Quick answers to common problems

Over 40 engaging recipes that will help you implement a full-featured XenDesktop® 7.6 architecture and its main satellite components

Citrix XenDesktop® Cookbook
Third Edition
Gaspare A. Silvestri

This book will help you understand how to implement, configure, and optimize migration from a physical to a VDI architecture, moving from a standard application approach to a centralized and more secure way to assign and release resources to the end users.

The book begins with the upgrade and installation procedures for the core infrastructural components, along with an explanation of how to deploy and optimize procedures for desktop virtual machines. Moving on, you will perform desktop and applications deployment through the XenDesktop core plus integrated publishing platforms, such as Microsoft App-V.

Finally, the book explains how to install and configure important collateral platforms such as the NetScaler, CloudBridge, and XenMobile platforms, along with the execution of the most advanced activities and configurations.

Who this book is written 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. Experience of the virtualized environment and an understanding of the general concepts of desktop virtualization (VDI) are required.

What you will learn from this book

- Configure and deploy virtual machines for XenDesktop 7.6
- Perform configuration and optimization operations for desktop and server OS images for future deployments
- Execute desktop environment administration tasks, including catalog creation, power management, and resource allocation
- Understand how to publish the hosted applications, Local Access Apps (LAA), and applications using Microsoft App-V
- Work with PowerShell to reduce the time required to perform management tasks with the creation of the PowerShell scripts
- Implement the two-factor hardware and software authentication for XenDesktop
- Install and configure NetScaler Gateway 10.5 and XenMobile 10 to improve the quality, performance, and manageability of your Virtual Desktop Infrastructure (VDI) architecture

In this package, you will find:

- The author biography
- A preview chapter from the book, Chapter 7 'XenDesktop® Infrastructure Tuning'
- A synopsis of the book’s content
- More information on Citrix XenDesktop® Cookbook Third Edition
Gaspare A. Silvestri is an IT specialist with 10 years of experience in the information technology market. During his career, he covered a set of different infrastructural roles, including the important role of CTO for an ICT company, based in Italy. He considers his job to be the most enduring of all his passions, with a particular preference in the areas of virtualization and Unix.

He is always curious and in search of new IT projects on which he performs his research activities.

Gaspare has been involved in the design, tuning, and consolidation of physical and virtual infrastructures for the important system integration companies that are based in Italy.

Gaspare is also the author of Citrix XenDesktop 5.6 Cookbook and Citrix® XenDesktop® 7 Cookbook, published by Packt Publishing.
Introduction

The way to work is changing. Jobs and workplaces are evolving; tasks can be accomplished anytime, anywhere, and from any device, thanks to the evolution of technologies and higher network connectivity levels.

In the era of mobile and BYOD (Bring your own Device), Citrix® has still improved its products in terms of integration, performance, usability, and user experience. Moving a step forward in this market by powering its desktop and application virtualization platforms, Citrix® integrates the ability to publish virtual and physical desktops with the ability to assign applications and content in a secure manner, with all the products strongly focused on the mobile and mobility markets. This is XenDesktop® 7.6.

In this book, we will discuss the evolution of the XenDesktop® platform, discussing how implementing and optimizing the new mobile world-oriented features is done. Also, we will learn how separating personal data from company working spaces is achieved by using a personal device. We will discuss the changes in the component's releases, such as StoreFront™ or NetScaler®, plus integrating the practical steps of the XenMobile® and the EMM (Enterprise Mobility Management) platforms provided by Citrix®.

After reading this book, readers will be able to understand how to implement a full XenDesktop® 7.6 architecture from its core components to its satellite features, which will allow them to receive a stronger user experience with an improved security of the personal information.
What this book covers

Chapter 1, *XenDesktop® 7.6 – Upgrading, Installation, and Configuration*, will discuss in detail the way to upgrade to the latest release from the previous XenDesktop versions for both the MCS and PVS architectures. Moreover, we will install and configure the main platform components, such as the database (the Microsoft SQL Server 2012 platform), StoreFront™, and the Licensing Services.

Chapter 2, *Configuring and Deploying Virtual Machines for XenDesktop® 7.6*, will show you how to interface XenDesktop® with hypervisor's hosts for Farm and the 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*, is focused on the configuration and optimization operations that are realized on the base desktop, server, or the physical workstation images for future deployments.

Chapter 4, *User Experience – Planning and Configuring*, will discuss how to implement the profile management techniques, the virtual desktop agent versions (Server, Desktop, and the Remote PC), and the main version of the Citrix Receiver™ component (agent and HTML5 agentless).

Chapter 5, *Creating and Configuring a Desktop Environment*, will perform the implementation and optimization activities for the infrastructural satellite components, such as Citrix Merchandising Server™ or the CloudBridge™ platform.

Chapter 6, *Deploying Applications*, will explain in detail how to deploy and migrate applications with the integrated XenApp® platform: the Hosted applications, the Local Access App, Microsoft App-V, and the AppDNA® platform.

Chapter 7, *XenDesktop® Infrastructure Tuning*, will perform optimization activities to enrich the quality level of the VDI with the use of the XenDesktop® policies and printers.

Chapter 8, *XenDesktop® Component Integration*, will explain the setup and the configuration phases of the main infrastructural Citrix® components that are required to enrich the XenDesktop® offering (CloudBridge®, NetScaler Gateway®, and XenMobile®).

Chapter 9, *Working with PowerShell*, will be an advanced guide to Powershell modules. With these, we will realize the high level configurations by using the command line.

Chapter 10, *Configuring the XenDesktop® Advanced Logon*, will explain the operations to implement the secure and strong authentication for the XenDesktop® 7 architecture.
In this chapter, we will cover the following recipes:

- Configuring the XenDesktop policies
- Configuring printers
- Configuring USB devices
- Configuring the XenDesktop logging

**Introduction**

XenDesktop offers a modular architecture in which both security and user experience are important options to consider and balance. Citrix provides best practice documents to deliver a VDI solution that the end user likes to work with. Citrix products permit you a deeper protection and avoid performance issues by enabling the right policies.

During this chapter, we will discuss the configuration of the XenDesktop infrastructural policies, the capability to regulate the use of external devices such as printers and removable storage devices, and the way to configure the logging of the activities performed on the XenDesktop infrastructure.
Configuring the XenDesktop® policies

Now that the XenDesktop infrastructure has been configured, it is time to activate and populate the Virtual Desktop Infrastructure policies. This is an extremely important part of the implementation process because, with them, you can regulate the resource use and assignment, but you will also improve the general virtual desktop performance.

