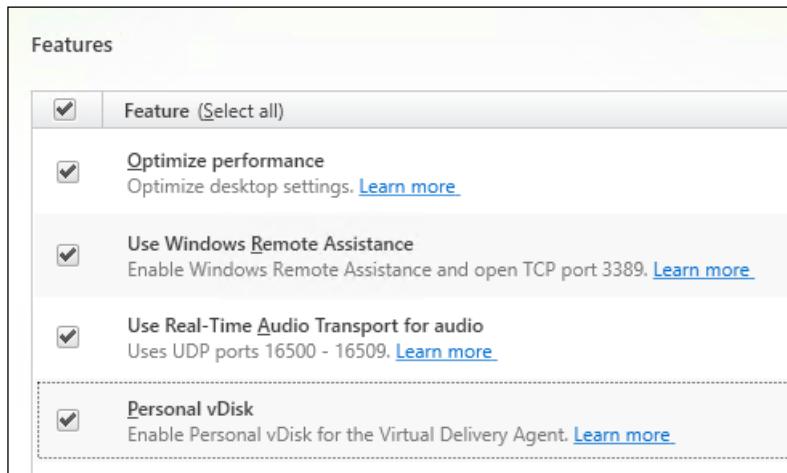
7. In the **HDX 3D Pro** section, select whether or not to install the Citrix HDX 3D Pro plugin, and click on **Next**.



In the next recipe, *Installing and configuring HDX Monitor*, we will obtain some more information about the user experience analysis.

8. In the **Core Components** section, select a valid location to install the agent; flag the Citrix Receiver component; and click on the **Next** button.
9. In the **Delivery Controller** section, select **Do it manually** from the drop-down list in order to manually configure the delivery controller; type a valid controller FQDN; then click on the **Add** button; and click on **Next** to continue.

10. In the **Features** section, select the options you want to be enabled during the VDA installation. Take particular care about the Citrix Personal vDisk component activation based on your profile management policies. After completing this action, click on **Next**.



11. In the **Firewall** section, select the correct radio button to open the required firewall ports, automatically, in case you're using the Windows Firewall, or manually if you've got a firewall other than that on board. After completing this action, click on the **Next** button.
12. If the options in the **Summary** screen are correct, click on the **Install** button to complete the installation procedure.

How it works...

The Virtual Desktop Agent is the client software that connects your client machine to the XenDesktop infrastructural servers. A standard installation of the VDA will use the normal HDX protocol version using an ICA connection to interact with the centralized controller servers. In the case of the Windows Display Driver Model (WDDM) system driver, the agent setup will try to uninstall it in order to avoid graphical problems with your desktop instances.

Whenever possible, you should uninstall the WDDM driver before the Virtual Desktop Agent installation, especially when configuring XenDesktop with a VMWare ESX Hypervisor host. WDDM could give you unexpected graphical behaviors and system crashes.

The main difference between the previous releases of the Virtual Desktop Agent is the ability to choose whether to install it on a machine that will be used as a Master Image template, or on a physical/virtual machine, which will be accessed directly from a remote location. This is the new XenDesktop feature known as Remote PC Access; this powerful feature makes stronger use of company resources from a (remote) personal device in terms of user experience and security (any connection to the company device is encrypted and managed by the NetScaler Gateway and XenDesktop 7 architectures).

In the case of a configured server OS remote machine, IT professionals have got a different way to deploy desktops and applications. In fact, on the server OS machine, Remote Desktop licensing will be activated, enabling the administrator to publish resources in a XenApp style using the new version of this Citrix software integrated in the XenDesktop architecture.



Deploying server OS machines for MCS architectures will allow provisioning XenApp style servers in a faster way.



In the next step, you will be prompted to choose whether to install the standard HDX suite or the HDX 3D Pro version. Unlike the previous version of XenDesktop, the 3D-Pro suite is an integrated part of VDA, configurable by the use of the Citrix policies.



In Chapter 8, *XenDesktop® Tuning and Security*, we will explain how to configure HDX based on the specific platform usage (standard, 3D graphics, and mobile).



After this section the installation procedure continues with the selection of the most important components for the VDA client: Virtual Desktop Agent, and Citrix Receiver.



An alternative way to install Citrix Receiver is using the Merchandising Server, which will be discussed in the next chapter.



Then, the next step requires inserting the Desktop Controller server FQDN and checking its availability. This is not mandatory in this section (you can also configure it later), but in order to complete all the required steps, you should insert this information now.

The last configuration step is about the firewall. You have to open the required ports for the VDA architecture in the case of a firewall different from the Windows Firewall platform. In the case of this last technology the XenDesktop VDA setup will be able to automatically open the following required ports:

- ▶ Controller communications: TCP 80, TCP 1494, TCP 2598, TCP 8008
- ▶ Remote assistance: TCP 3389
- ▶ Real-time audio: UDP 16500 – 16509

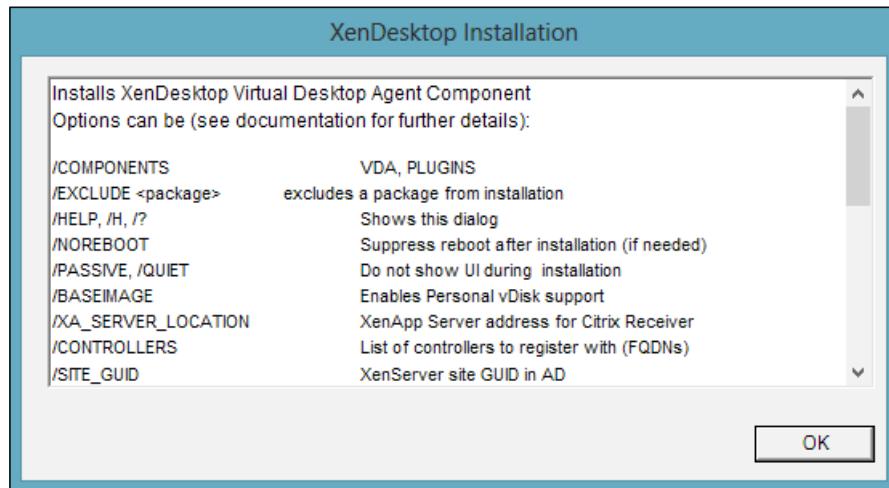
There's more...

Users have also got the ability to run setup steps from the command line and not only from the graphical interface. Citrix offers an executable file that can substitute the previously seen installation procedure.

This file is named `XenDesktopVdaSetup.exe`, and you can find it either on your XenDesktop installation media at the `x86\XenDesktop Setup` path for 32-bit installations or at `x64\XenDesktop Setup` path for 64-bit installations. Run it from the command line to perform the required installation. To view the complete options list for this executable file, run the following command:

```
XenDesktopVdaSetup.exe /?
```

You will receive a pop-up screen with the entire list as shown in the following screenshot:



So, for example, to install Virtual Desktop Agent with the Personal vDisk enabled, with both the VDA and receiver components and with the specified delivery controller address, you have to run the following instructions from the Windows command line:

```
XenDesktopVdaSetup.exe /BASEIMAGE /COMPONENTS VDA,PLUGINS /CONTROLLERS  
vmxd7-xddc-01.xdseven.local
```

See also

- ▶ The *Configuring the XenDesktop® policies* recipe in *Chapter 8, XenDesktop® Tuning and Security*

Installing and configuring HDX Monitor

Citrix HDX is a collection of capabilities offered by XenDesktop, which is based on the well-known and stable ICA protocol. HDX is a set of features oriented to high performances without losing the resolution quality for both audio and video reproduction. HDX Monitor is a powerful tool, which permits system administrator verification and configuration of the parameters for high-level user experience.

Getting ready

You need to download HDX Monitor software available at <https://taas.citrix.com/hdx/download>.

To install it, you have to connect to the related machine with domain administrative credentials, having already installed the .NET 3.5 Framework.



You could have issues during the .NET 3.5 Framework installation process on Windows 8 / Windows Server 2012 platforms; please refer to the Microsoft article for installation, available at <http://technet.microsoft.com/en-us/library/hh831809.aspx>.

HDX Monitor can only work with XenDesktop versions starting from 5.5. It's not compatible with any previous version.

How to do it...

The following steps will explain how to install and use Citrix HDX Monitor:

1. Connect to the Desktop OS master image with domain administrative credentials.
2. Locate the folder on which you've downloaded HDX Monitor software, and then double-click on the `hdx-monitor.msi` file to run it.

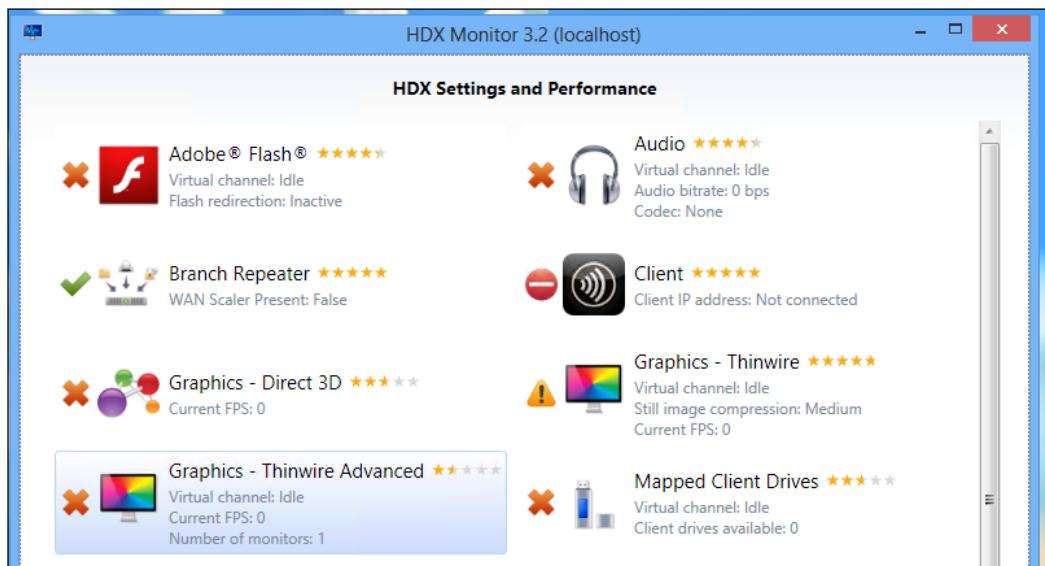
3. On the **Welcome** screen, click on the **Next** button to continue.



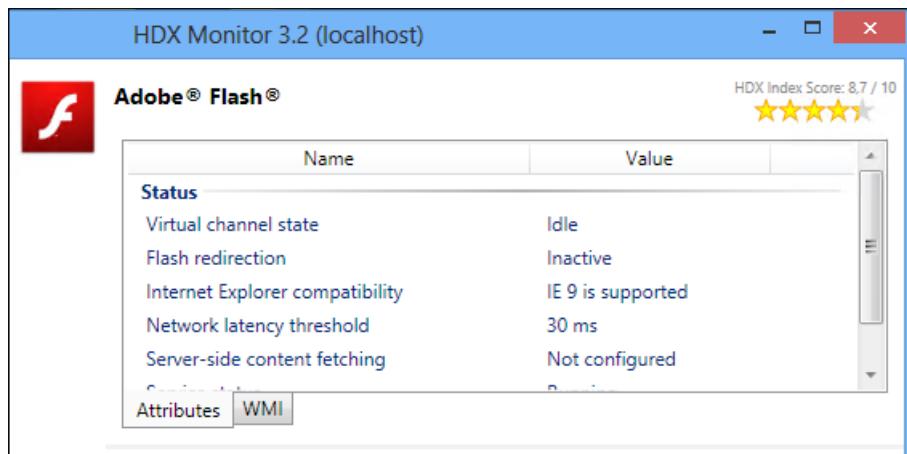
4. In the **License Agreement** section, select the **I Agree** radio button, and click on **Next**.
5. In the **Select Installation folder** screen, choose a valid path on which you will install the software, and click on **Next** to continue.
6. After completing this action, click on the **Next** button on the **Confirm Installation** screen to complete the software setup.
7. After completing the installation, click on the **Close** button to end the setup procedure.
8. After the end of installation, double-click on the **Citrix HDX Monitor** icon on the desktop.
9. On the main menu, insert a valid machine address for which you want to check the configuration. In this case, insert the local IP address, and click on the **Open** button.



10. After connecting to the target device, you will be prompted for a summary screen with the current status of the configured components as shown in the following screenshot:



11. Click on one of the HDX settings icons to obtain further details about the selected component.

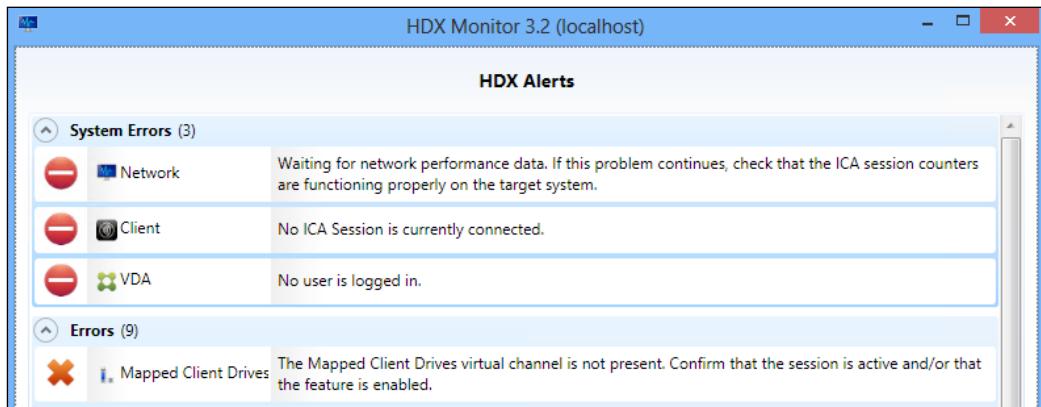


On the right-hand side corner of the component section users can find the HDX score assigned to the component configuration.

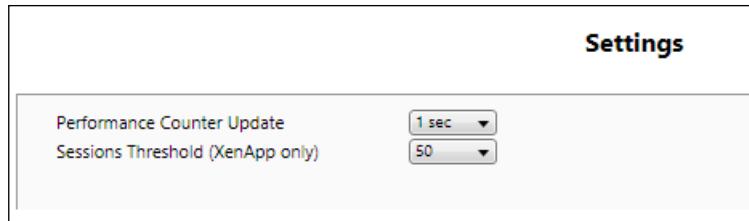
12. To change the component configuration view, click on one of the sections on the left-hand side menu.



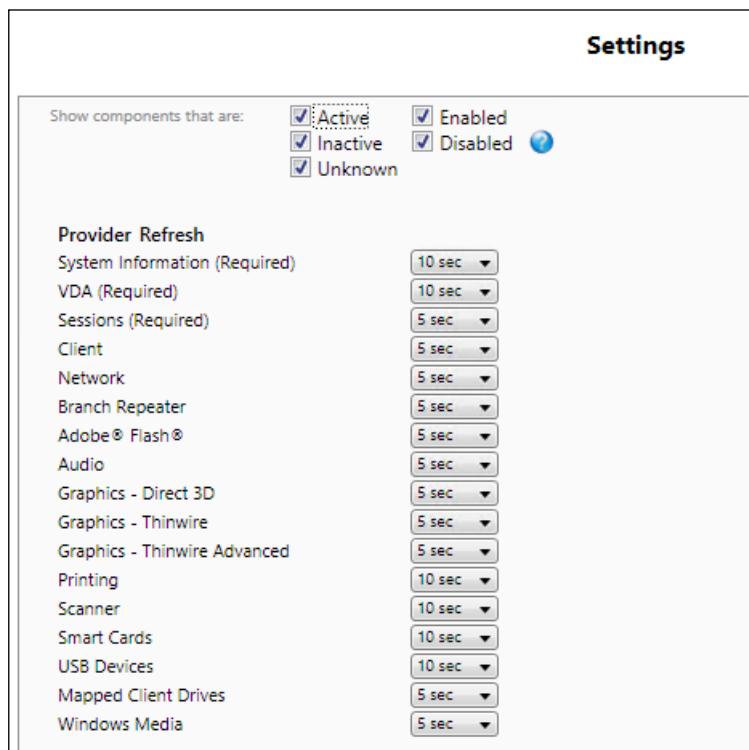
13. To see the full list of alerts presented by HDX Monitor, click on the **Alerts** link on the top of the **Monitor menu** section. To come back to the main menu, click on the **Home** link.



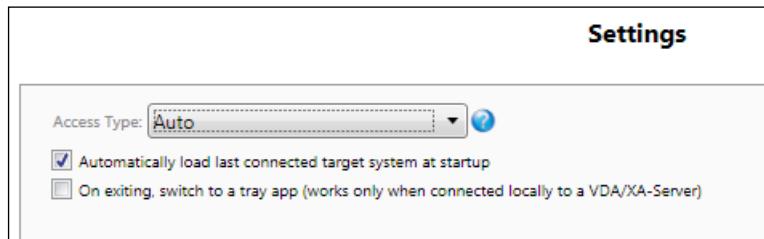
14. To configure HDX Monitor, click on the **Settings** link in the component menu.
15. The first option tab is the **Performance Counter Update** section. Here, you can configure the time interval (in seconds) on which you will be updating the system counters as shown in the following screenshot:



16. On the second tab, HDX Components, you have the updating time parameters on the system metrics for which you are collecting statistics. You can also configure the kind of components that are to be shown within the monitor.



17. In the **Monitor** tab, you can select an **Access Type** option from the drop-down menu list (**Auto**, **Winrm**, and **COM/DCOM**). Moreover, you can decide if it automatically reconnects the last analyzed system at startup as shown in the following screenshot:



18. In the **Logging** tab, you can specify a valid path and file name on which you will be logging all the monitor activities.
19. In the last section, **Alerts**, you can enable a long list of available preconfigured alerts for your monitored machines.

Ignore	Component	Level	Message	URL	Condition
<input checked="" type="checkbox"/>	Adobe® Flash®	HighWarning	The HDX Flash V1 latency threshold		HDXFlashVersion
<input type="checkbox"/>	Adobe® Flash®	HighError	The version of Internet Explorer inst	http://www.microsoft.com/windows	ieVersionNumber
<input type="checkbox"/>	Adobe® Flash®	HighError	The installed Flash Player is not sup		installedVersion
<input type="checkbox"/>	Adobe® Flash®	LowWarning	Adobe® Flash® redirection has bee		isEnabled
<input type="checkbox"/>	Audio	LowWarning	Audio redirection has been disable		isEnabled
<input checked="" type="checkbox"/>	Audio	LowWarning	? redirection has been disabled with		isEnabled
<input type="checkbox"/>	Audio	HighError	The ? virtual channel is not present.		isEnabled && lis
<input type="checkbox"/>	Audio	HighError	The Audio virtual channel is not pre		isEnabled && lis
<input checked="" type="checkbox"/>	Audio	HighWarning	No audio devices found.		IfAnyDeviceExist
<input type="checkbox"/>	Audio	HighError	The Audio service (CtxAudioSrv) has		status == Servic
<input checked="" type="checkbox"/>	Audio	HighWarning	Codec ? is not optimized to reduce		ifAnyDeviceExist
<input checked="" type="checkbox"/>	Audio	HighWarning	Virtual channel priority should be se	http://support.citrix.com/search/bas	(priority != Virtu
<input type="checkbox"/>	Audio	System	No user is logged in.		SessionID == nu
<input checked="" type="checkbox"/>	Audio	HighWarning	Virtual channel priority should be se	http://support.citrix.com/search/bas	(priority != Virtu
<input type="checkbox"/>	Audio	LowWarning	Audio over UDP could not be used		CurrentUDPProg
<input type="checkbox"/>	Audio	HighWarning	Audio capture is disabled. Input fro		ifAnyDeviceExist

- 

Some of the preconfigured alerts contains link to a related Citrix or Microsoft support page in order to make problem analysis easier.
20. After completing all the configurations, click on the **Save settings** button to make all the changes permanent, and then restart HDX Monitor to apply them.

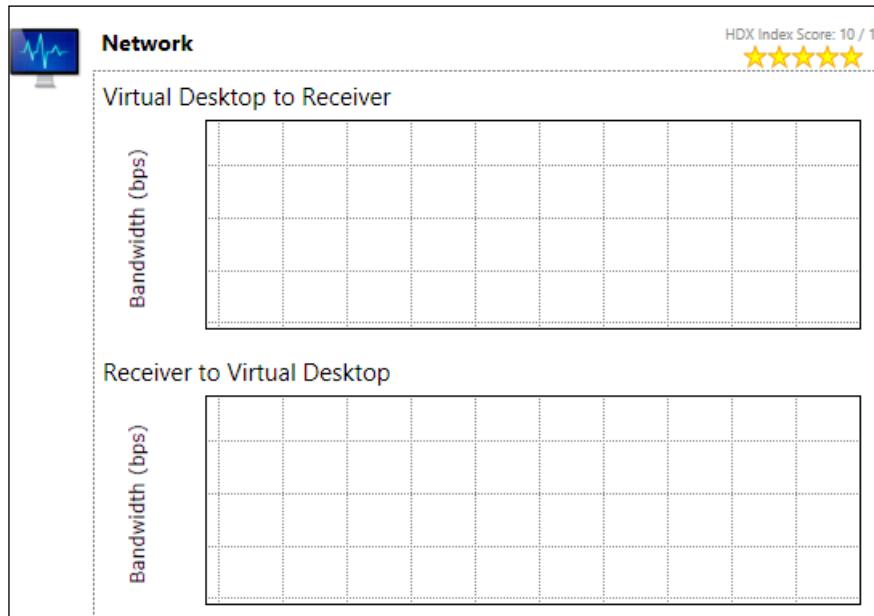
21. HDX Monitor permits you to export the report generated on the collected data. To perform this, you have to use the Generate report link in the components menu. The report will be generated in the HTML format.

How it works...

HDX Monitor is a powerful tool developed by Citrix to check the status of a configured master image in depth. The release associated with XenDesktop 7 is the 3.2 Version. The tool is in the form of an MSI package, installable on a Windows compatible machine. The tool is able to remotely connect to a target machine (a desktop master image configured to be used to deploy machine instances) on which the Monitor is collecting real-time data to give the status of the most important user experience components. The Monitor collects data for the following objects:

- ▶ Adobe Flash
- ▶ Audio
- ▶ Branch Repeater
- ▶ Client
- ▶ Graphics—Direct 3D
- ▶ Graphics—Thinwire
- ▶ Graphics—Thinwire advanced
- ▶ Mapped client drives
- ▶ Network
- ▶ Printing
- ▶ Scanner
- ▶ Smart cards
- ▶ System information
- ▶ USB devices
- ▶ VDA
- ▶ Windows Media

For each of these components, a **Diagnostics** section is available to retrieve the state of the network performance or the registered event logs as shown in the following screenshot:



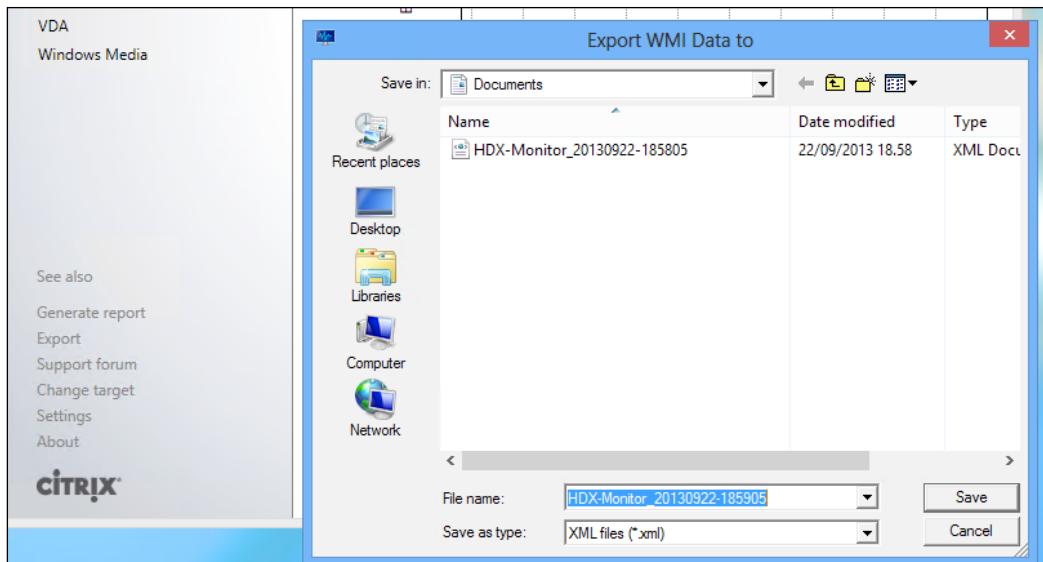
From the collected data, it is possible to generate reports that could be used to trace the evolution or the degradation of the general system performance.

There's more...

HDX Monitor permits you to export and reimport the saved configurations and the collected data by exporting them in the XML format.

To accomplish this task, you have to go to the component view, click on the **Export** link, and assign a name to the XML parameters file.

This WMI data can be reimported on any other HDX Monitor installation within your infrastructure.



See also

- ▶ *Chapter 7, Deploying Applications*

Configuring Citrix Receiver™

Citrix Receiver is the last component to be configured for Virtual Desktop Agent. This plugin is the connector used by any device (laptops, smart phones, tablets) to connect to the server's sites, in order to receive the assigned desktops or the published applications.

Getting ready

No preliminary operations are required to perform the configurations for Citrix Receiver. In fact, you have already installed all the necessary components to use the Citrix plugin. On the other hand, a XenDesktop configured server and a StoreFront store are required to use the plugin for its main purpose—interaction with the published resources.

How to do it...

In the following steps, we will configure the Citrix Receiver component used by the user's devices to connect to the published resources:

1. Log in to the configured StoreFront server with domain administrative credentials.
2. Run the StoreFront console by searching for it within the Windows Apps catalog
(Press the Windows + C key combination; click on the **Search** button; and search for the Citrix StoreFront application).

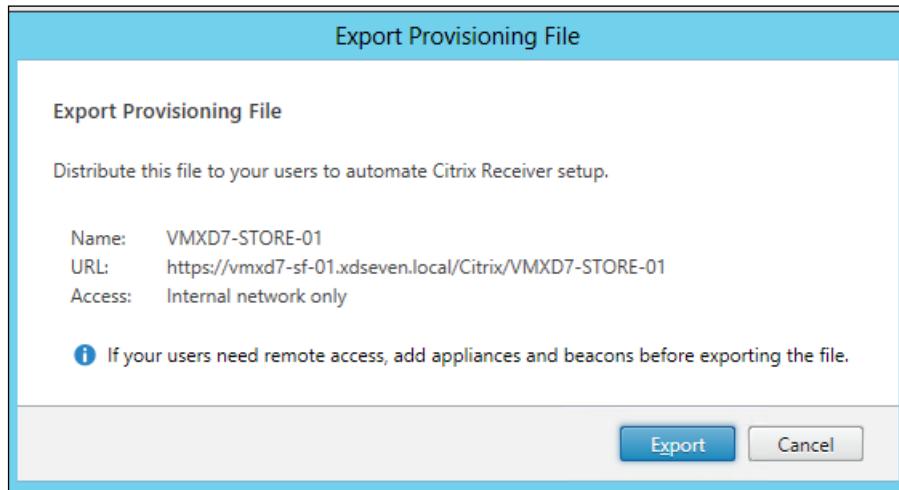


You can also manage the StoreFront configured store by using the **Citrix Studio** console.

3. On the StoreFront console left-hand side menu, click on the **Stores** link and select **Export Provisioning File** on the right-hand side menu.



- When prompted to save the Provisioning file, click on the **Export** button to complete the procedure.

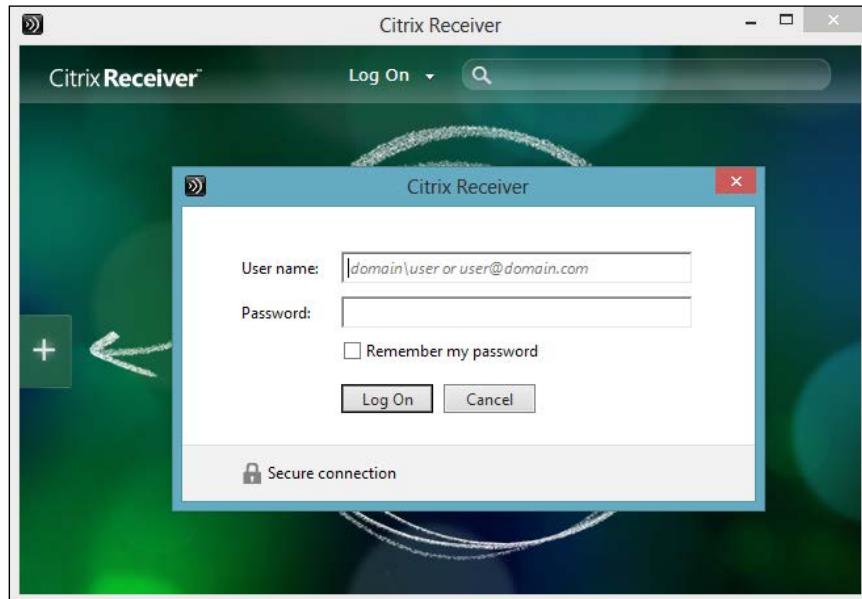


- Select a valid path on which you will be saving the .crx file, and then click on the **Save** button.
- Copy the generated store file to the master image template; double-click on it to configure the Citrix Receiver; and click on the **Add** button when prompted for the Citrix Receiver configuration confirmation.



[Be sure you have installed the right StoreFront SSL certificate in the Trusted Root Certification Authorities store on the destination machine; otherwise, you won't be able to use the preconfigured store file.]

7. When prompted for the logon, enter valid domain credentials in order to be authenticated by the StoreFront server.



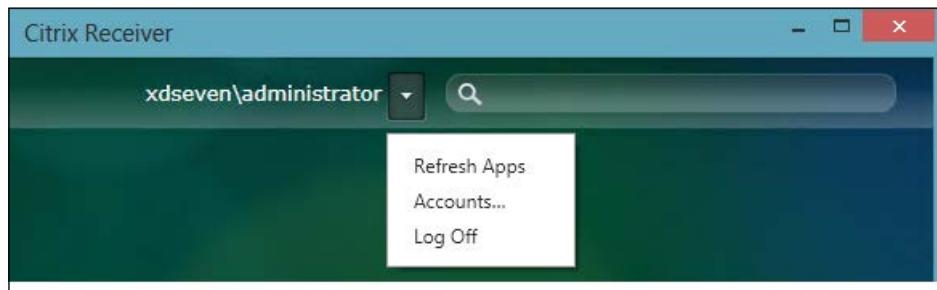
8. Click on the Plus (+) symbol on the left-hand side to show the list of available resources (applications and desktops).



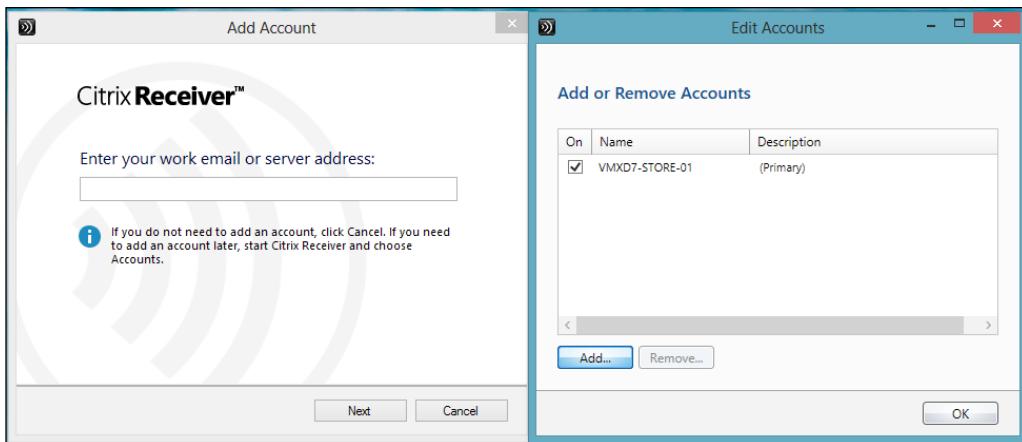
9. In the **User Settings** section, you can flag both the presented options. These are recommended parameters you should activate for your client.

[ By default, you will find the Citrix Online applications (Citrix **GoToMeeting**, **GoToTraining**, and **GoToWebinar**) already available for your account.]

10. To configure additional accounts within Citrix Receiver, click on the username link on the top of the windows, and then select the Accounts option from the list.



11. In the **Edit Accounts** window, click on the **Add** button, then insert a valid e-mail address linked to the account you want to add. As an alternative, you can retype a valid StoreFront address.



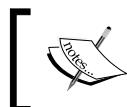
12. Now that all the configuration steps have been completed, Citrix Receiver is ready to work with the server farm's components.

How it works...

Citrix Receiver is a set of features used to receive the applications and the desktops installed and presented to the end users, or streamed and published for them.

The XenDesktop 7 release presents two different versions of Citrix Receiver. The client, discussed in this chapter in terms of implementation and configuration, is one. The other version is the Web Client, which we talked about in the *Installing and configuring StoreFront 2.0* recipe in Chapter 1, *XenDesktop® 7 – Upgrading, Installing, and Configuring*.

After you've logged in with your domain credentials you will see your applications published on your desktop or on your Start menu, if configured as later in this book. All the changes made to your applications, such as a new software assigned to your user or a previously existent application removed from your area, are immediately reported to your running desktop(s). Moreover, you can also customize the appearance and the quality of your applications in order to improve the speed in some situations, or decide to have a higher quality image with a probable impact on the general performance. All these features permit us to have an extremely flexible approach. You could have a Windows client machine without any installed application and could populate it with software from other clients and servers based on the permissions assigned to a user on that specific application. This could permit you to reduce the operating system attack surface, separating the applications from the operating system area, using XenDesktop 7 integrated application packaging platforms, such as Microsoft App-V.

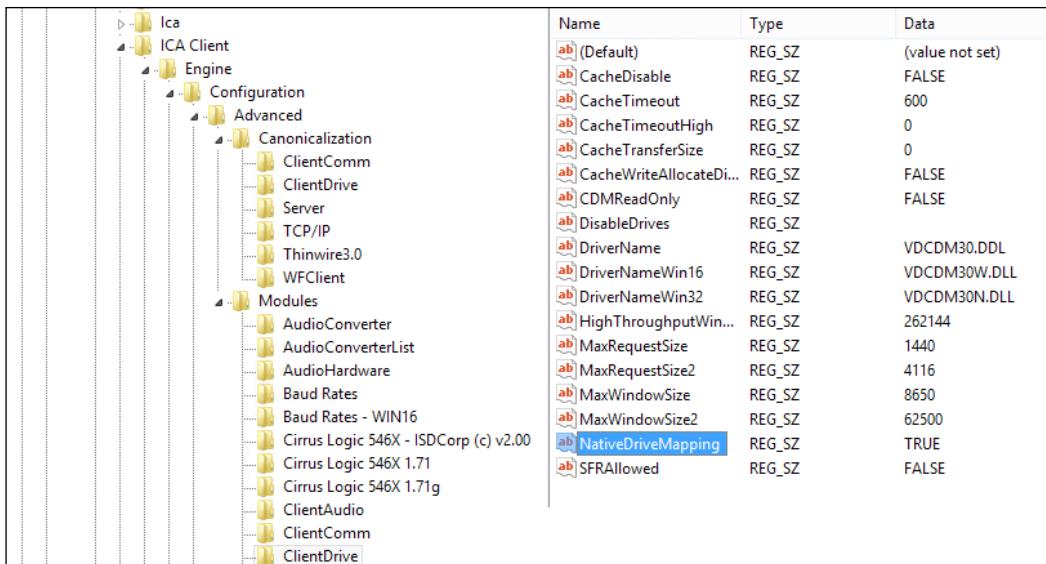


Citrix Receiver Store can be also configured by the use of Domain Group Policies. In this way, it's possible to avoid updating Master Image after you've changed the StoreFront configuration.

There's more...

When using a remote application published with XenDesktop 7, you could have a content redirection problem upon double-clicking on a file associated to specific software. For instance, you could have Microsoft Word published to your virtual desktop and need to open a .doc file located on your desktop instance. Without any further operation on the client, you would probably receive an error for the file path location. To avoid this problem, you have to perform the following tasks:

- ▶ Modify the registry key NativeDriveMapping located at `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientDrive` (32 bit machines) or located at `HKEY_LOCAL_MACHINE\ SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientDrive` (64 bit machines), assigning to it the value, TRUE.



The screenshot shows the Windows Registry Editor with the following path selected:

```

    HKEY_CURRENT_USER\Software\ICa\ICA Client\Engine\Configuration\Advanced\Canonicalization\ClientDrive
  
```

The right pane displays the following registry keys and their values:

Name	Type	Data
(Default)	REG_SZ	(value not set)
CacheDisable	REG_SZ	FALSE
CacheTimeout	REG_SZ	600
CacheTimeoutHigh	REG_SZ	0
CacheTransferSize	REG_SZ	0
CacheWriteAllocateDi...	REG_SZ	FALSE
CDMReadOnly	REG_SZ	FALSE
DisableDrives	REG_SZ	
DriverName	REG_SZ	VDCDM30.DLL
DriverNameWin16	REG_SZ	VDCDM30W.DLL
DriverNameWin32	REG_SZ	VDCDM30N.DLL
HighThroughputWin...	REG_SZ	262144
MaxRequestSize	REG_SZ	1440
MaxRequestSize2	REG_SZ	4116
MaxWindowSize	REG_SZ	8650
MaxWindowSize2	REG_SZ	62500
NativeDriveMapping	REG_SZ	TRUE
SFRAllowed	REG_SZ	FALSE

- ▶ Modify the module.ini file located at your Citrix Online Plugin installation path (usually C:\Program Files (x86)\Citrix\Online Plugin\Configuration). Search for the [**ClientDrive**] section, and assign to the NativeDriveMapping key the TRUE value.

```

[ClientDrive]
  DriverName          = VDCDM30.DLL
  DriverNameWin16     = VDCDM30W.DLL
  DriverNameWin32     = VDCDM30N.DLL
  MaxWindowSize       = 8650
  MaxWindowSize2      = 62500
  MaxRequestSize      = 1440
  MaxRequestSize2     = 4116
  CacheTimeout        = 600
  CacheTimeoutHigh    = 0
  CacheTransferSize   = 0
  CacheDisable         = FALSE
  CacheWriteAllocateDisable = FALSE
  DisableDrives        =
  CDMReadOnly          = FALSE
NativeDriveMapping = TRUE
  SFRAllowed           = FALSE
  HighThroughputWindowSize = 262144
  
```

After completing, you will receive no more errors when trying to access a file type redirected to its native application.

See also

- ▶ *Configuring the Merchandising Server recipe in Chapter 5, Configuring Additional Architectural Components*

5

Configuring Additional Architectural Components

In this chapter, we will cover the following recipes:

- ▶ Configuring the Merchandising Server
- ▶ Configuring the CloudBridge platform
- ▶ Installing and configuring XenDesktop® Collector

Introduction

XenDesktop 7 can be described as a suite made up of a lot of different features, some of which act as additional features to the core architectural software. In this chapter, we're going to discuss the important components that have the purpose to improve the quality, performance, and manageability of your **Virtual Desktop Infrastructure (VDI)** architecture, such as Merchandising Server (the management software used to manage the Citrix plugin delivery and update), CloudBridge Platform Virtual Appliance (the Citrix infrastructure optimization platform for WAN connections and branch offices), and XenDesktop Collector (the Citrix support tool used to directly upload system traces and log on to Citrix technical support).

Configuring the Merchandising Server

In the previous chapter, we've seen why and how to configure the Citrix Receiver plugin; this is a fundamental component to view and use the applications and the desktops assigned to a user. It must be installed on any device that needs to access online or offline resources; this could need an additional effort in the maintenance tasks such as upgrading activities. How could you avoid this problem? With the use of Merchandising Server, a centralized store from which you can download the latest version of the Receiver software for any supported platform, we are able to have a single and centralized point of maintenance.

Getting ready

Citrix Merchandising Server is a Virtual Appliance developed for the following hypervisors: Citrix XenServer (in the form of bz2 template and VMware vSphere (in the form of OVF template). So you need to download it from your MyCitrix account (from the website <https://www.citrix.com/account>) and import it into your hypervisor. Merchandising Server also needs to communicate with a Windows Active Directory domain on which the XenDesktop infrastructure has been configured. So, it will also require you to have administrative credentials for your company domain.

How to do it...

In this section, we will deploy and configure the Citrix Merchandising Server virtual appliance:

1. After you've imported the virtual appliance in to your hypervisor, connect to the console of the created virtual machine. You will find a text menu with seven options.



The screenshot shows a black terminal window displaying a text-based menu for the Citrix Merchandising Server. The menu is framed by a border of '#'. It displays the following text:

```
#####
#          Citrix Merchandising Server      #
#          Network Configuration           #
#####
[1]  Hostname
[2]  IP
[3]  Netmask
[4]  Gateway
[5]  Domain Name System
[8]  Diagnostics
[0]  Refresh
```

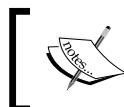
2. Select the first option **Hostname**, to assign a hostname to the virtual appliance. After completing this step, press *Enter* to confirm.
3. Select the second option **IP** to assign an IP address to Merchandising Server. Press *Enter* to complete the procedure.
4. Assign a net mask by selecting the third option **Netmask** and press *Enter* to proceed.
5. Configure the default gateway by selecting the fourth option **Gateway** after you've typed the required IP address, press *Enter*.
6. Insert all the required DNS server IP address information in order to configure a complete name resolution for the fifth option **Domain Name System**. After this press *Enter* to complete this task.

```
#####
# Enter IP addresses of DNS servers #
# Leave blank and press enter to quit. #
#####
nameserver 1: 8.8.8.8
nameserver 2: 4.4.4.4
nameserver 3:
Domain search: ctxlab.local_
```

7. Select the eighth option **Diagnostics**, if you want to verify the availability of a network address by using the ping and tracert command.

```
Citrix Merchandising Server version 2.2 on VMWare Tue Aug 14 10:43:04 UTC 2012
login: root
Password: _
```

8. After completing all the console configurations, you can open a compatible web browser and type the Merchandising Server administrative address in the form of: //hostname/appliance. So you need to type the URL `https://merchandising.ctxlab.local/appliance`. The default credentials to log in are `root/Citrix321`.



Merchandising Server Administrator Console supports browsers such as Internet Explorer starting from Version 7 and Mozilla Firefox starting from Version 4.

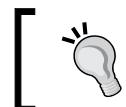


9. On the **Setup Guide** welcome screen, click on the first link, **Configure Active Directory**, in order to connect Merchandising Server with your company domain.

Welcome to the Citrix Merchandising Server Administrator Console
The root login to the Citrix Merchandising Server Administrator Console gives you access Once you complete these tasks you can log back in with your user account name to have

1. [Configure Active Directory](#)
You must enter your Active Directory server information and perform a sync to load your co
2. [Set Permissions](#)
Grant Auditor permissions to your corporate user account.
3. [Log off](#)
Log off of the Administrator Console. Then log back in with your administrator user name

10. Configure at least a valid primary domain controller and, if possible, a back-up DC server, specifying the domain name (the **Source Name** field), whether or not enabling the **Secure connection** option (for security reasons, you should activate this), the DC **Server Address** for both the machines, the **Server Port**, the username and password of a domain service user (the **Bind DN** and **Bind Password** fields), **Base DN ***, and the time interval in which you want to synchronize the server with your AD Domain (Day—Week—Month—3 Months). For this last option, you should consider activating the syncs every day. Having completed every section's fields, click on the **Save and sync** button.



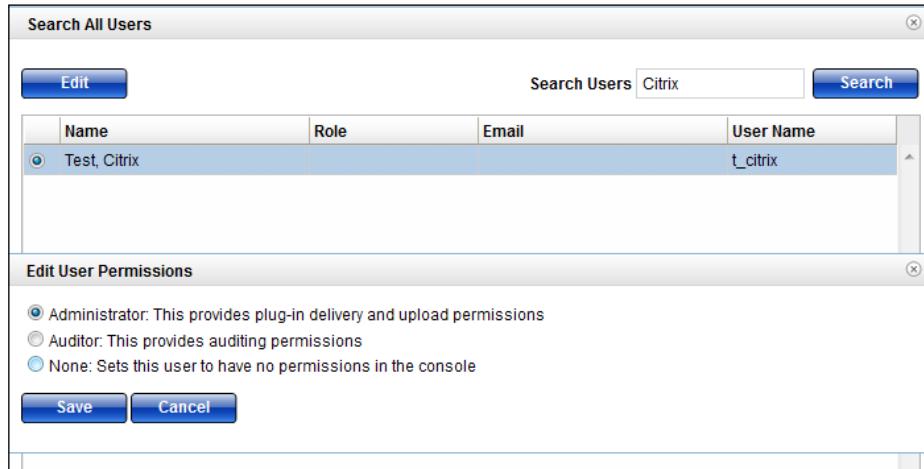
To find the correct Base DN, you can use the AdsiEdit Microsoft tool found at [http://technet.microsoft.com/en-us/library/cc773354\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc773354(v=ws.10).aspx).

11. On the left-hand side panel, click on the **Set Up Guide** link to come back to the previous page, and then select the second link on the welcome screen, **Set Permissions**, in order to configure a domain user other than root to administer Merchandising Server.
12. In the **Search Users** text box, insert a valid name of a user belonging to your domain, and then click on **Search** to proceed.

The screenshot shows a search interface with the following elements:

- A title bar with the text "Search Users" and "Citrix".
- A search input field containing the placeholder text "User Name".
- A blue "Search" button.
- A results table with one visible row. The first column contains a small thumbnail icon, and the second column contains the text "User Name".

13. A pop-up box will be presented to you with the found domain user. Select the corresponding radio button, and click on the **Edit** button to assign a role to this user (**Administrator**, **Auditor**, and **None** to set no roles for the user). In this case, you have to assign the **Administrator** role. Click on the **Save** button to complete the procedure.



14. On the left-hand side menu, click on the **Change Root Password** link, and assign a new password for the root user in order to change the default installation parameter.
15. Log off from the application and log on again using the last configured administrative user in the form of domain/username.
16. The left-hand side menu has changed and has new options available. On the welcome page, you will have some useful links such as **Documentation** and **Video Links**, and a counter for the newly available plugins for your infrastructure (the **New Plug-ins available** section). Click on the **View New Plug-ins** link to proceed with the required operations.
17. Select the desired plugin, checking its radio button, and click on **Download Plug-in** to copy it from Merchandising Server to your local machine. If you want to download all of the available plugins directly from the Citrix website to Merchandising Server, you have to click on **Download All to Server**.
18. After that, the plugins download is complete, so click on the **Uploaded Plug-ins** link on the left-hand side menu in order to view the terms and conditions agreement (the **View Readme** and **View EULA** buttons) and/or delete the imported components (the **Delete** button).

Uploaded Plug-ins		
These plug-ins are now available for delivery.		
Name	Version	Platform
Acceleration Plug-in	5.5.4.26	Vista Win7 XP
Online Plug-in	11.2.0.169077	MacOS10.5 MacOS10.6
Secure Access Plug-in	5.0.1	Vista Vista64 Win7 Win764 XP
Self-service Plug-in	2.0.0.27090	Win7 Win764 XP XP64
Self-service Plug-in	2.1.0.32645	Win7 Win764 XP XP64

19. On the left-hand side menu, in the **Deliveries** section, click on the **Rules** link. In this area, you can create the delivery rules specific to your company based on destination targets, such as User or Computer Domain Membership, Operating System type, Machine Name, or IP Address Range. Populate all the required fields (**Name**, **Description**, **Field**, **Operator**, and **Value**), and click on **Save** to create the rule.

Rule Create/Edit
Use this screen to create and edit delivery rules.

Name:	<input type="text" value="OS_W7_x64"/>
Description:	<input type="text" value="Windows 7 x64 operating system delivery rule."/>
Field:	<input type="text" value="Operating System"/>
Operator:	<input type="text" value="Is"/>
Value:	<input type="text" value="Windows 7 64 bit"/> 
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

20. On the left-hand side menu, in the **Deliveries** section, click on the **Create/Edit** to generate a delivery action or edit an existing one.

The screenshot shows a 'Create a Delivery' wizard with five tabs: 1 - General, 2 - Plug-ins, 3 - Configuration, 4 - Rules, and 5 - Schedule. The 'Delivery name:' field is required.

21. Click on the first tab, **1 - General**, and populate the following fields:

- ❑ **Delivery name:** This field is mandatory. It is the name to be assigned to your delivery.
- ❑ **Evaluation order:** It is the priority assigned to a delivery when distributing it to the users.
- ❑ **Default delivery:** It is a checkbox that selects this component as the default plugin release technique.
- ❑ **Silent install:** Using this, you can decide whether or not to allow the users to see and stop the component installation by selecting either the **Yes** radio button or the **No** radio button.
- ❑ **Check for Updates:** In this field, you can specify how many days have to pass for the clients to contact Merchandising Server for an updates check.
- ❑ **Completion text:** You can insert here the message that you want to send to the users at the end of the component's installation.
- ❑ **Support email address:** If you want, you can insert an e-mail address that refers to a support area. This e-mail will be displayed in the Citrix Receiver support panel.
- ❑ **Support website:** This is the possible website support, which will appear in the Citrix Receiver support panel.
- ❑ **Support phone number:** This is the contact number for the support shown in the Citrix Receiver support panel.

[ Only one Delivery Group can be the default delivery!]

22. Click on the second tab, **2 - Plug-ins**, and then click on the **Add** button to select the quantity of plugins that you want to assign to this delivery. Please also specify the action to be performed on these components in the destination client (**Install** or **Uninstall**).

Add Plug-ins to Delivery					
Adding plug-ins from below will ensure that any user receiving this delivery will have those plug-ins installed on their system.					
	Name	Platform	Version	Language	Action:
	XP64				<input type="button" value="Install"/> <input type="button" value="Uninstall"/>
<input type="checkbox"/>	Offline Plug-in	2K3 2K364 Vista Vista64 WS08 WS08_64 Win7 Win764 XP XP64	6.0.0.1304	de en es fr ja ko ru zh-cn zh-tw	Streams applications to your desktops and executes them in an isolation environment.
<input checked="" type="checkbox"/>	Online Plug-in	2K3 2K364 Vista Vista64 WS08 WS08R2 WS08_64 Win7 Win764 XP XP64	13.1.0.89	de en es fr ja ko ru zh-cn zh-tw	Citrix Receiver (Consumer) includes the Self Service plug-in and enables access to hosted applications and desktop, and SingleSignOn.

23. The third tab, **3 - Configuration**, covers the configuration parameters for Citrix collateral components such as **StoreFront**. To populate mandatory fields, you have to enter the information for the following areas:

- ❑ **Online Plug-in:** Enter the information about the Citrix Store configuration
- ❑ **Acceleration Plug-in:** Hostname or IP Address for the Citrix CloudBridge server

Online Plug-in
Enter configuration information to accompany the Dazzle delivery. Users' store configurations are updated with one or more application stores.
<input type="checkbox"/> Open Dazzle for new users when Receiver starts
Store configuration <input type="text"/> ! (required) (Example: Store name;https://xenapp.citrix.com/Citrix/PNAgent/config.xml)
Create a new item
Acceleration Plug-in
Enter the Signaling IP addresses of the Branch Repeaters separated by commas and without spaces. If the
Hostname(s) or IP Address(s) <input type="text"/> ! (required) (Example: 10.20.30.40,some.domain.com:4433)

Configuring Additional Architectural Components

- ❑ **Online Plug-in:** In the security section StoreFront stores configuration.

The screenshot shows the 'Store configuration' section of the StoreFront stores configuration. It includes fields for security settings like ICA file signature verification and certificate prompts, a text area for Trusted Certificate Thumbprints with an example value, and a link to 'Create a new item'. Below this is a 'Store configuration' field with a placeholder and a note about examples. Further down are sections for allowing users to add stores (with a required field), saving passwords for PNA based stores (also required), and various user interface and reconnect options. A note at the bottom indicates that advanced user menu items can be disabled or enabled by default.

24. In the fourth tab, **Rules**, click on the **Add** button, and select one of the rules previously created. After you've performed the selection, click on **Add** again to complete the task.

The screenshot shows the 'Add Rule to Delivery' dialog box. It features an 'Add' button, a search bar, and a table listing a single rule. The rule is named 'OS_W7_x64' and is described as a 'Windows 7 x64 operating system delivery rule.' It specifies the field as 'Operating System', the operator as 'Is', and the value as 'Win764'. The 'Add' button is highlighted with a red box.

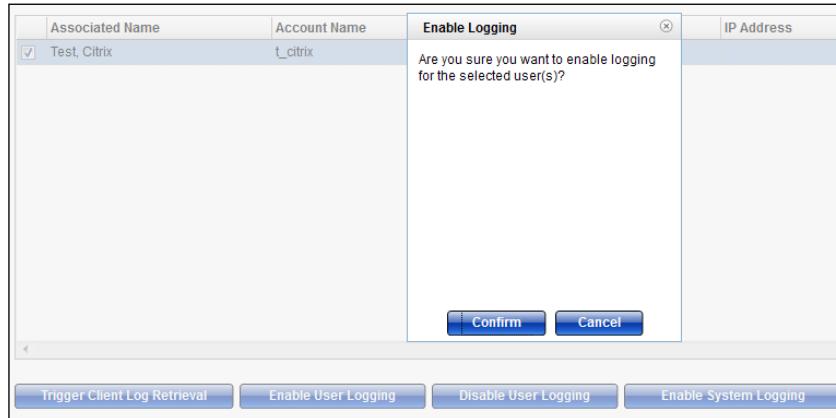
Name	Description	Field	Operator	Value
OS_W7_x64	Windows 7 x64 operating system delivery rule.	Operating System	Is	Win764

25. In the last tab for this section, **5 - Schedule**, please choose **Deliver Now** or **Deliver Later**. In the latter case, please specify the date and time for the action, and then click on the **Schedule** button.



26. After you finish the Delivery configuration, in the left-hand side menu, **Reporting and Logging** section, you can choose among the following tasks:

- ❑ **Delivery reporting:** With this option you can export the reports for the Citrix packages delivery activities.
- ❑ **Enable/disable logging:** For every configured user in Merchandising Server, you can decide to enable or disable the logging activities by flagging the record referring to it. Moreover, you will also be able to activate system logging.



- ❑ **View log files:** Using this option, you will be able to view and download the Client and Server log files for troubleshooting and analysis activities.

Configuring Additional Architectural Components

Once you have completed all the configuration tasks, you can test the availability of Citrix Receiver by typing its FQDN in your browser's address bar in the form of `http://hostname.domainname` or `https://hostname.domainname`. A website will appear, giving to you the possibility to manually download the latest release in your infrastructure of Citrix Receiver.



© Citrix Systems, Inc. All Rights Reserved.

How it works...

Citrix Merchandising Server allows you to make the delivery of plugins easier and more centralized and secure for both the internal and remote user categories, giving the user the ability to work with both online and offline plugin types. Virtual Appliance is initially configured to only work with the default administrative user root. In order to make all the options available, you have to connect Merchandising Server with Active Directory Domain, configuring a primary **domain controller (DC)** and if possible, also a back up DC. To perform this operation, you need to create a user account in your domain to permit Virtual Appliance to read Active Directory and synchronize with it. Once the domain configuration has been completed, it's time to assign the administrative permission to one of the domain users. A good solution could be assigning them to your user domain.

With Merchandising Server, you can archive all the available plugins for the supported platforms. This is the base on which to structure the rules and the deliveries, the way, and the policies by which this virtual appliance distributes the agents to all the connection devices. A rule is made of a set of conditions that must be satisfied to activate the associated event. Merchandising Server offers you a range of categories such as Operating System, IP Address Range, and Machine Name. With these choices, you can filter the application scope for a rule.

After a rule has been created, it can be associated to a delivery, which is the container of the distribution policies applied to the devices.

Moreover, you have to configure the priority assigned to the delivery (which will reflect the distribution priority) for the plugins to send to the user devices, such as PCs or smart phones.

After linking a previously created rule to the delivery, the last step is to configure a valid schedule time to execute the component's distribution, deletion, and/or upgrade: if you've correctly planned the deliveries and the rules contained in it, you could have a huge reduction in manual and repetitive activities.

There's more...

Citrix Merchandising Server optionally offers you the possibility to connect with Citrix Receiver through an SSL secure channel; to use this kind of connection, you need a certificate for validating the communication established with the server. On the left-hand side panel of the management area, you have the **SSL Certificate Management** link; in this section, you will find a drop-down menu with all the possible activities about the **Certification Authority (CA)** management:

- ❑ **Manage SSL Certificates:** In this option, the server will display the current certificate configuration. No further operational activities are permitted.
- ❑ **Generate self-signed certificate:** A self-signed certificate is generated by default from Merchandising Server with a validity of 30 days. Selecting this option requires certificate regeneration every month. To regenerate after the expiration time period, you have to populate all the required fields, such as **Common Name, Organization Name, Organization Unit, Locality Name, State Name, and Country Code**.
- ❑ **Export certificate signing request:** With this option, you will generate a request to obtain an SSL certificate. As previously seen, you have to populate all the required fields to generate a valid request (**Common Name, Organization Name, Organization Unit, Locality Name, State Name, and Country Code**) plus the certificate key size (**2048, 4096, or 8192**).



Remember that you have to populate the **Common Name** textbox with the Merchandising Server FQDN for both the **Generate** and **Export** tasks.

- ❑ **Import certificate from a certificate authority:** In the presence of an already-existing CA architecture, Merchandising Server allows you to import an SSL certificate located on an external CA server (for instance, a CA based on Microsoft Windows technology). As a mandatory object, you have to load **Public Certificate File**; optionally, you can insert **Intermediate Certificates** and the **Private Key** files and populate the last textbox with **Private Key Password**.
- ❑ **Import root certificate:** This is an optional operation to be performed in case of a certificate is generated by an external CA. In such a case, you need to import **Root Certificate File** and insert the **Alias** certificate to make the certificate identification process easier. Both options are mandatory.

In the presence of specific platforms, such as Android devices, some SSL authorities cannot be recognized. To check the validity of the certificate chain, you could refer to the available check tools, such as www.sslchecker.com.

See also

- ▶ *Chapter 7, Deploying Applications*

Configuring the CloudBridge platform

When we refer to a Citrix architecture, we usually intend a complex infrastructure located in the same area or building. In some cases, especially in the presence of huge organizations, you could have a central infrastructure used by many remote locations, also known as branch offices. In this case, the native optimization of the ICA protocol may be not sufficient to get the performance needed by the remote users to work without having performance issues because of the WAN connection. In this scenario, Citrix presents CloudBridge, which is a WAN optimizer, developed for such kinds of situations. It is in the form of some physical network devices and Virtual Appliance. In this chapter, we're going to discuss this second solution.

Getting ready

CloudBridge Virtual Appliance is downloadable from your MyCitrix account as a single component or as a part of the XenDesktop 7 suite Platinum version. This component is available for downloading in the form of a template for the XenServer, vSphere, and Hyper-V Hypervisors. After downloading, you need to import it into your infrastructure and assign a network to both the configured network cards, one connected to the LAN area and the other pointing to the WAN network. You also need to generate a license file for this platform from the license portal in your MyCitrix account; you have to assign the required number of licenses to allow all the users working from remote locations. Then you have to import the generated file in License server as shown in the *Installing and configuring the Citrix Licensing Services – 11.11.1 recipe, Chapter 1, XenDesktop® 7 – Upgrading, Installing, and Configuring*.

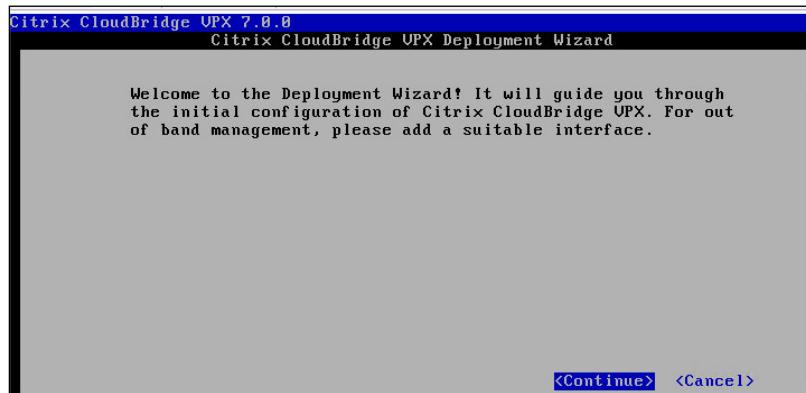


To generate a valid license file for CloudBridge Virtual Appliance, you have to insert the Host ID of your license server. You can find this information in the **System Information** section of the **Administration** panel.

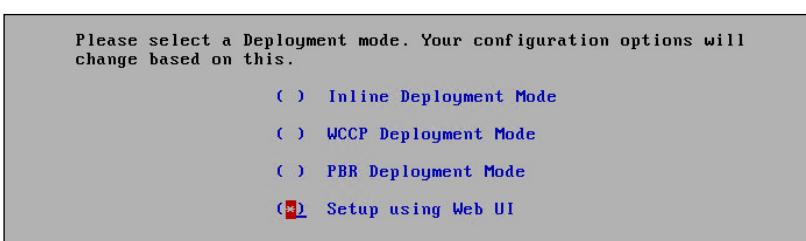
How to do it...