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 to enable and use the configuration rules.

How to do it...

In the following steps we will explain the configuration for the user and machine policies offered by XenDesktop:

1. Connect to the Delivery Controller server with an administrative domain user.
2. Run 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 menu, and then select Create Policy in the right-hand panel.
4. In the **Categories** menu, click on the following sections and configure the values for the policies that will be applied to the clients:

**ICA section**
- **ICA Listener connection timeout**: Insert a value in milliseconds—default 12000.
- **ICA listener port number**: 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, values can be either set as **Enabled** or **Disabled**. With this policy, you can decide whether to enable the rendering of the Flash contents on the client side, only in legacy mode.

  By enabling this policy, you have the ability to reduce the network usage 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 that your client supports this feature.
Flash background color list: Specify a set of colors to apply 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, values can either be set as Enabled or Disabled. With this policy you can choose to 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, respectively enabling the most recent Citrix for Flash features (including the client-side processing), permitting only server-side processed contents, or blocking any Flash content. In this policy, values can either be set as follows:

- Enable Flash acceleration
- Disable Flash acceleration
- Block Flash player

Flash event logging: In this policy, values can be either Enabled or Disabled. Decide whether to create system logs for the Adobe Flash events.

Flash intelligent fallback: In this policy, values can be either Enabled or Disabled. This policy, if enabled, activates the server-side Flash content processing when the client-side Flash content is not required.

Flash latency threshold: This policy specifies a value, in milliseconds, to apply as a maximum latency threshold. The default value is 30 milliseconds.

Flash server-side content fetching URL list: This policy specifies a list of web URLs for which Flash contents can be downloaded to the server and then be sent to the client devices.

Consider using this policy when the Internet connection is not present on the client devices.

Flash URL compatibility list: This policy specifies a list of rules, for a specific web URL, to render Flash content on the client side, on the server side, or to block any rendering.

The Flash Redirection feature has been strongly improved starting from the 5.5 version of XenDesktop.

Audio subsection

Audio over UDP real-time transport: This policy can either be set as 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 to transmit. UDP should be better in terms of performance and bandwidth consumption.
Audio Plug N Play: In this policy, values can be set as either Allowed or Prohibited to allow or prohibit the ability to use multiple audio devices.

Audio quality: The values can be set as Low, Medium or High. These parameters depend on a compromise between the quality of the network connections and the audio level, and they respectively cover the low-speed connections, optimized for speech, and high-definition audio cases.

Client audio redirection: The values can be set as either 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, values can be either Allowed or Prohibited. This policy permits you to map client microphone devices to use within a desktop session.

Try to reduce the network and load impact of the multimedia components and devices where the high user experience is not required.
Auto Client Reconnect subsection

- **Auto client reconnect**: The values *Allowed* or *Prohibited* specify whether to automatically reconnect a broken connection from a client.

- **Auto client reconnect authentication**: The values *Do not require authentication* or *Require authentication* decide whether the Citrix infrastructure should request your credentials every time you have to reperform a login operation.

- **Auto client reconnect logging**: In this policy, values can be set as 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 case of active auto client reconnect, you should also activate its logging.

Bandwidth subsection

- **Audio redirection bandwidth limit**: In this policy, insert a value in Kbps to set the maximum bandwidth assigned to playing and recording audio activities.

- **Audio redirection bandwidth limit percent**: In this policy, a maximum percentage value to play and record audio can be inserted.

- **Client USB device redirection bandwidth limit**: Insert a value in Kbps to set the maximum bandwidth assigned to the USB devices redirection.

- **Client USB device redirection bandwidth limit percent**: In this policy, insert a maximum percentage value for the USB devices redirection.

- **Clipboard redirection bandwidth limit**: In this policy, a value in Kbps can be inserted to set the maximum bandwidth assigned to the clipboard traffic from the local client to the remote session.

- **Clipboard redirection bandwidth limit percent**: Insert a maximum percentage value for the clipboard traffic from the local client to the remote session.

- **COM port redirection bandwidth limit**: Insert a value in Kbps to set the maximum bandwidth assigned to the client COM port-redirected traffic.

- **COM port redirection bandwidth limit percent**: In this policy, insert a maximum percentage value for the client COM port-redirected traffic.

- **File redirection bandwidth limit**: Insert a value in Kbps to set the maximum bandwidth assigned to the client drives redirection.

- **File redirection bandwidth limit percent**: Insert a maximum percentage value for the client drives redirection.

- **HDX MediaStream Multimedia Acceleration bandwidth limit**: Insert 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**: Insert a maximum percentage value for the multimedia contents redirected through the HDX MediaStream acceleration.
LPT port redirection bandwidth limit: Insert a value in Kbps to set the maximum bandwidth assigned to the client LPT port-redirected traffic.

LPT port redirection bandwidth limit percent: Insert a maximum percentage value for the client LPT port-redirected traffic.

Overall session bandwidth limit: Specify a value in Kbps for the total bandwidth assigned to the client sessions.

Printer redirection bandwidth limit: Insert a value in Kbps to set the maximum bandwidth assigned to access a client printer.

Printer redirection bandwidth limit percent: Insert a maximum percentage value to access a printer in a client device session.

TWAIN device redirection bandwidth limit: Insert a value in Kbps to set the maximum bandwidth assigned to a TWAIN scanner device.

TWAIN device redirection bandwidth limit percent: Insert a maximum percentage value to access TWAIN imaging.

In the presence of both bandwidth limit and bandwidth limit percent enabled policies, the most restrictive value will be used.

Client Sensors subsection

Allow applications to use the physical location of the client device – Values: Allowed or Prohibited. With this policy you can permit applications to use the physical location of a client device.

Desktop UI subsection

Desktop Composition graphics quality: In this policy, values can be set as 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, values can be set as either Enabled or Disabled. This policy permits use of the Desktop Composition from the Virtual Desktop Agent to the client device.

By enabling this policy, users will obtain a richer user experience. You cannot apply it to delivered Server OS instances.

Desktop wallpaper: In this policy, values can be set as either Allowed or Prohibited. Through this policy you can permit use of the desktop wallpaper in your session. Disable this policy if you want to standardize your desktop deployment.
Menu animation: In this policy, values can be either **Allowed** or **Prohibited**. This policy permits use of the animated menu of the Microsoft operating systems. The choice depends on what kind of performances you need for your desktops.

View window contents while dragging: In this policy, values can be set as either **Allowed** or **Prohibited**. This policy gives you the ability to see the entire window contents during the drag-and-drop activities between windows, if enabled. Otherwise, you will see only the window's border.

**End User Monitoring subsection**

- **ICA round trip calculation**: In this policy, values can be set as either **Enabled** or **Disabled**. Through this policy you can permit enabling calculation of the ICA network traffic time.
- **ICA round trip calculation interval**: Insert the time interval in seconds for the period of the round trip calculation.
- **ICA round trip calculations for idle connections**: In this policy, values can be set as **Enabled** or **Disabled**. You can decide whether to enable the round trip calculation for connections that are not performing traffic. Enable this policy only if necessary.

**The Enhanced Desktop Experience subsection**

- **Enhanced Desktop Experience**: In this policy, values can be set as **Allowed** or **Prohibited**. This policy, applicable only to the Server OS instances, enriches the machine graphical experience in a published desktop session, making the user experience near to the client device operating system.

**File Redirection subsection**

- **Auto connect client drives**: In this policy, values can be either set as **Enabled** or **Disabled**. With this policy the local drives of your client either will or won't be automatically connected at the logon time.
- **Client drive redirection**: In this policy, values can be set as either **Allowed** or **Prohibited**. With the drive redirection it is possible to permit saving files locally on the client machine drives.
- **Client fixed drives**: In this policy, values can be set as **Allowed** or **Prohibited**. This policy permits reading data from, and saving information to, the fixed drives of your client machine.
- **Client floppy drives**: In this policy, values can be set as **Allowed** or **Prohibited**. This policy permits reading data from, and saving information to, the floppy drives of your client machine. This should be allowed only in presence of an existing floppy drive, otherwise it has no value to your infrastructure.
- **Client network drives**: In this policy, values can be set as **Allowed** or **Prohibited**. With this policy you have the possibility to map the remote network drives from your client.
Chapter 7

- **Client optical drives**: In this policy, values can be set as **Allowed** or **Prohibited**. With this policy, you can enable or prevent the access to the optical client drives, such as CD-ROM or DVD-ROM.

- **Client removable drives**: In this policy, values can be set as **Allowed** or **Prohibited**. This policy allows or prohibits mapping in order to read and save removable drives from your client, such as USB keys.

- **Host to client redirection**: In this policy, values can be set as **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, values can be set as **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, values can be set as **Enabled** or **Disabled**. Enabling this policy will not permit accessing in write mode, the mapped client drivers. By default, this policy is disabled, to permit full drive access. To reduce the impact on client security, you should enable it, then modify when necessary.

> These are powerful policies 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, values can be set as **Allowed** or **Prohibited**. Allowing the policy will point the Desktop and Documents user's folders to the client's directories. On the other case, they will point the host locations.

- **Use asynchronous writes**: In this policy, values can be set as **Enabled** or **Disabled**. Allows enabling of the asynchronous data disk writes. By default, they are disabled.

> You should enable this latest 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 to assign to the video buffer for a session. This policy only applies to the deployed Server OS desktops.

- **Display mode degrade preference**: In this policy, values can be set as **Degrade color depth first** or **Degrade resolution first**. Configure a parameter to lower the resolution or the color quality in case of graphic memory overflow.
Dynamic Windows Preview: The values are either Enabled or Disabled. With this policy, you have the ability to turn on the high-level preview of the open windows on the screen.

Image caching: In this policy, values can be either Enabled or Disabled. With this parameter, you can cache images on the client to obtain a faster response.

Legacy graphics mode: In this policy, values can be 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 degrading the graphic quality.

Maximum allowed color depth: In this policy, values can be 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.

The higher the color depth, the higher the memory usage.

Notify user when display mode is degraded: The values are 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 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 reused images.

Queueing and tossing: In this policy, values are either Enabled or Disabled. By enabling this policy you can stop the processing of images being replaced by other pictures.

In the presence of slow or WAN network connections, you should create a separate policy group, which reduces the display memory size, configures the Degrade color depth policy, activates the image caching, and removes the advanced Windows graphical features.

Keep Alive subsection

ICA keep alive timeout: Insert a value in seconds to configure the keep alive timeout for the ICA connections.

ICA keep alive: This policy includes the values Do not send ICA keep alive messages or Send ICA keep alive messages. Configure if you want to send keep alive signals for the running sessions.
Local App Access subsection

- **Allow local app access:** In this policy, values can be set as *Allowed* or *Prohibited*. This policy permits the use of the LAA within your environment.

- **URL redirection black list:** In this policy, specify a set of web URLs to run on the physical client device, out of your VDI resources.

- **URL redirection white list:** In this policy, specify a set of web URLs to run within your assigned VDI resources.

We have already discussed the LAA in *Chapter 6, Deploying Applications*.

Mobile Experience subsection

- **Automatic keyboard display:** In this policy, *Allowed* or *Prohibited* values allow you to automatically display the display keyboard on mobile devices. This policy is disabled by default.

- **Launch touch-optimized desktop:** In this policy, values are either *Allowed* or *Prohibited*. This policy will permit you to use or disable the execution of an optimized mobile touch-pad version.

- **Remote the combo box:** In this policy, values are *Allowed* or *Prohibited*. This policy will configure the type of combo boxes to use on your device: allow it to use the Windows combo box version on any device, such as iOS, or prohibit the use of the native combo box version.

Multimedia subsection

- **Limit video quality:** Choose the video quality level of the HDX connections from the following options:
  - Not Configured
  - Maximum Video Quality 1080p/8.5Mbps
  - Maximum Video Quality 720p/4Mbps
  - Maximum Video Quality 480p/720Kbps
  - Maximum Video Quality 380p/400Kbps
  - Maximum Video Quality 240p/200Kbps

The level of the HDX quality should always be configured based on the speed of your network connection.
Multimedia conferencing: In this policy, values can be set as either Allowed or Prohibited. This policy permits the use of video conferencing applications, in terms of webcam device use and office communicator software support.

Optimization for Windows Media multimedia redirection over WAN: In this policy, values are either Allowed or Prohibited. If allowed, this policy permits Windows media content compression over a WAN connection.

Use GPU for optimizing Windows Media multimedia redirection over WAN: In this policy, values can be set as either 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, values are either Allowed or Prohibited. When allowed, this policy permits client devices 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 this last policy. The Windows Media Redirection policy configured to Allowed is a prerequisite to use the client-side content fetching policy.

Windows Media Redirection: The values set as either Allowed or Prohibited decide whether to redirect the multimedia execution on the Citrix server(s) and then stream it to clients.