In the following steps, we will perform the installation and configuration of Citrix CloudBridge Virtual Appliance, also known as CloudBridge VPX:

1. Mount or extract the CloudBridge ISO file, select the template version for your hypervisor (VMWare vSphere, Citrix XenServer, or Microsoft Hyper-V), and import the template in your virtual infrastructure.
2. Connect to your hypervisor host, and open the console of the imported Virtual Appliance.
3. In **Citrix CloudBridge VPX Deployment Wizard**, select the <Continue> option to proceed with the first platform setup:



- [ In the **Warning** screen, be sure you have not connected the CloudBridge interfaces on the same virtual switch configured on your Hypervisor; this could make you experience network loop issues.]
4. In the **Select Deployment Mode** screen, choose one of the available options, and then select <Continue>:

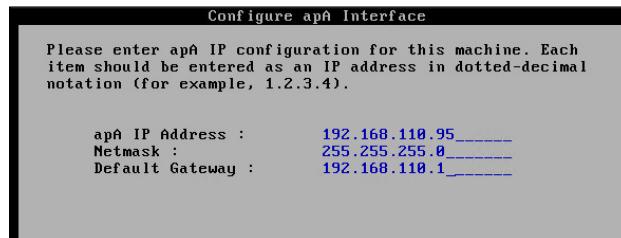




For the scope of this chapter, you have to choose the **Setup using Web UI** option in the previous menu.



5. Assign a valid network configuration in the **Configure apA Interface** screen, and after completion, click on the <Ok> option:

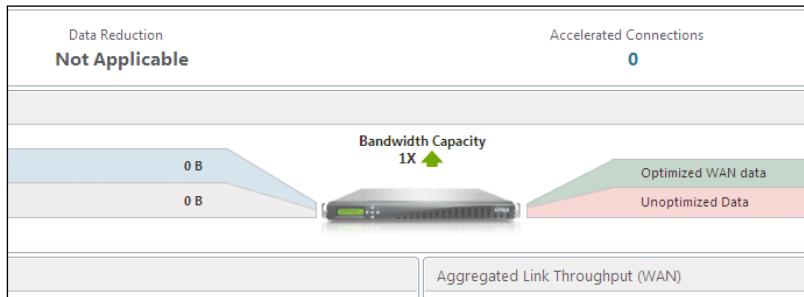


6. After reviewing the configured options in the **Configured Parameters** menu, click on the <**Finish**> button to complete the first configuration phase.
7. Verify whether the restart has been completed successfully by pinging the IP address assigned to the CloudBridge network adapter.
8. Open a web browser, and type the URL, https://CloudBridge_IP_address, in the address bar. You will see the web login interface for this Virtual Appliance as follows:

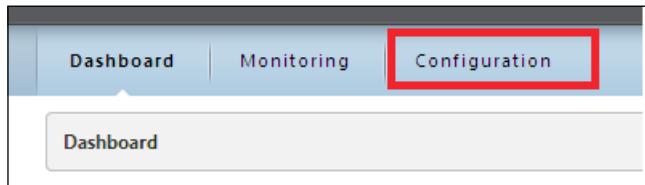


9. Insert the default credentials (admin/password), and click on the **Login** button.

10. You will be prompted with the **Dashboard** screen in order to retrieve the current state of CloudBridge Platform:



11. In the menu bar on the top of the screen, click on the **Configuration** link, in order to proceed with the customization of the CloudBridge settings:



12. In the left-hand side menu, expand the **Appliance Settings** section, and click on the **Licensing** link. In the **License Server Location** tab, select the **Remote** radio button, and populate all the required fields with the details of the license server. Then, click on the **Apply** button, and wait for the time needed to restart the repeater:

License Server Configuration

License Server Location:	<input type="radio"/> Local <input checked="" type="radio"/> Remote
Remote License Server Address:	vmxd7-xddc-01.xdseven.local
Remote License Server Port:	27000
Model:	Citrix CloudBridge V45
Crypto License (from Remote License Server):	<input type="checkbox"/> Requested
MaxBW Enabler License (from Remote License Server):	<input type="checkbox"/> Requested
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	



Remember that you need to preallocate the licenses to the license server by generating the required file containing the CloudBridge licenses.

13. In the **Appliance Settings** section in the left-hand side menu, click on the **Administrator Interface** link; select the **User Accounts** tab; and modify the default password for the **Admin** user. If you want, you can also add additional users:

User Name	Type	
Admin	Admin	Modify

Add New User

Modify 'Admin'

Change:

Password:

Re-enter:

Type: Admin

[Update](#) [Cancel](#)

14. In the left-hand side menu, go to **Windows Domain | Appliance Settings**; this will open a domain configuration page. Then, click on the **Join Domain** button, and populate the information fields to complete the task. After this, click on the **Join** button, and then wait for the restart of the Citrix CloudBridge platform:

Domain Name	xdseven.local
Domain User	administrator
Domain Password

[Join](#) [Cancel](#)

[ Join the CloudBridge platform to the same XenDesktop domain in order to have a single and centralized authentication platform.]

15. In the **Optimization Rules** section, located in the left-hand side menu, select the **Application Classifiers: Edit Application** link; in this area, you can view and edit the application group(s) configured by Citrix, and you can also create new applications to permit CloudBridge Virtual Appliance to identify them during acceleration activities. Select an application category from the drop-down list, and then click on the **Edit** button in the **Action** column. In the following screenshot, we've selected the **Citrix Protocols** as **Application Group**:

Application Classifiers: Edit Application

Name	ICA
Description	XenApp and XenDesktop Traffic (ICA)
Application Group	Citrix Protocols Client-Server Content Delivery Custom
Classification Type	TCP
Classification Parameters	TCP Port: 1494 <small>Range, list or number between 0 and 65535. examples: 1501 1501, 1502, 1503 1501-1505, 1507</small>

16. In the left-hand side menu, in the **Appliance Settings** section, click on the **Logging/Monitoring** link. In the first tab, **Log Options**, select a suitable **Log Max Size** value in MB (default **1024**), the **Max Export Count Default** value (default value **10000**) and the log category that you want to collect (**Log System Records**, **Log Adapter Records**, **Log Flow Records**, **Log Connection Records**, **Log Open/Close Records**, **Log Text Records**, **Log Alert Records**, or **Log CIFS/SMB records**). After that, click on the **Update** button to make the changes persistent.
17. In the **Alert Options** tab of the **Logging/Monitoring** category, you can configure the monitoring sensor to assign the configured system groups(**Alerted**, **Logged**, and **Disabled**) and the percentages threshold levels wherever possible. After this configuration, click on the **Update Alert Message Settings** button.

Logging/Monitoring: Alert Options

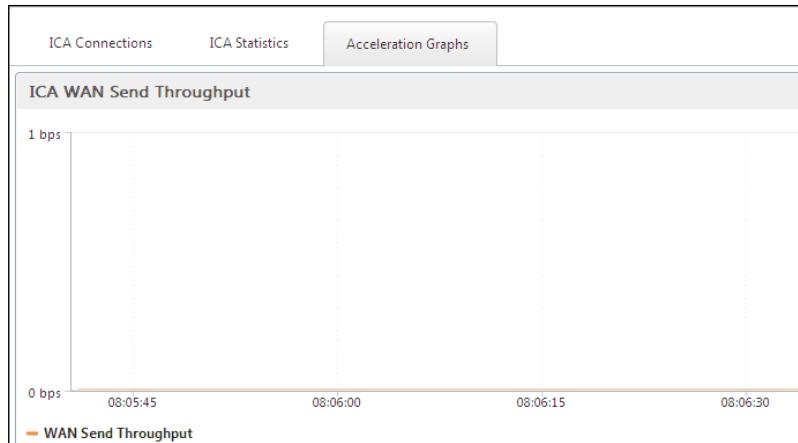
Alerted	Logged	Disabled	Description
<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	WAN Loss Rate
<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	LAN Loss Rate
<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	Connection Stalled, Probable Application Hang
<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	Connection Timed Out
<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	Invalid Connection Attempt
<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	NIC Negotiated Half Duplex

18. Select the **Syslog Server** tab in the **Logging/Monitoring** category if you have got a Syslog server to which it can send the collected logs. In this case, you have to tick the **Send To Syslog Server** option, specifying the **Syslog Server IP** and **Syslog Server** port. After this is completed, click on **Update**.
19. In the **Optimization Rules** section, click on the **Links** menu, and edit the traffic link shown in the **Link Definition** tab. For all of this link, you can configure **Name**, **Link Type (LAN or WAN)**, associated bandwidth (**Bandwidth In** and **Bandwidth Out**), and, if necessary, you can implement filter rules by specifying network parameters such as source and destination IP addresses or network adapters MAC addresses. After this is completed, click on the **Save** button.

Links: Edit Link		
Link Definition Hardboost/Softboost Traffic Shaping		
Name	Link (apA.1)	
Link Type	LAN	
Bandwidth In	1	gbps
Bandwidth Out	1	gbps
Filter Rules	Adapter apA.1	Src IP Any
Click on filter rule field to edit		

[ The **Bandwidth** parameter is based on the CloudBridge VPX license that has been purchased. Make sure you have configured the **Bandwidth In** and **Bandwidth Out** parameters in line with your license..]

20. Click on the **Monitoring** link on the menu bar (at the top of the information section), and then select the **Citrix (ICA/CGP)** link. In the **ICA Statistics** tab, you can find statistics about the use and the optimization of the ICA protocol. In the same section, clicking on the **Acceleration Graphs**, you will obtain a real-time graphical representation of the optimized ICA traffic.



21. You can obtain similar information about the network file systems or the Outlook MAPI protocol use by clicking on the left-hand side menu links called **Filesystem (CIFS/SMB)** and **Outlook (MAPI)**.
22. Click on the **Usage Graph** link in the left-hand side menu—**Usage Graph Monitoring section**—to have general traffic information about the WAN and LAN network usage with **Last Minute, Hour, Day, Week, and Month** views.

How it works...

Citrix CloudBridge Virtual Appliance, also known as CloudBridge VPX, is a less expensive and more flexible solution to optimize and improve the WAN connection among remote locations; the opposite product is the complete range of CloudBridge appliances.

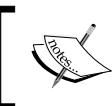
CloudBridge VPX has been developed to run as a virtual machine under Citrix XenServer, VMware vSphere, and recently also on Microsoft Hyper-V. Within these hypervisors you have two possible scenarios: the first is made up of a set of CloudBridge virtual appliances equal to the number of the remote offices, each of them in communication with the main CloudBridge office. The second scenario is constituted by a single CloudBridge in the main office and the peripheral locations linked by the use of a plugin called the Repeater Acceleration plugin. With this second scenario, an SSL VPN connection and Citrix NetScaler Gateway are necessary.



We will discuss the NetScaler® Gateway in *Chapter 8, XenDesktop® Tuning and Security*.

If you are using two or more Virtual Appliances in the common configuration, for best practice, you can choose between two different network topologies:

- ❑ **Inline mode:** With this modality, you need two network interfaces, which can be attached to two physical interfaces, to one physical interface and one virtual interface, or to two virtual interfaces. The last case is used only for test and simulation purposes.
- ❑ **One Armed mode (WCCP):** Also, in this case, you need two network adapters, but one of them must be directly attached to a router through a physical network card, and the other must point through a virtual interface to CloudBridge VPX.



You can find further details about the network configurations at
<http://support.citrix.com/article/CTX131015>.



With the VPX version, the only way to implement an HA configuration is given by the high availability of the hypervisor system. You can't configure two virtual appliances in an active/passive clustered configuration.

Once you've installed Virtual Appliance, the first operation to perform is its configuration with the use of the CLI. In this way, you will configure the virtual network adapters (identified with the `apA.x` name, where `x` is a number equal to the configured interfaces) by assigning the network parameters such as the IP Address or the VLAN ID. After every critical configuration, a restart is needed in order to make the changes active. Now that the web management console is available, you can login with the same username and password used to connect to the CLI (default admin/password). Once logged in, the first action to perform is interfacing CloudBridge with the license server of your company. Remember that with the non-express version of this product you must use the standard license server. To use the internal CloudBridge license platform, you need the express version. You have to license the right version—be careful about the final part of the product name (`Vx`)—the associated number refers to the speed of the network link in MBps for which you've bought the licenses).



Information on the available licenses can be found at <http://www.citrix.com/products/cloudbridge/features/editions.html>.



After this step has been completed, modify the default administrative password; moreover, by joining CloudBridge to the company domain, you'll be able to add users other than the default account.

The latest version of the VPX is loaded with preconfigured applications divided by category; each application has its communication ports already configured; thanks to this implementation, the CloudBridge platform is able by default to optimize the network use of critical applications, such as Citrix Protocols, Microsoft Exchange, LDAP, or database platforms; and you can also create and insert any missing application. This section is strongly linked to the **Traffic Shaping** policies and the **Service Classes** sections. For every configured application, you have the capability to specify **Acceleration Policy** (disk, memory, or flow control) and the traffic priority for the specified application. This way, you have full control and regulation of the use of the network by the application's users.



An important configuration parameter is the available bandwidth assigned to the WAN and LAN area. Don't forget to rightly configure these two values in the Links section!



Usually, Citrix also in such cases offers the logging feature, which is can be configured to perform troubleshooting activities. In addition to the log size and the areas on which you are logging, you can decide to generate a message alert or an event log for every configured alert option, such as **WAN or LAN loss rate**, **Out of CPU or Memory resources**, and **Compression Error detected**.

The point of strength for CloudBridge is its great ability in the compression and "de-duplication" of network traffic. You can monitor these activities in real time, thanks to the integrated monitoring platform offered by CloudBridge VPX.

There's more...

The CloudBridge plugin, which is an alternative to allowing the remote users to communicate with the CloudBridge platform located in the main office, is configurable using two different approaches:

- ▶ **Redirector modality:** With this configuration, the plugin transfers the traffic directed to a server machine from the user client to the CloudBridge VPX. Then, the accelerator transfers the request to the destination server. To enable this mode, you have to select the **CloudBridge Plug-ins** link in the left-hand side menu of the VPX appliance and select the **Redirector** radio button. This configuration should be used only when it's necessary to your infrastructure using the target appliance as a proxy, which redirects the traffic from the plugin to the destination server and back.

- ▶ **Transparent modality:** With this configuration, you have a situation similar to the connection between two appliances. So after the plugin has successfully contacted the VPX, it performs a download of the acceleration rules, which will be seen to verify if the established connection is regulated with the acceleration policies. To enable this mode you have to select the **CloudBridge Plug-ins** link in the left-hand side menu of the VPX appliance and select the **Transparent** radio button. This option should be used in the presence of a set of preconfigured CloudBridge appliances using a pass-through connection between the client plugin and the destination virtual appliances. Citrix recommends using this second plugin mode.

For both the options, you have to specify a private IP address, which will be available only after you've established the secure VPN connection, and a port in the **Signaling IP** and **Signaling Port** textboxes.

CloudBridge Plug-in: Signaling Channel Configuration	
Status:	Configuring
State:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Signaling IP:	192.168.110.99
Signaling Port:	443
Signaling Channel Source Filtering:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Connection Mode:	<input checked="" type="radio"/> Redirector <input type="radio"/> Transparent
LAN Detection:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled Round Trip Time: 20 ms
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

See also

- ▶ The *Installing and configuring Citrix® NetScaler Gateway 10.1* recipe in Chapter 8, *XenDesktop® Tuning and Security*

Installing and configuring the XenDesktop® Collector

In some situations, an expert IT system administrator would not be capable of understanding a problem during the log collection and analysis activities.

In this case, vendor support could be the only way to solve the problem. Citrix offers IT professionals a log-collecting software, which can directly upload the required information to the support working team; this is the XenDesktop Collector program.

Getting ready

Citrix XenDesktop Collector is a ZIP archive that contains two setups in the form of an msi package for both 32-bit and 64-bit operating system versions, downloadable from your MyCitrix account. You need to connect to your Desktop Controller server with administrative credentials in order to be able to install this program.

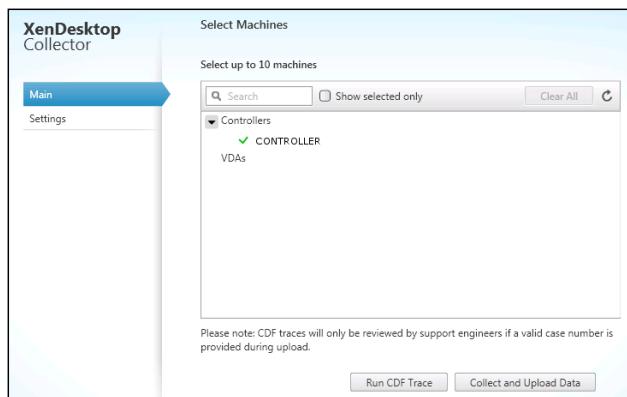
How to do it...

In this section, we will configure the Citrix software used to collect the XenDesktop system logs:

1. Extract the Collector archive on your Desktop Controller machine, and double-click on the setup for your operating system version (XDCollector.msi for 32-bit and XDCollectorx64.msi for 64-bit).
2. On the welcome screen, click on the **Next** button to proceed, accept **End-User License Terms**, and then click on **Next** to continue.
3. Select the installation path for Collector; the default location is C:\Program Files\Citrix\XenDesktopCollector\. Click on the **Next** button to proceed.
4. To complete the installation procedure, click on the **Install** button.
5. After completing the previous step, leave the **Launch Citrix XenDesktop Collector** option checked, and click on the **Finish** button.
6. On the first Collector screen, you can find information about the configured controllers on which you are operating. If you want to register an error trace during an error reproduction, you have to click on the **Run CDF Trace** button.

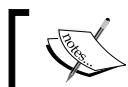


The CDF Trace acronym stands for Citrix Diagnostic Facility Trace.



7. To start the error and data collection on Desktop Controller, click on the **Collect and Upload Data** button. After it's completed, the XenDesktop Collector will present you with a login screen in which you insert a username and password for the Citrix Auto Support platform in order to upload your data to Citrix Support. As an optional field to populate, you can insert a ticket number assigned by the support platform to analyze the generated CDF traces. If you want, you can view the collected items by clicking on the **View Data** link.

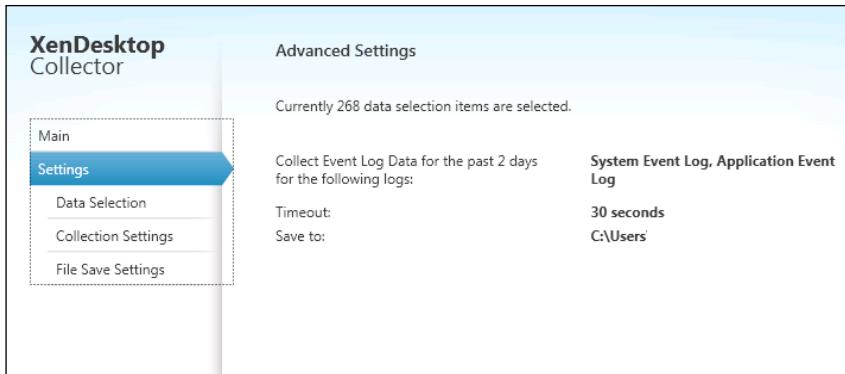
The screenshot shows a web-based interface for data collection. At the top, a message says "Data Collection completed" with a green checkmark icon and "164 items on 1 machines (6 kb)". A blue "View Data" link is next to it. Below this, there is a section titled "Please login to upload: (Required)" with "Username" and "Password" fields. The "Username" field contains "username" and the "Password" field contains "*****". A link "Account locked or forgotten your password?" is provided. Further down, there is a "Support case number:" field with the placeholder "(Required for analyzing CDF traces)" and an empty input field. At the bottom right is a blue "Upload" button.



The Citrix Auto Support platform can be also used by customers without an active support subscription.



8. After the first log collection has been completed, you can modify the default configuration by clicking on the **Settings** link in the left-hand side panel. In the **Settings Panel Alert** pop-up screen, click on the **Continue** button to bypass the Citrix advice and continue with the operations. In the **Advanced Settings** main menu, you will find an overview of the current collection configuration.



9. Click on the **Data Selection** link, and select the collection options for the categories shown beneath them; if possible you should leave all the default options checked:
 - ▶ **Site**
 - ▶ **Controller**
 - ▶ **VDA**
10. Click on the **Collection Settings** link, and select either **Collect all Event Logs**, or specify the interval data collection in days. After this step, flag the log types to collect (**System Event log**, **Application Event log**, or **Security Event log**), and specify **Collection Timeout** in seconds and the maximum number of machines on which data will be collected. If you've modified at least one of these settings, click on the **Save Settings** button to register your changes.

Collection Settings

Event Log

Days of Event Logs to collect

Collect all Event Logs

Logs to Collect

System Event Log
 Application Event Log
 Security Event Log

Collection Timeout

Maximum seconds to collect an individual data point
 Data points that exceed the timeout value will be skipped and noted in the error log.

Machine Settings

Maximum number of selectable machines

11. By clicking on the **File Save Settings** link in the left-hand side menu, you can specify the location in which to save the generated reports. If you want to delete them after a successful upload, please flag the **Delete reports after they are successfully uploaded** option.

How it works...

The Citrix XenDesktop Collector tool helps the system administrators to automate the log collection activities. This software cooperates with the Citrix Auto Support platform, also known as TAAS, which is a public Cloud portal on which you can transfer the result of the collections in your infrastructure, allowing Citrix Support to analyze them to work on your architectural issues.



You can log in to the Citrix TAAS platform at <https://taas.citrix.com> with your MyCitrix account credentials.



The Collector method is quite simple to work with because it runs a series of queries to collect configuration information at three different levels: Site level, Controller level, and **Virtual Desktop Agent (VDA)** level. These categories cover all the hardware and software aspects, such as Desktop Controller hardware, software and registry configurations, XenDesktop Catalog and Desktop Groups, the Virtual Desktop Agent software parameters, and everything concerning the Citrix policies implementation. You also have the possibility of choosing the time period to run these system statistics and determining the number of machines to be included in the reporting activity. You can perform the collection in two different ways: the first, called CDF Trace, which runs during the reproduction of a specific problem, and the second is called Collect, which is a full gathering of all the system information.

There's more...

If you want, you can work with XenDesktop Collector in an advanced way using its **Command-line Interface (CLI)**. This is a powerful tool used to manage and control the log collection not only by the use of the GUI. At the software installation path (by default, which is `C:\Program Files\Citrix\XenDesktopCollector`), there is the executable file to run the CLI command, `XDCollector.exe`. The following are the CLI principal commands and their abbreviations:

Description	Command	Abbreviation
Run in GUI mode	<code>--gui-mode</code>	<code>-g</code> or <code>-gm</code>
List infrastructure machines	<code>--list-machines</code>	<code>-m</code> or <code>-lm</code>
Collect data	<code>--collect</code>	<code>-c</code>

Description	Command	Abbreviation
Output file for the collection data	--output-file=filename	-o or -of
Include machines by their FQDN—Comma separated	--include-machines=FQDN1, FQDN2...	-q or -im
Upload the collected archive	--upload	-U
Username for the upload action	--upload-user	-u or -uun
Password for the upload action	--upload-password=your password	-p or -up
Server for the upload action—Default https://taas.citrix.com	--upload-server=server address	-S or -us
Run the trace collection on the specified machines—FQDN comma separated	--trace-machines=FQDN1, FQDN2...	-Q or -tm
Run CDF Trace	--trace	-t

So, for instance, if you want to list all the configured controllers for your infrastructure, run the following command:

```
XDCollectore.exe --list-machines
```



To avoid resource lock problems, run XenDesktop Collector using either GUI or CLI, but not both.

See also

- ▶ [Chapter 8, XenDesktop® Tuning and Security](#)

6

Creating and Configuring a Desktop Environment

In this chapter, we will cover the following recipes:

- ▶ Creating and configuring the Machine Catalog
- ▶ Modifying an existing Machine Catalog
- ▶ Using the new Citrix® Director platform
- ▶ Configuring printers
- ▶ Configuring USB devices

Introduction

In the first five chapters of this book, we have installed and configured all the main architectural components used to implement the XenDesktop suite and to use different useful technologies.

Now it's time to proceed with the creation of the Virtual Desktop instances. The copies of the virtual image template will be released to and used by end users. In this chapter, we'll learn how to perform this task, maintain and modify the desktop collections—both server and desktop OS—and gain the ability to use existing machines (physical or virtual), collecting them in delivery groups.

Creating and configuring the Machine Catalog

All the virtual resources released to the end users are part of a group collection called **Machine Catalog**. This contains information about the kind and the number of Virtual Desktop instances, the configurations, and the assignment based on the Active Directory objects (users, groups, and computers). In this recipe, we're going to perform a full creation and configuration of all of these elements.

Getting ready

To correctly perform the configuration tasks you need administrative credentials for the Delivery Controller server, and to be able to use the created Virtual Desktop(s), you first need to install and configure the required **Virtual Desktop Agent (VDA)** plugin on the client device, as shown in *Chapter 5, Configuring Additional Architectural Components*.

You also have to generate a snapshot within your **hypervisor environment** for the Master-image virtual machine created to deploy the Virtual Desktop instances. The VM creation has been discussed in *Chapter 3, Master Image Configuration and Tuning*.

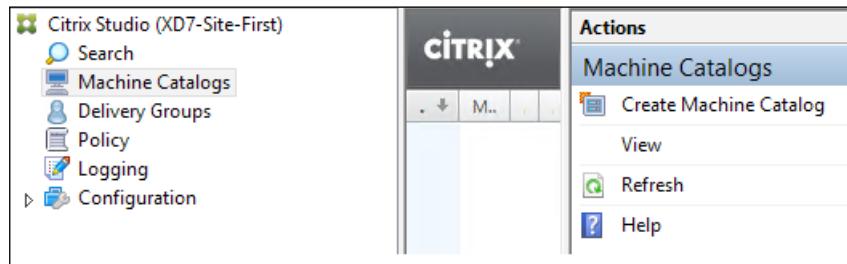
How to do it...

The following steps explain how to create and manage a XenDesktop Machine Catalog:

1. Connect to the Delivery Controller server as an administrative domain user.
2. Hit the Windows + C key combination, search for the Citrix Studio icon in the Citrix software section, and click on it.



3. Based on the connection to the hypervisor explained in *Chapter 2, Configuring and Deploying Virtual Machines for XenDesktop®*, on the left-hand menu, select the **Machine Catalogs** link. After selecting the link, click on the **Create Machine Catalog** link on the right-hand panel.



4. On the **Getting Started** screen, click on the **Next** button to proceed.

Windows Desktop OS – catalog configuration

The following is the configuration procedure for the Windows Desktop OS:

1. In the **Operating System and Hardware** section, select the type of desktop you want to create (**Windows Desktop OS**). After selecting the appropriate radio button, click on **Next**.

Studio

Operating System and Hardware

We want to help you create the correct type of Machine Catalog by asking a few questions to provide a recommendation

[Learn more](#)

Select an operating system and machine type for this Machine Catalog.

Windows Desktop OS
The Desktop OS Machine Catalog provides VDI desktops ideal for a variety of different users.

Windows Server OS
The Server OS Machine Catalog provides hosted shared desktops for a large-scale deployment of standardized machines.

Remote PC Access
The Remote PC Access Machine Catalog provides users with remote access to their physical office desktops, allowing them to work at any time.

2. In the **Machine Management** section, select the kind of infrastructure to use to deploy the resources (**Virtual machines** or **Physical hardware**). Then choose the methodology to use to manage the catalog resources (MCS, PVS, or instances already configured). After completion, click on the **Next** button.



Please refer to the *How it works* section included in this recipe to understand the differences between the listed catalogs and machine types.

Machine Management

As part of creating a Machine Catalog, the way you plan to provision machines influences the recommended Machine Catalog type.

[Learn more](#)

This infrastructure will be built using:

- Virtual machines
- Physical hardware

Desktop images are managed using:

- Machine Creation Services (MCS)
- Provisioning Services (PVS)
- Another service or technology

I will manage my desktop images with something other than Citrix technology. I have existing Master Images already prepared.



If you choose PVS management, you have to specify a valid provisioning service server address and Windows domain for the device collection.

3. In the **Desktop Experience** section, select an option to assign resources to users each time they log on and whether or not to save users' personal data within the existing virtual desktops. After completion, click on **Next**.

Desktop Experience

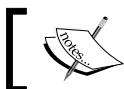
Consider the tasks your users perform and then decide which desktop experience would be best.

Which desktop experience do you want users to have?

- I want users to connect to a new (random) desktop each time they log on.
- I want users to connect to the same (static) desktop each time they log on.

Do you want to save any changes that the user makes to the desktop?

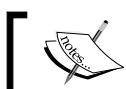
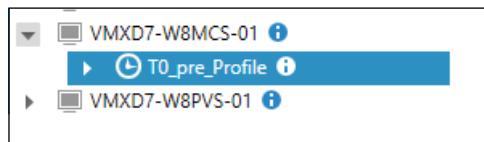
- Yes, save changes on a separate Personal vDisk.
- Yes, create a dedicated virtual machine and save changes on the local disk.
- No, discard all changes and clear virtual desktops when the user logs off.
If configured, folder redirection will not be affected.



If you select the first option, random desktop allocation, you won't be able to select the location in which the users' saves the profile data.



4. Select a master image from the list in order to select the master image from which the desktop instances will be generated. After completion, click on **Next**.



The image selected from the list is a snapshot that refers to the original virtual machine disk.



5. In the **Virtual Machines** section, select how many machines must be generated by incrementing the value of the **Number of virtual machines needed** section. After this, you need to configure the resources to assign to any instance—**Virtual CPUs** and **Memory (MB)**. Click on **Next** to proceed.

A screenshot of the 'Virtual Machines' configuration screen. It shows the following settings:

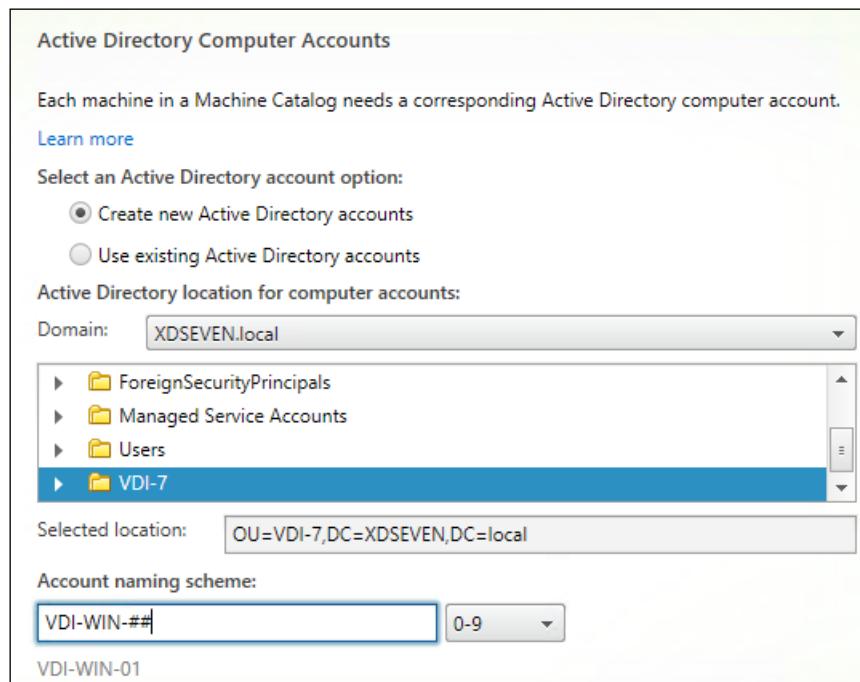
Virtual Machines	
Number of virtual machines needed:	
2	- +
Configure your machines:	
Name:	T0_pre_Profile
Virtual CPUs:	2
Memory (MB):	2048
Hard disk (GB):	32



Note that you can't modify the operating system disk size parameter because it depends on the master image template configuration. On the template, make sure you have mapped the virtual disk with ID 0:0 (first created disk for the machine); otherwise, you will receive an error during this configuration step.



6. In the **Active Directory Computer Accounts** section, choose **Create new Active Directory accounts** or **Use existing Active Directory accounts**. To better understand all the creation features in this section, we will select the first option.
7. In the **Active Directory location for computer accounts section**, select from the dropdown list the domain on which you are working and choose the organizational unit on which you want to create the computer accounts. Then select an **Account naming scheme**, of the form MachineName##, where the two final characters identify a progressive code made up of letters or digits (A-Z or 0-9). After completion, click on the **Next** button.



8. In the **Summary** section, assign a name and an optional description in the respective fields (**Machine Catalog Name** and **Machine Catalog description for administrators**), then click on the **Finish** button to complete the configuration operations.

Summary

Machine type:	Windows Desktop OS
Machine management:	Virtual
Provisioning method:	Machine creation services (MCS)
Desktop experience:	Users connect to the same desktop each time they log on Discard all changes when the user logs off
Resources:	VMware01
Master Image name:	T0_pre_Profile
Number of VMs to create:	1
Virtual CPUs:	2

Machine Catalog name:
Desktop-C01

Machine Catalog description for administrators: (Optional)
Desktop-C01

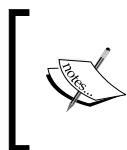
Note: To complete the deployment, assign this machine catalog to a Delivery Group by selecting Delivery Groups and then Create or Edit a Delivery Group.

Back **Finish** **Cancel**

Windows Server OS – catalog configuration

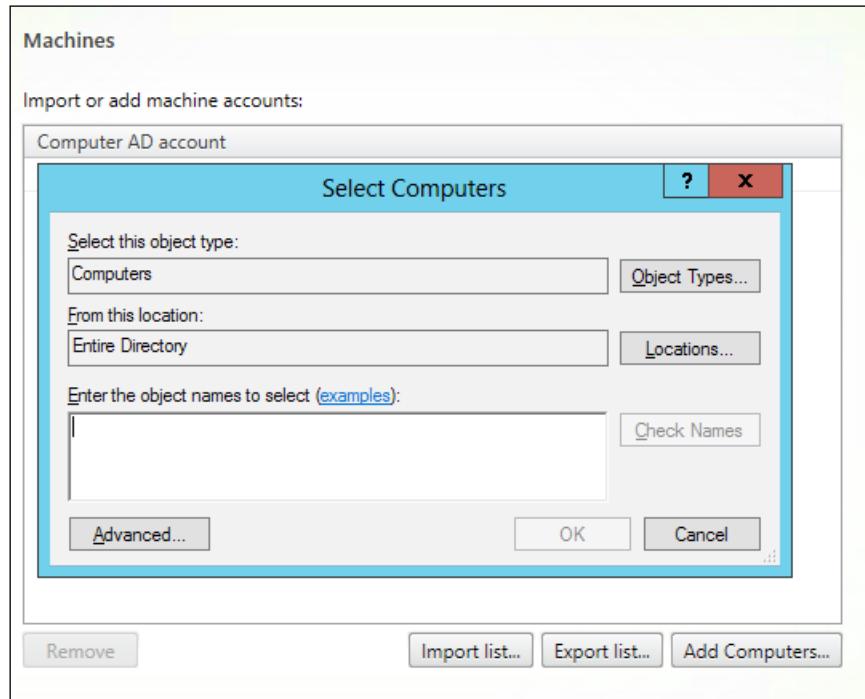
The following is the configuration procedure for the Windows Server OS:

1. In the **Operating System and Hardware** section, select the type of desktop you want to create (**Windows Server OS**). After selecting the appropriate radio button, click on **Next**.
2. In the **Machine Management** section, select the kind of infrastructure to use to deploy the resources (**Virtual machines** or **Physical hardware**), and then choose the methodology to use to manage the catalog resources (MCS, PVS, or master images already configured). After completion, click on the **Next** button.



In this subsection, we will select the use of physical machines plus the existing Master Image option. In case of virtual machine selection, you have to repeat the steps seen earlier in the *Windows Desktop OS* section, for both MCS and PVS deployment options.

3. In the **Machines** section, add an existing domain-joined server to the catalog by clicking on the **Add Computers...** button and then on **Next** to continue.



4. In the **Summary** section, enter a name and an optional description in the respective fields (**Machine Catalog Name** and **Machine Catalog description for administrators**), and then click on the **Finish** button to complete the configuration operations.

Remote PC Access – catalog configuration

The following is the configuration procedure for Remote PC Access:

1. In the **Operating System and Hardware** section, select the type of desktop you want to create (**Remote PC Access**). After selecting the appropriate radio button, click on **Next**.
2. On the **Machine Accounts** screen, add an existing domain machine account, or a group of them, by clicking on the **Add OUs...** button; then click on **Next** to continue.

Machine Accounts

Machines in your network domain have an associated machine account. The machine account name is usually the same name as the machine. The machine accounts you choose must match the machines that users use for remote access. To add groups of machines by Organizational Units (OUs), select Add OUs.

Select the machine accounts and/or OUs associated with your users:

To get started, add a machine account or OU.
[Learn more](#)

Add machine accounts... Add OUs... Remove

Some machine accounts or organizational units running Windows XP.
 You should also select this option if the physical PC is running Windows 7 with any VDA prior to 7.0

3. In the **Summary** section, assign a name and an optional description in the respective fields (**Machine Catalog Name** and **Machine Catalog description for administrators**), and then click on the **Finish** button to complete the configuration operations.
5. To verify that the catalog has been successfully created, click on the **Machine Catalogs** link on the left-hand menu.
6. To check that all the required machines have been generated, right-click on the catalog name in the **Machine Catalogs** section and select the **View machines** option. You will get back the full list of generated desktop instances.

Search results for '(Machine Catalog Is "Desktop-C01")'			
Desktop OS Machines (1)		Server OS Machines (0)	Sessions (0)
Name	Machine Catalog	Delivery Group	
VDI-WIN-01.XDSEVEN.local	Desktop-C01	-	

Now we will perform the creation operations for Delivery Groups:

7. On the left-hand menu, click on the **Delivery Groups** link; then select the **Create Delivery Group** option on the right-hand side of the window.
8. On the **Getting Started** screen, click on the **Next** button to continue.
9. In the **Machines** section, select an existing catalog from the list and choose how many machines need to be added to Delivery Group from the available machine pool(s). After completing this, click on **Next**.

Machines

Select a Machine Catalog:

Catalog	Type	Machines
Desktop-C01	VDI MCS Static Discard	1
Desktop-C01		

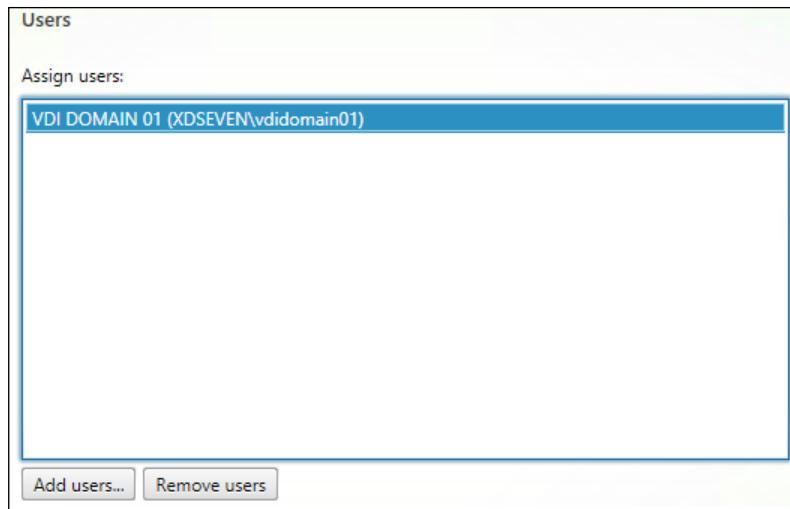
Choose number of machines to add: - +

10. In the **Delivery Type** section, select the purpose for the Delivery Group we're going to create (**Desktops** or **Applications**). In our case, select the **Desktops** option and click on **Next**.

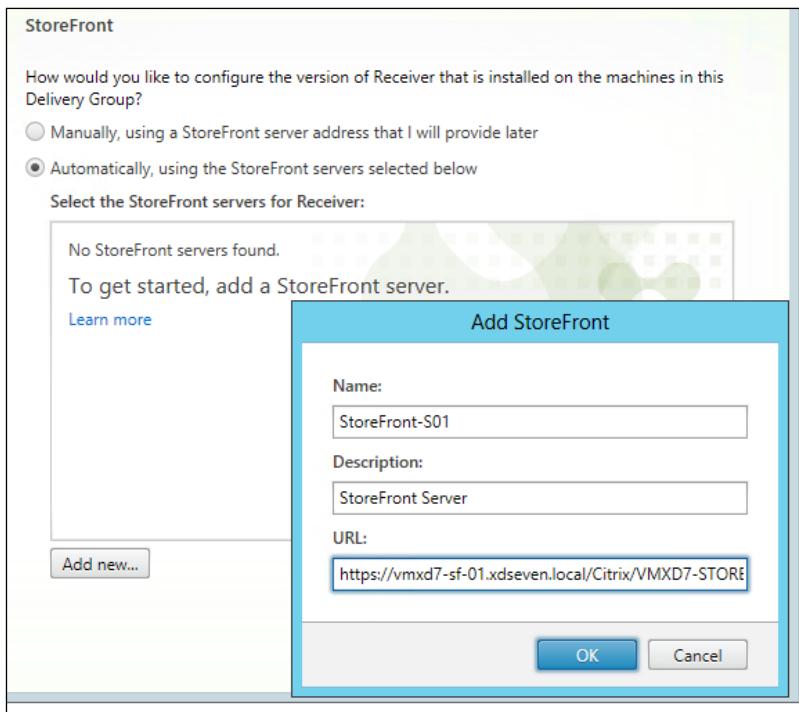


In the Chapter 7, *Deploying Applications*, we will discuss Applications Delivery Groups.

11. In the **Users** section, add one or more user(s) or groups to which to assign permissions on the delivered desktops. Click on the **Next** button to continue with the configuration steps.



12. On the **StoreFront** menu, click on the **Automatically, using the StoreFront servers selected below** radio button. Then click on the **Add new...** button and populate the pop-up screen with the required StoreFront server information. After this, click the **OK** button, and then click on **Next**.



13. On the **Summary** screen, select a name for the Delivery Group, a **Display Name** for the desktops, and an optional Delivery Group description. Click on the **Finish** button to complete the creation procedure.

The screenshot shows the 'Summary' step of a delivery group creation process. It displays the following configuration details:

Source Machine Catalog:	Desktop-C01
Machine type:	Windows Desktop OS
Allocation type:	Static
Number of machines added:	1 unassigned
Delivery type:	Desktops
Users:	VDI DOMAIN 01 (XDSEVEN\vdidomain01)
Storefronts:	1
Scopes:	-

Below the summary, there are fields for defining the delivery group:

- Delivery Group name:** Windows Desktop Delivery Group
- Display name:** Windows Machine
- Delivery Group description for users: (Optional)** Windows Desktop Delivery Group

At the bottom are three buttons: **Back**, **Finish** (highlighted in blue), and **Cancel**.



Be careful with the desktop assigned to every user. You must respect both the number of generated machines and the available licenses.

14. Click again on the **Delivery Groups** link on the left-hand menu. Now you can see the results of the last-performed operations with an information area about the utilization of the assigned desktops (on the **Details** tab).

The screenshot shows the Citrix Delivery Groups interface. At the top, there's a navigation bar with tabs for 'Delivery Groups' and 'Applications (0)'. Below this is a table with columns: 'Delivery Group', 'Machine type', 'No. of machines', and 'Sessions in use'. A single row is visible for a 'Windows Desktop Delivery Group' which is a 'Windows Desktop OS'. It shows 1 machine, 0 sessions in use, and status information: 'State: Enabled', 'Unregistered: 0', and 'Disconnected: 0'. Below the table, a section titled 'Details - Windows Desktop Delivery Group' is expanded. It contains four tabs: 'Details' (which is selected), 'Machine Catalogs', 'Usage', and 'Administrators'. Under the 'Details' tab, there's a 'Delivery Group' section with the following details:

Name:	Windows Desktop Delivery Group
Display Name:	Windows Machine
Description:	Windows Desktop Delivery Group
Type:	Static Desktops
Users:	VDI DOMAIN 01 (XDSEVEN\vdidomain01)
Scopes:	All
StoreFronts:	https://vmxd7-sf-01.xdseven.local/Citrix/VMXD7-STORE-01

15. Using a configured client device, open a Web browser and type the address of your StoreFront configured store. Log in with the credentials of one of the users with an assigned desktop. After the login phase, you will receive a screen with the desktop and the applications available for that user.



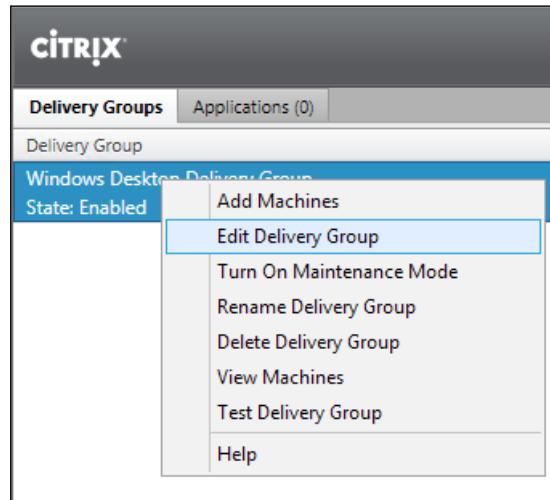
The Virtual Desktop icon shown in the previous image will be gray when waiting for an available resource.



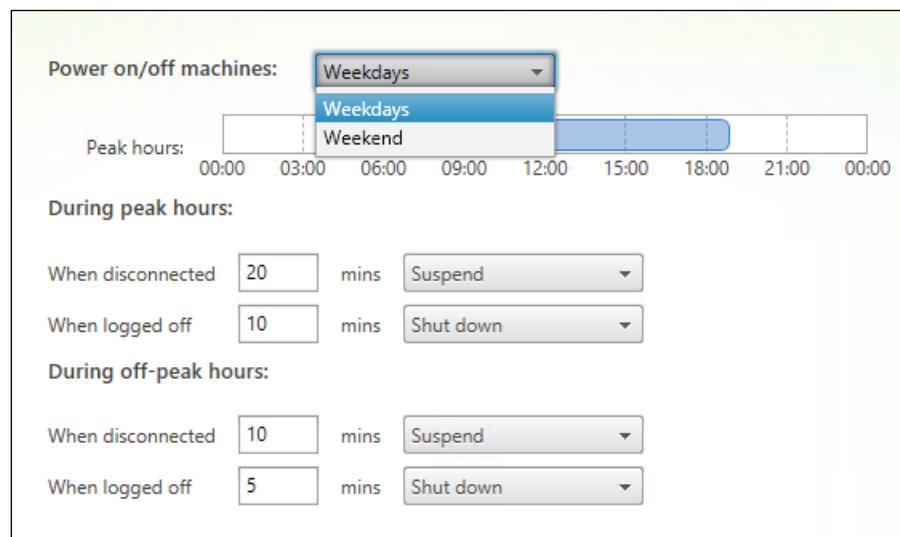
16. Click on the published resource or wait for some minutes in order to let Citrix connect to the Desktop. Once completed, the desktop instance is available to be used.

Now we will manage the power and access management:

17. Click on the **Delivery Groups** link located on the left-hand menu, right-click on the desired Delivery Group and select the **Edit Delivery Group** option.



18. Select the **Power management** section and choose from the **Power on/off machines** area the week period to configure (**Weekdays** or **Weekend**). Click on the **During peak hours** bar to set the time interval to consider as the highest working activities period (in the screenshot, it's configured from 9 a.m. to 6 p.m.). After configuring all the options, click on **OK**.





In the presence of more than five virtual machines, if you specify to start only one virtual desktop, the XenDesktop broker will automatically power up three virtual desktops in order to prevent the possibility of the user having to wait till a virtual desktop is powered up.

19. In the **During peak hours** zone, assign a time period in minutes for the two configured conditions (**When disconnected** and **When logged off**) and select the action to execute in case of condition verification (**Suspend** for disconnection; **Suspend** or **Shutdown** for logoff). Repeat the same steps for the **During off-peak hours** section.
20. Select the **Access policy** section and choose the desired option(s) in the **Allow the following connection area** (**All connection not through NetScaler Gateway** or **Connections through NetScaler Gateway**). If you want, you can configure personalized filters by flagging the third option, **Connections meeting any of the following filters**, and clicking on the **Add** button to insert the filter rule.
21. Click on the **End User Settings** link and configure the **Description**, **Color depth (16 or 256 colors, High, or True color)**, and **Time zone** setting for the Delivery Group of the clients. Then, if you want to use an encrypted connection between the client and the XenDesktop farm, flag the **Enable Secure ICA** option. After this, click on the **OK** button to register all the modifications.

End User Settings	
Description:	Windows Desktop Delivery Group
<input checked="" type="checkbox"/> Enabled	
Desktops per user:	1 <input type="button" value="-"/> <input type="button" value="+"/>
Color depth:	True Color
Time zone:	(UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
<input checked="" type="checkbox"/> Enable Secure ICA	

How it works...

The creation of the XenDesktop catalog is a fundamental operation in order to redistribute the desktop and application resources to end-user devices. The most important choice to make is what kind of machines the catalog creates, depending on specific company requirements.

In this latest release of XenDesktop, the first choice to make is about the kind of desktop you want to deploy to the end user. Starting with the fact that the XenApp platform has been integrated in this release, you have the ability to deploy both Server OS and Desktop OS instances, applying your choice for existing physical or virtual machines. Another important feature for this software version is given by Remote PC Access. This substantially permits users to link their clients to existing physical or virtual PCs in order to use them as their default client(s). This solution could prevent system administrators and end users from migrating contents and applications to a VDI architecture, centrally managing the company workstation through Citrix Studio.

Desktops can be deployed in one of the following ways:

- ▶ **Random:** This choice is equal to what was called **Pooled catalog** in previous versions. This means that every time a user logs on, a new desktop can be released, basing the assignment only on the logon priority.
- ▶ **Static:** By selecting this option, the same desktop will be assigned to the same user at every logon phase. With this option, you have got the ability to select three more options: saving the changes written to the user data area on a separate disk—the Personal vDisk (non-persistent machines), creating a dedicated machine (persistent mode), or discarding all the changes made to the desktop, including the user data area, when users log off (non-persistent mode).

Non-persistent machines let you consume less storage space, based on the fact that a single virtual machine is used, and starting from it, all the other instances are generated as linked clones, snapshots of the original disk. This configuration applies to the MCS infrastructure. In this case, you have to take care about the way to save the user data. Centralized profiles, such as Microsoft Roaming Profile or Citrix Profile Management, or the use of the Personal vDisk technology permit you to avoid loss of data; without these choices, all changes will be lost.

The Personal vDisk is a virtual disk created on the Hypervisor's data store. This file size will be equal to the **quota** assigned in the user disk creation procedure, but it will be generated as a **thin** virtual disk. In this case, the virtual disk file size will increase only when the space is actually used by a user and will only increase up to the predefined maximum size.

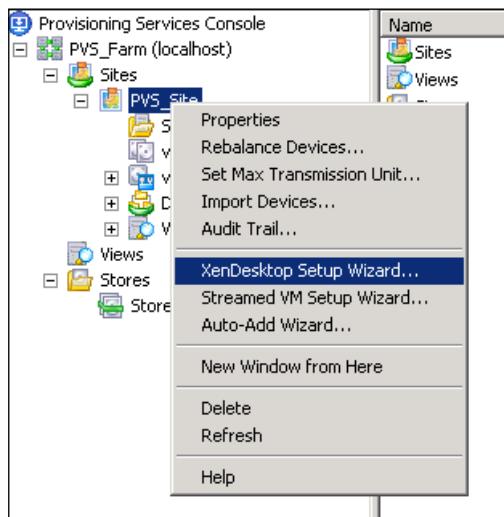
Persistent machines, on the other hand, give you the assurance that user data won't be lost at the expense of higher consumption of storage space.



This catalog type, based on the MCS architecture, has the limitation to use only one NIC for the virtual desktops. To be able to use more network cards, you have to refer to the Streamed catalogs (PVS architecture).

Moreover, we can also generate a catalog of existing virtual or physical machines by the use of Delivery Controller. This will make it possible to import already-generated workstations, assigning them to the domain users. This method of operation is quite different from the general purpose of a VDI infrastructure. You could use this to manage existing company resources under the central XenDesktop management console, but this is not the standard VDI pooling approach.

The last available catalog is the PVS catalog. In this case, the Delivery Controller will create machines starting from an existing desktop—physical or virtual—generated under the Citrix Provisioning Services machine, as explained in the first chapter. For this kind of deployment, you have to connect to the PVS server created in *Chapter 1, XenDesktop 7 – Upgrading, Installing, and Configuring*, right-click on the configured site, and select the **XenDesktop Setup Wizard** option from the menu.



 Be sure you have configured at least one of your PVS-configured vDisks in Standard Image access mode; otherwise, you will not be able to deploy a XenDesktop Streamed catalog.

You can also create a streamed catalog from the Citrix Studio wizard (by typing the PVS server address and specifying the Windows domain on which to operate and the type of the existing target device (virtual or physical). This method should be used only to synchronize the Desktop Studio with an existing streamed catalog created under the PVS server

For all the supported catalogs, except the existing and physical types, you have to specify the way in which to create computer accounts under your Active Directory domain. In this last scenario, you can reuse existing domain accounts or generate them from scratch, choosing the right naming convention for your company.



Be sure to create the computer and user accounts within an OU included in the Citrix Policies application discussed earlier in this book.



An important component contained by the catalog is the Delivery Group. This object allows you to allocate all or part of the available machines in the catalog to the domain users. You can create more than one Delivery Group; the only required parameter is that you have available machine instances to populate the group.

There's more...

In the **Machine Creation** section previously explained, we've seen how to create desktop instances and how to configure all the related parameters. For some of these desktop pools, however, some more options have to be discussed.

When selecting the static desktop assignment with the separate Personal vDisk option, we need to specify, in the **Number of virtual machines needed** section, values for **Specify the size and location of the Personal vDisk**.

A screenshot of a Windows-style dialog box titled "Specify the size and location of the Personal vDisk:". It contains two input fields: "Personal vDisk size (GB)" with a value of "10" and a plus/minus button, and "Personal vDisk drive letter:" with a dropdown menu showing "P:".

We have explained what the personal vDisk is and how it works in the *Chapter 4, User Experience – Planning and Configuring*.



If you have decided to deploy streamed machines in a PVS configuration, you need to configure this from the **Provisioning Service** console, specifying as **Machine Type** the **Streamed with personal vDisk** option, assigning a name and a description to the catalog, selecting a domain administrative account, and then choosing the vDisk parameters shown in the following screenshot:

A screenshot of a Windows-style configuration dialog box. It shows the following settings:

Number of virtual machines to create:	1
vCPUs:	1
Memory:	1024 MB
Local write cache disk:	4096 MB
Personal vDisk size:	10 GB
Personal vDisk drive letter:	P:

See also

- ▶ The *Configuring XenDesktop® policies* recipe in Chapter 8, *XenDesktop® Tuning and Security*

Modifying an existing machine catalog

Now that we've deployed and configured the machine catalog, we are able to use and work on the Citrix Desktop infrastructure. In some cases, it could be necessary to modify the configurations, for instance when it's necessary to add a new desktop to the catalog because of a new colleague in the company. In this recipe, we will explain how to modify the machines, their assignments, and the configured catalogs.

Getting ready

All the operations performed in this section are on already-existing objects; so, all you need is to have administrative credentials at two different levels. You have to be administrator of the involved virtual machine's templates and administrator of your XenDesktop architecture to be able to modify the Director configurations.

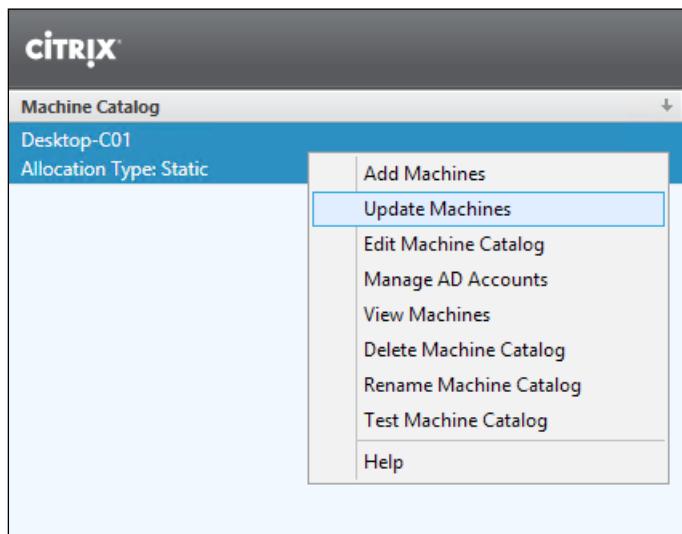
How to do it...

Let's start by updating the existing virtual desktop machines.

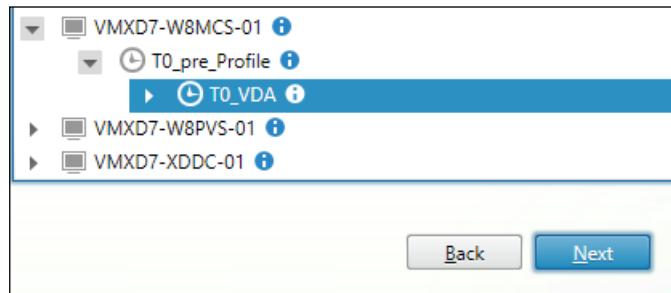
Updating virtual desktop machines

1. Log on to the Windows desktop template, apply all the system and configuration changes you need, and then log off.
2. Connect to your hypervisor machine(s) or management console with administrative credentials on the specific machine and generate a new snapshot for the virtual machine disk in order to register the applied modifications.

3. Connect to the Delivery Controller server, click on the **Machine Catalog** link in the left-hand menu, right-click on the desired Desktop Catalog, and select the **Update Machines** option.



4. Select the Delivery Group you want to update in the **Overview** section, and then click on the **Next** button.
5. Select your master image and the last created virtual machine snapshot and then click on **Next**.



6. In the **Rollout Strategy** section, select a way to restart the desktops included in the update operations, deciding whether to update the images on the next reboot or to restart them immediately, whether or not to notify the users about this operation, and whether to restart all the machines at once or delay the operations within a specified time period. After selecting this, click on the **Next** button.

Rollout Strategy

When do you want to update this image?

On the next restart (not right now)
 Notify users of the update
 Immediately (restart the machine now)

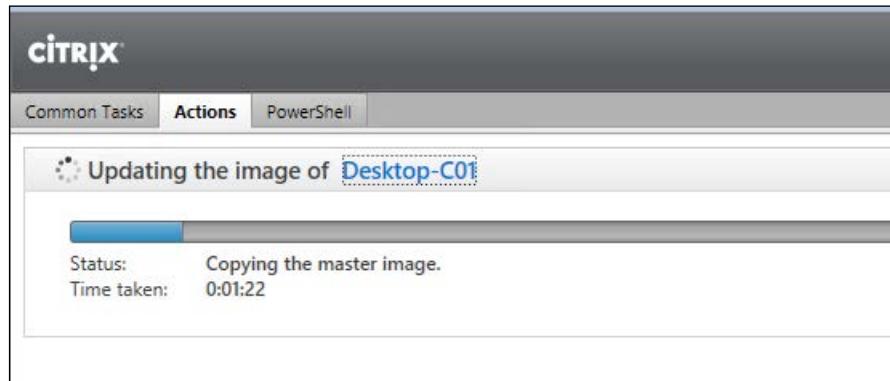
Distribution time:

Restart all machines at once ▾
Notify users of the update:
1 minute before user is logged... ▾

Message:

The desktop will be updated asap.

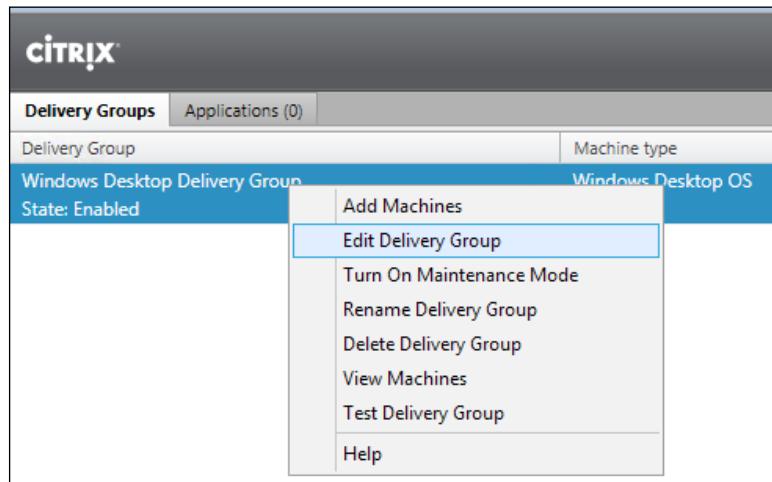
7. After reviewing the information in the **Summary** section, click on **Finish** to complete the machine update.
8. Click on the Citrix Studio link on the left-hand menu, and in the main panel, select the **Actions** tab. Here, you can verify the status of the updating task.