Windows Media Redirection Buffer Size: Insert a value, in seconds, for the buffer used to deliver multimedia contents to clients.

Windows Media Redirection Buffer Size Use: The values can be set as either Enabled or Disabled. This policy lets you use the previously configured media buffer size.

Multi-Stream Connections subsection

Audio over UDP: The values can be set as either Allowed or Prohibited. This policy, where allowed, permits opening a UDP port on which to transfer the audio media for a client.

Audio UDP Port Range: This policy specifies a port range for the UDP connections used to stream audio data. The default range is 16500-16509.

Multi-Port Policy: This policy configures the traffic shaping to implement the QoS (Quality of Service). You have to specify from two to four ports and assign them a priority level.
- **Multi-Stream computer setting**: The values can be set as Enabled or Disabled. Decide whether to activate the Multi-Stream ports previously configured, on the server side.

- **Multi-Stream user setting**: The value set as Enabled or Disabled decides whether to activate the Multi-Stream feature for specific users.

To be able to use the Multi-Stream user setting, you need to activate the **Multi-Stream computer setting** policy.

### Port Redirection subsection

- **Auto connect client COM ports**: The values can be set as Enabled or Disabled. If enabled, this policy automatically maps the client COM ports.

- **Auto connect client LPT ports**: The values can be either Enabled or Disabled. This policy auto connects the client LPT ports, if enabled.

- **Client COM port redirection**: The values can be set as Allowed or Prohibited. This policy configures the COM port redirection between the client and the remote session.

- **Client LPT port redirection**: The values can be set as Allowed or Prohibited. This policy configures the LPT port redirection between the client and the remote session.

You only have to enable the necessary ports, so disable the policies for the missing COM or LPT.
Security subsection

- **Secure ICA minimum encryption level**: This configuration permits assigning an encryption level to data sent between the client and the server during a XenDesktop session. This policy only applies to Server OS instances. The values can be set as:
  - Basic
  - RC5 (128 bit) log on only
  - RC5 (40 bit)
  - RC5 (56 bit)
  - RC5 (128 bit)


- **Server idle timer interval**: This policy specifies a value in milliseconds to set the interval on which to maintain active idle sessions (no input from users). This policy only applies to Server OS instances.

Session Limits subsection

- **Concurrent logon limit**: This policy specifies a numeric value to set the maximum number of connections made by a single user. This policy only applies to Server OS instances.

- **Disconnected session timer**: The values can be set as **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 the **Smooth Roaming** feature: this is a term for making user's 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 can only be less than the configured disconnected time.

- **Disconnected session timer interval**: Insert a value in minutes that will be used as a counter reference value to log off locked workstations. Base this parameter on a real inactivity time for your company employers.

- **Session connection timer**: The values can be set as **Enabled** or **Disabled**. This policy will permit using 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 (1440 minutes).

Session idle timer: The values can be set as Enabled or Disabled. If enabled, this policy will disconnect a client session after a certain amount 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 (1440 minutes).

Session Reliability subsection

Session reliability connections: The values can be set as Allowed or Prohibited. By enabling this policy, you permit the sessions to remain active in case of network problems, permitting users to see the content of published desktops or applications, such as a screenshot of the last state, while the network issues are restored, keeping the session active.

Session reliability port number: This policy specifies the port used by ICA to check the reliability of incoming connections. The default port is 2598.

Session reliability timeout: This policy specifies 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 have been activated. They cannot be enabled together.

Time zone control subsection

Estimate local time for legacy clients: The values can be set as Enabled or Disabled. If enabled, this policy will try to estimate the client time zone, in case of a lack of information. This can be only applied to Server OS instances.

Use local time of client: The values can be set as 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 client or server-configured time zone.

TWAIN Devices subsection

Client TWAIN device redirection: The values can be set as Allowed or Prohibited. If enabled, this policy permits mapping existing TWAIN image devices, as scanners, for example.

TWAIN compression level: The values can be set as None, Low, Medium, or High. With this policy, you can specify the compression level for transferred media files from client to server.
Visual Display subsection

- **Extra color compression**: The values can be set as *Enabled* or *Disabled*. If enabled, the global image quality level will be reduced to obtain a faster responsiveness.

- **Extra color compression threshold**: Insert a value in Kbps to specify a threshold for the color compression execution.

- **Heavyweight compression**: The values can be set as *Enabled* or *Disabled*. Based on a CPU consuming algorithm, this policy, if enabled, will apply a progressive data compression, reducing the global bandwidth. It can be only used by the Citrix Receiver.

- **Lossy compression level**: The values can be set as *None*, *Low*, *Medium*, or *High*. This policy should only be used when the quality level for the images is not important, because of the compression applied to the graphical data.

- **Lossy compression threshold value**: Insert a value in Kbps to specify a threshold for the lossy compression policy application.

- **Minimum image quality**: The values can be set as *Low*, *Normal*, *High*, *Very High*, or *Ultra High*. This policy specifies the quality level to apply to the images display. The higher the level, the higher the resource consumption.

- **Moving image compression**: *Enabled* or *Disabled*. When enabled, this policy activates the adaptive display feature – the ability to adjust automatically the quality graphics levels based on the available bandwidth.

- **Progressive compression level**: The values can be set as *None*, *Low*, *Medium*, *High*, *Very High*, or *Ultra High*. This policy sets a lossy compression-related quality image level, starting from a less detailed and faster display.

  The value of the progressive compression level must be higher than the lossy compression policy, as mandatory configuration.

- **Progressive compression threshold value**: 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 not to go under this fps parameter, in the presence of bandwidth problems.

- **Visual quality**: The values can be set as *Low*, *Medium*, *High*, *Build to Lossless*, or *Always Lossless*. These parameters configure the quality level for the image visualization; the higher the level, the higher the bandwidth usage. This policy only applies to Desktop OS instances.
The **Always Lossless** option gives more importance to the image quality, and the **Build to Lossless** parameter either decreases or increases the image quality based on the network and resources usage level.

### WebSockets subsection

- **WebSockets connections**: The values can be set as **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 specifying the WebSockets protocol port number for incoming connections. The default value is **8008**.
- **WebSockets trusted origin server list**: In this case, it is possible to specify a list of trusted server's URLs as valid WebSockets platforms. By default, all the servers are included in this list, by the use of a wildcard (***）.

![WebSockets trusted origin server list](image)

---

### Load Management section

- **Concurrent logons tolerance**: The values can be set as **Enabled** or **Disabled**. When enabled, this policy permits you to specify the number of maximum concurrent log ons for a XenDesktop server site. This policy can only be applied to Server OS instances.
- **CPU usage**: The values can be set as **Enabled** or **Disabled**. When enabled, this policy configures the percentage CPU usage threshold considered as a maximum load for the XenDesktop server. This policy can only be applied to Server OS instances.
- **CPU usage excluded process priority** – Values: **Enabled** or **Disabled**. Enable or disable the consideration of the global server CPU usage for the system background processes, including, when disabled, their resource consumption in the global load calculation. This policy can only be applied to Server OS instances.
Disk usage: The values can be set as Enabled or Disabled. When enabled, this policy lets you configure the disk queue length at which to consider the global disk usage at 75% of load. This policy can only be applied to Server OS instances.

This policy permits an understanding of 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: The values can be set as Enabled or Disabled. When enabling this policy, you can specify the maximum number of sessions per single XenDesktop server. This policy can only be applied to Server OS instances.

Memory usage: The values can be set as Enabled or Disabled. By enabling this policy, you can configure the memory usage percentage value considered as full load for the server. This policy can only be applied to Server OS instances.

Memory usage base load: The values can be set as Enabled or Disabled. By enabling this policy, you can tune the zero load parameter in MB, to use as a threshold for the server load calculation. This policy can only be applied to Server OS instances.

Following is the explanation for the subsections included in the Profile Management section:

Advanced settings subsection

- Disable automatic configuration: The values can be set as Enabled or Disabled. With this policy, you can decide whether to activate the automatic configuration for the Profile Management, based on the environment configuration.

- Log off user if a problem is encountered: The values can be set as Enabled or Disabled. If enabled, in case of problems during the logon phase, the user will be prompted with an alert, then 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 log off: The values can be set as Enabled or Disabled. This policy, when enabled, removes any unnecessary web cookies after a session logoff.

Basic settings subsection

- Active write back: The values can be set as 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 users log off.
- **Enable profile management**: The values can be set as **Enabled** or **Disabled**. By enabling this policy, you can decide whether to activate the logon and logoff processes for the Citrix Profile Management.

- **Excluded groups**: The values can be set as **Enabled** or **Disabled**. When enabled, this policy permits you to exclude specific domain groups from the Profile Management processing.

- **Offline profile support**: The values can be set as **Enabled** or **Disabled**. Enable this policy to permit using profiles even when disconnected from the network.

- **Path to user store**: The values can be set as **Enabled** or **Disabled**. Enable this policy and specify the network path on which profiles are located, to use the Citrix Profile Management.

We have discussed the Citrix Profile Management and the path to user store in the Using Citrix Profile Management 5.x recipe in Chapter 4, User Experience – Planning and Configuring.

- **Process logons of local administrators**: The values can be set as **Enabled** or **Disabled**. This policy processes, if respectively enabled or disabled, profile members of the local administrators' machine group.

- **Processed groups**: The values can be set as **Enabled** or **Disabled**. When enabled, this policy permits you to specify domain groups that must be processed by the Citrix Profile Manager.
Cross-Platform Settings subsection

- **Cross-platforms settings user groups**: The values can be set as **Enabled** or **Disabled**. If enabled, the cross-platform parameter of the Citrix Profile Management will only be applied to the specified domain groups.

- **Enable cross-platforms settings**: The values can be set as **Enabled** or **Disabled**. With this policy, you can turn on or off the cross-platform option for the Citrix Profile Management software.

- **Path to cross-platforms definitions**: The values can be set as **Enabled** or **Disabled**. In case of an enabled policy, you have to specify a valid network path on which to locate the cross-platform definition files.

- **Path to cross-platforms settings store**: The values can be set as **Enabled** or **Disabled**. In case of an enabled policy, you have to specify a valid network path on which to save the user's cross-platform settings.

File System subsection

- **Directories to synchronize**: The values can be set as 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 user profiles.

- **Exclusion list – directories**: The values can be set as either **Enabled** or **Disabled**. Enable this policy and specify a list of folders to exclude during the profile synchronization activities.

- **Exclusion list – files**: The values can be set as either **Enabled** or **Disabled**. Enable this policy and specify a list of files to exclude during the profile synchronization activities.

- **Files to synchronize**: The values can be set as 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 user profiles.

- **Folders to mirror**: The values can be set as either **Enabled** or **Disabled**. Enable this policy and list a set of folders to replicate in mirror mode.

  This policy is useful when critical profile data need having not only a single existing file.

Folder Redirection subsection

- **AppData(Roaming) path**: The values can be set as either **Enabled** or **Disabled**. If enabled, this policy will let you specify a network path on which to redirect AppData folders. If disabled, the specified folder will not be redirected. This is for Roaming Profile configurations.
Contacts path: The values can be set as either Enabled or Disabled. Enable this policy and specify a network location path on which to redirect the Contacts directory. If disabled, the specified folder will not be redirected.

Desktop path: The values can be set as either Enabled or Disabled. Enable this policy and specify a network location path on which to redirect the Desktop directory. If disabled, the specified folder will not be redirected.

Documents path: The values can be set as either Enabled or Disabled. Enable this policy and specify a network location path on which to redirect the Documents directory. If disabled, the specified folder will not be redirected.

Download path: The values can be set as either Enabled or Disabled. Enable this policy and specify a network location path on which to redirect the Download directory. If disabled, the specified folder will not be redirected.

Favorites path: The values can be set as either Enabled or Disabled. Enable this policy and specify a network location path on which to redirect the Favorites directory. If disabled, the specified folder will not be redirected.

Grant administrator access: The values can be set as either Enabled or Disabled. If enabled, you can configure the ability for administrators and users to access the redirected folder's contents. By default, only users can access their own redirected folders.

Include domain name: The values can be set as either Enabled or Disabled. This policy permits including (when enabled) the %userdomain% variable in the UNC path.

Links path: The values can be set as either Enabled or Disabled. Enable this policy and specify a network location path on which to redirect the Links directory. If disabled, the specified folder will not be redirected.

Music path: The values can be set as either Enabled or Disabled. Enable this policy and specify a network location path on which to redirect the Music directory. If disabled, the specified folder will not be redirected.

Pictures path: The values can be set as either Enabled or Disabled. Enable this policy and specify a network location path on which to redirect the Pictures directory. If disabled, the specified folder will not 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.

All the Redirection settings policies by default are configured as "Redirect to the following UNC path". You can specify a precious path on the next set of policies.

Saved Games path: The values can be set as either Enabled or Disabled. Enable this policy and specify a network location path on which to redirect the Saved Games directory. If disabled, the specified folder will not be redirected.