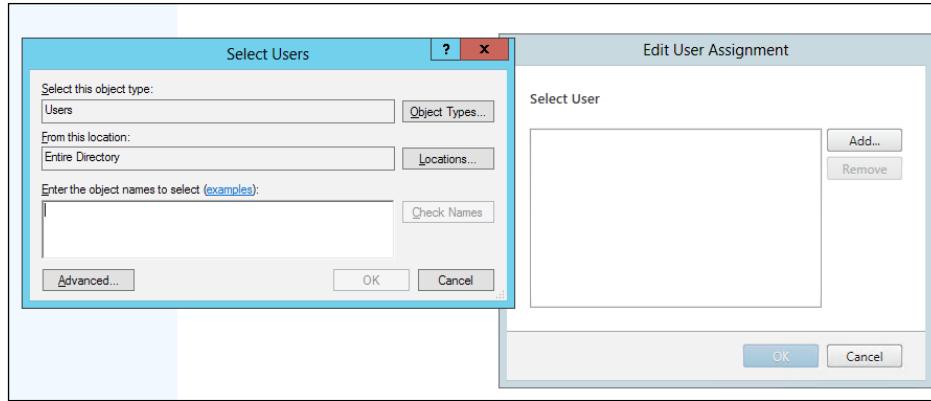
9. After all the operations have been completed, connect to a desktop instance through the StoreFront store and verify that all the updates are available.

Now we will see how to modify the machine assignment:

1. On the left-hand menu, select the **Delivery Groups** link; then, right-click on the group that you want to modify and run the **Edit Delivery Group** option.



2. Select the **Machine Allocation** section, and then click on the button in the **Users** field to browse for a configured domain user to which to assign the virtual desktop instance.
3. To add more users to the Desktop Group, in order to let them use any available desktop instance in the pool, click on the **Users** area of the **Edit Delivery Group** option and browse for the desired domain users to add to the group. After completing all the configurations, click the **OK** button.
4. You can also configure the machine assignment in another way. In the left-hand menu, select the **Delivery Groups** link and then right-click on the desired machine catalog and select the **View Machines** option.
5. On the newly opened screen, right-click on the virtual machine instance you want to modify and select the **Change user** option. Now, you can remove the configured user and add the new virtual machine owner.



The following steps help add new machines to an existing catalog:

1. On the left-hand side menu, select the **Machine Catalogs** link, right-click on the desired catalog and click on **Add machines**.
2. In the **Virtual Machines** section, select the number of instances you want to add to this catalog and then click on **Next**.
3. In the **Computer accounts** section, select **Create new Active Directory accounts** or **Use Existing Active Directory accounts**. Once done, click on the **Next** button.
4. If you've chosen to use existing accounts, you should consider maintaining the same naming convention used for the other desktop instances in the catalog, and you should also choose between resetting all account passwords and using the same password for all the accounts. After you complete this, click on **Next**.

Active Directory Computer Accounts

Each machine in a Machine Catalog needs a corresponding Active Directory computer account.
[Learn more](#)

Select an Active Directory account option:

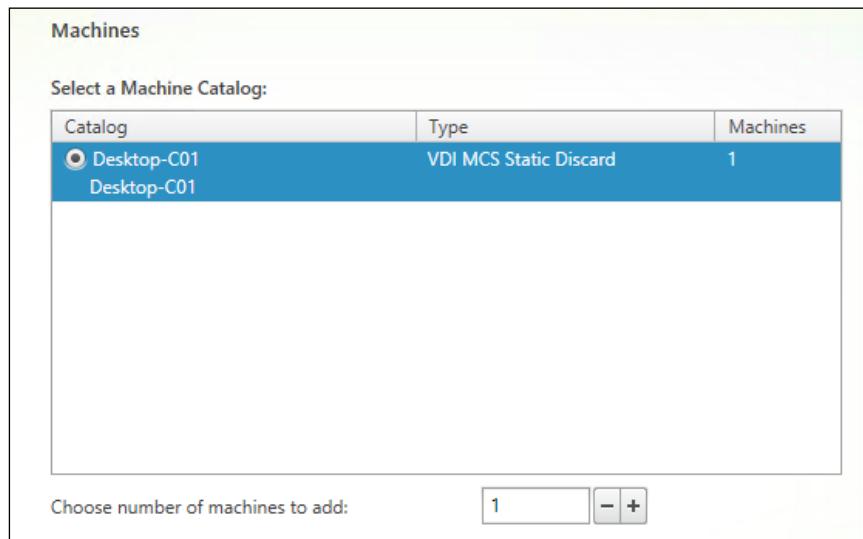
Create new Active Directory accounts
 Use existing Active Directory accounts

Required: 1 Added: 0

Computer account password management

Reset all account passwords
 All accounts have the same password

5. On the **Summary** screen, click on the **Finish** button to complete the procedure.
6. After the task has been completed, click on the **Delivery Groups** link on the left-hand side, right-click on the Desktop Group that you want to modify, and select the **Add Machines** option.
7. Highlight the catalog and insert the number of machines you want to add. This number must be equal to or less than the number of machines listed in the **Machines** column. After this click on **Next**.

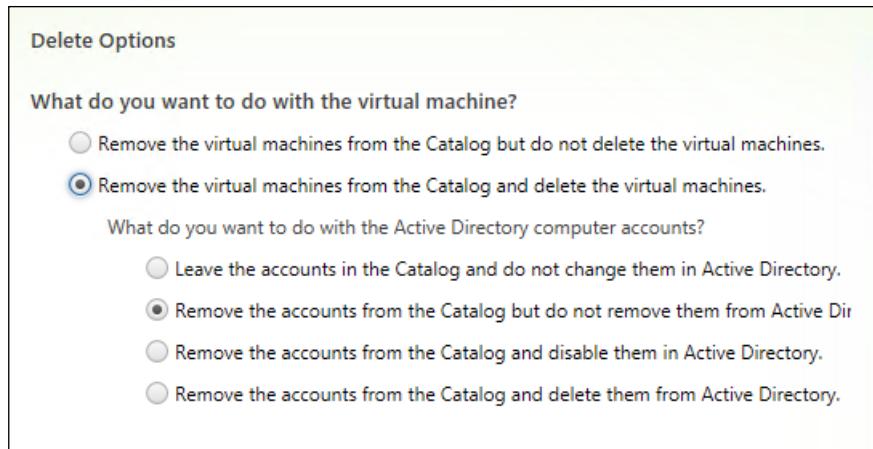


8. If all the information on the **Summary** screen appears to be correct, click on **Finish** to complete the process.

Now we will see how to remove assigned machines from an existing catalog:

1. Click on the **Machine Catalogs** link on the left-hand menu, right-click on the desired catalog, and select the **View Machines** voice.
2. In the machine list, select the machine that you want to remove from the Desktop Group in the catalog, right-click on it, and select **Turn On Maintenance Mode**. Click on the **Yes** button to confirm the operation.
3. After the operation has been completed (you can verify this by checking for the presence of the **Enabled** value in the **Maintenance Mode** column), right-click on the desktop instance again, and select the **Remove from Delivery Group** option. Click on **Yes** to confirm the operation.
4. After that, you will find no more information about Desktop Group assignment for the desktop machine. To completely remove the desktop, click on the **Machine Catalogs** link in the left-hand side menu, right-click on the involved catalog, and click on the **View Machines** link.

5. Select the desktop you'd previously removed from the Delivery Group, right-click on it, and click on the **Delete** option.
6. In the **Deletion Options** section, select which kind of operation we need to perform. If you decide to delete the virtual machine (which will perform an instance deletion at the Hypervisor level), you have to choose whether to re-use the virtual machine instance or remove the machine from XenDesktop and leave, disable, or delete in Active Directory. After that, click on the **Next** button.



7. If all the information in the **Summary** screen is correct click on **Finish** to complete the task.

[ To be sure to be able to complete this procedure, force shutdown of the desired virtual desktop instances before proceeding.]

Now we will perform the deletion of a configured XenDesktop catalog:

1. Click on the **Machine Catalogs** link in the left-hand menu, right-click on the right catalog, and select the **View Machines** option.
2. Put every desktop instance in the Desktop Group in **Maintenance Mode**, and then repeat the deletion procedures as seen earlier.
3. After completing all the removal activities, return to the **Machine Catalogs** section, right-click on the catalog, and select the **Delete Machine Catalog** option.
4. In the **Summary** section of the opened window, click on the **Finish** button to complete the deletion procedure.

How it works...

The XenDesktop machine catalog is a modifiable entity, which allows you to update or rollback the configurations previously implemented.

In the presence of the MCS architecture, the machine update is perhaps the most used and important modification task. This task is usually executed when modifications are made to the desktop base image template, for instance, software changes that must be applied to all the created desktop instances as well.

The following is a set of steps and considerations for this procedure:

- ▶ After all the required updates to the machine template have been completed, you have to regenerate a virtual machine snapshot under your hypervisor platform.
- ▶ After completing the previous step, update content for the desktop instances through the Citrix Studio console, starting with this last-created snapshot.
- ▶ An important option about that it takes care is the Rollout strategy. With this option, you can choose the right way to interact with users in order to complete the regeneration steps.
- ▶ A desktop instance restart is required in order to apply the changes. You can choose between sending a message to the connected users about the required restart, restarting the desktops immediately, and restarting after a configured delay time.
- ▶ The rollout process can be really short for PVS configurations. For MCS architectures, with 50 or more machines, the process can be very long, with a huge impact on the I/O storage performance.



In order to avoid problems when stopping the desktops during working hours, it is better to update the machines during the non-peak working hours and immediately restart the desktops.

You can also add or remove machines from the catalog. These are quite simple operations that contain all the powerful maintenance tasks of a VDI architecture. In fact, you can add instances by simply selecting the number of desired desktops. The greater part of this activity has already been performed during the creation and configuration of the desktop base image template. In the same way, you can remove single desktop instances from the catalog by right-clicking on them and selecting the appropriate deletion option. In this case, you can choose to completely delete a computer account (from both the XenDesktop architecture and Active Directory) or simply remove its assignment and preserve the desktop instance to be reused by another user.

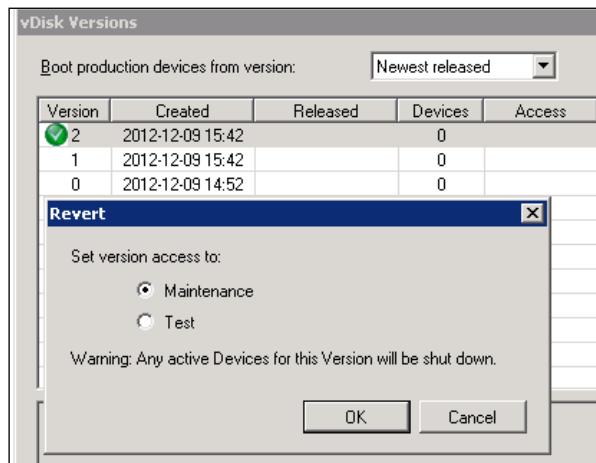
There's more...

If your users experience problems after updating the desktop image, the Citrix Studio allows you to roll back to a previous consistent machine state.

In the **Machine Catalogs** section already used during this chapter, you can repeat the procedure used to generate the desktop instances by selecting a snapshot generated earlier than the current machine state. This procedure is different from the rollback task used in XenDesktop Version 5.6. Instead of having a rollback point managed by Citrix Studio, you have now to maintain the snapshots at the hypervisor level.

Also, in this case, you need to select a Rollout strategy when stopping the desktop instances to complete the rollback activities. As previously described, you should plan a rollback strategy with a really low impact on user operation during working hours.

For the Provisioning services infrastructure, a rollback activity is managed in quite a different way. The vDisks are based on versions and category. Every virtual disk has a version number assigned and a category assigned to it (**Access version: Maintenance, Test, and Production**). In case of failure after a disk update, you have the ability to revert a disk from Production to Test or Maintenance. In this way, the previously generated disk version will become the Production disk, permitting virtual machines to boot from it after they have been rebooted. This method permits you to easily manage multiple disk versions within your XenDesktop environment.



See also

- ▶ The *Managing the Citrix® Desktop Controller and its resources – Broker and AppV cmdlets* recipe in Chapter 9, *Working with XenDesktop® PowerShell*

Using the new Citrix® Director platform

In the presence of huge VDI architectures, it could be hard to find standard and advanced information about the generated desktop instances, the configured users, and the relations that may occur between these two objects. Citrix Director is a useful web console that helps system administrators to easily find information about the status and the operation of desktop infrastructure. In this latest version, we will also discuss the integrated **Citrix EdgeSight** features.

Getting ready

To use Desktop Director, you need an already installed and configured Citrix XenDesktop 7 architecture because of its necessity to interface with your Active Directory domain. You also need to configure and use a username that is able to read your AD structure.

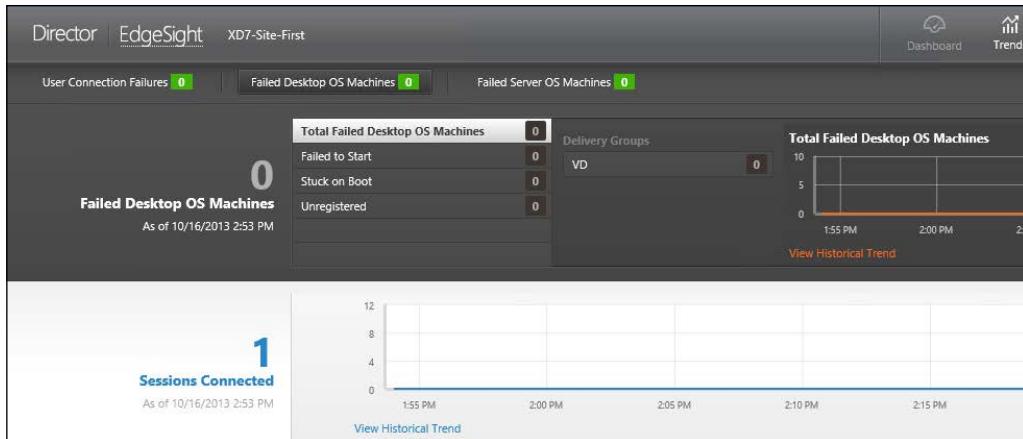
How to do it...

In this section, we will explain the Citrix Director platform and the way to use it:

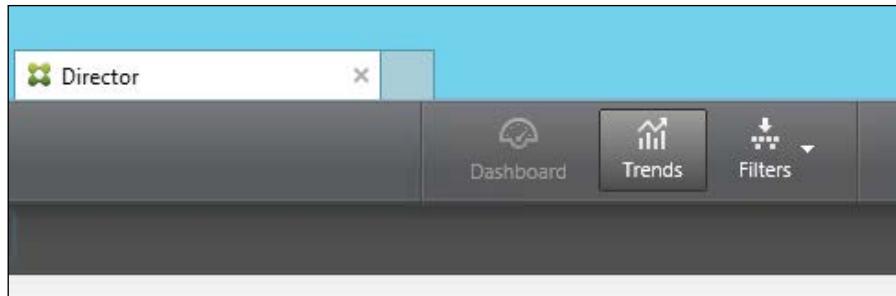
1. Connect to the Delivery Controller machine, hit the Windows + C key combination, and search for the Citrix Director icon in the Citrix software section. Click on the icon to run the software.
2. On the login screen, insert a valid username and password, specifying the domain on which XenDesktop is operating, and click on the **Log on** button.



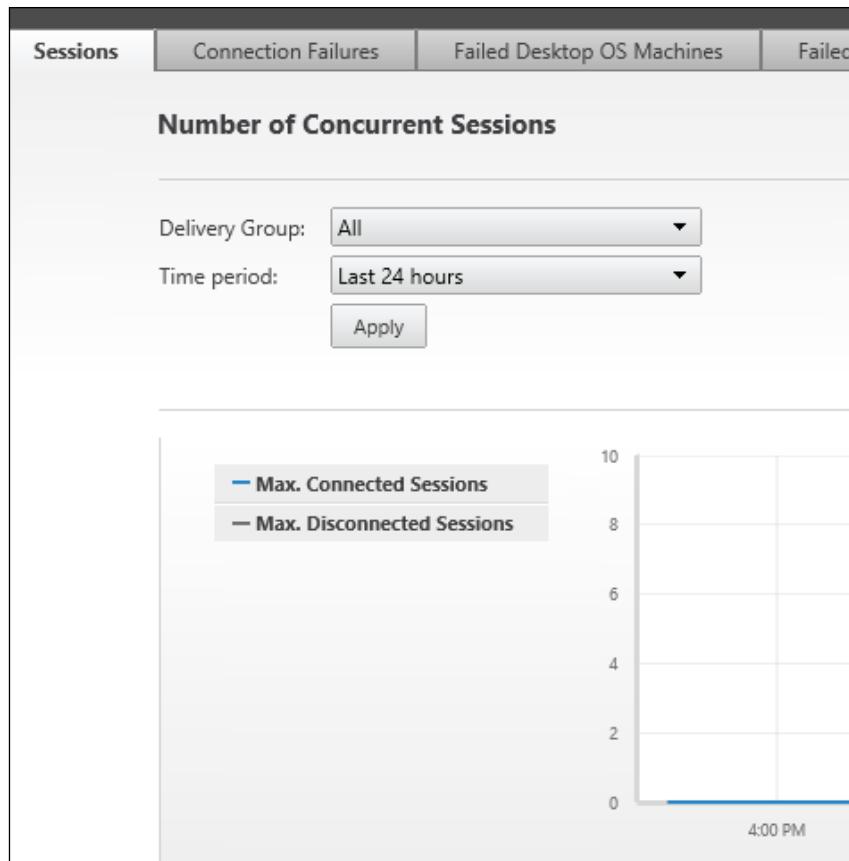
3. After you have logged in, you will be introduced to a dashboard, on which you can analyze and verify data about the current connected sessions, the average of the logon duration phase, and generic data about the failed desktop or server OS.



4. Click on the **Trends** icon on the top of the screen in order to analyze the data collected by the counters in the **Director** section.

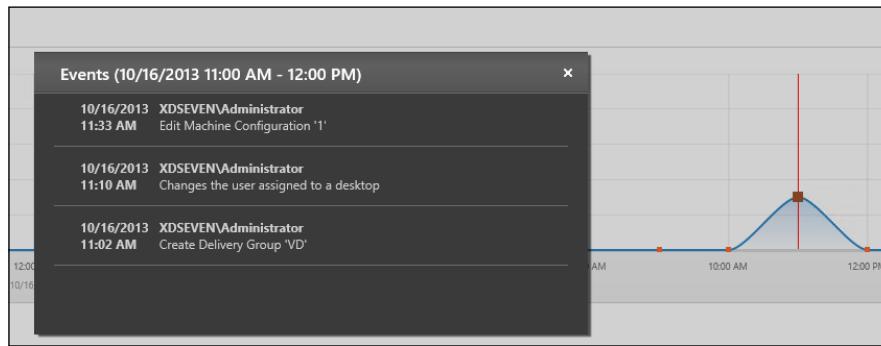


5. On the first tab **Sessions**, you will find information about the concurrent sessions, which can be obtained for a specified time period (**Last 24 hours**, **Last 7 days**, **Last month**, **Last year**, or **Custom period**).

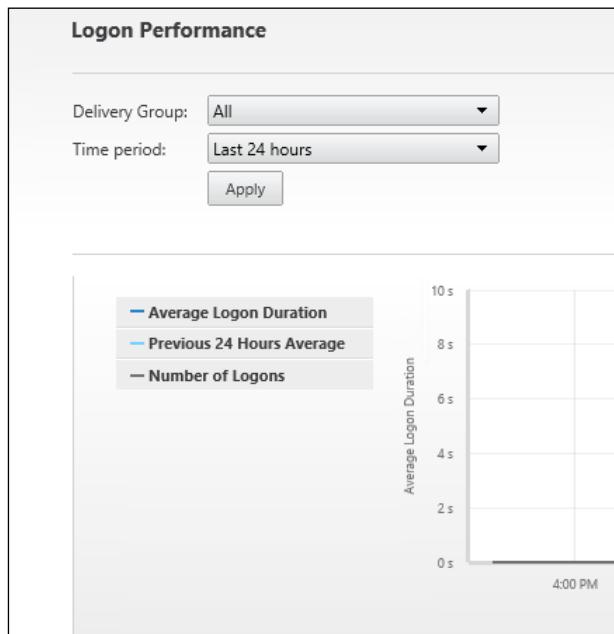


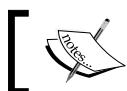
You can also filter the session data per Delivery Group.

- In the **Connection Failures** tab, the Director collects data about these problems during resource usage: **Client Connection Failures, Configuration Errors, Machine Failures, Unavailable Capacity, and Unavailable Licenses**. By clicking on the graphics in this section, it is also possible to obtain the details about the problems detected by the Director.



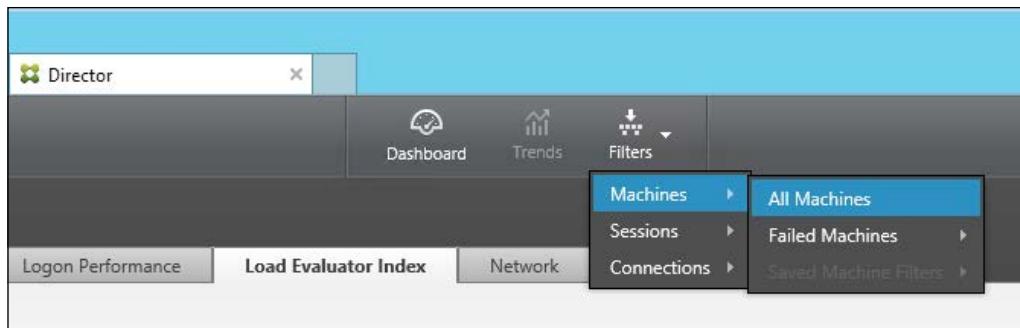
- The same analysis can be performed by clicking on one of the other existing tabs: **Failed Desktop OS Machines** and **Failed Server OS Machines**. Also, in this case, the graph can give administrators or help desk technicians more details about the encountered problems.
- The **Logon Performance** tab permits analysis of the time required by the user logon phase. Even in this case, you can filter the data for the desired time period.





This section is really useful when it comes to finding and understanding the bottlenecks during user attempts to log on to their virtual desktops.

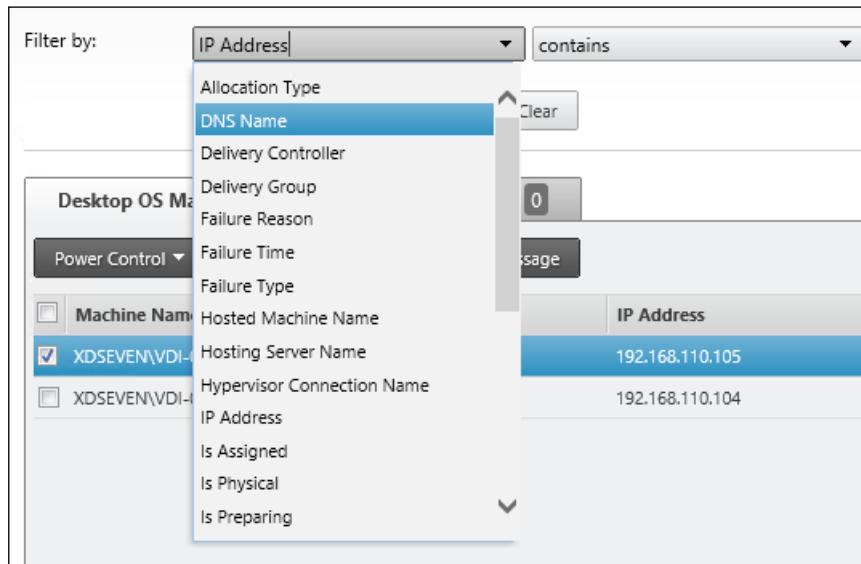
9. In the **Load Evaluator Index** and **Network** tabs, you can collect useful information about the load average for resource usage (such as **CPU**, **Memory**, or **Disk**) or retrieve information about the global usage of the network resources, respectively.
10. Click on the **Filters** icon above the **Director** menu and then navigate to **Machines | All Machines**.



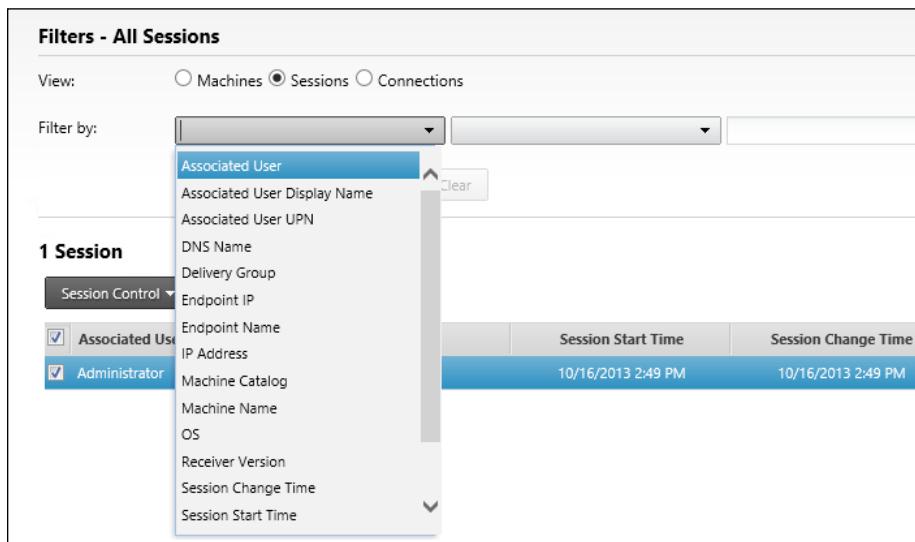
11. In the **View** section, click on the **Machines** radio button, and then click on one of the desired tabs (**Desktop OS Machines** or **Server OS Machines**) and select one or more desktops you want to manage. After that, you can use the **Power Control** button (power management of the virtual desktop), the **Maintenance Mode** button (turning on or off the mode for the desired machine), and also sending a message to the user that is currently using the desktop.

Machine Name	Is Assigned	IP Address	Delivery Group
XDSEVEN\VDI-01	Yes	192.168.110.105	VD
XDSEVEN\VDI-02	Yes	192.168.110.104	VD

12. In presence of an elevated number of machines within your infrastructure, you can filter the information based on the **Filter by** section, filtering data for **DNS Name**, **Delivery Group**, **IP Address**, **OS version**, and so on.



13. In the **View** section, click on the **Sessions** radio button, flag one of the active user sessions, and choose whether to disconnect or log the user off (the **Session Control** button) or whether to send them a message on a specific resource. Also, in this case, you can filter the results based on predefined filtering categories.





An alternative to **Sessions** is the **Connections** radio button. In this category, you can manage the connection status plus the active sessions.

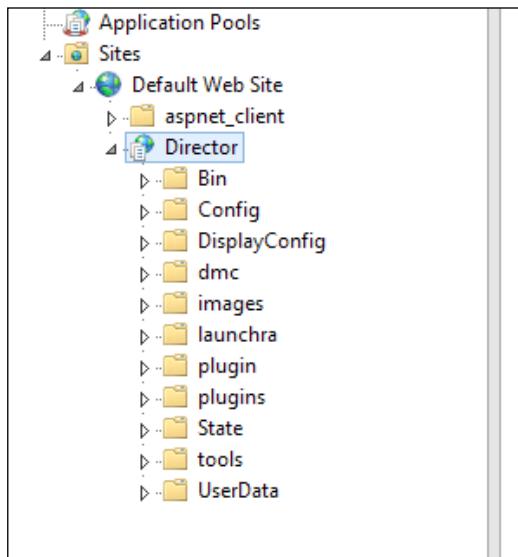


How it works...

Citrix Director is a web application that allows system administrators to verify and analyze the status of their Citrix infrastructure, checking the utilization statistics for the entire XenDesktop infrastructure. Despite its previous versions, in this latest release, an important Citrix component has been integrated. This is Citrix EdgeSight, and thanks to its presence, better-collected data can be used by IT professionals to troubleshoot infrastructural problems.

The main changes users will notice are in the system dashboard. Here it is possible to verify the status of the infrastructure and the delivery controller and monitor in real time the number of concurrent connections, the time needed by the end users to log on to their resources, and moreover, the information about the Desktop or Server OS faults. This last feature gives the ability to understand more quickly the existing problems of a VDI architecture.

The Citrix Director portal is composed of a website configured under the IIS web server installed on the Windows machine that hosts the Citrix Director installation.



Going deeper into the details, you can obtain a lot of information about the configured desktop instances. Use the filters to find the specific resources on which they are operating, and apply on the results the information fields you want to get back. Some of these are about the **Machine** identification data (**Name**, **Desktop Group**, **Machine Type**, and **OS**), the **Power State** for the machines, or the **Connection** status (**Last connection** and **Endpoint** from which the connection has been established).

The most interesting part is composed of the set of active operation that you can execute on desktop machines. It's possible, in fact, to manage the power state of the machines; for instance, you have the ability to restart or power on a desktop when necessary. Moreover, you can change the desktop assignment, moving an instance among your domain users, because of the ability of the Desktop Director to interface with the Active Directory structure. This enables you to manage and retrieve information about the domain users.



To manage the power state of the virtual machines created under a VMware hypervisor, you need to install the VMware tools on the guest machine.



All the collected metrics are exportable from the Desktop Director in a report, in the form of an XML file.

The integration of the Citrix EdgeSight platform with the entire set of collected data has given more detailed information. This is the key that will help IT professionals to reduce the time to intercept problems with the help of Citrix Director.

There's more...

The Citrix Director platform can be managed by different users with different levels of permissions.

The roles and the scopes to manage the troubleshooting web platform can be configured in the Citrix Studio by navigating to the **Administrators** | **Configuration** section in the menu on the left.

Creating and Configuring a Desktop Environment

By clicking on the **Create Administrator** link, you can select a domain user to whom we can assign permissions to the XenDesktop site objects. This is formerly known as **Role**.

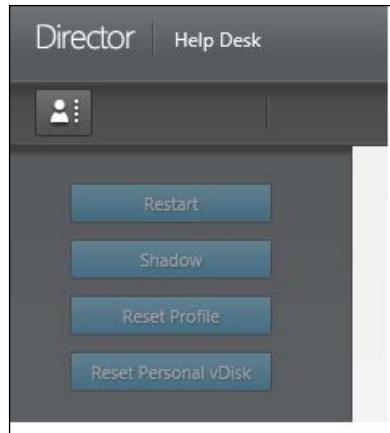
The screenshot shows the XenDesktop Studio interface. On the left, there's a navigation pane with 'Administrator and Scope' selected under 'Studio'. In the main area, there are two tabs: 'Administrator and Scope' and 'Role'. Under 'Administrator and Scope', a sub-menu shows 'Scope name' with 'All' and 'All objects' selected. Under 'Role', a sub-menu shows a list of built-in roles:

Name	Type
Delivery Group Administrator	Built In
Full Administrator	Built In
Help Desk Administrator	Built In
Host Administrator	Built In
Machine Catalog Administrator	Built In
Read Only Administrator	Built In

For instance, assigning a user the **Help Desk Administrator** permissions will enable her/him to manage the user sessions, applying remediation tasks by connecting to the desktop user through session shadowing or resetting the assigned personal vDisk.



Shadowing is the ability to remotely control the desktop of a user in order to offer remote assistance to troubleshoot issues.



These configurations are powerful solutions to use to delegate non-critical activities to existing company departments (help desk, customer care, monitoring area, or less privileged administrators).

See also

- ▶ The *Configuring the XenDesktop® logging* recipe in Chapter 8, *XenDesktop® Tuning and Security*

Configuring printers

To give users the feel of working on a virtual system as near as possible to a standard physical workstation, you have to furnish all the peripherals available in a non-VDI architecture. One of these is given by the configuration and use of printers. In this recipe, we're going to discuss these kinds of policies.

Getting ready

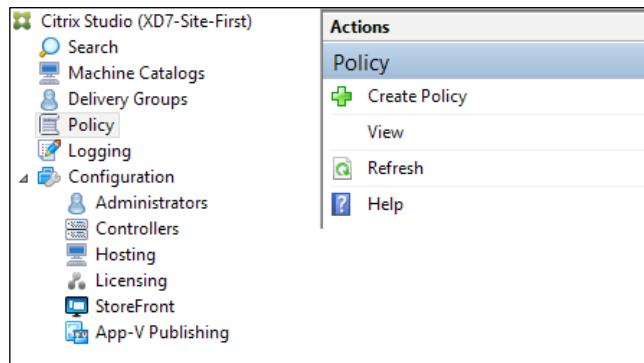
Depending on your company's requirements, you should have a lot of different network printers to configure within the virtual desktop environment. In this case, a prerequisite (and also a best practice) is configuring a **Print Server** on which we install all the devices and then deploy them through the use of Microsoft domain GPO.

You can install the required drivers for the printer that will be used on the master image; as you've already seen, in this way, you will propagate printer mapping to all the desktop instances in the pool.

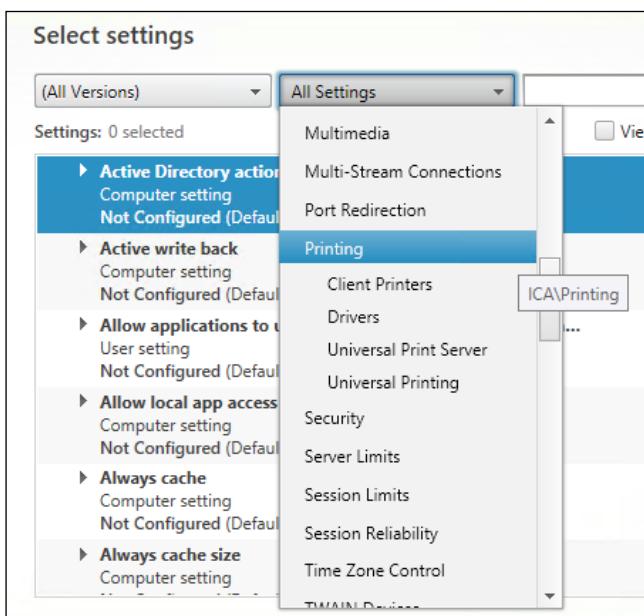
How to do it...

In this section, we will perform the configuration of the printers within the XenDesktop 7 environment:

1. Connect to the Citrix Controller machine and press the Windows + C key combination. Search for the Citrix Studio icon in the Citrix software section and click on it.
2. On the left-hand menu click on the **Policy** link, and then select the **Create Policy** option on the right-hand menu.



3. On the **Select settings** screen, choose the **Printing (ICA)** option in the second dropdown list.



4. Configure the following filtered policies:

- Auto-create client printers**
- Auto-create generic universal printer**
- Automatic installation of in-box printer drivers**
- Client printer names**
- Client printer redirection**
- Default printer**
- Direct connections to print servers**
- Printer assignments**
- Printer auto-creation event log preference**
- Printer driver mapping and compatibility**
- Printer properties retention**
- Retained and restored client printers**
- Session printers**
- Universal driver preference**
- Universal print driver usage**
- Universal Print Server enable**
- Universal Print Server print data stream (CGP) port**
- Universal Print Server print stream input bandwidth limit**
- Universal Print Server web service (HTTP / SOAP) port**
- Universal printing EMF processing mode**
- Universal printing image compression limit**
- Universal printing optimization defaults**
- Universal printing preview preference**
- Universal printing print quality limit**

□ **Wait for printers to be created (desktop)**

Select settings

(All Versions) ▾ Printing ▾ View selected only

Settings: 0 selected

- ▶ Auto-create client printers Select
User setting
Not Configured (Default: Auto-create all client printers)
- ▶ Auto-create generic universal printer Select
User setting
Not Configured (Default: Disabled)
- ▼ Automatic installation of in-box printer drivers Select
User setting
Not Configured (Default: Enabled)
Enables or disables the automatic installation of printer drivers from the Windows in-box driver set or from driver packages which have been staged onto the host using "pnputil.exe /a". By default, these drivers are installed as needed.
- ▶ Client printer names Select
User setting
Not Configured (Default: Standard printer names)
- ▶ Client printer redirection Select
User setting



By default, all the policies are in the **Not Configured** state.

5. After configuring the desired policies, click on the **Next** button to continue.
6. In the **User and Machines** section, you can apply the configured printing rules for a specific set of filtered objects, such as specific IP addresses or Delivery Groups, or use the policies for the entire configured XenDesktop site. After that, click on **Next**.

Assign policy to user and machine objects

Assign to selected user and machine objects Assign to all objects in a site

User and machine objects: 0 selected View selected only

- ▶ **Access control**
Applies to user settings only [Assign](#)
- ▶ **Citrix CloudBridge**
Applies to user settings only [Assign](#)
- ▼ **Client IP address**
Applies to user settings only
Apply policy based on the IP address of the user device used to connect to the session. [Assign](#)
- ▶ **Client name**
Applies to user settings only [Assign](#)
- ▼ **Delivery Group**
Applies to all settings
Apply policy based on the delivery group membership of the desktop running the session. [Assign](#)

7. On the **Summary** screen, assign a name to the generated policy, flag the **Enable policy** option, and click on **Finish**.

Summary

View a summary of the settings you configured and provide a name for your new policy.

Policy name:	<input type="text" value="Policy - Printers"/>	<input checked="" type="checkbox"/> Enable policy
Description:	<input type="text" value="Policy - Printers configuration"/>	



Later in this book, we will discuss in more depth the configuration of the XenDesktop 7 policies.

How it works

The printer configuration process is quite a complex activity that requires you to deeply understand and study the specific needs of the users in your company.

The following are the explanation of the main configuration policies:

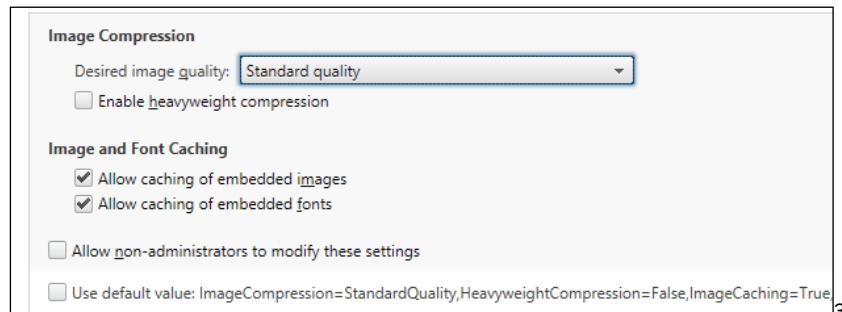
- ▶ **Auto-create client printers:** **Auto-create all client printers**, **Auto-create local (non-network) client printers only**, **Auto-create the client's default printer only**, and **Do not auto-create client printers**: With this policy you decide whether to autocreate all the listed categories by default, or one of them, including locally attached printers. You can also configure not to automatically create the printers.
- ▶ **Auto-create generic universal printer:** **Enabled** or **Disabled**: With this policy you can decide whether or not to use the Citrix Universal Printer object. As explained earlier, this could be a useful option when trying to avoid printer and driver fragmentation because of the use of a single generic printing driver.
- ▶ **Automatic installation of in-box printer drivers:** **Enabled** or **Disabled**: With this policy you can decide whether or not to enable automatic installation of the in-box Windows printer drivers. The in-box drivers are those included in the operating system's distribution, tested, and optimized for better performance within that environment.
- ▶ **Client printer names:** **Standard printer names** or **Legacy printer names**: This policy allows you to choose the naming convention to use during generic printer creation. You should always use the standard naming convention, and only use the other option when compatibility with older Citrix versions is required.
- ▶ **Client printer redirection:** **Allowed** or **Prohibited**: Allowed by default, this policy permits you to redirect to a server the client printer mapping.
- ▶ **Default printer:** **Set default printer to the client's main printer** or **Do not adjust the user's default printer**: With this policy you can configure how the default user printer is chosen. The first option uses the current configured printer as default device, the second instead load the printer from the user profile, based on the domain policies and the loaded printer driver. This technique is usually used for the **Proximity Printing** approach, the technique of publishing the closer network printer to a user.
- ▶ **Direct connections to print servers:** **Enabled** or **Disabled**: With this configuration you can permit the users to directly access the network printer, for faster printing. This is only available in LAN connections. In case of WAN printer mappings, you have to use a non-direct connection.

- ▶ **Printer assignments:** This policy allows you to specify a list of client and default assigned printers and the session printer, by specifying one for each client machine.

Client Names/IP's	Default Printer	Session Printers
VDI-01	Client main printer	Add...

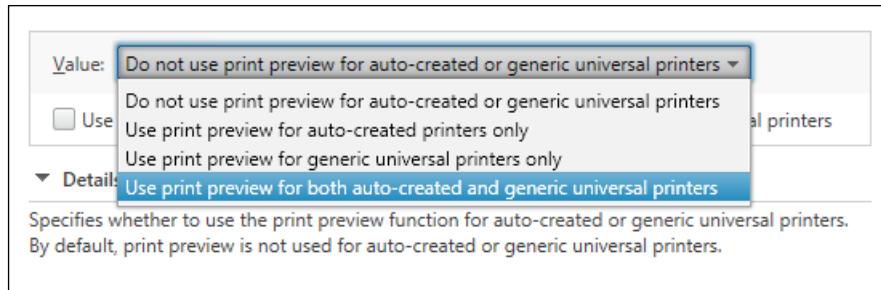
- ▶ **Printer auto-creation event log preference: Log errors and warnings, Log errors only, and Do not log errors or warnings:** This policy allows you to configure the level of logging for the printer autocreation activities. You can decide to log no events, warnings or errors only, or both.
- ▶ **Printer driver mapping and compatibility:** With this policy you can import a set of printer drivers which can be used to define compatibility and substitutions for the client drivers. This means that you can define a rule to override customized settings, in order to standardize the printing architecture.
- ▶ **Printer properties retention: Held in profile only if not saved on the client, Retained in user profile only, Saved on the client device only, and Do not retain printer properties:** This policy lets you decide if and where to save the configured printer settings. You should consider to save this settings in the user profile, especially in presence of a centralized profile manager, and a non-persistent desktop machine.
- ▶ **Retained and restored client printers: Allowed or Prohibited:** In case of customized printer configurations you can have the ability to maintain these settings and restore them in the event of configuration problems.
- ▶ **Session printers:** This policy permits you to add a list of the network printers that can be autocreated with XenDesktop. You have to specify the printer UNC path when adding the network resource.
- ▶ **Universal driver preference:** Using this policy you can choose the order in which to use the Universal Printer drivers, such as **EMF, PCL** in its different versions, **XPS** or **PS**.
- ▶ **Universal print driver usage: Use only printer model specific drivers, Use universal printing only, Use universal printing only if requested driver is unavailable, and Use printer model specific drivers only if universal printing is unavailable:** This policy manages the situations on which to use the universal printer driver. By default this driver is used only when a specific driver is not available.

- ▶ **Universal Print Server enable:** **Disabled**, **Enabled with fallback to Windows' native remote printing**, and **Enabled with no fallback to Windows' native remote printing**. This policy, disabled by default, configures the use of the **Universal Print Server** feature. In the event of fault or compatibility problems, you have the ability to configure the policy to roll back to the Windows native printing driver.
- ▶ **Universal Print Server print data stream (CGP) port:** This policy is particular useful in the case of a networked printing environment. It's possible to configure the port used by the Print Server's data stream listener. The default value is 7229.
- ▶ **Universal Print Server print stream input bandwidth limit:** With this parameter you can specify the rate, in Kbps, for print data transferring. The default limit is equal to 0 Kbps.
- ▶ **Universal Print Server web service (HTTP/SOAP) port:** This policy configures the port used by the Print Server SOAP service (Web listener). The default value is 8080.
- ▶ **Universal printing EMF processing mode: Spool directly to printer or Reprocess EMFs for printer:** This policy checks the way to process the EMF spooling queue (**Enhanced Metafile Format (EMF)**, is a device-independent format able to intercept the graphical elements in a printing task).
- ▶ **Universal printing image compression limit: No compression, Best quality (lossless compression), High quality, Standard quality, and Reduced quality (maximum compression):** This is an important policy which allows you to configure the quality level of the printed images, deciding on whether to give precedence to the quality or to the compression level.
- ▶ **Universal printing optimization defaults: Best quality (lossless compression), High quality, Standard quality, and Reduced quality (maximum compression):** This policy permits you to configure the image quality and compression to apply to the Universal Printer session.



3

- ▶ **Universal printing preview preference:** This option allows you to configure the options for previewing documents to be printed, as shown in the following screenshot:



- ▶ **Universal printing print quality limit: No Limit, Draft (150 DPI), Low Resolution (300 DPI), Medium Resolution (600 DPI), High Resolution (1200 DPI):** This policy allows you to configure the resolution for generated printing jobs.
- ▶ **Wait for printers to be created (desktop): Enabled or Disabled:** With these parameters you can decide whether or not to wait for the printer creation process when connecting with your user profile. You can't apply this policy to a published resource.



When possible, you should only use the generic Citrix Universal Printer driver instead of many different printer drivers and avoid automatically installing the printer drivers on the desktop instances in order to reduce troubleshooting activities in case of issues. If you do not have client printers, consider using unified printer drivers and try to consolidate the printer types in your company if possible.

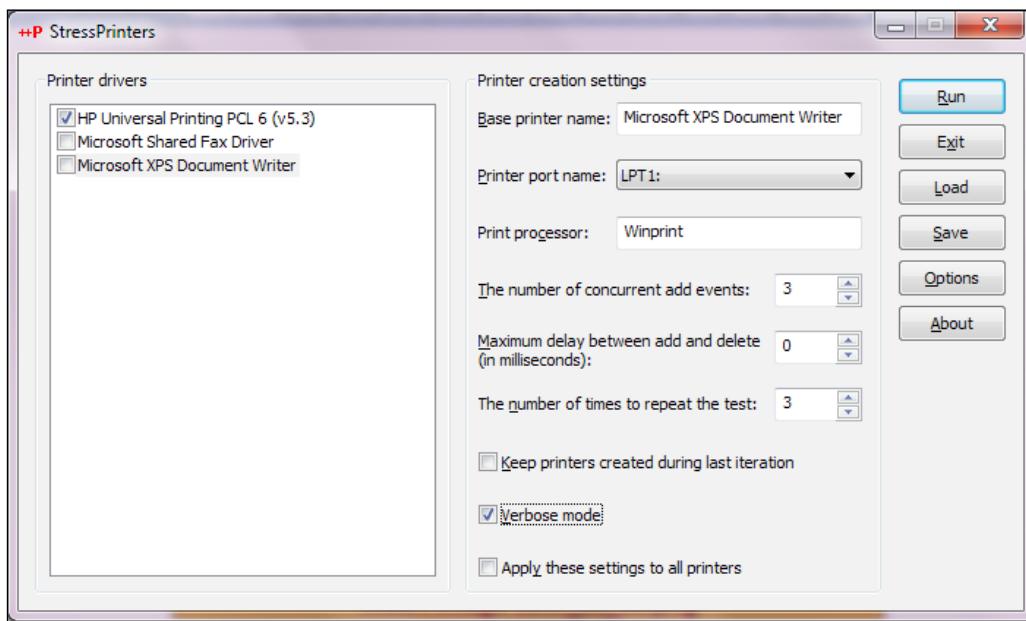
There's more...

In the wide range of free Citrix tools, you will find the Citrix Stress Printers software. It allows you to simulate multiple sessions using configured printer drivers in order to test the capability of using the driver and its response in terms of physical and virtual resource usage.

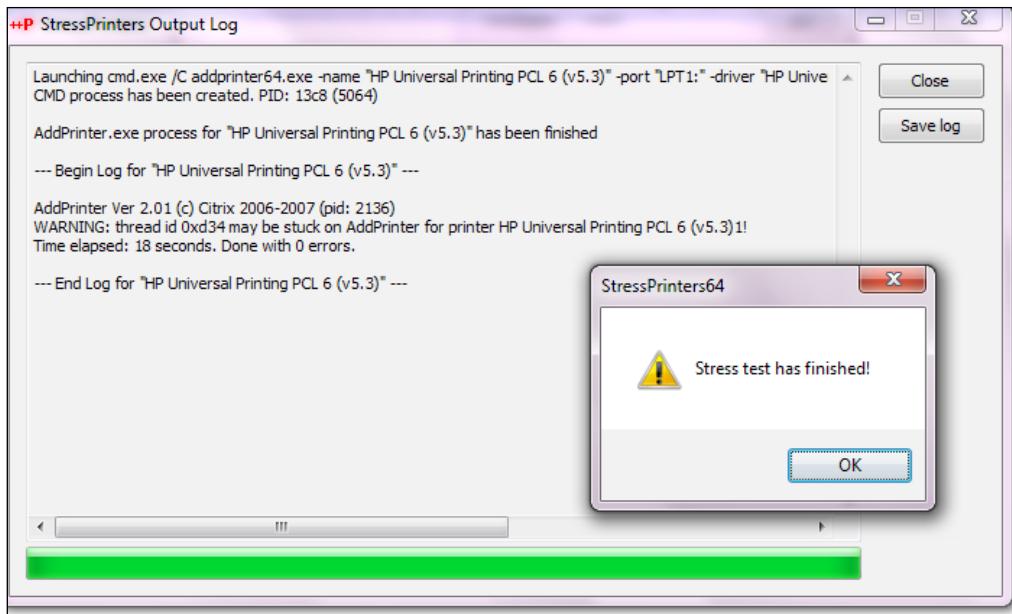


You can download the zip file archive at the location:
<http://support.citrix.com/article/CTX109374>

Run the right version for your infrastructure by double-clicking on the 32-bit or 64-bit executable file. The software will let you select the driver on which to perform the load tests, the printer name and port (for instance, LPT1 for a local printer or the configured IP address for a network device), the number of concurrent events, and how many times to repeat the tests. If you want, you can run the test in verbose mode by flagging the appropriate option checkbox. By clicking on the **Save** button, you can archive in a text file the configured tests to be loaded and later run again. To execute the tests, you have to click on the **Run** button.



After that, you'll receive a summary of the executed tests; if you want, you can save the related log file by clicking on the **Save log** button.



See also

- ▶ The *Configuring XenDesktop® policies* recipe in Chapter 8, *XenDesktop® Tuning and Security*

Configuring USB devices

When making a decision about the migration from physical to virtual desktop infrastructure, the managers and the IT technician should always consider maintaining a high operational level for their users, such as elevated user experience or the ability to use external devices. In this recipe, we will discuss how to use and map the USB devices, while also taking a look at the security aspects involved in this operation.

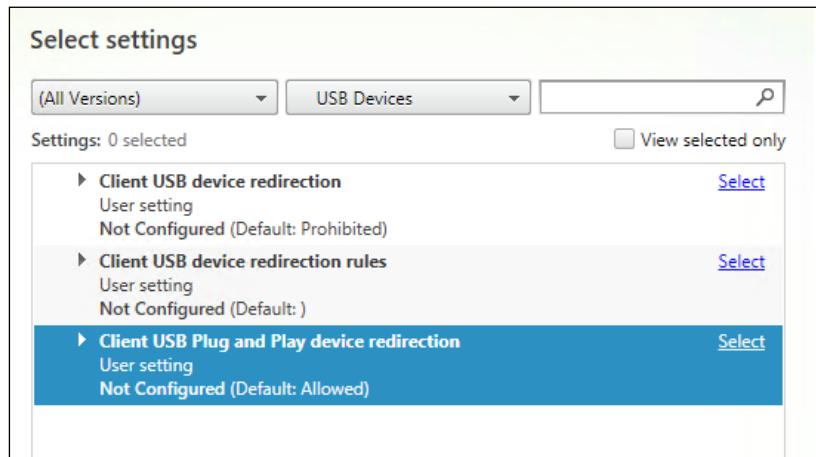
Getting ready

You need administrative access to the Citrix Controller machine in order to configure the required policies. The presence of Citrix Receiver on the desktop base image template is, of course, a mandatory prerequisite.

How to do it...

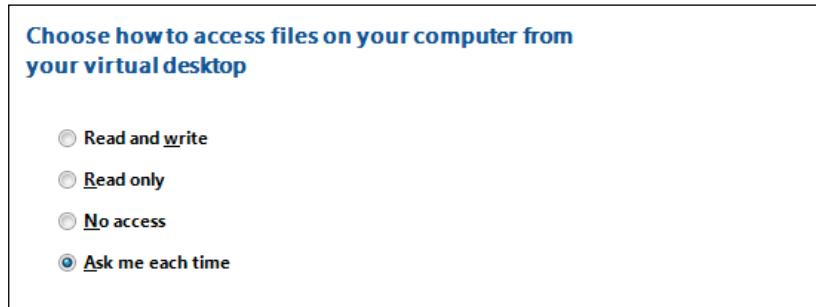
In this section, we will explain how to configure the use of the physical USB devices within the Citrix XenDesktop virtual environment:

1. Connect to the Citrix Controller machine and hit the Windows + C key combination. Search for the Citrix Studio icon in the Citrix software section and click on it.
2. In the left-hand menu click on the **Policy** link, and then select the **Create Policy** option on the right-hand menu.
3. On the **Select settings** screen, choose the **USB Devices** option in the second dropdown list.
4. Edit the **Client USB device redirection** policy, choosing whether to allow or prohibit the mappings of the USB devices. After that, click on the **OK** button.
5. Edit the **Client USB Plug and Play device redirection** policies, choosing whether to allow or prohibit the mapping of Plug and Play devices, such as cameras or POS. After that, click on the **OK** button.

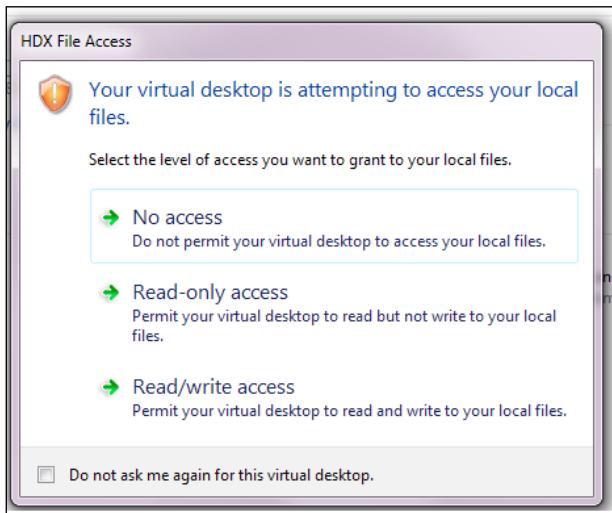


6. Connect to one of the desktop instances, and in the **Citrix** menu bar on the top of the VDI session, click on the **Preferences** tab.

7. Select the **File Access** section, and decide which type of access to the USB device to give to the virtual desktop. (**No Access**, **Read only**, **Read and write**, and **Ask me each time**). After that, click on the **OK** button.



8. Attach a USB disk to your physical client to test the ability of the Citrix Desktop instance to see and to interact with it.



How it works...

With the USB devices policies, administrators can decide whether to give the user the ability to mount and use external devices, with particular attention to USB mass storage devices. As explained later in this recipe, you can secure the resources in your infrastructure by implementing some kind of device control, limiting usage and access to only the configured USB peripherals.

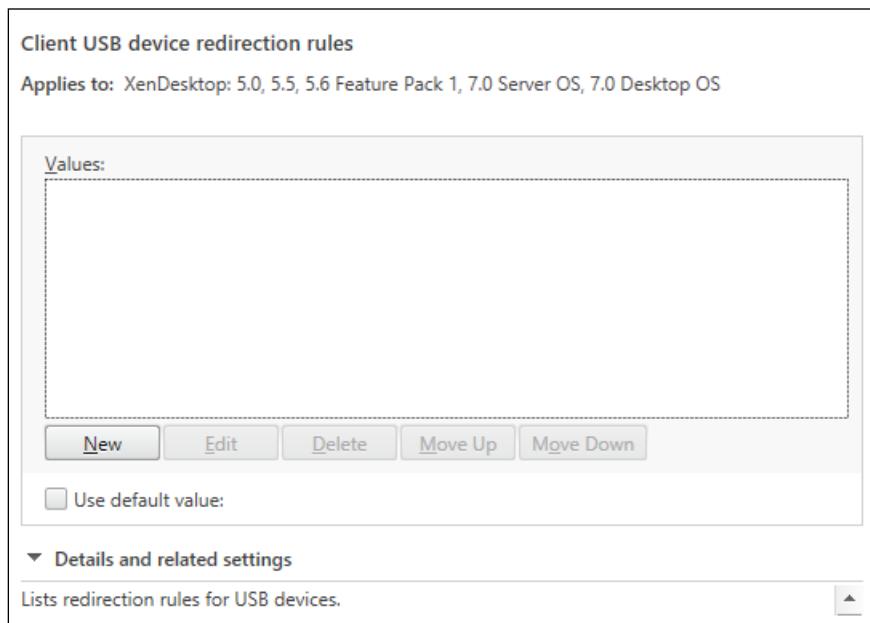
After the configuration of the policies, you have to choose which way a desktop instance can access data on a mounted USB device. You could prohibit total access to the resource, allowing basic read-only access, or give full read-and-write privileges to fully operate on the available data.

This process applies when you connect a USB key or storage device to your physical client (thin client, notebook, and so on). The communication passes to the Citrix Receiver client, which performs a check on the applied system policies, permitting you or restricting access to the content on the device.

There's more...

The second USB device policy (**Client USB device redirection rules**) permits you to implement a filter based on the model of the USB product you're going to mount on your virtual desktop. This means that you can allow or deny the use of a specific USB disk, based on hardware parameters, such as **Vendor ID (VID)**, **Product ID (PID)**, or **Release ID (REL)**.

To create a rule, edit the discussed policy and click on the **New** button, or click on **Edit** to modify an existing one.



The filtering rule must be generated by using the following parameters:

- ▶ [Allow | Deny] : [Category] = [Category Code]

In the category section, you have to use one of the following parameters:

- ▶ **VID:** This is the Vendor ID for the USB device
- ▶ **PID:** This is the Product ID for the USB device
- ▶ **REL:** This is the Release ID for the USB device
- ▶ **Class:** This is the category to which the USB device belongs
- ▶ **SubClass:** This is the subcategory part of the class earlier described
- ▶ **Prot:** This is the communication protocol used by the device

The following is an example of a configured USB device rule:

- ▶ Allow: Class=08 SubClass=03 # Mass storage devices



Please refer to the USB community (<http://www.usb.org/home>) to find all the required information about the vendor and product IDs of USB devices.

See also

- ▶ The *Configuring XenDesktop® policies* recipe in Chapter 8, *XenDesktop® Tuning and Security*

7

Deploying Applications

In this chapter, we will cover the following recipes:

- ▶ Publishing the hosted applications
- ▶ Publishing the Local Access Apps (LAA)
- ▶ Publishing applications using Microsoft App-V

Introduction

When you think about the Citrix XenDesktop suite, you only consider the virtual desktop implementation part. This approach could be correct when creating a machine with the full set of applications already installed, but not when we consider delivering only specific applications for every domain user.

In this chapter, we're going to discuss this second approach by the use of the three supported technologies to deliver applications to the user's desktops: the creation of *hosted applications*, the **Local Access Apps (LAA)** with XenDesktop, and the most recent way to publish applications, the App-V platform developed by Microsoft.



In XenDesktop 7, for the Server OS deployment, the hosted applications technique is the successor to XenApp 6.5, which is now integrated in this XenDesktop release.

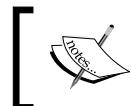
Publishing the hosted applications

The hosted applications approach is the simplest and nearest to a standard pre-installed desktop instance. With this technique, anyway, you will be able to reduce the impact on the infrastructural components because of the absence of the terminal server licenses required in other applications deployment solutions, such as the old Citrix XenApp approach. On the other hand, you have to consider the necessity to have more XenDesktop licenses.

Getting ready

To be able to deploy the hosted applications, you need the right number of XenDesktop licenses within your infrastructure: remember that for any single application or set of applications, you need a XenDesktop license corresponding to a deployed desktop instance.

Moreover, you need to generate a number of desktop instances in your catalog that is equal to or greater than the number of users accessing the applications. A good reference for the licensing model to apply can be found at the following link: <http://www.citrix.com/products/xendesktop/how-it-works/licensing.html>.



Please refer to the *Creating and configuring the Machine Catalog* recipe in *Chapter 6, Creating and Configuring a Desktop Environment* for the creation of the machine catalog.



How to do it...

We will explain how to publish the hosted apps based on the XenDesktop application catalogs:

1. Connect to the Delivery Controller server with a domain user with administrative privileges.
2. Use the Windows + C key combination; search for the **Citrix Studio** icon in the Citrix software section; and click on it.
3. Click on the **Machine Catalogs** link in the left-hand side menu, and then select **Create Machine Catalog** in the right-hand side panel.
4. In the **Getting Started** screen, click on the **Next** button to proceed.
5. In the **Operating System and Hardware** section, select the type of desktop you want to create (**Windows Desktop OS**). After selecting the appropriate radio button, click on **Next**.

6. In the **Machine Management** section, select the kind of infrastructure to use to deploy the resources (*Virtual* or *Physical* machines), and then choose the **MCS** methodology to use to manage the catalog. After the completion of this task, click on the **Next** button.
7. In the **Desktop Experience** section, select the way to assign the resources to the users each time they log on and whether or not the user's personal data would be saved within the existing virtual desktops. After completing this task, click on **Next**.
8. Select a master image from the list from which we have to generate the desktop instances. After completing this task, click on **Next**.
9. In the **Virtual Machines** section, select how many machines must be generated by incrementing the value of the **Number of virtual machines needed** section. After this, you need to configure the resources to be assigned to any instance (**Virtual CPUs** and **Memory (MB)**). Click on **Next** to proceed.



To differentiate the machines in a desktop group from that in an application group, you should always create new machine accounts with a naming convention other than that of the machines in the desktop group.