Searches path: The values can be set as either Enabled or Disabled. Enable this policy and specify a network location path on which to redirect the Searches directory. If disabled, the specified folder will not be redirected.

Start Menu path: The values can be set as either Enabled or Disabled. Enable this policy and specify a network location path on which to redirect the Start Menu directory. If disabled, the specified folder will not be redirected.

Videos path: The values can be set as either Enabled or Disabled. Enable this policy and specify a network location path on which to redirect the Videos directory. If disabled, the specified folder will not be redirected.

Later in this chapter we will discuss the Logging policies applied to the XenDesktop infrastructure.
Profile Handling subsection

- **Delay before deleting cached profiles**: Configure a value, in seconds, as a delay for the cached profile deletion after a session logoff.

- **Delete locally cached profiles on log off**: The values can be set as **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 to **Use local profile**, **Delete local profile** or **Rename local profile**.

  Choosing the renaming of the local profile permits you to back it up, and then use the centralized profiles. This is useful for rollback actions.

- **Migration of existing profiles**: In this policy, values can be set as **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 log on.

- **Path to the template profile**: The values can be set as either **Enabled** or **Disabled**. This policy, when enabled, allows you to specify a network path on which to save and locate a user profile template, which will be used for any profile creation operation.

- **Template profile overrides local profile**: In this policy, values can be 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 (second case)—**local profile**—on the computer used for the first log on.

- **Template profile overrides roaming profile**: In this policy, the values can be set as 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 (second case)—**Microsoft Roaming profile**—on the computer used for the first log on.

Registry subsection

- **Exclusion list**: The values can be set as either **Enabled** or **Disabled**. Enabling this policy will let you specify a set of registry keys—`HKEY_CURRENT_USER` section—to ignore during the logon phase.
Inclusion list: The values can be set as Enabled or Disabled. Enabling this policy will let you specify a set of registry keys—HKEY_CURRENT_USER section—to process 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:** The values can be set as either Enabled or Disabled. With this policy, you can decide whether to always cache data with streamed profiles. If enabled, the global limit of the cached files will be lower in size.
- **Always cache:** Assign a value to the cache area size, which will be associated to the Always cache policy.
- **Profile streaming:** In this policy, values are set as either Enabled or Disabled. By 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 folders are only when accessed by users.
- **Streamed user profile groups:** The values can be set as Enabled or Disabled. If enabled, this policy will permit you to insert a list of domain groups containing users to configure as streamed profiles.
- **Timeout for pending area lock files (days):** Assign a value, in days, after which user's locked pending files are rolled back to the user store, instead of being written to the destination server.

Receiver section

- **StoreFront account list:** Insert a list of StoreFront-configured locations with the following syntax:
  
  StoreName;StoreURL;StoreState(Value=On/Off);StoreDescription

  A configuration example for the previous policy could be the following: MyCompany;https://companysf01.xdseven.local/Citrix/Store/discovery;On;"Company store"
Virtual Delivery Agent Settings section

- **Enable auto update of controllers**: This policy has values either **Enabled** or **Disabled**. If enabled, you can apply a list of XenDesktop Controllers to the initial bootstrap connection; if disabled, you will manage them manually.

- **Enable lossless**: In this policy, values can be set as either **Enabled** or **Disabled**. This policy either allows or prohibits the use of lossless codec.

- **HDX 3D-Pro quality settings**: This policy configures the minimum and maximum quality level for the 3D-Pro codec. The permitted values are between 0 and 100, and the maximum level must be greater than the minimum.

After configuring all the policies perform the following steps

1. Click the **Next** button to continue.
2. In the **Users and Machines** section, choose whether to apply the configured policies to specific users and/or computer, or assign them to all the site's objects. After completion, click the **Next** button.
3. 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.

![Summary section](image)

**How it works...**

The 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 applying them to different virtual desktop's configurations.

By using the **ICA settings**, you are able to configure the standard ICA port on which to listen and the relative connection timeouts. It's possible to decide whether to automatically reconnect a broken session to a client. (**Auto client reconnect** policy: enabling this policy could be the right solution in some cases, especially when you have interrupted an important working session; on the other hand, the Citrix Broker could run a new session in the presence of issues with the session cookies. So, activate it based on your priorities.)
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 that involve graphic 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 problems with 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. Therefore, you should consider disabling this policy, thereby demanding the processing of audio and video to the clients, only when you can see no particular benefits.

Another important feature offered by this policy is the QoS (Quality of Service) implementation: you can enable the Multi-Stream Connections configurations and apply them to the traffic priority levels, permitting precedence and more bandwidth to traffic considered more critical than others.

The Multi-Stream policies for the Quality of Service can be considered a less powerful alternative to the CloudBridge platform. You could also use them together, for a better, more powerful, user experience.

Other important configurations are, for instance, the Adobe Flash contents processing, deciding whether to activate compatibility with the oldest version of this software, and whether 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 (when 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: by this, you can assign, in the form of maximum Kbps or percentages, the values for the following traffic types: **Audio**, **USB**, **Clipboard**, **COM**, and **LPT ports**, and **File redirection**. These configurations require a good analysis of 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, removable or not, such as CD-ROM or DVD-ROM, removable USB devices and fixed drives as the client device operating system root. This option gives you the flexibility to transfer information from the local device to the XenDesktop instance, by the Virtual Desktop Agent properly configured. You should consider deactivating all the redirects that are not really needed, in order to save the bandwidth.

This last device policy could make your infrastructure more secure, thanks to the use of the USB device redirection rules; through it, in fact, you could only permit the use of USB keys approved by your company, prohibiting any other non-policy-compliant device.

In this version of XenDesktop, the **Mobile Experience** policies are also really important: we have seen, in fact, that we are able to configure and use an optimized version of the touch interface for devices such as tablets or smartphones, enriching the user experience on this category of devices.

**There's more...**

Within XenDesktop 7.6, not only can you 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 for the site's parameters:

**Policy templates**

With this feature, you can use a preconfigured group of policies, which 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 application, in the presence of a high level of network and elaboration resources.

- **High Server Scalability**: This preconfigured policy fits 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**: This preconfigured policy is for remote workers with offices connected over 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, improving the global security level, but degrading also the available bandwidth because of the high network usage.

You can convert your own customized policies in a template to reuse for future purposes. In the Policy section, click the **Save as Template** link on the right-hand menu.
**Policy comparison**

With this feature, you can compare two or more templates and/or policies, in order to verify the current applied options, and also check the eventual redundant configurations.

**Policy modeling**

To verify the effective running and applied policies to your VDI infrastructure, there is a tool inside the HDX Policy menu that performs this task—the **Citrix Group Policy Modeling Wizard**. This tool performs a simulation for the policy applications, providing you with 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 of the Domain Controllers configured within your domain, being able to test the application to specific user or computer objects, including the OU containing them.
Moreover, you can apply filters based on the **Client IP address**, the **Client name**, the type of machine (**Private** or **Shared Desktop**, **Private** or **Shared Application**), or apply the simulation to a specific **Desktop group**.

In the **Advanced Options** section, you can simulate **Slow network connections** and/or **Loopback processing** (a policy application only based 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.
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

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 the use of printers. In this recipe, we are going to discuss these kinds of policies.

Getting ready

Depending on your company's requirements, you should have many different printers (network, local, multifunctional...) to configure within the virtual desktop environment. In most cases, a prerequisite (and a best practice) is configuring a Print Server on which we install all the devices and then deploy them using the Microsoft domain GPO.

You can install the required drivers for the printer that will be used on the Master Image; as you have already seen, in this way, you will propagate printer mapping to all the desktop instances in the pool.

Note that printers need to be RDS (Remote Desktop Services) compliant.

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 run 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 drop-down 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)
The following screenshot shows the available options while configuring the printer:

[Select settings screenshot]

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**.

7. On the **Summary** screen, assign a name to the generated policy, flag the **Enable policy** option, and click on **Finish**.
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**: With this policy, you decide whether to auto-create all the listed categories by default, or one of them, including local attached printers. You can also configure to not automatically operate on the creation of the printers. The options available are:
  - Auto-create all client printers
  - Auto-create local (non-network) client printers only
  - Auto-create the client's default printer only
  - Do not auto-create client printers

- **Auto-create generic universal printer**: This policy can be set as either Enabled or Disabled. With this policy, you can decide whether 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**: This policy can be set as either Enabled or Disabled. With this policy, you can decide whether to enable the automatic installation for the in-box printer Windows 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**: In this policy, the options available are **Standard printer names** or **Legacy printer names**. This policy permits you to choose the naming convention to use in each phase of 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**: In this policy, either Allowed or Prohibited option can be selected. Allowed by default, this policy permits you to redirect to a server the client printer mapping.

- **Default printer**: In this policy, we can choose either **Set default printer to the client's main printer** or **Do not adjust the user's default printer** option. With this policy, you can configure the way in which it chooses the default user printer. The first option uses the current configured printer as the default device, and the second loads the printer from the user profile instead, 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.
XenDesktop® Infrastructure Tuning

- **Direct connections to print servers**: In this policy, there are either **Enabled** or **Disabled** options. With this configuration, you can permit user access directly to the network printer, in order for faster printing. This is only available in LAN connections. In the case of WAN printer mappings, you have to use a non-direct connection.

- **Printer assignments**: This policy permits you to specify a list of client and default assigned printers and the session printer, by specifying one for each client machine.

- **Printer auto-creation event log preference**: This policy gives us options to **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 not to log any events, warnings or errors only, or both.

- **Printer driver mapping and compatibility**: With this policy, you can import a set of printer drivers on which to operate and 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**: This policy lets you decide if and where to save the configured printer settings. You should consider saving these settings in the user profile, especially in the presence of a centralized profile manager, and a non-persistent desktop machine. In this policy we have the following options:
  - Held in profile only if not saved on the client
  - Retained in user profile only
  - Saved on the client device only
  - Do not retain printer properties

- **Retained and restored client printers**: In this policy, we can choose either the **Allowed** or **Prohibited** option. In the case of customized printer configurations, you can have the ability to maintain these settings and restore them in case of configuration problems.

- **Session printers**: This policy permits you to add the list of network printers that can be autocreated with XenDesktop. You have to specify the printer UNC path when adding the network resource.
Universal driver preference: By the use of this policy, you can choose the order the Universal Printer drivers are used, such as EMF, PCL in its different versions, XPS or PS.

Universal print driver usage: This policy manages the situation of whether to use the universal printer driver. By default, this driver is used only when a specific driver is not available. The following options are available in this policy:

- Use only printer model specific drivers
- Use universal printing only
- Use universal printing only if requested driver is unavailable
- Use printer model specific drivers only if universal printing is unavailable

Universal Print Server enable: This policy, disabled by default, configures the use of the Universal Print Server feature. In case of a 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 particularly useful in the presence of a networked printing environment. It is 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 the 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: This policy lets us choose either Spool directly to printer or Reprocess EMFs for printer option. This policy checks the way to process the Enhanced Metafile Format (EMF) spooling queue (EMF is a device-independent format able to intercept the graphical elements in a printing task).

Universal printing image compression limit: This is an important policy that allows you to configure the quality level of the printed images, deciding whether to give precedence to the quality or to the compression level. It provides us the following options:

- No compression
- Best quality (lossless compression)
- High quality
- Standard quality
- Reduced quality (maximum compression)
XenDesktop® Infrastructure Tuning

**Universal printing optimization defaults**: This policy permits you to configure the image quality and compression to apply to the Universal Printer session. It lets us choose from the following options:

- **Best quality (lossless compression)**
- **High quality**
- **Standard quality**
- **Reduced quality (maximum compression)**

The following screenshot shows the options available in compression of images:

![Image Compression](image.png)

**Universal printing preview preference**: With this configurable option, you can enable the preview for the documents to print, by configuring one of the options listed in the next screenshot:

![Universal printing preview preference](image2.png)

Specifies whether to use the print preview function for auto-created or generic universal printers. By default, print preview is not used for auto-created or generic universal printers.
Universal printing print quality limit: This policy permits you to configure the resolution for the generated printing jobs. This policy provides the following options:

- No Limit, Draft (150 DPI)
- Low Resolution (300 DPI)
- Medium Resolution (600 DPI)
- High Resolution (1200 DPI)

Wait for printers to be created (desktop): In this policy, the options are either Enabled or Disabled. With this parameter, you can decide whether to wait for the printer creation process when connecting with your user profile. You cannot 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 the 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 http://support.citrix.com/article/CTX109374
XenDesktop® Infrastructure Tuning

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 will 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 the XenDesktop® policies recipe in Chapter 7, XenDesktop® Infrastructure Tuning.