10. In the **Active Directory computer accounts** section, choose either **Create new Active Directory accounts** or **Use existing Active Directory accounts**. To better understand all the creation features, in this section we will select the creation of new computer accounts.
11. In the **Active Directory location for computer accounts** section, select from the drop-down list the **Domain** on which you are working, and choose an organizational unit on which you are creating the computer accounts. Then select an **Account naming scheme**, in the form of `MachineName##`, where the two final characters identify a progressive code made up of either letters or digits (**A-Z** or **0-9**). After completing this task, click on the **Next** button.

12. In the **Summary** section, assign a name and an optional description in the respective fields (**Machine Catalog Name** and **Machine Catalog description for administrators**), and then click on the **Finish** button to complete the configuration operations.

The screenshot shows the 'Summary' configuration screen. It displays various settings for a new machine catalog:

Machine type:	Windows Desktop OS
Machine management:	Virtual
Provisioning method:	Machine creation services (MCS)
Desktop experience:	Users connect to a new desktop each time they log on
Resources:	VMware01
Master Image name:	T0_VDA
Number of VMs to create:	2
Virtual CPUs:	2

Below the summary table, there are input fields for the Machine Catalog name and description:

Machine Catalog name:

Machine Catalog description for administrators: (Optional)

Note: To complete the deployment, assign this machine catalog to a Delivery Group by selecting Delivery Groups and then Create or Edit a Delivery Group.

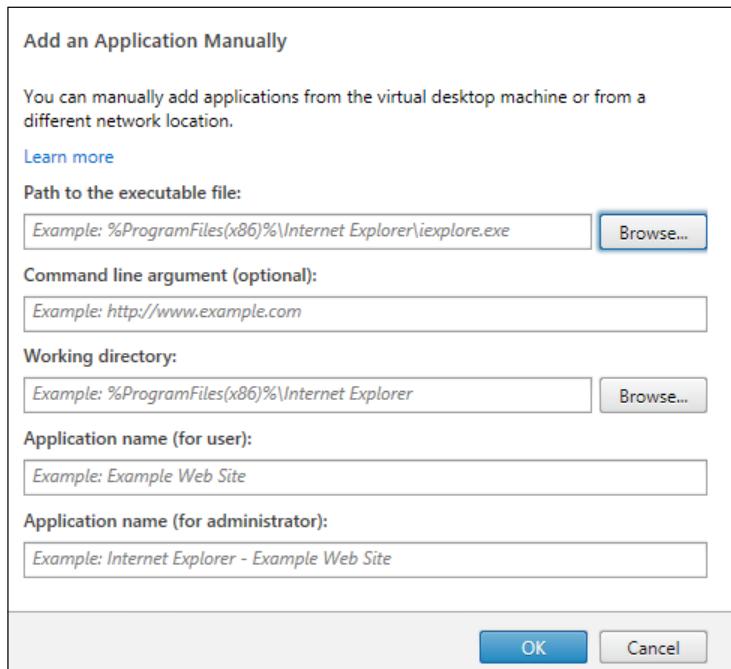
[ In the previous chapter, we've already seen how to create a catalog, so we will work on an existing catalog in this case. For more details please refer to the *Creating and configuring the Machine Catalog* recipe in Chapter 6, *Creating and Configuring a Desktop Environment*.]

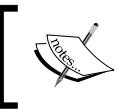
13. Click on the **Delivery Groups** link in the left-hand side menu, and then select **Create Delivery Group** on the right-hand side of the screen.
14. After clicking on **Next** in the **Introduction** section, in the **Machines** screen, select the catalog from which we take the desktop instances, and select the number of machines to be added, with a number equal to or less than the number of available machines. Then click on **Next**.

15. In the **Delivery Type** section, select the **Applications** radio button, and then click on **Next**.



16. In the **Users** section, select the users or the groups to which will be assigned the application desktop instances, and then click on the **Next** button.
17. In the **Applications** section, select one of the listed discovered software, or click on **Add applications manually** to select the application to add to the delivery group. In this second case, a pop-up screen will ask you for the application details you want to add as shown in the next picture. After completing this task, click on **Next**.





If you have configured an administrative scope, you will have the ability to assign it to the published Delivery Group.

18. In the **Summary** screen, assign a name and an optional description to the applications delivery group, and click on **Finish** to complete the procedure.

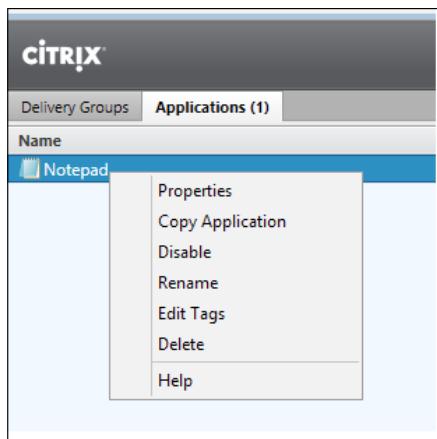
The screenshot shows the 'Summary' screen of the Citrix application deployment wizard. It displays the following configuration details:

Source Machine Catalog:	VDI
Machine type:	Windows Desktop OS
Allocation type:	Static
Number of machines added:	1 unassigned
Delivery type:	Applications
Users:	-
Applications:	1
Scopes:	All

Below the summary table, there are fields for defining the delivery group:

- Delivery Group name:** Application-Group
- Delivery Group description for users: (Optional)** Application-Group

19. Right-click on the published application, and select the **Properties** option.



20. In the **Identification** section, insert an application name in the **Application name** field for both the user and the administrator to use and an optional application **Description**.

Identification

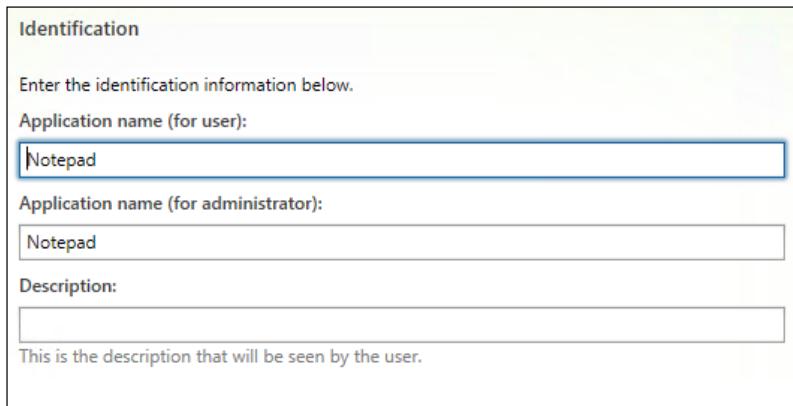
Enter the identification information below.

Application name (for user):
Notepad

Application name (for administrator):
Notepad

Description:

This is the description that will be seen by the user.



21. In the **Delivery** menu, you can select the icon to associate it with the application, as an optional category on which to group the app, and to enable the **Add shortcut on user's desktop** flag.

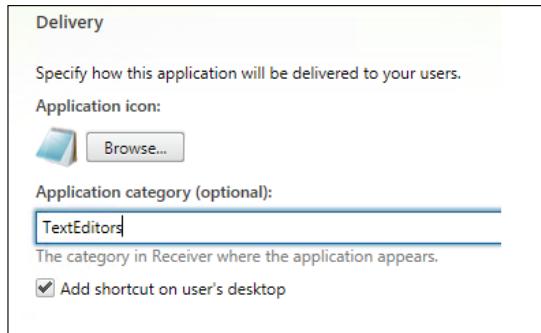
Delivery

Specify how this application will be delivered to your users.

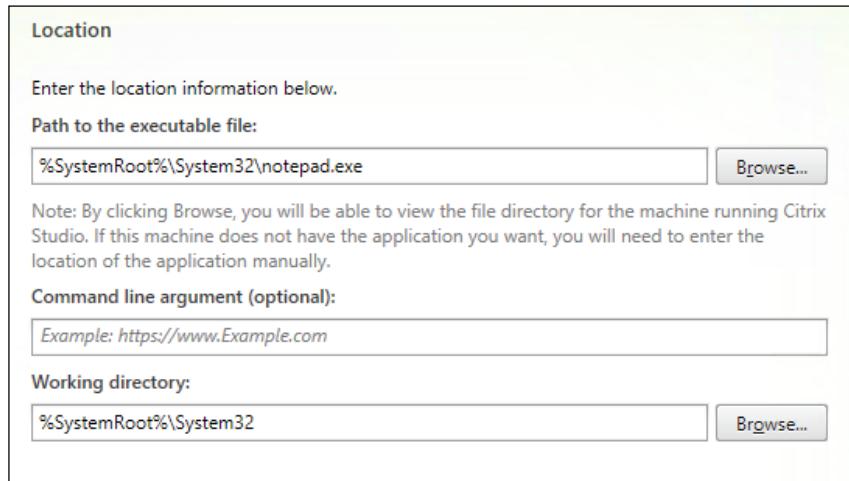
Application icon:


Application category (optional):
TextEditors

The category in Receiver where the application appears.
 Add shortcut on user's desktop



22. In the **Location** section, select the application path executable file, the optional command-line parameters, and the **Working directory**.

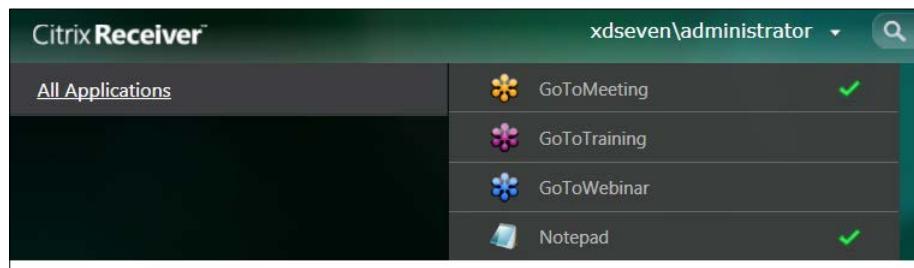


23. In the **Limit Visibility** section, you can decide whether to show the application to the entire Delivery Group's members or make it only usable for specific users. After completing these configurations, click on the **OK** button.



You'll have more details about the Content redirection section later in this recipe.

24. Connect to the StoreFront configured store, and log in using the credentials of a user holding one or more published application(s). In the resources menu, you can now find the linked software in the application's catalog. You can click on the application link to start using it.



25. Come back to the Citrix Studio console; click on the **Machine Catalogs** link in the left-hand side menu; and select **Create Machine Catalog** in the right-hand side panel.

26. In the **Getting Started** screen, click on the **Next** button to proceed.
27. In the **Operating System and Hardware** section, select the type of desktop you want to create (**Windows Server OS**). After selecting the appropriate radio button, click on **Next**.



28. In the **Machine Management** section, select the kind of infrastructure to use to deploy the resources (*Virtual* or *Physical* machines), and then choose the **MCS** methodology to use to manage the catalog. After completing this task, click on the **Next** button.
29. Select a **Master Image** from the list from which to generate the desktop instances. After completing this task, click on **Next**.
30. In the **Virtual Machines** section, select how many machines must be generated by incrementing the value of the **Number of virtual machines needed** section. After this, you need to configure the resources to be assigned to any instance (**Virtual CPUs** and **Memory (MB)**). Click on **Next** to proceed.
31. In the **Active Directory computer accounts** section, choose either **Create new Active Directory accounts** or **Use existing Active Directory accounts**. In this section, we will select the creation of new computer accounts to better understand all the creation features.
32. In the **Active Directory location for computer accounts** section, select from the drop-down list the **Domain** on which you are working, and choose an organizational unit on which we are creating the computer accounts. Then select an **Account naming scheme**, in the form of **MachineName##**, where the two final characters identify a progressive code made up of letters or digits (**A-Z** or **0-9**). After completing this task, click on the **Next** button.
33. In the **Summary** section, assign a name and an optional description in the respective fields (**Machine Catalog Name** and **Machine Catalog description for administrators**), and then click on the **Finish** button to complete the configuration operations.

34. Click on the **Delivery Groups** link in the left-hand side menu, and then select the **Create Delivery Group** on the right-hand side of the screen.
35. After clicking on **Next** in the **Introduction** section, in the **Machines** screen, select the catalog from which we take the desktop instances, and select the number of machines to be added, with a number equal to or less than the number of available machines. Then click on **Next**.
36. In the **Delivery Type** section, select the **Applications** radio button, and then click on **Next**.



With the choice of a server OS machine catalog, you will also have the ability to deploy desktops and applications delivery group types.

Delivery Type

You can use the machines in the Catalog to deliver desktops and applications to your users.

[Learn more](#)

Use the machines to deliver:

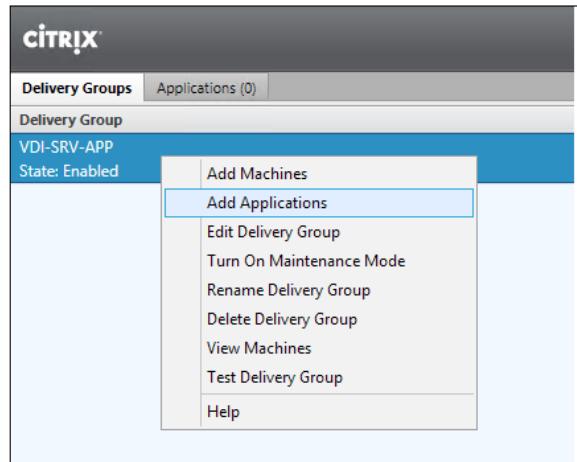
Desktops

Desktops and Applications

Applications

37. In the **Users** section, select the users or the groups to which will be assigned the application desktop instances, and then click on the **Next** button.
38. In the **Applications** section, click on **Next** to continue. We will deploy the required apps in the next steps.
39. In the **Summary** screen, assign a name and an optional description to the applications delivery group, and click on **Finish** to complete the procedure.

40. Right-click on the **Delivery Group** tab created earlier, and select the **Add Applications** option.



41. Click on the **Next** button on the **Introduction** screen, and then select one of the listed applications available on the server OS instance. Click on **Next**.
42. In the **Summary** screen, click on the **Finish** button to complete the procedure.
43. Connect to the StoreFront configured store, and log in using the credentials of a user holding one or more published application(s). In the resources menu, you can now find the linked software in the application's catalog. You can click on the application link to start using it.



Despite the execution of applications with desktop OS machines, you will see no login phase during the published application execution.

How it works...

Hosted applications deployment is one of the recent techniques offered by Citrix to deploy applications to the users. Through this approach, you can deliver software to published desktops or simply let the users run a single application.

The two ways to perform this kind of deployment are explained as follows:

- ▶ Hosted applications on Windows desktop operating systems (Windows 7 and Windows 8.x): In this kind of application deployment, a single published machine is able to serve a single user each time. For this reason, every application associated to a delivered desktop instance allows only one connection and not multiple accesses to the assigned software. This deployment approach could also be useful when you don't want to use the application streaming offered by platforms such as Microsoft App-V, as that software can only be installed on desktop machines. With this configuration, you won't need Terminal Server licenses, but any deployed application can become a consumed Citrix XenDesktop license.
- ▶ Hosted applications on **Windows Server** operating systems (**Windows Server 2008 R2**, **Windows Server 2012**, and **Server 2012 R2**): In this kind of application deployment, a single machine is able to serve multiple users each time. This deployment approach is based on the use of Terminal Server licenses with the consumption of XenDesktop licenses only for the number of deployed server machines. Remember that a single server machine can serve a number of users that is equal to the number of remote desktop-installed licenses. This is one of the new features for the XenDesktop platform. In fact, this is the integrated part of the old separated XenApp platform.

The user experience obtained by an application deployed with a desktop operating system is worse than the other technique (based on the old XenApp way of deploying applications). In fact, with a server OS, you will only see the execution progress bar for the launched application, while with a desktop OS-hosted app, the entire desktop logon process will be visible, decreasing the user experience performance.

All the hosted apps are part of a delivery group quite different from the standard group used till now. It's called **Application Delivery Group**, and is an application container on which it is possible to assign permissions and parameters of specific software.

You can decide to publish an application link on the user desktop, and also populate the Start menu with a shortcut; this way, the user will seem to be running the application locally on his/her desktop.

In the presence of the Citrix NetScaler Gateway, it's possible to configure an advanced access control policy. Instead of allowing any kind of connection, you can permit the connections to the applications only through the NetScaler platform, and eventually decide if filtering them through it is what's required.



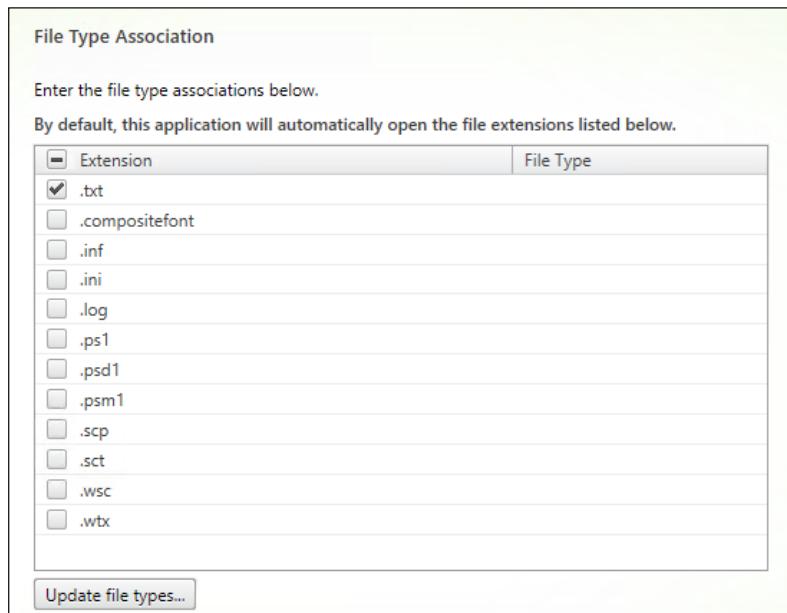
We will discuss the NetScaler Gateway platform in *Chapter 8, XenDesktop® Tuning and Security*.



There's more...

To complete the application publishing process, it's necessary to assign the file type (or types) to the software; to execute this task you need to perform a process called **Content Redirection**.

To be able to operate on the file extension assignment, you need to put the desktop that is offering the application in maintenance mode (this is needed only for a desktop OS deployment). After this, select the application on which you want to operate, and edit its properties. In the **Content redirection** section, click on the **Update file types** button, and select the machine from which to import the file types definition. At this time you will be able to select one or more file extensions to associate with the application (in this example, the .txt file types have been associated with the published *Microsoft Notepad*).



This operation will allow the users to double-click on the associated files and open them using the associated software with the hosted app technique.



Remember to disable the maintenance mode after completing this procedure!



See also

- ▶ The *Configuring and optimizing a Desktop OS master image* and the *Configuring and optimizing a Server OS master image* recipes in *Chapter 3, Master Image Configuration and Tuning*

Publishing the Local Access Apps (LAA)

In some cases, you would not want to migrate or reinstall applications installed on an existing working environment for various reasons (performance issues, installation or compatibility problems). Which way can these necessities match with a VDI migration project?

XenDesktop 7 has got the key. In fact, in this latest version, you have the ability to deploy **Local Access Apps (LAA)**, a technique that will permit you to re-use the applications that are already in use, without performing any setup or configuration procedures. In this recipe, we are going to discuss the required steps to implement it.

Getting ready

To be able to publish streamed Local Access Apps, you need a compatible source operating system (Windows Server 2012 / 2012 R2, Windows Server 2008 R2, Windows 7 and Windows 8/8.1) and at least Version 4.0 of Citrix Receiver.



The Local Access Apps deployment can *only* be applied to desktop delivery groups, and not to applications delivery groups.

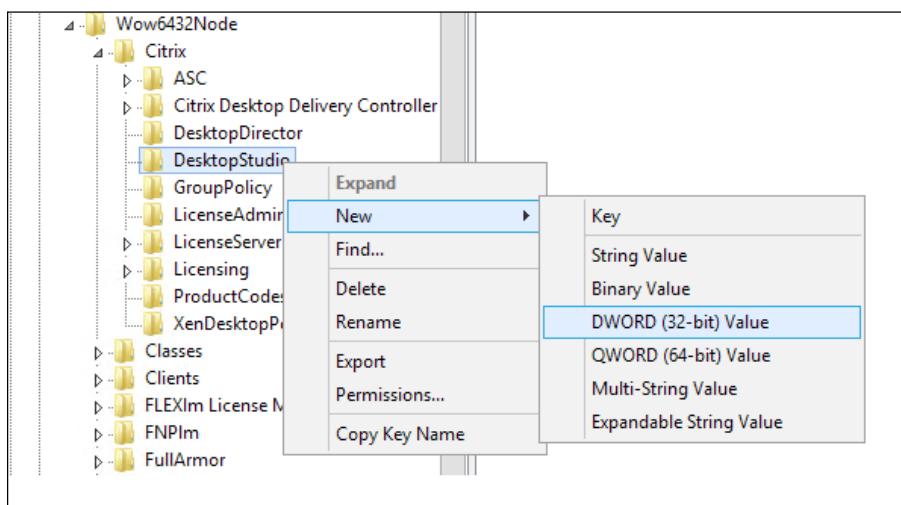
How to do it...

In this recipe, we are going to explain how to use the Local Access Apps feature:

1. Connect to the Delivery Controller server with an administrative domain user.
2. Press the Windows + X key combination, select the **Run** option, and type the following command:

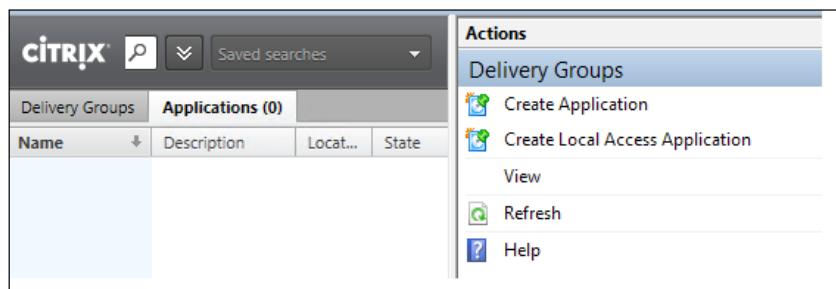
`regedit`

3. In the opened window, search for the register location `HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\DesktopStudio`. After you've found it, right-click on the **DesktopStudio** location, select **New | DWORD (32-bit) Value**, and insert the following registry key: **ClientHostedAppsEnabled | Value = 1**. This is necessary to enable the LAA usage.



 After completing this operation, remember that you need to restart the Delivery Controller machine.

4. After the reboot has been completed, connect again to the Delivery Controller server as an administrative domain user.
5. Press the Windows + C key combination, search for the **Citrix Studio** icon in the Citrix software section, and click on it.
6. Click on the **Delivery Groups** link in the left-hand side menu, and then select the **Applications** tab. After moving on to this section, click on the **Create Local Access Application** option on the right-hand side menu.





We have already described the way to create and configure catalogs and Delivery Groups. For this reason, we will perform the recipe's tasks on a configured infrastructure.

7. In the **Introduction** screen, click on the **Next** button to proceed.
8. In the **Delivery Group** section, select an available desktop group to which the application should be deployed in the *LAA* way, and then click on **Next**.

Delivery Group

Select the Delivery Group that contains the applications that you want to deliver.

[Learn more](#)

Select a Delivery Group:

Name	Type	Available machines
Remote	Windows Desktop OS	1
<input checked="" type="radio"/> VDI-DESK	Windows Desktop OS	1

9. In the **Location** section, select an application from the list of the locally installed applications, and then assign an optional command-line argument and a **Working Directory**. After completing this step, click on **Next**.

Location

Enter the location information below.

Enter path of the local application on the end users operating system:

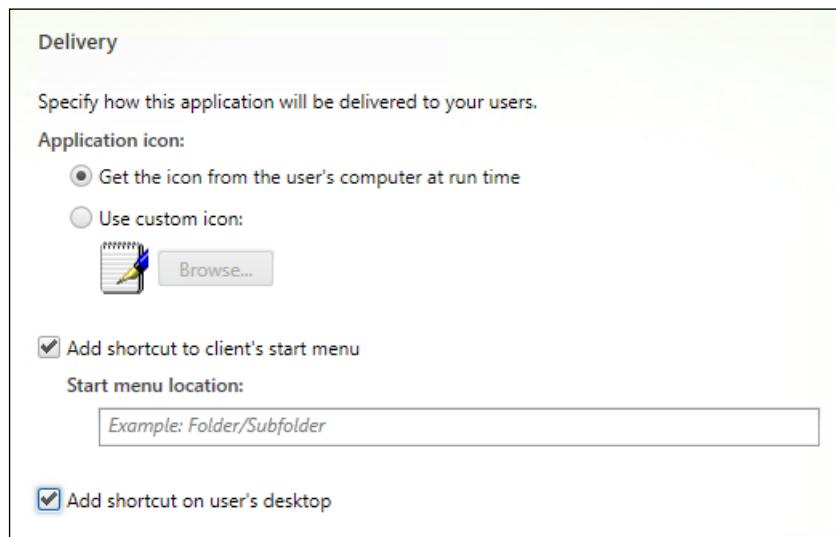
Note: By clicking Browse, you will be able to view the file directory for the machine running Citrix Studio. If this machine does not have the application you want, you will need to enter the location of the application manually.

Command line argument (optional):

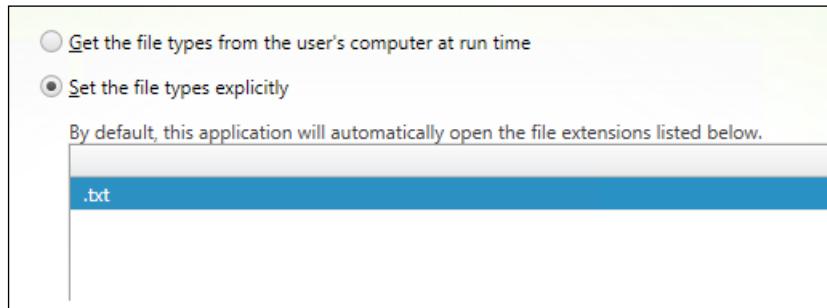
Working directory:

10. In the **Identification** menu, assign a name for users and administrators of the selected software, and provide an optional description. Click on the **Next** button to further proceed with the configuration steps.

11. In the **Delivery** section, choose the preferred application's icon, and decide whether or not to add the software to the desktop and Start menu of the user's desktop environment. Click on **Next** to continue.

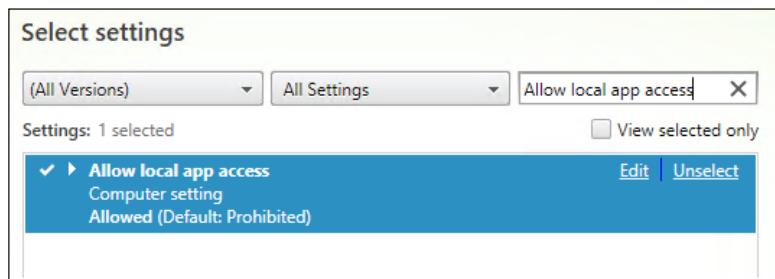


12. In the **Summary** screen, click on the **Finish** button to complete the configuration procedure.
13. Right-click on the published application, and select the **Properties** option.
14. Select the **File Type Association** section, and choose whether to associate the file type extensions at run time from the user's computer, or to specify one or more file types. Click on the **OK** button after completing this process.

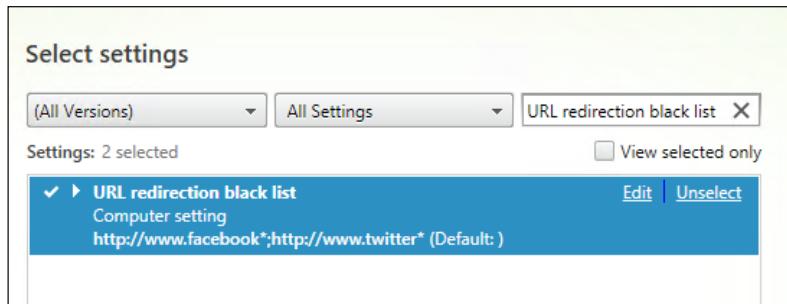


15. Select the **Policy** link in the left-hand side menu, and then edit an existing one or create a new policy.

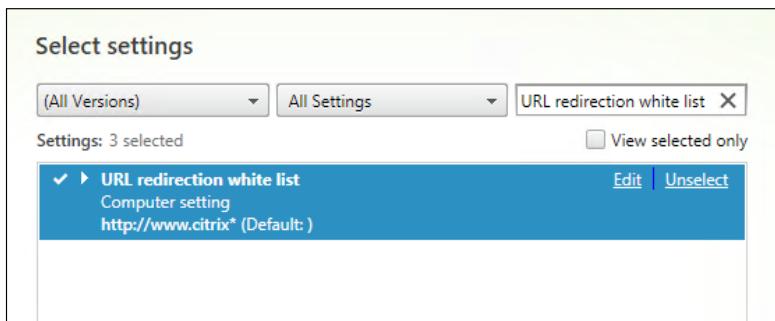
16. In the Search field, search for the policy: **Allow local app access**, and configure it as **Allowed**.



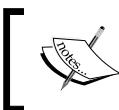
17. Use the search field to filter for the **URL redirection black list** policy; within this URL list, you will have to insert all the web addresses you want to execute out of the assigned VDI desktop on your personal device.



18. Filter the Citrix policies for **URL redirection white list**. In this list, you will have to insert all the web URLs you want to run on the company-assigned virtual desktop. After completing this task, click on **Next**.



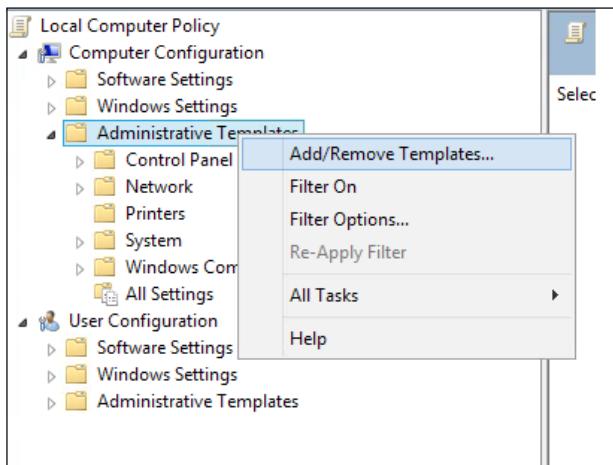
19. Connect to the personal user device involved in the LAA configuration, and execute the following command to run the **Group Policy management console** `gpedit.msc`.



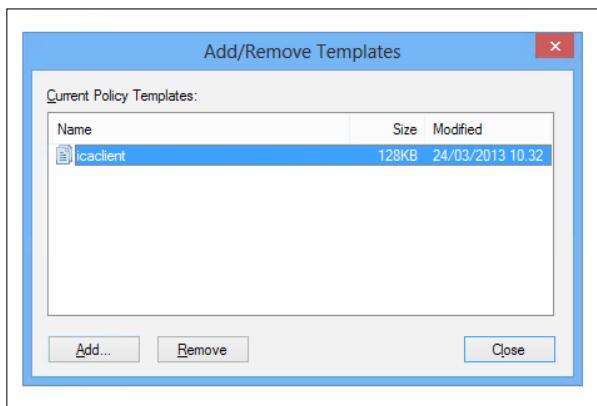
As an alternative, you can apply the configured settings by using **Domain Group Policy Objects (Domain GPO)**. In this case, we are applying the local user device GPO.



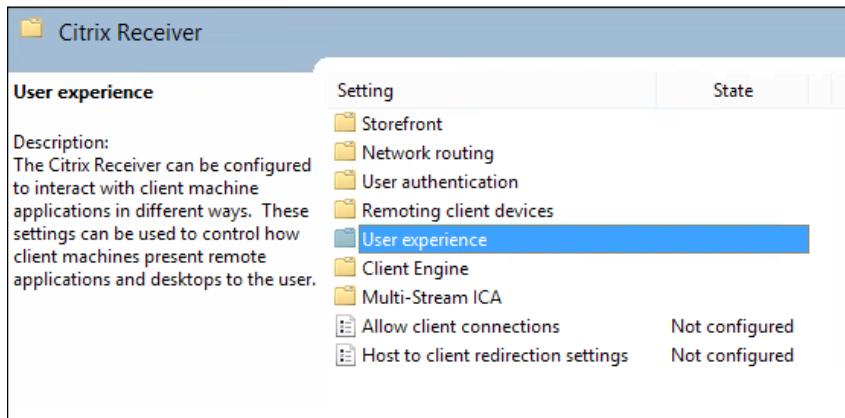
20. Expand the **Computer Configuration** section; right-click on the **Administrative Templates** folder, and select **Add/Remove Templates**.



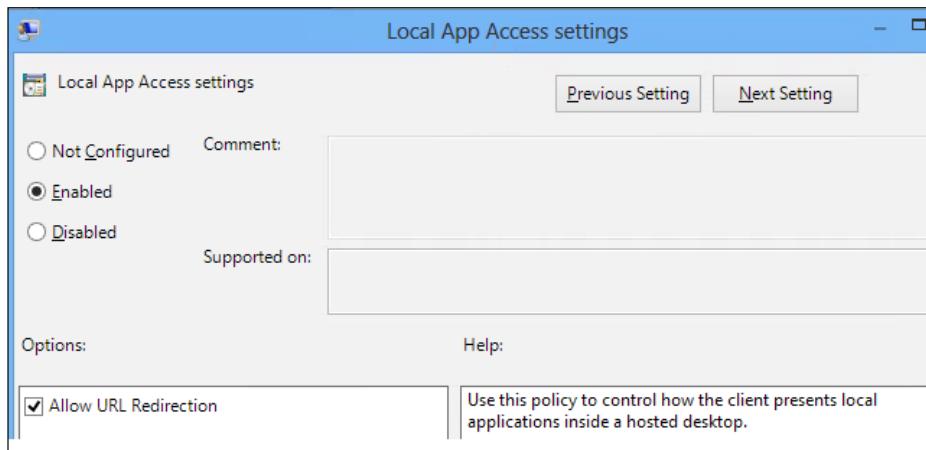
21. In the **Add/Remove Templates** screen, click on the **Add** button, and then browse for the `icaclient.adm` template file located at `C:\Program Files (x86)\Citrix\ICA Client\Configuration`. After you've added the file, click on the **Close** button.



22. Navigate to **Computer Configuration | Administrative Templates | Classic Administrative Templates (ADM) | Citrix Components | Citrix Receiver**, and select the **User Experience** folder.



23. Double-click on the **Local App Access settings** policy; select the **Enabled** option; and flag **Allow URL Redirection**. After completing this step, click on **Apply**, and then click on the **OK** button.



24. Run a Windows shell prompt with administrative credentials, and execute the following command to force the policy application:

```
gpupdate /force /target:computer
```



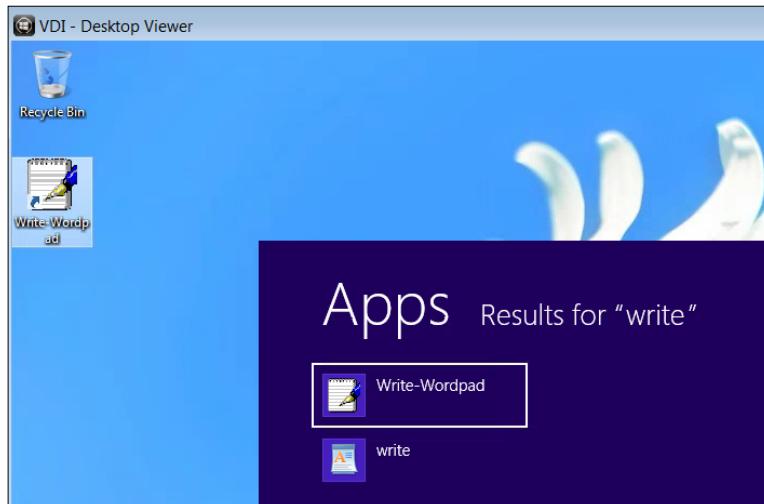
If you don't want to use the Microsoft Group policies to enable the LAA, you need to install in the first instance Citrix Receiver, enabling the following option by the command line:

```
CitrixReceiver.exe /ALLOW_CLIENTHOSTEDAPPSURL=1
```

25. On the same client device running Citrix Receiver, launch a Windows command shell prompt with administrative credentials, and execute one of the following commands required to enable the URL redirection for the configured Internet browser (for *Internet Explorer*, *Google Chrome*, and *Mozilla Firefox* respectively or for all the listed browsers):

```
c:\Program Files (x86)\Citrix\ICA Client\redirector.exe /regIE  
c:\Program Files (x86)\Citrix\ICA Client\redirector.exe /regChrome  
c:\Program Files (x86)\Citrix\ICA Client\redirector.exe /regFF  
c:\Program Files (x86)\Citrix\ICA Client\redirector.exe /regAll
```

26. Connect to the StoreFront portal a domain user with published applications and desktops, and then access one of the available Windows machines. You will find the published Local Access App on your desktop and Start menu, if configured.



27. Execute the published Local Access Application; the software will run out of the virtual desktop, directly on the physical personal device.



To avoid problems and confusion during the use of Local Access App, you should always run the virtual desktop in full-screen mode. This is necessary to operate and obtain a better user experience.

How it works...

The Local Access App functionality is a powerful option included by default with XenDesktop 7, which permits users and IT professionals to better improve the isolation between the personal devices and the corporate professional instruments.

By deploying it, you have the ability to decide what kind of applications are being directly executed on the end user's device without impacting the security and the policy for your company VDI architecture. The LAA resource groups can either be deployed using locally installed apps on the Citrix Delivery Controller servers, or they can be used in a more powerful way, by creating catalogs and delivered groups of remote PCs. These are domain-joined machines, physical or virtual, assigned to a specific end user, and generally populated with software and platforms that do not need to be migrated.

Moreover, with this second approach, you can also filter the execution of performance-impacting applications on your VDI client; you could, for example, use graphical applications directly on your personal client or reproduce web and media contents out of your company's virtual desktop. In the second case, the URL redirection features appear to be particularly important. In fact, by using XenDesktop policies, you can differentiate the kinds of web content and sites replicating on the two different areas (working and personal profiles). For this, you can use an addresses **black list** (with contents transferred on the physical device) or **white list** (websites data can be viewed within the VDI infrastructure).



The Local Access Application feature is also typically used for special hardware connected to the end-user devices that could not be redirected to a remote session.



There's more...

Once a VDI session disconnects, you can decide to configure the way to operate the Local Access Apps configured that must apply; after a logoff phase, in fact, an application can continue to run on the personal end user device, or you can decide to stop it after a Windows-user session has been logged off.

To configure your choice on which way to operate, you have to connect to the machine configured as a personal user device (out of your company), run the **regedit** command, and locate the registry key `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Client Hosted Apps\Policies\Session State`. By assigning the value 1 to this key, the LAA will continue to run after that the user has logged off. Instead, if you configure it with the value 3, the locally running applications will disconnect.

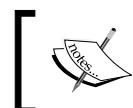
See also

- ▶ The *Configuring the XenDesktop® policies* recipe in Chapter 8, *XenDesktop® Tuning and Security*

Publishing applications using Microsoft App-V

An alternative to the Citrix XenApp streaming method is offered by Microsoft with its **App-V** platforms. The Microsoft App-V software, which is quite similar to the XenApp application profiling technique, permits you to publish the software to the end user desktop through the use of a specific client.

In this chapter, we will discuss the components and the way in which Microsoft App-V works.



To learn how to implement an App-V architecture, you can refer to the *Microsoft Application Virtualization Advanced Guide* book by Augusto Alvarez published by Packt Publishing.



Getting ready

For a full version of the App-V infrastructure, you need two or more servers on which to install and configure the following roles:

- ▶ **App-V Management System:** This component is the centralized management console for all the configured applications and the associated users.



- ▶ **App-V Management Server:** This is the application broker, the core of the App-V infrastructure, which delivers the software to the clients. App-V also permits you to use independent file streaming, the ability to directly stream the applications from a network share without using the management server.



IIS 7.0, .NET framework, and at least SQL Server 2008 R2 are required in order to implement the Management Server.

- ▶ **App-V Sequencer:** This is the packaging software that creates the application profiles. This must be installed on a client machine (Windows 8.x, Windows 7) on which are located the application's setups.
- ▶ **App-V Streaming Server:** This server is used to stream the published applications to the clients.

On the XenDesktop base image template, you need to install the Microsoft Application Virtualization Desktop Client component, in order to be able to contact the App-V infrastructure.

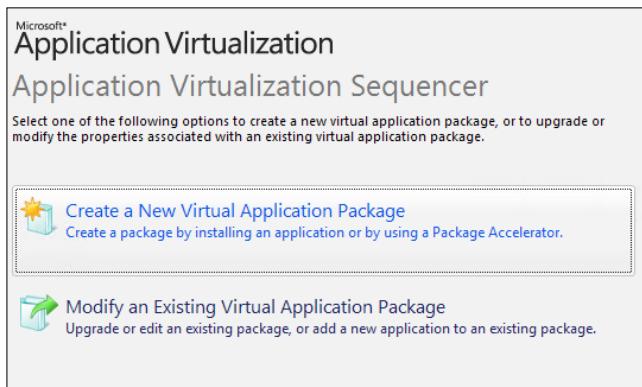


Remember that after installing the App-V client, you have to update the existing XenDesktop machine instances in order to use the client on the assigned virtual desktops.

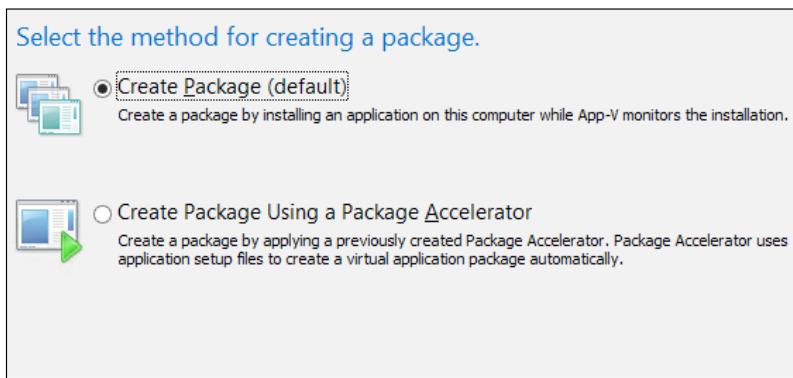
How to do it...

The following are the necessary steps to implement application sequencing and deployment using the Microsoft App-V platform:

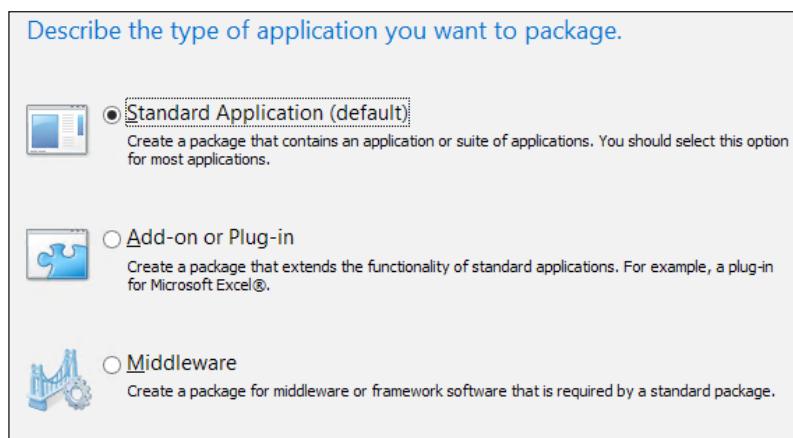
1. Connect to the App-V Sequencer machine with domain administrative credentials; use the Windows + C key combination; search for the **Microsoft Application Virtualization Sequencer** icon; and click on it.
2. On the **Application Virtualization** menu, click on the **Create a New Virtual Application Package** option.



3. From the **Packaging Method** section, select the **Create Package (default)**, and click on **Next**.

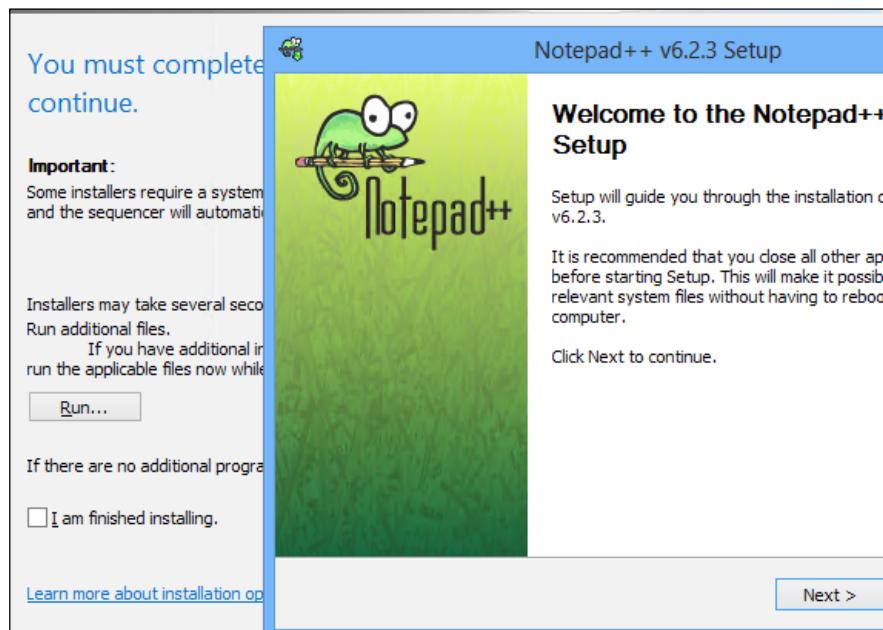


4. In the **Type of Application** section, select the **Standard Application (default)** option, and then click on **Next**.

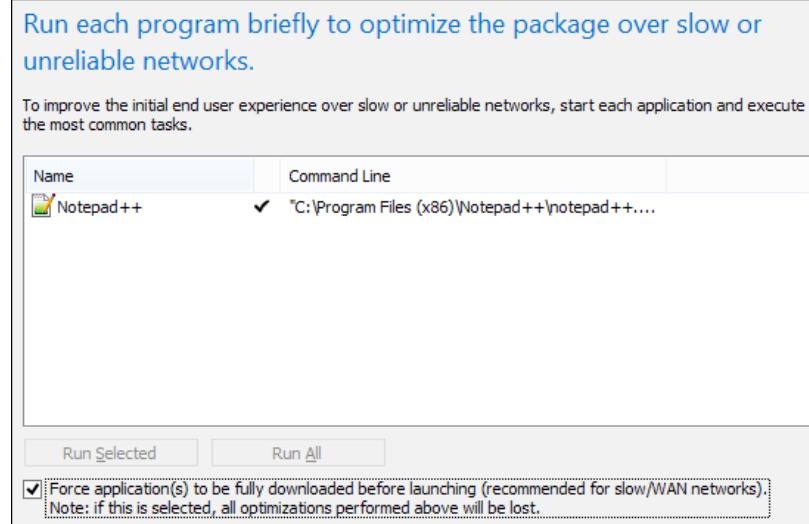


5. In the **Select Installer** menu, browse for the software setup previously copied on the Sequencer server, and click on **Next**. The application chosen for this step is the **Notepad++** text editor.
6. In the **Package Name** section, assign a name to the virtual application and the location on which the package will be stored (**Primary Virtual Application Directory** field). After completing this step, click on **Next**.

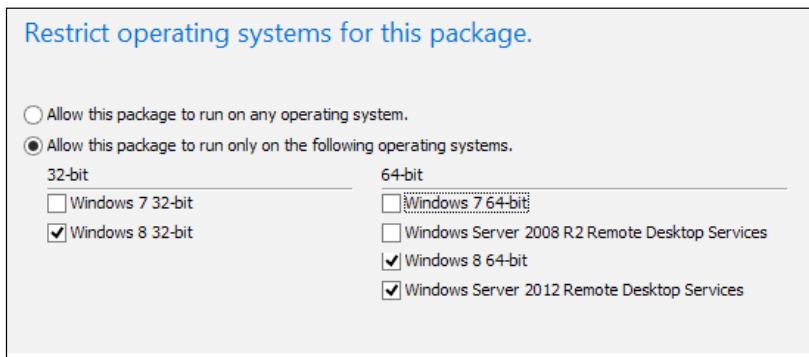
7. In the **Installation** section, perform and complete the installation procedure for the selected software. After completing this step, check the **I am finished installing** option, and click on **Next**.



8. In the **Configure Software** section, select the application installed earlier, and run it in order to complete the required configurations during the first application execution, and then click on **Next**.
9. If the **Installation Report** section notifies you about no warnings, you can continue by clicking on the **Next** button.
10. In the **Customize** section, select the **Customize** option, and click on **Next**.
11. In the **Streaming** section, highlight the software, and click on the **Run Selected** button to test again its ability to be executed, and then flag the full download option in the event of slow network connections. After completing this step, click on the **Next** button.



12. In the **Target OS** area, you can choose to filter the target operating system versions that allow the application to run. After this, click on **Next**.



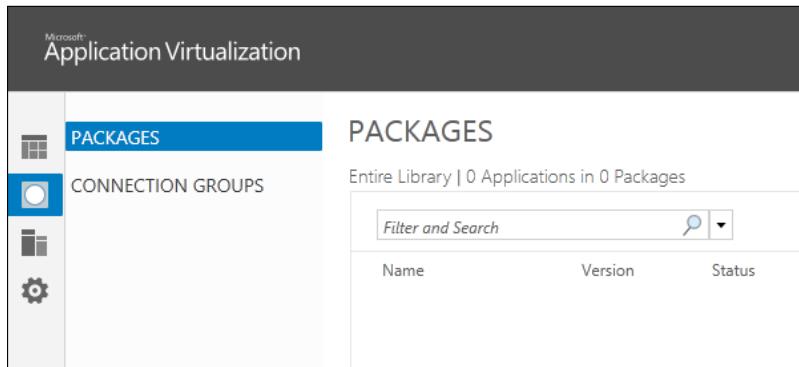
[ Remember that you always sequence an application on the same operating system family. For instance, apps deployed on Windows 8 should not be deployed on Windows 7 OS versions because of compatibility and functionality problems.]

13. In the **Create Package** section, choose the **Save the package now** option; optionally, add a **Description** to the packaged software; and select the location path previously used. To complete the entire procedure, click on the **Create** button.
14. In the **Completion** menu, click on **Close** to exit from the creation wizard.

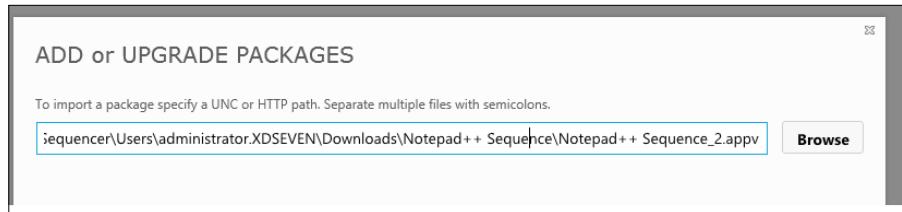
15. Connect to the App-V Management System server with domain administrative credentials; use the Windows + C key combination; search for the **Application Virtualization Management Console** icon; and click on it.

[ Microsoft Silverlight is required to run the App-V Management Console. Be sure you've installed it for the Internet Explorer browser.]

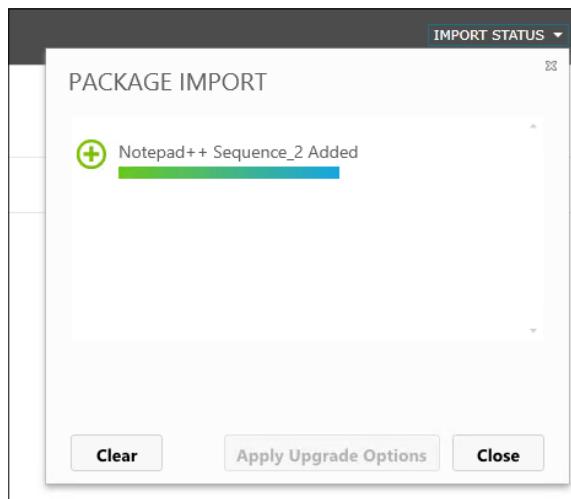
16. On the left-hand side menu, click on the packages link, and then select the **ADD or UPGRADE PACKAGES** link on the right-hand side of the window.



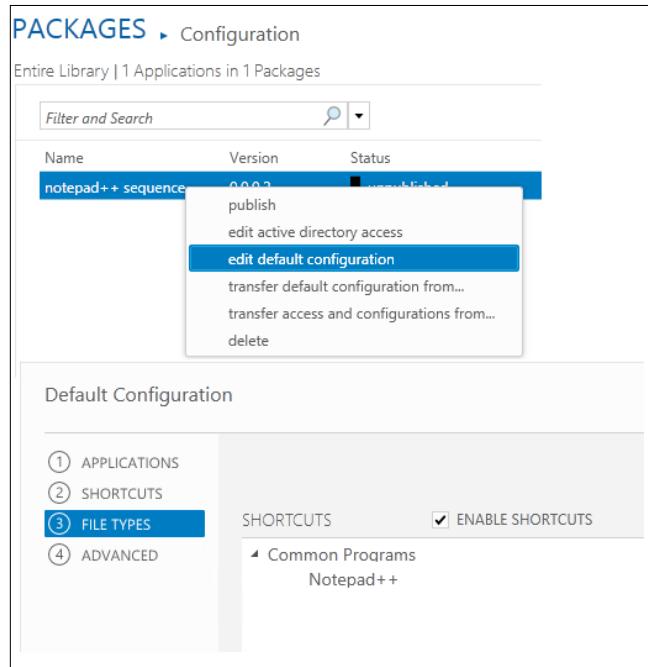
17. In the pop-up screen, insert the network path on which we have previously generated the App-V sequence, and locate the .appv sequence file. After this, click on the **Add** button to complete the procedure.



18. Wait for the package import procedure, and then click on the **Close** button on the **PACKAGE IMPORT** screen.



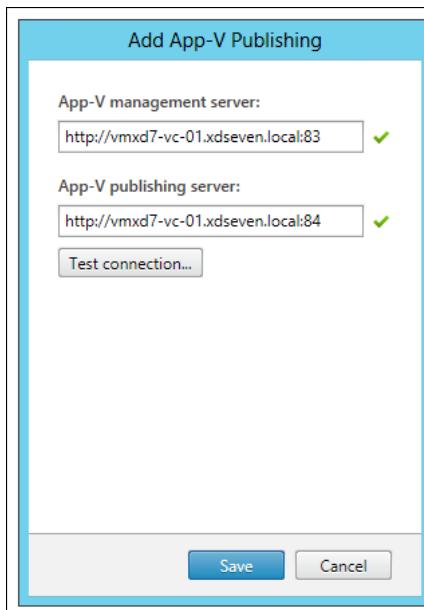
19. In the **Packages** menu, right-click on the imported sequence, and select to edit one of the listed configurable options. In the following screenshot, the default configuration menu has been reported:





You have to configure the permissions for the involved Active Directory users or groups in the right way; otherwise, you won't see the deployed App-V applications within the Citrix Studio Delivery Groups console.

20. If all the configurations are correct, right-click on the imported sequence, and select the **Publish** link. The application status LED will become green.
21. Connect to the Delivery Controller server as an administrative domain user.
22. Use the Windows + C key combination; search for the **Citrix Studio** icon in the Citrix software section; and click on it.
23. Right-click on the **App-V Publishing** link on the left-hand side menu; select the **Add App-V Publishing** option; insert two valid addresses for the App-V Management and Publishing servers in the form of `http://fqdn:<portnumber>`. After completion, click on the **Test connection** button to verify if you are able to connect to the App-V infrastructure.



During the application selection process from the delivery group application list, you will also find the associated App-V delivered packages.

24. During the application deployment process, you will now be able to see the software delivered by the App-V infrastructure.

The screenshot shows a list of applications in a management interface. The applications listed are:

Application name	Location
Immersive Control Panel	Master Image
iSCSI Initiator	Master Image
Magnify	Master Image
Math Input Panel	Master Image
Memory Diagnostics Tool	Master Image
Narrator	Master Image
Notepad	Master Image
Notepad++	App-V
ODBC Data Sources 32-bit	Master Image
ODBC Data Sources 64-bit	Master Image
Open Keyboard	Master Image

25. Connect to the StoreFront configured store, and log in using the credentials of a user holding one or more published application(s). In the resources menu, you can now find the linked software in the application's catalog.

The screenshot shows the Citrix Receiver application window. The 'All Applications' catalog is displayed, listing the following applications:

Application	Status
GoToMeeting	✓
GoToTraining	
GoToWebinar	
Notepad++	✓
VDI	✓

26. Connect to the Windows base image template on which you have installed the App-V Client, and run it. If all the steps have been correctly executed, you will be able to see the application link on your desktop and in your Start menu.

How it works...

The Microsoft App-V platform is based on a **Central Management Console** that manages the application's profiles generated on a different location, publishing them to the clients installed on the user desktops. The process of creating application profiles to redistribute to the users is called **sequencing**, the procedure earlier discussed during application installation monitoring; the machine on which the sequencing process runs must be equal to the target clients to whom the applications will be delivered. Through the publishing process, you have the possibility of filtering the destination operating system versions. This process is now integrated in the XenDesktop 7 Studio console with the possibility of associating the App-V infrastructural servers to the Citrix infrastructure, deploying application catalogs using the App-V offering and the Citrix Delivery Controller platform.

After generating the application sequence, it's time to use the App-V Management Server. With this platform it's now possible to load the application sequence and generate the software that will be delivered to the users. In this section, you can also assign a particular file extension to the software, which means implementing the user experience also for the application virtualization, applying it when a user needs to open a certain file.

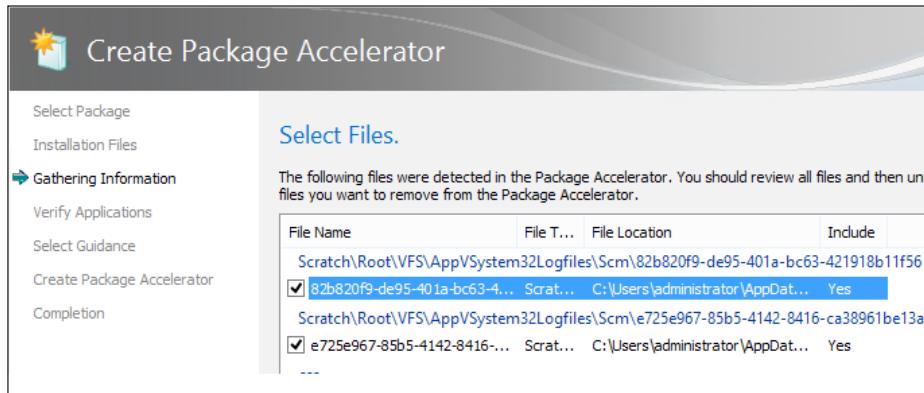
To improve the application flow from the server to the clients, App-V permits you to use the **streaming** technology. This is based on the concept of the old Citrix XenApp application streaming, which is used when bandwidth problems are the main issues to deal with.

There's more...

Through Microsoft App-V, you can also publish particular application packages called **Package Accelerator**: these are packages formerly generated from original installation media of complex applications with the setup procedure that converges at the end in a .cab archive.

Starting from this, you can create application packages to publish to the users without the necessity to repeat the installation procedure in the creation phase.

You can run the CAB generation procedure from the **Create Accelerator** section of the **Tools** menu in the **Sequencer** main menu. During the creation activities, you have to specify the installation file's location, guidance for administrators (a file in **rtf** format generated by you that should contain information about the application package use), and the destination location for the archive. Once this step has been completed, you can use the CAB file to create the application package by selecting the **Create Package Using a Package Accelerator** in the **Packaging Method** screen.



See also

- ▶ The *Configuring XenDesktop® to interact with Microsoft Hyper-V 3.0 – SCVMM 2012 SP1* recipe in Chapter 2, *Configuring and Deploying Virtual Machines for XenDesktop®*

8

XenDesktop® Tuning and Security

In this chapter, we will cover the following recipes:

- ▶ Configuring the XenDesktop® policies
- ▶ Installing and configuring Citrix® NetScaler Gateway 10.1
- ▶ Configuring the XenDesktop® logging

Introduction

Citrix XenDesktop offers a modular architecture in which security as well as the user experience is important. Citrix offers best practice documents to deliver a VDI solution in which the end user likes to work. Similar to a puzzle, all pieces have to fit. This does not mean that it's not possible to increase and develop both the levels. Citrix platforms or different vendor systems permit you to have a deeper protection and avoid performance issues by enabling the right policies.

During the course of this chapter, we will discuss about the configuration of the XenDesktop infrastructural policies; and we'll use critical platforms such as the Citrix NetScaler Gateway.

Configuring the XenDesktop® policies

Now that the XenDesktop infrastructure has been configured, it's time to activate and populate the VDI policies. This is an extremely important part of the implementation process. With these policies, you will not only regulate the resource use and assignment, but you will also improve the general virtual desktop performance.

 In this chapter, we won't discuss about the policies that will be applied to the printer's and USB device's areas. We have already described these policies in *Chapter 6, Creating and Configuring a Desktop Environment*.

Getting ready

All the policies will be applied to the deployed virtual desktop instances and the assigned users, so you need an already existent XenDesktop infrastructure on which you can enable and use the configuration rules.

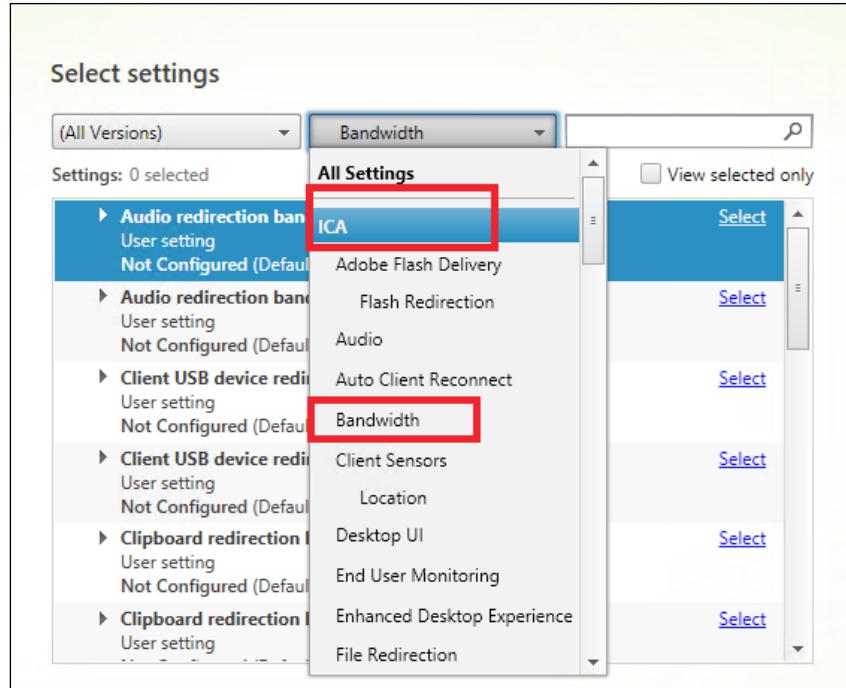
How to do it...

In the following steps, we will explain the configuration for the user and the machine policies offered by Citrix XenDesktop:

1. Connect to the Delivery Controller server as an administrative domain user.
2. Hit the Windows + C key combination, search for the **Citrix Studio (XD7-Site-First)** icon in the Citrix software section, and click on it.
3. Click on the **Policy** link in the left-hand side menu, and then select **Create Policy** in the right-hand side panel:



4. In the **Categories** menu, click on the following sections that are discussed and configure the values for the policies that will be applied to the clients:



ICA section

- ❑ **ICA Listener connection Timeout:** In this policy, insert a value in milliseconds. The default value is **12000**.
- ❑ **ICA listener port number:** This is the TCP/IP port number on which the ICA protocol will try to establish the connection. The default value is **1494**.

Adobe Flash Delivery subsection

- ❑ **Flash acceleration:** In this policy, the values are either **Enabled** or **Disabled**. With this policy, you can decide whether or not to enable the rendering of the Flash contents on the client side, but only in the legacy mode.

 After enabling this policy, you will have the ability to reduce the network usage by executing the Flash web components directly on the client machine. To use this configuration, you need the latest Citrix Receiver and Adobe Flash versions. Moreover, be sure your client supports this feature.

- ❑ **Flash background color list:** In this policy, specify a set of colors that will be applied to a specific URL with Flash contents. Even in this case, Flash will be rendered on the client side.

- ❑ **Flash backwards compatibility:** In this policy, the values are either **Enabled** or **Disabled**. With this policy, you can activate the compatibility of older Citrix Receiver versions with the most recent Citrix Flash policies and features.
- ❑ **Flash default behavior:** This policy regulates the use of the Adobe Flash technology. In this, the values are **Enable Flash acceleration**, **Disable Flash acceleration**, and **Block Flash player**, which can enable the most recent Citrix for Flash features (including the client-side processing), permit only server-side processed contents, or block any Flash content respectively.
- ❑ **Flash event logging:** In this policy, the values are either **Enabled** or **Disabled**. This policy lets you decide if create system logs for the Adobe Flash events.
- ❑ **Flash intelligent fallback:** In this , the values are either **Enabled** or **Disabled**. This policy, if enabled, can activate the server-side Flash content processing when the client-side is not required.
- ❑ **Flash latency threshold:** In this policy, specify a value in milliseconds that will be applied as the maximum latency threshold. The default value is **30 milliseconds**.
- ❑ **Flash server-side content fetching URL list:** In this policy, specify a list of web URLs for which Flash contents can be downloaded to the server and then sent to the client devices.



Consider using this policy when the Internet connection is not present on the client devices.



- ❑ **Flash URL compatibility list:** In this policy, specify a list of rules for specific web URLs to render Flash content on the client side or the server side, or block any rendering.



The Flash Redirection feature has been strongly improved starting from the XenDesktop Version 5.5.



Audio subsection

- ❑ **Audio over UDP Real-time transport:** In this policy, the values are either **Enabled** or **Disabled**. With this policy, you decide on which protocols to transmit the audio packets: RTP/UDP (policy enabled) or TCP (policy disabled). The choice depends on the kind of audio traffic that will be transmitted. UDP should be better in terms of performance and bandwidth consumption.
- ❑ **Audio Plug N Play:** In this policy, the values are either **Allowed** or **Prohibited**. This feature allows or prohibits the ability to use multiple audio devices.

- ❑ **Audio quality:** In this policy, the values are **Low**, **Medium**, or **High**. These parameters depend on a compromise between the quality of the network connections and the audio level. They cover the low-speed connections, optimized for speech, and high-definition audio cases respectively.
- ❑ **Client audio redirection:** In this policy, the values are **Allowed** or **Prohibited**. Allowing or prohibiting this policy permits applications to use the audio device on the client machine(s).
- ❑ **Client microphone redirection:** In this policy, the values are **Allowed** or **Prohibited**. This policy permits you to map client microphone devices that will be used within a desktop session.



Try to reduce the network and load impact of the multimedia components and devices where high user experience is not required.

Select settings

(All Versions) ▾ Audio ▾

Settings: 14 selected View selected only

✓ ▶ Audio over UDP real-time transport User setting Enabled (Default: Enabled)	Edit Unselect
✓ ▶ Audio Plug N Play User setting Allowed (Default: Allowed)	Edit Unselect
✓ ▶ Audio quality User setting (Default: High - high definition audio)	Edit Unselect
✓ ▶ Client audio redirection User setting Allowed (Default: Allowed)	Edit Unselect
✓ ▶ Client microphone redirection User setting Allowed (Default: Allowed)	Edit Unselect

Auto client reconnect subsection

- ❑ **Auto client reconnect:** In this policy, the values are **Allowed** or **Prohibited**. This policy can be used to specify whether to automatically reconnect a broken connection from a client or not.
- ❑ **Auto client reconnect authentication:** In this policy, the values are either **Do not require authentication** or **Require authentication**. This policy lets you decide whether to let the Citrix infrastructure ask you for the credentials each time you have to redo a login operation.

- ❑ **Auto client reconnect logging:** In this policy, the values are either **Do Not Log auto-reconnect events** or **Log auto-reconnect events**. This policy enables or disables the logging activities in the system log for the reconnection process. In the case of active auto client reconnect, you should also activate its logging.

Bandwidth subsection

- ❑ **Audio redirection bandwidth limit:** In this policy, enter a value in Kbps to set the maximum bandwidth assigned to the playing and recording audio activities.
- ❑ **Audio redirection bandwidth limit percent:** In this policy, enter a maximum percentage value to play and record audio.
- ❑ **Client USB device redirection bandwidth limit:** In this policy, enter a value in Kbps to set the maximum bandwidth assigned to the USB device's redirection.
- ❑ **Client USB device redirection bandwidth limit percent:** In this policy, enter a maximum percentage value for the USB device's redirection.
- ❑ **Clipboard redirection bandwidth limit:** Enter here a value in Kbps to set the maximum bandwidth assigned to the clipboard traffic from the local client to the remote session.
- ❑ **Clipboard redirection bandwidth limit percent:** Enter here a maximum percentage value for the clipboard traffic from the local client to the remote session.
- ❑ **COM port redirection bandwidth limit:** Enter here a value in Kbps to set the maximum bandwidth assigned to the client COM port-redirected traffic.
- ❑ **COM port redirection bandwidth limit percent:** Enter here a maximum percentage value for the client COM port-redirected traffic.
- ❑ **File redirection bandwidth limit:** Enter here a value in Kbps to set the maximum bandwidth assigned to the client drive's redirection.
- ❑ **File redirection bandwidth limit percent:** Enter here a maximum percentage value for the client drive's redirection.
- ❑ **HDX MediaStream Multimedia Acceleration bandwidth limit:** Enter here a value in Kbps to set the maximum bandwidth assigned to the multimedia contents redirected through the HDX MediaStream acceleration.
- ❑ **HDX MediaStream Multimedia Acceleration bandwidth limit percent:** Enter here a maximum percentage value for the multimedia contents redirected through the HDX MediaStream acceleration.
- ❑ **LPT port redirection bandwidth limit:** Enter here a value in Kbps to set the maximum bandwidth assigned to the client LPT port-redirected traffic.
- ❑ **LPT port redirection bandwidth limit percent:** Enter here a maximum percentage value for the client LPT port-redirected traffic.

- ❑ **Overall session bandwidth limit:** Here specify a value in Kbps for the total bandwidth assigned to the client sessions.
- ❑ **Printer redirection bandwidth limit:** Enter here a value in Kbps to set the maximum bandwidth assigned to access a client printer.
- ❑ **Printer redirection bandwidth limit percent:** Enter here a maximum percentage value to access a printer in a client device session.
- ❑ **TWAIN device redirection bandwidth limit:** Enter here a value in Kbps to set the maximum bandwidth assigned to a TWAIN scanner device.
- ❑ **TWAIN device redirection bandwidth limit percent:** Enter here a maximum percentage value to access a TWAIN imaging device.



In the event of enabled policies for both bandwidth limit and bandwidth limit percent, the most restrictive value will be used.



Client Sensors subsection

- ❑ **Allow applications to use the physical location of the client device:** In this policy, the values are **Allowed** or **Prohibited**. With this policy, you can allow the applications to use the physical location of a client device.

Desktop UI subsection

- ❑ **Desktop Composition graphics quality:** In this policy, the values are **Lossless**, **High**, **Medium**, and **Low**. This policy lets you set the quality level for the Desktop Composition redirection. The default value is **Medium**.
- ❑ **Desktop Composition Redirection:** In this policy, the values are either **Enabled** or **Disabled**. This policy permits the use of Desktop Composition from the Virtual Desktop Agent to the client device.



When this policy is enabled, users will obtain a richer user experience. You can't apply it to delivered server OS instances.



- ❑ **Desktop wallpaper:** In this policy, the values are **Allowed** or **Prohibited**. Through this policy, you can permit the users to have the desktop wallpaper in your session. Disable this policy if you want to standardize your desktop deployment.
- ❑ **Menu animation:** In this policy, the values are **Allowed** or **Prohibited**. This policy permits you to have the animated menu of the Microsoft operating systems. The choice depends on what kind of performance you need for your desktops.

- ❑ **View window contents while dragging:** In this policy, the values are **Allowed** or **Prohibited**. If enabled, this policy gives you the ability to see the contents of the entire window during the drag-and-drop activities between windows. Otherwise, you'll see only the window's border.

End User Monitoring subsection

- ❑ **ICA round trip calculation:** In this policy, the values are either **Enabled** or **Disabled**. This feature can enable the calculation of the ICA network traffic time.
- ❑ **ICA round trip calculation interval:** In this policy, enter the time interval (in seconds) for the period of the round trip calculation.
- ❑ **ICA round trip calculations for idle connections:** In this policy, the values are either **Enabled** or **Disabled**. This policy lets you decide whether to enable the round trip calculation for connections which are not creating traffic. Enable this policy only if necessary.

Enhanced Desktop Experience subsection

- ❑ **Enhanced Desktop Experience:** In this policy, the values are **Allowed** or **Prohibited**. This policy is applicable only to the server OS instances, enriching the machine graphical experience in a published desktop session and making the user experience as good as the client device operating system.

File Redirection subsection

- ❑ **Auto connect client drives:** In this policy, the values are **Enabled** or **Disabled**. With this policy, the local drives of your client can be automatically connected at the logon time.
- ❑ **Client drive redirection:** In this policy, the values are **Allowed** or **Prohibited**. With drive redirection, it is possible to permit the saving of files locally on the client machine drives.
- ❑ **Client fixed drives:** In this policy, the values are **Allowed** or **Prohibited**. This policy decides whether or not to permit the reading of data from and saving information to the fixed drives of your client machine.
- ❑ **Client floppy drives:** In this policy, the values are **Allowed** or **Prohibited**. This policy decides whether or not to permit you to read data from and save information to the floppy drives of your client machine. This should be allowed only in the presence of an existing floppy drive; otherwise, it has no value to your infrastructure.
- ❑ **Client network drives:** In this policy, the values are **Allowed** or **Prohibited**. With this policy, you have the possibility to map remote network drives from your client.

- ❑ **Client optical drives:** In this policy, the values are **Allowed** or **Prohibited**. With this policy, you can enable or prevent access to the optical client drives, such as CD-ROM or DVD-ROM.
- ❑ **Client removable drives:** In this policy, the values are **Allowed** or **Prohibited**. This policy allows or prohibits your mapping to read and save removable drives, such as USB keys, from your client.
- ❑ **Host to client redirection:** In this policy, the values are either **Enabled** or **Disabled**. Enabling this policy will associate and execute media content to the client device. If you disable it, all the media will be executed on the server.
- ❑ **Preserve client drive letters:** In this policy, the values are either **Enabled** or **Disabled**. Enabling this policy offers you the possibility to maintain the client drive letters when mapping them in the remote session when possible.
- ❑ **Read-only client drive access:** In this policy, the values are either **Enabled** or **Disabled**. Enabling this policy will not permit you to access in write mode the mapped client drives. By default, this policy is disabled to permit the full drive access. To reduce the impact on the client security, you should enable it; and then modify it when necessary.



These aforementioned are the powerful policies that are used to regulate the access to the physical storage resources. You should configure them to be consistent with your company security policies.

- ❑ **Special folder redirection:** In this policy, the values are **Allowed** or **Prohibited**. Allowing the policy will point the Desktop and Documents users' folders to the clients' directories. In the other case, they will point to the host locations.
- ❑ **Use asynchronous writes:** In this policy, the values are either **Enabled** or **Disabled**. They are disabled by default. This policy lets you choose whether asynchronous data disk writes will be permitted.



You should enable this policy only in the presence of WAN connections and remote connected users.

Graphics subsection

- ❑ **Display memory limit:** In this policy, configure the maximum value in KB that will be assigned to the video buffer for a session. This policy only applies to the deployed desktops of the server OS.
- ❑ **Display mode degrade preference:** In this policy, the values are **Degrade color depth first** or **Degrade resolution first**. Configure a parameter to lower the resolution or the color quality in the case of graphic memory overflow.

- ❑ **Dynamic Windows Preview:** The values are either **Enabled** or **Disabled**. With this policy, you have the ability to decide whether to turn on the high-level preview of the open windows on the screen.
- ❑ **Image caching:** The default values for this policy are either **Enabled** or **Disabled**. With this parameter, you can cache images on the client to obtain a faster response.
- ❑ **Legacy graphics mode:** The default values for this policy are either **Enabled** or **Disabled**. By enabling this policy, you will reduce the quality of the global user experience, improving the ability to scale up resources. But, doing so degrades the graphic quality.
- ❑ **Maximum allowed color depth:** The values for this policy are **8 bits per pixel, 15 bits per pixel, 16 bits per pixel, 24 bits per pixel, and 32 bits per pixel**. This policy permits you to specify the maximum permitted color depth for a session.



Remember that the higher the color depth, the higher is the memory usage.

- ❑ **Notify user when display mode is degraded:** The values for this policy are either **Enabled** or **Disabled**. In case of degraded connections, you can display a pop-up to send a notification to the involved users. This only applies to the server OS instances.
- ❑ **Persistent cache threshold:** In this policy, specify a value in Kbps to cache bitmaps on the client disk. This is used in case of frequently re-used images.
- ❑ **Queuing and tossing:** In this policy, the values are either **Enabled** or **Disabled**. By enabling this policy, you can stop the processing of those images replaced by other pictures.



In the presence of slow or WAN network connections, you should create a separate policy group. This policy group should include features such as reducing the display memory size, configuring the Degrade color depth first policy, activating the image caching, and removing the advanced Windows graphical features.

Keep Alive subsection

- ❑ **ICA keep alive timeout:** In this policy, insert a value in seconds to configure the keep alive timeout for the ICA connections.
- ❑ **ICA keep alives:** This policy includes the values **Do not send ICA keep alive messages** or **Send ICA keep alive messages**. Configure if you want to send the keep-alive signals for the running sessions.

Local App access subsection

- ❑ **Allow local app access:** In this policy, the default values are either **Allowed** or **Prohibited**. This policy decides whether or not to permit the use of **Local Access Apps (LAA)** within your environment.
- ❑ **URL redirection black list:** In this policy, specify a set of web URLs that will be run on the physical client device, out of your VDI resources.
- ❑ **URL redirection white list:** In this policy, specify a set of web URLs that will be run within your assigned VDI resources.



We have already discussed about the LAA in *Chapter 7, Deploying Applications*.



Mobile Experience subsection

- ❑ **Automatic keyboard display:** In this policy, the values are **Allowed** or **Prohibited**. This option automatically decides whether or not to display the display keyboard on mobile devices. This policy is disabled by default.
- ❑ **Launch touch-optimized desktop:** In this policy, the values are **Allowed** or **Prohibited**. This policy will permit you to use or disable the execution of an optimized mobile touchpad version.
- ❑ **Remote the combo box:** In this policy, the values are **Allowed** or **Prohibited**. This policy configures the type of comboboxes that will be used on your device, that is, it allows you to use the Windows combobox version on any device, such as iOS, thereby prohibiting from using the native combobox version.



Aforementioned are the mobile configuration features added in the XenDesktop 7 version.



Multimedia subsection

- ❑ **Limit video quality:** In this policy, the values are **Not Configured**, **Maximum Video Quality 1080p/8.5mbps**, **Maximum Video Quality 720p/4Mbps**, **Maximum Video Quality 480p/720kbps**, **Maximum Video Quality 380p/400kbps**, and **Maximum Video Quality 240p/200kbps**. This policy is used to choose the video quality level of the HDX connections.



The level of the HDX quality should always be configured based on the speed of your network connection.



- ❑ **Multimedia conferencing:** In this policy, the values are **Allowed** or **Prohibited**. With this policy, you can decide whether or not to permit the use of video conferencing applications, in terms of the use of the webcam device and office communicator software support.
- ❑ **Optimization for Windows Media multimedia redirection over WAN:** In this policy, the values are **Allowed** or **Prohibited**. If allowed, this policy permits the windows media content's compression over a WAN connection.
- ❑ **Use GPU for optimizing Windows Media multimedia redirection over WAN:** In this policy, the values are **Allowed** or **Prohibited**. This policy permits the use of GPU to optimize media content elaboration over a WAN connection.
- ❑ **Windows Media client-side content fetching:** In this policy, the values are **Allowed** or **Prohibited**. When allowed, this policy permits the client device to directly stream multimedia contents from the source, bypassing the XenDesktop host server.



In order to reduce the load on the XenDesktop server components, you should allow the **Windows Media client-side content fetching** policy. The **Windows Media Redirection** policy is configured to **Allowed** as a prerequisite to use the client-side content fetching policy.

- ❑ **Windows Media Redirection:** In this policy, the values are **Allowed** or **Prohibited**. This policy lets you decide whether you want to redirect the multimedia execution on the Citrix server(s) and then stream it to the clients.
- ❑ **Windows Media Redirection Buffer Size:** In this policy, insert a value in seconds for the buffer used to deliver multimedia contents to the clients.
- ❑ **Windows Media Redirection Buffer Size Use:** In this policy, the values are either **Enabled** or **Disabled**. This policy lets you decide whether or not to use the previously configured media's buffer size.

Multi-Stream Connections subsection

- ❑ **Audio over UDP:** In this policy, the values are **Allowed** or **Prohibited**. When allowed, this policy permits the opening of a UDP port for a client on which you wish to transfer the audio media.
- ❑ **Audio UDP Port Range:** In this policy, specify a port range for the UDP connections used to stream audio data. The default range is 16,500 to 16,509.
- ❑ **Multi-Port Policy:** This policy configures the traffic shaping to implement the **Quality of Service (QoS)**. You have to specify from two to four ports, and assign them a priority level as well.

Edit Setting

Multi-Port Policy

Applies to: XenDesktop: 5.5, 5.6 Feature Pack 1, 7.0 Server OS, 7.0 Desktop OS

CGP default port: <input type="text" value="Default Port"/>	CGP default port priority: <input type="text" value="High"/>
CGP port1: <input type="text" value="5100"/>	CGP port1 priority: <input type="text" value="Very High"/>
CGP port2: <input type="text" value="5004"/>	CGP port2 priority: <input type="text" value="Medium"/>
CGP port3: <input type="text" value="9100"/>	CGP port3 priority: <input type="text" value="Low"/>
<input type="checkbox"/> Use default value:	

- ❑ **Multi-Stream computer setting:** In this policy, the values are either **Enabled** or **Disabled**. Decide whether or not you want to activate the Multi-Stream ports previously configured on the server side.
- ❑ **Multi-Stream user setting:** In this policy, the values are either **Enabled** or **Disabled**. This policy lets you decide whether or not you want to activate the Multi-Stream feature for specific users.



To be able to use **Multi-Stream user setting**, you need activate the **Multi-Stream computer setting** policy.



Port Redirection subsection

- ❑ **Auto connect client COM ports:** In this policy, the values are either **Enabled** or **Disabled**. If enabled, this policy automatically maps the client COM ports.
- ❑ **Auto connect client LPT ports:** In this policy, the values are either **Enabled** or **Disabled**. If enabled, this policy autoconnects the client LPT ports.
- ❑ **Client COM port redirection:** In this policy, the values are **Allowed** or **Prohibited**. This policy configures the COM port redirection between the client and the remote session.
- ❑ **Client LPT port redirection:** In this policy, the values are **Allowed** or **Prohibited**. This policy configures the LPT port redirection between the client and the remote session.



You have to enable the necessary ports only, so disable the policies for the missing COM or LPT.

Security subsection

- ❑ **Secure ICA minimum encryption level:** In this policy, the values are **Basic**, **RC5 (128 bit) logon only**, **RC5 (40 bit)**, **RC5 (56 bit)**, and **RC5 (128 bit)**. This configuration permits the assigning of an encryption level to the data sent between the client and the server during a XenDesktop session. This policy only applies to the server OS.



You can find an explanation about the RC5 encryption algorithm at <http://en.wikipedia.org/wiki/RC5>.

Server limits subsection

- ❑ **Server idle timer interval:** In this policy, specify a value in milliseconds to set the interval for which it will keep the idle sessions active (no input from users). This policy only applies to the server OS instances.

Session limits subsection

- ❑ **Concurrent logon limit:** In this policy, specify a numeric value to set the maximum number of connections that can be made by a single user. This policy only applies to the server OS instances.
- ❑ **Disconnected session timer:** In this policy, the values are either **Enabled** or **Disabled**. This policy enables or disables the counter used to migrate from a locked workstation to a logged off session. For security reasons, you should enable the automatic logoff of the idle sessions.



Based on the **Disconnected session timer** parameter, we have got the SmoothRoaming feature. This is a term to make the users' sessions move from one end device to another end device. Smooth roaming is based on disconnected session time, and the time in between the movement from a device to another will always only be less than the configured disconnected time.

- ❑ **Disconnected session timer interval:** In this policy, insert a value in minutes, which will be used as a counter reference value to log off locked workstations. Base this parameter on a real inactivity time for your company employees.

- ❑ **Session connection timer:** In this policy, the values are either **Enabled** or **Disabled**. This policy will decide whether or not to use a timer to measure the duration of active connections from clients to the remote sessions.
- ❑ **Session connection timer interval:** This policy specifies the maximum duration for an uninterrupted connection between a user device and a client. The maximum value is 24 hours (1,440 minutes).
- ❑ **Session idle timer:** In this policy, the values are either **Enabled** or **Disabled**. If enabled, this policy will disconnect a client's session after a certain time of inactivity. The value is specified in the next policy.
- ❑ **Session idle timer interval:** This policy specifies the maximum duration for an idle connection (no input) between a user device and a client. The maximum value is 24 hours (1,440 minutes).

Session Reliability subsection

- ❑ **Session reliability connections:** In this policy, the values are **Allowed** or **Prohibited**. By enabling this policy, you are permitting the sessions to remain active in the event of network problems and permitting the users to see the content of published desktops or applications like a screenshot of the last state, while the network issues are being restored and the session is kept active.
- ❑ **Session reliability port number:** In this policy, specify the port used by ICA to check the reliability of incoming connections. The default port is 2598.
- ❑ **Session reliability timeout:** In this policy, specify a value in seconds used by the session reliability manager component to wait for a client reconnection.



You cannot enable the **ICA keep alives** policy if the **Session Reliability** policies has been activated. They can't be enabled together.

Time zone control subsection

- ❑ **Estimate local time for legacy clients:** In this policy, the values are either **Enabled** or **Disabled**. If enabled, this policy will try to estimate the client time zone in the event of a lack of information. This can be applied only to the server OS.
- ❑ **Use local time of client:** In this policy, the values are **Use server time zone** or **Use client time zone**. Based on the policy configuration, the time zone for a XenDesktop session will be based on the time zone configured by the client or server.

TWAIN Devices

- ❑ **Client TWAIN device redirection:** In this policy, the values are **Allowed** or **Prohibited**. If enabled, this policy permits mapping with the existing TWAIN image devices, for example, as scanners.
- ❑ **TWAIN compression level:** In this policy, the values are **None**, **Low**, **Medium**, or **High**. With this policy, you can specify the compression level for media files that are transferred from client to server.

Visual Display subsection

- ❑ **Extra color compression:** In this policy, the values are either **Enabled** or **Disabled**. If enabled, the global image quality level will be reduced to obtain a faster response.
- ❑ **Extra color compression threshold:** Insert here a value in Kbps to specify a threshold for the color compression execution.
- ❑ **Heavyweight compression:** In this policy, the values are either **Enabled** or **Disabled**. Based on a CPU-consuming algorithm, if enabled, this policy will apply a progressive data compression, reducing the global bandwidth. It can be used by the Citrix Receiver only.
- ❑ **Lossy compression level:** In this policy, the values are **None**, **Low**, **Medium**, or **High**. This policy should be used only when the quality level for the images is not important because of the compression applied to the graphical data.
- ❑ **Lossy compression threshold value:** In this policy, insert a value in Kbps to specify a threshold for the lossy compression policy application.
- ❑ **Minimum image quality:** In this policy, the values are **Low**, **Normal**, **High**, **Very High**, or **Ultra High**. This policy specifies the quality level that will be applied to the displayed images. The higher the level, the higher is the resource consumption.
- ❑ **Moving image compression:** In this policy, the values are either **Enabled** or **Disabled**. When enabled, this policy activates the adaptive display feature, which has the ability to automatically adjust the quality levels of graphics based on the available bandwidth.
- ❑ **Progressive compression level:** In this policy, the values are **None**, **Low**, **Medium**, **High**, **Very High**, or **Ultra High**. This policy sets a lossy compression-related image-quality level, starting from a less-detailed and faster display.



As a mandatory configuration, the value of **Progressive compression level** must be higher than the **Lossy compression level** policy.

- ❑ **Progressive compression threshold value:** In this policy, insert a value in Kbps to specify a threshold for the progressive compression policy application.

- ❑ **Target frame rate:** In this policy, specify a value, in terms of **frame per second (FPS)**, as the maximum number of frames sent to a client in a second.
- ❑ **Target minimum frame rate:** With this parameter, XenDesktop will try to avoid going under the FPS parameter in presence of bandwidth problems.
- ❑ **Visual quality:** In this policy, the values are **Low, Medium, High, Build to Lossless**, or **Always Lossless**. These parameters configure the quality level of the image visualization; the higher the level, the higher is the bandwidth usage. This policy only applies to Desktop OS.



The **Always Lossless** option gives more importance to the image quality, and the **Build to Lossless** parameter decreases or increases the image quality based on the network and resource usage level.

WebSockets subsection

- ❑ **WebSockets connections:** In this policy, the values are **Allowed** or **Prohibited**. If permitted, this policy activates a dual channel communication between a web application and the XenDesktop server, based on the WebSocket protocol.
- ❑ **WebSockets port number:** This policy permits you to specify the WebSocket protocol's port number for the incoming connections. The default value is 8008.
- ❑ **WebSockets trusted origin server list:** With this policy, it's possible to specify a list of trusted server URLs as valid WebSockets platforms. By default, all the servers are included in this list by using a wildcard (*).

WebSockets trusted origin server list

Applies to: XenDesktop: 7.0 Server OS, 7.0 Desktop OS

Value:	<code>https://192.168.*</code>
<input type="checkbox"/> Use default value: *	
▼ Details and related settings <hr/> Comma-separated list of trusted origin servers expressed as URLs with the option of using wildcards.	

Load Management section

- ❑ **Concurrent logons tolerance:** In this policy, the values are either **Enabled** or **Disabled**. When enabled, this policy permits you to specify the number of maximum concurrent logons for a XenDesktop server site. This policy can be applied only to the server OS.
- ❑ **CPU usage:** In this policy, the values are either **Enabled** or **Disabled**. When enabled, this policy configures the percentage CPU usage threshold that is considered as the maximum load for the XenDesktop server. This policy can be applied only to the server OS.
- ❑ **CPU usage excluded process priority:** In this policy, the values are either **Enabled** or **Disabled**. This policy allows you to enable or disable the consideration of the global server CPU usage for the system background processes, including their resource consumption in the global load calculation when this policy is disabled. This policy can be applied only to the server OS.
- ❑ **Disk usage:** In this policy, the values are either **Enabled** or **Disabled**. When this policy is enabled, it lets you configure the disk queue length at which you consider the global disk usage at 75 percent of the load. This policy can be applied only to the server OS.



This policy permits you to understand the disk bottleneck situations. This usually happens when the disk queue length is greater than the number of disk spindles multiplied by two.

- ❑ **Maximum number of sessions:** In this policy, the values are either **Enabled** or **Disabled**. By enabling this policy, you can specify the maximum number of sessions per single XenDesktop server. This policy can be applied only to the server OS.
- ❑ **Memory usage:** In this policy, the values are either **Enabled** or **Disabled**. By enabling this policy, you can configure the memory usage percentage value that is considered as the full load for the server. This policy can be applied only to the server OS.
- ❑ **Memory usage base load:** In this policy, the values are either **Enabled** or **Disabled**. By enabling this policy, you can tune the zero load parameter (in MB) that will be used as threshold for the server load calculation. This policy can be applied only to the Server OS.

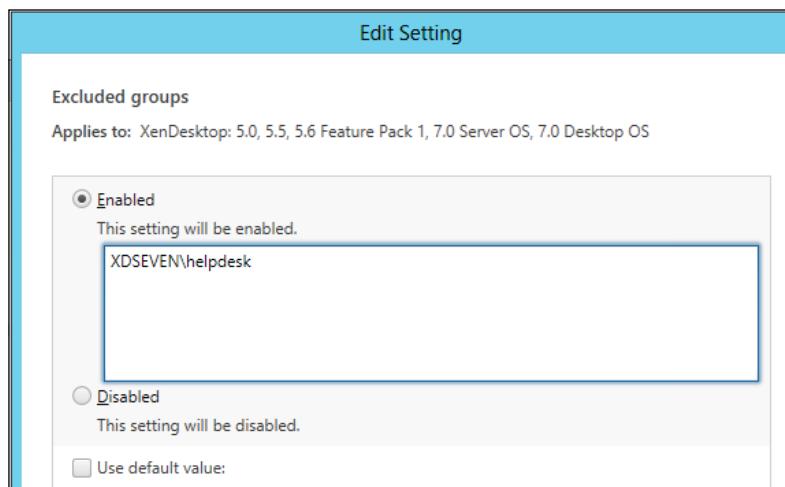
The subsections included in the Profile Management section are discussed as follows:

Advanced settings subsection

- ❑ **Disable automatic configuration:** In this policy, the values are either **Enabled** or **Disabled**. With this policy, you can decide whether or not to activate the automatic configuration for the profile management, based on the environment configuration.
- ❑ **Log off user if a problem is encountered:** In this policy, the values are either **Enabled** or **Disabled**. If you will enable this policy, the user will be prompted with an alert in case of problems during the log on phase, and then he/she will be disconnected. If disabled, a temporary profile will be assigned to the user.
- ❑ **Number of retries when accessing locked files:** In this policy, specify a numeric value to retry accessing files that are locked.
- ❑ **Process internet cookie files on logoff:** In this policy, the values are either **Enabled** or **Disabled**. When enabled, this policy removes unnecessary web cookies after a session logoff.

Basic settings subsection

- ❑ **Active write back:** In this policy, the values are either **Enabled** or **Disabled**. By enabling this policy, all the modified files and directories will be synchronized in the middle of a session with the central profile store, before the user's logoff.
- ❑ **Enable profile management:** In this policy, the values are **Enabled** or **Disabled**. This policy lets you decide whether or not you want to activate the logon and logoff processes' management for Citrix Profile Management.
- ❑ **Excluded groups:** In this policy, the values are either **Enabled** or **Disabled**. When enabled, this policy permits you to continue processing, but excludes specific domain groups from the profile management.



- ❑ **Offline profile support:** In this policy, the values are either **Enabled** or **Disabled**. Enable this policy to permit the use of profiles even when disconnected from the network.
- ❑ **Path to user store:** In this policy, the values are either **Enabled** or **Disabled**. To use the Citrix Profile Management, enable this policy and specify the network path on which profiles are located.



We have discussed about the Citrix Profile Management and the path to the user store in the *Using Citrix Profile Management 5.0* recipe in *Chapter 4, User Experience – Planning and Configuring*.

- ❑ **Process logons of local administrators:** In this policy, the values are either **Enabled** or **Disabled**. This policy decides whether or not to process the profile members of the local administrator's machine group.
- ❑ **Processed groups:** In this policy, the values are either **Enabled** or **Disabled**. When enabled, this policy permits you to specify the domain groups that must be processed by the Citrix Profile Manager.

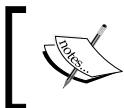
Cross-Platform settings subsection

- ❑ **Cross-platforms settings user groups:** In this policy, the values are either **Enabled** or **Disabled**. If enabled, the cross-platform parameter of Citrix Profile Management will be applied only to the specified domain groups.
- ❑ **Enable Cross-platforms settings:** In this policy, the values are either **Enabled** or **Disabled**. With this policy, you can turn on or turn off the cross-platform option for the Citrix Profile Management software.
- ❑ **Path to cross-platforms definitions:** In this policy, the values are either **Enabled** or **Disabled**. If the policy is enabled, you have to specify a valid network path on which you will be locating the cross-platform definition files.
- ❑ **Path to cross-platforms settings store:** In this policy, the values are either **Enabled** or **Disabled**. If you enable this policy, you have to specify a valid network path on which you will be saving the user's cross-platform settings.

File system subsection

- ❑ **Directories to synchronize:** In this policy, the values are either **Enabled** or **Disabled**. Enable this policy and specify a list of folders if you want to activate sync for specific additional directories other than the user profiles.
- ❑ **Exclusion list – directories:** In this policy, the values are either **Enabled** or **Disabled**. Enable this policy and specify a list of folders that will be excluded during the profile synchronization activities.

- ❑ **Exclusion list – files:** In this policy, the values are either **Enabled** or **Disabled**. Enable this policy and specify a list of files that will be excluded during the profile synchronization activities.
- ❑ **Files to synchronize:** In this policy, the values are either **Enabled** or **Disabled**. Enable this policy and specify a list of files if you want to activate sync for specific additional files other than the user profiles.
- ❑ **Folders to mirror:** In this policy, the values are either **Enabled** or **Disabled**. Enable this policy and list a set of folders that will be replicated in mirror mode.



This policy is useful when critical profile data needs to have more than one existing file.



Folder redirection subsection

- ❑ **AppData (Roaming) path:** In this policy, the values are either **Enabled** or **Disabled**. If enabled, this policy will let you specify a network path on which you want to redirect the AppData folders. If disabled, the specified folder won't be redirected. This is for roaming profile configurations.
- ❑ **Contacts path:** In this policy, the values are either **Enabled** or **Disabled**. Enable this policy and specify a network location path on which you want to redirect the Contacts directory. If disabled, the specified folder won't be redirected.
- ❑ **Desktop path:** In this policy, the values are either **Enabled** or **Disabled**. Enable this policy and specify a network location path on which you want to redirect the Desktop directory. If disabled, the specified folder won't be redirected.
- ❑ **Documents path:** In this policy, the values are either **Enabled** or **Disabled**. Enable this policy and specify a network location path on which you want to redirect the Documents directory. If disabled, the specified folder won't be redirected.
- ❑ **Download path:** In this policy, the values are either **Enabled** or **Disabled**. Enable this policy and specify a network location path on which you want to redirect the Download directory. If disabled, the specified folder won't be redirected.
- ❑ **Favorites path:** In this policy, the values are either **Enabled** or **Disabled**. Enable this policy and specify a network location path on which you want to redirect the Favorites directory. If disabled, the specified folder won't be redirected.

- ❑ **Grant administrator access:** In this policy, the values are either **Enabled** or **Disabled**. With this policy, you can configure the ability of administrator users to access the redirected folder's contents. By default, only users can access their own redirected folders.
- ❑ **Include domain name:** In this policy, the values are either **Enabled** or **Disabled**. This policy permits including (when enabled) the %userdomain% variable in the UNC path.
- ❑ **Links path:** In this policy, the values are either **Enabled** or **Disabled**. Enable this policy and specify a network location path on which you want to redirect the `Links` directory. If disabled, the specified folder won't be redirected.
- ❑ **Music path:** In this policy, the values are either **Enabled** or **Disabled**. Enable this policy and specify a network location path on which you want to redirect the `Music` directory. If disabled, the specified folder won't be redirected.
- ❑ **Pictures path:** In this policy, the values are either **Enabled** or **Disabled**. Enable this policy and specify a network location path on which you want to redirect the `Pictures` directory. If disabled, the specified folder won't be redirected.
- ❑ **Redirection settings for AppData (Roaming):** In this policy, you can specify the way to redirect the `AppData` folder for configured roaming profiles.
- ❑ **Redirection settings for Contacts:** In this policy, you can specify the way to redirect the `Contacts` folder for configured roaming profiles.
- ❑ **Redirection settings for Desktop:** In this policy, you can specify the way to redirect the `Desktop` folder for configured roaming profiles.
- ❑ **Redirection settings for Documents:** In this policy, you can specify the way to redirect the `Documents` folder for configured roaming profiles.
- ❑ **Redirection settings for Downloads:** In this policy, you can specify the way to redirect the `Downloads` folder for configured roaming profiles.
- ❑ **Redirection settings for Favorites:** In this policy, you can specify the way to redirect the `Favorites` folder for configured roaming profiles.
- ❑ **Redirection settings for Links:** In this policy, you can specify the way to redirect the `Links` folder for configured roaming profiles.
- ❑ **Redirection settings for Music:** In this policy, you can specify the way to redirect the `Music` folder for configured roaming profiles.
- ❑ **Redirection settings for Pictures:** In this policy, you can specify the way to redirect the `Pictures` folder for configured roaming profiles.
- ❑ **Redirection settings for Saved Games:** In this policy, you can specify the way to redirect the `Saved Games` folder for configured roaming profiles.
- ❑ **Redirection settings for Searches:** In this policy, you can specify the way to redirect the `Searches` folder for configured roaming profiles.

- ❑ **Redirection settings for Start Menu:** In this policy, you can specify the way to redirect the Start Menu folder for configured roaming profiles.
- ❑ **Redirection settings for Videos:** In this policy, you can specify the way to redirect the Videos folder for configured roaming profiles.



By default, all the redirection settings policies are configured as **Redirect to the following UNC path**. You can specify a particular path in the next set of policies.

- ❑ **Saved Games path:** In this policy, the values are either **Enabled** or **Disabled**. Enable this policy and specify a network location path on which you want to redirect the Saved Games directory. If disabled, the specified folder won't be redirected.
- ❑ **Searches path:** In this policy, the values are either **Enabled** or **Disabled**. Enable this policy and specify a network location path on which you want to redirect the Searches directory. If disabled, the specified folder won't be redirected.
- ❑ **Start Menu path:** In this policy, the values are either **Enabled** or **Disabled**. Enable this policy and specify a network location path on which you want to redirect the Start Menu directory. If disabled, the specified folder won't be redirected.
- ❑ **Videos path:** In this policy, the values are either **Enabled** or **Disabled**. Enable this policy and specify a network location path on which you want to redirect the Videos directory. If disabled, the specified folder won't be redirected.



Later in this chapter, we will discuss about the logging policies applied to the XenDesktop infrastructure.

Profile Handling subsection

- ❑ **Delay before deleting cached profiles:** Configure a value, in seconds, as the delay for the cached profile deletion after a session logoff.
- ❑ **Delete locally cached profiles on logoff:** In this policy, the values are either **Enabled** or **Disabled**. With this policy, you can decide whether to delete the cached profile after a session has been logged off.



The **Delay before deleting cached profiles** policy requires the activation of the **Delete locally cached profiles on logoff** policy.

- ❑ **Local profiles conflict handling:** This policy manages the profile management action in case of conflict between the centralized profile and the Windows local profile. You can configure **Use local profile**, **Delete local profile**, or **Rename local profile**.

 Choosing to rename the local profile permits you to first back it up and then use the centralized profiles. This is useful for rollback actions.

- ❑ **Migration of existing profiles:** In this policy, the values are **Local and Roaming**, **Local**, **Roaming**, or **None**. With this policy, it is possible to migrate the existing profiles (local or roaming) to the central user store, after the first user logs on.
- ❑ **Path to the template profile:** In this policy, the values are either **Enabled** or **Disabled**. When enabled, this policy allows you to specify a network path on which you will first save and then locate a user profile template that will be used for any profile-creation operation.
- ❑ **Template profile overrides local profile:** In this policy, the values are either **Enabled** or **Disabled**. Enabling or disabling this policy will create new user profiles from the centralized template (first case) or from the default user profile—the local profile—on the computer, which is used for the first logon (second case).
- ❑ **Template profile overrides roaming profile:** In this the values are either **Enabled** or **Disabled**. Enabling or disabling this policy will create new user profiles from the centralized template (first case) or from the default user profile—Microsoft Roaming profile—on the computer, which is used for the first logon (second case).

Registry subsection

- ❑ **Exclusion list:** In this policy, the values are either **Enabled** or **Disabled**. Enabling this policy will let you specify a set of registry keys in the **HKEY_CURRENT_USER** section, which will be ignored during the logon phase.
- ❑ **Inclusion list:** In this policy, the values are either **Enabled** or **Disabled**. Enabling this policy will let you specify a set of registry keys in the **HKEY_CURRENT_USER** section, which will be processed during the logon phase.

 You have to understand that with this latest policy enabled, only the listed registry keys will be processed at the logon phase.

Streamed user profiles subsection

- ❑ **Always cache:** In this policy, the values are either **Enabled** or **Disabled**. With this policy, you can decide whether you want to always cache data with streamed profiles. If enabled, the global limit of the cached files will be lower in size. Assign a value to the cache area size, which will be associated to the policy.
- ❑ **Profile streaming:** In this policy, the values are either **Enabled** or **Disabled**. On enabling this policy, the streamed user profiles will be synchronized on the local computer only when needed. Registry keys are always cached, and files and folder are cached only when accessed by users.
- ❑ **Streamed user profile groups:** In this policy, the values are either **Enabled** or **Disabled**. If enabled, this policy will permit you to insert a list of domain groups containing users that will be configured as streamed profiles.
- ❑ **Timeout for pending area lock files (days):** Assign a value (in days) after which the users locked, pending files are rolled back to the user store, instead of being written to the destination server.

Receiver section

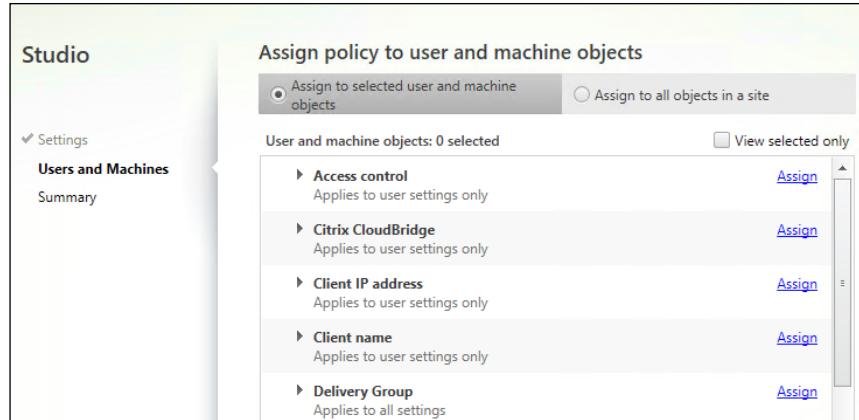
- ❑ **Storefront account list:** In this policy, insert a list of StoreFront-configured locations with the syntax `StoreName;StoreURL;StoreState (Value=On/Off);StoreDescription`.

 A configuration example for the previous policy could be found at `MyCompany;https://companysf01.xdseven.local/Citrix/Store/discovery;On;"Company store"`.

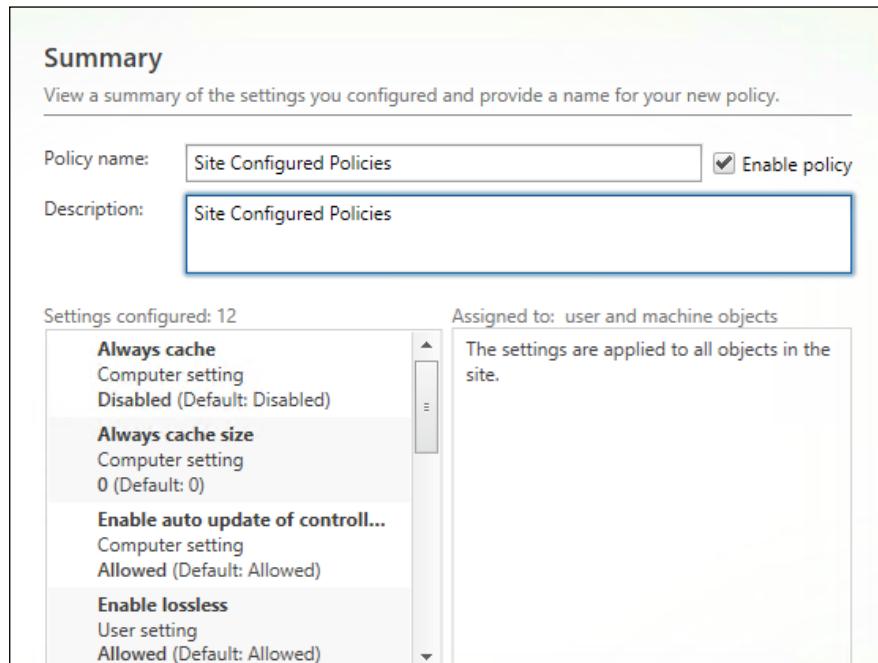
Virtual Delivery Agent Settings section

- ❑ **Enable auto update of controllers:** In this policy, the values are either **Enabled** or **Disabled**. If this policy is enabled, you can apply a list of XenDesktop Controllers to the initial bootstrap connection; if disabled, you will have to manage them manually.
- ❑ **Enable lossless:** In this policy, the values are either **Enabled** or **Disabled**. This policy allows or prohibits the use of lossless codec.
- ❑ **HDX3DPro quality settings:** Configure the minimum and maximum quality level for the 3D-Pro codec. The permitted values are between zero and one hundred, and the maximum level must be greater than the minimum.

5. After configuring all the policies, click on the **Next** button to continue.
6. In the **Users and Machines** section, choose whether you want to apply the configured policies to specific users and/or computers, or assign them to all the site's objects. After completing these steps, click on the **Next** button.



7. In the **Summary** section, assign a name and an optional description to the configured group of policies. Then, flag the **Enable** policy option and click on **Finish** to complete the procedure.



How it works...

The Citrix XenDesktop policies permit you to apply specific configurations based on the corporate requirements. These configurations must be strongly oriented to the performance and security optimization.

For this reason, you should consider generating different sets of policies and apply them to different virtual desktop's configurations.

Using **ICA settings** you are able to configure the standard ICA port on which you are listening, and the relative connection goes into timeout. It's possible to decide whether to automatically reconnect a broken session to a client. There is the **Auto client reconnect** policy. Enabling this policy could be right in some cases, especially when you have interrupted an important working session. But on the other hand, you could have an uncalculated waste of resources because the Citrix broker could run a new session in the presence of issues with the session cookies.

With the **ICA round trip** policies, you can monitor the response time for the operations made by the users. This data permits you to understand the responsiveness of your Citrix infrastructure.

Moreover, you could also apply remediation to the configuration, especially for those policies which involve graphics components. You could size the display memory and the image caching area, or turn on or off specific Windows advanced graphical features, such as the **Dynamic Windows Preview (DWP)**.



With the **Queuing and tossing** policy active, you could have the problem of lost frames when reproducing animations.

The **Windows media redirection** policy optimizes the reproduction of multimedia objects. By applying the correct sizing to its buffer size, you should obtain evident improvements in the streaming and reproduction operations. So, you should consider disabling this policy, demanding the processing of audio and video to the clients only when you can see no particular benefits.

Another important feature offered by this policies area is the QoS implementation. You can enable the **Multi-Stream Connections** configurations and apply the traffic priority levels to them, permitting precedence and more bandwidth to the traffic that is considered more critical than others.



The Multi-Stream policies for the QoS can be considered a less powerful alternative to the Citrix CloudBridge platform. You could also use them together for a better and more powerful user experience.

Other important configurations are, for instance, the Adobe Flash contents processing that allows you to decide whether you want to activate the compatibility with the oldest version of this software and whether you want to elaborate the Flash multimedia objects on the user's clients or on the Citrix servers. Moreover, you can configure the **Audio** settings, such as Audio and Microphone client redirection (in sense of using the local device resources), the **Desktop** settings (such as desktop wallpapers and so on), or the HDX and HDX 3D-Pro protocol quality settings.



Be careful when applying policies for the desktop graphical settings. Remember to be consistent with the master image template configurations performed in *Chapter 3, Master Image Configuration and Tuning* and *Chapter 4, User Experience – Planning and Configuring*.

To optimize the information transmission for the desktops, the **Bandwidth** policy is extremely important. With this policy, you can assign (in form of maximum Kbps or percentage) the values such as Audio, USB, Clipboard, COM and LPT ports, and File redirection for the traffic types. These configurations require a good analysis of the traffic levels and their priorities within your organization.

The last great configuration is the redirection of the client drives to the remote Citrix sessions. In fact, you can activate the mount (automatic or not) and the users' rights (read only or read and write) on the client drives, which can be removable drives such as CD-ROM, DVD-ROM, or removable USB devices and fixed drives such as the client-device operating system root. This option gives you the flexibility to transfer information from the local device to the XenDesktop instance, through the use of the Virtual Desktop Agent properly configured. In order to save the bandwidth, you should consider deactivating all the redirects that are not really needed.



This last device policy could make your infrastructure more secure, thanks to the use of the USB device redirection rules. In fact, using this policy, you could permit the use of only those USB keys that are approved by your company, prohibiting any other device that is not compliant with the policies.

In this version of XenDesktop, the **Mobile Experience** policies are also really important. In fact, we have seen that we are able to configure and use an optimized version of the touch for devices such as tablets or smartphones, enriching the user experience on this category of devices.

There's more...

With XenDesktop 7, you can not only configure the policy on your own, but you have the ability to use the following existing tools which will help you during the configuration and the optimization of the site's parameters:

Policy templates

With this feature, you can use a preconfigured group of policies that should be applied in one of the following existing categories:

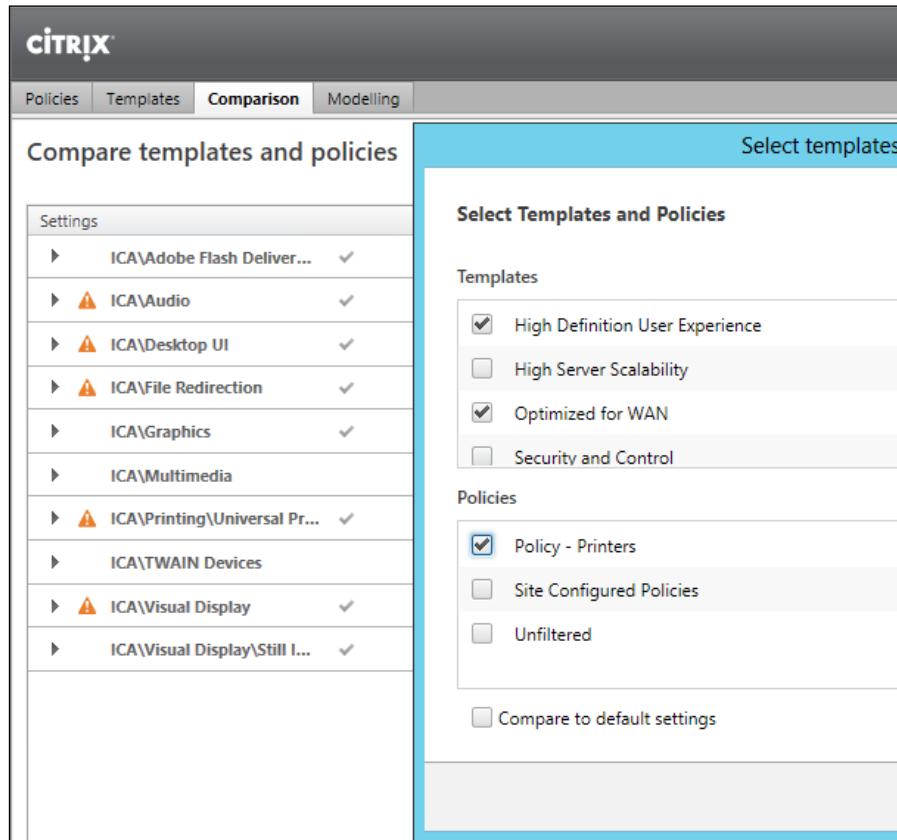
- ▶ **High Definition User Experience:** These preconfigured policies are for high-quality graphics, audio, and video applications, in the presence of a high-level network and elaborate resources.
- ▶ **High Server Scalability:** These preconfigured policies are fit for applications on which resource usage and user experience must be balanced. The global experience level can be improved by scaling up the number of XenDesktop Controller servers.
- ▶ **Optimized for WAN:** These preconfigured policies are for remote workers with offices connected over a WAN. The template is made to optimize bandwidth usage.
- ▶ **Security and Control:** This preconfigured template disables most of the remote user devices, such as USB peripherals and fixed drives, or client-side media rendering. This improves the global security level, but also degrades the available bandwidth because of the high network usage.



You can convert your own customized policies in the template to re-use them for future purposes. In the **Policy** section, click on the **Save as Template** link on the right-hand side menu.

Policy Comparison

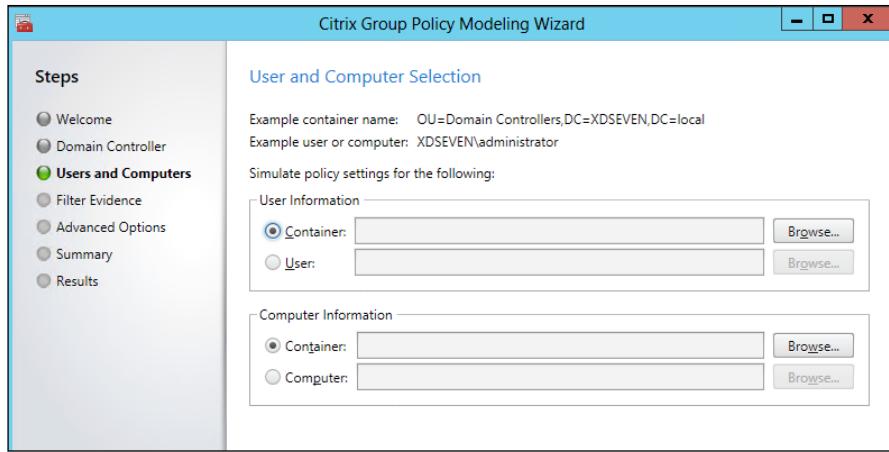
With this feature, you can compare two or more templates and/or policies in order to verify the options currently applied. You can also check for eventually redundant configurations.



Policy Modelling

To verify the effective running of and the policies that are applied to your VDI infrastructure, there's a tool inside the **HDX Policy** menu that performs this task, **Citrix Group Policy Modeling Wizard**. This tool performs a simulation for the policy applications, returning you a report with the current configuration. This is something similar to the Microsoft Windows Domain Group Policy Results.

The simulations apply to one or all the **Domain Controller** options configured within your domain, being able to test the application to specific user or computer objects, including organizational units containing them.



Moreover, you can apply filters based on **Client IP address**, **Client name** and the type of machine (**Private Desktop** or **Shared Desktop** and/or **Private Application** or **Shared Application**), or you can apply the simulation to a specific **Desktop group**.

In the **Advanced Options** section, you can simulate **Slow network connections** and/or **Loopback processing** (basically, a policy application based only on the computer object locations, instead of both the user and computer object positions) for a configured XenDesktop site.

After running the policy application test, you can check the results by right-clicking on the generated report name and selecting the **View Report** option.

Citrix Computer Policies		
Filter Results		
Setting	Value	Winning GPO / Citrix Policy
Virtual IP adapter address filtering	Disabled	Machine Site Settings/Site Configured Policies
Enable auto update of controllers	Allowed	Machine Site Settings/Site Configured Policies
Exclusion list		Machine Site Settings/Site Configured Policies
Inclusion list		Machine Site Settings/Site Configured Policies

Citrix User Policies		
Filter Results		
Setting	Value	Winning GPO / Citrix Policy
HDX3DPro quality settings	6553600	User Site Settings/Site Configured Policies
Enable lossless	Allowed	User Site Settings/Site Configured Policies
Receiver\Storefronts		User Site Settings/Site Configured Policies
Default printer	Disabled	User Site Settings/Policy - Printers
Printer driver mapping and compatibility	Disabled	User Site Settings/Policy - Printers
Session printers	Disabled	User Site Settings/Policy - Printers
Universal driver preference	Disabled	User Site Settings/Policy - Printers

These are extremely powerful tools when you have to verify unexpected behaviors of your desktop instances or user rights because of incorrect policy applications.

See also

- ▶ The *Installing and configuring the Master Image policies* recipe in Chapter 3, *Master Image Configuration and Tuning*

Installing and configuring Citrix® NetScaler Gateway 10.1

Performance tuning is not the only optimization work that is performed on the IT infrastructures. The IT staff should focus their attention on the security features as well. These concepts need particular care in infrastructures where access is granted to the users' resources. For the Citrix VDI architectures, the Citrix NetScaler Gateway permits a secure gateway in front of your connection manager, the Citrix StoreFront platform.

In this chapter, we're going to discuss how to implement the virtual appliance version of the NetScaler Gateway.

Getting ready

In order to perform the configuration of Citrix NetScaler Gateway, first of all you need to download it from your MyCitrix account. Go to the **Download** area by clicking on **NetScaler Access Gateway | Virtual Appliances**, and now download the appropriate VPX version for your hypervisor (the supported systems are Citrix XenServer, VMware ESX/ESXi, and Microsoft Hyper-V). After the download is complete, you have to import it into your virtual infrastructure.



When importing the Virtual Appliance, you should assign two different networks to the Virtual Appliance's virtual network cards during the configuration steps—one pointing to the private network and the other configured for the public network.

Moreover, you need to allocate a number of licenses equal to the number of your XenDesktop users. As seen in the first chapter, you have to generate a license file and associate it to the NetScaler Gateway hostname Virtual Appliance.



You can find information about the NetScaler Gateway licensing model at <http://support.citrix.com/proddocs/topic/netscaler-gateway-101/ng-license-platform-universal-con.html>.

How to do it...

In this section, we will perform the tasks to configure the Citrix Access Gateway virtual appliance:

1. Connect to the console of the configured Access Gateway virtual machine, and configure the following network parameters: IPv4 address, Netmask, and Gateway IPv4 address. After completing these steps, select the fourth option and then click on **Save and quit**.

```
Your identification has been saved in /nsconfig/ssh/ssh_host_dsa_key.
Your public key has been saved in /nsconfig/ssh/ssh_host_dsa_key.pub.
The key fingerprint is:
34:01:49:89:35:0e:7d:f9:ef:f6:56:ec:b7:3c:ec:40 root@ns
.
Machdep.cpu_idle_hlt: 0 -> 1
Start daemons: syslogd Oct  7 15:14:15 <kern.info> ns syslogd: kernel boot file
is /flash/ns-10.0-70.7
inetd cron httpd monit sshd vmware_guestd .

!There is no ns.conf in the /nsconfig!

Start Netscaler software
tput: no terminal type specified and no TERM environmental variable.
No machine id

Enter NetScaler's IPv4 address []: █
```

2. Open a compatible web browser. In the address bar, type the address that was previously assigned to the virtual appliance.

3. Enter the default web portal credentials (nsroot/nsroot), select **NetScaler Gateway** as **Deployment Type**, and click on the **Login** button to continue.

The screenshot shows the Citrix login interface. At the top is the Citrix logo. Below it is a 'Login' section with 'User Name' and 'Password' fields, both containing 'nsroot'. Underneath is a 'Deployment Type' dropdown menu. The options listed are 'NetScaler Gateway', 'NetScaler ADC', 'NetScaler Gateway' (which is selected and highlighted in blue), 'XenMobile MDM', and 'CloudBridge Connector'. A 'Login' button is located at the bottom right of the dropdown menu.