Configuring USB devices

When making a decision about the migration from physical to virtual desktop infrastructure, the managers and IT technicians should always consider maintaining a high operational level for their users, such as an 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 looking 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 a Citrix Receiver on the endpoints 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 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 drop-down 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 give the virtual desktop to the USB device (**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 interact with it.

How it works...

With the USB device 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 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 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 are 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 corporation (http://www.usb.org/home) to find all the required information about the vendor and product IDs of USB devices.

**See also**

- The Configuring the XenDesktop® policies recipe in Chapter 7, XenDesktop® Infrastructure Tuning.

### Configuring the XenDesktop® logging

Any operation performed on a system, automatically or manually executed by the users, should be registered in a log file in order to troubleshoot problems and be able to reconstruct the activities for any kind of reason— for instance in case of security or legal checks. In this recipe, we will discuss the main logging activities performed by the 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 to 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. Run 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 menu, then select Create Policy in the right-hand panel or edit an existing one.
4. In the **Categories** menu, select the **Log settings** section, and configure the following policies:

- **Active Directory actions**: This policy can be set as either **Enabled** or **Disabled**. If enabled, this policy will log all the domain-related events, in relation with the profile management activities.

- **Common information**: This policy provides option to be 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**: This policy can be set as 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**: This policy provides the option to be either **Enabled** or **Disabled**. If enabled, this policy will activate the verbose logging, also known as debug mode.

- **File system actions**: This policy can be set as 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**: This policy provides the option to be either **Enabled** or **Disabled**. If enabled, this policy will log all the operations applied to the filesystem(s) in a verbose manner.

- **Log off**: This policy can be set as either **Enabled** or **Disabled**. If enabled, this policy will activate verbose logging for the user logoff operations.

- **Log on**: This policy provides option to be either **Enabled** or **Disabled**. If enabled, this policy will activate verbose logging for the user logon operations.

- **Maximum size of the log file**: Insert a value in bytes as a maximum size for the log file. 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 log file will be generated.

- **Path to log files**: This policy provides the option to be either **Enabled** or **Disabled**. With this policy, you can specify, if enabled, a particular network path on which to create the log files; if disabled, the default path will be used (%SystemRoot%\System32\LogFiles\UserProfileManager)

- **Personalized user information**: This policy can be set as either **Enabled** or **Disabled**. If enabled, this policy will log all the user information customizations in a verbose manner.
- **Policy values at log on and log off**: This policy provides the option to be 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**: This policy can be set as either **Enabled** or **Disabled**. If enabled, this policy will activate verbose logging for the operations on the registry during user sessions.

- **Registry differences at log off**: This policy provides the option to be either **Enabled** or **Disabled**. If enabled, this policy will log in a verbose manner all the changes applied to the registry during user sessions, when a user performs a log off from the assigned resource.

5. After completing the required configurations, save the policy changes, as seen earlier in this chapter.

6. By clicking on the **Logging** link in the left-hand menu, you will be prompted with a list of operations performed in the last activity times.

<table>
<thead>
<tr>
<th>Administrator</th>
<th>Main task</th>
<th>Start</th>
<th>End</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>XDEVEN/Administrator</td>
<td>Update HDX Policies</td>
<td>9/9/2013: 17:41.29</td>
<td>9/9/2013: 17:41.32</td>
<td>Successful</td>
</tr>
<tr>
<td>XDEVEN/Administrator</td>
<td>Create Application 'Notepad++'</td>
<td>27/10/2013: 02:57.41</td>
<td>27/10/2013: 02:58.20</td>
<td>Successful</td>
</tr>
<tr>
<td>XDEVEN/Administrator</td>
<td>Remove Machine Configuration '&lt;' from Deste...</td>
<td>27/10/2013: 02:47.58</td>
<td>27/10/2013: 02:47.58</td>
<td>Successful</td>
</tr>
<tr>
<td>XDEVEN/Administrator</td>
<td>Delete Application 'Notepad++'</td>
<td>27/10/2013: 02:47.29</td>
<td>27/10/2013: 02:47.39</td>
<td>Successful</td>
</tr>
<tr>
<td>XDEVEN/Administrator</td>
<td>Update Application 'Notepad++'</td>
<td>27/10/2013: 02:36.36</td>
<td>27/10/2013: 02:36.52</td>
<td>Successful</td>
</tr>
<tr>
<td>XDEVEN/Administrator</td>
<td>Update Application 'Notepad++'</td>
<td>27/10/2013: 02:33.58</td>
<td>27/10/2013: 02:34.19</td>
<td>Successful</td>
</tr>
</tbody>
</table>

7. Click on the **Preferences** link in the right-hand menu, then configure whether to enable or disable the logging of administrative tasks, and also whether to modify the database on which logs are stored. After completion, click the **OK** button.

```
Configuration Logging

□ Disable
○ Enable

Logging database (where configuration logs are stored)
  Database size: 0
  Server location: sql\Database\Server\scheven.local\CITRIX_M.34
  Database name: CitrixXDF-Site-First

Security:
▪ Allow changes when the database is disconnected
  Administrators can make untrusted changes.
```

287
8. Click on the **Create Custom Report** link in the right-hand menu and select the date range for which to generate the required report. After selecting it, click on the **Next** button.

![Date Range Form]

9. In the **Format and Location** section, specify whether to save the report in CSV format, HTML format or both, then give a valid path location on which to create the report file. After completion, click on **Next**.

![Format and Location Form]

10. In the **Summary** screen, click on the **Finish** button to complete the report-generation procedure.
Chapter 7

How it works...

The XenDesktop logging discussed in this chapter can be divided into two different major areas: the first, configured under the XenDesktop Policies section, configures all the logging parameters for the user profile components, especially in the presence of the configured Citrix Profile Management.

These policies are particularly useful in situations where the changes to the deployed desktop also need to be logged: 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 could be tracked and intercepted, for instance.

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 administrators and delegated users for the XenDesktop 7 infrastructure. The logs can also be exported in .csv format (useful as source data to reimport on other data collections, such as external databases or spreadsheets), or in HTML format, which will give you a formatted and human-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 menu and, when prompted, choose a valid location on which to archive data before their cancellation.

Before performing the log deletion, you will be prompted to log in with administrative credentials on the site database on which logs are stored.
Logs can be saved in .csv or .txt formats.

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 HDX Monitor recipe in Chapter 4, User Experience – Planning and Configuring
Where to buy this book

You can buy Citrix XenDesktop® Cookbook Third Edition from the Packt Publishing website.

Alternatively, you can buy the book from Amazon, BN.com, Computer Manuals and most internet book retailers.

Click here for ordering and shipping details.