4. After the first login, configure the network parameters that are required by the NetScaler Gateway (management address, subnet IP address, hostname, and so on). After completing these steps, click on **Continue**.

The screenshot shows the 'System' configuration page. It includes fields for 'NetScaler IP Address*', 'Subnet IP Address*', 'Netmask*', 'Hostname', 'DNS (IP Address)', and 'Time Zone*'. The 'Time Zone*' field is set to 'GMT+01:00-CET-Europe/Rome'. There is also a checkbox for 'Change Administrator Password' and a 'Continue' button at the bottom.

5. In the left-hand side menu, expand the **System** section, and click on the **Licenses** link.
6. In the **Licenses** main menu, click on the **Manage Licenses** option. Then, in the **Update Licenses** section, click on the **Upload License Files** radio button. Then, click on the **Browse** button and search for the license file available for you. After completing these steps, click on the **OK** button. On the new prompted window, flag the **Save configuration** option and accept to restart the virtual appliance.

Manage Licenses

Below is the list of license files present on the system.

No Licenses.

Update Licenses

- Use Hardware Serial Number (HE2H81UJ47)
- Use License Activation Code
- Upload License Files

Browse

7. Click on the **Home** button on the top menu toolbar, and then select the **Get Started** button in the **Wizard** menu.
8. In the **NetScaler Gateway Settings** screen, assign a name to the virtual server name, an IP address, and configure the port as **443** (secure connection). After completing these steps, click on **Continue**.



You can select the option **Redirect requests from port 80 to secure port*** in order to force the HTTP requests to be redirected to the HTTPS.

NetScaler Gateway Settings

Name*	VPX-VServer
IP Address*	192 . 168 . 110 . 88
Port*	443
<input type="checkbox"/> Redirect requests from port 80 to secure port*	
Continue	Cancel

9. In the **Certificate** section, choose if you want to install a valid certificate, wherever available, or use a self-signed testing certificate. In the second case, you have to insert a valid NetScaler Gateway FQDN for the certificate. Click on the **Continue** button to proceed.

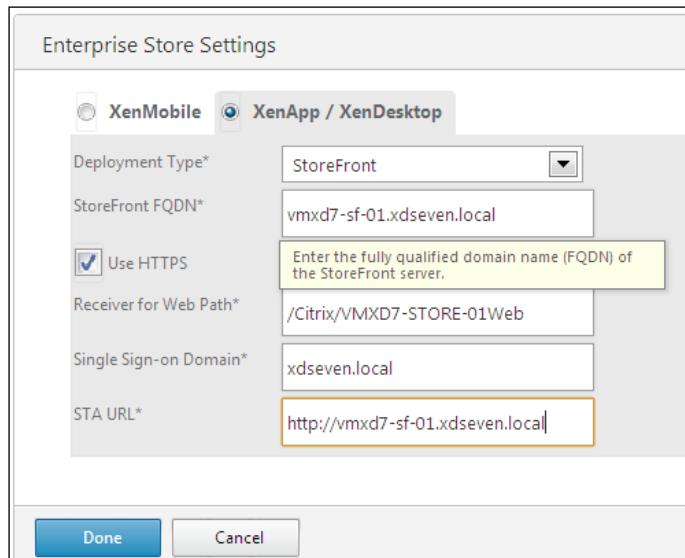
The screenshot shows the 'NetScaler Gateway Settings' dialog. In the 'Name' field, 'VPX-VServer' is entered. In the 'IP Address' field, '192.168.110.88' is entered. Under the 'Certificate' section, the 'Use Test Certificate' radio button is selected. In the 'Certificate FQDN*' field, 'ngw01.xdseven.local' is entered. At the bottom, there are 'Continue' and 'Cancel' buttons, with 'Continue' being highlighted.

10. In the **Authentication Settings** section, select **LDAP** as the authentication method, then select the **Configure New** radio button, and insert valid data for an existing configured domain. After completing these steps, click the **Continue** button.

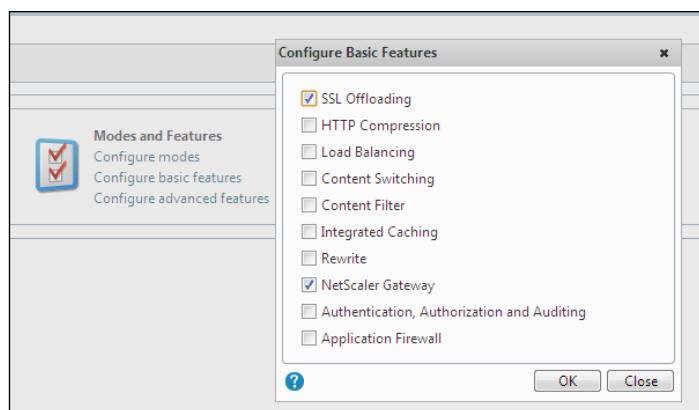
The screenshot shows the 'Authentication Settings' dialog. Under 'Primary Authentication*', 'LDAP' is selected. The 'Configure New' radio button is selected. The configuration fields are as follows:

- IP Address*: 192 . 168 . 110 . 20 (IPv6 checkbox is unchecked)
- Port*: 389
- Time out (seconds)*: 3
- Base DN*: CN=Users,DC=XDSEVEN,DC=local
- Admin Base DN*: administrator@xdseven.local
- Server Logon Name Attribute*: administrator@xdseven.local
- Password*: (redacted)
- Confirm Password*: (redacted)

11. In the **Enterprise Store Settings** menu, select the **XenApp/XenDesktop** radio button, then select **StoreFront** from the drop-down list, and populate the required fields with valid StoreFront configuration information. Click on **Done** to complete the procedure.

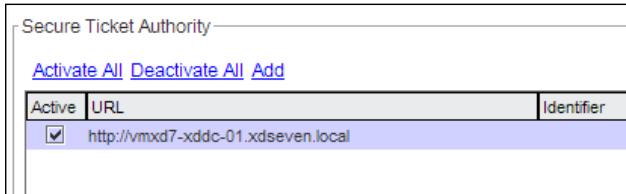


12. Click on the **Configuration** button on the bar at the top of the screen, and then expand the **System** section in the left-hand side menu.
13. In the **System** menu, click on the **Settings** link. Then select the **Configure basic features** voice, and verify that the **NetScaler Gateway** checkbox has been flagged. After pressing on **OK**, click on the **save** icon (in the form of a floppy disk) to register all the changes.

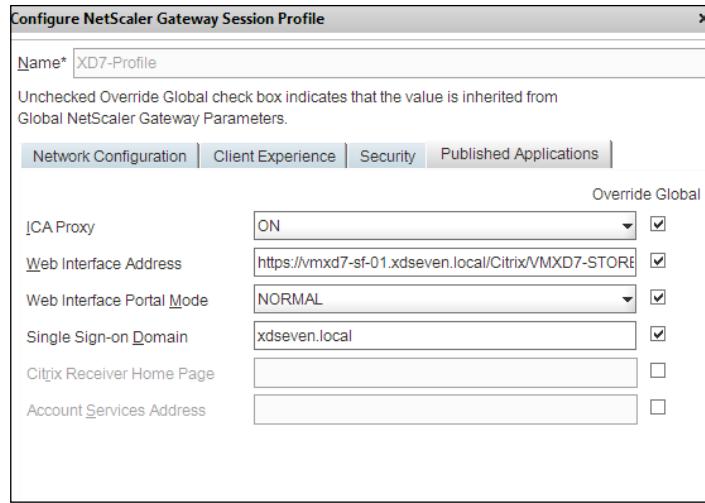


 Follow the standard procedures to generate a self-signed certificate or a CA verified certificate. In this book, we will not discuss about the full generation of a certificate, but remember that you need at least a Root CA certificate and a Server certificate to configure the NetScaler Gateway. For more details, you can refer to the following Microsoft online article <http://technet.microsoft.com/en-us/library/hh831740.aspx>.

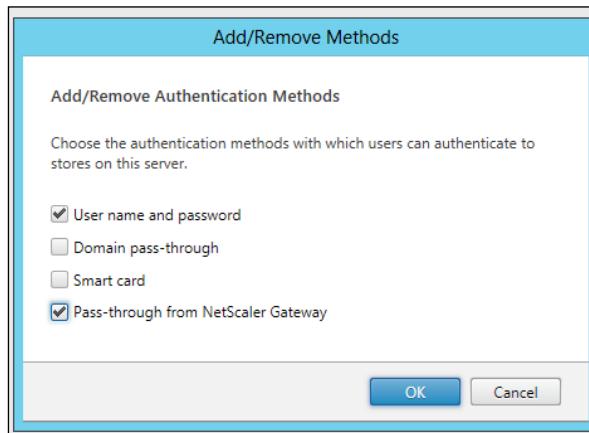
14. In the left-hand side menu, expand the **NetScaler Gateway** section and click on the **Virtual Servers** link. Select the previously created **Virtual Server**, and click on the **Open** button at the bottom of the page.
15. Select the **Published Applications** tab, and verify that the previously configured **Secure Ticket Authority (STA)** link is in the form of a URL such as `http://XenDesktopControllerFQDN` or `https://XenDesktopControllerFQDN`. After completing these steps, flag the mapped server link, click on the **Activate All** link, and then click on **OK**.



16. Click on the **Policies** tab, and click on the **Insert Policy** link at the bottom of the page.
17. Assign a **Name*** to the policy, and then click on the **New** button for the **Request Profile** section.
18. In **Create Access Gateway Session Profile**, assign a name to the profile, select the **Published Applications** tab, and flag the first four option fields to **Override Global** settings.
19. Insert the required information such as **ICA Proxy: ON, Web Interface Address**. Insert the configured NetScaler Gateway website address for StoreFront, **Web Interface Portal Mode: NORMAL**, and **Single Sign-On Domain**. Finally, insert the configured domain for your company, and then click on the **Create** button.



20. In the **Session Policy** screen, select **General** and **True Value** as **Named Expressions** and click on the **Add Expression** link. Then click on **Create**.
21. Connect to your StoreFront machine with domain administrative credentials, press the Windows + C key combination, search for the **StoreFront** icon in the Citrix software section, and then click on it.
22. Click on the **Authentication** link in the left-hand side menu, select the **Add/Remove** methods option in the right-hand side menu, and then add the **Pass-through from NetScaler Gateway** flag option. After completing the steps, click the **OK** button.



23. Click on the **Stores** link in the left-hand side menu, select the **Enable Remote Access** option in the right-hand side menu, then select the **Full VPN tunnel** radio button, and click on the **Add** button.

Enable Remote Access

Select NetScaler Gateway appliances to provide user access from external networks.

Remote access:

None

No VPN tunnel i

Full VPN tunnel i

NetScaler Gateway appliances:

Add...

Default appliance:



Choosing the **Full VPN tunnel** option will require you to install the Secure Access Plug-in, having full access to the entire set of published resources; to avoid installing it, consider using the **No VPN tunnel** option. This second choice will give you reduced access to the apps and desktop resources.

24. In the **General Settings** screen, populate the required fields in order to link the previously configured NetScaler Gateway to the StoreFront store. After completing, click on **Next**.

General Settings

The display name is visible to users in Citrix Receiver preferences.

Display name: Netscaler Infrastructure

NetScaler Gateway URL: https://nsgw01.xdseven.local

Version: 10.0 (Build 69.4) or later

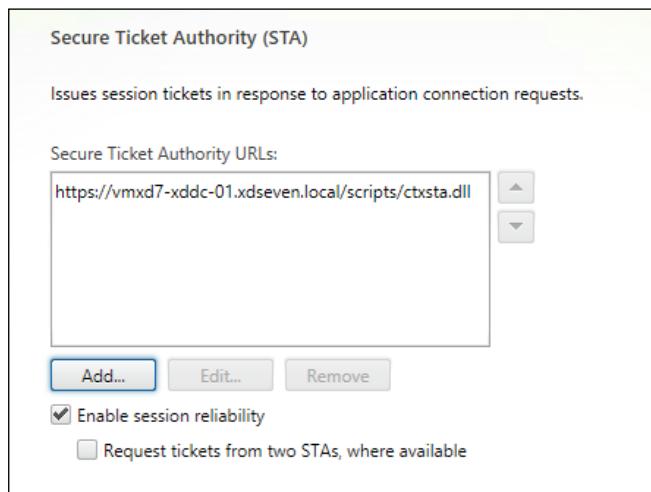
Subnet IP address: 192.168.110.88

Logon type: Domain

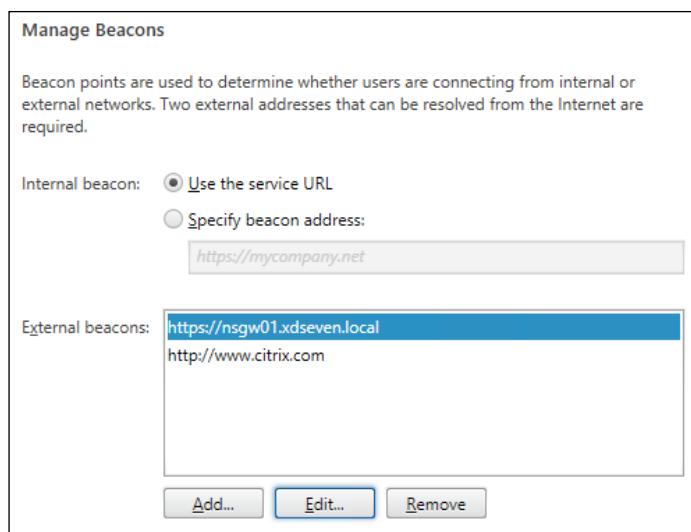
Smart card fallback: None

Callback URL: i https://nsgw01.xdseven.local /CitrixAuthService/AuthService.asmx

25. In the **Secure Ticket Authority (STA)** screen, configure a valid STA address in the form of `https://DesktopControllerFQDN/scripts/ctxsta.dll`. After completing these steps, click on the **Create** button.



26. Click on the **Beacons** link in the left-hand side menu, and select the **Manage Beacons** option in the right-hand side menu.
27. In the **Internal beacon** section, decide if you want to use the service URL or a specific URL configured only for internal access. For the **External beacons** section, add one or more web addresses that must be resolved from external networks. After completing this step, click on the **OK** button.





The beacons configurations are used to determine if users access resources from internal or external networks. For the **External beacons** section, you have to specify at least two Internet addresses.

28. Open a web browser and type the address of the configured FQDN VIP NetScaler Gateway, in the form of `https://NetScalerGatewayAddress`. You'll receive a logon screen on which you can insert the valid domain credentials. At this point, you will be able to connect to your published resources through the NetScaler Gateway.



To avoid resolution errors for the NetScaler Gateway VIP address, you should create a DNS record for it, or insert a row in the host file of the StoreFront server.

How it works...

The Citrix NetScaler Gateway is a secure gateway, which permits users to connect to an existing XenDesktop infrastructure in a secured manner.

The installation procedure for the Virtual Appliance only consists of the import activities under the supported hypervisor. After this phase, you have to configure the two network interfaces assigned to the gateway. One is used to communicate with the internal area of your architecture, and the other one connects the infrastructure to the outside world. This is not a mandatory configuration, but it's preferable to differentiate the traffic for the internal and the external worlds.

During the configuration of the network, especially when configuring the Gateway IP Address, which is also known as **NetScaler IP Address (NSIP)**, you will find two other kinds of network addresses: the **Mapped IP Address (MIP)** and the **Subnet IP Address (SNIP)**. The first address is used to contact the backend machines, and the second address allows users to access the NetScaler Access Gateway from the hosts located on different networks. Another important network component is given by the **Virtual IP Address (VIP)** associated to a configured Virtual Server, which was formerly the gateway web interface contacted by users and systems to access published virtual resources.

A fundamental operation is linking the NetScaler Gateway to the existing StoreFront installations. In this way, you will establish the communication between the first point of access for the users (NetScaler Gateway) and the stores configured with StoreFront, which has been transformed into a sort of backend authentication server in this configuration.

To be able to communicate with the NetScaler Gateway, it's necessary to generate a certificate that will be installed on the server and the client machines. This certificate can be self-signed or generated from an existing Certification Authority (such as Microsoft CA, and so on). Remember that in order to connect the gateway platform to the related components such as Citrix StoreFront, the certificate must be at least 1,024 bits in size.



You should always consider generating a certificate from a valid and existing Certification Authority. The self-signed one should be used only for PoC and testing environments.

An important aspect is the ability to contact a LDAP server, including the Microsoft Active Directory domains. You will be able to use a single authentication method for the secure gateway, the applications, and the virtual desktop created for your infrastructure.



In *Chapter 10, Configuring the XenDesktop® Advanced Logon*, we will discuss about different strong authentication methods that can be implemented with XenDesktop.

At this point, the critical configurations move from the NetScaler VPX to the configured StoreFront system(s). The configured NetScaler needs to be linked to the existing store infrastructure, specifying a passthrough authentication for the NetScaler and then linking the gateway web interface address previously configured (VIP address). Moreover, we have also registered the STA by specifying the XenDesktop controller address in the prepopulated global STA URL section. An STA server is used to release authorization tickets when a connection request has been performed in order to access a published resource (a XenApp application or a XenDesktop virtual desktop instance).



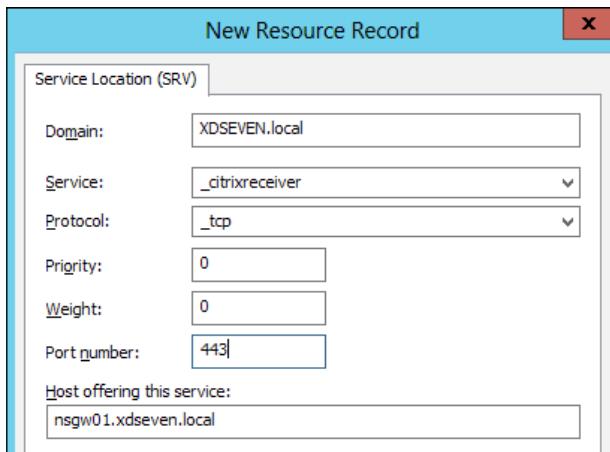
You should save your configuration after you have tested it. It runs in a running-config manner. Without explicitly registering the modifications, you will lose any update in the event of Virtual Appliance failure or reboot!

There's more

With the NetScaler Gateway platform, it is possible to configure the **Email-Based account discovery** feature. This feature permits users to authenticate to the Citrix StoreFront platform by using their own domain-related e-mail addresses.

To perform this, you need to execute the following configuration steps:

1. On your infrastructure's DNS server(s), you need to add a **Service Location (SRV)** record. This step is made up of the following tasks:
 1. Right-click on the configured DNS **Forward Lookup Zone**, and select the **Other New Records** option.
 2. Select the **Service Location (SRV)** option on the **Resource Record Type** screen, and click on the **Create Record** button.
 3. Populate the **Service** field with `_citrixreceiver`, the **Protocol** field with the `_tcp` value, the **Port number** field with `443`, and the **Host offering this service** field with your NetScaler Gateway FQDN.



2. On your NetScaler Gateway virtual appliance, edit the configured session policy, select the **Published Applications** tab, locate the **Account Service address** field, check the **Override Global** option, and type your Citrix StoreFront address in the form of `https://StoreFront/Citrix/Roaming/Accounts`:





Please refer to the *How it works* section for the session profile configuration.

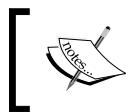
3. In the same **Session Policy** section, select the **Client Experience** tab and enable the **Clientless access** by checking the **Override Global** checkbox and selecting the **On** option:

Client Experience	
Home Page	<input type="text"/> <input checked="" type="checkbox"/> Display Home Page <input type="checkbox"/>
URL for Web-Based Email	<input type="text"/> <input type="checkbox"/>
Split Tunnel	<input type="text"/> OFF <input type="checkbox"/>
Session Time-out (mins)	<input type="text"/> 30 <input type="checkbox"/>
Client Idle Time-out (mins)	<input type="text"/> <input type="checkbox"/>
Clientless Access	<input type="text"/> On <input checked="" type="checkbox"/>

4. To complete the configuration, add to the **Expression** section the highlighted expressions indicated in the following screenshot:

Expression
ns_true
REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver
REQ.HTTP.HEADER CitrixGateway EXISTS

Users will be now able to authenticate to StoreFront using their corporate e-mail address.



You can better understand how the e-mail-based account discovery feature works by reading the Citrix article at <http://support.citrix.com/article/CTX139059>.

See also

- ▶ The *Installing and configuring StoreFront 2.0* recipe in Chapter 1, XenDesktop® 7 – Upgrading, Installing, and Configuring

Configuring the XenDesktop® logging

Any operation performed on a system, which is automatically or manually executed by the users, should be registered in a logfile in order to troubleshoot problems and reconstruct the activities for any kind of reason. For instance, in the event of security or legal checks. In this recipe, we will discuss about the main logging activities performed by the Citrix XenDesktop machines and the way to implement them.

Getting ready

All the policies will be applied to the deployed virtual desktop instances and the assigned users, so you need an already-existent XenDesktop infrastructure on which you will enable and use the configuration rules.

How to do it...

In this recipe, we will explain how to configure XenDesktop logging features:

1. Connect to the Delivery Controller server with an administrative domain user.
2. Press the Windows + C key combination, search for the **Citrix Studio** icon in the Citrix software section, and click on it.
3. Click on the **Policy** link in the left-hand side menu, then select **Create Policy** in the right-hand side panel or edit an existing one.
4. In the **Categories** menu, select the **Log settings** section and configure the following policies:
 - ❑ **Active Directory actions:** In this policy, the values are either **Enabled** or **Disabled**. If enabled, this policy will log all the domain-related events, in relation with the profile management activities.
 - ❑ **Common information:** In this policy, the values are either **Enabled** or **Disabled**. If enabled, this policy will log all the common information-related events in a verbose manner, in relation with the profile management activities.
 - ❑ **Common warnings:** In this policy, the values are either **Enabled** or **Disabled**. If enabled, this policy will log all the common warnings-related events in a verbose manner, in relation with the profile management activities.

- ❑ **Enable logging:** In this policy, the values are either **Enabled** or **Disabled**. If enabled, this policy will activate the verbose logging, which is also known as the debug mode.
- ❑ **File system actions:** In this policy, the values are either **Enabled** or **Disabled**. If enabled, this policy will log all the operations applied to the filesystem(s) in a verbose manner.
- ❑ **File system notifications:** In this policy, the values are either **Enabled** or **Disabled**. If enabled, this policy will log all the operations applied to the filesystem(s) in a verbose manner.
- ❑ **Logoff:** In this policy, the values are either **Enabled** or **Disabled**. If enabled, this policy will activate verbose logging for the user logoff operations.
- ❑ **Logon:** In this policy, the values are either **Enabled** or **Disabled**. If enabled, this policy will activate verbose logging for the user logon operations.
- ❑ **Maximum size of the log file:** In this policy, insert a value in bytes as the maximum size for the logfile. After the maximum size has been reached, the file is rotated in a .bak file and a new log file is generated.



If a .bak already exists, this will be deleted and then the new backup logfile will be generated.



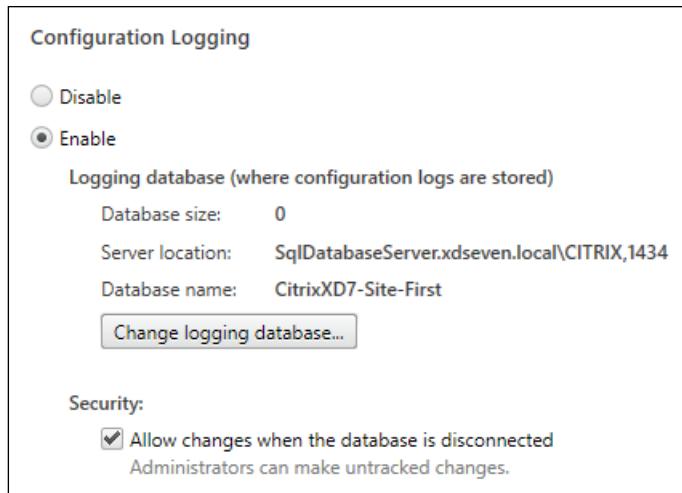
- ❑ **Path to log files:** In this policy, the values are either **Enabled** or **Disabled**. With this policy, you can specify a particular network path on which you will create the log files. If this policy is disabled, the default path will be used (%SystemRoot%\System32\LogFiles\UserProfileManager).
- ❑ **Personalized user information:** In this policy, the values are either **Enabled** or **Disabled**. If enabled, this policy will log all the user information customizations in a verbose manner.
- ❑ **Policy values at logon and logoff:** In this policy, the values are either **Enabled** or **Disabled**. If enabled, this policy will log all the changes applied to the policy in the time interval between the logon and logoff phase.
- ❑ **Registry actions:** In this policy, the values are either **Enabled** or **Disabled**. If enabled, this policy will activate verbose logging for the operations on the registry during user sessions.
- ❑ **Registry differences at logoff:** In this policy, the values are either **Enabled** or **Disabled**. If enabled, this policy will log in a verbose manner all the changes that are applied to the registry during user sessions, when a user performs a logoff from the assigned resource.

5. After completing the required configurations, save the policy changes as seen earlier in this chapter.
6. Click on the **Logging** link in the left-hand side menu. You will be prompted with a list of operations performed in the latest activity times.

The screenshot shows the Citrix XenDesktop interface with the title 'cITRIX' at the top. On the left, there's a navigation menu with 'Administrator' selected. In the center, there's a table titled 'Main task' with columns for 'Start', 'End', and 'Status'. The table lists several administrative tasks performed by 'XDSEVEN\Administrator' over the last three weeks, all marked as 'Successful'. The tasks include updating HDX Policies, creating and removing application configurations, and updating Notepad++ applications.

Administrator	Main task	Start	End	Status
Today				
XDSEVEN\Administrator	Update HDX Policies	10/11/2013 : 11.29.49	10/11/2013 : 11.29.52	Successful
Yesterday				
XDSEVEN\Administrator	Update HDX Policies	09/11/2013 : 17.41.29	09/11/2013 : 17.41.32	Successful
Three Weeks Ago				
XDSEVEN\Administrator	Create Application 'Notepad++'	27/10/2013 : 02.57.41	27/10/2013 : 02.58.20	Successful
XDSEVEN\Administrator	Remove Machine Configuration '5' from Deskt...	27/10/2013 : 02.47.53	27/10/2013 : 02.47.56	Successful
XDSEVEN\Administrator	Delete Application 'Notepad++'	27/10/2013 : 02.47.29	27/10/2013 : 02.47.59	Successful
XDSEVEN\Administrator	Update Application 'Notepad++'	27/10/2013 : 02.36.36	27/10/2013 : 02.36.52	Successful
XDSEVEN\Administrator	Update Application 'Notepad++'	27/10/2013 : 02.33.58	27/10/2013 : 02.34.19	Successful

7. Click on the **Preferences** link in the right-hand side menu. Then, configure whether you want to enable or disable the logging of administrative tasks and also whether you want to modify the database on which the logs are stored. After completing the steps, click the **OK** button.



8. Click on the **Create Custom Report** link in the right-hand side menu, and select the date range for which you are generating the required report. Then click on the **Next** button.

Date Range

Select a date range:

All
 Last 24 hours
 Last 7 days
 Last 4 weeks
 Custom

Start date:

End date:

9. In the **Format and Location** section, specify whether you want to save the report in CSV format, HTML format, or both. Then, give a valid path location on which you will create the report file. After completing these steps, click on **Next**.

Format and Location

Select a format:

CSV file
Best for exporting to a spreadsheet.

HTML
Best for viewing or printing.

Both

Location where you want to save your report:

10. In the **Summary** screen, click on the **Finish** button to complete the report-generation procedure.

How it works...

The Citrix XenDesktop logging discussed in this chapter can be divided into two major areas: the first, which is configured under the Citrix XenDesktop Policies section, configures all the logging parameters for the user profile components—especially in the case of configured Citrix Profile Management.

These policies are particularly useful in situations where the changes to the deployed desktop need to be logged as well. In fact, we have configured parameters such as the registry changes during a user session, or the performed logon and logoff actions. This means that activities on the corporate desktops can be tracked and intercepted.

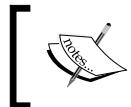
The other log analysis can be performed at XenDesktop infrastructural level. Within the Desktop Studio, you have the ability to see all the tasks performed by the administrators and delegated users for the XenDesktop 7 infrastructure. The logs can also be exported in the CSV format (useful as source data to reimport on other data collections, such as external databases or spreadsheets) or in the HTML format, which will give you a formatted and readable report. All the administrative tasks are logged in the associated site database.



You should consider implementing a log rotation script in order to maintain the history of the operations performed on your XenDesktop infrastructure systems.

There's more...

When the XenDesktop site logs increase too much, in terms of the amount of data and number of records, you can delete and archive them by using the Desktop Studio console. In the **Logging** section, click on **Delete Logs** on the right-hand side menu; and when prompted, choose a valid location on which the data will be archived before their cancellation.



Before performing the log deletion process, you will be prompted to log in with administrative credentials on the site database on which the logs are stored.

Delete Configuration Logs

Configuration Logs will be deleted. Save a copy?

No

Yes

Select where to save the copy:

C:\Users\administrator.XDSEVEN\Documents\Log-Archi



Logs can be saved in .csv or .txt format.

This will permit you to maintain a history of all the collected data and manage the volume of the logging on the system database(s).

See also

- ▶ The *Installing and configuring the XenDesktop® Collector* recipe in Chapter 5, *Configuring Additional Architectural Components*

9

Working with XenDesktop® PowerShell

In this chapter, we will cover the following recipes:

- ▶ Retrieving system information – configuration service cmdlets
- ▶ Managing Active Directory accounts – ADIdentity cmdlets
- ▶ Managing the Citrix® Desktop Controller and its resources – Broker and AppV cmdlets
- ▶ Administering hosts and machines – Host and Machine Creation cmdlets
- ▶ Managing additional components – StoreFront Admin and Logging cmdlets

Introduction

At this point in the book, we have implemented a fully functioning XenDesktop architecture made of the core components along with additional features in terms of security and performance.

With hundreds or thousands of hosts to configure and machines to deploy, configuring all the components manually could be difficult. For the XenDesktop 5.6 release as well as XenDesktop Version 7, you can find an integrated and customized version of Microsoft PowerShell; with its use, IT technicians are able to reduce the time required to perform management tasks by the creation of PowerShell scripts that will be used to deploy at scale the greatest part of the XenDesktop components.

Working with the PowerShell instead of XenDesktop GUI will give you more flexibility in terms of what kind of operations to execute, having a set of additional features to use during the infrastructure creation and configuration phases.

Retrieving system information – configuration Service cmdlets

In this recipe, we will use and explain a general-purpose PowerShell cmdlet: the **Configuration Service** category. This is used to retrieve general configuration parameters and to obtain information about the implementation of the XenDesktop configuration service.

Getting ready

No preliminary tasks are required. You have already installed the Citrix XenDesktop PowerShell SDK during the installation of Desktop Controller role machine(s).

To be sure you are able to run a PowerShell script (.ps1 format), you have to force enable script execution from the PowerShell prompt as follows:

```
Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Force
```

How to do it...

In this section, we will explain and execute the commands associated with the XenDesktop System and Services configuration area:

1. Connect to one of the Desktop Broker servers, say using a Remote Desktop connection.
2. Right-click on the PowerShell icon installed on the Windows taskbar and select the **Run as Administrator** option.
3. Load the Citrix PowerShell modules by typing the following command and then pressing the *Enter* key:

```
Asnp Citrix*
```



As an alternative to the Asnp command, you can use the Add-PSSnapin command.

4. Retrieve the active and configured Desktop Controller features by running the following command:

```
Get-ConfigEnabledFeature
```

5. To retrieve the current status of Config Service, run the following command; the output result will be **OK** in the absence of configuration issues.

```
Get-ConfigServiceStatus
```

6. To get the connection string used by the configuration service and to connect to the XenDesktop database, run the following command:

```
Get-ConfigDBConnection
```

7. Starting from the previously received output, it's possible to configure the connection string to let the configuration service use the system DB. For this command, you have to specify the Server, Initial Catalog, and Integrated Security parameters:

```
Set-ConfigDBConnection -DBConnection "Server=<Servername>\<InstanceName>; Initial Catalog=<DatabaseName>; Integrated Security=<True | False>"
```

8. Starting with an existing Citrix database, you can generate a SQL procedure file to use as a backup to recreate the database. Run the following command to complete this task, specifying the DatabaseName and the ServiceGroupName parameters:

```
Get-ConfigDBSchema -DatabaseName <DatabaseName>
-ServiceGroupName <ServiceGroupName> > Path:\FileName.sql
```



You need to configure a destination database with the same name of the source DB; otherwise, the script will fail!

9. To retrieve information about the active configuration service objects (Instance, Service, and Service Group), run the following three commands:

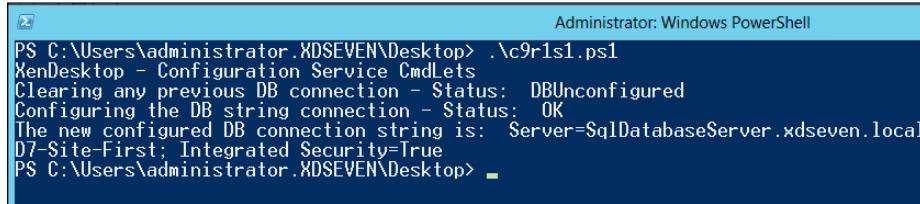
```
Get-ConfigRegisteredServiceInstance
Get-ConfigService
Get-ConfigServiceGroup
```

10. To test a set of operations to check the status of the configuration service, run the following script:

```
#----- Script - Configuration Service
#----- Define Variables
$Server_Conn="SqlDatabaseServer.xdseven.local\CITRIX,1434"
$Catalog_Conn="CitrixXD7-Site-First"
#-----
write-Host "XenDesktop - Configuration Service CmdLets"
#----- Clear the existing Configuration Service DB connection
$Clear = Set-ConfigDBConnection -DBConnection $null
Write-Host "Clearing any previous DB connection - Status: " $Clear
#----- Set the Configuration Service DB connection string
$New_Conn = Set-ConfigDBConnection -DBConnection "Server=$Server_Conn; Initial Catalog=$Catalog_Conn; Integrated Security=$true"
```

```
Write-Host "Configuring the DB string connection - Status: " $New_Conn
$Configured_String = Get-ConfigDBConnection
Write-Host "The new configured DB connection string is: "
$Configured_String
exit
```

[ You have to save this script with the .ps1 extension in order to invoke it with the PowerShell. Be sure to change the specific parameters related to your infrastructure in order to be able to run the script.]



A screenshot of a Windows PowerShell window titled "Administrator: Windows PowerShell". The command ".\c9r1s1.ps1" is run from the path "C:\Users\administrator.XDSEVEN\Desktop". The output shows the process of clearing any previous DB connection, configuring a new one with the status "OK", and displaying the new DB connection string which includes "Server=SqlDatabaseServer.xdseven.local", "D7-Site-First", and "Integrated Security=True". The command "PS C:\Users\administrator.XDSEVEN\Desktop>" is visible at the bottom.

How it works...

The Configuration Service cmdlets of the XenDesktop PowerShell permit the managing of the configuration service and its related information: the Metadata for the entire XenDesktop infrastructure, the Service instances registered within the VDI architecture, and the collections of these services, called Service Groups.

This set of commands offers the ability to retrieve and check the DB connection string to contact the configured XenDesktop SQL Server database. These operations are permitted by the `Get-ConfigDBConnection` command ("retrieve the current configuration") and the `Set-ConfigDBConnection` command ("configure the DB connection string"); both the commands use the DB Server Name with the instance name, the database name, and integrated security as information fields.

In the attached script, we have regenerated a database connection string. To be sure we will be able to recreate it, we have first cleared any existing connection, setting it to `null` (verify the command associated with the `$Clear` variable); then, we have defined the `$New_Conn` variable, using the `Set-ConfigDBConnection` command; all the parameters are defined at the top of the script in the form of variables.



Use the `Write-Host` command to echo results on the standard output.

There's more...

In some cases, you could need to retrieve the state of the registered services in order to verify their availability. You can use the `Test-ConfigServiceInstanceAvailability` cmdlet, to find out whether the service is responding and its response time. Run the following example to test the use of this command:

```
Get-ConfigRegisteredServiceInstance | Test-ConfigServiceInstanceAvailability | more
```



Use the `-ForceWaitForOneOfType` parameter to stop the check for a service category when one of its services responds.



See also

- ▶ The *Preparing the SQL Server 2012 Database* recipe in Chapter 1, XenDesktop® – Upgrading, Installing, and Configuring

Managing Active Directory accounts – ADIdentity cmdlets

In this recipe, we will discuss the utilization of the **Active Directory Identity** cmdlets. This is a functionality that permits retrieving and configuring the Active Directory objects used by Citrix XenDesktop, such as machine accounts assigned to existing desktop catalogs.

Getting ready

No preliminary tasks are required. You have already installed the Citrix XenDesktop PowerShell SDK during the installation of Desktop Controller role machine(s).

To be sure to be able to run a PowerShell script (.ps1 format), you have to enable script execution from the PowerShell prompt using the following command:

```
Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Force
```

How to do it...

The following are the steps required to manage XenDesktop machine identity through the use of Powershell:

1. Connect to one of the Desktop Broker servers, using for instance a Remote Desktop connection.
2. Click on the PowerShell icon installed on the Windows taskbar.
3. Load the Citrix PowerShell modules by typing the following command, and then press the *Enter* key.

Asnp Citrix*

4. To generate a new desktop catalog and interface it with your company domain, run the following PowerShell command. The parameters involved are `-NamingScheme` and `-NamingSchemeType`.

```
New-AcctIdentityPool -IdentityPoolName <PoolName>
-NamingScheme <Machine-Name-Structure##> -Domain
<ADDomainName> -NamingSchemeType <Numeric | Alphabetic>
```

5. To retrieve information on the currently existing machine catalogs, you have to use the following command. You can use filters such as `-IdentityPoolName`, `-IdentityPoolUid`, and `-AdminAddress`, which permit you to specify the address of a particular Desktop Controller.

Get-AcctIdentityPool



You can sort the output results using the `-SortBy` parameter, specifying the file for which you want to sort the output.

6. To rename an existing catalog/identity pool, execute the following command:

```
Rename-AcctIdentityPool -IdentityPoolName <CurrentName>
-NewIdentityPoolName <NewName>
```



To modify a catalog configuration parameter, use the `Set-AcctIdentityPool` command. You can retrieve information about its use with the following command:

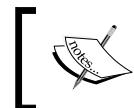
```
Get-Help Set-AcctIdentityPool -detailed | more.
```

7. To remove a created machine catalog from your XenDesktop architecture, use the `Remove-AcctIdentityPool` cmdlet in one of the following two ways:

- ❑ - `Remove-AcctIdentityPool -IdentityPoolName <PoolName>`
- ❑ - `Remove-AcctIdentityPool -IdentityPoolUid <PoolUID>`

8. To populate the created catalogs with domain machine accounts, execute the following command:

```
New-AcctADAccount -IdentityPoolName <CatalogName> -Count <NumberofAccounts> -StartCount <Number> -AdminAddress <ControllerIPAddress>
```



You can run this command only one instance at a time; you cannot execute parallel account creations because of the serial execution nature of the command.



9. Retrieve the generated computer account data by running the following command. You can filter the information using the `-IdentityPoolName` and `-Lock` parameters.

```
Get-AcctADAccount
```

10. The following command performs the required updates on the imported Active Directory computer accounts in a catalog. Optionally, you can use the `-AllAccounts` and `-AdminAddress` options.

```
Update-AcctADAccount -IdentityPoolName <PoolName>
```

11. Finally, you have the ability to remove computer accounts from an existing identity pool in the following way. Use the `-Force` option to proceed in the case of system exceptions:

```
Remove-AcctADAccount -IdentityPoolName <PoolName> -ADAccountName <ComputerAccountName> -RemovalOption <option>
```



You can reset the machine account password by running the following command:

```
Repair-AcctADAccount -ADAccountName "domain\computerName" -Force
```



12. Execute the following script to operate the creation of the catalog and machine accounts:

```
#----- Script - Configuration Service
#----- Define Variables
$AD_Domain="ctxlab.local"
$ID_Pool="Test-Pool-01"
$Controller_Address="192.168.1.60"

#----- Creating and Identity Pool
write-Host "XenDesktop - Creating an Identity Pool"
```

```
$ID_Pool_Create = New-AcctIdentityPool -IdentityPoolName $ID_Pool -NamingScheme Desk-T## -Domain $AD_Domain -NamingSchemeType Numeric
Write-Output "Pool creation activities - Status: " $ID_Pool_Create

#----- Verify the pool creation
$Check_Pool = Get-AcctIdentityPool -IdentityPoolName $ID_Pool | measure

if ($Check_Pool.Count -gt 0)
    {Write-Host "Identity Pool correctly created."}

else
    {Write-Host "Identity pool not correctly generated. Please verify."}

exit }

#----- Creating AD computer accounts

New-AcctADAccount -IdentityPoolName $ID_Pool -Count 3 -StartCount 10 -AdminAddress $Controller_Address

exit
```

```
Administrator: Windows PowerShell
PS C:\Users\administrator.XDSEVEN\Desktop> .\c9r2s1.ps1
XenDesktop - Creating an Identity Pool
Pool creation activities - Status:

AvailableAccounts : 0
Domain           : XDSEVEN.local
ErrorAccounts    : 0
IdentityPoolName : Test-Pool-01
IdentityPoolUid  : a942b55f-cfbe-47b6-a0cd-6f17a98e45ed
InUseAccounts    : 0
Lock              : False
MetadataMap       :
NamingScheme     : Desk-T##
NamingSchemeType : Numeric
OU                :
StartCount        : 1
TaintedAccounts   : 0
Scopes            : {}

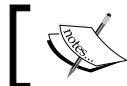
Identity Pool correctly created.
SuccessfulAccounts : {XDSEVEN\Desktop-T10$, XDSEVEN\Desktop-T11$, XDSEVEN\Desktop-T12$}
SuccessfulAccountsCount : 3
FailedAccountsCount : 0
FailedAccounts     : {}
```

How it works...

In this recipe, we discussed the management of the XenDesktop Identity Pools and their objects as well as the Active Directory computer accounts contained within the pools. These commands could be particularly useful in the case of advanced management of the pools and the computer accounts within, in terms of changes, deletion, creation, and advanced management of the Active Directory machine accounts.

The first command collections discuss Identity Pools and the four main operations that can be performed on them: the creation (`New-AcctIdentityPool`), the list of resources (`Get-AcctIdentityPool`), the renaming (`Rename-AcctIdentityPool`), and the deletion (`Remove-AcctIdentityPool`). The creation of an Identity Pool is based on the specification of the name of the AD objects container, on the Desktop Controller address to which the pool will refer, and on the two main configurable characteristics: the **Naming Scheme** (the naming convention assigned to the AD computer accounts generated within an Identity Pool, in the form of `MachineName##`, where the sharp symbols specify the machine progressive numbering) and the **Naming Scheme Type** (alphabetic or numeric progression). For instance, you could specify an alphabetical machine naming convention in the following way: `Desk-T-AA`.

The `Rename-AcctIdentityPool` command permits you to rename existing pools. You only have to specify the old pool name and the new name to use in its place. As simple it may seem, the last Identity Pool command, `Remove-AcctIdentityPool`, filters data for the pool name or the pool UID and lets you delete one or more existing pools.



You can remove a pool only when it has no associated machine accounts.



The second command group permits you to manage the Active Directory machine accounts, which can be grouped with the Identity Pools. The `New-AcctADAccount` cmdlet lets you create a computer account within your domain. Based on the naming convention defined in the pool on which the machine account is linked, you can specify the starting progressive machine number (the `-StartCount` parameter) and the number of accounts to create (the `-Count` parameter). To remove created computer accounts, you have to use the `Remove-AcctADAccount` command. What is particularly interesting about this cmdlet is the presence of the modality to perform computer account deletion. With the `-RemovalOption` command, you can remove machine accounts only from XenDesktop (the `None` option), remove them also from the Active Directory domain (the `Delete` option), or disable the accounts in the AD domain (the `Disable` option).



Use the `-Force` parameter to remove the accounts and in case of warnings.

The script at the end of the recipe permits you to create an Identity Pool referring to the related Desktop Controller. After verifying its correct creation, the pool will be populated with a set of three computer accounts, based on the naming convention configured for the Identity Pool (Desk-T## with numeric progression). To count the number of objects, in order to verify the pool creation, the `measure` command has been used, combined with the `count` property of the variable containing the number of retrieved pools (`$Check_Pool.count`).

There's more...

With the XenDesktop PowerShell it's also possible to use existing Active Directory computer accounts to generate machine catalog accounts, importing them in the XenDesktop infrastructure, as seen earlier in this book for the GUI component.

You can perform this operation through the command line using the `Add-AcctADAccount` PowerShell command in the following syntax:

```
Add-AcctADAccount -IdentityPoolName <PoolName>
-ADAccountName <ComputerName>
```

You can specify the AD computer account in all the common forms, such as `Domain\Computer Name`, `ComputerName@Domain`, or through its FQDN.

See also

- ▶ The *Creating and configuring the Machine Catalog* recipe in *Chapter 6, Creating and Configuring a Desktop Environment*

Managing the Citrix® Desktop Controller and its resources – the Broker and AppV cmdlets

This is one of the principal PowerShell command groups for XenDesktop because of the interaction with the Desktop Broker component. This section will be about the use of the set of commands to manage the Broker in terms of displaying configurations and setting components and parameters, including the applications published with the XenDesktop 7 infrastructure or App-V existing architectures.

Getting ready

No preliminary tasks are required. You have already installed the Citrix XenDesktop PowerShell SDK during the installation of the Desktop Controller role machine(s).

To be sure to be able to run a PowerShell script (.ps1 format), you have to enable script execution from the PowerShell prompt using the following command:

```
Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Force
```

How to do it...

The following is the explanation of the commands included in the Desktop Controllers Powershell command set:

1. Connect to one of the Desktop Broker servers.
2. Click on the PowerShell icon installed on the Windows taskbar.
3. Load the Citrix PowerShell modules by typing the following command and then press the *Enter* key:
Asnp Citrix*
4. To retrieve the configuration of the XenDesktop broker site, run the following command:

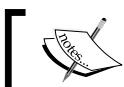
Get-BrokerSite

5. To modify the parameters of an existing XenDesktop broker site, run the following command. The most important parameters involved are **-BaseOU**, **-DnsResolutionEnabled**, and **-AdminAddress**.

Set-BrokerSite -BaseOU <DefaultDesktopRegistrationOU>
-AdminAddress <BrokerAddress>

6. Run the following command in order to create a desktop catalog for your infrastructure. In case of a Provisioning Service catalog, you have to use the **-PvsAddress** and **-PvsDomain** parameters.

New-BrokerCatalog -Name <CatalogName> -ProvisioningType <Manual | MCS | PVS> -Description <CatalogDescription>



For the **ProvisioningType** parameter, the **PVS** option permits you to specify both physical and virtual machines.

7. After creating the desktop catalog, you can retrieve information on the existing catalogs by running the following command. Filtering through the catalogs for information, such as the allocation type (the **-AllocationType** parameter). Without any specific option, you will list the entire infrastructure catalog.

Get-BrokerCatalog

8. To modify the previously configured catalog characteristics, you have to run the following command:

Set-BrokerCatalog -Description -isRemotePC -PvsAddress
-PvsDomain -PvsForVM



You cannot modify the allocation type and catalog kind settings!

To remove an existing catalog, run the following cmdlet:

Remove-BrokerCatalog -Name <CatalogName>

9. To list the entire set of existing desktops in your site, run the following command:

```
Get-BrokerDesktop
```



Later in this recipe, we will list the most important parameters for this command.



10. To configure a desktop group in your Citrix broker, execute this cmdlet:

```
New-BrokerDesktopGroup -Name <DesktopGroupName> -DesktopKind  
<Private|Shared> -Enabled <True|False> -PublishedName  
<DesktopDisplayName> -SecureIcaRequired <True|False>
```



The `-AutomaticPowerOnForAssigned` parameter is usable only for private desktops, while the `-ShutdownDesktopsAfterUse` parameter can be activated only in presence of power-managed desktops.

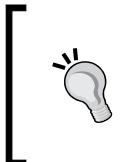


11. After creating a Broker Desktop Group, you can retrieve information by using the following command. You can use the same filters explained in the previous step.

```
Get-BrokerDesktopGroup
```

12. To modify the configuration of an existing group, you have to use the `Set-BrokerDesktopGroup` cmdlet. For instance, you could use `-InMaintenanceMode`, a desktop group, in the following way:

```
Set-BrokerDesktopGroup <GroupName> -InMaintenanceMode $true
```



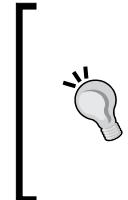
To display the historical usage of desktop groups, run the following command:

```
Get-BrokerDesktopUsage -DesktopGroupName  
<DesktopGroupName> -MaxRecordCount  
<MaxNumberofRecords>
```



13. To populate the previously configured desktop groups, you have to use the following cmdlet:

```
Add-BrokerMachinesToDesktopGroup -Catalog <CatalogName>  
-DesktopGroup <DesktopGroupName> -Count <NumberofMachines>
```



After creating a desktop group machine, you can prepare it for Personal vDisk creation by running the following command:

```
Start-BrokerMachinePvdImagePrepare -InputObject  
<MachineName>.
```

The task will be performed the next time the machine is started.



14. To retrieve any existing private desktop group, run the following PowerShell commands. Useful filters are `-MachineName`, `-DesktopGroupUid`, `-InMaintenanceMode`, and `-OSType`.

```
Get-BrokerPrivateDesktop
```



To verify the resources to which a user has access, use the `Get-BrokerResource` command, filtering for `-User <Username>` and/or `-Group <GroupName>` (AD group membership for the specified user).

15. After completing machine creation and grouping, it's time to publish applications and to assign them to the existing virtual desktops. The first useful command permits you to create applications. Using XenDesktop, without combining it with XenApp, the only allowed application type is hosted applications.

```
New-BrokerApplication -CommandLineExecutable <FullApplicationPath>
-BrowserName <InternalAppName>
-Enabled <True|False> -ShortcutAddedToDesktop <True|False>
-ShortcutAddedToStartMenu <True|False> -IconFromClient
<True|False> -Description <AppDescription>
```



You can also use resource control parameters such as `-CpuPriorityLevel` (Low, BelowNormal, Normal, AboveNormal, and High) and `-WaitForPrinterCreation`.

16. To retrieve published applications, use the following PowerShell cmdlet, combining it with filters such as `-DisplayName`, `-Enabled`, or `-BrowserName`:

```
Get-BrokerApplication
```



To rename an already published application, use the following command:

```
Rename-BrokerApplication -Name
<CurrentAdministrativeName> -NewName
<NewAdministrativeName>.
```

17. Use the following PowerShell cmdlet to associate one or more file extension(s) with a published application:

```
New-BrokerConfiguredFTA -ExtensionName <Extension>
-ApplicationUid <ApplicationID>
```

18. To retrieve the association between file types and software, run the following command. You can use filters such as `-Uid` (specific file type by its UID) and `-ExtensionName`.

```
Get-BrokerConfiguredFTA
```

19. To remove a published application from the XenDesktop infrastructure, use the following PowerShell cmdlet:

```
Remove-BrokerApplication -Name <ApplicationName> -DesktopGroup <DeskGroupName> -AdminAddress <BrokerAddress>
```

20. Once all the application configuration has been completed, you have to assign the software to an existing desktop group in the following way:

```
Add-BrokerApplication -BrowserName <ApplicationBrowserName> -DesktopGroup <DeskGroupName>
```

21. A fundamental implementation is access control on the XenDesktop site resources. Use the following command and related syntax to configure a rule:

```
New-BrokerAccessPolicyRule -Name <RuleName> -IncludedUserFilterEnabled <True|False> -IncludedUsers <Domain\>User|Group> -IncludedDesktopGroupFilterEnabled <True|False> -IncludedDesktopGroups <DesktopGroupName> -AllowRestart <True|False>
```



You can also use excluding filters: `-ExcludedClientIPs` and `-ExcludedUsers`.



22. To retrieve the configured access rules, execute the following cmdlet using the same filters previously explained for the rule creation process:

```
Get-BrokerAccessPolicyRule
```



Remove an existing access rule using the following command:

```
Remove-BrokerAccessPolicyRule -Name <RuleName>.
```



23. To create a new assignment rule, use the following syntax:

```
New-BrokerAssignmentPolicyRule -Name <RuleName> -DesktopGroupUid <DesktopGroupUID> -IncludedUsers <Domain\>User|Group> -PublishedName <DesktopGroupName>
```



To modify and remove an assignment policy, run the `Set-BrokerAssignmentPolicyRule` cmdlet and the `Remove-BrokerAssignmentPolicyRule` command, respectively.



24. After that, you can retrieve the currently configured assignment rules by running the following command:

```
Get-BrokerAssignmentPolicyRule -Name <RuleName>
```

The following are the explanations and examples for the **AppV** cmdlets:

1. The following command, which is part of the AppV cmdlet, will list all the applications published using a connected App-V infrastructure:

```
Get-CtxAppVApplication -AppVManagementServer <AppVServer>
```

2. To retrieve information about a specific application within an existing App-V package, run the following command:

```
Get-CtxAppVApplicationInfo -AppVManagementServer <AppVServer>  
-AppId <ApplicationID> -PackageID <PackageID>
```

3. To link a new App-V setup, including the management and publishing servers, execute the following command:

```
New-CtxAppVServer -PublishingServer <PublishingServer>  
-ManagementServer <ManagementServer>
```

 You can also configure these parameters: -UserRefreshEnabled, -UserRefreshOnLogon, -UserRefreshInterval, -GlobalRefreshEnabled, -GlobalRefreshOnLogon, and -GlobalRefreshInterval. They are used to enable and set the interval for the packages' refresh when a user executes logon normally or in a specific configured interval. GlobalRefresh<> applies to the machine groups.

4. The following command will give you the list of the existing App-V servers (both publishing and management) existing within your XenDesktop 7 infrastructure. You have to associate this command with the ByteArray parameter as follows:

```
Get-CtxAppVServer -ByteArray <AppVCreatedPolicy>
```

 The value for the ByteArray parameter can be retrieved by running the following command:

```
Get-BrokerMachineConfiguration -Name appv*
```

5. To check a retrieved URL for an App-V Management server, you have to execute the following command:

```
Test-CtxAppVServer -AppVManagementServer <AppvManagementServer>
```

 We have discussed the App-V components in the *Publishing applications using Microsoft App-V* recipe in Chapter 7, Deploying Applications.

6. The following script operates on part of the discussed Broker commands:

```
#----- Script - Hosting + MCS
#-----
#----- Define Variables
$LicSRV="192.168.110.30"
$BrokerAddress = "192.168.110.30"
$LicPort="27000"
$CatName="SRV-APP-00"
$DeliveryGroupName="Delivery-00"
$app_Path="C:\Windows\System32\notepad.exe"

#----- Create a XenDesktop Catalog
New-BrokerCatalog -Name $CatName -AllocationType Random
-CatalogKind PowerManaged -Description "Catalog-Book-Number-01"

#----- Create a Desktop Group
New-BrokerDesktopGroup -Name $DeliveryGroupName -DesktopKind
Shared -Enabled $true -PublishedName "Book Desktop Group"
-SecureIcaRequired $true -ShutdownDesktopsAfterUse $true

#----- Deploying Machines
Add-BrokerMachinesToDesktopGroup -Catalog $CatName -DesktopGroup
$DeliveryGroupName -Count 4

#----- Publish Notepad Application
New-BrokerApplication -CommandLineExecutable $app_Path
-PropertyName NotepadExe -DisplayName "Windows Notepad" -Enabled
$true -ShortcutAddedToDesktop $true -ShortcutAddedToStartMenu
$false -Description "Notepad Text Editor"

#----- Associate the .txt extension
$appID=$(Get-BrokerApplication -PropertyName NotepadExe)
New-BrokerConfiguredFTA -ExtensionName ".txt" -ApplicationUid
$appID.Uid -HandlerName "textfile"

#----- Retrieve published applications
Get-BrokerApplication
```

```
#----- Filter the resources for the Help Desk team
New-BrokerAccessPolicyRule -Name HelpDeskFilter-Rule-01
-IncludedUserFilterEnabled $true -IncludedUsers "XDSEVEN\hd01"
-IncludedDesktopGroupFilterEnabled $true -IncludedDesktopGroups
$DeliveryGroupName -AllowRestart $true

exit
```

Administrator: Windows PowerShell	
ExtensionData	: System.Runtime.Serialization.ExtensionDataObject
AllocationType	: Random
AssignedCount	: 0
AvailableAssignedCount	: 0
AvailableCount	: 0
AvailableUnassignedCount	: 0
Description	Catalog-Book-Number-01
HypervisorConnectionUid	
IsRemotePC	: False
MachinesArePhysical	: False
MetadataMap	: {}
MinimumFunctionalLevel	: L7
Name	SRV-APP-00
PersistUserChanges	: OnLocal
ProvisioningSchemeId	
ProvisioningType	: Manual
PusAddress	

How it works...

Using and configuring the Broker cmdlet category has permitted to generate resource containers (catalogs and desktop groups), with which we can assign end-user resources (Desktops and Applications) and filtering rules (Access and Assignment). Using this division, we can discuss the five main PowerShell Broker command subcategories:

- ▶ **Site and catalog subsection:** In this area, we've configured the XenDesktop site and the contained catalogs; then, we have retrieved information about them. The New-BrokerCatalog command performs the creation of a machine catalog. The **ThinCloned** catalogs and the **SingleImage** catalogs are parts of the **Provisioning Services architecture (PVS)**. It's also possible to configure catalogs with the Personal vDisk technology for both the MCS and PVS infrastructures. The New-BrokerCatalog command lets you create random or static-assigned resource catalogs, specifying which type of catalog you want to create.
- ▶ **Desktops and desktop groups subsection:** In this subsection, we've created and managed the desktop groups and related desktops. For this second object type, the Get-BrokerDesktop command permits retrieving existing desktop machines by filtering the search for information uses the following commands:
 - –MachineName (in the form of Domain\ComputerName)

- ❑ -ApplicationInUse, -CatalogName, -DesktopCondition (high resource usage or latency, parameters in form of --CPU, --ICALLatency, and --UPMLogonTime)
- ❑ -DesktopGroupName, -DesktopKind (a desktop can be private or shared)
- ❑ -ImageOutOfDate (a desktop not compliant with the latest base image template updates MCS architecture only)
- ❑ -InMaintenanceMode, -IsAssigned (a desktop resource already or not assigned to a user)
- ❑ -LastConnectionTime, -LastConnectionUser, -OSType, -PowerState (the current situation for the Desktop, in form of **On | Off | TurningOn | TurningOff | Suspending | Resuming | Unmanaged | Unavailable | Unknown**)
- ❑ -Protocol (for instance, HDX or RDP) and -LastDeregistrationReason. This option permits you to discover why a deregistration has occurred, retrieving as result data AgentShutdown, AgentSuspended, BrokerRegistrationLimitReached, AgentNotContactable, ContactLost, BrokerError, DesktopRemoved, and several others.

After this, we have used the New-BrokerDesktopGroup command to generate a desktop group and then linked the existing machine with the related desktop group by using the Add-BrokerMachinesToDesktopGroup command (the main parameters are the desktop group name and the number of machines to deploy).

- ▶ **Applications subsection:** In this subsection we have created, modified, and copied hosted applications in the XenDesktop architecture using the command line for both the XenDesktop applications and the App-V linked architectures. The New-BrokerApplication command permits you to publish existing applications already installed on desktops, which are part of an Application Desktop Group, as seen earlier in this book. Also, in this case, you can specify the main application option already discussed, such as link publication for the desktop and the Start menu and the visibility and enabling of the app (the -Visible and -Enabled parameters). For any app, you can specify the file type association (explicitly specifying it with the -ExtensionName parameter or importing them from the Citrix known list using the -ImportedFTA parameter) with the New-BrokerConfiguredFTA command. After completing software publication, you can assign them to existing desktops through the Add-BrokerApplication command, associating the application BrowserName with the desktop group name to which you want to assign it. With respect to the App-V components, the AppV.Admin cmdlet permits the linking of an existing App-V infrastructure (made up of both management and publishing servers with the ability to list the configurations applied) and the already published applications with their parameters.



The **BrowserName** for a published application must be unique within a XenDesktop infrastructure!

- ▶ **The Access and assignment filtering rules subsection:** This last subsection has covered the configuration of access and assignment rules. In other words, using these two policy categories, it has been possible to regulate the resource usage and access for the users. The New-BrokerAccessPolicyRule command creates an **access policy rule** for the existing XenDesktop resources, setting which users have the ability to access and use defined desktop resources. You have to enable the inclusion (-IncludedClientIPFilterEnabled, -IncludedClientNameFilterEnabled and -IncludedDesktopGroupFilterEnabled) and exclusion (-ExcludedClientIPFilterEnabled and -ExcludedClientNameFilterEnabled) filters to be sure that the included (-IncludedClientIPs, -IncludedClientNames and -IncludedDesktopGroups) and excluded (-ExcludedClientIPs and -ExcludedClientNames) resources are managed in the right way. For the assignment policy rule, the command to use is New-BrokerAssignmentPolicyRule, specifying the included and/or excluded users (for excluded users, you have to enable the ExcludedUserFilterEnabled filter) and the Desktop Group UID to which we apply the assignment task.

There's more...

With the Broker cmdlets group, it is also possible to manage the power actions to apply to the catalog machines. You can create a new power action related to an existing desktop machine using the following command:

```
New-BrokerHostingPowerAction -MachineName <DesktopName> -Action <TurnOn|TurnOff|ShutDown|Reset|Restart|Suspend|Resume> -ActualPriority <PriorityValue>
```

And then to retrieve it we use the following command:

```
Get-BrokerHostingPowerAction
```



The lower the priority value, the higher is its importance.

Moreover, you can also create and manage a full power time scheme for a desktop group using the creation power time cmdlet using the following command:

```
New-BrokerPowerTimeScheme -Name <TimeSchemeName> -DaysOfWeek <SpecificDay|WeekDays|Weekend> -DesktopGroupId <GroupUID> -DisplayName <Name> -PeakHours <PeakHoursExpression>
```

And to retrieve the existing configurations, we can use the following command:

```
Get-BrokerPowerTimeScheme
```

The PeakHoursExpression parameter has this construction: FromHour..ToHour | % {\$_ -gt <Hour> and \$_ -lt <Hour> }. For example, for the entire day, you can set the peak hour time from 10 a.m. to 17 a.m. in the following way: (0..23 | % {\$_ -gt 10 and \$_ -lt 17 }).

See also

- ▶ The *Publishing applications using Microsoft App-V* recipe in *Chapter 7, Deploying Applications*

Administering hosts and machines – the Host and Machine Creation cmdlets

In this recipe, we will describe how to create the connection between the Hypervisor and the XenDesktop servers and the way to generate machines to assign to the end users, all by using the Citrix PowerShell.

Getting ready

No preliminary tasks are required. You have already installed the Citrix XenDesktop PowerShell SDK during the installation of Desktop Controller role machine(s).

To be sure to be able to run a PowerShell script (.ps1 format), you have to enable the script execution from the PowerShell prompt using the following command:

```
Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Force
```

How to do it...

In this section, we will discuss the Powershell commands used to connect XenDesktop with the supported hypervisors plus the creation of the machines from the command line:

1. Connect to one of the Desktop Broker servers.
2. Click on the PowerShell icon installed on the Windows taskbar.
3. Load the Citrix PowerShell modules by typing the following command, and then press the *Enter* key:

```
Asnp Citrix*
```

4. To list the available Hypervisor types, execute the following command:

```
Get-HypHypervisorPlugin -AdminAddress <BrokerAddress>
```

5. To list the configured properties for the XenDesktop Root level location (XDhyp : \), execute the following command:

```
Get-ChildItem XDhyp:\HostingUnits
```



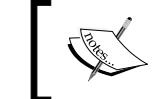
Please refer to the PSPath, Storage, and PersonalvDiskStorage output fields to retrieve information on the storage configuration.

6. Execute the following cmdlet to add a storage resource to the XenDesktop Controller host:

```
Add-HypHostingUnitStorage -LiteralPath <HostPathLocation>  
-StoragePath <StoragePath> -StorageType <OSStorage|PersonalvDiskStorage> - AdminAddress <BrokerAddress>
```

7. To generate a snapshot for an existing VM, perform the following task:

```
New-HypVMSnapshot -LiteralPath <HostPathLocation>  
-SnapshotDescription <Description>
```



Use the Get-HypVMMacAddress -LiteralPath <HostPathLocation> command to list the MAC address of specified Desktop VMs.

8. To provision machine instances starting from the Desktop base image template, run the following command:

```
New-ProvScheme -ProvisioningSchemeName <SchemeName>  
-HostingUnitName <HypervisorServer> -IdentityPoolName  
<PoolName> -MasterImageVM <BaseImageTemplatePath> -VMMemoryMB  
<MemoryAssigned> -VMCpuCount <NumberofCPU>
```

9. To specify the creation of instances with the Personal vDisk technology, use this option: -UsePersonalvDiskStorage.

10. After the creation process, retrieve the provisioning scheme information by running the following command:

```
Get-ProvScheme -ProvisioningSchemeName <SchemeName>
```



To modify the resources assigned to desktop instances in a provisioning scheme, use the Set-ProvScheme cmdlet. Permitted parameters are –ProvisioningSchemeName, –VMCpuCount, and –VMMemoryMB.

11. To update the desktop instances to the latest version of the Desktop Base Image template, run the following cmdlet:

```
Publish-ProvMasterVmImage -ProvisioningSchemeName <SchemeName>  
-MasterImageVM <BaseImageTemplatePath>
```



If you don't want to maintain the preupdate instance version to use as restore checkpoint, use the –DoNotStoreOldImage option.

12. To create machine instances based on the previously configured provisioning scheme for an MCS architecture, run the following command:

```
New-ProvVM -ProvisioningSchemeName <SchemeName> -ADAccountName  
"Domain\MachineAccount"
```



Use the –FastBuild option to make the machine creation process faster. On the other hand, you can't start up the machines until the process has been completed.

13. Retrieve the configured desktop instances using the following cmdlet:

```
Get-ProvVM -ProvisioningSchemeName <SchemeName> -VMName  
<MachineName>
```

14. To remove an existing virtual desktop, use the following command:

```
Remove-ProvVM -ProvisioningSchemeName <SchemeName> -VMName  
<MachineName> -AdminAddress <BrokerAddress>
```

15. The following script will combine the use of some of the commands listed in this recipe:

```
#----- Script - Hosting + MCS
#-----
#----- Define Variables
$LitPath = "XDHyp:\HostingUnits\VMware01"
```

```

$StorPath = "XDHyp:\HostingUnits\VMware01\datastore1.storage"
$Controller_Address="192.168.110.30"
$HostUnitName = "Vmware01"
$IDPool = $(Get-AcctIdentityPool -IdentityPoolName VDI-DESKTOP)
$BaseVMPATH = "XDHyp:\HostingUnits\VMware01\VMXD7-W8MCS-01.vm"

#----- Creating a storage location
Add-HypHostingUnitStorage -LiteralPath $LitPath -StoragePath
$StorPath -StorageType OSStorage -AdminAddress $Controller_Address

#----- Creating a Provisioning Scheme
New-ProvScheme -ProvisioningSchemeName Deploy_01 -HostingUnitName
$HostUnitName -IdentityPoolName $IDPool.IdentityPoolName
-MasterImageVM $BaseVMPATH\T0-Post.snapshot -VMMemoryMB 4096
-VMCpuCount 2 -CleanOnBoot

#----- List the VM configured on the Hypervisor Host
dir $LitPath\*.vm

exit

```

How it works...

The Host and Machine Creation cmdlet groups manage interfacing with the Hypervisor hosts in terms of machines and storage resources. This permits creating the desktop instances to assign to the end user, starting with an existing and mapped Desktop virtual machine.

The Get-HypHypervisorPlugin command retrieves and lists the available hypervisors to use to deploy virtual desktops and to configure storage types. As already discussed earlier in this book, you can configure an operating system storage area or a personal vDisk storage zone. The way to map an existing storage location from the Hypervisor to the XenDesktop controller is running the Add-HypHostingUnitStorage cmdlet. In this case, you have to specify the destination path on which the storage object will be created (`LiteralPath`), the source storage path on the Hypervisor machine(s) (`StoragePath`), and `StorageType` previously discussed. The storage types are in form of `XDhyp:\HostingUnits\<UnitName>`.



To list all the configured storage objects, execute the following command:

```
dir XDhyp:\HostingUnits\<UnitName> \*.storage
```

After configuring the storage area, we've discussed the **Machine Creation Service (MCS)** architecture. In this collection of cmdlets, we have commands available to generate VM snapshots from which deploying desktop instances (`New-HypVMSnapshot`), specifying a name and a description for the generated disk snapshot. Starting with the available disk image, the `New-ProvScheme` command permits you to create a resource provisioning scheme, on which you can specify the desktop base image, the resources to assign to the desktop instances (in terms of CPU and RAM or `-VMCpuCount` and `-VMMemoryMB`), and whether to generate these virtual desktops in a non-persistent mode (`-CleanOnBoot` option) and with or without the use of the Personal vDisk technology (`-UsePersonalVDiskStorage`). It's possible to update the deployed instances to the latest base image update through the use of the `Publish-ProvMasterVmImage` command.

In the generated script, we have located all the main storage locations (`LitPath` and `StorPath` variables) useful for realizing a provisioning scheme; then, we implemented a provisioning procedure for a desktop, based on an existing base image snapshot, with two vCPUs and 4GB of RAM for the delivered instances, which will be cleaned every time they stop and start (the `-CleanOnBoot` option).



You can navigate the local and remote storage paths configured with the XenDesktop Broker machine. To list an object category (such as VM or Snapshot) you can execute the following command:

```
dir XDhyp:\HostingUnits\<UnitName>\*.<category>
```

There's more...

The discussed cmdlets also offer you a technique with which to preserve a virtual desktop from accidental deletion or unauthorized use. With the Machine Creation cmdlets group, you have the ability to use a particular command that permits you to lock critical desktops: `Lock-ProvVM`. This cmdlet requires as parameters the name of the scheme to which to refer (`-ProvisioningSchemeName`) and the ID of the virtual desktop to lock (`-VMID`).



You can retrieve the virtual machine ID running the `Get-ProvVM` command discussed previously.

To reverse the machine lock and free the desktop instance from accidental deletion or improper use, you have to execute the `Unlock-ProvVM` cmdlet, using the same parameter shown for the lock procedure.

See also

- ▶ *Chapter 2, Configuring and Deploying Virtual Machines for XenDesktop®*

Managing additional components – the StoreFront Admin and Logging cmdlets

In this recipe, we will use and explain the way to manage and configure the StoreFront component using the available Citrix PowerShell cmdlets. Moreover, we will explain how to manage and check the configurations for system logging activities.

Getting ready

No preliminary tasks are required. You have already installed the Citrix XenDesktop PowerShell SDK during the installation of Desktop Controller role machine(s).

To be sure to be able to run a PowerShell script (.ps1 format), you have to enable script execution from the PowerShell prompt using the following command:

```
Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Force
```

How to do it...

In this section, we will explain and execute the commands associated with the Citrix Storefront system:

1. Connect to one of the Desktop Broker servers.
2. Click on the PowerShell icon installed on the Windows taskbar.
3. Load the Citrix PowerShell modules by typing the following command, and then press the *Enter* key:

```
Asnp Citrix*
```



To execute a command, you have to press the *Enter* key after completing the right command syntax.

4. Retrieve the currently existing StoreFront service instances by running the following command:

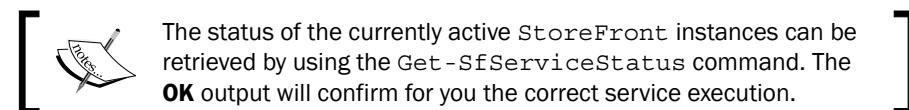
```
Get-SfService
```



To limit the number of rows as output result, you can add the `-MaxRecordCount <value>` parameter.

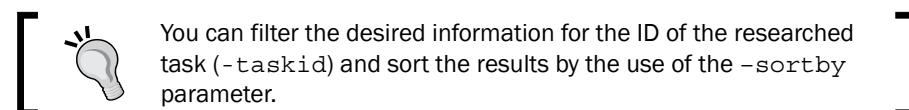
5. To list the detailed information about the StoreFront service(s) currently configured, execute the following command:

```
Get-SfServiceInstance -AdminAddress <ControllerAddress>
```



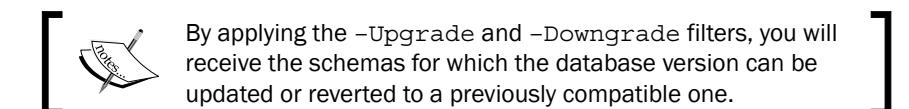
6. To list the task history associated with the configured StoreFront instances, you have to run the following command:

```
Get-SfTask
```



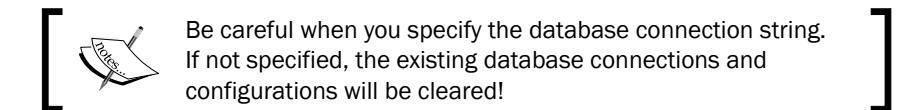
7. To retrieve the installed database schema versions, you can execute the following command:

```
Get-SfInstalledDBVersion
```



8. To modify the StoreFront configurations to register its state on a different database, you can use the following command:

```
Set-SfDBConnection -DBConnection <DBConnectionString>  
-AdminAddress <ControllerAddress>
```



9. To check that the database connection has been correctly configured, the following command is available:

```
Test-SfDBConnection -DBConnection <DBConnectionString>  
-AdminAddress <ControllerAddress>
```

10. The second discussed cmdlet is the Logging group. To retrieve information about the current status of the logging service, run the following command:

```
Get-LogServiceStatus
```

11. To verify the used language and whether the logging service has been enabled, run the following command:

```
Get-LogSite
```



Available configurable locales are: **en**, **ja**, **zh-CN**, **de**, **es**, and **fr**. Available states are: **Enabled**, **Disabled**, **NotSupported**, and **Mandatory**. The **NotSupported** state will show you an incorrect configuration for the listed parameters.

12. To retrieve detailed information about the running logging service, you have to use the following command:

```
Get-LogService
```



As discussed earlier for the StoreFront commands, you can filter the output by applying the `-MaxRecordCount <value>` parameter.

13. In order to get all the operations logged within a specified time range, run the following command. This will return the global operations count.

```
Get-LogSummary -StartDateRange <StartDate> -EndDateRange <EndDate>
```



The date format must be as follows:

AAAA-MM-GG HH:MM:SS.

14. To list the collected operations per day in the specified time range period, run the previous command in the following way:

```
Get-LogSummary -StartDateRange <StartDate> -EndDateRange <EndDate>
-intervalSeconds 86400
```



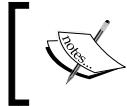
The value 86400 is the number of seconds that are present in a day.

15. To retrieve the connection string information about the database on which logging data is stored, execute the following command:

```
Get-LogDataStore
```

16. To retrieve detailed information about the high-level operations performed on the XenDesktop infrastructure, you have to run the following command:

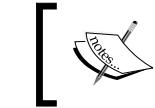
```
Get-LogHighLevelOperation -Text <TextincludedintheOperation>
-StartTime <FormattedDateandTime> -EndTime <FormattedDateandTime>
-IsSuccessful <true | false> -User <DomainUserName> -OperationType
<AdminActivity | ConfigurationChange>
```



The indicated filters are not mandatory. If you apply no filters, all the logged operations will be returned. This could be some very lengthy output.

17. The same information can be retrieved for low-level system operations in the following way:

```
Get-LogLowLevelOperation -StartTime <FormattedDateandTime>
-EndTime <FormattedDateandTime> -IsSuccessful <true | false>
-User <DomainUserName> -OperationType <AdminActivity |
ConfigurationChange>
```



In the *How it works* section, we will explain the difference between high-level and low-level operations.

18. To log when a high-level operation starts and stops, use the following two commands, respectively:

```
Start-LogHighLevelOperation -Text <OperationDescriptionText>
-Source <OperationSource> -StartTime <FormattedDateandTime>
-OperationType <AdminActivity | ConfigurationChange>
```

```
Stop-LogHighLevelOperation -HighLevelOperationId <OperationID>
-IsSuccessful <true | false>
```



The Stop-LogHighLevelOperation parameter must have a related Start-LogHighLevelOperation parameter because they are related tasks.

How it works...

In this latest section, we have discussed two newly introduced PowerShell command collections for the XenDesktop 7 versions: the cmdlet related to the StoreFront platform and the "activity logging" set of commands.

The first collection is quite limited in terms of operations, despite the other discussed cmdlets. In fact, the only actions permitted with the StoreFront PowerShell set of commands are retrieving configurations and settings about the configured stores and the linked database. Some more activities can be performed regarding the modification of existing StoreFront clusters using the `Get-SfCluster`, `Add-SfServerToCluster`, `New-SfCluster`, and `Set-SfCluster` sets of operations.

More interesting is the PowerShell Logging collection. In this case, you can retrieve all the system logged data, differentiating them in two principal categories:

- ▶ **High-level operations:** These tasks group all the system configuration changes that are executed by using Desktop Studio, Desktop Director, or Citrix PowerShell.
- ▶ **Low-level operations:** This category is related to all the system configuration changes that are executed by a service and not using the system software's consoles.



With the low-level operations discussed, you can filter for a specific high-level operation to which the low-level refers by specifying the `-HighLevelOperationId` parameter.

This cmdlet category also gives you the ability to track the start and stop of a high-level operation by the use of the `Start-LogHighLevelOperation` and `Stop-LogHighLevelOperation` parameters. In this second case, you have to specify the previously started high-level operation.

There's more...

In case of too much information in the log store, you have the ability to clear all of it. To refresh all the log entries, we use the following command:

```
Remove-LogOperation -UserName <DBAdministrativeCredentials> -Password  
<DBUserPassword> -StartDateRange <StartDate> -EndDateRange <EndDate>
```



The nonencrypted `-Password` parameter can be substituted by `-SecurePassword`, which is the password indicated in secure string form.

The credentials must be database administrative credentials with deleting permissions on the destination database.

This is a not reversible operation, so be sure that you want to delete the logs in the specified time range or verify that you have got some form of data backup.

See also

- ▶ The *Configuring the XenDesktop® logging* recipe in Chapter 8, *XenDesktop® Tuning and Security*

10

Configuring the XenDesktop® Advanced Logon

In this chapter, we will cover the following recipes:

- ▶ Implementing the two-factor hardware authentication for XenDesktop® 7
- ▶ Implementing strong authentication for XenDesktop® 7 using the RADIUS platform
- ▶ Implementing the two-factor software authentication for XenDesktop® 7

Introduction

Infrastructure security is an IT area that involves a lot of different technologies and implementation techniques. The same can be said about the Citrix XenDesktop architecture. As seen earlier, secure connections can be realized through the use of a secure gateway located in front of the entire VDI architecture. The implementation of a strong authentication method is another important step. In this chapter, we will discuss the use of hardware devices (such as Smart Cards, PKI tokens, and special USB keys that are used to authenticate users) to perform the login phase by using a valid certificate. Then, we will discuss how to configure a two-factor authentication with software tokens. At the end of this chapter, we will discuss about the implementation of a strong authentication logon method, a more robust and secure way to manage the user logon phase, using the **Remote Authentication Dial-In User Service (RADIUS)** platform.

Implementing the two-factor hardware authentication for XenDesktop® 7

With your personal data archived on your desktop machine, the standard authentication that is made up of a username and password combination could be insufficient to avoid privacy and security problems.

A valid solution to this situation is the use of devices such as Smart Cards or PKI tokens when trying to access your working resources.

Citrix XenDesktop is able to use this type of strong authentication. In this recipe, we will study the implementation of this process in detail.

Getting ready

In order to utilize valid certificates, you need to perform the following configuration tasks:

1. Use an existing Enterprise CA or install an Enterprise Certification Authority machine to generate valid certificates. You can find more information about this at <http://technet.microsoft.com/en-us/library/hh831740.aspx>.
2. Configure an existing domain machine as an enrollment agent station in order to configure the Smart Cards with your certificates. You can find more information at <http://technet.microsoft.com/en-us/library/hh831649.aspx>.
3. On the Enrollment agent station, install the specific CSP drivers for your authentication devices vendor.
4. On the StoreFront server, make sure that you have installed the Client Certificate Mapping Authentication service for the IIS 8 installed role.



You have to be a member of the Enterprise Admins group in order to generate and release a certificate on the authentication devices.

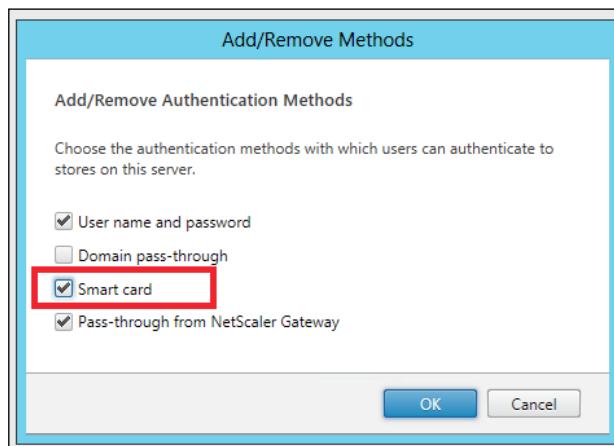


How to do it...

In this recipe, we will explain how to authenticate users by using the Smart Cards or PKI tokens with a personal certificate on board:

1. Connect to the StoreFront machine, and run the StoreFront console by searching for it within the Windows Apps catalog (press the Windows + C key combination, click on the **Search** button, and search for the **Citrix StoreFront** application).
2. Click on the **Authentication** link on the left-hand side menu, and then select the **Add/Remove Methods** link on the right-hand side menu.

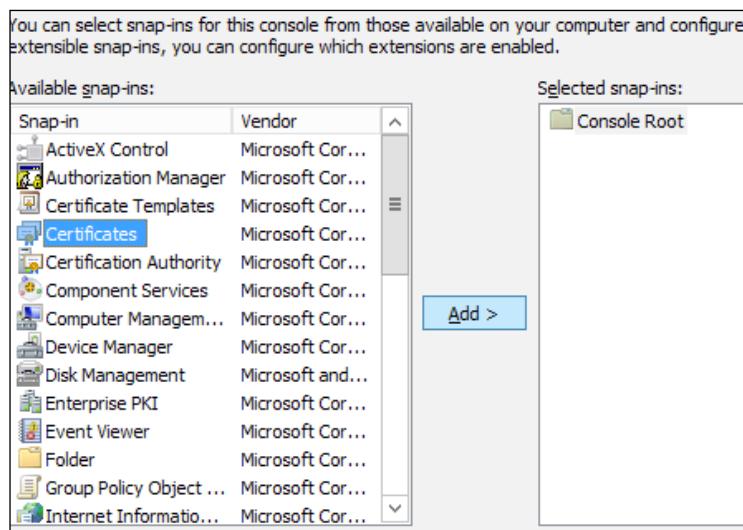
3. Check the **Smart card** option on the pop-up screen in order to enable it. Then, click on the **OK** button as shown in the following screenshot:



Citrix recommends us to have a configured store for each authentication method. Consider creating a different store for any kind of logon.



4. Connect to your Enrollment station machine, press the Windows + X key combination, select the **Run** link, and run the `mmc` command.
5. Use the **Ctrl + M** key combination to open the snap-in selection menu, double-click on the **Certificates** snap-in from the list, and click on the **Add** button.

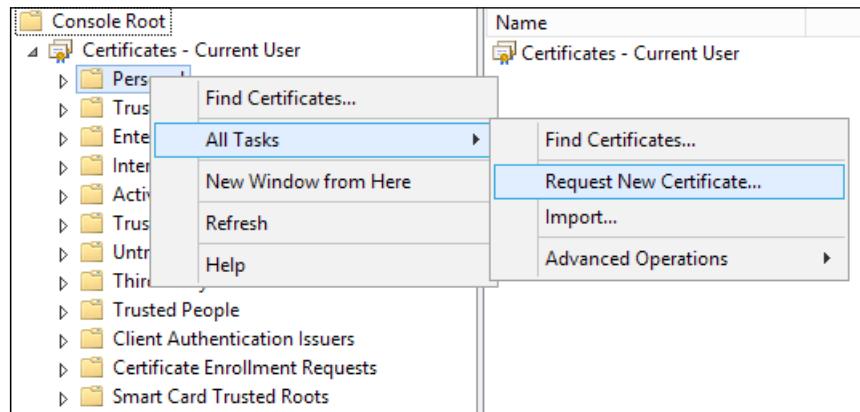


Configuring the XenDesktop® Advanced Logon

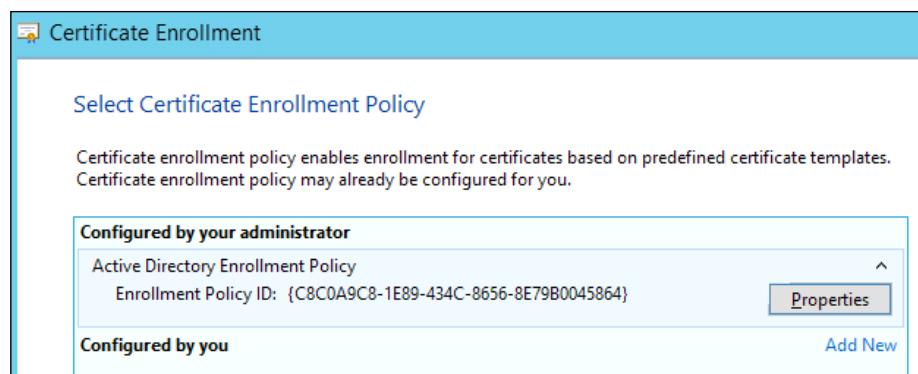
6. When prompted for the selection, choose the **My User account** as a certificate store and click on **Finish**. To end the console selection, click on the **OK** button.



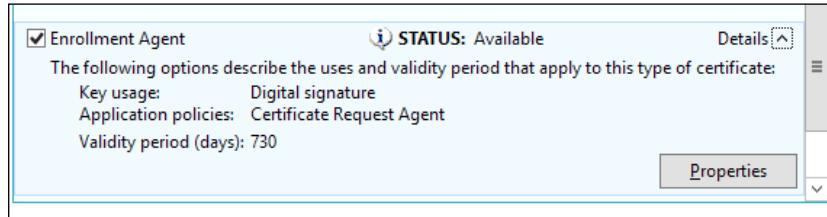
7. Expand the **Certificates - Current User** tree, right-click on the **Personal** folder, select **All tasks**, and click on the **Request new certificate** link, as shown in the following screenshot:



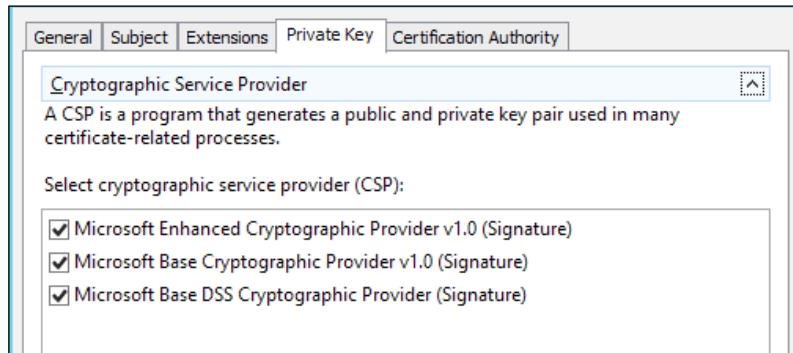
8. Click on **Next** in the **Before You Begin** section, select **Active Directory Enrollment Policy**, and click on the **Next** button:



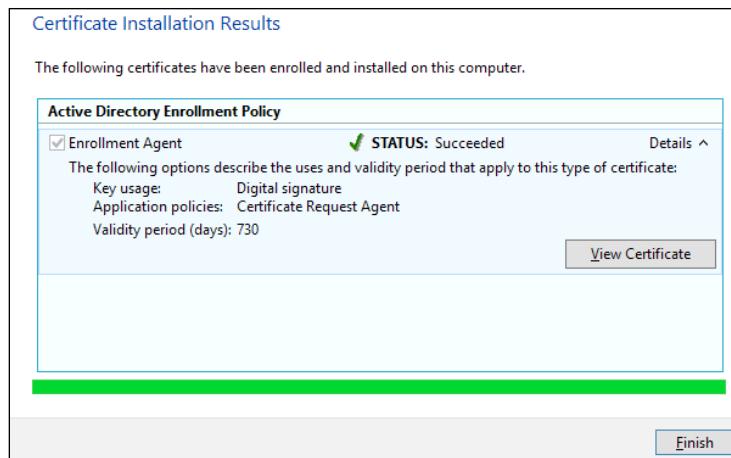
9. Check the **Enrollment Agent** option, expand it, and click on the **Properties** button, as shown in the following screenshot:



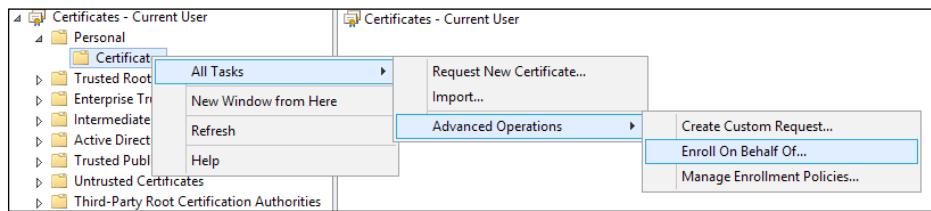
10. In the **Private Key** tab, expand the **Cryptographic Service Provider** option and verify that the **Microsoft Base Cryptographic Provider v1.0 (Signature)** option has been flagged. After completing these steps, click on **OK**.



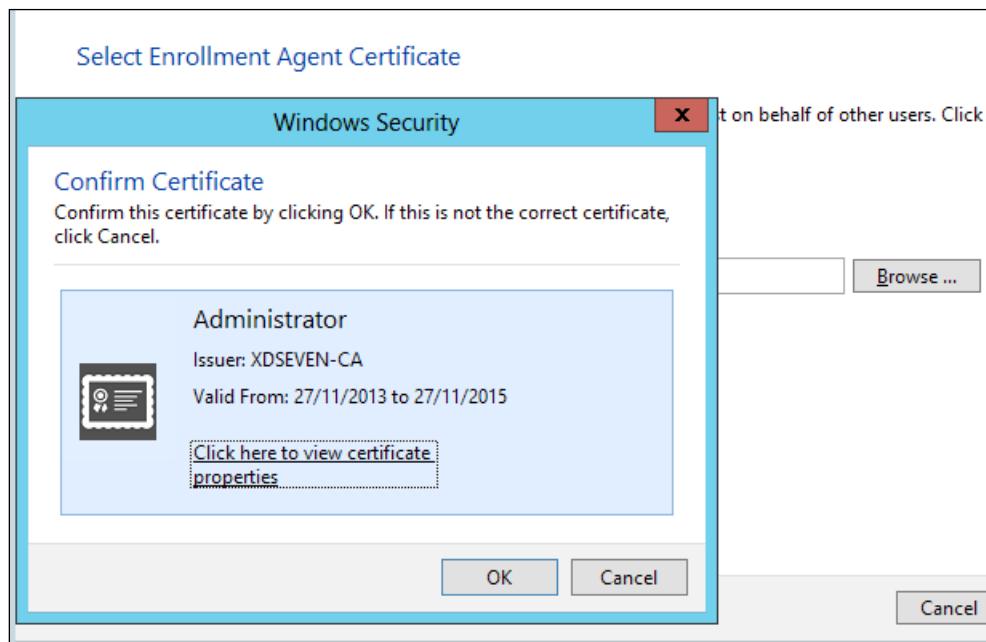
11. On the **Certificate Enrollment** screen, click on the **Enroll** button to generate the certificate request. After completing these steps, click on the **Finish** button.



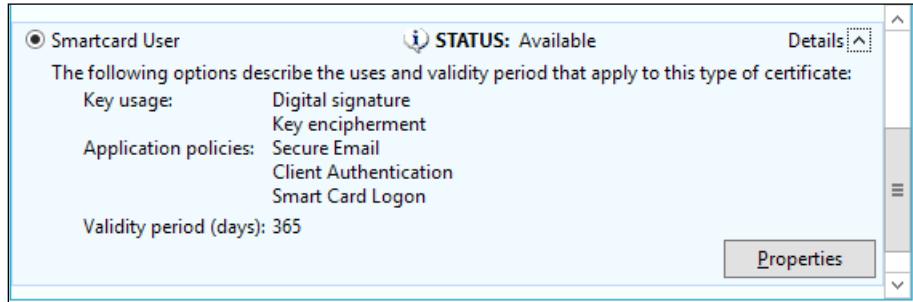
12. Expand the **Personal** folder, then right-click on **Certificates**, navigate to **Advanced Operations** in the **All Tasks** option, and click on the **Enroll On Behalf Of** link, as shown in the following screenshot:



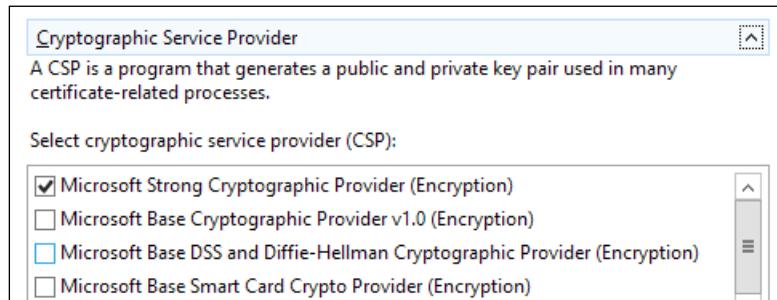
13. Click on the **Next** button in the **Before You Begin** section, select the **Active Directory Enrollment Policy** option, and click on the **Next** button.
14. Click on **Browse** on the **Select Enrollment Agent Certificate** screen, choose the certificate previously generated, and click on the **OK** button. After completing these steps, click on **Next** to proceed.



15. In the **Request Certificates** section, select the **Smartcard User** radio button, expand this section, and click on **Properties**, as shown in the following screenshot:



16. Expand the **Cryptographic Service Provider** section in the **Private Key** tab, and select your vendor-specific CSP. After completing this step, click on **OK** to exit from the **Properties** menu. Then, click on **Next** to continue.



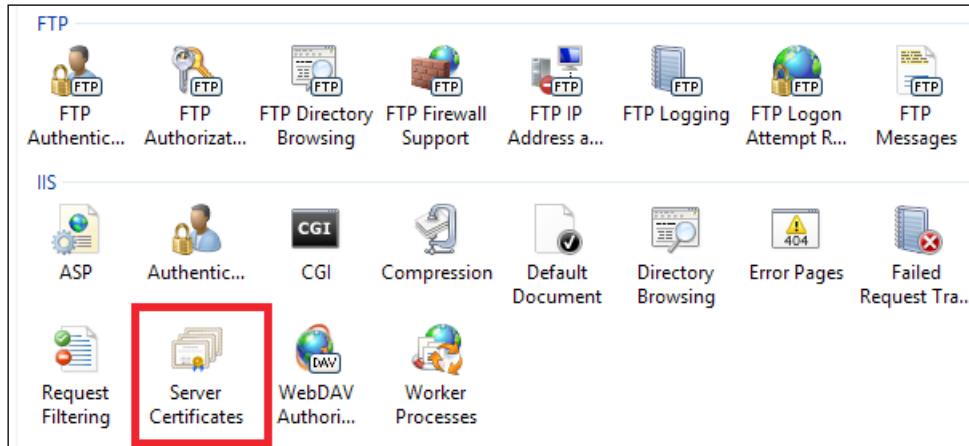
17. In the **Select a user** screen, browse your domain for the user for whom you want to enroll the certificate. After selecting, click on the **Enroll** button.
18. When required, insert the Smart Card / PKI token device and wait for the completion of the enrollment process. After completing these steps, click on **Close** to stop the certificate distribution, or click on the **Next User** button to continue for another user.
19. Connect to the StoreFront server and run the **Internet Information Services (IIS) Manager** by searching for it within the Windows Apps catalog (press the Windows + C key combination, click on the **Search** button, and search for the IIS application).



All the next configuration steps will be performed for the IIS 8 Version.

Configuring the XenDesktop® Advanced Logon

20. In the IIS management console, select the server name from the left-hand side menu. Then, on the central window zone, double-click on the **Server Certificates** icon in the IIS section.



21. Click on the **Create Certificate** link on the right-hand side menu, populate all the fields, and click on **Next** to continue.

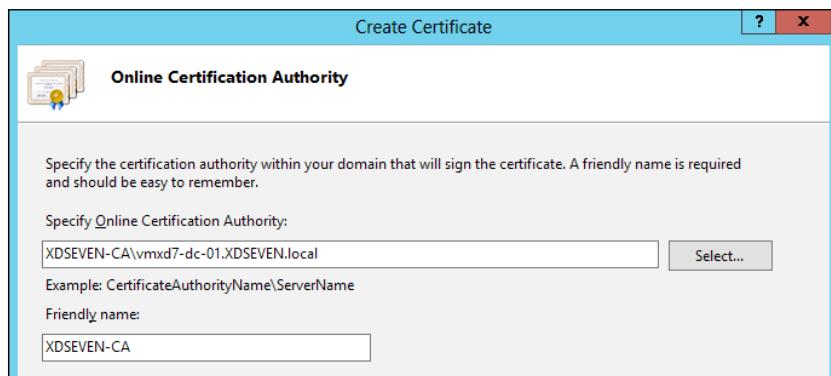
The screenshot shows the 'Create Certificate' wizard with the title 'Create Certificate' at the top. Below it is a section titled 'Distinguished Name Properties' with a small icon of three certificates. The main area contains a note: 'Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.' Below this are six input fields:

Common name:	vmxd7-sf-01.xdseven.local
Organization:	Packt Publishing
Organizational unit:	Enterprise
City/locality	Birmingham
State/province:	England
Country/region:	UK

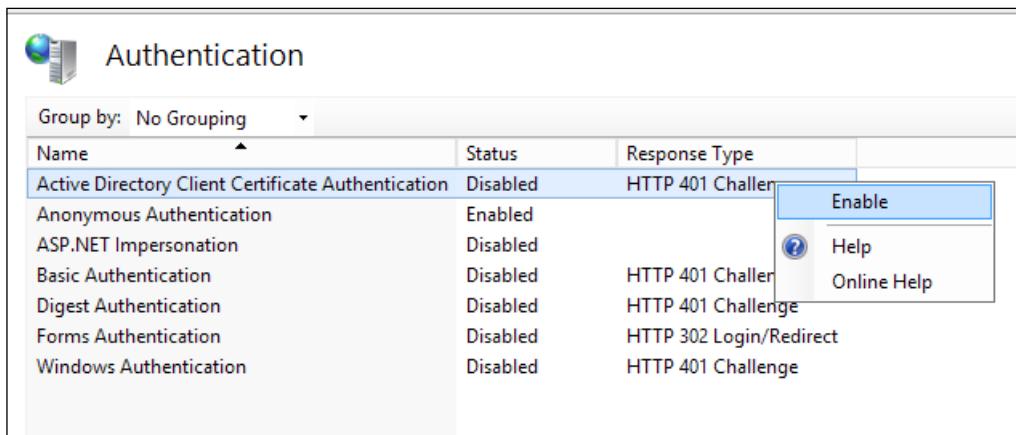


In the **Common name** field, you have to insert the **Full Qualified Domain Name (FQDN)** of the Citrix StoreFront server.

22. In the **Online Certification Authority** section, click on the **Select** button and choose your configured Certification Authority. Populate the **Friendly name** field with a value referring to your CA, and then click on **Finish** to complete.

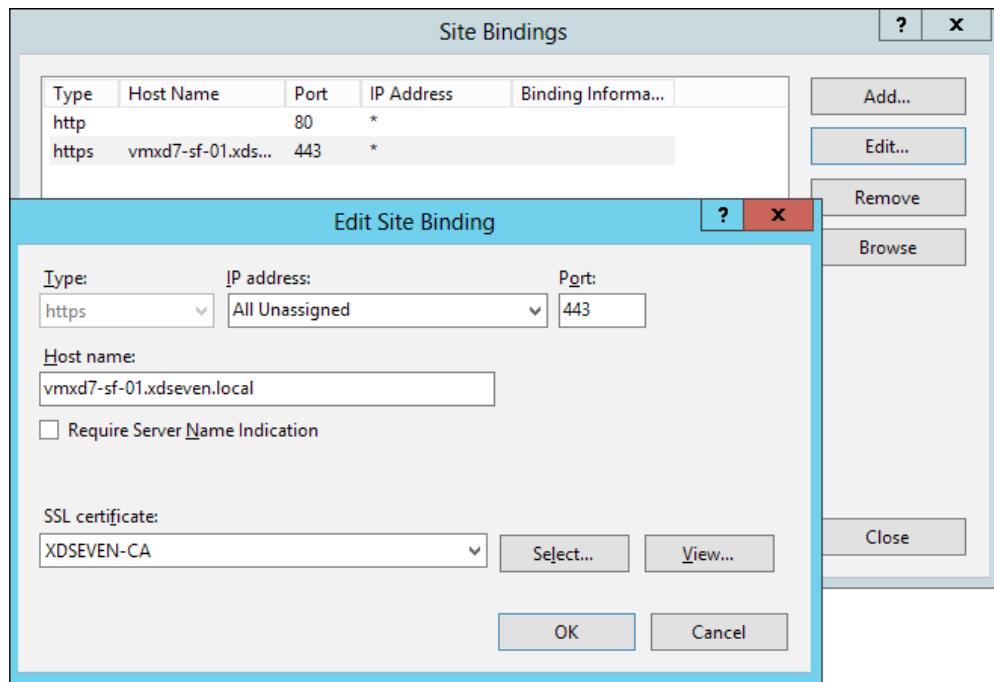


23. Click again on the server name on the left-hand side menu, double-click on the **Authentication** icon in the IIS section, enable the **Active Directory Client Certificate Authentication** option by right-clicking on it, and select **Enable**, as shown in the following screenshot:

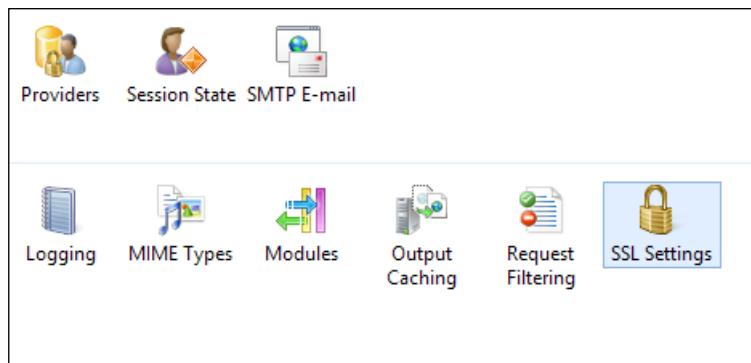


Configuring the XenDesktop® Advanced Logon

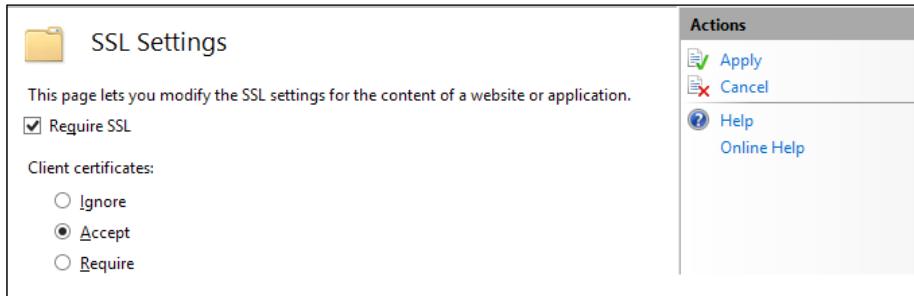
24. In the left-hand side menu, select the **Default Web Site** link and then click on the **Bindings** option in the right-hand side menu.
25. Click on the **Add** button in the **Site Bindings** screen and configure the HTTPS protocol **Type**, the **IP Address**, and the **Host name**. All these parameters are configured for the StoreFront store with the Smart Card authentication and the existing **SSL Certificate** from the drop-down list. After completing these steps, click on **OK** first, and then click on **Close** to exit from the bindings menu.



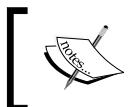
26. In the left-hand side menu, expand the **Default Web Site** tree, select the **Citrix** folder, and double-click on the **SSL Settings** icon in the central part of the menu.



27. Select the **Require SSL** option, and select the **Accept** radio button for the **Client certificates** section. Click on the **Apply** link on the right-hand side menu to confirm your choice, as shown in the following screenshot:



28. Add the StoreFront site to the Trusted Site zone of your browser. Then, insert your Smart Card / PKI token in the appropriate device drive and connect to the configured store by using the Citrix Receiver on your physical machine. If required, type the associated PIN in your authentication hardware token. It's now possible to complete the authentication phase using the Smart Card authentication method.



The Smart Card authentication is only supported when we use the Citrix Receiver to authenticate StoreFront. The website store is not able to use this kind of authentication (not supported by default).

How it works...

The use of Smart Cards / tokens with the Citrix StoreFront platform permits the users to authenticate in a stronger and more secure way. In fact, they can access the assigned resources only by presenting the personal certificate installed on the physical support.

In this recipe, we have implemented the XenDesktop strong authentication in three different stages:

- ▶ **Enterprise Certification Authority and Enrollment Station:** Even if not explicitly discussed, creation of an Enterprise CA (based on, for instance, the Microsoft CA), configuration of an Enrollment Station through which the generated certificate request will be assigned to the Windows domain users, and registration of this certificate on the Smart Card or PKI token device are the prerequisites to complete the strong authentication configuration. The association between the certificate and the physical device is granted by the **Cryptographic Service Provider (CSP)**, which can be based on the Microsoft native library (using a generic and compatible Smart Card device), or it is equipped by the vendor of the token you've decided to use.

- ▶ **Web Server – IIS 8:** At this stage, the fundamental step is to implement the SSL for the web server machine, which hosts the StoreFront store site (usually the StoreFront machine itself). First of all, it's necessary to have a domain certificate to the previously configured CA. This certificate will then be used to bind the default IIS website configuration on the SSL port (443) in order to establish a secure connection using the HTTPS protocol. Moreover, it's also necessary to enable the SSL at the web server level. We've completed it by navigating to the SSL settings zone, enabling the secure protocol, and accepting the client certificates.
- ▶ **StoreFront:** At the StoreFront level, it is possible to use the existing website (not recommended), or create a new one only for the strong authentication type (the recommended solution). The configuration is based on the enabling of the authentication method based on the **Smart Card** option.

There's more...

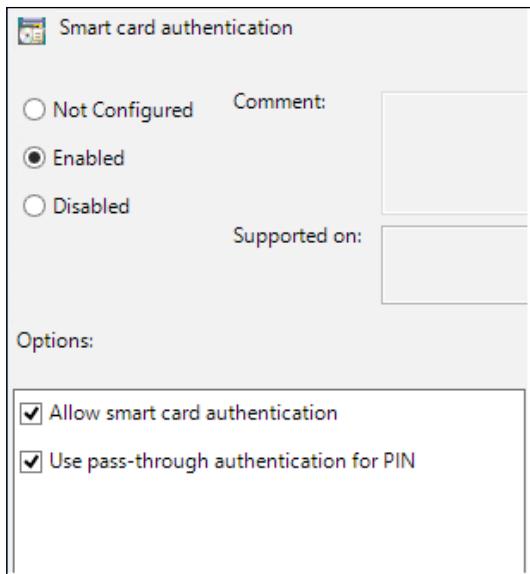
With StoreFront, it's also possible to use an alternative Smart Card logon technique—the pass-through with Smart Card authentication. This method is able to re-use the user credentials from the physical machine (at the first logon step), eliminating the need for retyping the logon information every time.

To correctly configure this option, you need to insert the StoreFront site in the **Local Intranet** zone of your web browser (instead of the **Trusted Site** zone previously used for the standard Smart Card mode). Then, enable the SSL in the **SSL Settings** zone; but this time, configure the **Client Certificates** section with the **Ignore** value.

On the Smart Card reader client machine, open the Local Policy editor in the following ways:

- ▶ For Windows 7 physical devices, click on **Start**, go to **Run**, and type the `gpedit.msc` command
- ▶ For Windows 8 physical devices, press the Windows + X key combination, select the **Run** link, and type the `gpedit.msc` command

After you've executed the Group Policy editor, import the `icaclient.adm` template located at your Citrix Receiver installation (usually `C:\Program Files (x86)\Citrix\ICA Client\Configuration`) and enable the **Smart Card authentication** policy located at **Computer Configuration | Administrative Templates | Classic Administrative Templates (ADM) | Citrix Components | Citrix Receiver | User authentication** to configure it, as shown in the following screenshot:



Connect to the StoreFront server and open the `default.ica` file with a text editor. This file is located at the IIS configured store path (by default, `C:\inetpub\wwwroot\Citrix\<StoreName>\App_Data`). Once the file is opened, add the **DisableCtrlAltDel=Off** option in the **Application** section.

```
[Application]
TransportDriver=TCP/IP
DoNotUseDefaultCSL=On
BrowserProtocol=HTTPonTCP
LocHttpBrowserAddress=!
WinStationDriver=ICA 3.0
ProxyTimeout=30000
AutologonAllowed=ON
DisableCtrlAltDel=Off
```

 The previously configured parameter is for the connection made without a NetScaler platform. In the presence of a NetScaler Gateway, the parameter to configure in the **Application** section is **UseLocalUserAndPassword=On**.

See also

- ▶ The *Installing and configuring Citrix® NetScaler Gateway 10.1* recipe in Chapter 8, *XenDesktop® Tuning and Security*

Implementing strong authentication for XenDesktop® 7 using the RADIUS platform

An alternative method to the Smart Card authentication is the two-factor authentication. This strong authentication type forces the user to connect to the assigned resources by using the password and a second authentication key. In this recipe, we're going to discuss the configuration of the Remote Authentication Dial-In User Service (RADIUS) authentication with the Citrix NetScaler Gateway, which is a strong authentication type based on the combination of a username, a password, and a preshared key that can be delivered in the form of a static key or as a **One-Time Password (OTP)**.

Getting ready

In order to implement the strong authentication method discussed earlier, you have to install a RADIUS server. This task can be accomplished by using the Microsoft RADIUS role **Network Policy Server (NPS)** or by installing a Linux-based authentication server, such as **FreeRADIUS**.



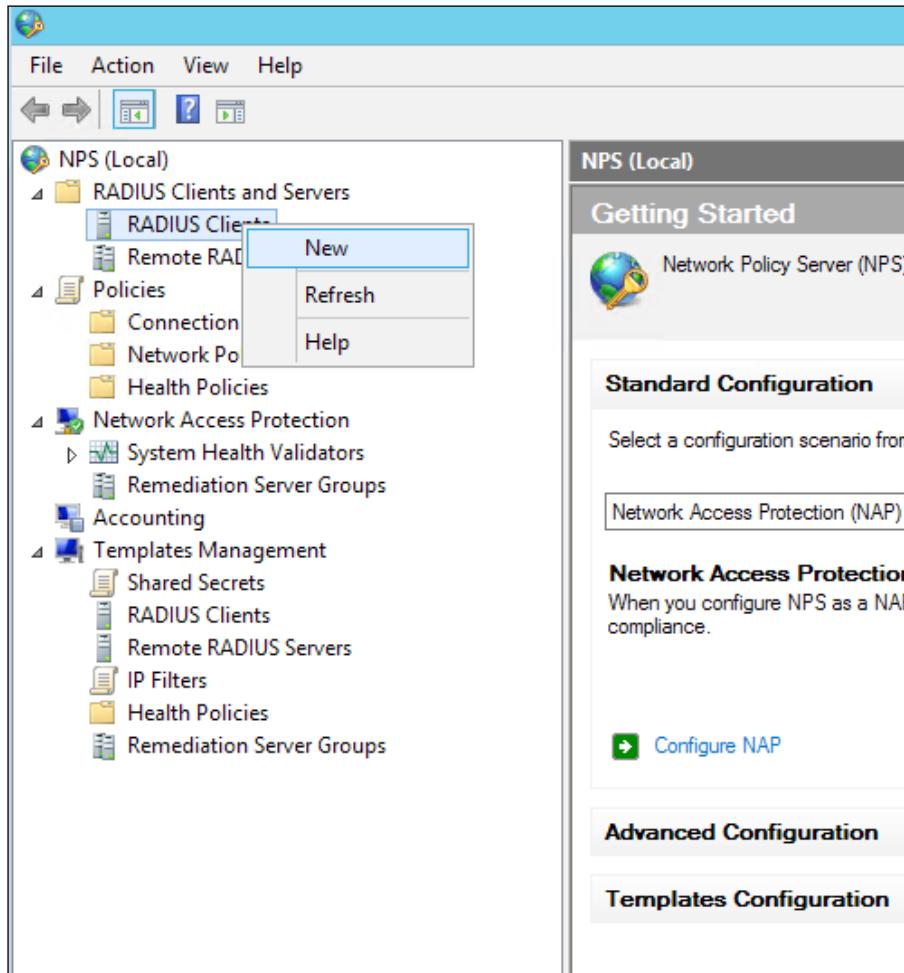
In this recipe, we will use the Windows version of the RADIUS server by installing the Network Policy Server role on a Windows Server 2012 machine. You can find more information about the installation procedure at [http://technet.microsoft.com/en-us/library/cc725922\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc725922(v=ws.10).aspx).

How to do it...

In this section, we will explain how to configure a Windows RADIUS server in order to implement a multifactor authentication through the Citrix StoreFront platform:

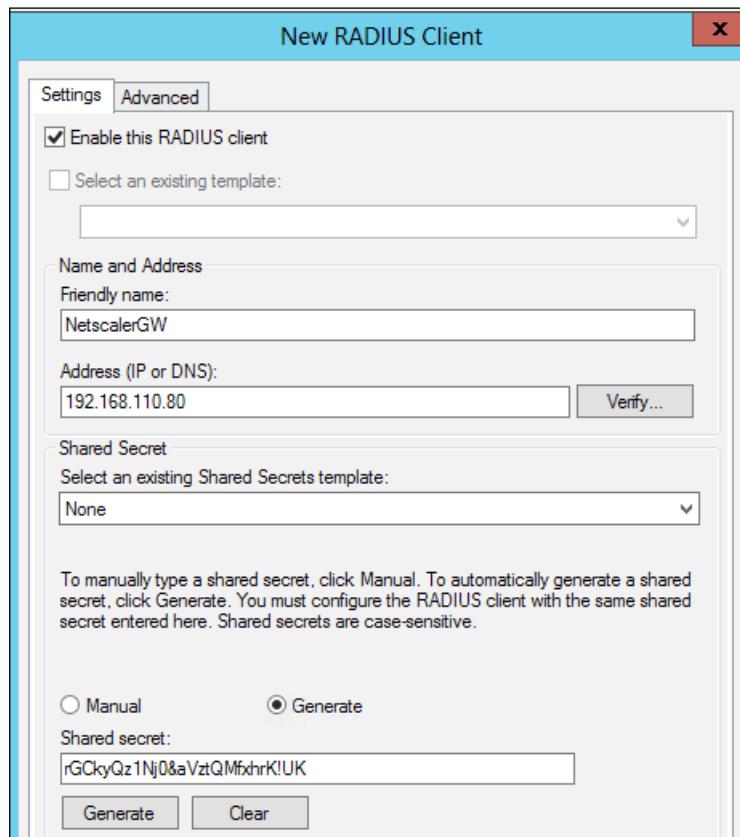
1. Connect to the Windows RADIUS (NPS) server with domain administrator credentials, and run the Network Policy Server by searching for it within the Windows Apps catalog (press the Windows + C key combination, click on the **Search** button, and search for the Network Policy Server application).

2. In the left-hand side menu, expand the **RADIUS Clients and Servers** folder, right-click on the **RADIUS Clients** link, and select **New**, as shown in the following screenshot:



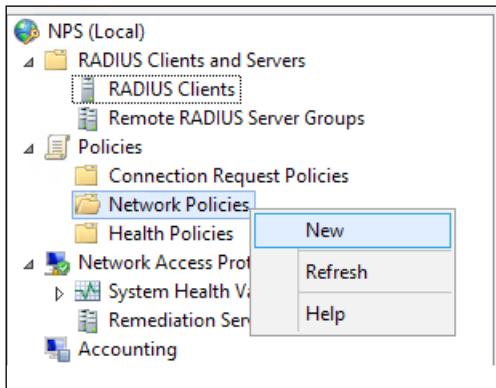
Configuring the XenDesktop® Advanced Logon

3. Assign an identification name to populate the **Friendly name** field, then insert the IP address or the FQDN of your NetScaler Gateway machine (NSIP, NetScaler IP Address), and insert a shared secret key by selecting the **Manual** radio button and typing the security code, or use a randomly generated secret code by selecting the **Generate** radio button and clicking on the **Generate** button. After completing these steps, click on **OK**.

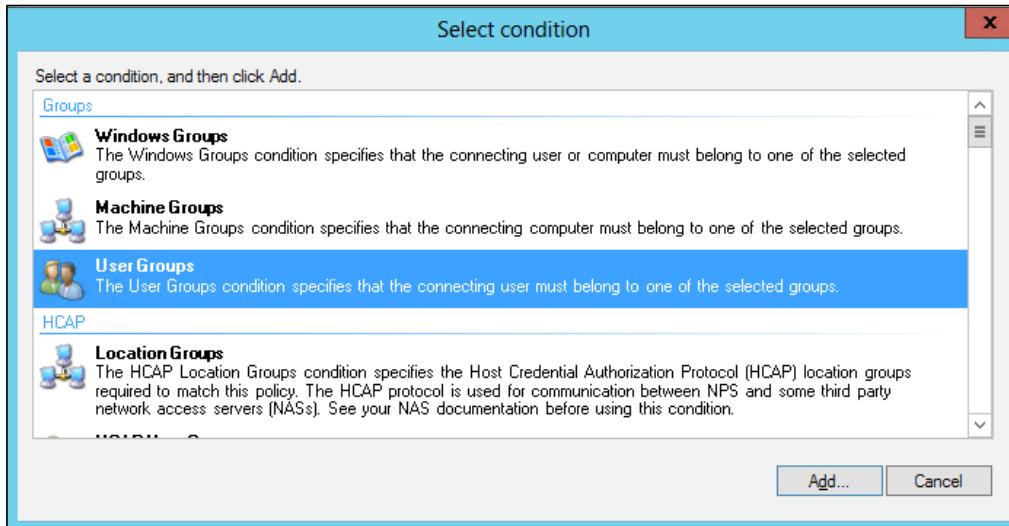


Remember that the secret key is case sensitive, so you have to be careful when using it in the client configuration phase.

4. Expand the **Policies** section in the left-hand side menu, right-click on the **Network Policies** folder, and select the **New** link.

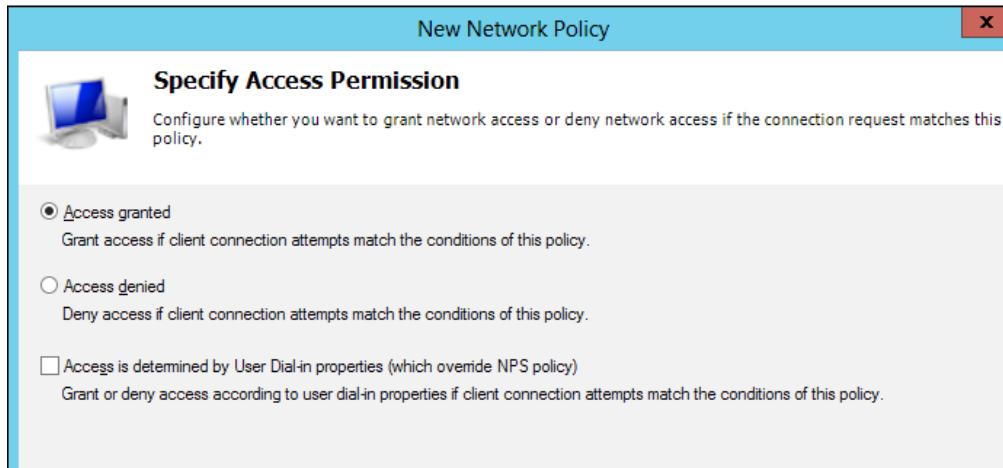


5. Assign a name to the policy in the **Policy name** field, select the **Unspecified** option for the **Type of network access server** section, and click on **Next** to continue.
6. Click on the **Add** button in the **Select condition** screen, select the **User Groups** option from the list, and click on the **Add...** button, as shown in the following screenshot:

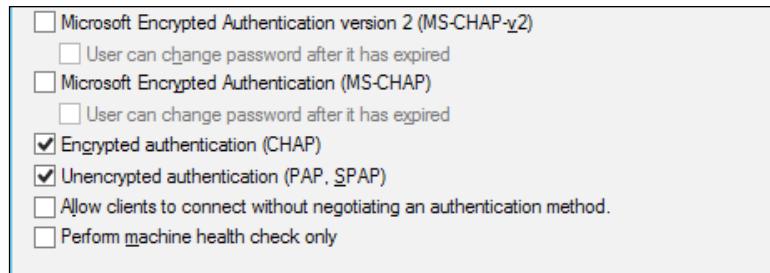


7. In the **User Groups** screen, click on the **Add Groups** button and browse for the domain group for which you want to configure the strong authentication. After completing these steps, click on **OK** to close the pop-up screen. Then click on the **Next** button to proceed with the configuration.

8. In the **Specify Access Permission** section, select the **Access granted** radio button and click on **Next**, as shown in the following screenshot:



9. In the **Configure Authentication Methods** screen, clear any configured option and check one of the supported authentication methods (CHAP, MS-CHAP v1/v2, and PAP). After completing these steps, click on **Next**.



10. In the **Configure Constraints** section, you can configure specific connection options such as **Idle Timeout**, **Session Timeout**, or **Day and time restrictions**. After completing, click on **Next** to proceed.



These are collateral options that are not essential for the correct functioning of the RADIUS server that is connected to the NetScaler Gateway platform.

11. In the **Configure Settings** screen, remove the configured attributes under the **Standard** category by selecting the desired attribute and clicking on the **Remove** button.

New Network Policy

Configure Settings

NPS applies settings to the connection request if all of the network policy conditions matched.

Configure the settings for this network policy. If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

RADIUS Attributes	To send additional attributes to RADIUS clients, select a RADIUS attribute from the list, then click Edit. If you do not configure an attribute, it is not sent to your RADIUS client documentation for required attributes.
<input checked="" type="checkbox"/> Standard	
<input type="checkbox"/> Vendor Specific	
Network Access Protection	
<input type="checkbox"/> NAP Enforcement	
<input type="checkbox"/> Extended State	
Routing and Remote Access	
<input type="checkbox"/> Multilink and Bandwidth Allocation Protocol (BAP)	
<input type="checkbox"/> IP Filters	
<input type="checkbox"/> Encryption	
<input checked="" type="checkbox"/> IP Settings	

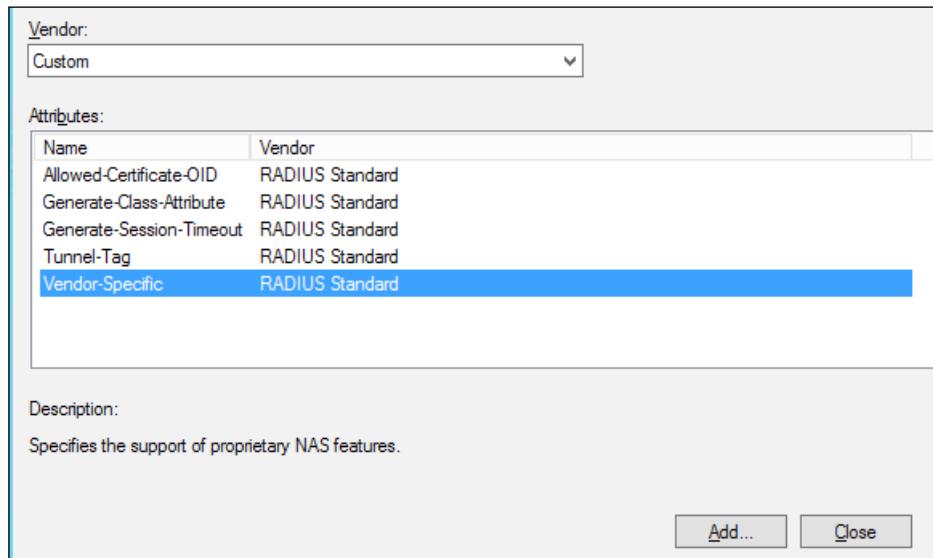
Attributes:

Name	Value
Framed-Protocol	PPP
Service-Type	Framed

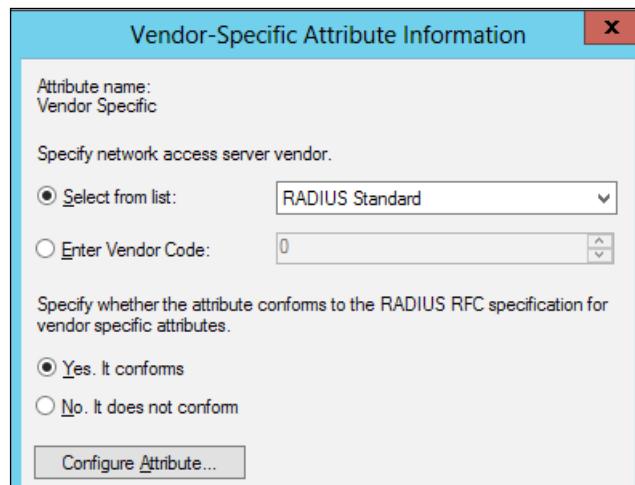
Add... **Edit...** **Remove**

Configuring the XenDesktop® Advanced Logon

12. In the left-hand side menu, select the **Vendor Specific** option, click on **Add**, choose the **Custom** option from the **Vendor** list, and select the **Vendor-Specific** attributes. After selecting, click on the **Add** button. This is shown in the following screenshot:



13. In the **Attribute Information** screen, click on the **Add** button. In the **Vendor-Specific Attribute Information** menu, choose the **RADIUS Standard** option for the **Select from list** section and select the **Yes. It conforms** radio button.



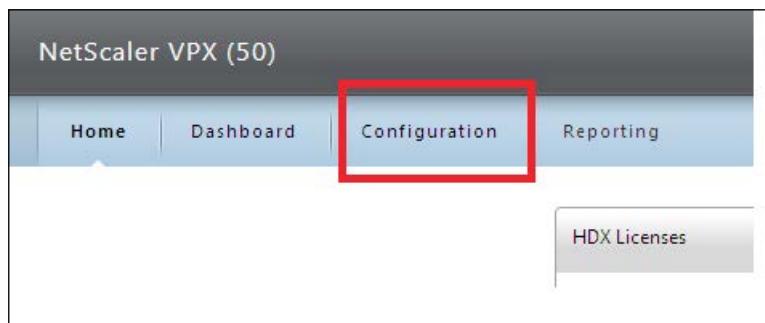
14. After these selections, double-click on the **OK** button and then close to complete the configuration. In the **Configure Settings** main screen, click on the **Next** button to continue.
15. In the **Completing New Network Policy** section, click on **Finish** to complete the procedure.
16. In the **Network Policies** section, be sure that the created rule has a higher priority than other configured rules.

Policy Name	Status	Processing Order
NetscalerGW-Policy-01	Enabled	1
Connections to Microsoft Routing and Remote Access server	Enabled	999998
Connections to other access servers	Enabled	999999

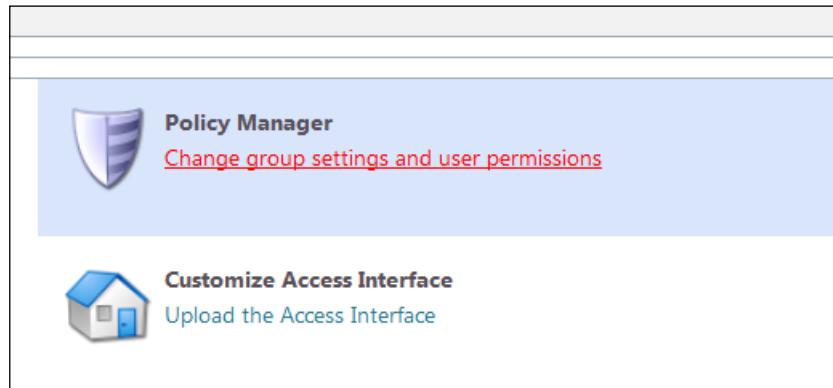
17. Open a compatible web browser. In the address bar, type the address previously assigned to the virtual appliance.
18. Insert the web portal credentials (default: nsroot), select **NetScaler Gateway** as the **Deployment Type** option, and click on the **Login** button to continue.

[ We have discussed the installation and configuration of the NetScaler Gateway platform in *Chapter 8, XenDesktop® Tuning and Security*.]

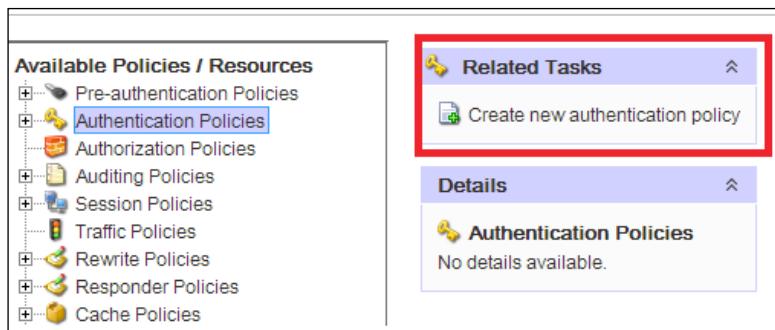
19. After you've been logged in, click on the **Configuration** button in the main menu option bar.



20. In the **Configuration** section, click on the **NetScaler Gateway** link. Then select the **Change group settings and user permissions** link in the **Policy Manager** section.



21. Select the **Authentication Policies** link in the **Available Policies / Resources** section, and then click on **Create new authentication policy**.



22. In the **Create Authentication Policy** pop-up screen, assign a name to the created policy, select the **RADIUS** option in the **Authentication Type** drop-down list, and click on the **New** button in the **Server** section, as shown in the following screenshot:

A screenshot of the "Create Authentication Policy" dialog box. It has several input fields: "Name*" with the value "Policy_Radius", "Authentication Type" dropdown set to "RADIUS", "Server" dropdown set to "No configured Servers-", and an "Expression" section with a large text area labeled "Expression". There are also "New..." and "Modify..." buttons next to the server dropdown.

23. In the **Create Authentication Server** screen, assign a name to the configured RADIUS server and fill the following fields:

- ❑ **IP Address:** This is the RADIUS IP address
- ❑ **Port:** This is the RADIUS configured port
- ❑ **Secret Key:** This is the RADIUS secret key
- ❑ **Password Encoding:** This is the password encoding type

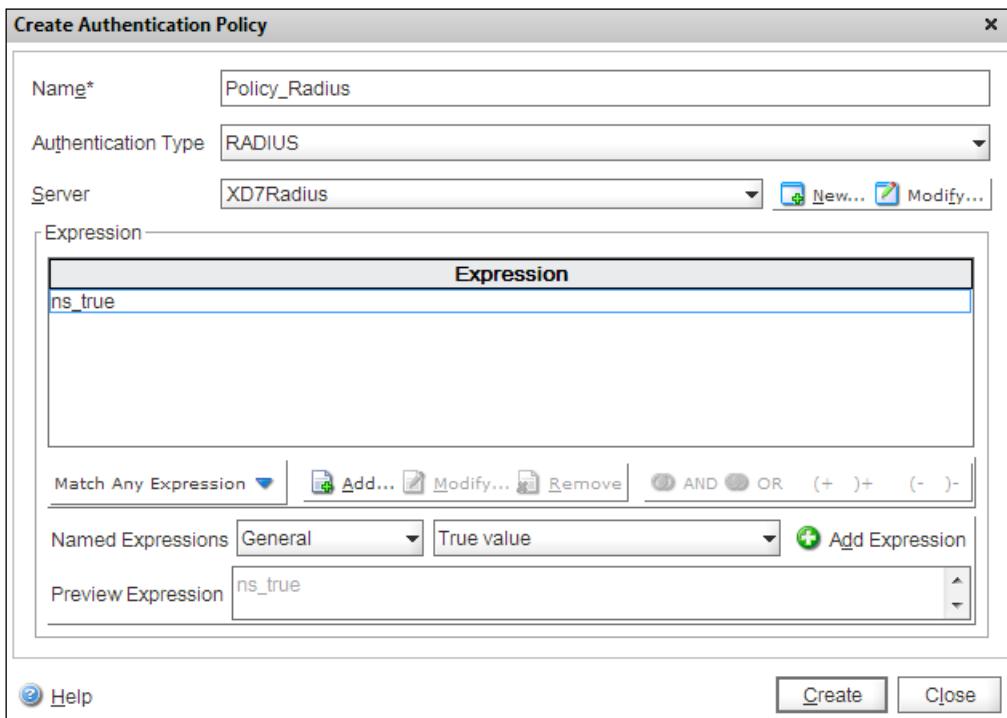
After completing these steps, click on the **Create** button.

Create Authentication Server

Name*	XD7Radius
Authentication Type	RADIUS
Server	
IP Address*	192 . 168 . 110 . 47
IPv6	<input type="checkbox"/>
Port	1812
Details	
Secret Key*	*****
Confirm Secret Key*	*****
<input type="checkbox"/> Send Calling Station ID	
Group Vendor Identifier	
Group Attribute Type	
IP Address Vendor Identifier	
Password Vendor Identifier	
Password Encoding	pap
Default Authentication Group	<input type="button" value="pap"/> <input type="button" value="chap"/> <input type="button" value="mschapv1"/> <input type="button" value="mschapv2"/>

Configuring the XenDesktop® Advanced Logon

24. In the **Expression** section, select the **General** value configured to **True value** for the **Named Expressions** field, click on the **Add** expression, and click on the **Create** button to complete the procedure. Then click on **Close** to return to the previous menu.



25. After completing the configuration steps, the NetScaler Gateway will be available to authenticate users by contacting the configured RADIUS platform.

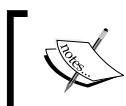
How it works...

RADIUS is a strong authentication method based on the same protocol, which is an AAA (Authentication, Authorization, and Accounting) kind of platform used as a network resource regulator, in order to manage the access to the network resources.

The first operation executed in this recipe, Microsoft RADIUS server configuration, was done using the Network Policy Server (NPS) role that was configured on the Windows Server 2012 machine. In order to let the RADIUS platform communicate with the NetScaler Gateway Virtual Appliance, the second factor has to be configured as a client under the RADIUS server. To accomplish this task, it is necessary to insert the FQDN or the IP address of the NetScaler platform, which will generate a secret key that will be used as the second authentication factor.

This code should be complex in order to make its cracking harder. On the other hand, it should be not too long, because some clients may not be able to read and use it.

After the RADIUS configuration has been completed, this authentication method needs to be configured under the NetScaler Gateway platform. This task can be accomplished by configuring the RADIUS parameters (the IP, name, and secret key that was previously generated) within the **Policy Manager** section. In this way, RADIUS will be considered as a secondary authentication method, permitting the filtering and blocking of users who have no rights within your XenDesktop infrastructure.



Access to the published resources is given by the configuration of the domain groups under the Windows NPS network policy category.



There's more...

It's possible to configure the NetScaler to obtain the IP addresses that will be directly assigned to the users by the RADIUS server. This is IP Address Extraction configuration.

To use this configuration, you have to set the following two parameters:

- ▶ The Vendor Identifier (ID), which permits the release of the local IP addresses to the users who make a request.
- ▶ The attribute type, which is a value from 1 to 255 (equal to the remote IP RADIUS response).

To configure the NetScaler, you have to connect to the NetScaler Gateway, modify the configured authentication policy for RADIUS, type the required vendor ID, and check the **Enable NAS IP address extraction** option.



We have already discussed the RADIUS policy creation in this recipe.



The screenshot shows the 'Server' configuration page for a RADIUS policy. The 'Server' tab is selected. The 'IP Address*' field contains '192 . 168 . 110 . 47'. The 'Port' field is set to '1812'. The 'Time-out (seconds)' field is set to '3'. In the 'Details' section, there are fields for 'Secret Key*' and 'Confirm Secret Key*', both containing masked values. A checkbox 'Send Calling Station ID' is unchecked. To the right, there is a section for 'NAS ID' with a value of '1' and a checked checkbox 'Enable NAS IP address extraction'. This entire section is highlighted with a red rectangle.

See also

- ▶ The *Installing and configuring Citrix® NetScaler Gateway 10.1* recipe in Chapter 8, *XenDesktop® Tuning and Security*

Implementing the two-factor software authentication for XenDesktop® 7

An alternative method to the Smart Card authentication is two-factor software authentication. This strong authentication type forces the user to connect to the assigned resources using the password and a second authentication key, a **One-Time Password (OTP)** token that is usually sent to the user's e-mail address or mobile device. In this recipe, we're going to discuss the configuration of a specific platform that permits the use of this kind of authentication—the SMS2 software developed by the WrightCCS company.

Getting ready

For this recipe, the following tasks and configurations are required:

- ▶ You need to download the SMS2 software from the following link: <http://www.wrightccs.com/get/>. Insert the required data, and wait for the download link and the activation code that will be sent to the specified e-mail address.
- ▶ To install the software domain, administrator credentials are needed for the Windows Server 2012 machine on which you're going to install SMS2. You also need a SQL Server machine to create the SMS2 database.
- ▶ A previously configured RADIUS platform is needed in order to interact with the platform.
- ▶ A previously configured NetScaler Gateway platform is needed in order to interact with the platform.

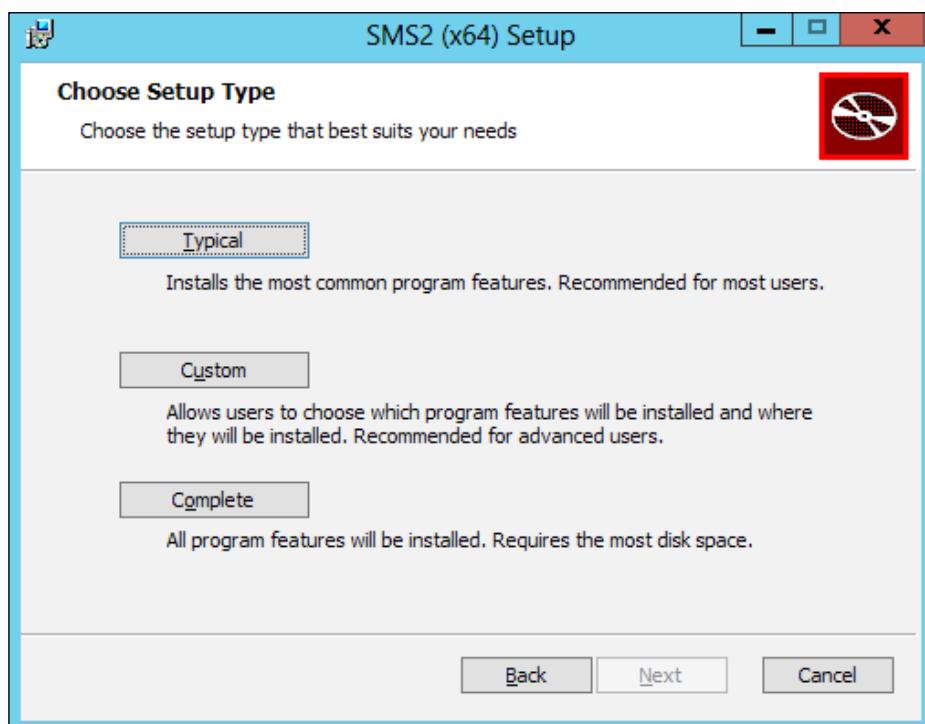


Refer to the previous recipe to check the NPS RADIUS and NetScaler Gateway configurations for strong authentication.

How to do it...

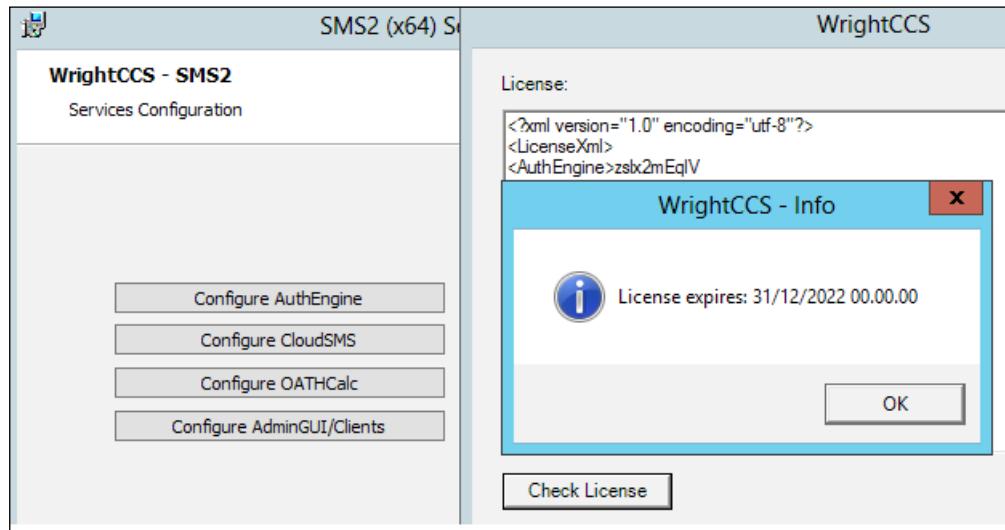
The following steps are required to install and configure the SMS2 two-factor authentication software:

1. Connect to the Windows Server 2012 selected as the SMS2 server with domain administrator credentials.
2. Locate the downloaded setup (use the `.x86_rg.msi` extension for 32-bit and the `.x64.msi` extension for 64-bit Version) and double-click on it.
3. On the **Welcome** screen, click on the **Next** button to continue.
4. In the **Choose Setup Type** section, select the **Complete** installation option.



Configuring the XenDesktop® Advanced Logon

5. In the **Services configuration** screen, click on the **Configure AuthEngine** button. Then insert the received license in the form of XML, and click on the **Check License** button. If the check is passed, click on **Next** to continue.



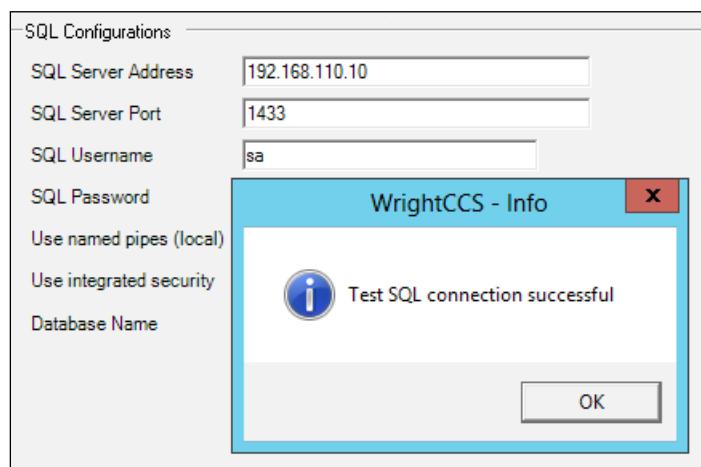
6. In the **AuthEngine Service User** section, specify a service account (**Local System**, **Local Service**, or **Network Service**), and then click on **Next** to continue.
7. Configure the network settings and the necessary **Active Directory** parameters, and then click on the **Next** button to continue.

The screenshot shows the 'Network Bindings' and 'Active Directory' configuration sections. Under 'Network Bindings', the 'AuthEngine Address' is set to '192.168.110.47' and the 'AuthEngine Port' is '9060'. Under 'Active Directory', the 'AD/LDAP Server' is '192.168.110.20', the 'AD/LDAP Query Account' is 'Administrator', the 'AD/LDAP Password' is masked, the 'AD/LDAP BaseDN' is 'DC=XDSEVEN,DC=local', and the 'AD/LDAP Container (optional)' and 'AD/LDAP Filter (optional)' fields are empty. A 'Test AD/LDAP Config' button is at the bottom.

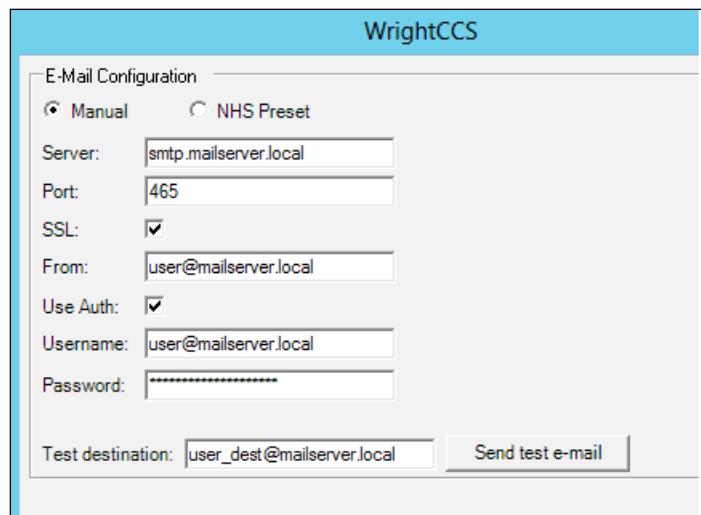


Click on the **Test AD/LDAP Config** button to ensure that you've correctly configured all the parameters.

8. In order to create the SMS2 database, insert the valid information to connect to a platform installed by SQL Server. After completing this step, click on **Test Connection** to ensure the validity of the data. Then click on **Next**.



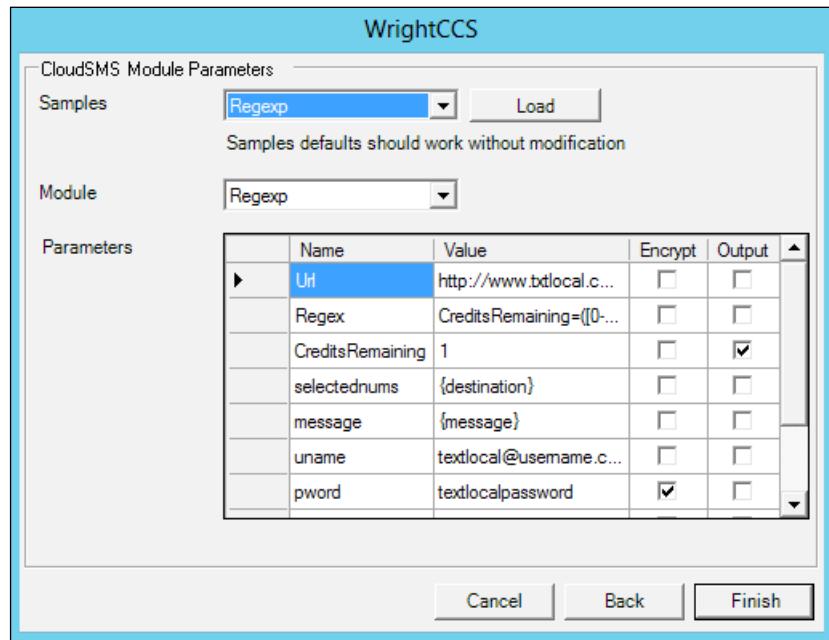
9. In the **E-Mail Configuration** section, specify a valid e-mail server and an e-mail account from which we will send the authentication token in the form of an e-mail. Click on the **Finish** button to complete the procedure.



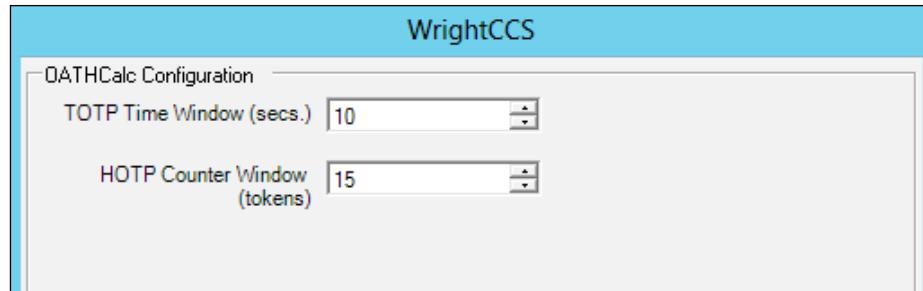


Type a valid destination e-mail address, and click on **Send test e-mail** to check the functionality of the mail server.

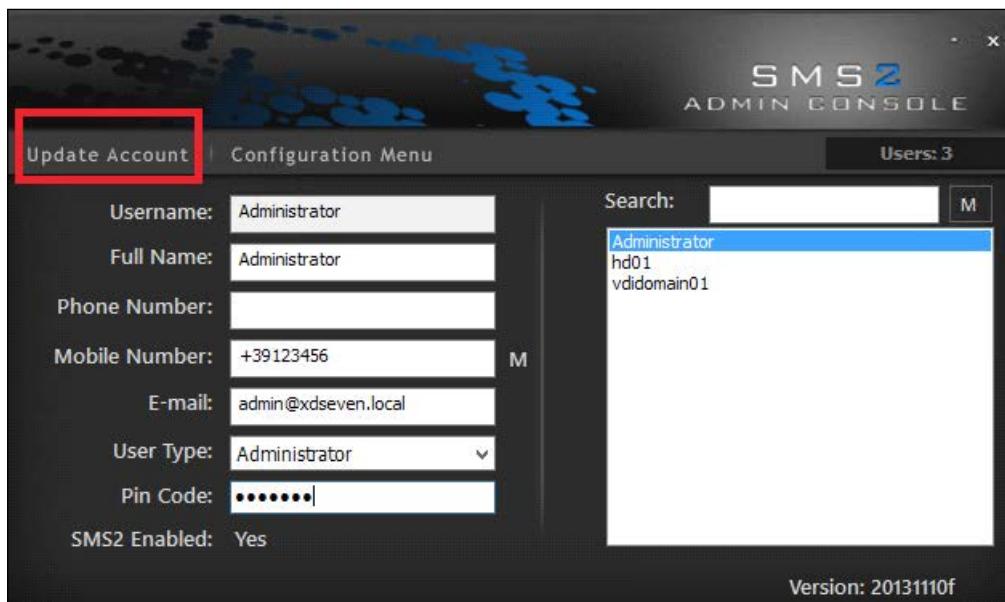
10. On the **Services Configuration** main menu, click on the **Configure CloudSMS** button. In the **CloudSMS Service User** section, configure a service account as performed earlier for the e-mail service. Click on **Next** to continue.
11. In the **CloudSMS Module Parameters** section, select an SMS provider from the drop-down list, click on the **Load** button, and select a valid module from the relative section. If necessary, modify the configured parameters in order to be able to send an SMS to the destination user's device. Click on **Finish** to complete the procedure.



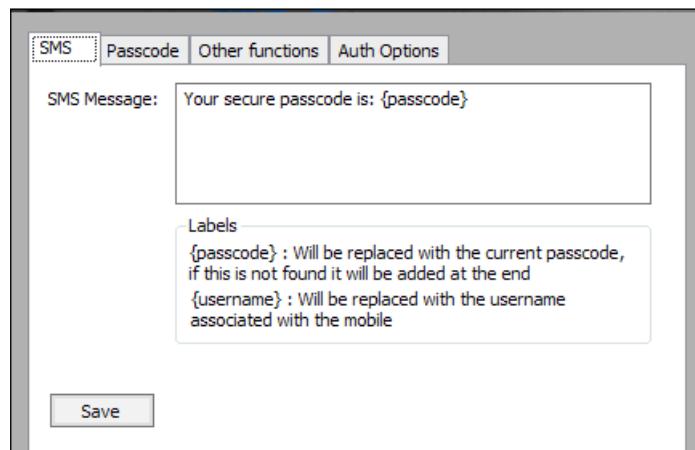
12. On the **Services Configuration** main menu, click on the **Configure OATHCalc** button. In the **CloudSMS Service User** section, configure a service account as seen earlier for the e-mail service. Click on **Next** to continue.
13. In the **OATHCalc Configuration** screen, configure the time settings and the number of tokens managed by the SMS2 Windows platform. Click on the **Finish** button to complete the configuration.



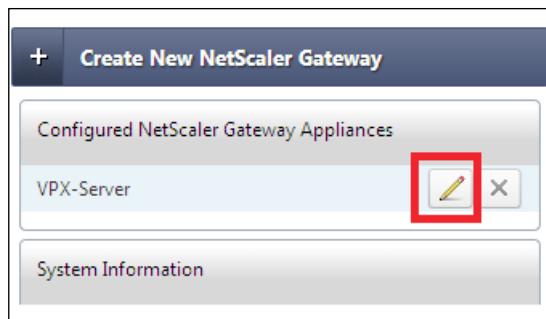
14. On the **Services Configuration** main menu, click on the **Configure AdminGUI/Clients** button. In the **Network Bindings** section, specify a valid IP address and port. Click on **Finish** to complete the procedure, and then click on **Next** to continue.
15. On the **Citrix Web Interface Directory** menu, click on **Next** to ignore the deprecation of the Citrix component configuration.
16. In the **Ready to install SMS2** section, click on **Install** to complete the procedure. Click on **Finish** when the procedure is complete.
17. Run the **SMS2 Administration Console** by searching for it within the Windows Apps catalog (press the Windows + C key combination, click on the **Search** button, and search for the SMS2 application).
18. After the console has been loaded, select a user and configure the missing data, such as **Mobile Number** or **Pin Code**. To maintain the updated information, click on the **Update Account** button.



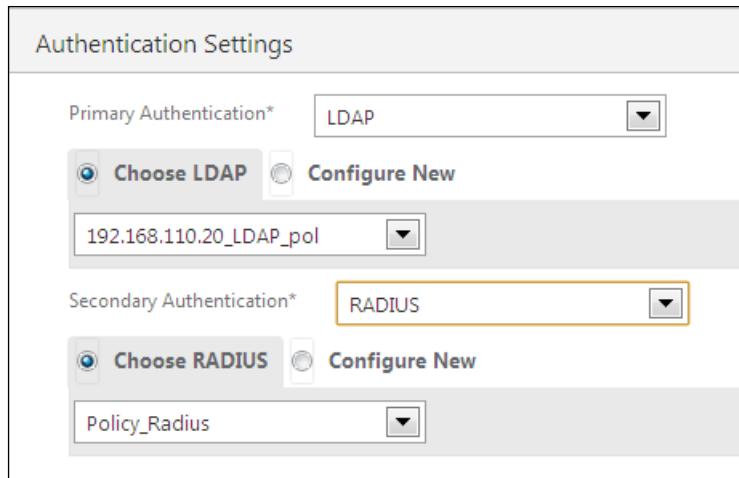
19. Click on the **Configuration Menu** link. On the **SMS** tab, configure the body of the message that will be sent to the user. Then click on **Save** to update the modified information.



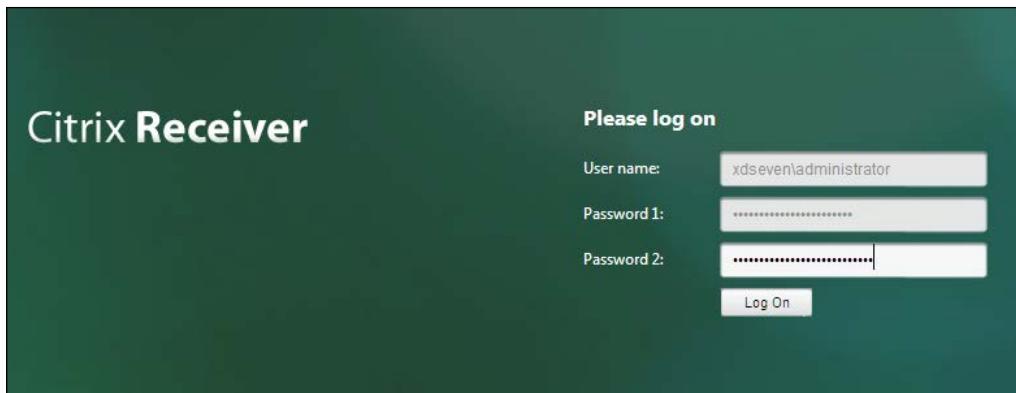
20. On the **Passcode** tab, configure the length of the software token sent to the users. Click on the **Save** button to update the modified parameter.
21. Open a compatible web browser. In the address bar, type the address that was previously assigned to the virtual NetScaler appliance.
22. Insert the web portal credentials (default: nsroot), select **NetScaler Gateway** as **Deployment Type** option, and click on the **Login** button to continue.
23. Edit **Configured NetScaler Gateway Appliances** by clicking on the edit icon on the right-hand side menu.



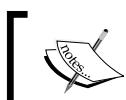
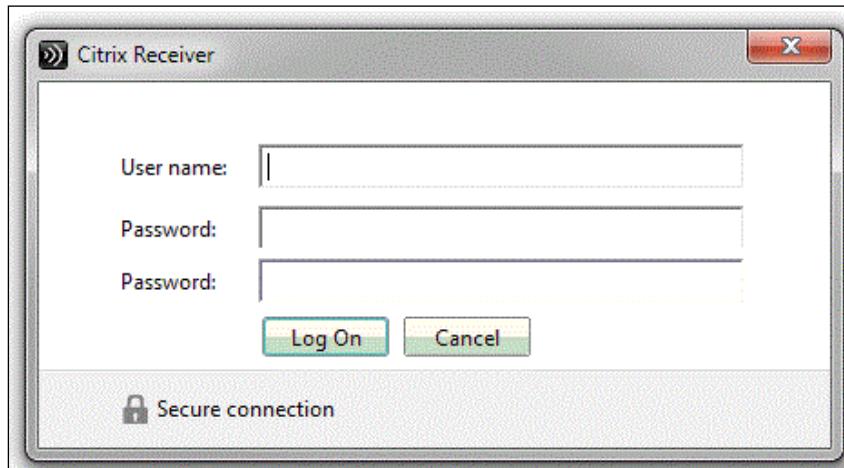
24. Click on the **Edit** button in the **Authentication Settings** section.
25. In the **Secondary Authentication** section, select the **RADIUS** option from the drop-down list and select the RADIUS server configured in the previous recipe, or add a new one by selecting the **Configure New** option. After completing these steps, click on the **Continue** button.



26. Log in to the user access address of your NetScaler platform. You'll find the second authentication factor added to the login web portal.



27. The same multifactor authentication will be possible with the help of Citrix Receiver, as indicated in the following screenshot:



Because we're using the SMS2 platform, the second password is the PIN assigned to the user by the SMS2 administration console.



How it works...

SMS2 is a free two-factor authentication platform that permits user authentication in a secure way to configure the Citrix XenDesktop infrastructure.

The process on which multifactor authentication platforms are based is quite simple. Together with the standard credentials (username/password) assigned to a specific user, a second authentication factor is added in order to make it difficult for malicious activities to succeed. This is similar to the Smart Cards / PKI tokens authentication, except for the fact that the second authentication factor is in the form of software code and not a hardware device.

The SMS2 software is based on this kind of architecture. The software, which is interacting with the required architectural components (an LDAP directory such as Microsoft Active Directory, a RADIUS platform, a SQL Server database, and an optional secure access gateway such as Citrix NetScaler), is able to associate the generated PIN codes to specific domain users. This code must be used as the second password to authenticate and use the published corporate resources, such as desktops and/or applications.

Additionally, it's also possible to configure a third authentication factor, OTP technology. This is a temporary code that must be combined with the user's PIN plus the password, and it can be in form of an e-mail message, proprietary token device, or SMS on your mobile phone.



The following proprietary—not free—alternatives to the SMS2 platform can be used:

- ▶ SafeNet OTP: <http://www.safenet-inc.com/data-protection/authentication/otp-authentication/>
- ▶ Symantec OTP: <https://www.symantec.com/verisign/vip-authentication-service>
- ▶ RSA OTP: <http://www.emc.com/security/rsa-securid.htm>

Together with the operations performed by the two-factor authentication platforms, there's the NetScaler Gateway. It is necessary to configure the existing RADIUS platform(s) to use it as a second factor authentication.

There's more...

With the SMS2 platform, it's possible to add a third authentication factor to logon, which will permit users to receive an e-mail or an SMS directly on their personal accounts or mobile devices. The users are prompted for the required code after the first logon phase, in which the standard credentials plus the associated PIN have been inserted.

To enable this configuration, edit the Configuration.xml file that is located at C:\Program Files\WrightCCS2\Settings by default, and set the following XML parameters:

- ▶ <AuthEngineChallengeResponse>True</AuthEngineChallengeResponse>
- ▶ <AuthEnginePinCodeTokenSeparated>True</AuthEnginePinCodeTokenSeparated>



In order to apply the modified parameters, you have to restart the **Wright AuthEngine** service.

In this way, users will be prompted to type the third factor authentication. In the case of wrong credentials on the first login step with the second specified parameters, the logon process will be stopped instead of proceeding anyway with the request of the OTP.

See also

- ▶ The *Installing and configuring Citrix® NetScaler Gateway 10.1* recipe in Chapter 8, *XenDesktop® Tuning and Security*

Index

Symbols

.cr extension 37

A

Active Directory accounts

managing 324-327

Active Directory Identity cmdlets 323

Add-AcctADAccount command 328

Add-HypHostingUnitStorage cmdlet 341

Add-PSSnapin command 320

ADIdentity cmdlets 327

Adobe Flash Delivery subsection

about 269

Flash acceleration policy 269

Flash background color list policy 269

Flash backwards compatibility policy 270

Flash default behavior policy 270

Flash event logging policy 270

Flash intelligent fallback policy 270

Flash latency threshold policy 270

Flash server-side content fetching URL list policy 270

Flash URL compatibility list policy 270

AdsiEdit Microsoft tool

URL 155

Advanced settings subsection

about 285

Disable automatic configuration policy 285

Log off user if a problem is encountered policy 285

Number of retries when accessing locked files policy 285

Process internet cookie files on logoff policy 285

Application Delivery Group 244

applications

publishing, Microsoft App-V used 255-264

AppV cmdlets 333, 334

App-V Management Server 255

App-V Management System 255

App-V Sequencer 256

App-V Streaming Server 256

assigned machines

removing, from catalog 204

Audio subsection

about 270

Audio over UDP Real-time transport policy 270

Audio Plug N Play policy 270

Audio quality policy 271

Client audio redirection policy 271

Client microphone redirection policy 271

Auto client reconnect subsection

about 271

Auto client reconnect authentication policy 271

Auto client reconnect logging policy 272

Auto client reconnect policy 271

B

Background Intelligent Transfer Services (BITS) 95

Bandwidth subsection

about 272

Audio redirection bandwidth limit percent policy 272

Audio redirection bandwidth limit policy 272

Client USB device redirection bandwidth limit percent policy 272

Client USB device redirection bandwidth limit policy 272

Clipboard redirection bandwidth limit percent policy 272

Clipboard redirection bandwidth limit policy 272

COM port redirection bandwidth limit percent policy 272

COM port redirection bandwidth limit policy 272

File redirection bandwidth limit percent policy 272

File redirection bandwidth limit policy 272

HDX MediaStream Multimedia Acceleration bandwidth limit percent policy 272

HDX MediaStream Multimedia Acceleration bandwidth limit policy 272

LPT port redirection bandwidth limit percent policy 272

LPT port redirection bandwidth limit policy 272

Overall session bandwidth limit policy 273

Printer redirection bandwidth limit percent policy 273

Printer redirection bandwidth limit policy 273

TWAIN device redirection bandwidth limit percent policy 273

TWAIN device redirection bandwidth limit policy 273

bare-metal hypervisor 61

Basic settings subsection

- about 285
- Active write back policy 285
- Enable profile management policy 285
- Excluded groups policy 285
- Offline profile support policy 286
- Path to user store policy 286
- Processed groups policy 286
- Process logons of local administrators policy 286

Boot Device Manager feature 41

BYOD (Bring Your Own Device) 5

C

catalog

- assigned machines, removing from 204, 205
- machines, adding to 203, 204

catalog configuration, Remote PC Access 188-196

catalog configuration, Windows Desktop OS 183-186

catalog configuration, Windows Server OS 187, 188

CDF Trace 175, 178

Central Management Console 264

Certification Authority (CA) management

- about 163
- activities 163

Citrix® Desktop Controller

- managing 328-335

Citrix® Diagnostic Facility Trace. See CDF Trace

Citrix® Director platform

- using 208-216

Citrix® EdgeSight features 208

Citrix® Flexcast technique 7

Citrix® Licensing Services

- configuring 19-24
- installing 19-24
- working 24

Citrix® Netscaler Gateway 10.1

- configuring 298-308
- installing 298-308
- working 308-311

Citrix® Profile Management

- latest release, features 124

Citrix® Profile Management 5.0

- about 118
- used, for implementing profile architecture 118, 119

Citrix Receiver™

- about 143
- configuring 144-148

Citrix® Studio console 144

Citrix® XenDesktop® 267

Citrix XenDesktop® 7 architecture

- prerequisites 6

Citrix® XenDesktop® policies

- working 293, 294

Citrix® XenServer 152

Client Sensors subsection

- about 273
- Allow applications to use the physical location

- of the client device policy 273
- CloudBridge**
configurable approaches 173, 174
- CloudBridge platform**
configuring 164-173
- CloudBridge VPX** 165
- Command-line Interface (CLI)** 178
- components, XenDesktop®** 7
installing 25-29
- configuration, Citrix Licensing Services** 19-24
- configuration, Citrix® Netscaler Gateway** 10.1 298-308
- configuration, Citrix Receiver™** 144-148
- configuration, CloudBridge platform** 164-173
- configuration, desktop OS master image** 88-95
- configuration, master image policies** 111-115
- configuration, Merchandising Server** 152-161
- configuration, printers** 217-225
- configuration, Provisioning Services** 7 41-52
- configuration, server OS master image** 97-103
- Configuration Service cmdlets** 320
- configuration, StoreFront 2.0** 30-39
- configuration, target device** 103-110
- configuration, USB devices** 227-230
- configuration, Windows 7 master image** 88-91
- configuration, Windows 8 master image** 91-95
- configuration, XenDesktop®**
- for interaction, with Citrix® XenServer** 61-65
for interaction, with Microsoft Hyper-V 73-85
for interaction, with VMware vSphere 5.1 67-72
- configuration, XenDesktop® Collector** 175-178
- configuration, XenDesktop® logging** 312-316
- configuration, XenDesktop® policies** 267, 268
- configuration, XenDesktop® site** 56-60
- configured XenDesktop® catalog**
deleting 205
- content redirection** 245
- Cross-Platform settings subsection**
about 286
- Cross-platforms settings user groups policy 286
- Enable Cross-platforms settings policy 286
- Path to cross-platforms definitions policy 286
- Cryptographic Service Provider (CSP)** 359
- D**
- Delivery Group** 198
- desktop OS machine**
VDA, installing for 130, 131
- desktop OS master image**
configuring 88-95
optimizing 88-95
- Desktop UI subsection**
about 273
Desktop Composition graphics quality policy 273
Desktop Composition Redirection policy 273
Desktop wallpaper policy 273
Menu animation policy 273
View window contents while dragging policy 274
- Desktop Windows Manager (DWM) service** 95
- domain controller (DC)** 162
- Domain Group Policy Objects (Domain GPO)** 251
- Dynamic Windows Preview (DWP)** 293
- E**
- e-mail-based account discovery feature** 40
- EMF** 223
- End User Monitoring subsection**
about 274
ICA round trip calculation interval policy 274
ICA round trip calculation policy 274
ICA round trip calculations for idle connections policy 274
- Enhanced Desktop Experience subsection**
about 274
Enhanced Desktop Experience policy 274
- Enhanced Metafile Format (EMF)** 224
- existing machine catalog**
modifying 199-207

F

File Redirection subsection

- about 274
- Auto connect client drives policy 274
- Client drive redirection policy 274
- Client fixed drives policy 274
- Client floppy drives policy 274
- Client network drives policy 274
- Client optical drives policy 275
- Client removable drives policy 275
- Host to client redirection policy 275
- Preserve client drive letters policy 275
- Read-only client drive access policy 275
- Special folder redirection policy 275
- Use asynchronous writes policy 275

File system subsection

- about 286
- Directories to synchronize policy 286
- Exclusion list directories policy 286
- Exclusion list files policy 287
- Files to synchronize policy 287
- Folders to mirror policy 287

Flexcast approach 9

Folder redirection subsection

- about 287
- AppData (Roaming) path policy 287
- Contacts path policy 287
- Desktop path policy 287
- Documents path policy 287
- Download path policy 287
- Favorites path policy 287
- Grant administrator access policy 288
- Include domain name policy 288
- Links path policy 288
- Music path policy 288
- Pictures path policy 288
- Redirection settings for AppData (Roaming) policy 288
- Redirection settings for Contacts policy 288
- Redirection settings for Desktop policy 288
- Redirection settings for Documents policy 288
- Redirection settings for Downloads policy 288
- Redirection settings for Favorites policy 288
- Redirection settings for Links policy 288
- Redirection settings for Music policy 288

Redirection settings for Pictures policy 288
Redirection settings for Saved Games policy 288

Redirection settings for Searches policy 288
Redirection settings for Start Menu policy 289
Redirection settings for Videos policy 289
Saved Games path policy 289
Searches path policy 289
Start Menu path policy 289
Videos path policy 289

FreeRADIUS 362

Full Qualified Domain Name (FQDN) 21, 357

G

Get-BrokerDesktop command 335

Get-ConfigDBConnection command 322

Get-HypHypervisorPlugin command 341

Get-SfServiceStatus command 344

gpedit.msc command 360

Graphics subsection

- about 275
- Display memory limit policy 275
- Display mode degrade preference policy 275
- Dynamic Windows Preview policy 276
- Image caching policy 276
- Legacy graphics mode policy 276
- Maximum allowed color depth policy 276
- Notify user when display mode is degraded policy 276
- Persistent cache threshold policy 276
- Queuing and tossing policy 276

H

HDX Monitor

- about 135
- installing 135-140
- URL, for downloading software 135
- working 141, 142

Host and Machine Creation cmdlet 341

hosted applications

- about 234
- publishing 234-244

hosts

- administering 338-342

hypervisor environment 182

I

ICA section

- about 269
- ICA Listener connection Timeout policy 269
- ICA listener port number policy 269
- infrastructure security 349**
- installation, Citrix Licensing Services 19-24**
- installation, Citrix® Netscaler Gateway 10.1 298-308**
- installation, HDX Monitor 135-140**
- installation, master image policies 111-115**
- installation, Provisioning Services 7 41-52**
- installation, StoreFront 2.0 30-39**
- installation, VDA**
 - for desktop OS machine 130-132
 - for server OS machine 126-129
- installation, XenDesktop® 7 components 25-29**
- installation, XenDesktop® Collector 175-178**
- I/O boot storm phenomenon 8**
- IP Address Extraction configuration 373**

K

Keep Alive subsection

- about 276
- ICA keep alives policy 276
- ICA keep alive timeout policy 276

L

Load Management section

- about 284
- Concurrent logons tolerance policy 284
- CPU usage excluded process priority policy 284
- CPU usage policy 284
- Disk usage 284
- Maximum number of sessions policy 284
- Memory usage base load policy 284
- Memory usage policy 284

Local Access Apps (LAA)

- about 233, 246, 277
- publishing 246-254

Local App access subsection

- about 277
- Allow local app access policy 277

URL redirection black list policy 277
URL redirection white list policy 277

Local Area Network (LAN) 115

M

machine assignment

- modifying 202

Machine Catalog

- about 182
- creating 182-197
- managing 182-197

Machine Creation Service (MCS) 342

machines

- adding, to catalog 203, 204
- administering 338-342

Mapped IP Address (MIP) 308

master image policies

- configuring 111-115
- installing 111-115

Master Target Devices 52

MCS 7

MCS architecture

- about 6, 7
- implementing 8

Merchandising Server

- about 152
- configuring 152-161
- working 162, 163

Merchandising Server Administrator Console

- about 154

Microsoft App-V

- used, for publishing applications 255-264

Microsoft Internet Information Services (IIS) 7.0 6

Microsoft Roaming Profiles 118

Mobile Experience subsection

- about 277
- Automatic keyboard display policy 277
- Launch touch-optimized desktop policy 277
- Remote the combo box policy 277

msiexec command 24

Multimedia subsection

- about 277
- Limit video quality policy 277
- Multimedia conferencing policy 278
- Optimization for Windows Media multimedia

redirection over WAN policy 278
Use GPU for optimizing Windows Media multimedia redirection over WAN policy 278
Windows Media client-side content fetching policy 278
Windows Media Redirection Buffer Size policy 278
Windows Media Redirection Buffer Size Use policy 278
Windows Media Redirection policy 278

Multi-Stream Connections subsection
about 278
Audio over UDP policy 278
Audio UDP Port Range policy 278
Multi-Port Policy 278
Multi-Stream computer setting policy 279
Multi-Stream user setting policy 279

N

Naming Scheme 327
Naming Scheme Type 327
NetScaler Gateway 383
Netscaler IP Address (NSIP) 308
Network Policy Server (NPS) 362
New-AcctADAccount cmdlet 327
New-BrokerCatalog command 335
New-ProvScheme command 342
NFS (Network File System) 7

O

One Time Password (OTP) 362, 374

P

Package Accelerator 264
PCL 223
Personal vDisk
about 118
used, for implementing profile architecture 121
ping command 153
Policy Comparison 296
Policy Modelling 296, 297
policy templates 295
Pooled catalog 196

Port Redirection subsection
about 279
Auto connect client COM ports policy 279
Auto connect client LPT ports policy 279
Client COM port redirection policy 279
Client LPT port redirection policy 279

PowerShell Broker command
Access and assignment filtering rules
subsection 337
applications subsection 336
desktops and desktop groups subsection 335, 336
site and catalog subsection 335

printers
configuring 217-225

Print Server 217

Product ID (PID) 230

profile architecture
implementing 118-125

implementing, Citrix® Profile Management used 118, 119
implementing, Personal vDisk used 121
implementing, roaming profiles used 120

Profile Handling subsection
about 289
Delay before deleting cached profiles
policy 289
Delete locally cached profiles on logoff
policy 289
Local profiles conflict handling policy 290
Migration of existing profiles policy 290
Path to the template profile policy 290
Template profile overrides local profile
policy 290
Template profile overrides roaming profile
policy 290

profile technology
Citrix® Profile Management 125
local profile 125
Personal vDisk 125
roaming profile 125

Provisioning Services 7
configuring 41-52
installing 41-52

Provisioning Services architecture (PVS) 335

Proximity Printing 222

PS 223

Publish-ProvMasterVmImage command	342	Secure ICA minimum encryption level policy	
PVS		280	
about	7, 8		
working	52		
PVS architecture		sequencing	264
about	6, 103	Server limits subsection	
implementing	8	about	280
		Server idle timer interval policy	280
Q		server OS machine	
Quality of Service (QoS)	278	VDA, installing for	126-129
R		server OS master image	
RADIUS	349	configuring	97-103
RADIUS platform		optimizing	97-103
used, for implementing strong authentication		Service Principal Name (SPN)	52
for XenDesktop® 7	362-373	Session limits subsection	
Receiver section		about	280
about	291	Concurrent logon limit policy	280
Storefront account list policy	291	Disconnected session timer interval policy	
regedit command	254	280	
Registry subsection		Disconnected session timer policy	280
about	290	Session connection timer interval policy	281
Exclusion list policy	290	Session connection timer policy	281
Inclusion list policy	290	Session idle timer interval policy	281
Release ID (REL)	230	Session idle timer policy	281
Remote Authentication Dial In User Service.		Session Reliability subsection	
<i>See RADIUS</i>		about	281
Remote PC Access		Session reliability connections policy	281
catalog configuration	188-196	Session reliability port number policy	281
Remove-AcctADAccount command	327	Session reliability timeout policy	281
Remove-AcctIdentityPool cmdlet	324	Set-AcctIdentityPool command	
Remove-AcctIdentityPool command	327	about	324
Remove-BrokerAssignmentPolicyRule command	332	Set-BrokerAssignmentPolicyRule cmdlet	332
Rename-AcctIdentityPool command	327	Set-ConfigDBConnection command	322
roaming profiles		Set-ProvScheme cmdlet	340
used, for implementing profile architecture		shadowing	216
120		SmoothRoaming feature	280
S		SMS2	382
SAN(Storage Area Network)	7	SQL Server 2012 database	
SCVMM 2012 SP1	73	preparing	16-18
Secure Ticket Authority (STA)	304	StoreFront	7
Security subsection		StoreFront 2.0	
about	280	about	6, 30
		configuring	30-39
		installing	30-39
		working	40
		Streamed user profiles subsection	
		about	291
		Always cache policy	291
		Profile streaming policy	291

Streamed user profile groups policy 291
Timeout for pending area lock files (days)
 policy 291
streaming technology 264
strong authentication stages, XenDesktop®
 Enterprise Certification Authority and
 Enrollment Station 359
 StoreFront 360
 Web Server - IIS 8 360
Subnet IP Address (SNIP) 308
system information
 retrieving 320-322
system logging activities
 configurations, verifying 343-347
 managing 343-347

T

TAAS 178
target device
 configuring 103-110
Test-ConfigServiceInstanceAvailability
 cmdlet 323
thin virtual disk 196
Time zone control subsection
 about 281
 Estimate local time for legacy clients policy
 281
 Use local time of client policy 281
tracert command 153
TWAIN Devices
 about 282
 Client TWAIN device redirection policy 282
 TWAIN compression level policy 282
two-factor hardware authentication
implementing, for XenDesktop® 7 350-359
two-factor software authentication
implementing, for XenDesktop® 7 374-383

U

USB devices
 configuring 227-229

V

valid certificates utilization
 configuration tasks 350

VDA
 installing 126
 installing, for desktop OS machine 130-132
 installing, for server OS machine 126-129
 working 132-134
VDI architecture 87, 117, 151
Vendor ID (VID) 230
VHDMountPoint 125
Virtual Appliance 152
Virtual Delivery Agent Settings section
 about 291
 Enable auto update of controllers policy 291
 Enable lossless policy 291
 HDX3DPro quality settings policy 291
Virtual Desktop Agent (VDA) plugin 178, 182
Virtual Desktop Infrastructure. *See VDI architecture*
virtual desktop machines
 updating 199-201
virtual desktops 7
Virtual IP Address (VIP) 308
Visual Display subsection
 about 282
 Extra color compression policy 282
 Extra color compression threshold policy 282
 Heavyweight compression policy 282
 Lossy compression level policy 282
 Lossy compression threshold value policy
 282
 Minimum image quality policy 282
 Moving image compression policy 282
 Progressive compression level policy 282
 Progressive compression threshold value
 policy 282
 Target frame rate policy 283
 Target minimum frame rate policy 283
 Visual quality policy 283

W

WAN optimizer 164
WebSockets subsection
 about 283
 WebSockets connections policy 283
 WebSockets port number policy 283
 WebSockets trusted origin server list policy
 283

Windows 8 machine
configuring, as target device 103-110
Windows Desktop OS
catalog configuration 183-186
Windows machines
operating system configurations, applying for
improving responsiveness 97
Windows Server operating systems 244
Windows Server OS
catalog configuration 187, 188
Write-Host command 322

X

XenDesktop®
configuring, for interaction with Citrix®
XenServer 61-65
configuring, for interaction with Microsoft
Hyper-V 73-85
configuring, for interaction with VMware
vSphere 5.1 67-72
stages, for strong authentication 359, 360
XenDesktop® 5.6
upgrading, to XenDesktop® 7 9-14
XenDesktop® 7
about 5, 151
strong authentication, implementing with
RADIUS platform 362-373
two-factor hardware authentication, imple-
menting for 350-359
two-factor software authentication, imple-
menting for 374-382
XenDesktop® 5.6, upgrading to 9-14
XenDesktop® 7 components
installing 25-29
XenDesktop® Collector
about 175
configuring 175-178
installing 175-178
XenDesktop® logging
configuring 312-316
XenDesktop® policies
configuring 267, 268
XenDesktop® site
configuring 56-60
XenServer 61
XPS 223



Thank you for buying Citrix® XenDesktop® 7 Cookbook

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, which focuses on producing quality, cutting-edge books for communities of developers, administrators, and newbies alike. For more information, please visit our website: www.PacktPub.com.

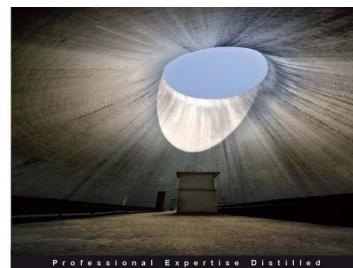
About Packt Enterprise

In 2010, Packt launched two new brands, Packt Enterprise and Packt Open Source, in order to continue its focus on specialization. This book is part of the Packt Enterprise brand, home to books published on enterprise software – software created by major vendors, including (but not limited to) IBM, Microsoft and Oracle, often for use in other corporations. Its titles will offer information relevant to a range of users of this software, including administrators, developers, architects, and end users.

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, 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.



Getting Started with Citrix XenApp 6.5

Design and implement Citrix farms based on XenApp 6.5

Guillermo Musumeci

[PACKT] enterprise
PUBLISHING

Getting Started with Citrix XenApp 6.5

ISBN: 978-1-84968-666-2 Paperback: 478 pages

Design and implement Citrix farms based on XenApp 6.5

1. Use Citrix management tools to publish applications and resources on client devices with this book and eBook
2. Deploy and optimize XenApp 6.5 on Citrix XenServer, VMware ESX, and Microsoft Hyper-V virtual machines and physical servers
3. Understand new features included in XenApp 6.5 including a brand new chapter on advanced XenApp deployment covering topics such as unattended install of XenApp 6.5, using dynamic data center provisioning, and more



Citrix XenApp Performance Essentials

A practical guide for tuning and optimizing the performance of XenApp farms using real-world examples

Luca Dentella

[PACKT] enterprise
PUBLISHING

Citrix XenApp Performance Essentials

ISBN: 978-1-78217-044-0 Paperback: 126 pages

A practical guide for tuning and optimizing the performance of XenApp farms using real-world examples

1. Design a scalable XenApp infrastructure
2. Monitor and optimize server performance
3. Improve end user experience
4. Tune the farm for WAN connections
5. Real world examples, ready-to-use suggestions, and best practices

Please check www.PacktPub.com for information on our titles



Getting Started with Citrix VDI-in-a-Box

Design and deploy virtual desktops using Citrix VDI-in-a-Box

Stuart Arthur Brown

[PACKT] enterprise publishing

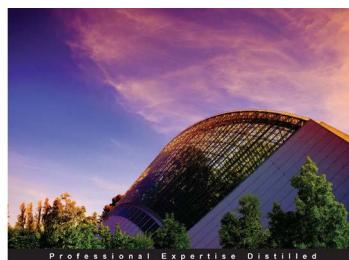
Getting Started with Citrix VDI-in-a-Box

ISBN: 978-1-78217-104-1

Paperback: 86 pages

Design and deploy virtual desktops using Citrix VDI-in-a-Box

1. Design a Citrix VDI-in-a-Box solution
2. Get the budget for Citrix VDI-in-a-Box by building a case
3. Implement a Citrix VDI-in-a-Box proof of concept and Citrix VDI-in-a-Box solution



Citrix Access Gateway VPX 5.04 Essentials

A practical step-by-step guide to provide secure remote access using the Citrix Access Gateway VPX

Andrew Mallett

[PACKT] enterprise publishing

Citrix Access Gateway VPX 5.04 Essentials

ISBN: 978-1-84968-822-2

Paperback: 234 pages

A practical step-by-step guide to provide secure remote access using the Citrix Access Gateway VPX

1. A complete administration companion guiding you through the complexity of providing secure remote access using the Citrix Access Gateway 5 virtual appliance
2. Establish secure access using ICA-Proxy to your Citrix XenApp and XenDesktop hosted environments
3. Use SmartAccess technology to evaluate end users' devices before they connect to your protected network

Please check www.PacktPub.com for information on our titles